Schriften zum IT-Sicherheitsrecht 4

Christoph Werner

Die Resilienz als neue Anforderung des Rechts der Daten- und IT-Sicherheit

Eine Untersuchung anhand der exemplarischen Betrachtung kritischer, personalisierter Dienste

Nomos

Schriften zum IT-Sicherheitsrecht

Herausgegeben von

Prof. Dr. Gerrit Hornung
Prof. Dr. Ralf Poscher
MinDir a.D. Martin Schallbruch
Prof. Dr. Tobias Singelnstein
Prof. Dr. Gerald Spindler
Prof. Dr. Louisa Specht-Riemenschneider
Prof. Dr. Indra Spiecker gen. Döhmann

Band 4

Christoph Werner

Die Resilienz als neue Anforderung des Rechts der Daten- und IT-Sicherheit

Eine Untersuchung anhand der exemplarischen Betrachtung kritischer, personalisierter Dienste

Nomos

Dissertation an der rechtswissenschaftlichen Fakultät
der Albert-Ludwigs-Universität Freiburg

Dekan:	Prof. Dr. Jan Lieder, LL.M. (Harvard)
Erstgutachter:	Prof. Dr. Thomas Dreier, M.C.J.
Zweitgutachter:	Prof. Dr. Jens-Peter Schneider
Mündliche Prüfung:	08.-09.07.2024
Dissertationsort:	Freiburg im Breisgau
Erscheinungsjahr:	2025

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Freiburg im Breisgau, Univ., Diss., 2024

1. Auflage 2025

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-0144-6
ISBN (ePDF): 978-3-7489-4752-3

DOI: https://doi.org/10.5771/9783748947523

Onlineversion
Nomos eLibrary

Für Leonie und Henri

Vorwort

Diese Untersuchung zur Resilienz im Recht der Daten- und IT-Sicherheit entstand in einer Zeit großen Wandels nicht zuletzt auch in der digitalen Entwicklung. Eine tendenziell zunehmend kritische Lage in der Daten- und IT-Sicherheit, neue digitale Produkte wie KI-basierte Chatbots und Bildgenerierungswerkzeuge sowie eine gesellschaftlich als auch rechtlich zunehmend bedenkliche öffentliche Diskursentfaltung in sozialen Medien sind nur einige Beispiele, die insbesondere den europäischen Gesetzgeber motivierten, eine Vielzahl von Gesetzen auf den Weg zu bringen, von denen auch einige in dieser Untersuchung Beachtung finden werden.

Am bedeutendsten für die hiesige Untersuchung ist dabei die NIS2-RL, deren nationale Umsetzung insbesondere in das BSIG zum Abschluss dieser Untersuchung leider noch im Stadium eines Regierungsentwurfs vom 22.07.2024 in Form eines Artikelgesetzes mit dem Titel NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) verharrt. Da die NIS2-RL und damit auch das künftige BSIG aber bis auf Weiteres die zentralen Rahmenwerke des IT-Sicherheitsrecht darstellen (werden), wird in dieser Untersuchung bereits die NIS2-RL und der Regierungsentwurf zum BSIG (RegE BSIG) zugrunde gelegt. Die zum Zeitpunkt der Veröffentlichung noch bestehende nationale Rechtslage wird aber gleichwohl einbezogen.

Bedanken möchte ich mich bei Prof. Dr. Oliver Raabe, der mit seinen stets hilfreichen und analytisch äußerst scharfsinnigen Gedanken die Entstehung dieser Dissertation bereichert hat, mir zugleich im Rahmen dieser großartigen Betreuung aber auch einen angenehmen Freiraum ließ. Hinsichtlich der zügigen und inhaltlich anregenden Begutachtung dieser Untersuchung gilt mein Dank Prof. Dr. Thomas Dreier und Prof. Dr. Jens-Peter Schneider.

Außerdem möchte ich mich bei den Kolleg:innen von ITSR.sys, KASTEL sowie der Forschungsgruppe ITR bedanken. Aus letzterer ist insbesondere unsere Sekretärin Sandra Schommer hervorzuheben, die mir stets nach besten Möglichkeiten alle „nicht-wissenschaftlichen" Anliegen ferngehalten oder andernfalls zumindest mit allen Kräften bei der Bewältigung derselben unterstützt hat.

Schließlich möchte ich mich bei meiner lieben Lebensgefährtin und Kollegin Leonie Sterz bedanken, die mit ihrer liebe- und humorvollen sowie stets unterstützenden Art den erfolgreichen Abschluss dieser Dissertation in dieser Form erst ermöglicht hat. Und in diesem Zusammenhang ist natürlich unser gemeinsamer Sohn Henri nicht zu vergessen, der insbesondere noch bis zur Abgabe dieser Dissertation gewartet hat, bis er zu uns gekommen ist.

Rechtslage, Literatur und Rechtsprechung wurden bis zum 15.04.2024 berücksichtigt, lediglich die laufende Gesetzesentwicklung wurde insbesondere mit dem benannten Regierungsentwurf zum NIS2UmsuCG vom 22.07.2024 nachträglich eingearbeitet. Die Open-Access-Veröffentlichung wurde dankenswerterweise von den KASTEL Security Research Labs finanziell unterstützt.

Karlsruhe, November 2024 *Christoph Werner*

Inhaltsübersicht

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

a.A.	anderer Ansicht/Auffassung
ABl.	Amtsblatt der Europäischen Union
a.E.	am Ende
a.F.	alte Fassung
Art.	Artikel
AS-Nr.	Aufsatznummer
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
BKartA	Bundeskartellamt
BMI	Bundesministerium des Innern und für Heimat
BR-Drs.	Bundesratsdrucksache
BReg	Bundesregierung
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik in seiner Fassung ab dem 23.06.2021
BT-Drs.	Bundestagsdrucksache
BW	Baden-Württemberg
bzgl.	Bezüglich
bzw.	Beziehungsweise
CISA	Cybersecurity and Infrastructure Security Agency (USA)
CR	Computer und Recht
CRA-E	Entwurf für eine EU-VO über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final.
CSA	Cybersecurity Act (EU-VO 2019/881)
DDoS	Distributed Denial-of-Service
DIW-Modell	Daten-, Informations-, Wissensmodell
DoD	United States Department of Defense (Verteidigungsministerium der USA)

DORA	EU-VO 2022/2554 des europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (Digital Operational Resilience Act), ABl. 2022 L 333, 1
DSA	EU-VO 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Digital Services Act), Abl. 2022 L 277, 1
DS-RL	RL 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281/31 (alte Rechtslage, aufgehoben durch die DSGVO am 25.05.2018)
DSGVO	EU-VO 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/1
DSK	Datenschutzkonferenz (Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder)
DVO	Durchführungsverordnung
ebd.	ebenda
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäische Datenschutzbeauftragte
EL	Ergänzungslieferung
en	Englisch
EU	Europäische Union
(EU-)VO	Europäische Verordnung
EuG	Gericht der Europäischen Union
EuGH	Europäische Gerichtshof
EG	Erwägungsgrund
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
Hs.	Halbsatz
i.d.R.	in der Regel/im Regelfall

IEEE	Institute of Electrical and Electronics Engineers (Globaler Berufsverband mit Sitz in New York, USA)
ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
i.e.S.	im engeren Sinn
IT	Informationstechnik/Informationstechnologie
IT-Sicherheit	Sicherheit in der Informationstechnik
i.V.m.	in Verbindung mit
i.w.S.	im weiteren Sinn
KI	Künstliche Intelligenz
KI-VO-E	Entwurf einer Verordnung zu harmonisierten Vorschriften über Künstliche Intelligenz, Stand: 16.01.2024, 5662/24.
LfDI BW	Landesbeauftragte für den Datenschutz und die Informationsfreiheit BW
lit	littera (lateinisch für Buchstabe)
IT-Sicherheitsrecht	Recht der Sicherheit in der Informationstechnik
MedizinProdVO	EU-VO 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates, ABl. 2017 L 117/1
ML	Maschinelles Lernen
m.w.N.	mit weiteren Nachweisen
NIS-RL	RL über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (RL 2016/1148), Abl. 2016 L 194/1
NIS2-RL	RL 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 (RL 2022/2555), ABl. 2022 L 333/80
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
o.g.	oben genannt
RED	RL 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften

	der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG Text von Bedeutung für den EWR (en: Radio Equipment Directive), ABl. 2014 L 153/62
RefE	Referentenentwurf
RefE BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik *Referentenentwurf des BMI aus dem NIS2UmsuCG vom 22.12.2023*
RefE KRITIS-DachG	Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen, *Referentenentwurf des BMI vom 21.12.2023*
RefE NIS2Umsu-CG	NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz *Referentenentwurf des BMI vom 22.12.2023*
RegE	Regierungsentwurf
RegE BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, *Regierungsentwurf des NIS2UmsuCG vom 22.07.2024, 380/24*
RKE-RL	Richtlinie für die Resilienz kritischer Einrichtungen,
RL	Europäische Richtlinie
S.	Satz / Seite
sog.	sogenannt
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutzgesetz (ehemals TTDSG)
toM	technische und organisatorische Maßnahmen
UEBA	User and Entitiy Behavior Analysis
UN-R 155	UN-Regelung Nr. 155 — Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2021/387], ABl. 2021 L 82/30
USA	Vereinigte Staaten von Amerika
Vol.	Volume (en), bezeichnet v.a. bei ausländischen Fachzeitschriften eine Menge von Heften (en.: Issue) in einem bestimmten Zeitraum.
z.B.	Zum Beispiel
Ziff.	Ziffer

1. Kapitel: Einleitung

A. Motivation

Informationstechnik wird heute in den verschiedensten Bereichen eingesetzt und ist dabei inzwischen oft derart integraler Bestandteil, dass es als unabdingbares Kernelement sowohl in soziotechnischen Strukturen wie Unternehmen und Behörden als auch in der privaten Lebensführung anzusehen ist. In gleichem Maße hat mit dieser Entwicklung auch die Bedeutung der Sicherheit in der Informationstechnik (*kurz: IT-Sicherheit*) und der Sicherheit personenbezogener Daten *(kurz: Datensicherheit)* stetig zugenommen, wodurch auch das zugehörige Recht vor immer neue Herausforderungen gestellt wird.

Durch die ubiquitäre Verbreitung der Informationstechnologie wird es für den demokratischen Gesetzgeber zunehmend schwieriger, die damit verbundenen und sich sehr dynamisch entwickelnden Realweltphänomene schnell genug zu erfassen und angemessen zu regulieren.

So existieren für viele einzelne Bereiche inzwischen gesetzliche Anforderungen an die Daten- und IT-Sicherheit, die jedoch oft unterschiedlich ausgeprägt und zumeist unabhängig voneinander gewachsen sind. Immer häufiger ist nun aber auch zu beobachten, dass sich diese unterschiedlichen Rechtsregime überschneiden, soweit v.a. große Digitalunternehmen von mehreren Rechtsregimen betroffen sind. Herausfordernd ist dies für die betroffenen Unternehmen insbesondere dann, wenn sich die gesetzlichen Anforderungen an die Gewährleistung der Daten- bzw. IT-Sicherheit inhaltlich unterscheiden. Dies ist etwa dann der Fall, wenn im Zuge einer Gesetzesnovellierung durch einen neuen Rechtsbegriff neue Anforderungen implementiert werden, zu denen in anderen Gesetzen noch eine Entsprechung fehlt. So verhielt es sich auch bei dem hiesigen Untersuchungsgegenstand, als mit der Ablösung der DS-RL[1] durch die DSGVO[2] die *Resilienz*[3]

1 Datenschutzrichtlinie, RL 95/46/EG.
2 Datenschutzgrundverordnung, EU-VO 2016/679.
3 Im deutschen Gesetzeswortlaut wird von „Belastbarkeit" gesprochen. Im Rahmen dieser Arbeit wird hingegen zwecks einheitlicher Lesbarkeit durchgehend der Begriff „Resilienz" verwendet. Warum dieser vorzugswürdig ist, ausführlich: S. 121 ff.

erstmals in einem Gesetz des europäischen Daten- bzw. IT-Sicherheitsrechts als ausdrückliche, zusätzliche Anforderung aufgenommen wurde.

Im Rahmen dieser Motivation werden zunächst mit der „digitalen Entwicklungen der Gesellschaft" die Realweltphänomene erläutert, die hinter den jeweiligen kollidierenden Rechtsregimen stehen (I.). Im Anschluss wird die zugehörige rechtliche Ausgangslage näher beleuchtet (II.) Darauf folgt die Darstellung eines konkreten Szenarios, an dem die Bedeutung und Funktionsweise der Resilienz demonstriert werden soll (III.). Unter IV. wird aufgezeigt, dass dem Aspekt der Überschneidung von Daten- und IT-Sicherheitsrecht auch übergreifende Bedeutung zukommt und schließlich werden diese die Untersuchung motivierenden Aspekte in einem Fazit zusammengefasst (V.).

I. Digitale Entwicklung der Gesellschaft

Im Rahmen dieser einleitenden Motivation werden zunächst zwei besonders wichtige Realweltphänomene aus der digitalen Entwicklung der Gesellschaft beleuchtet, namentlich die zunehmende Entwicklung in der Verarbeitung personenbezogener Daten (1.) sowie die stark wachsende wirtschaftliche und gesellschaftliche Bedeutung von digitalen Diensten (2.) Anschließend wird beschrieben, wie sich die beiden Phänomene bei den digitalen Diensten treffen (3.). Unter 4. wird dargelegt, vor welchen Herausforderungen die digitalen Dienste angesichts einer zunehmenden Ungewissheit stehen und diese Gemengelage schließlich in einem Fazit zusammengefasst (5.).

1. Die Welt der personenbezogenen Daten

Zunächst ist eine expandierende Verarbeitung personenbezogener Daten zu beobachten. Dies betrifft sowohl die Qualität als auch insbesondere die Quantität der Daten. Im Alltag bleibt diese Entwicklung oft unsichtbar, werden die Daten doch nur zu einem kleinen Teil bewusst preisgegeben, etwa durch das Teilen von Inhalten in sozialen Netzwerken. Ein weit größerer Teil wird dagegen „unbewusst" preisgegeben, etwa durch das *Tracking*, d.h. das Sammeln, Auswerten und ggf. Vermarkten von Nutzerverhaltensdaten etwa bezüglich besuchter Webseiten, genutzter Smartphone-Apps

oder durchgeführter Such- und Produktanfragen.[4] Hinzu kommen in Zeiten des Internet of Things (IoT) weitere Datenquellen, da i.d.R. jedes smarte Haushaltsgerät, vernetzte Fahrzeug und jeder andere digitale Begleiter (z.B. Fitnesstracker) Daten erzeugt, die gesammelt, ausgewertet und dabei auch einer Person zugeordnet werden können.

Im Rahmen der Auswertung werden diese Daten für das sog. *Profiling* verwendet. Dies wird in der DSGVO definiert als die Verarbeitung personenbezogener Daten, um persönliche Aspekte zu bewerten, um wiederrum beispielsweise die wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen und Verhalten dieser Person zu analysieren oder vorherzusagen.[5] Durch diese spezifische Verarbeitungsfunktion kommt der Verwendung personenbezogener Daten eine neue Gewichtung zu, die sich insoweit auch im Datenschutzrecht widerspiegelt. Während Datenschutz im Sinne des *Volkszählungsurteils* v.a. noch auf die Befugnis abzielte, Dritte per se von den persönlichen Informationen auszuschließen,[6] rückt mit modernen Verarbeitungsformen wie dem Profiling v.a. die Verwendung der personenbezogenen Daten in den Vordergrund. Schließlich erfolgt diese Bildung von Profilen nicht als Selbstzweck, sondern diese werden von Unternehmen für automatisierte, individuelle Entscheidungen gegenüber den Kund:innen genutzt, etwa für die Präsentation von Werbeanzeigen und Produktvorschlägen, für Ergebnisse in Suchmaschinen oder von Inhalten einschließlich politischer Nachrichten in sozialen Medien. Genereller formuliert findet also eine *Personalisierung* der wahrgenommenen und ggf. auch wahrnehmbaren Inhalten der digitalen Welt statt.[7] Daneben eröffnet

4 Zwar belegt das Datenschutzrecht die Verantwortlichen mit Informationspflichten, diese Informationen werden aber insbesondere hinsichtlich des Webseiten-Trackings durch Cookies häufig nicht von den Nutzer:innen wahrgenommen bzw. gewürdigt siehe hierzu: bitkom e.V., Umfrage: Cookie-Banner spalten Internetnutzer, 10.11.2020; Begriffserläuterung „Tracking": *R. Grimm/Waidner*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 33 (49), Rn. 76.

5 Art. 4 Nr. 4 DSGVO.

6 *BVerfG*, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., NJW 1983, 419 (421 f.).

7 Unter Personalisierung sind Methoden zu verstehen, mit denen digitale Inhalte anhand von Informationen über Merkmale einzelner Nutzer:innen, wie insbesondere deren Präferenzen, individualisiert werden, siehe: *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 98 (104, 106); *Montgomery/M. D. Smith*, Journal of Interactive Marketing 2009, 130 (130); ähnlich auch: *Paal/Hennemann*, JZ 2017, 641 (644). Teilweise wird auch von „personalisierter Informationsfilterung" gesprochen, so: *Koene et al.*, in: Internet Science, 2nd International Conference (INSCI 2015), Ethics of Personalized Information Filtering, 123 (123).

die Digitalisierung die Möglichkeit die Preise für eine spezifische Leistung zu personalisieren, z.B. im Online-Handel oder bei Versicherungsprämien (z.B. bei KFZ-Haftpflichtversicherungen, sog. pay-as-you-drive[8]).

Für die Datensicherheit kumulieren sich damit verschiedene Risiken im Umgang mit personenbezogenen Daten. Nicht nur werden immer größere Mengen an qualitativ hochwertigen Daten erhoben und genutzt, sie werden darüber hinaus auch durch Algorithmen weiterverarbeitet, um dadurch personenbezogenes Wissen zu generieren und im Ergebnis bestimmte, individuelle Entscheidungen herbeizuführen. Durch diesen individuellen Zuschnitt potenzieren sich die Auswirkungen auf die Grundrechte der jeweiligen Person, wenn dieser Vorgang der Personalisierung fehlerhaft ist oder – für die hiesige Untersuchung im Daten- und IT-Sicherheitsrecht entscheidend – aktiv manipuliert wird.

2. Die kritischen Dienste der Gesellschaft

Die andere wesentliche, aber eher von gesellschaftlichem Interesse geprägte Entwicklung folgt aus der wachsenden Durchdringung der Gesellschaft durch die Digitalisierung.

Dadurch, dass nahezu kein Unternehmen dem digitalen Wandel fernbleiben kann, erwachsen neue, digitale Abhängigkeiten: So sind viele Einzelunternehmen zunehmend abhängig von großen Digitalunternehmen, die Dienste anbieten, die für die Funktionsfähigkeit dieser Unternehmen immer öfter unverzichtbar sind. Insoweit hat der europäische Gesetzgeber einigen dieser „digitalen Dienste": nämlich „Online-Suchmaschinen", „Online-Marktplätze" und „Anbieter von Plattformen für Dienste sozialer Netzwerke" (nachfolgend nur: „soziale Netzwerke")[9] eine besondere Kritikalität attestiert; deren „Sicherheit, Verfügbarkeit und Verlässlichkeit […] [sei] für das reibungslose Funktionieren vieler Unternehmen von wesentlicher Bedeutung. Aus der Perspektive der Wirtschaft handelt es sich um *unver-*

8 Siehe hierzu S. 44.

9 Die Dienste sind legaldefiniert in: Art. 6 Nr. 28, 29, 33 NIS2-RL; anders als die „übrigen" digitalen Dienste werden soziale Netzwerke nicht in ihrer Definition (wohl aber in Anhang II, Ziff. 6 NIS2-RL) als digitale Dienste, sondern als „Plattform" definiert. Dies ist jedoch wohl eher als sprachliche Inkonsistenz aufgrund der nachträglichen Ergänzung der sozialen Netzwerke durch die NIS2-RL zurückzuführen; ein sachlicher Grund für die unterschiedliche Bezeichnung ist nicht ersichtlich. Insbesondere handelt es sich bei sozialen Netzwerken ähnlich wie bei Online-Suchmaschinen und Online-Marktplätzen um Intermediäre.

zichtbare Schnittstellen zum Angebot von Waren und Dienstleistungen an (potenzielle) Kund:innen.

Daneben folgt eine gesellschaftliche Bedeutung daraus, dass insbesondere Online-Suchmaschinen und soziale Netzwerke die *zentralen, digitalen Informations- und Meinungsplattformen* für die Bürger:innen darstellen.[10] Auch diese gesellschaftliche Bedeutung führt zu entsprechend großen Risikofolgen (z.B. die Verbreitung von Falschinformationen in der Gesellschaft), die im Rahmen der Gewähr der IT-Sicherheit zu berücksichtigen sind.

Insgesamt stellt somit auch der europäische Gesetzgeber die herausgehobene wirtschaftliche und gesellschaftliche Bedeutung digitaler Dienste fest[11] und unterwirft sie deshalb entsprechenden IT-Sicherheitsvorgaben.

3. Zweifache Bedeutung digitaler Dienste

Insbesondere bei den genannten Online-Suchmaschinen, Online-Marktplätzen als auch sozialen Netzwerken kommt es nun zu einer Parallelität beider Aspekte, da die zugehörigen Unternehmen für die Bereitstellung ihrer wirtschaftlich und gesellschaftlich kritischen Dienste in hohem Maße personenbezogene Daten in Algorithmen verwenden, um ihr Angebot zu personalisieren (*algorithmenbasierte Personalisierung*).[12] So bietet die Google Suche insbesondere eine „Relevanzsortierung". Je nachdem, welches Persönlichkeitsprofil einer Suchanfrage zugeordnet wird, erscheinen die Suchergebnisse in unterschiedlicher Reihenfolge. Nach bisherigen Studien ist der Grad der Personalisierung zwar gering, aber durchaus messbar.[13] Weiterhin personalisieren soziale Netzwerke in hohem Maße ihre „Feeds", in denen sie ihren Nutzer:innen für sie (vermeintlich) relevante Inhalte

10 Vgl. *Paal/Hennemann*, JZ 2017, 641 (641, 643); außerdem zu sozialen Netzwerken: *Pille*, Meinungsmacht sozialer Netzwerke, S. 301 f. m.w.N.; zu Online-Suchmaschinen ähnlich: *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 98 (98).

11 Vgl. ursprünglich noch mit Cloud-Computing-Diensten statt sozialen Netzwerken: EG 48 NIS-RL.

12 Vgl. zur Verwendung dieses Begriffs diesem Begriff bereits: *Weiber* im Geleitwort zu *Gabriel*, Die Macht digitaler Plattformen, S. VII f.

13 *Koene et al.*, in: Internet Science, 2nd International Conference (INSCI 2015), Ethics of Personalized Information Filtering, 123 (123); *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 98 (129).

präsentieren.[14] Schließlich findet auch bei einer Produktsuche auf der Webseite des Unternehmens Amazon, wozu auch der Amazon Marketplace gehört, eine Personalisierung[15] der angezeigten Produkte bei einer Suchanfrage oder sonstigen Empfehlungen statt. Auch die Werbeanzeigen auf all diesen Diensten sind entsprechend individuell zugeschnitten. Die Personalisierung wird als ein Schlüsselelement für den wirtschaftlichen Erfolg dieser Unternehmen angesehen,[16] so dass mit einer zunehmenden Verbreitung der Personalisierung zu rechnen ist.

Diese enge Verschränkung von der Verarbeitung personenbezogener Daten und der Erbringung eines kritischen Dienstes bzw. einer kritischen Dienstleistung ist charakteristisch für die oben genannten digitalen Dienste. Zur Erbringung traditionell „kritischer" Dienstleistungen wie der Energie- oder Wasserversorgung ist die Verarbeitung personenbezogener Daten zwar notwendig (insbesondere zu Abrechnungszwecken), aber sie beeinflusst die kritische Dienstleistung als solche in der Regel nicht. Dagegen ist die Verarbeitung personenbezogener Daten bei den digitalen Diensten nicht nur Bestandteil, sondern sogar eine entscheidende Voraussetzung im Sinne einer *conditio sine qua non* der Diensterbringung in ihrer konkreten Ausgestaltung.

4. Technische Innovation in Ungewissheit

Eine weitere maßgebliche Entwicklung besteht darin, dass es sich bei modernen IT-Systemen wie sie auch zur Erbringung der o.g. Dienste verwendet werden, zumeist nicht um geschlossene, sondern um offene, verteilte Systeme handelt.[17]

Klassische, geschlossene Systeme zeichnen sich dadurch aus, dass der Betreiber die überwiegende, wenn nicht sogar die vollständige Kontrolle über

14 *C. Yang et al.*, Telematics and Informatics, Vol. 82 (2023), AS-Nr.: 101999, S. 1 f.; *Reviglio/Agosti*, SM+S 2020, Heft 2, 28.04.2020, S. 2.

15 Teilweise wird statt „Personalisierung" auch der Begriff „Individualisierung" verwendet, so etwa: *Schwenke*, Individualisierung und Datenschutz, S. 1 ff. Im Sinne dieser Arbeit sind beide Begriffe als synonym zu verstehen.

16 *Koene et al.*, in: Internet Science, 2nd International Conference (INSCI 2015), Ethics of Personalized Information Filtering, 123 (123).

17 Vgl. grundlegend bereits zu diesem Wandel: *Wedde*, in: Däubler, Bundesdatenschutzgesetz [a.F.], 5. Auflage 2016, § 9, Rn. 41; ausführlicher dazu mit Blick auf die digitalen Dienste im Rahmen der teleologischen Auslegung nach Art. 32 DSGVO, S. 208 ff.

diese ausübt und bei denen alle Nutzer:innen bekannt sind.[18] Dies gewährt im Ausgangspunkt ein hohes Maß an Gewissheit über die ordnungsgemäße Funktionsweise der Systeme; Angriffe können nur über bekannte Schnittstellen erfolgen und lassen sich daher als spezifische Risiken mit Blick auf die klassischen Schutzziele (Verfügbarkeit, Vertraulichkeit, Integrität) bewältigen.

Dagegen handelt es sich bei den Systemen, wie sie auch zur Erbringung der o.g. Dienste erbracht werden i.d.R. um offene, verteilte Systeme. Diese bestehen aus heterogenen Teilsystemen, die nicht zentral durch einen Betreiber/Verantwortlichen kontrolliert werden (können).[19] Als Subsysteme gehören dazu insbesondere die Systeme der Nutzer:innen, also deren Endgeräte wie Computer, Smartphones und IoT-Geräte. Sie fungieren durch die Eingaben der Nutzer:innen als Datenquellen für die Erbringung der digitalen Dienste, liegen aber zumeist gleichwohl außerhalb des Kontrollbereichs (der engeren „Systemgrenzen") des Verantwortlichen/Betreibers.[20] Damit besteht für diesen eine hohe Ungewissheit über die Qualität der Daten als solche ebenso wie über Faktoren, die die Datenqualität beeinflussen können. Wer aus welchen Gründen die Daten ggf. schon auf dem Endgerät manipuliert oder unterdrückt haben könnte, ist für den Verantwortlichen/Betreiber in einem offenen, verteilten System nicht (mehr) zu antizipieren.

5. Fazit

Die Gesellschaft ist wie beschrieben durch eine starke Abhängigkeit von bestimmten digitalen Diensten (Online-Marktplätze, Online-Suchmaschinen, soziale Netzwerke) geprägt, die ihrerseits in hohem Maße auf die Verarbeitung personenbezogener Daten angewiesen sind. Damit potenzieren sich bei diesen digitalen Diensten die Risiken mit sowohl datenschutzrechtlichen als auch IT-sicherheitsrechtlichen Schadfolgen. Gleichzeitig sind die Anbieter dieser Dienste u.a. aufgrund der für diese Diensterbringung notwendigerweise offenen Systemarchitektur einem faktischen Verlust an Kontrolle und somit größerer Ungewissheit ausgesetzt.

18 Vgl. *Eckert*, IT-Sicherheit, S. 3.
19 *Eckert*, IT-Sicherheit, S. 3.
20 Ausnahmen, bei denen alle beteiligten Subsysteme vom Verantwortlichen (hergestellt und) kontrolliert werden, liegen bei Unternehmen vor, die sog. „digitale Ökosysteme" aufbauen, wie etwa bei *Apple*.

II. Rechtliche Ausgangslage

Das Recht unterwirft die Anbieter dieser digitalen Dienste zum einen in datenschutzrechtlicher Hinsicht dem *Datensicherheitsrecht* der DSGVO (Art. 32 DSGVO) als auch dem § 30 RegE BSIG[21] (derzeit noch § 8c BSIG[22]) aus dem IT-Sicherheitsrecht im engeren Sinn.[23]

Zum IT-Sicherheitsrecht im engeren Sinn (i.e.S.) gehören alle öffentlich-rechtlichen Pflichtennormen, die entweder Herstellern von Produkten oder Betreibern von informationstechnischen Systemen Pflichten zur Gewährleistung von IT-Sicherheit auferlegen.[24] Betreiberbezogen ist insbesondere das IT-Sicherheitsrecht mit dem hier gegenständlichen § 30 RegE BSIG sowie § 165 TKG oder Art 6 ff. DORA[25] und Teile des KI-VO-E. Herstellerbezogen sind ebenfalls Teile des KI-VO-E sowie der Entwurf zum sog. Cyberresilience-Act (CRA-E),[26] die Medizinprodukte-Verordnung (MedizinProdVO)[27] oder die Richtlinie über die Bereitstellung von Funkanlagen

21 Der Regierungsentwurf zum BSIG ist Teil des Regierungsentwurfs zu dem Artikelgesetz NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) vom 22.07.2024.

22 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG).

23 Vgl. zur parallelen Anwendbarkeit der genannten Vorschriften (statt auf § 30 RegE BSIG mit Blick auf die noch geltenden Vorschriften, §§ 8a, 8c BSIG): *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 99; *Voigt*, in: Bussche/Voigt, Konzerndatenschutz, Teil 5, Kap. 3, Rn. 38; mit Blick auch auf NIS-RL ebenso: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 16. Zu den Gründen für die begriffliche Differenzierung zwischen Datensicherheits- und IT-Sicherheitsrecht siehe außerdem *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (393 ff.), Rn 7 ff.; zu den inhaltlichen Unterschieden von Daten- und IT-Sicherheit außerdem in dieser Untersuchung: S. 298 f.

24 Grundlegend zur Unterteilung des IT-Sicherheitsrechts i.e.S. und i.w.S.: *Raabe/Schallbruch/Steinbrück*, CR 2018, 706 (707); *Werner*, in: Baumgärtel/Kiparski, DGRI-Jahrbuch 2021/2022, 161 (163), Rn. 5.

25 Auch die unter die DORA fallenden Finanzinstitute sind z.T. kritische Infrastrukturen. Der RegE BSIG sieht aber in § 28 Abs. 6 und Abs. 7 entsprechende Ausnahmen für der DORA unterfallende Finanzinstitute vor, so dass diese nur und gemeinsam mit den übrigen Finanzinstituten von der DORA reguliert werden.

26 Entwurf einer EU-VO über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final.

27 EU-VO 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates.

(RED).[28] Das IT-Sicherheitsrecht im weiteren Sinn umfasst zusätzlich die zugehörigen Melde- (z.B. § 32 RegE BSIG) und Transparenzpflichten, Regelungen des Zivilrechts (etwa mit Blick auf die IT-Sicherheit als Sachmangel in Produkten mit digitalen Elementen, §§ 434, 475b BGB) oder auch strafrechtliche Vorschriften, die IT-Sicherheitsangriffe sanktionieren (z.B. §§ 303a f. StGB).

1. Datensicherheitsrecht und IT-Sicherheitsrecht

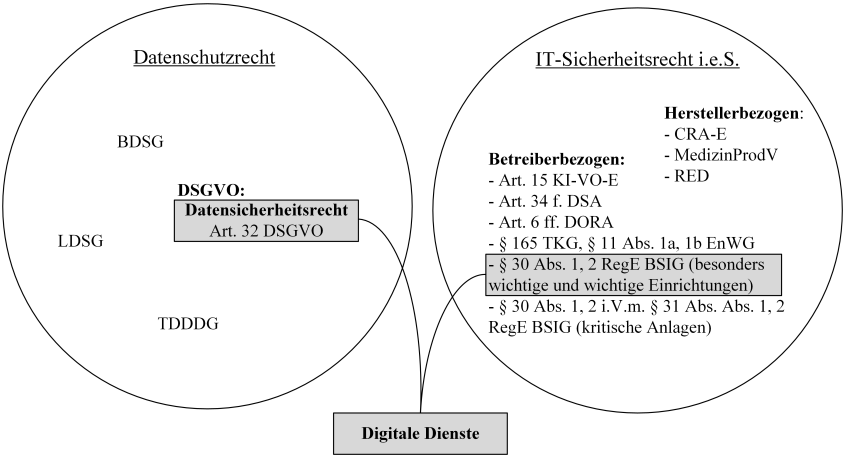

Abbildung 1: Datenschutzrecht und IT-Sicherheitsrecht

Die hier gegenständliche Untersuchung befasst sich ausschließlich mit dem IT-Sicherheitsrecht i.e.S. und auch davon im Wesentlichen nur mit den Vorgaben nach § 30 Abs. 1 RegE BSIG an besonders wichtige und wichtige Einrichtungen, wobei die hier betrachteten digitale Dienste zu den wichtigen Einrichtungen gehören. Zusätzlich wird auch auf Betreiber kritischer Anlagen eingegangen, für die nach § 31 RegE BSIG zusätzliche Anforderungen bestehen.

28 RL 2014/53/EU des Europäischen Parlaments und des Rates vom 16. April 2014 über die Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Funkanlagen auf dem Markt und zur Aufhebung der Richtlinie 1999/5/EG Text von Bedeutung für den EWR (en: *Radio Equipment Directive*, RED), in Deutschland umgesetzt durch das Funkanlagengesetz.

Zur Pointierung des Vergleichs gegenüber dem Datensicherheitsrecht werden diese Regelungen des BSIG stets stellvertretend als das *IT-Sicherheitsrecht* bezeichnet. Auf die rechtlichen Unterschiede zwischen Datensicherheits- und dem in diesem Sinne verstandenen IT-Sicherheitsrecht wird sogleich überblicksartig und an den passenden Stellen der Untersuchung vertieft eingegangen.

2. Unterschiede beider Rechtsgebiete

Zwischen dem Datensicherheits- und dem IT-Sicherheitsrecht besteht derzeit *kein kohärentes Verhältnis:* Da ist zunächst der im Einzelnen noch zu untersuchende Umstand, dass die beiden Regelungsregime, wie bereits angedeutet, unterschiedliche Schutzgüter sichern. Die DSGVO schützt die Rechte und Freiheiten natürlicher Personen, insbesondere deren *Recht auf Schutz personenbezogener Daten* (Art. 1 Abs. 2, EG 2 DSGVO, Art. 8 Abs. 1 GRC[29]). Sie dient damit v.a. dem Individualgüterschutz.[30] Dagegen legt das IT-Sicherheitsrecht, auf europäischer Ebene durch die NIS2-RL[31] normiert und in Deutschland v.a. durch den RegE BSIG abgebildet den Fokus auf die *Funktionsfähigkeit des Gemeinwesens* mit seinen gesellschaftlichen und wirtschaftlichen Tätigkeiten und dient daher insbesondere auch öffentlichen Interessen.[32]

Das damit derselbe Sachgegenstand durch zwei unterschiedliche Regelungsregime betroffen ist, ist an sich noch nicht ungewöhnlich: vielmehr ist es in einer komplexen Rechtsordnung geradezu erwartbar, dass einzelne Sachbereiche aus mehreren Schutzrichtungen heraus rechtlich reguliert werden. In der viel beachteten Facebook-Entscheidung des BKartA wurde die Zusammenführung von personenbezogenen Daten mit anderen konzerneigenen Diensten (insb. Instagram, Whatsapp) im Ergebnis nicht aus dem Datenschutzrecht, sondern entsprechend der Zuständigkeit aus dem

29 Charta der Grundrechte der Europäischen Union.

30 *Bieker/M. Hansen/Friedewald*, RDV 2016, 188 (188).

31 NIS-2-Richtlinie, RL 2022/2555.

32 EG 1, 3 NIS2-RL; EG 1, 48 NIS-RL; § 2 Nr. 24 RegE BSIG, § 2 Abs. 10 Nr. 2 BSIG; Vgl. *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 16; ähnlich mit Blick auf die „gesamtgesellschaftliche Perspektive" des IT-Sicherheitsrechts auch *Sattler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 197 (201); ausführlich zu den Schutzgütern des IT-Sicherheitsrechts: S. 222 ff.

Wettbewerbsrecht heraus untersagt.[33] Und die Regelungen des TKG beziehen sich nach § 2 Abs. 2 sogar ausdrücklich auf verschiedene Rechtsgüter und Ziele aus den Bereichen von Verbraucherschutz, Wettbewerb, Sicherstellung gleichwertige Lebensverhältnisse in städtischen und ländlichen Räumen bis hin zur öffentlichen Sicherheit.

Allerdings kommt weiterhin hinzu, dass die insbesondere durch die Schutzziele beschriebenen Anforderungen an die IT- bzw. Datensicherheit nicht übereinstimmen. Die DSGVO etabliert als viertes „Merkmal" neben den klassischen Schutzzielen die *Resilienz*, das BSIG und die NIS(2)-RL hingegen die *Authentizität*. Damit treten in beiden Rechtsordnungen neue Merkmale neben die drei klassischen Schutzziele der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit und Integrität)[34] und erweitern somit das Schutzprogramm jeweils eigenständig.

Schließlich beziehen sich die klassischen Schutzziele sowie die zusätzlichen Merkmale auch auf unterschiedliche Schutzobjekte: Nach Art. 32 Abs. 1 lit b), Abs. 2 DSGVO sollen sie für personenbezogene Daten, Systeme und Dienste sichergestellt werden, die NIS2-RL bezieht sie hingegen gerade nicht auf Systeme, sondern lediglich auf (alle) Daten und Dienste. Das System ist nach dem Wortlaut der NIS2-RL lediglich der Maßnahmenträger, der die Schutzziele für Daten und Dienste sicherstellen soll.

Die Regelungsregime der DSGVO und des RegE BSIG bzw. der NIS(2)-RL knüpfen weiterhin an einen Risikobegriff an und fordern, ein *dem Risiko angemessenes Schutzniveau* zu gewährleisten. Schon bei der Frage der Definition des Risikos besteht aber keine Einigkeit. Die DSGVO enthält sich einer eigenständigen Definition und ob die durch Auslegung ermittelten Definitionen hier mit der Legaldefinition des Risikos nach der NIS2-RL übereinstimmen, ist zumindest zweifelhaft.

3. Überschneidungsbereich

Der sich so ergebende Umstand *mangelnder Kohärenz*[35] zwischen Daten- und IT-Sicherheitsrecht ist aus regulationstechnischer Sicht in hohem

33 BKartA, Pressemitteilung vom 07.02.2019, 07.02.2019.

34 *Samonas/Coss*, JISSec, Vol. 10 (2014), Heft 3, 21 (23 f.).

35 Kohärenz zwischen Rechtsnormen liegt nach europäischem Verständnis (Art. 7 AEUV) vor, wenn diese konzeptionell und inhaltlich aufeinander bezogen (und abgestimmt) sind, *Schorkopf*, in: Grabitz/Hilf/Nettesheim, Das Recht der europäischen

Maße unbefriedigend. Denn viele Unternehmen müssen beide Schutzprogramme einhalten, die sich aber in ihrer Gestaltung deutlich unterscheiden. Insbesondere bei Online-Marktplätzen, Online-Suchmaschinen oder sozialen Netzwerken liegen wie ausgeführt informationstechnische Systeme vor, die sowohl die personenbezogenen Daten beinhalten, als auch gerade durch deren Verarbeitung die kritische Dienstleistung bereitstellen, so dass sie im Ergebnis den rechtlichen Anforderungen sowohl des Daten- als auch des IT-Sicherheitsrechts entsprechen müssen.[36] Sie müssen somit als *wichtige Einrichtungen* des IT-Sicherheitsrechts (§ 28 Abs. 2 Nr. 1 i.V.m. Anlage 2, Ziff. 6 RegE BSIG) einen *sicheren Dienst* nach § 30 Abs. 1 RegE BSIG anbieten als auch als *Verantwortliche* (Art. 4 Nr. 7 DSGVO) die personenbezogenen Daten nach Art. 32 DSGVO schützen (*Datensicherheit*), die sie im Rahmen ihrer Diensterbringung nutzen.

Es kommt daher zu einer faktischen Überschneidung der beiden Rechtsgebiete, die unterschiedliche Anforderungen an denselben tatsächlichen Vorgang stellen, um jeweils unterschiedliche Rechtsgüter zu schützen.[37]

Für eine möglichst effiziente Sicherheitsgewährleistung ist aber eine einheitliche, normative Konzeption anzustreben, die ein gemeinsames Verfahren zum Umgang mit Risiken (Risikomethodik bzw. -management) ermöglicht. Dadurch kann der Aufwand der Normbefolgung deutlich reduziert werden. Außerdem können kumulierende Risiken (also Risiken, deren Folgen sowohl die Schutzgüter der DSGVO als auch jene des RegE BSIG betreffen) angemessen berücksichtigt und mögliche Zielkonflikte direkt erkannt und bewältigt werden.[38]

Dadurch motiviert und auf Basis der skizzierten rechtlichen Ausgangslage gilt es in dieser Arbeit zu untersuchen, ob zumindest das Merkmal der *Resilienz* sich aus der DSGVO auch auf den RegE BSIG übertragen lässt und insoweit zum einen die Kohärenz der Schutzprogramme zugunsten der eben genannten Vorteile erhöht werden kann und zum anderen der

---

Union, 80. EL 2023, Art. 7 AEUV, Rn. 11; teilweise wird auch der Begriff der Konsistenz verwendet, wobei dessen Verhältnis zum Begriff der Kohärenz zweifelhaft ist, *Schorkopf*, ebd.; *Pagenkopf*, NJW 2011, 513 (516).

36 Vgl. *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 11.

37 Siehe Fn. 23.

38 Die Alternative ohne die genannten Vorteile besteht darin, für beide Rechtsgebiete jeweils getrennte Risikomanagementprozesse durchzuführen und für den Überschneidungsbereich am Ende die jeweils höheren Maßnahmen zu wählen, in diesem Sinne wohl *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 12.

mögliche Mehrwert dieser neuen rechtlichen Anforderung ggf. auch im RegE BSIG genutzt werden könnte und sollte.

Dabei sind aufgrund der engen Verknüpfung insbesondere auch die mit der Resilienz in Zusammenhang stehen Rechtsbegriffe wie das Risiko, die Systeme und Dienste sowie die Schutzziele zu untersuchen.

III. Adressaten und Störungsszenario

Um die mögliche Funktionsweise und die Bedeutung der Resilienz in der digitalen Gesellschaft zu demonstrieren, soll im Rahmen dieser Untersuchung auf *personalisierte Dienste* abgestellt werden, d.h. solche Dienste, die entweder eine angebotene (digitale) Leistung oder den Preis für ein Produkt an den jeweiligen Nutzer anpassen (personalisieren) und hierzu personenbezogene Daten verarbeiten.

Aktuell sind solche Dienste insbesondere die *Google Suche* (Alphabet), verschiedene soziale Netzwerke wie *Facebook* und *Instagram* (Meta), *TikTok*, *X (vormals Twitter)* sowie der von Amazon betriebene *Amazon Marketplace* als Online-Marktplatz. Auf deren Personalisierung wurde bereits hingewiesen: Die Sortierung der Suchergebnisse bei Webinhalten (Google Suche) oder Produkten (Online-Marktplatz) sowie der Feeds in sozialen Netzwerken und die Personalisierung der auf all diesen Diensten geschalteten Werbung.

Daneben beginnt bereits und wird in Zukunft verstärkt erwartet eine weitere Form der Personalisierung, nämlich die *Personalisierung von Preisen* im Online- wie langfristig auch im Offline-Handel. Auch der Gesetzgeber hat insofern in Art. 246a § 1 Nr. 6 EGBGB für Fernabsatzverträge bereits eine Regelung vorgesehen, wonach der Unternehmer den Verbraucher darauf hinweisen muss, wenn „der Preis auf der Grundlage einer automatisierten Entscheidungsfindung personalisiert wurde". Künftig erscheint es insofern nicht ausgeschlossen, dass es im Online-Handel generell und damit auch auf Online-Marktplätzen[39] auch *personalisierte, d.h. auf Grundlage personenbezogener Daten individuell angepasste, Preise geben* könnte.[40]

39 Es ist auch anzunehmen, dass dieser Preis auch durch den Online-Marktplatz und nicht durch den (Dritt-)Händler festgesetzt würde, da erstgenannter am ehesten über die hierfür notwendigen personenbezogenen Daten der Kund:innen verfügt.

40 Siehe zu personalisierten Preisen im Online-Handel: *G. Wagner/Eidenmüller*, ZfPW 2019, 220 (224 ff.); Als voraussichtliche KI-Anwendung: *Sattler*, in: Ebers/Steinrötter,

Im Rahmen dieser Untersuchung wird abstrakt auf die personalisierten Dienste abgestellt werden, um die Bedeutung der Resilienz herauszuarbeiten.[41] Bei diesen Diensten spitzt sich die Datenverarbeitung (einschließlich etwaiger Manipulationen) zu, da ihr Ergebnis in einer konkreten, personalisierten Entscheidung erfolgt. Die entwickelten Ergebnisse dieser Untersuchung sind somit umgekehrt grundsätzlich auf alle Dienste anwendbar, die anhand von persönlichen Informationen Wissen generieren und auf Basis dessen eine automatisierte, personalisierte Entscheidung treffen. Für die Resilienz entscheidend ist außerdem, dass diese dynamischen, auf offenen Systemen beruhenden Dienste andere Anforderungen an die Daten- und IT-Sicherheit stellen als statische Dienste auf Basis geschlossener Systeme. Folglich kann die Resilienz auch für andere Dienste von Bedeutung sein, sofern sie dem soeben skizzierten Profil entsprechen.

Für das Störungsszenario ist vorauszuschicken, dass bei jeder Nutzung eines personalisierten Dienstes ein faktisch *unteilbarer Datenverarbeitungsvorgang* stattfindet, der sowohl nach dem Datensicherheitsrecht als auch dem IT-Sicherheitsrecht zu schützen ist. Dieser Datenverarbeitungsvorgang kann insbesondere dadurch gestört werden, dass objektiv unrichtige Informationen eingespeist werden. Betroffen sind insbesondere jene dynamischen Informationen, die sich auf die Online-Aktivität beziehen, also v.a. Seitenaufrufe, Produktsuchen, die Tätigkeiten in sozialen Netzwerken und der Medienkonsum. Objektiv unrichtig sind solche Informationen mit Blick auf den Kontext der Verarbeitung immer dann, wenn sie nicht das Abbild tatsächlicher Aktivitäten bzw. der Interessen der Nutzer:innen sind, etwa weil deren Endgeräte durch Schadsoftware kompromittiert sind, welche die (insofern manipulierten) Anfragen von den jeweiligen Geräten ausführen.

Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 197 (223); Zum wissenschaftlichen Nachweis bereits bestehender Preis-Personalisierung auf US-amerikanischen E-Commerce-Webseiten: *Hannak et al.*, in: Proceedings of the 2014 Conference on Internet Measurement Conference, Measuring Price Discrimination and Steering on E-commerce Web Sites, 305 (305 f.).

41 Weitere Beispiele finden sich auf den S. 44 ff.

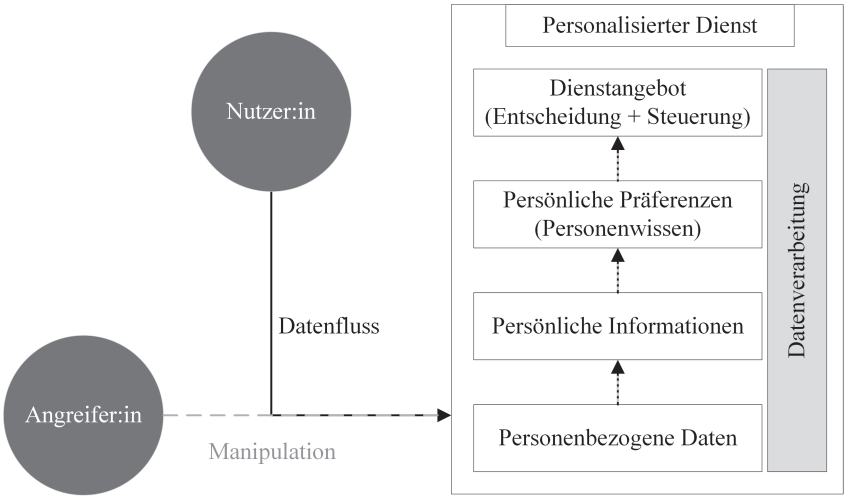

Abbildung 2: Manipulation von personalisierten Diensten

In diesem Fall wird zum einen durch den Algorithmus möglicherweise ein falsches Ergebnis auf eine bestimme Anfrage ausgegeben. Dabei verfälscht sich ggf. auch das Profil des/der Kund:in, sodass das Wissen um seine/ihre Präferenzen (*Personenwissen*) unrichtig wird. Auch besteht die Möglichkeit, dass wenn viele Identitäten korrumpiert sind und dementsprechend falsche Informationen übermitteln, die regelmäßig eingesetzten Machine-Learning-Systeme (ML-System) in ihrem abstrakten *Lernwissen* (z.B. über Präferenzzusammenhänge zwischen zwei Elementen) „umtrainiert" werden. Im Ergebnis werden dann durch den Dienst falsche Personalisierungsentscheidungen getroffen und somit ggf. auch falsche Steuerungsanreize gesetzt (zu den Details hierzu siehe S. 77 ff.).

Das *Personenwissen* könnte beispielsweise manipuliert werden, damit einzelnen Personen einseitige Personalisierungsentscheidungen (etwa bei der Recherche in Online-Suchmaschinen) erteilt werden (z.B. bei Journalist:innen oder Politiker:innen). Die Manipulation des *Lernwissens* wäre hingegen das Ziel groß angelegter Angriffe, um z.B. bestimmte Produktempfehlungen auf einem Online-Marktplatz zu erreichen oder in sozialen Netzwerken und in Online-Suchmaschinen[42] die öffentliche Meinung

42 Zumindest in Deutschland gibt es bei Online-Suchmaschinen Hinweise, dass die von vorneherein bestehende „politische Personalisierung" von Google ohnehin nur sehr

und damit ggf. auch Wahlen durch entsprechend manipulierte Personalisierungsentscheidungen dieser Dienste zu beeinflussen.

Es drohen somit unterschiedliche Angriffe, die die Datensicherheit bzw. IT-Sicherheit betreffen können. Diese beziehen sich aber auf dieselben informationstechnischen Systeme, so dass es wie beschrieben wünschenswert wäre, wenn die entsprechenden Regelungen (DSGVO und RegE BSIG) ein möglichst kohärentes Verhältnis aufweisen, damit auch diesen beiden Angriffen innerhalb eines gemeinsamen Verfahrens zur Gewährleistung der Daten- und IT-Sicherheit begegnet werden.

IV. Übergreifende Bedeutung des Szenarios

Solche Überschneidungen zwischen Daten- und IT-Sicherheitsrecht sind nicht auf die genannten, personalisierten digitalen Dienste (Online-Marktplätze, Online-Suchmaschinen, Soziale Netzwerke) beschränkt.

Ein sowohl rechtlich als auch sachlich sehr artverwandtes Phänomen sind sog. *Telematik-Versicherungen* im KFZ-Bereich (pay-as-you-drive). Auch hier werden durch die Verarbeitung personenbezogener Daten „personalisierte Tarife" erstellt, die für die Kund:innen in Abhängigkeit von ihrem Fahrprofil individuelle Prämien festsetzen.[43] Rechtlich ist ebenso eine Überschneidung von Datensicherheits- und IT-Sicherheitsrecht anzunehmen, da Schadens- und Unfallversicherungen ab 500.000 Schadensfällen pro Jahr nach der KritisV zugleich Kritische Infrastrukturen (nach RegE BSIG: kritische Anlagen) sind.[44]

Weitere Beispiele finden sich im Bereich des Energierechts (1.), der Gesundheitsversorgung (2.) sowie allgemein in digitalen Ökosystemen, die viele Dienste kombinieren (3.), wobei die Überschneidung von Datenschutz- und IT-Sicherheitsrecht teilweise explizit normiert wurde. Schließlich sei auch auf andere Überschneidungen hingewiesen, z.B. zwischen DSGVO und TKG (4.).

---

geringfügig ist; *Krafft et al.,* Filterblase geplatzt? Kaum Raum für Personalisierung bei Google-Suchen zur Bundestagswahl 2017, S. 1.

43 *Klimke*, r+s 2015, 217 (217 ff.).

44 § 7 Abs. 1 Nr. 5, Abs. 6; Anhang 6, Teil 1 Nr. 1 lit x), Anhang 6, Teil 3, Ziff. 5.1.7 KritisV.

I. Energierecht

Eine Überschneidung zwischen IT-Sicherheitsrecht und DSGVO ist auch im Energierecht denkbar. Zwar benötigen die Betreiber von Energieversorgungsnetzen oder Energieanlagen keine personenbezogenen Daten zur unmittelbaren Erbringung ihrer Dienste.[45] Im Zuge der Energiewende sollen allerdings die bisherigen Stromzähler zunehmend durch Smart-Meter ersetzt werden, um den Strombedarf zu analysieren und die Nachfrage an das Angebot anpassen zu können. Folglich sind Smart-Meter künftig für die Sicherheit der Versorgung mit Elektrizität von hoher Bedeutung.

Dabei verarbeiten sie in großem Umfang Daten über den Verbrauch von Elektrizität des jeweiligen Haushalts. Diese Daten lassen sich zumindest dem jeweiligen Anschlussinhaber zuordnen und sind mithin personenbezogen.[46] Aus diesen Daten lassen sich auch tiefgehende Rückschlüsse auf das Privatleben der Haushaltsmitglieder ziehen lassen (wie etwa Schlaf- und An- bzw. Abwesenheitszeiten).[47] Mithin ist auch die Datensicherheit zur Vermeidung von Beeinträchtigungen an Rechten und Freiheiten der betroffenen Personen von hoher Bedeutung.

Sachlich liegt also auch hier eine Überschneidung vor, bei der mit dem Smart-Meter als „zentraler Baustein des digitalisierten Energienetzes" und damit gleichsam als „Teil einer kritischen Infrastruktur" zugleich auch in großem Umfang personenbezogene Daten verarbeitet werden.[48] Allerdings werden die Anforderungen an Smart-Meter im Messstellenbetriebsgesetz (MsbG) geregelt, dessen technische Vorschriften (§§ 19 Abs. 1, Abs. 2, 21 Abs. 1, 22 Abs. 1 MsbG) diese beiden Aspekte berücksichtigen.[49] Insofern existiert hier bereits eine lex specialis, die für den kleinen Bereich der Smart-Meter eine einheitliche Regelung sowohl mit Blick auf die IT-Sicherheit als auch die Datensicherheit enthält.

45 Aber gleichwohl mittelbar, etwa zu Abrechnungszwecken.
46 *Bretthauer*, EnWZ 2017, 56 (57); *Keppler*, EnWZ 2016, 99 (100).
47 *Bretthauer*, EnWZ 2017, 56 (57) m.w.N.
48 *Stevens*, CR 2021, 841 (841).
49 *Stevens*, CR 2021, 841 (842, 844).

2. Gesundheitsversorgung

Auch im Kontext der Gesundheitsversorgung liegt eine solche Überschneidung vor. Krankenhäuser i.S.d. § 108 SGB V stellen nach bisheriger Rechtslage (§ 6, Anhang 5, Ziff. 1.1 BSI-KritisV) eine kritische Infrastruktur dar[50] und werden wohl auch unter der künftigen Rechtslage als (besonders) wichtige Einrichtungen (§ 28 Abs. 1 Nr. 4, Abs. 2 Nr. 3 i.V.m. Anlage 1, Ziff. 4.1.1. RegE BSIG) und ggf. auch als kritische Anlagen (§ 28 Abs. 1 Nr. 1 i.V.m. §§ 2 Nr. 22, 56 Abs. 4 RegE BSIG) erfasst. Gleichzeitig verarbeiten sie mit den Patientendaten (besonders sensible) personenbezogene Daten im Sinne der DSGVO.[51] Dabei liegen erneut einheitliche informationstechnische Systeme vor, so dass bei sicherheitsrelevanten Ereignissen entsprechend auch die Schutzgüter beider Rechtsregime betroffen sein können.[52]

3. Dienste in digitalen Ökosystemen

Weiterhin stellt sich die Problematik im Bereich der Zahlungsdienste. Anbieter[53] derselben müssen sowohl die Vorgaben nach Art. 6 ff. DORA (*lex specialis* gegenüber dem RegE BSIG im IT-Sicherheitsrecht)[54] als auch der DSGVO einhalten. Daneben müssen Cloud-Dienste soweit sie personenbezogene Daten verarbeiten erneut die DSGVO als auch den RegE BSIG[55] einhalten. Schließlich tritt beim automatisierten Fahren neben die DSGVO auch das fahrzeugbezogene IT-Sicherheitsrecht der UN-R 155.[56]

---

50 Sofern sie den Schwellenwert von 30.000 vollstationären Fällen pro Jahr übersteigen, Anhang 5, Teil 3, Ziff. 1.1 BSI-KritisV.

51 Sog. Gesundheitsdaten werden in Art. 4 Nr. 15 DSGVO auch ausdrücklich definiert. Zum Umgang mit Patientendaten unter der DSGVO: *Bieresborn*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 8 ff.; *Schütze/Spyra*, RDV 2016, 285 (285 ff.).

52 Zu Compliance-Anforderungen sowohl aus DSGVO als auch BSIG sowie weiteren Vorschriften siehe: *Nadeborn/Dittrich*, Int. Cybersecur. Law Rev. 2022, 147 (153 ff.).

53 Zu den Kategorien erfasster Unternehmen im Einzelnen: Art. 2 Abs. 1 DORA.

54 Siehe die entsprechende Ausnahme von der Erfassung als (besonders) wichtige Einrichtung sowie als kritische Anlage in § 28 Abs. 5 Nr. 1, Abs. 6RegE BSIG.

55 Siehe § 28 Abs. 1 Nr. 4, Abs. 2 Nr. 3, Anhang I, Ziff. 6.1.4. RegE BSIG.

56 UN-Regelung Nr. 155 zur Cybersicherheit und zum Cybersicherheitsmanagement bei Fahrzeugen; siehe zu den Verweisen aus dem europäischen Recht: Art. 5 Abs. 1, Anhang II D4 VO 2018/858 i.V.m. Art. 4 Abs. 5 lit. d, Anhang II D 4 VO 2019/2144.

Diese Dienste werden darüber hinaus inzwischen von großen Digitalkonzernen angeboten, die ausgehend von ihrem ursprünglichen Geschäftsbereich weiter in andere (elementare) Lebensbereiche vordringen und auf diese Art sog. digitale Ökosysteme[57] aufbauen. So verhält es sich etwa bei Alphabet und Apple, die neben vielen anderen Diensten u.a. eigene Zahlungsdienste und eigene Cloud-Dienste[58] anbieten und im Fall von Alphabet darüber hinaus im Bereich des automatisierten sowie des vernetzten Fahrens (Tochterfirma: *Waymo*) engagiert sind.[59] Es zeigt sich mithin die Tendenz dieser Unternehmen immer neue, häufig auch verbundene Märkte zu erschließen.[60] Zugleich sind alle diese Märkte in hohem Maße datengetrieben und die Verarbeitungen fallen daher in den Anwendungsbereich der DSGVO.

Es ist daher zu erwarten, dass bei diesen Unternehmen die Personalisierung und die dafür notwendige Verarbeitung personenbezogener Daten größere Dimensionen annimmt, als bei Unternehmen die ausschließlich auf einzelnen Märkten aktiv sind. Damit dürfte die Angriffsmotivation sowie die Folgen von Zwischenfällen in diesen Ökosystemen wachsen, sowohl mit Blick auf die größere Menge personenbezogener Daten als auch der Betroffenheit verschiedener (kritischer) Dienste. Gleichzeitig wird sich in diesen Strukturen die Überschneidung von Sicherheitsanforderungen an die Informationstechnik aus dem Datensicherheitsrecht und verschiedenen Bereichen des IT-Sicherheitsrechts (z.B. RegE BSIG, DORA, UN-R 155) stetig ausweiten.[61]

57 In einem solchen werden somit verschiedene Dienste wie etwa Zahlungs-, Cloud- und Streamingdienste „unter einem Dach" angeboten, Vgl. *Bosse et al*., DuD 2024, 82 (83); *Bräutigam*, in: Bräutigam/Rücker, E-Commerce, 1 (22, 25 ff.) mit der Differenzierung u.a. nach suchmaschinenbasierten Ökosystemen (Alphabet), Commerce-basierte Ökosysteme (Amazon), endgerätebasierten Ökosystemen (Apple) und Social Media-basierte Ökosysteme (Meta).

58 Explizit zur Erfassung von iCloud, allerdings noch unter der alten Rechtslage: *M. Fischer*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 299 (320), Rn. 99.

59 *Scheuer*, Waymo - Was ein Robotaxi-Selbstversuch über autonomes Fahren sagt, Handelsblatt vom 11.08.2023.

60 Hoeffer/Lehr, Online-Plattformen und Big-Data auf dem Prüfstand, NZKart 2019, 10 (11).

61 Grundlegend ebenso: *Hornung/Schallbruch*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 23 (31), Rn 36.

4. Telekommunikationsrecht

Hinsichtlich des Telekommunikationsrechts nimmt die DSGVO in Art. 95 DSGVO (EG 173) zwar eine horizontale Abgrenzung zum Kommunikationsrecht vor,[62] allerdings verhindert dies nicht, dass die Daten über einen Lebenszyklus hinweg unterschiedlichen IT-Sicherheitsanforderungen unterworfen sind.

Das TKG verpflichtet in § 165 Abs. 1 i.V.m. § 3 Nr. 61, 40 die Anbieter sog. nummernunabhängige, interpersoneller Kommunikationsdienste dazu, die Sicherheit dieser Dienste zu gewährleisten. Hierzu gehören nach EG 17 der umgesetzten EECC-RL insbesondere auch E-Mail-Dienste, die folglich für den Kommunikationsprozess dem TKG unterfallen.

Allerdings verarbeiten E-Mail-Dienste die Daten teilweise auch darüber hinaus weiter. So werden etwa von *Gmail* Inhaltsdaten wie folgt erhoben: „Wir erheben auch die Inhalte, die Sie bei der Nutzung unserer Dienste erstellen, hochladen oder von anderen erhalten. Dazu gehören beispielsweise E-Mails, die Sie verfassen und empfangen […]."[63] Als Zwecke werden insoweit angegeben die „Bereitstellung unserer Dienste", die „Wartung und Verbesserung unserer Dienste" als auch die „Personalisierung unserer Dienste".[64] Lediglich hinsichtlich personalisierter Werbung wird eine Verarbeitung der E-Mail-Daten (und anderen u.a. sensiblen Daten) ausgeschlossen.[65]

Da diese Verarbeitungen in keinem Zusammenhang mehr mit dem eigentlichen Kommunikationsvorgang stehen, dürften sie nicht mehr unter das Telekommunikationsrecht, sondern die DSGVO fallen. Damit unterfallen die personenbezogenen Daten in einem informationstechnischen System (Mail-Server) im Laufe der Verarbeitung zunächst dem TKG und dann der DSGVO, so dass auch hier eine Schnittmenge (etwa bei der Systemsicherheit) entsteht.

62 Jedenfalls soweit es öffentlich zugängliche Kommunikationsdienste betrifft, *J. Eckhardt*, in: Geppert/Schütz, Beck'scher Kommentar zum TKG, 5. Auflage 2023, § 165, Rn. 9.

63 Alphabet, Google-Datenschutzerklärung, 04.03.2024, abrufbar unter: https://policies.google.com/privacy#infocollect, zugegriffen am 17.04.2024.

64 Wie zuvor.

65 Wie zuvor.

V. Fazit

Insgesamt zeigt sich auch anhand der dargestellten, unterschiedlich geprägten Überschneidungsbereiche, dass eine Harmonisierung der unterschiedlichen Regelungen ein wichtiges Anliegen für die zukünftige Ausgestaltung des Daten- und IT-Sicherheitsrechts darstellt. Immer mehr Unternehmen, wie auch die Anbieter der digitalen Dienste, unterfallen in diesem Bereich mehreren Gesetzen. In der bisherigen Ausgestaltung sind die Gesetze diesbezüglich nur wenig hilfreich und geben ohne eine nachvollziehbare Systematik unterschiedliche Schutzziele vor, die obendrein auf unterschiedliche Schutzobjekte bezogen werden. Es fehlt an übereinstimmenden Definitionen des Risikos ebenso wie an der gesetzlichen Vorgabe der zugehörigen Risikomethodik. Es bestehen somit wie gezeigt insgesamt erhebliche Inkohärenzen.

Deshalb sollten insbesondere das Datensicherheits- und das IT-Sicherheitsrecht stärker harmonisiert werden, um Widersprüche zu vermeiden und ein effizientes Risikomanagement in diesen Bereichen zu ermöglichen. Dies reduziert wie aufgezeigt nicht nur den Aufwand für die betroffenen Unternehmen; wichtiger ist aus normativer Sicht vielmehr, dass die jeweiligen Schutzgüter effizienter geschützt werden, wenn diese in einem gemeinsamen Managementprozess erfasst werden und so auch etwaige Wechselwirkungen berücksichtigt werden können. Insbesondere können so sowohl kumulierende Risiken, d.h. solche Risiken die sowohl datensicherheits- als auch aus IT-Sicherheitsrechtliche Folgen haben optimal erfasst werden als auch mögliche Zielkonflikte erkannt und bewältigt werden.

Der Anspruch der Harmonisierung gilt in besonderem Maße für die Anforderungen an die Sicherheitsgewähr in Form von Schutzzielen und auch dem hier untersuchten Prinzip der Resilienz, da diese den Begriff der Sicherheit maßgeblich konturieren und damit der wesentliche Anknüpfungspunkt dafür sind, welche Schutzmaßnahmen zu treffen sind.

All dies betrifft insbesondere auch die hier exemplarisch herangezogenen digitalen Dienste. Auf sachlicher Ebene tritt auch bei diesen zusätzlich wie beschrieben noch die offene Systemarchitektur hinzu, die neben anderen Aspekten zu einer hohen Ungewissheit führt. Mit der Resilienz (nur) in der DSGVO wird nun ein weiteres, möglicherweise gerade mit Blick auf Ungewissheiten inhaltlich sehr sinnvolles, aber zunächst jedenfalls auch rechtlich disharmonisches Element implementiert, was deshalb im Folgenden untersucht werden soll.

B. Untersuchungsgegenstand

Diese Untersuchung leistet einen Beitrag zur Bewältigung der soeben skizzierten Ausgangslage, indem sie die neue Anforderung der Resilienz aus dem Datensicherheitsrecht untersucht und die Möglichkeit eines Transfers derselben in das IT-Sicherheitsrecht eruiert, um eine Harmonisierung der beiden Rechtsregime voranzubringen und den regulatorischen Mehrwert der Resilienz bei der Sicherheitsgewährleistung auch im IT-Sicherheitsrecht nutzen zu können.

In einem zweiten Schritt wird hierzu das *neue Merkmal der Resilienz in Art. 32 Abs. 1 lit b) DSGVO* in seinem Bedeutungsgehalt für die genannten, ungewissen Herausforderungen beschrieben. Methodisch wird dabei eine nach den vier juristischen Auslegungsmethoden (sog. canones)[66] konsistente Definition geliefert und diese anhand o.g. Szenarios der Manipulation personalisierter digitaler Dienste, welches zuvor noch genauer modelliert und beschrieben wird (erster Schritt), überprüft.
Drittens wird untersucht, ob sich der so definierte Begriff der Resilienz, unter Herausarbeitung aller relevanten Unterschiede zwischen dem Daten- und IT-Sicherheitsrecht, auch in letzteres, *namentlich § 30 Abs. 1 RegE BSIG, übertragen lässt* und somit der regulatorische Mehrwert des Resilienzbegriffs auch hier genutzt sowie ein höheres Maß an rechtlicher Kohärenz erreicht werden kann. Auch hier wird zur Überprüfung der Ergebnisse wieder das genannte Szenario bemüht.
Am Ende der Untersuchung wird neben einer Zusammenfassung der Ergebnisse eine *rechtliche Gestaltungsempfehlung zur Resilienz im Daten- und IT-Sicherheitsrecht* gegeben. Zu den einzelnen Schritten wird auf den Gang der Untersuchung (S. 53 ff.) verwiesen.

Neben dem hier gegenständlichen RegE BSIG existieren wie bereits bei der rechtlichen Ausgangslage noch zahlreiche weitere Vorschriften des IT-Sicherheitsrechts i.e.S., die hier jedoch nicht in den Untersuchungsgegenstand mit einbezogen werden. Sie sollen aber in *Eingrenzung des Untersuchungsgegenstandes* an dieser Stelle kurz angedeutet werden:

Hierzu gehören innerhalb des IT-Sicherheitsrecht i.e.S. zunächst insbesondere auch §§ 11 Abs 1a, 1b EnWG oder § 165 TKG und Art. 6 ff. DORA. Daneben verlangt auch der Art. 34 Abs 2 UAbs. 2 DSA von Anbietern

66 *Rüthers/C. Fischer/Birk*, Rechtstheorie, S. 432 ff.; *Savigny*, System des heutigen Römischen Rechts, Band 1, 1840, S. 213 f.

sehr großer Online-Plattformen und sehr großer Online-Suchmaschinen, mithin auch aller hier genannten digitalen Dienste,[67] u.a. die Risiken zu berücksichtigen, die durch „vorsätzliche Manipulation ihres Dienstes, auch durch unauthentische Verwendung oder automatisierte Ausnutzung des Dienstes" und nach Art. 35 Abs. 1 entsprechend zu mindern, was nach hiesigem Verständnis ebenfalls eine Anforderung der IT-Sicherheit darstellt.

Außerdem regeln die Art. 9, 15 KI-VO-E, dass für Hoch-Risiko-KI-Systeme ein Risikomanagement etabliert und hierdurch auch deren „Cybersicherheit"[68] gewährleistet werden muss. Als Hoch-Risiko-KI-Systeme sind insbesondere auch KI-Systeme erfasst, die als „Safety"-Komponenten in kritischen Infrastrukturen eingesetzt werden (Anhang III, Ziff. 2; Art. 2 Nr. 44h KI-VO-E). Allerdings sind die hier im Szenario behandelten KI-Systeme in den digitalen Diensten zum Ranking bzw. zur Empfehlung von Webinhalten *keine Hoch-Risiko-KI-Systeme*[69] und folglich auch diesen Anforderungen nicht unterworfen. Sie werden daher ebenfalls nicht weiter berücksichtigt.

Ebenfalls keine Berücksichtigung in dieser Arbeit finden die Anforderungen nach § 19 Abs. 4 TDDDG, wonach Anbieter von geschäftsmäßig angebotenen Telemedien, im Rahmen des technisch möglichen und wirtschaftlich Zumutbaren, technische und organisatorische Maßnahmen treffen müssen, die einen Zugang auf die technischen Einrichtungen ihrer Telemedienangebote ausschließen und diese Einrichtungen gegen Störungen durch äußere Angriffe sichern.

Diese Vorgaben gelten auch für Anbieter digitaler Dienste, da es sich bei diesen Diensten zugleich um geschäftsmäßig angebotene Telemedien handelt.[70] Insofern besteht eine idealkonkurrierende Verpflichtung.[71] Der Gesetzgeber sah hierin aber jedenfalls bislang keine Schwierigkeit; vielmehr sei diese Doppelerfassung wegen der unterschiedlichen Schutzgüter geboten: Der § 8c BSIG (§ 30 RegE BSIG) verfolge als Umsetzung von Art. 16

67 Siehe die Benennung durch die EU-Kommission, Pressemitteilung vom 25.04.2023, abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_23_2413, zuletzt abgerufen am 16.04.2024.

68 Ob und inwieweit in Zeiten allgegenwärtiger Vernetzung tatsächlich ein Unterschied zwischen Cybersicherheit und IT-Sicherheit besteht ist zweifelhaft, siehe hierzu: *Kipker*, in: Kipker, Cybersecurity, 1 (2 f.).

69 Siehe hierzu die Liste der Hoch-Risiko-KI-Systeme in Anhang 3, KI-VO-E.

70 *Schallbruch*, CR 2016, 663 (666).

71 Vgl. *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity, 499 (566), Rn. 240; *Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechts-Handbuch, 50.1, Rn. 420.

NIS-RL die Gewährleistung der Verfügbarkeit der digitalen Dienste,[72] wohingegen die Vorgängervorschrift des § 19 Abs. 4 TDDDG (§ 13 Abs. 7 TMG a.F.) die (individuelle) Gewährleistung der informationellen Selbstbestimmung sowie der Vertraulichkeit und Integrität informationstechnischer Systeme der Nutzer verfolge.[73]

Da der Schutz personenbezogener Daten, der in § 13 Abs. 7 TMG a.F. enthalten war aber in der Neufassung entfallen ist, dürfte zumindest das Recht auf informationelle Selbstbestimmung kein Schutzgut mehr sein.[74] Damit verbleibt für § 19 Abs. 4 TDDDG lediglich das Schutzgut der Vertraulichkeit und Integrität informationstechnischer Systeme der Webseitennutzer;[75] wobei sich die Frage stellt, ob § 8c BSIG (§ 30 RegE BSIG) dieses Schutzgut nicht jedenfalls auch mit abdeckt, so dass bei digitalen Diensten eine unnötige Doppelregulierung vorläge.

Weiterhin existiert mit dem Entwurf zum Cyber-Resilience-Act (CRA-E) bald auch eine horizontale (d.h. nicht auf bestimmte Sektoren beschränkte), produktbezogene Regulierung, die bereits dem Namen nach einen Bezug zum hiesigen Untersuchungsgegenstand der Resilienz aufweisen könnte. Daneben existieren produktbezogene Regulierungsansätze mit Vorgaben an Hersteller kritischer Komponenten (§ 41 RegE BSIG) sowie in einzelnen Sektoren wie etwa für Medizinprodukte (MedizinProdVO) oder Funkanlagen (RED).

Im Unterschied dazu betreffen sowohl die DSGVO als auch § 30 RegE BSIG die IT- bzw. Datensicherheit in komplexen, informationstechnischen Systemen eines Betreibers bzw. eines Verantwortlichen. Die einzelnen Komponenten dieser Systeme werden im Regelfall nicht von diesen selbst hergestellt, sondern nur zusammengefügt, betrieben und müssen sodann als Ganzes durch entsprechende technische organisatorische Maßnahmen gesichert werden. Hierin liegt ein fundamentaler Unterschied zu der durch den CRA-E und die anderen genannten Regulierungen forcierten Gewähr von IT-Sicherheit einzelner Produkte, welche insbesondere durch den Her-

72 Diese Beschränkung auf die „Verfügbarkeit" dürfte das Schutzgut der NIS-RL des BSIG nur unzureichend beschreiben, siehe: EG 1, 48 NIS-RL; ausführlich S. 222 ff.

73 BT-Drs. 18/11620, S. 5, a.E.; kritisch dazu: *Schallbruch*, CR 2017, 798 (800).

74 Vgl. *J. Eckhardt/Lepperhoff*, in: Schwartmann/Jaspers/Eckhardt, TTDSG 2022, § 19, Rn. 70, wonach die Sicherheit der Verarbeitung nun (ausschließlich) unter Art. 32 DSGVO fällt.

75 Ursprüngliche Ziel war insofern die IT-Systeme der Nutzer vor über Webseiten verbreitete Schadsoftware zu schützen: *J. Eckhardt/Lepperhoff*, in: Schwartmann/Jaspers/Eckhardt, TTDSG 2022, § 19, Rn. 83; BT-Drs. 18/4096, S. 34.

steller und somit auch bereits bei Entwicklung zu leisten ist. Die daraus folgenden Differenzen zwischen beiden Regelungsansätzen werden daher als zu hoch eingeschätzt, um diese im Rahmen der gegenständlichen Untersuchung zur Bestimmung der Resilienz noch adäquat bewältigen zu können, obwohl sicherlich auch die Resilienz einzelner informationstechnischer Produkte für eine holistische IT- und Datensicherheit von hoher Bedeutung sein dürfte.[76]

C. Gang der Untersuchung

Im folgenden Abschnitt werden die bereits angedeuteten Einzelschritte der Untersuchung detailliert dargestellt:

I. Funktionsweise und Manipulation von Personalisierungsalgorithmen

Um die für die rechtlichen Untersuchungsgegenstände bestehenden, sachlichen Grundlagen zu schaffen, stellt das *zweite Kapitel* dieser Untersuchung das Szenario und damit zunächst die Funktionsweise der *algorithmenbasierten Personalisierung* näher dar und ordnet dabei den Vorgang der Personalisierung anhand von personenbezogenen Daten zunächst in die Kategorien *Daten, Information, Wissen* (DIW-Modell) ein (A.).

Die Generierung von Wissen mit dem Ziel autonome, personalisierte Entscheidungen zu treffen, stellt in Zeiten zunehmend leistungsfähiger IT-Anwendungen eine immer häufigere Erscheinungsform in digitalen Diensten dar.[77] Die entsprechenden technischen Grundlagen mit der Entwicklung von automatisierter Verarbeitung, über die autonome Verarbeitung und maschinelles Lernen bis hin zu den konkreten autonomen Entscheidungen in personalisierten Diensten werden sodann unter (B.) erläutert.

Schließlich werden in Abschnitt C. mit Blick auf die Gewährleistung der Daten- und IT-Sicherheit die unterschiedlichen *Möglichkeiten der Manipulation* der algorithmenbasierten Personalisierung beschrieben. Dies erfolgt sowohl abstrakt anhand des unter A. dargestellten Modells als auch anhand einer kurzen Abhandlung der technischen Angriffsmöglichkeiten. Dabei

76 Gleiches gilt auch für die Adressierung kritischer Komponenten; mehr dazu im Ausblick, S. 335 ff.

77 Vgl. zur Verbreitung der Personalisierung: *Montgomery/M. D. Smith*, Journal of Interactive Marketing 2009, 130 (132 ff.); *Pariser*, Filter Bubble, S 14 ff.

werden die zwei unterschiedlichen Angriffsvektoren des Szenarios herausgearbeitet: Erstens die *singuläre Informationsmanipulation* (II.), bei der das Personenprofil eines einzelnen Nutzers (Personenwissen) und somit seine individuellen Dienstergebnisse manipuliert werden. Dieser Angriffsvektor ist somit für die Datensicherheit und Art. 32 DSGVO relevant. Zweitens die *plurale Informationsmanipulation* (III.) bei der in großflächiger Weise manipulierte Informationen von zahlreichen (gefälschten) Nutzeridentitäten eingebracht werden, die das abstrakte Lernwissen beeinträchtigen, die Dienstergebnisse somit generell verändern und daher für § 30 RegE BSIG und die IT-Sicherheit relevant sind.

II. Resilienz in Art. 32 DSGVO

Im *dritten Kapitel* wird sodann als mögliche Antwort auf die zuvor beschriebenen Situationen auf die Bedeutung des Merkmals der Resilienz eingegangen. Die Resilienz wird zunächst aus Art. 32 DSGVO heraus definiert, der in Abs. 1 lit b) als Maßnahme die Fähigkeit verlangt, „die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit [Resilienz] der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen."

Zum Vorverständnis werden hierfür der Anwendungsbereich des Art. 32 innerhalb der DSGVO (A.) und die Schutzgüter (Individualrechtsgüter) erläutert, zur Sicherung derer die Datensicherheit gewährleistet werden soll (B.). Anschließend folgt die Bestimmung des Merkmals „Resilienz" nach den vier juristischen Auslegungsmethoden (C.). Hierfür werden zunächst die wichtigen Vorbegriffe Datensicherheit, Maßnahmen, Systeme, und Dienste erläutert (I.). Diese Begriffe sind einer Befassung mit dem Rechtsbegriff Resilienz denklogisch vorgelagert, zum einen da die Resilienz als eine Anforderung der *Datensicherheit* ebenfalls durch *Maßnahmen* umgesetzt wird und zum anderen, weil sich die Resilienz als Merkmal zusammen mit den Schutzzielen auf *Systeme* und *Dienste* bezieht.

Die eigentliche Auslegung beginnt sodann mit dem *Wortlaut* (II.), wobei mangels eines allgemeingültigen Verständnisses auf verschiedene Fachdisziplinen, die den Begriff der Resilienz verwenden, zurückgegriffen wird. Anschließend folgt die *systematische Auslegung* mit Blick auf die übrigen, für die Resilienz maßgeblichen Elemente des Rechtssatzes in Art. 32 Abs. 1 lit b), namentlich den Risikobegriff (sowie die Risikomethodik), die Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) sowie die Syste-

me und Dienste. Es folgt noch die Auslegung nach der *Historie* (IV.), in der auf die vorangegangene DS-RL und die Entwicklung der DSGVO eingegangen wird sowie nach dem *Telos* mit Blick auf die neuen Realweltphänomene, auf die die Resilienz eine Antwort geben kann (V.). Schließlich wird in VI. das Auslegungsergebnis mit einer Definition der Resilienz vorgestellt.

Nachdem nun eine solche Definition besteht, wird die Bedeutung und Funktionsweise der Resilienz anhand der personalisierten Dienste und dem Angriffsvektor der singulären Informationsmanipulation demonstriert (D.), wobei neben der hier bestehenden Ungewissheit (I.) insbesondere auf die einzelnen Elemente der Resilienzdefinition: Ereigniserkennung (II.1), Anpassungsfähigkeit (II.2) und Erholung (III.3) eingegangen wird. Schließlich wird noch die abstrakte Angemessenheit der Resilienzmaßnahmen erläutert (III.)

III. Übertragbarkeit in § 30 RegE BSIG

Im *vierten Kapitel* wird gezeigt, ob und inwieweit die Resilienz in das IT-Sicherheitsrecht, namentlich den für digitale Dienste relevanten § 30 RegE BSIG, übertragen werden könnte.

Hier wird zunächst auf die *Schutzgüter des IT-Sicherheitsrechts* eingegangen (A.), die anders als im Datensicherheitsrecht jedenfalls nicht primär im Bereich des Individualgüterschutzes, sondern v.a. auch im Schutz von Gemeinschaftsrechtsgütern[78] liegen, die auf die kontinuierliche und sichere Erbringung bestimmter (kritischer) Dienstleistungen (hier in digitaler Form: Suchmaschinen, Online-Marktplätze und soziale Netzwerke) angewiesen sind. Zur genaueren Bestimmung der Schutzgüter wird zunächst die historische Entwicklung des (RegE) BSIG nachgezeichnet (I.). In einem zweiten Schritt werden dann die Schutzgüter der für diese Regelung prägenden kritischen Anlagen herausgearbeitet (II). Anschließend wird untersucht, wie im Verhältnis dazu die Schutzgutbetroffenheit bei den digitalen Diensten ausfällt (III.).

78 Der Begriff Gemeinschaftsrechtsgüter bezeichnet in dieser Untersuchung öffentliche Interessen, die (analog zu Individualrechtsgütern wie Grundrechten) durch eine fehlende IT-Sicherheit beeinträchtigt werden können: Hierunter fallen insbesondere *Gemeinwohlziele* sowie Teile der *öffentlichen Sicherheit* (Funktionsfähigkeit des Staates und seiner Einrichtungen sowie der Schutz der objektiven Rechtsordnung) und der Erhalt der Umwelt; ausführlich dazu ab S. 230.

Im nächsten Abschnitt (B.) werden sodann die IT-Sicherheitsvorgaben des RegE BSIG systematisch beschrieben, in die sich die Resilienz einfügen müsste. Hierzu gehören die Begriffe der IT-Sicherheit und die Schutzziele (I.), außerdem die Systeme, Dienste, Daten und Informationen (II.) sowie schließlich das Risiko (auch unter Berücksichtigung der Risikomethodik) und die Angemessenheit (III.).

Im Anschluss werden in C. die genannten Vorgaben mit jenen der DSGVO, wie sie bereits im Abschnitt zur Resilienz (3. Kapitel, C., I. und III.) herausgearbeitet wurden, gegenübergestellt und -soweit Unterschiede vorliegen- die Folgen derselben für eine Integration der Resilienz herausgearbeitet. Dies betrifft insbesondere die Unterschiede zwischen den Definitionen der Daten- und IT-Sicherheit (I.), der Bedeutung der Schutzziele und des Dienstes (II.) sowie den Systemverständnissen (III.). Schließlich werden noch die (kleineren) Unterschiede bei dem Risiko und der Risikomethodik einschließlich der Angemessenheit betrachtet (IV.). In der Zusammenfassung (V.) werden sodann alle relevanten Unterschiede zwischen Art. 32 DSGVO und § 30 RegE BSIG dargestellt und die jeweiligen Folgen für die Resilienz benannt.

Schließlich wird unter D. die gleichwohl mögliche Übertragung der Resilienz in den RegE BSIG untersucht. Hierfür werden bestehende Elemente im IT-Sicherheitsrecht untersucht, die bereits in die Richtung der Resilienz weisen (I.) und die telelogischen Gründe dargelegt, die auch für eine Einführung der Resilienz im IT-Sicherheitsrecht sprechen (II.). Das Kapitel schließt mit einer Bewertung der Implementierungsmöglichkeiten der Resilienz in den RegE BSIG (III.).

Unter E. wird schließlich demonstriert, dass die Resilienz auch im Sinne des RegE BSIG für den Angriffsvektor der pluralen Informationsmanipulation einen Mehrwert für die Gewährleistung der IT-Sicherheit im gewählten Szenario liefern kann. Dabei werden die Ungewissheit (I.) und insbesondere die hier teilweise abweichenden Maßnahmen für die einzelnen Resilienzelemente (Ereigniserkennung, II.1, Anpassungsfähigkeit II.2, Erholung, II.3) dargestellt. Zum Abschluss (III.) wird erneut die abstrakte Angemessenheit der Resilienzmaßnahmen bestimmt.

IV. Zusammenfassung und Gestaltungsempfehlung

Die Arbeit schließt mit dem *fünften Kapitel,* in dem zunächst die Ergebnisse zusammengefasst werden (A.). Dies umfasst sowohl die Definition der

Resilienz nach der DSGVO (I.) als auch die Ergebnisse zu den identifizierten Unterschieden zwischen DSGVO und RegE BSIG und in der Folge der Übertragbarkeit des Resilienzbegriffs in das IT-Sicherheitsrecht (II.).

Anschließend wird noch eine Gestaltungsempfehlung (B.) gegeben, wie der Rechtsrahmen des Daten- und IT-Sicherheitsrecht für eine wirksame Umsetzung der Resilienz gestaltet werden sollte.

Die Untersuchung endet mit einem Ausblick (C.) zu möglichen Weiterentwicklungen der Resilienz im IT-Sicherheitsrecht und darüber hinaus.

2. Kapitel: Funktion und Manipulation der algorithmenbasierten Personalisierung

Nach dieser Einleitung wird nun im *zweiten Kapitel* vertieft auf das Szenario dieser Untersuchung eingegangen, an dem die praktische Bedeutung der Resilienz als Rechtsbegriff für die Daten- und IT-Sicherheit später demonstriert werden soll. Dabei werden v.a. die Funktionsweise der *algorithmenbasierten Personalisierung* und die Möglichkeit zur *Manipulation* dargestellt.

Im Einzelnen wird zunächst eine Darstellung anhand des Daten-, Informations-, Wissensmodells (DIW-Modells) vorgenommen (A.), mithilfe dessen die grundlegende Funktionsweise aus einer informationsrechtlichen Sicht nachgezeichnet werden soll. Als Ergänzung sollen in einem weiteren Schritt zumindest grob die zugrundeliegenden technischen Aspekte erläutert werden (B.). Im letzten Abschnitt dieses Teils (C.) wird sodann die Manipulation der Informationen als Angriff in diesem Szenario dargestellt.

A. Ermittlung von Personenwissen nach dem DIW-Modell

In einem ersten Schritt soll hierfür die Verarbeitung von Daten für die Personalisierung näher dargestellt werden.

Dabei ist Personalisierung ein Ausdruck einer neuen Form der Informationsverarbeitung: So waren IT-Systeme früher meist eher statische Systeme in denen Informationen vorrangig nur aufbewahrt, organisiert und zu spezifisch festgelegten Zwecken verarbeitet wurden, z.B. die Verwaltung und Pflege einer Kund:innendatenbank. Eine neue Erscheinung sind hingegen sog. „lernende Systeme", die automatisiert und teilweise sogar autonom (dazu in Abschnitt B.) aus den Daten zunächst Informationen sowie Wissen erzeugen, auf Basis dessen sie dann eine Entscheidung treffen und eine Steuerungswirkung herbeiführen. Zu beachten ist, dass sich das hier beschriebene Modell nur auf elektronische Datenverarbeitung bezieht und somit keine allgemeingültigen Definitionen für „Informationen" und „Wissen" liefern kann, welche weit über den Gegenstand der hier vorliegenden Untersuchung hinausgehen und wohl bis in philosophische Fragestellungen

hinein reichen würde.[79] Siehe zur Illustration der nachfolgenden Ausführungen bereits die Abbildung, S. 43, Abb. 2.

I. Daten

Die erste Kategorie des Informationsmodells bilden die Daten. Entgegen dem Sprachgebrauch bilden die Daten selbst oft gar nicht den Anknüpfungspunkt für rechtliche Regelungen wie etwa das Datenschutzrecht.[80] Denn der Begriff Daten beschreibt lediglich Zeichen, die durch Speicherung auf einem Datenträger physisch verkörpert werden und als (potenzielle) Grundlage für Informationen[81] sowie letztlich auch für Wissen und Entscheidungen dienen.[82] Diese Zeichen sind als solche jedoch rein syntaktischer Natur und können daher als „global" und „neutral" angesehen werden.[83] Sie erschöpfen sich auf tiefster Computer-Ebene bekanntlich in sog. Bits, deren Wert nur 0 oder 1 betragen kann. Jeweils 8 Bits bilden ein Byte, was in der IT regelmäßig das kleinste adressierbare Element mit 256 (2 hoch 8) möglichen Zuständen darstellt. Eine logische Ebene höher werden in der Informatik verschiedene Datentypen unterschieden, so z.B. Ganze Zahlen (INTEGER), Zeichen/Buchstaben (Char) oder logische Werte, insbesondere true/false (BOOLEAN). Aus mehreren Einzeldaten (ggf. mit unterschiedlichen Datentypen) lassen sich schließlich komplexere Datenstrukturen wie ein Datensatz abbilden. Ein Datensatz könne etwa in einem Serverlog-Eintrag wie diesem bestehen:

> 203.0.113.195 - user [07/Oct/2024:10:43:00 +0200] "GET /index.html HTTP/2.0" 200 2326

Diese Datensätze tragen schon erste Kennzeichen einer Semantik, da im Rahmen der Programmierung die Auswahl und die Anordnung der einzelnen Daten bereits mit einer verwendungsspezifischen Intention erfolgte. Damit wird der an sich der Information zuzuordnende Verwendungskon-

79 Vgl. *Aamodt/Nygård*, Data & Knowledge Engineering, Vol. 16 (1995), 191 (193).
80 BT-Drs. 17/8999, Fünfter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft", S. 21.
81 *Albers*, in: Spiecker gen. Döhmann/Collin, Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 50 (54); *Spiecker gen. Döhmann*, RW 2010, 247 (253); *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (400), Rn. 23.
82 *Kloepfer*, Informationsrecht, S. 26; *Ebsen*, DVBl 1997, 1039 (1039).
83 *Aamodt/Nygård*, Data & Knowledge Engineering, Vol. 16 (1995), 191 (203).

text bereits in die Datenerhebung hineingetragen (bei einem Server-Log z.B. die Erkennung von Angriffen oder aber die Reichweiten-Messung). Insofern kann man attestieren, dass die jeweils erzeugten Datenstrukturen bereits *durch den informatorischen Verwendungskontext* determiniert sind.[84] Oder anders formuliert: Die Semantik der erzeugten Datensätze ist so gestaltet, wie es zur Interpretation zumindest der primären Informationen dienlich ist.

Damit von „personenbezogenen Daten" gesprochen werden kann, müssen diese Daten bzw. die daraus interpretierbaren Informationen zumindest einer Person zugeordnet werden können (auch dazu sogleich ausführlicher).

II. (Persönliche) Information

Die nächsthöhere Kategorie im Verarbeitungsprozess stellen die Informationen dar; sie sind von den Daten zu unterscheiden, aus denen sie interpretiert wurden.[85] Auch durch die eben beschriebenen determinierten Datenstrukturen reduziert sich de facto lediglich das Maß der Interpretationsleistung, die erforderlich ist, damit ein Datensatz zu einem Sinnelement und damit zu einer Information werden kann.[86]

Zur Interpretation dieser Daten sind stets entsprechende Kontextinformationen bzw. Kontextwissen erforderlich,[87] etwa über den Datentyp: Andernfalls lässt sich beispielsweise nicht erkennen, ob die Zeichenkette „AFFE" als das gleichnamige Säugetier (Datentyp: char) oder die Zahl 45054 (hexadezimal) interpretiert werden soll.[88]

Einen Sonderfall bei der Informationsinterpretation aus Daten stellen sog. Big-Data-Anwendungen dar. Dort werden große Datenmengen analy-

84 Vgl. *Aamodt/Nygård*, Data & Knowledge Engineering, Vol. 16 (1995), 191 (203), die insofern dahingehend differenzieren, dass zwar die Daten an sich neutral sind, aber nicht die Art und Weise der Datenerzeugung.

85 *Jendrian/Weinmann*, DuD 2010, 108 (108); *Eckert*, IT-Sicherheit, S. 4.

86 *Albers*, in: Spiecker gen. Döhmann/Collin, Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 50 (54).

87 *Freimuth,* Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, S. 66; *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts, 107, § 22, Rn. 12 f.; zur Abgrenzung zwischen Informationen und Wissen sogleich unter III.

88 *Jendrian/Weinmann*, DuD 2010, 108 (108); weiterführend zu den Schwierigkeiten bei Datensignatur und Informationsinterpretation: *Fox*, DuD 1997, 386 (387).

siert, die häufig ursprünglich zu anderen Zwecken erhoben wurden.[89] Aus diesen Daten soll folglich dann eine andere, als die ursprünglich vorgesehene Information interpretiert werden, so dass die jeweilige Semantik der Datensätze nicht mehr zwingend hilfreich ist, sondern ganz im Gegenteil sogar erhöhten Aufwand hervorrufen und größeren Raum für Fehlinterpretationen schaffen kann.

Eine durch Interpretation gewonnene oder auch jede sonstige Information enthält bei logischer Betrachtung[90] zumindest ein Subjekt[91] sowie einen Wert, eine Handlung oder eine Eigenschaft (nachfolgend: Parameter), den sie diesem Subjekt zuweist. Nur eine Information bietet somit auch für das Datenschutzrecht hinreichende persönlichkeitsrechtlich relevante Anknüpfungspunkte, die ihre Verarbeitung unter Aspekten des „Datenschutzes" daher entweder als legitim oder als verboten erscheinen lassen können. Insbesondere knüpfen an die Information die Interessen des Trägers des Grundrechts auf informationelle Selbstbestimmung, ob und inwieweit staatliche Stellen oder private Dritte diese Information erhalten und verarbeiten können sollen.[92] Das dem Schutz der informationellen Selbstbestimmung dienende Datenschutzrecht müsste daher streng genommen auch „Informationsschutzrecht" heißen.[93] Bezüglich der „Datensicherheit" ist der Begriff hingegen sachgerecht, da durch ein entsprechendes Ereignis wie einen Hacker-Angriff stets zunächst die Daten betroffen sind.

Eine Information kann und wird regelmäßig aus mehreren Parametern, also Einzelinformationen bestehen, die sich aber zweckgerichtet als eine Information zusammenfassen lassen.[94]

89 Vgl. *S. Schulz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 6, Rn. 151.

90 Siehe zur syntaktischen, semantischen und pragmatischen Dimension von Information: *Kloepfer*, Informationsrecht, S. 24, Rn. 53 ff.

91 Im Datenschutzrecht stets eine Person; in Abgrenzung dazu eine Sache, wenn es sich um eine Sachinformation handelt.

92 Fn. 80.

93 *Spiecker gen. Döhmann*, RW 2010, 247 (255); *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts, 107 (114), Rn. 8 f.; auch die DSGVO knüpft in der insoweit missverständlichen Definition „personenbezogener Daten" im Kern an Informationen an, die sich auf eine betroffene Person beziehen (Art. 4 Nr. 1 DSGVO): *Veil*, NVwZ 2018, 686 (687).

94 Vgl. *Steinmüller*, Informationstechnologie und Gesellschaft, S. 197.

Beispiele für persönliche Informationen aus o.g. Auflistung sind daher:

– Bei seinem Webseitenaufruf am 01.03.2024 um 15:00 nutzte X das Endgerät Y.
– Am [Datum, Uhrzeit] suchte X nach das Produkt Y.

Aus der Interpretation von Daten ergeben sich indes nicht zwingend sinnstiftende Informationen. Dies ist zwar der Regelfall und insbesondere dann zu erwarten, wenn Informationen von Hand in ein IT-System eingegeben werden, also z.B. in das Bestellformular eines Webshops und damit quasi erst durch die Eingabe in Daten überführt werden.

Es mag allerdings auch andere Fälle geben. Im Normalfall wird bei o.g. Beispiel auf programmtechnischer Ebene des Webshops höchstwahrscheinlich eine MySQL-Datenbank gefüllt, wenn der/die Nutzer:in das Bestellformular ausfüllt. In dieser Datenbank, die sich letztlich als Tabelle verstehen lässt, wird eine neue Zeile angelegt und entsprechend der Spalten (z.B. „Vor- und Nachname" „Anschrift", „Zahlungsdaten") befüllt. Mithin wurden persönliche Informationen eingegeben, die im Idealfall nun durch die Daten als Träger repräsentiert werden.[95]

Gehen wir aber davon aus, der Programmierer des Webshops beherrschte sein Handwerk nicht und die Eingabe-Funktion ist grob fehlerhaft: Sie legt nicht für jede(n) Kund:in eine neue Zeile an, sondern verteilt die einzelnen Angaben eines bzw. einer Kund:in nach dem Zufallsprinzip über die Zeilen der Tabelle. In diesem Fall wurden unstreitig Daten geschaffen, eine Information zu einer einzelnen Person werden sie aus diesen Daten indes kaum erkennen können. Besteht die gewünschte Information dagegen darin, aus welchen PLZ-Bereichen die Kund:innen kommen, so lässt sich diese Information gleichwohl auch aus einer solch „fehlerhaft" gefüllten Datenbank interpretieren.[96]

Insofern verdeutlicht sich an diesem Beispiel die Subjektivität der Interpretation, d.h. die Gewinnung von Informationen durch die Interpretation

95 *M. Wagner,* Datenökonomie und Selbstdatenschutz, S. 33; *Börding et al.*, CR 2017, 134 (134).

96 Jenseits dessen gibt es außerdem Fälle, etwa in Folge von Angriffsszenarien oder auch bei technischen Defekten, bei denen sog. Stör- oder Zufallsdaten, die sich auch bei noch so ambitionierter Interpretation überhaupt nicht zu einer Information zusammenführen lassen. Dies müsste im Idealfall auch auf dieser Ebene der „Datenanalyse" erkannt werden, bevor hieraus unzutreffende Informationen interpretiert werden; *Tremmel*, Neue Schadsoftware möchte IoT-Geräte zerstören, golem.de vom 26.06.2019.

von Daten ist stark von dem individuellen Zweck- und Verwendungskontext abhängig[97] und jede Information ist damit „zweckrelativ".[98] Werden Informationen an Dritte weitergegeben, werden sie zunächst (wieder) in Daten überführt und müssen vom Empfänger neu als Informationen interpretiert werden. Diese Informationen sollten zwar zumeist, müssen aber nicht zwingend mit der ursprünglichen Information übereinstimmen.

III. Wissen

Aus Informationen kann in einem weiteren Schritt „Wissen" generiert werden. Auch wenn es kaum eine allgemeingültige Abgrenzung zwischen Information und Wissen geben kann,[99] lässt sich zumindest attestieren, dass Wissen durch die lernende Verknüpfung von Einzelinformationen entsteht.[100] Die Einzelinformationen werden hierbei „organisiert und systematisiert",[101] um daraus einen über die quantitative Informationsmenge hinausgehenden Erkenntnisgewinn zu erzielen.

Wissensgenerierung ist damit, wie zuvor die Interpretation von Daten zur Informationserlangung, ein subjektiver Prozess, der abhängig von dem Verarbeitungskontext und der Zweckrichtung des Verarbeiters ist (dazu sogleich mit einem Beispiel). Erfolgt diese Interpretation im Wege einer automatisierten Verarbeitung durch Algorithmen, so treffen diese diverse Zwischenentscheidungen im Umgang mit den verfügbaren Informationen. Diese können insbesondere in die vier Kategorien *Priorisierung, Klassifikation, Assoziation* und *Filterung* unterteilt werden.[102]

Für das zu erlangende Wissen ist für das hier betrachtete Szenario zwischen zwei Kategorien zu unterscheiden. Zum einen das Wissen über eine spezifische Person, das z.B. in einem Profil mit entsprechenden übergreifenden Eigenschaften zusammengefasst wird und am Ende z.B. in der Zahlungsbereitschaft für ein bestimmtes Produkt ausgedrückt wird. Es wird in diesem Kontext als *Personenwissen* bezeichnet.

---

97 Vgl. *M. Wagner,* Datenökonomie und Selbstdatenschutz, S. 32

98 *Steinmüller*, Informationstechnologie und Gesellschaft, S. 199 f.; *Aamodt/Nygård*, Data & Knowledge Engineering, Vol. 16 (1995), 191 (198).

99 *M. Wagner,* Datenökonomie und Selbstdatenschutz, S. 30.

100 Vgl. *Aamodt/Nygård*, Data & Knowledge Engineering, Vol. 16 (1995), 191 (200); als „subjektive […] Vernetzung von Informationen": *Picot/Neuburger*, ZfCM 2005, 76 (76).

101 *Spiecker gen. Döhmann*, RW 2010, 247 (253).

102 *Diakopoulos*, Digital Journalism 2015, 398 (400 ff.).

Zum anderen gibt es Wissen aus der vergleichenden Betrachtung von Informationen vieler Personen, etwa um bestimmte Muster zu erkennen (z.B. dass sich Nutzer:innen die sich für das Produkt A (oder auch zugleich für B und C) interessieren mit hoher Wahrscheinlichkeit auch für Produkt D interessant finden werden). Dies kann man auch als *abstraktes Lernwissen oder Wissensbasis*[103] bezeichnen.

Diese Wissensgenerierung kann auch weiter verschachtelt sein, so dass aus einzelnen Wissenskategorien eine übergeordnete Erkenntnis erlangt werden kann.[104] Im Fall personalisierter Preise setzt sich das Wissen über die Zahlungsbereitschaft beispielsweise aus zwei Unterkategorien zusammen, wie dem Wissen über die Produktinteressen und dem Wissen über die Preissensibilität.

Schließlich ist zu berücksichtigen, dass auch die Kategorisierung in Informationen und Wissen subjektiver Natur ist. Für denjenigen, der die Verarbeitung vornimmt, werden aus Daten Informationen interpretiert und hieraus Wissen generiert. Wird das Wissen z.B. über ein Produktinteresse hingegen an Dritte weitergegeben, kann es sich für diesen wiederrum zunächst nur als aus Daten interpretierte Information darstellen.

IV. Entscheidung und Verhaltenssteuerung

Die zuvor genannten Wissenskategorien werden im Rahmen des Entscheidungsprozesses unterschiedlich einbezogen. Zum einen muss situationsabhängig untersucht werden, welches Personenwissen für eine bestimmte Entscheidung relevant ist. Hinsichtlich des abstrakten Lernwissens muss darüber hinaus noch geprüft werden, ob dieses auf die konkrete Person anwendbar ist, z.B. indem eine entsprechende Gruppenzugehörigkeit festgestellt wird.

Am Ende einer solchen Verarbeitung steht eine Entscheidung, bei der das gewonnene Wissen angewendet und in eine Interaktion mit dem Nutzer überführt wird. Die o.g. Wissenskategorien wirken sich dabei wie folgt aus: Zum einen wird verglichen, wie sich andere Personen in der Situation verhalten haben - das Profil des Betroffenen wird insoweit verwendet, als dass eine Zuordnung zu einer bestimmten Gruppe vorgenommen wird.

103 Siehe zu dem Begriff Wissensbasis: *Beierle/Kern-Isberner*, Methoden wissensbasierter Systeme, S. 11.

104 Vgl. *Aamodt/Nygård*, Data & Knowledge Engineering, Vol. 16 (1995), 191 (200).

Daneben wird das Personenwissen, also z.B. das Wissen über Produktinteressen aus Informationen wie der individuellen Bestellhistorie oder bisherige Reaktionen in sozialen Netzwerken abgeleitet.

Beides zusammen führt dann zu einer *algorithmenbasierten Entscheidung*[105] wie etwa dem/der Nutzer:in einen bestimmen Inhalt, ein Produkt oder einen ermittelten Preis für ein Produkt anzubieten. Damit findet eine indirekte *Steuerung* des/der Nutzer:in statt, d.h. im Erfolgsfalle wird diese(r) aufgrund der (passenden) Entscheidung des Algorithmus' zur Annahme des Angebots motiviert.

Die Steuerungswirkung auf den/die Nutzer:in liegt mithin entweder in der Auswahl, d.h. Filterung und der Präsentation von bestimmten Inhalten oder in der Vorgabe eines (vermeintlich) attraktiven Preises. Der/die Nutzer:in, welche(r) ein solches Angebot annimmt, hat diese Steuerungswirkung gebilligt und sich insoweit -idealtypisch freiwillig und wissentlich- aus Sicht des Dienstanbieters steuern lassen. Die Steuerung beschreibt im Falle personalisierter Dienste die Übernahme eines Entscheidungsprozesses, d.h. der/die Nutzer:in verzichtet im Vertrauen auf das Dienstangebot auf eine eigene, persönliche Entscheidung.

Schlägt die Steuerungswirkung fehl, reagiert der/die Nutzer:in also nicht wie beabsichtigt, so kann aus dessen/deren Reaktion, die wiederrum eine Information darstellt, aber zumindest neues individuelles Wissen „erlernt" werden. Etwa wenn der/die Nutzer:in eine Produktseite mit einem personalisierten Preis aufruft und sodann unter „Ähnliche Artikel" ein günstigeres Produkt aussucht. Das spräche möglicherweise dafür, dass die Zahlungsbereitschaft zu hoch angesetzt wurde, was bei künftigen Preisentscheidungen berücksichtigt werden kann. Im Ergebnis führt auch dies zu einer stetigen Präzisierung auch des Wissens über jede einzelne Person und damit grundsätzlich zu immer besseren Entscheidungen und erfolgreicherer Verhaltenssteuerung.

105 Es ist insofern darauf hinzuweisen, dass die Datenethikkommission ein abweichendes Begriffsverständnis verwendet, welches teilweise auch in der Kommentarliteratur zu Art. 22 DSGVO rezipiert wird: Hier meinen algorithmenbasierte Entscheidungen solche, bei denen für eine Entscheidung immer noch ein Mensch verantwortlich ist, der aber durch Algorithmen unterstützt wird; Was hier als algorithmenbasierten Entscheidung beschrieben wird, entspricht nach der Begrifflichkeit der Datenethikkommission dem algorithmendeterminierten Entscheidung, siehe: DEK, Gutachten der DEK, Oktober 2019, S. 17; *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 22, Rn. 14.

V. Zusammenfassung

Die Daten stellen die technische Grundlage dar, die durch Algorithmen verarbeitet werden. Aus ihnen werden im ersten Interpretationsschritt Informationen und aus diesen wiederrum in einem zweiten Interpretationsschritt Wissen gewonnen. Hierzu zählt sowohl individuelles *Personenwissen* (Person A interessiert sich für X) als auch *abstraktes Lernwissen*, z.B. über bestimmte Gruppeneigenschaften (Gruppen mit Eigenschaft B, C, D interessieren sich mit hoher Wahrscheinlichkeit für X). Beide Wissenskategorien dienen als Grundlage einer automatisierten, personalisierten Entscheidung und diese verursacht bei positivem Verlauf eine Steuerungswirkung bei dem von dieser Entscheidung Betroffenen.

B. Technische Grundlagen

Im nun folgenden Schritt werden die technischen Grundlagen für den zuvor dargestellten Veredlungsprozess von Daten über Informationen und Wissen bis hin zu einer Entscheidung kurz erläutert. Grundlegend findet dieser Prozess in Form einer Verarbeitung statt. Eine solche kann sowohl automatisiert (I.) als auch autonom (II.) erfolgen. Unter III. wird dann noch spezifisch auf die Verarbeitung im Rahmen personalisierter Dienste eingegangen.

I. Automatisierte Verarbeitung

Von einer Automatisierung i.S.d. Art. 4 Nr. 2 DSGVO kann bereits dann gesprochen werden, wenn eine Verarbeitung mit technischen Hilfsmitteln vorgenommen wird.[106] Dies umfasst insbesondere die elektronische Datenverarbeitung (EDV),[107] bei der die Daten anhand einer programmtechnisch, d.h. durch Algorithmen vorgegebene Logik verarbeitet werden.

Denkbar sind damit etwa Empfehlungen anhand sachlicher Verknüpfungen, wie die Empfehlung entsprechender Zubehör- zu einem Hauptartikel. Bei dieser Form der Verarbeitung wurde programmtechnisch eine entsprechende Funktion implementiert, mit der in einer Datenbank einem Haupt-

106 *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 4, Rn. 17.

107 *Schild*, in: BeckOK DatenschutzR, 47. Edition 2024, Art. 4 DSGVO, Rn. 34.

artikel ein oder mehrere Zubehörartikel zugeordnet werden können und diese daher dem/der Kundin, wenn er oder sie den Hauptartikel kauft, angeboten werden. Auch automatisierte Empfehlungssysteme (dazu sogleich ausführlich), die z.B. Artikel mit ähnlichen Eigenschaften zu den bereits ausgewählten vorschlagen, fallen unter diese automatisierte Verarbeitung.

Entscheidend für die Abgrenzung zur nachfolgenden autonomen Verarbeitung ist insoweit, dass die Logik und die Entscheidung der Zuordnung und Empfehlung der Zubehörartikel final von einem menschlichen Entscheider festgelegt bzw. getroffen wird (*regelbasierte Programmierung*).[108] Das Sachwissen über diese Zuordnung (Zubehör-/Hauptartikel) oder zumindest das Regelwissen zur Programmierung, z.B. eines automatisierten Empfehlungssystems ist mithin bei diesem schon vorhanden und wird von ihm in das informationstechnische System eingebracht.

II. Autonome Verarbeitung durch maschinelles Lernen

Anders verhält es sich bei autonomer Verarbeitung. Hier beruhen die Empfehlungen des Systems auf Entscheidungen, denen ein maschinelles Lernverfahren vorangegangen ist. Wie die Bezeichnung des *maschinellen Lernens (ML)* bereits nahelegt, ist es hier nicht mehr (allein) ein menschlicher Entscheider, der durch die Programmierung auf Basis bereits vorhanden Wissens den Verarbeitungsprozess abschließend vorgibt.[109] Vielmehr kann ein ML-System nach einer entsprechenden Implementierung selbstständig lernen, d.h. Wissen erwerben,[110] indem es Muster oder Korrelationen erkennt[111] und auf dieser Basis auch eigenständige Entscheidungen trifft.[112] Es handelt sich mithin immer noch um eine algorithmenbasierte Personalisierung. Allerdings werden die Algorithmen zur Entscheidungsfindung nicht mehr (ausschließlich) durch ein(e) Programmierer:in vorgegeben;

108 Vgl. *Staehelin*, GRUR 2022, 1569 (1569); *Steege*, MMR 2019, 715 (716).

109 Vgl. *Sattler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 197 (220 f.).

110 *Portugal/Alencar/Cowan*, Expert Systems with Applications, Vol. 97 (2018), 205 (206).

111 *Buxmann/H. Schmidt*, in: Buxmann/Schmidt, Künstliche Intelligenz, 3 (11); *Sattler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 197 (220 f.) m.w.N.

112 *Hof*, in: Tinnefeld/Buchner/Petri/Hof, Einführung in das Datenschutzrecht, 477 (485), Rn. 18; zu den unterschiedlichen Verfahren des MLs: *Buxmann/H. Schmidt*, in: Buxmann/Schmidt, Künstliche Intelligenz, 3 (10 ff.).

vielmehr verändert sich die Entscheidungsfindung eines ML-Systems beim Lernen autonom.[113]

Es wird somit z.B. möglich die Aktivitäten der Nutzer:innen auf einem Online-Marktplatz, einem sozialen Netzwerk oder einer Online-Suchmaschine zu erfassen und hierin bislang unbekannte Muster zu erkennen und auf Basis dessen neue Empfehlungen zu generieren. Sowohl die Entscheidungen einer autonomen Verarbeitung, als auch solche die (ausschließlich) auf einer automatisierten Verarbeitung beruhen, unterfallen grundsätzlich dem Tatbestand des Art. 22 Abs. 1 DSGVO, der aber bei den hiesigen personalisierten Diensten mangels rechtlicher oder in ähnlicher Weise erheblich beeinträchtigenden Wirkung dieser Entscheidungen nicht erfüllt sein dürfte.[114]

III. Verarbeitung in personalisierten Dienstangeboten

Entscheidungen werden bei den digitalen Diensten in der Form personalisierter Dienstangebote getroffen. Hierfür werden (ggf. auch ML-gestützte) Empfehlungssysteme verwendet. So werden sie u.a. von dem Onlinemarktplatz-Anbieter *Amazon* genutzt, um dem/der Nutzer:in entsprechend personalisierte Angebote machen zu können.[115] Im Falle einer personalisierten Suche (z.B. *Google Personalized Search)* können auf eine Suchanfrage hin die Ergebnisse an den jeweiligen Nutzer angepasst werden, sowohl in ihrer Auswahl (z.B. durch das Entfernen zumindest vermeintlich irrelevanter Ergebnisse) als auch bezüglich der angezeigten Reihenfolge der Suchergebnisse (sog. Re-Ranking).[116] Schließlich werden Empfehlungssysteme für die

113 Vgl. *Buxmann/H. Schmidt*, in: Buxmann/Schmidt, Künstliche Intelligenz, 3 (9 f.).

114 So etwa zu Preisdifferenzierungen und personalisierter Werbung: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 22, Rn. 27 ff. Ob man bei den Feeds sozialer Netzwerke oder den Ergebnissen von einer Online-Suchmaschine das Erfordernis einer „nicht nur marginalen" Beeinflussung der persönlichen Entfaltungsfreiheit (*Martini*, ebd.) erreicht, und somit zu einem anderen Ergebnis kommt, wäre zumindest diskussionswürdig, soll aufgrund des Fokus' dieser Untersuchung auf die Datensicherheit aber nicht weiter verfolgt werden.

115 *Linden/B. Smith/York*, IEEE Internet Computing 2003, 76 (76).

116 *Z. Ma/Pant/Sheng*, ACM TOIS, Vol. 25 (2007), Heft 1, 1 (5); zu Begriff und Funktionsweise des Rankings: *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 75 (83 f.).

Auswahl der angezeigten Beiträge in den Feeds sozialer Netzwerke verwendet.[117]

Um eine verlässliche technische Darstellung vornehmen zu können, ist die Personalisierung von Preisen noch zu wenig verbreitet und wissenschaftlich erforscht, wobei die nachfolgenden Mechanismen grundsätzlich auch hierfür verwendet werden können.[118] Deshalb wird im Nachfolgenden nur auf die Personalisierung bei den zuvor genannten personalisierten Diensten eingegangen, d.h. die Personalisierung von Suchergebnissen einerseits und das Geben bzw. Hervorheben von Empfehlungen unabhängig von einer konkreten Suchanfrage andererseits.

Empfehlungssysteme (en: Recommender Systems) bringen ihre Entscheidung in der Empfehlung eines bestimmten Elements (en: Item) zum Ausdruck.[119] Inzwischen besteht in Art. 3 lit s) DSA[120] auch eine gesetzliche Definition: ein „Empfehlungssystem" ist demnach

> *„ein vollständig oder teilweise automatisiertes System, das von einer Online-Plattform verwendet wird, um auf ihrer Online-Schnittstelle den Nutzern bestimmte Informationen vorzuschlagen oder diese Informationen zu priorisieren, auch infolge einer vom Nutzer veranlassten Suche, oder das auf andere Weise die relative Reihenfolge oder Hervorhebung der angezeigten Informationen bestimmt;"*

Ein „vollständig automatisiertes System" dürfte wie in Art. 22 Abs. 1 DSGVO „ausschließlich auf einer automatisierten Verarbeitung beruhend" verstanden werden, so dass auch (teil-)autonom agierende, also ML-gestützte Empfehlungssysteme adressiert werden.

Bei den für Empfehlungssysteme verwendeten, technischen Ansätzen ist insbesondere zwischen „Content-based Filtering" (CBF) und „Collaborative Filtering" (CF) zu unterscheiden. In diesen finden sich auch die im Informationsmodell abgeschichteten Formen unterschiedlicher Wissensgenerierung wieder.

---

117 *Ziegler/Loepp*, in: Kollmann, Handbuch digitale Wirtschaft, 717 (719).

118 *Kamishima/Akaho*, in: Cantador/Brusilovsky/Kuflik, Proceedings of the 2nd International Workshop on Information Heterogeneity and Fusion in Recommender Systems, 57 (57 ff.).

119 *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 98 (105); *Ziegler/Loepp*, in: Kollmann, Handbuch digitale Wirtschaft, 717 (719); *Ricci et al.*, Recommender systems handbook, S. 1 ff.

120 Digital Services Act (EU-VO 2022/2065 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste).

Beim CBF werden die (bisherigen) Reaktionen (Feedback) der einzelnen Nutzer:innen auf bestimmte Elemente wie z.B. einem bestimmten Produkt auf einer Webseite erfasst. Äußert er oder sie dieses Feedback ausdrücklich auf Nachfrage zu einem zuvor empfohlenen Element, spricht man von explizitem Feedback; werden die Reaktionen hingegen nur „stillschweigend" überwacht und untersucht, spricht man von implizitem Feedback.[121] Ein Beispiel für letzteres ist, wenn ein(e) Nutzer:in einen Artikel auf einem Online-Marktplatz kauft oder auch nur danach sucht, was als positives Feedback bezüglich dieses Artikels angesehen werden kann.[122] Am Ende werden die aus diesen Feedbacks abzuleitenden Informationen über das bisherige Verhalten des Nutzers oder der Nutzerin in Form eines Profils zusammengeführt.[123] Dieses Profil wird sodann mit den verfügbaren „Content-", d.h. Inhaltsinformationen (auch als „Features" bezeichnet) über neue Elemente abgeglichen und bei einer entsprechenden Ähnlichkeit bzw. Übereinstimmung wird dann das jeweilige Element empfohlen.[124] Hat der/die Nutzer:in z.B. zuvor einen oder mehrere Film(e) positiv bewertet, die dem Comedy-Genre angehören (Feature), so würde das System ihm oder ihr noch weitere Filme aus diesem Genre empfehlen.[125] Das für diesen Abgleich verwendete individuelle Profil entspricht dem Personenwissen nach dem Informationsmodell.

Der Ansatz des CF ist dagegen nicht auf einzelne Nutzer*innen fokussiert, sondern nutzt das gesammelte Feedback von mehreren Nutzer:innen in einer kollaborativen Weise. Im Detail bestehen unterschiedliche Verfahren, zunächst können etwa Kohorten aus Nutzer:innen erstellt, die in der Vergangenheit an ähnlichen Elementen interessiert waren (kohortenbasiertes Verfahren).[126] Daraus wird geschlossen, dass die Übereinstimmungen innerhalb der Kohorten aus der Vergangenheit dazu führen, dass die zuge-

121 *Mahmoud/John*, in: SAI Intelligent Systems Conference (IntelliSys), Enhanced content-based filtering algorithm using Artificial Bee Colony optimisation, 155 (156).

122 *Aggarwal*, Recommender Systems, S. 1. Ausführlich zu dem von Amazon.com genutzten Collaborative Filtering: *Linden/B. Smith/York*, IEEE Internet Computing 2003, 76 (76, 78 f.).

123 *Mahmoud/John*, in: SAI Intelligent Systems Conference (IntelliSys), Enhanced content-based filtering algorithm using Artificial Bee Colony optimisation, 155 (155).

124 *Aggarwal*, Recommender Systems, S. 14. *Badriyah et al.*, in: Seventh International Conference on Innovative Computing Technology (INTECH), A hybrid recommendation system for E-commerce based on product description and user profile, 95 (95 f.).

125 *Ricci et al.*, Recommender systems handbook, S. 11.

126 *Aggarwal*, Recommender Systems, S. 2.

hörigen Nutzer:innen auch auf künftige Empfehlungen gleich oder zumindest ähnlich ansprechen.[127] Im Falle eines Online-Shops kann eine Kohorte aus ähnlichen Nutzer:innen gebildet werden, die in der Vergangenheit bestimmte Artikel gekauft oder bewertet haben. Die daraus aggregierte Menge an Elementen wird dann dem oder der jeweiligen Nutzer*in vorgeschlagen, wenn er/sie aufgrund des bisherigen Feedbacks ebenfalls dieser Kohorte zugeordnet werden kann; natürlich abzüglich aller Elemente, die der/die jeweilige Nutzer:in schon gekauft oder bewertet hat.[128] Daneben existieren auch weniger komplexe Ansätze wie etwa das Co-Visitation-Verfahren[129], bei dem zwei Elemente betrachtet werden, die von vielen Nutzer:innen gemeinsam bzw. direkt aufeinander folgend besucht werden (z.B. Gartenschere und Arbeitshandschuhe in einem Online-Shop). Es wird insofern davon ausgegangen, dass sich dieser Präferenzzusammenhang auch in Zukunft fortsetzt und daher den künftigen „Gartenscherenkund:innen" entsprechend empfohlen auch Arbeitshandschuhe zu kaufen.

Das Wissen über solche Präferenzzusammenhänge zwischen den Elementen (in den jeweiligen Kohorten) gehört im DIW-Modell in die Kategorie des abstrakten *Lernwissens*, was dann bei Erkennung einer entsprechenden Kohortenzugehörigkeit oder bei der Auswahl des entsprechenden Elements auf den/die jeweilige(n) Nutzer:in angewendet wird.

Werden CBF, CF und ggf. auch noch weitere Ansätze[130] kombiniert um eine Entscheidung zu treffen, spricht man von „hybrid filtering". In der Praxis ist dies innerhalb der Erbringung eines Dienstes häufig der Fall, um die Nachteile der einzelnen Ansätze zu kompensieren: So hat etwa CF den Nachteil, dass es keine neuen Elemente empfehlen wird, solange diese noch nicht von anderen Nutzer:innen bewertet wurden.[131] Dieses Problem hat CBF hingegen nicht, da es auch neue Elemente (nur) anhand der Ähnlichkeit zu anderen, bereits von dem/der Nutzer:in bewerteten Elementen

127 *Ricci et al.*, Recommender systems handbook, S. 2.

128 *Linden/B. Smith/York*, IEEE Internet Computing 2003, 76 (76).

129 *Mahmood/Adnan*, in: 9th International Conference on Networking, Systems and Security (NSysS), Detecting Fake Co-visitation Injection Attack in Graph-based Recommendation Systems, 30 (30 f.); *G. Yang/Gong/Cai*, in: Proceedings 2017 Network and Distributed System Security Symposium, Fake Co-visitation Injection Attacks to Recommender Systems, S. 2 f.

130 Exemplarischer weiterer Ansatz: Demographic Filtering, basiert auf demografischen Informationen über die Nutzer:innen wie Alter, Geschlecht, Beruf oder Bildung. um entsprechende Empfehlungen abzuleiten, vgl. *Aggarwal*, Recommender Systems, S. 19; *Ricci et al.*, Recommender systems handbook, S. 8.

131 *Ricci et al.*, Recommender systems handbook, S. 13.

vorschlagen kann.[132] Bei allen Ansätzen kann auch ML eingesetzt werden, um die Ergebnisse weiter zu verbessern.[133]

C. Manipulation der Informationen

Nach der modellhaften Beschreibung der algorithmenbasierten Personalisierung sowie den zugehörigen technischen Grundlagen werden nun die Möglichkeiten der Manipulation durch die Einspeisung korrumpierter Daten dargestellt. Aus diesen werden sodann unrichtige Informationen interpretiert, die dann die Wissenserzeugung sowie die darauf basierenden Entscheidungen beeinträchtigen.

Nach einer allgemeinen Darstellung (I.) wird auf die Unterfälle der singulären (II.) und der pluralen (III.) Informationsmanipulation eingegangen. Dieses Kapitel schließt mit einem Fazit, in dem die Resilienz als mögliche Gegenmaßnahme auf diese Manipulationen positioniert wird (IV.).

I. Allgemeine Darstellung

Es sind zunächst zwei Angriffsvektoren zu unterscheiden, die sich in ihrer unmittelbaren Wirkung unterscheiden:

1. Es werden für einzelne Identitäten der Nutzer:innen falsche Informationen in das System eingebracht. Diese werden im Rahmen des MLs richtig verarbeitet, also etwa klassifiziert, aber da die Informationen objektiv unrichtig sind, wird im System falsches *Personenwissen* erzeugt und am Ende trifft der personalisierte Dienst bezüglich dieser Person auch eine falsche, unpassende Entscheidung. Dies wird nachfolgend als *singuläre Informationsmanipulation* bezeichnet.
2. Werden hingegen viele Identitäten manipuliert bzw. viele künstliche Identitäten geschaffen und etwa über ein sog. Bot-Netz zentral gesteuert, ist es auch möglich, dass insbesondere ein im Modus des Online Lernens operierendes System „umtrainiert" wird, d.h. es wird falsches *Lernwissen* erzeugt indem etwa bei der Co-Visitation alle korrumpierten Systeme

132 Wie zuvor.

133 *Portugal/Alencar/Cowan*, Expert Systems with Applications, Vol. 97 (2018), 205 (205); teilweise wird dies dann auch als computational intelligence-based (CI-based) bezeichnet: *Lu et al.*, Decision Support Systems, Vol. 74 (2015), 12 (14 f.).

positives Feedback bezüglich zweier Elemente abgeben, zwischen denen tatsächlich kein Präferenz-Zusammenhang besteht. Für die Verarbeitung nach dem Informationsmodell bedeutet dies, dass künftig auch von echten, manipulationsfreien Nutzer:innen stammende Daten bzw. Informationen falsch verarbeitet werden, da Verarbeitung auf dem manipulierten Lernwissen beruht, was im Ergebnis deshalb auch bei diesen Nutzer:innen bzw. generell zu falschen Dienstentscheidungen führt. Dies wird nachfolgend als *plurale Informationsmanipulation* bezeichnet.

Beide Angriffsvektoren werden in den folgenden Abschnitten näher dargestellt.

II. Singuläre Informationsmanipulation

Werden nun z.B. durch das manipulierte Endgerät eines/einer Kund:in „unrichtige Informationen" in das System eingebracht, so stellt sich die Frage, wie sich dies im Rahmen des DIW-Modells auswirkt (1.). Anschließend wird die technische Ausgestaltung dieser Manipulation dargestellt (2.).

1. Wirkung nach dem DIW-Modell

In diesem Fall werden Einzelinformationen wie z.B. eine Suchanfrage in das System eingebracht, die wie folgt aussehen könnte:

Von dem Account des A fand am 08.08.19 um 13:30 Uhr eine Suche nach dem Produkt Y statt.

Zu beachten ist, dass diese Information bei einer technisch-neutralen Betrachtung nicht unrichtig ist. Die Produktsuche vom Account des A fand gleichwohl statt. Allerdings ist die abgeleitete Information vor dem vorliegenden Zweckkontext unrichtig. Hier sollen die Produktinteressen des A ermittelt werden. In diesem Kontext kommt es darauf an, ob die Produktsuche tatsächlich ein entsprechendes Produktinteresse indiziert und nicht ob rein technisch betrachtet eine entsprechende „Suchfunktion" aktiviert wurde. Mithin ist die Information vor diesem Hintergrund unrichtig, weil sie als Indikator für die Produktinteressen des A falsch ist.

Unter Berücksichtigung des o.g. Informationsmodells ist weiterhin festzustellen, dass die Datenbasis, die durch die Webseite bei der Suchfunktion

angelegt wurde, im Vergleich zu einem „echten" Suchvorgang unverändert ist. Mithin zeigt sich auch hier, dass es für die Frage, ob eine unrichtige oder richtige Information vorliegt auf den jeweiligen Zweck- und Interpretationskontext ankommt. Aus den manipulierten Daten wird unter Berücksichtigung des vorliegenden Zweckkontexts (Ermittlung der individuellen Präferenzen) eine unrichtige Information interpretiert. Man könnte daher auch formulieren, dass die Störungsursache darin liegt, dass die Daten nicht in diesen Zweckkontext passen, sondern missbräuchlich in diesen eingebracht wurden.[134]

2. Technische Ausgestaltung

Solche Einzelangriffe sind v.a. aus dem Bereich der sozialen Netzwerke[135] bekannt geworden: Grundlage ist i.d.R. das Ausspähen von Passwörtern ggf. i.V.m. der Ausnutzung fehlender 2-Faktor-Authentifizierung. Über den Kontozugriff werden dann nicht nur bereits vorhandene Daten ausgespäht oder manipuliert, sondern es werden vielmehr neue Daten in ein System eingebracht. Sofern die Personalisierung des Dienstangebots nicht (nur) über den Server, sondern auch über im Endgerät gespeicherte Daten (Cookies) erfolgt,[136] ist z.T. nicht mal ein Kontozugriff erforderlich.

Allgemein wurde das Phänomen des Einbringens von falschen Informationen bereits 2005 beobachtet, als der Wurm Samy neue, wenn auch belanglose Informationen in den Online-Dienst Myspace einbrachte: Durch den entsprechenden Schadcode fügte der Browser der Betroffenen unbemerkt den Autor des Wurms „Samy" auf Myspace als Freund hinzu und platzierte in den Profilen der Betroffenen die Zeichenfolge „but most of all, samy is my hero".[137] Ähnlich verhielt sich auch der Wurm Mikeyy, der

134 Dieser Gedanke findet sich auch in Art. 5 Abs. 1 lit b) DSGVO. Zwar spricht die DSGVO aufgrund der definitorischen Gleichstellung von Daten und Informationen in Art. 4 Nr. 1 DSGVO von „Datenrichtigkeit", konkretisiert aber in der Sache zutreffend, dass die Frage der Unrichtigkeit der Daten „im Hinblick auf die Zwecke ihrer Verarbeitung" zu beantworten ist.

135 *Sahoo/Gupta*, Enterprise Information Systems 2019, 832 (833).

136 *Xing et al.*, in: Proceedings of the 22nd USENIX Security Symposium, Take This Personally: Pollution Attacks on Personalized Services, 671 (680 f.).

137 *Grossman,* Cross-Site Scripting Worms & Viruses, Juni 2007, S. 8; *Alcorn*, Network Security 2006, 7 (8).

auf Twitter 2008 mindestens 190 Konten kompromittierte und von diesen mindestens 10.000 Tweets verschickte.[138]

Das hier gegenständliche Einbringen von Informationen zum Zwecke der zielgerichteten Manipulation eines Profils und damit letztlich auch des personalisierten Dienstes wird im Englischen auch als *„pollution attack"* bezeichnet.[139] Insofern wird nur der Dienst für den betroffenen Nutzer manipuliert, nicht hingegen der Empfehlungsdienst generell (dazu sogleich). In einer Studie konnte die Möglichkeit der Manipulation des Rankings der *Google Suche* als auch der von *Amazon* vorgeschlagenen Produkte bereits nachgewiesen werden. Hierfür wurden falsche Informationen im Sinne von tatsächlich nicht vom User vorgenommenen Suchanfragen bzw. Seitenaufrufen von Produkten in das Profil eingebracht und dieses somit verfälscht,[140] mithin falsches Personenwissen erzeugt. Dabei wurde der Umstand ausgenutzt, dass Web Authentifizierung in der Regel nur absichern kann, dass eine Anfrage von dem Browser oder der App eines Nutzers ausgelöst wurde, aber nicht sicherstellen kann, dass der Nutzer diese auch tatsächlich durchgeführt oder autorisiert hat.[141] Der vermeintlich vertrauenswürdige Endpunkt (Browser/App) wird mithin dahingehend korrumpiert, dass er bei seiner Benutzung unbemerkt manipulierte Anfragen an die jeweiligen Server richtet.

Auf beiden Webseiten (*Google Suche, Amazon*) konnten hierdurch die personalisierten Rankings der Suchergebisse bzw. die Produktempfehlungen manipuliert werden.[142] Grundsätzlich können solche *Pollution Attacks* gegen alle personalisierten Dienste und somit insbesondere auch gegen

138 *Luo et al.*, in: Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), An Analysis of Security in Social Networks, 648 (648); Teen claims responsibility for disrupting Twitter, CNN vom 13.04.2009.

139 *Xing et al.*, in: Proceedings of the 22nd USENIX Security Symposium, Take This Personally: Pollution Attacks on Personalized Services, 671 (671); *H. Huang et al.*, in: Proceedings 2021 Network and Distributed System Security Symposium, Data Poisoning Attacks to Deep Learning Based Recommender Systems, S. 3 f.; *M. Fang et al.*, in: Proceedings of the 34th Annual Computer Security Applications Conference, Poisoning Attacks to Graph-Based Recommender Systems, 381 (384); Technisch wird dies insbesondere durch sog. Cross-Site-Request-Forgery (kurz CSRF oder XSRF), umgesetzt, hierzu ausführlich: *Zeller/Felten,* Cross-Site Request Forgeries: Exploitation and Prevention S. 1 ff.

140 *Xing et al.*, in: Proceedings of the 22nd USENIX Security Symposium, Take This Personally: Pollution Attacks on Personalized Services, 671 (677 ff.).

141 *Zeller/Felten,* Cross-Site Request Forgeries: Exploitation and Prevention, S. 4.

142 Wie zuvor.

soziale Netzwerke wie *Facebook, Instagram* oder *Twitter* ausgeführt werden.[143]

III. Plurale Informationsmanipulation

1. Wirkung nach dem Informationsmodell

Bei der pluralen Informationsmanipulation werden anders als bei der singulären Informationsmanipulation unrichtige Informationen mit zahlreichen realen, aber korrumpierten oder gefakten Identitäten eingebracht. Dies kann zwar -bei realen Identitäten- wie zuvor zu einer Verfälschung des Personenwissens führen; vor allem wird aber durch diese Breite des Angriffs das *abstrakte Lernwissen* über die Beliebtheit von Items oder die Zusammenhänge zwischen mehreren Items beeinträchtigt.

2. Technische Gestaltung

Im Rahmen von Angriffen auf CF-Systeme spricht man hier auch von sog. *Shilling-Attacks:* Dabei wird eine große Anzahl von gefakten Identitäten erstellt oder es werden reale Identitäten manipuliert und mit diesen entweder positive (en: push-attack) oder negative Bewertungen (en: nuke-attack) abgegeben, um das System zur Abgabe falscher Empfehlungen zu zwingen.[144] So sind insbesondere sog. *Fake-Co-Visitation-Angriffe* möglich, d.h. es werden mit vielen Identitäten zwei Elemente (ein Zielelement und ein Ankerelement) aufgerufen, um zwischen diesen eine Präferenzverbindung *(Lernwissen)* herzustellen, so dass bei Auswahl des Ankerelements als nächstes das Zielelement empfohlen bzw. sogleich das bisherige Zielelement verdrängt wird.[145] Neben solchen gezielten Angriffen auf ein bestimmtes

143 *Xing et al.*, in: Proceedings of the 22nd USENIX Security Symposium, Take This Personally: Pollution Attacks on Personalized Services, 671 (684).

144 *Kaur/Goel*, in: 2016 International Conference on Inventive Computation Technologies (ICICT), Shilling attack models in recommender system, 1 (1 f.); *Sundar et al.*, IEEE Access, Vol. 8 (2020), 171703 (171704).

145 *G. Yang/Gong/Cai*, in: Proceedings 2017 Network and Distributed System Security Symposium, Fake Co-visitation Injection Attacks to Recommender Systems, S. 2, 10 ff.; *Y. Zhang et al.*, IEEE Trans. Inf. Forensics Secur., Vol. 15 (2020), 3807 (3809, 3813 f.); beispielsweise könnte im obigen Beispiel (S. 72) durch den Angriff bei Aus-

Empfehlungsverhalten sind außerdem ungezielte Angriffe möglich, die auf eine generelle Verschlechterung der Empfehlungsleistung abzielen.[146] In der Praxis ist beispielsweise der Online-Marktplatz *Amazon* nach einer wissenschaftlichen Untersuchung aus 2017 massiv von diesem Phänomen der falschen Bewertungen betroffen.[147] Im Recht benennt inzwischen auch der DSA dieses Phänomen in EG 57 mit Blick auf die „Einrichtung von Scheinkonten, die Nutzung von Bots und anderen automatisierten oder teilautomatisierten Verhaltensweisen".

Wird auch ML eingesetzt und soll ein dann zumeist online (auch: „inkrementell") lernendes ML-System manipuliert werden, spricht man auch von *Model Skewing* oder einer *Poisoning Attack* bzw. *Data Poisoning*.[148] Der entscheidende Angriffspfad liegt hier in dem Online-Training, d.h. in dem Umstand, dass regelmäßig neue Daten genutzt werden, um das Modell des ML-Systems zu aktualisieren.[149] Durch dieses fortlaufende Training mit neuen Daten kann es grundsätzlich ausreichen, nur geringe Datenmengen zu manipulieren um das Modell zu vergiften, d.h. es subtil „umzutrainieren", so dass es falsche Entscheidungen trifft.[150]

IV. Fazit und Ansatz für das Erfordernis der Resilienz

Wie voranstehend dargestellt können bei der Betrachtung von Angriffen zwei unterschiedliche Vektoren unterschieden werden. Zwar haben beide

---

wahl der Gartenschere (Ankerelement) statt der Arbeitshandschuhe eine Schreibtischlampe (Zielelement) empfohlen werden.

146 *Himeur et al.*, Computers & Security, Vol. 118 (2022), AS-Nr. 102746, S. 12; *Deldjoo/Di Noia/Merra*, ACM CSUR 2022, AS-Nr. 35, Heft 2, AS-Nr. 35, S. 8 ff.

147 *P. Liu et al.*, in: IEEE International Conference on Software Quality, Reliability and Security, Identifying Indicators of Fake Reviews Based on Spammer's Behavior Features, 396 (401 f.).

148 *Xue et al.*, IEEE Access, Vol. 8 (2020), 74720 (74723); diese Begriffe des Poisonings, also der Vergiftung, werden teilweise auch bei regelbasierten Empfehlungssystemen verwendet: *Chen et al.*, Trans Emerging Tel Tech 2021, AS-Nr. e3872, Heft 6, AS-Nr.: e3872.

149 *Heinemeyer/Herpig*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 65 (66); *Jagielski et al.*, in: 2018 IEEE Symposium on Security and Privacy (SP), Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning, 19 (19).

150 So reicht es beispielsweise in der personalisierten Medizin bereits aus bei den Sensoren der Medizingeräte weniger Patient:innen die Daten zu manipulieren, um die ML-Modelle, die für eine große Gruppe von Patient:innen genutzt werden, zu „vergiften": *Jagielski et al.,* wie zuvor.

Vektoren stark abstrahiert betrachtet den gleichen Auslöser (Manipulation des Datenflusses) sowie dieselbe informationstechnische Auswirkung (falsche Entscheidungen).

Allerdings werden bei einer *singulären Informationsmanipulation* lediglich bezüglich einzelner Identitäten falsche Informationen in das System eingebracht. Im Ergebnis ist damit insbesondere das Datenschutzgrundrecht betroffen, weil das persönliche Profil der jeweiligen Personen etwa durch die dargestellte *Pollution Attack* manipuliert wird. Es werden insoweit durch eine Sicherheitslücke unrichtige personenbezogene Daten in das System eingebracht und durch deren Verarbeitung wird im Ergebnis das *Personenwissen* in Gestalt des Profils beeinträchtigt.

Bei der *pluralen Informationsmanipulation* wird hingegen das *abstrakte Lernwissen* verändert, indem durch viele reale oder gefakte Accounts in großem Umfang falsche Informationen in das lernende System eingebracht werden (*Poisoning Attack*) und so die Entscheidungen des Systems generell beeinflusst werden. Ist dies erfolgreich, werden somit etwa Rahmen eines (ML-gestützten) CF-Empfehlungssystem auch für viele Personen falsche Entscheidungen getroffen, obwohl das individuelle Personenwissen auch weiterhin richtig sein kann.[151]

Die Ausgangslage für beide Angriffsvektoren besteht darin, dass von (vermeintlichen) Nutzer:innen stammende Informationen verwendet werden, die manipuliert sein können. Der Verantwortliche bzw. der Anbieter des jeweiligen Dienstes kann die Qualität der Informationen dabei nicht mit letzter Sicherheit garantieren, da diese Interaktionen beschreiben, die außerhalb seines Kontrollbereichs initiiert werden. So ist es ihm etwa nicht möglich mit letzter Sicherheit zu überprüfen, ob auf dem Endgerät, von welchem etwa Bewertungen oder Anfragen abgegeben werden, dieselben tatsächlich auch von der/dem jeweiligen Nutzer:in stammen. So könnte das Endgerät etwa kompromittiert sein; auf die Daten- und IT-Sicherheit desselben hat er regelmäßig keinen Einfluss.

Damit verbleibt eine erhebliche Ungewissheit über die Qualität der gesammelten Informationen und es kann insoweit als Hypothese vorweg gestellt werden, dass die *Resilienz* als besondere funktionale Anforderung solchen Ungewissheiten und den damit verbundenen Folgen entgegentreten muss.

151 Dies könnte grundsätzlich aber mit Art. 22 DSGVO angefochten werden, dazu sogleich.

Wichtig ist es, in diesem Zusammenhang darauf hinzuweisen, dass die weitere Untersuchung an dieser Stelle auf *die Resilienz als Erfordernis der Datensicherheit* ausgerichtet ist und insofern sich ausschließlich auf den Fall bezieht, dass personenbezogene Daten im Entscheidungsprozess manipuliert wurden. Nicht nachgegangen wird der Frage, ob und inwieweit eine automatisierte Entscheidung jenseits von Manipulationen der eigenen personenbezogenen Daten (etwa durch eine plurale Informationsmanipulation) nach Art. 22 DSGVO richtig sein muss. Nach Art. 22 Abs. 3 DSGVO kann eine automatisierte Entscheidung, die die betroffene Person als unbillig empfindet grundsätzlich im Rahmen des Art. 22 Abs. 3 DSGVO angefochten werden.[152]

152 Beachte allerdings zum Nicht-Vorliegen des Tatbestands des Art. 22 DSGVO bei personalisierten Inhaltsempfehlungen als auch bei der personalisierten Preisgestaltung bereits S. 69, Fn. 114.

3. Kapitel: Die Resilienz in der DSGVO

Der nachfolgend zu untersuchende Rechtsbegriff „Resilienz" wird in Art. 32 DSGVO eingeführt, der nach seiner Überschrift die „Sicherheit der Verarbeitung" zum Gegenstand hat.[153]

Um die Bedeutung dieses Rechtsbegriffs vollständig verstehen zu können, muss zunächst der Anwendungsbereich und der Normauftrag des Art. 32 innerhalb der DSGVO bestimmt werden (A.). Anschließend wird unter B. herausgearbeitet, welchem Schutzgut Art. 32 DSGVO und damit auch die Sicherstellung der Resilienz dient, wobei auch hierfür zunächst die Frage der Schutzgüter der DSGVO als solcher beantwortet werden muss.

Unter C. folgt die eigentliche Auslegung und Begriffsbestimmung der Resilienz. Im letzten Schritt dieses Teils (D.) wird die datensicherheitsrechtliche Bedeutung der so definierten Resilienz anhand der Manipulation personalisierter Dienste mit ihrer im vorangegangenen Teil dargestellten Funktionsweise demonstriert.

A. Anwendungsbereich von Art. 32 DSGVO

Zunächst wird der Anwendungsbereich von Art. 32 DSGVO dargestellt. Zur Gewährleistung der „Sicherheit der Verarbeitung" verpflichtet Abs. 1 den Verantwortlichen sowie den Auftragsverarbeiter zur Vornahme geeigneter technischer und organisatorischer Maßnahmen (toM). Diese Handlungspflicht findet sich in der DSGVO als solche auch in den Art. 24 und 25 DSGVO. Dadurch ist die Maßnahmenpflicht nun deutlich breiter ausgestaltet, als dass dies bislang durch § 9 BDSG i.V.m. der zugehörigen Anlage der Fall war.

153 In Deutschland war die Datensicherheit bis dahin ausschließlich in § 9 BDSG a.F. i.V.m. der zugehörigen Anlage geregelt. Nach dieser Vorschrift hatten die Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, „technische[n] und organisatorische[n] Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

Jedoch verfolgen diese drei Normen mit der Pflicht zur Implementierung von toM jeweils eigene Schutzzwecke:

Art. 24 spricht insoweit allgemein von der Sicherstellung und Nachweisbarkeit der Einhaltung der DSGVO, Art. 25 Abs. 1 von der wirksamen Umsetzung der Datenschutzgrundsätze nach Art. 5 DSGVO und der Aufnahme notwendiger Garantien (Datenschutz durch Technikgestaltung) bzw. Art. 25 Abs. 2 von der Gewährleistung von Datenschutz durch datenschutzfreundliche Voreinstellungen. Schließlich zielt Art. 32 unter der Überschrift „Sicherheit der Verarbeitung" auf die Gewährleistung eines dem Risiko für Rechte und Freiheiten natürlicher Personen angemessenen Schutzniveaus ab.

Eine trennscharfe Abgrenzung der Anwendungsbereiche ist mit dieser Feststellung jedoch insbesondere zwischen Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) (Grundsatz der Integrität und Vertraulichkeit) und Art. 32 DSGVO noch nicht erreicht. Im Weiteren folgt daher die Bestimmung des Anwendungsbereichs des Art. 32 DSGVO in zwei Schritten: Im ersten Schritt wird eine Normenübersicht der Art. 24, 25 und 32 DSGVO vorgenommen (I.). Im zweiten Schritt (II.) folgt auf dieser Grundlage die Einordnung des Art. 32 DSGVO und die Abgrenzung seines Anwendungsbereichs gegenüber dem sachnähesten Art. 25 Abs. 1 i.V.m. Art 5 Abs. 1 lit f) DSGVO.

I. Normenübersicht

Zunächst wird eine systematische Normenübersicht vorgenommen, wobei eine Dekomposition der Normen in ihre unterschiedlichen Bestandteile erfolgt (1.). Diese werden im Anschluss in einer Tabelle gegenübergestellt (2.)

I. Dekomposition der einzelnen Normen

a. Art. 24 DSGVO

Art. 24 DSGVO bildet als erste Norm des Abschnitts die Grund- bzw. Generalnorm.[154] Sie verlangt von dem Verantwortlichen unter „Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen [zu treffen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt."

Aus ihr lassen sich bereits vier für den Vergleich der Normen wichtige Kernelemente identifizieren: Zunächst die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung als „*Modalitäten der Verarbeitung*" (1.). Darauf folgt das „*Risiko*" (2.), beschrieben anhand der Merkmale der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere in Bezug auf die Rechte und Freiheiten natürlicher Personen.[155] Diese beiden Elemente sind die in allen drei Normen enthaltenden Kriterien, die es bei der Bestimmung von Art und Umfang der zu treffenden toM zu berücksichtigen gilt. Darauf folgt das ebenfalls in allen drei Normen vertretene Element des *Handlungsauftrags* (3.), nämlich die Pflicht zur Vornahme von toM. Schließlich besteht das divergierende Element des *Schutzzwecks (4.)*, hier in Form der Sicherstellung und des Nachweises der Einhaltung der DSGVO im Rahmen der Verarbeitung.

Allen Normen ist außerdem gemein, dass sie den Handlungsauftrag an das Risiko knüpfen, d.h. einen risikobasierten Ansatz verfolgen.[156] Daraus folgt auch, dass bei dem Pflichtenkanon der Art. 24, 25, 32 DSGVO stets eine Kosten-Nutzen-Analyse vorzunehmen ist, anhand derer die Risikoreduktion durch die Maßnahmen mit dem hierfür notwendigen Aufwand abgewogen werden muss.[157]

---

154 *Hartung*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 24, Rn. 9; *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 24, Rn. 5.

155 Vgl. EG 75 DSGVO.

156 Vgl. *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 2.

157 Ausführlich zur Angemessenheit: S. 167 f. Dabei wird nicht übersehen, dass in Art. 24 DSGVO ein expliziter Verweis auf die Implementierungskosten fehlt. Gleichwohl ergibt sich bereits aus Art. 52 Abs. 1 S. 2 GRC, dass der Verantwortliche nur

b. Art. 25 DSGVO

Die soeben vorgezeichnete Grundstruktur hält auch Art. 25 Abs. 1 DSGVO bei. Bei den zu berücksichtigenden Kriterien tritt nun jedoch zusätzlich der „Stand der Technik" sowie die „Implementierungskosten" hinzu.

Der Schutzzweck ist gegenüber Art. 24 DSGVO konkretisiert:[158] Er betrifft nun nicht mehr allgemein die Einhaltung der DSGVO, sondern nach Art. 25 Abs. 1 DSGVO sollen die *Datenschutzgrundsätze nach Art. 5 DSGVO wirksam umgesetzt* werden und es sollen die notwendigen Garantien getroffen werden, um den Anforderungen der DSGVO zu genügen. Nach Art. 25 Abs. 2 DSGVO sollen darüber hinaus toM zur Gewährleistung von datenschutzfreundlichen Voreinstellungen getroffen werden.

Zu den Datenschutzgrundsätzen gehört insbesondere auch Art. 5 Abs. 1 lit f) DSGVO, nämlich die Verarbeitung in einer Weise, „die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung […] (‚Integrität und Vertraulichkeit')". Die toM nach Art. 25 Abs. 1 DSGVO sollen damit in Umsetzung dieses Grundsatzes insbesondere die *Integrität und Vertraulichkeit von personenbezogenen Daten gewährleisten*. Zusätzlich wird auch das Schutzziel der *Verfügbarkeit* in diesen Grundsatz hineingelesen,[159] wofür insbesondere die Beeinträchtigungsalternativen des unbeabsichtigten Verlusts und der unbeabsichtigten Zerstörung von personenbezogenen Daten sprechen.

Daneben enthält Art. 25 Abs. 1 DSGVO ein *perspektivisches Element*. Der Verantwortliche soll die entsprechenden toM sowohl „zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung" treffen. Der Zeitpunkt der Festlegung der Mittel ist jener, „in dem der Verantwortliche entscheidet, wie die Verarbeitung durchgeführt wird, wie die Verarbeitung abläuft und welche Mechanismen

verhältnismäßige Maßnahmen treffen muss, wobei insbesondere die Risiken den Kosten gegenüberzustellen sind, *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 11; zum Teil wird das Merkmal der Angemessenheit außerdem auch aus der Pflicht zur Vornahme „geeigneter" Maßnahmen herausgelesen, *Mantz*, in: Sydow/Marsch, DS-GVO, BDSG, 3. Auflage 2022, Art. 32, Rn. 30 f.

158 *Baumgartner*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 25, Rn. 8.

159 *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 5, Rn. 167.

für die Durchführung der Verarbeitung genutzt werden."[160] Durch die Bezugnahme auf diesen Zeitpunkt bringt der Gesetzgeber zum Ausdruck, dass diese toM bereits frühestmöglich im Rahmen der Konzeption und der Entwicklung der Datenverarbeitungsvorgänge zu treffen sind und daher im Idealfall zu einem von vorneherein „eingebauten Datenschutz" führen.[161] Während der „eigentlichen Verarbeitung" muss der Verantwortliche dann die entsprechenden Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen aufrechterhalten, was insbesondere fortwährende Neubewertungen der Risiken sowie des Stands der Technik beinhaltet und -bei entsprechend erkanntem Bedarf- eine Aktualisierung der Maßnahmen erfordert.[162]

c. Art 32 Abs. 1 DSGVO

Art. 32 Abs. 1 verpflichtet zunächst anders als die übrigen genannten Normen bezüglich der Adressaten neben dem Verantwortlichen auch den Auftragsverarbeiter. Die zu berücksichtigenden Faktoren sind dagegen deckungsgleich zu Art. 25 Abs. 1 DSGVO (Stand der Technik, Implementierungskosten, Modalitäten der Verarbeitung sowie das Risiko). Der Schutzzweck hingegen besteht nun darin ein „dem Risiko angemessenes Schutzniveau zu gewährleisten."

Als weitere Besonderheit wird in Art. 32 DSGVO der Handlungsauftrag näher konkretisiert. Die toM schließen demnach „gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit [Resilienz] der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

160 EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, S. 12, Rn. 35.
161 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 25, Rn. 16 f. mit Verweis auf andere Sprachfassungen; *Baumgartner*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 25, Rn. 1.
162 EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, S. 12, Rn. 37 f.

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung."

Schließlich werden in Art. 32 Absatz 2 ähnlich Art. 5 Abs. 1 lit f) DSGVO zu vermeidende Ereignisse definiert, deren zugehörige Risiken entsprechend zu berücksichtigen sind: „Demnach sind bei der Beurteilung eines angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind." Auch hierin sind die *Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit* zu sehen.[163] *Perspektivisch* ist hier zu beachten, dass die Daten dem Wortlaut nach bereits „verarbeitet wurden", d.h. es wird von einer bestehenden Verarbeitung ausgegangen. Zur Verdeutlichung folgt nun unter 2. noch eine tabellarische Übersicht der genannten Normen.

2. Tabellarische Übersicht

Tabelle 1: Art. 24/25/32 DSGVO

	Art. 24 Abs. 1	**Art. 25 Abs. 1**	**Art. 32 Abs. 1, 2**
Einheitliche, zu berücksichtigende Kriterien	Modalitäten der Verarbeitung (Art, Umfang, Umstände, Zwecke), Risiko für Rechte und Freiheiten natürlicher Personen		
Besondere, zu berücksichtigende Kriterien		Stand der Technik Implementierungskosten	Stand der Technik Implementierungskosten
Schutzzweck:	nachweisbare Einhaltung der DSGVO	Wirksame Umsetzung der Datenschutzgrundsätze + entsprechender Garantien	Gewährleistung eines risikoangemessenen Schutzniveaus
Handlungsauftrag:	Geeignete technische und organisatorische Maßnahmen		

163 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 60; *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 61.

Adressat:	Verantwortlicher	Verantwortlicher	Verantwortlicher + Auftragsverarbeiter
Gewährleistung von Vertraulichkeit und Integrität bzw. Verfügbarkeit		*i.V.m. Art. 5 Abs. 1 lit f):* in einer Weise verarbeitet werden, die insb. Schutz gewährt vor: unbefugter oder unrechtmäßiger Verarbeitung; unbeabsichtigtem/er Verlust, Zerstörung, Schädigung	Minimierung von Risiken durch unbefugte Offenlegung unbefugten Zugang unbeabsichtigte oder unrechtmäßige(r) Vernichtung, Verlust oder Veränderung von personenbezogen Daten, die verarbeitet wurden

II. Verhältnis der Art. 25 Abs. 1, 32 DSGVO

Im Weiteren soll die konkrete Einordnung von Art. 32 DSGVO erfolgen. Dabei wird nun die Abgrenzung von Art. 25 Abs. 1 i.V.m. dem Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 lit f) DSGVO zu Art. 32 DSGVO vorgenommen, um den Anwendungsbereich von letzterem und damit auch der Resilienz zu bestimmen.

Zwar konkretisiert nämlich auch Art. 32 DSGVO den genannten Grundsatz,[164] gleichwohl ist davon auszugehen, dass sowohl dem Datenschutz durch Technikgestaltung in Umsetzung dieses Grundsatzes (Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f. DSGVO) als auch der Datensicherheit nach Art. 32 DSGVO jeweils eigenständige Anwendungsbereiche und Normaufträge zukommen.

164 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn 2; *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 1; *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 1 m.w.N.

Entscheidend für diese Abgrenzung sind insbesondere die inhaltlichen Unterschiede zwischen diesen Normen (1.), die nun gegenübergestellt werden. Anschließend wird EG 83 der DSGVO betrachtet, der übergeordnete Hinweise zum Anwendungsbereich der jeweiligen Normen enthält (2.). Schließlich werden unter 3. die so voneinander abgegrenzten Normaufträge noch einmal zusammengefasst.

1. Inhaltliche Unterschiede der Normen

Bei den inhaltlichen Unterschieden fallen zunächst (a.) die unterschiedlichen Perspektiven (Art. 25 DSGVO: Gestaltung der Verarbeitung, Art. 32 DSGVO: Sicherung der bestehenden Verarbeitung) auf. Weiterhin (b.) ist zu beachten, dass nur Art. 32 Abs. 1 lit b) DSGVO explizit auch die verarbeitenden Systeme und Dienste anspricht. Außerdem werden unterschiedliche Rollen (Verantwortlicher und/oder Auftragsverarbeiter) adressiert (c.) und es werden unterschiedliche Schutzrichtungen bei den drei Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität beschrieben (d.).

a. Perspektiven

Nach Art. 25 Abs. 1 DSGVO sind die Maßnahmen zur Umsetzung der Datenschutzgrundsätze wie beschrieben schon zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung zu treffen. Die Mittel meinen dabei die „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird,“[165] mithin die Gestaltung des Verarbeitungsvorgangs. Durch den Verweis auf den „Zeitpunkt dieser Gestaltung“ wird deutlich, dass die toM in den Gestaltungsvorgang implementiert werden sollen, die Verarbeitung also gleichermaßen mitgestalten.[166] Korrespondierend verlangt auch Art. 5 Abs. 1 lit f) DSGVO, dass personenbezogene Daten „*in einer Weise verarbeitet werden*“, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet.

Anders liegt es hingegen bei Art. 32 DSGVO: Eine ausdrückliche perspektivische Zuweisung zum Handlungsauftrag fehlt zwar, allerdings wird in Abs. 2 auf Beeinträchtigungen der Schutzziele an Daten abgestellt, die bereits „verarbeitet *wurden*“. Aus dieser grammatischen Gestaltung als pas-

165 Art.-29 Datenschutzgruppe, WP 169, 16.02.2010, S. 16.

166 Von einem „eingebauten Datenschutz“ sprechend: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 1.

sives Präteritum wird, wie bereits angedeutet, sichtbar, dass Art. 32 DSGVO perspektivisch von einer bereits bestehenden Verarbeitung ausgeht, im Rahmen derer die Daten z.B. bereits erhoben und gespeichert wurden und somit die zuvor genannte Gestaltung, d.h. insbesondere der Verarbeitungsablauf und -umfang abgeschlossen bzw. festgelegt ist. Der Normauftrag des Art. 32 DSGVO ist es nun diese bestehende Verarbeitung zu sichern.

b. Umsetzung der Verarbeitung durch Systeme und Dienste

Auch die explizite Adressierung von Systemen und Diensten in Art. 32 Abs. 1 lit b) DSGVO stützt diese These, da sich diese als (sozio-)technische Mittel der Verarbeitung logisch von der eigentlichen „Verarbeitung" unterscheiden lassen. Diese Verarbeitung ist nach Art. 4 Nr. 2 DSGVO nur der (mithilfe automatisierter Verfahren) vorgenommene Vorgang, der vom Verantwortlichen abstrakt beschrieben, festgelegt und ausgestaltet werden kann (z.B.: welche Daten werden verarbeitet und wie lange (Umfang), wie läuft diese ab, d.h. welche Abteilungen und ggf. auch Dritte[167] benötigen Zugang und wofür (Zwecke) und inwieweit kann auch mit pseudonymen/anonymen Daten gearbeitet werden). Im Rahmen dieser Ausgestaltung sollen nach Art. 25 Abs. 1 DSGVO insbesondere die Datenschutzgrundsätze wirksam umgesetzt werden.

Dagegen adressiert Art. 32 DSGVO die Datensicherheitsanforderungen in der Phase der praktischen Umsetzung der Verarbeitung, welche unter Zuhilfenahme von informationstechnischen Systemen und Diensten (sowie entsprechendem Bedienpersonal) durchgeführt wird.

c. Rollenansprache

Während Art. 25 DSGVO *nur den Verantwortlichen* adressiert, adressiert Art. 32 DSGVO daneben *auch den Auftragsverarbeiter*. Nach Art. 4 Nr. 7 DSGVO hat allein der Verantwortliche die Entscheidungsgewalt über Zwecke und Mittel der Verarbeitung,[168] d.h. nur er (und nicht der Auftragsverarbeiter Art. 4 Nr. 8, Art. 28 Abs. 3 lit a) DSGVO) bestimmt wie soeben

167 *Arning/Rothkegel*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art 4, Rn. 181.

168 *Klabunde*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 4, Rn. 36.

beschrieben über Zweck sowie Umfang und Gestaltung (d.h. die „Mittel") der Verarbeitung[169] im Rahmen des Art. 25 Abs. 1 DSGVO.

Dagegen kann und muss die *Sicherheit* der so gestalteten *Verarbeitung sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter* (Art. 32 Abs. 1, Art. 28 Abs. 3 lit b DSGVO) gewährleistet werden. Die insoweit zu treffenden technischen und organisatorischen Maßnahmen betreffen somit nicht die Gestaltung der eigentlichen Verarbeitung selbst, sondern setzen auf der Verarbeitung auf, um diese entsprechend zu sichern.

d. Voluntative Schutzrichtungen

Die bereits dargestellte Unterscheidung zwischen der Gestaltung der Verarbeitung und der Sicherung derselben wirkt sich auch mit Blick auf die Schutzziele und die jeweiligen voluntativen Schutzrichtungen aus, d.h. ob nur vor vorsätzlichen oder auch vor fahrlässigen Ereignissen geschützt werden soll.

i. Vertraulichkeit

Nach dem Wortlaut stellt Art. 25 Abs. 1 i.Vm. Art. 5 Abs. 1 lit f) DSGVO bezüglich des Schutzes der Vertraulichkeit[170] auf eine *unbefugte oder unrechtmäßige Verarbeitung* ab und nicht wie in Art. 32 Abs. 2 DSGVO auf eine *unbefugte Offenlegung* von bzw. den *unbefugten Zugang* zu Daten.

Unbefugt meint dabei die *Tätigkeit eines Dritten* i.S.v. Art 4 Nr. 10 DSGVO, der dem Verantwortlichen nicht zuzurechnen ist.[171] Ein Dritter ist negativ legaldefiniert als „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer

- der betroffenen Person,
- dem Verantwortlichen,
- dem Auftragsverarbeiter und

169 *Arning/Rothkegel*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art 4, Rn. 181; EDSA, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 02.09.2020, S. 13, Rn. 33.

170 Siehe hierzu auch EG 39, S. 12 DSGVO.

171 *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 5, Rn. 74.

– den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten".[172]

Unter den letztgenannten Punkt fallen über das Attribut der Befugnis auch alle Personen, die bei dem Verantwortlichen beschäftigt sind und für die gegenständliche Datenverarbeitung zuständig sind. Dritte sind umgekehrt somit auch die Personen unter unmittelbarer Verantwortung des Verantwortlichen oder Auftragsverarbeiters, die eine *unbefugte Verarbeitung* vornehmen, d.h. wenn sie Daten ohne entsprechende Weisung verarbeiten.[173]

Eine *unbefugte Verarbeitung* im Sinne des Art. 25 Abs. 1 i.Vm. Art. 5 Abs. 1 lit f) DSGVO liegt mithin vor, wenn die Verarbeitung durch Dritte, also entweder durch unzuständige Personen (bzw. Abteilungen) oder auch externe Dienstleister, die Zugriff auf die Verarbeitung haben (z.B. externe IT-Dienstleister), vorgenommen wird. *Unrechtmäßig* hingegen ist die Verarbeitung, die nicht durch einen Dritten, sondern insbesondere durch den Verantwortlichen selbst oder einen Auftragsverarbeiter vorgenommen wird, wenn hierfür keine Rechtsgrundlage existiert.[174] Man könnte durch die damit verbundene Überschreitung bestehender Verarbeitungsrechte auch von einer *überschießenden Verarbeitung* sprechen. Diese unzulässigen Verarbeitungen verletzten insoweit vorsätzlich die Vertraulichkeit der Daten.[175]

Art. 32 Abs. 2 DSGVO hingegen spricht hinsichtlich der Vertraulichkeit nicht von einer „Verarbeitung", sondern von *unbefugter Offenlegung* von bzw. dem *unbefugten Zugang* zu Daten. Dabei wird nicht verkannt, dass der Verarbeitungsbegriff nach Art. 4 Nr. 2 DSGVO die Offenlegung mitumfasst. Gleichwohl ist davon auszugehen, dass der Gesetzgeber hier (bewusst) keine Redundanz geschaffen hat, sondern die unterschiedliche Terminologie einem dahinterstehenden Regelungskonzept folgt: In diesem Kontext kann Verarbeitung im Sinne eines grundlegend geordneten Datenverarbeitungsvorgangs verstanden werden. Dagegen erfasst der Begriff des *unbefug-*

172 Die Listendarstellung wurde aus Gründen der Lesbarkeit durch den Autor ergänzt.

173 Vgl. hierzu exemplarisch die Bußgeldentscheidung des *LfDI BW* zu einem Polizeibeamten, der ohne dienstlichen Bezug die Halterdaten einer Zufallsbekanntschaft aus dem entsprechenden Informationssystem abfragte: LfDI BW, Pressemitteilung vom 18.06.2019, S. 1.

174 *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 5, Rn. 74.

175 Die (berechtigte) Vertraulichkeitserwartung schließt insofern mit ein, dass die preisgegeben Daten nur im Rahmen der jeweiligen Verarbeitung (in die ggf. eingewilligt und über die aufgeklärt wurde) verwendet werden.

ten Zugangs, den sich ein Dritter verschafft, vorsätzliche, *deliktstypische Handlungen*, die z.B. auch den Tatbestand des „Ausspähens von Daten" nach § 202a StGB erfüllen können. Dies beschreibt somit keine „Verarbeitungen", sondern Angriffe sowohl von außen als auch durch (böswillige) Mitarbeitende (Innentäter:innen) des Verantwortlichen.[176] Daneben kann eine *unbefugte Offenlegung* auch fahrlässig geschehen: So kann es durchaus vorkommen, dass personenbezogene Daten aufgrund von IT-Fehlern beim Verantwortlichen versehentlich öffentlich gemacht und damit unbefugten Personen offengelegt werden.

Insgesamt ist festzuhalten, dass Art. 25 Abs. 1 i.Vm. Art. 5 Abs. 1 lit f) DSGVO *unrechtmäßige und unbefugte, d.h. vorsätzliche Vertraulichkeitsverletzungen* durch unzulässige bzw. überschießende Verarbeitungen erfasst und Art. 32 Abs. 2 DSGVO *vorsätzliche* Vertraulichkeitsverletzungen durch Angriffe *unbefugter* Dritten, was demnach sowohl Innen- als auch Außentäter:innen sein können sowie *fahrlässige* Offenlegungen von Daten an unbefugte Dritte.

ii. Verfügbarkeit/Integrität

Auch im Rahmen des Schutzes der Verfügbarkeit[177] und Integrität bestehen entsprechende Unterschiede:

Nach Art. 5 Abs. 1 lit f) DSGVO gilt es *den/die unbeabsichtigte(n) Verlust, Zerstörung oder Schädigung* von Daten zu vermeiden. Dagegen will Art. 32 Abs. 2 DSGVO die Risken minimieren, die aus *Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig* der Daten resultieren. Somit gilt für die Modalitäten der Verfügbarkeits- und Integritätsverletzungen, dass nur Art. 32 Abs. 2 DSGVO neben unbeabsichtigten auch die unrechtmäßigen Verletzungen erfasst.

Unbeabsichtigt (engl. accidental) erfasst alle Verletzungen, die fahrlässig oder zufällig, also gewissermaßen als „Unfall" geschehen. *Unrechtmäßig* hingegen ist wie bereits dargestellt als vorsätzlicher Rechtsbruch zu verstehen; da sich der Begriff hier allerdings nicht auf die „Verarbeitung" bezieht,

176 Vgl. *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 34.

177 Siehe zur zusätzlichen Erfassung der Verfügbarkeit von Art. 5 Abs. 1 lit f) bereits zuvor S. 84, Fn. 159.

kann eine entsprechende Handlung prinzipiell von jedem und nicht nur von einem „Verarbeiter" vorgenommen werden.[178]

Entsprechend lassen sich die Tatbestandsalternativen im Sinne des Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO wie folgt auslegen: Es soll sichergestellt werden, dass befugte Personen die Daten im Rahmen der Verarbeitung nicht *unbeabsichtigt* (fahrlässig) löschen oder verändern.

Nach *Art. 32 Abs. 2 DSGVO* soll hingegen neben dem Schutz vor *unbeabsichtigten* Ereignissen (zur Abgrenzung im Fazit unter 3.) zusätzlich auch sichergestellt werden, dass die Daten nicht *unrechtmäßig,* mithin *vorsätzlich* beeinträchtigt werden. Dies betrifft zunächst deren vorsätzliche „Vernichtung" etwa durch einen Angriff in Form der Löschung oder der Verschlüsselung durch eine Ransomware. Zweitens soll der vorsätzliche „Verlust" der Daten, d.h. eine Vereitelung des Zugangs zu den noch existenten Daten vermieden werden, z.B. bei Ransomware oder bei Diebstahl von Speichermedien[179], vermieden werden. Beide Alternativen beziehen sich auf die *Verfügbarkeit.*[180] Schließlich soll neben der unbeabsichtigten auch die *unrechtmäßige Datenveränderung,* d.h. auch die böswillige Manipulation der Daten ausgeschlossen werden.

Im Ergebnis erfasst Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO *somit nur fahrlässige Integritäts- und Verfügbarkeitsverletzungen.* Art. 32 DSGVO hingegen erfasst sowohl *fahrlässige als auch vorsätzliche Integritäts- und Verfügbarkeitsverletzungen* durch Angriffe.

178 Diese Differenzierung im voluntativen Element (unbeabsichtigt ggü. unbeabsichtigt und unrechtmäßig) wollte der Gesetzgeber möglicherweise auch in den Verletzungsformen ausdrücken, soweit in Art. 5 Abs. 1 lit f) DSGVO neben Verlust von Schädigung (damage) statt wie in Art. 32 Abs. 2 DSGVO Veränderung (alteration) gesprochen wird. Semantisch könnte man hieraus erkennen, dass mit (unbeabsichtigter) Schädigung also gewissermaßen eher noch ein versehentliches Verhalten gemeint ist, wohingegen die (unbeabsichtigte oder unrechtmäßige) Veränderung etwas mehr noch auch ein zielgerichtetes Handeln umfasst: Bei einem versehentlichen Verhalten würde man dem allgemeinen Wortsinn nach wohl weniger von einer „Veränderung", sondern eher (nur) von einer Schädigung sprechen; so dass der Begriff Veränderung insoweit etwas generischer ist. Nach a.A.: *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (406), Fn. 82, hat die Trias „Vernichtung, Verlust, Veränderung" nach Art. 32 Abs. 2, Art. 4 Nr. 12 DSGVO aber dieselbe Bedeutung wie „Zerstörung, Verlust, Schädigung" nach Art. 5 Abs. 1 lit f) DSGVO.

179 In diesem Fall tritt dann zusätzlich zu der Verfügbarkeits- auch eine Vertraulichkeitsverletzung ein, sofern die Daten nicht verschlüsselt waren.

180 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 21; zur Bedeutung der Verfügbarkeit in der Datensicherheit siehe auch: EDSA, Guidelines 9/2022 on personal data breach notification under GDPR, 28.03.2023, S. 8 f.

2. Übergreifende Zuordnung in Erwägungsgrund 83

Die bisherigen Feststellungen lassen sich auch durch den Rückgriff auf EG 83 Satz 1 untermauern, in dem beide Aspekte zusammengeführt werden. Hier heißt es:

> „Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen."

Als erstes Indiz drängt sich im Wortlaut zunächst die unterschiedliche Rollenansprache auf: Während Art. 32 DSGVO wie dargestellt den Verantwortlichen *und* den Auftragsverarbeiter, aber Art. 25 DSGVO nur den Verantwortlichen anspricht, werden die beiden Rollen im EG 83 in einem Alternativ-Verhältnis genannt, so dass auch nur einer von beiden erfasst sein kann und damit eine Zuordnung sowohl zu Art. 25 als auch zu Art. 32 DSGVO möglich wird. Diese Zuordnung ergibt sich dann im Detail wie folgt:

Die *Aufrechterhaltung der Sicherheit* weist in Richtung des Art. 32 DSGVO: Dafür spricht der Wortlaut der Überschrift des Art. 32 DSGVO mit „Sicherheit der Verarbeitung"; anders als in Art. 25 Abs. 1 DSGVO, der gerade Datenschutz durch Technikgestaltung (privacy by design) und nicht etwa Sicherheit durch Technikgestaltung (security by design) fordert.[181] Außerdem korrespondiert das Erfordernis der „Aufrechterhaltung" mit Art. 32 Abs. 1 lit b) DSGVO, indem verlangt wird, dass „Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit [Resilienz] der Systeme und Dienste […] *auf Dauer sicherzustellen*" sind.

Die *Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung* weist im Umkehrschluss auf die Gestaltung der Verarbeitung nach Art. 25 Abs. 1 DSGVO hin. Das Merkmal der „Vorbeugung" korrespondiert durch den enthaltenen Präventionsgedanken mit dem in Art. 25 DSGVO ausdrücklich auch fokussierten „Zeitpunkt der Festlegung der Mittel" und bekräftigt damit die gestalterische Prägung des Art. 25 DSGVO, die Daten-

181 Auch wenn dies freilich mittelbar auf die Datensicherheit wirkt, da etwa durch eine Datenverarbeitung mit möglichst wenig Daten (Datenminimierung) und möglichst wenig Personen mit Zugang zu den Daten die dann nach Art. 32 Abs. 1 DSGVO zu sichernde Angriffsfläche verkleinert wird.

schutzgrundsätze gerade *in* der Verarbeitung *wirksam umzusetzen* bzw. zu implementieren. D.h. die Verarbeitung selbst soll vorbeugend von Anfang an („by Design") so gestaltet werden, dass die Verarbeitung den Anforderungen der DSGVO, insbesondere den Datenschutzgrundsätzen einschließlich Art. 5 Abs. 1 lit f) DSGVO entspricht[182] und eine gegen diese Verarbeitung verstoßende, insbesondere auch überschießende Verarbeitung, verhindert wird.

3. Normaufträge und Fazit

Fraglich ist nun, wie sich nach diesen Feststellungen die Anwendungsbereiche und damit auch die Normaufträge von Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO und dem für diese Untersuchung maßgeblichen Art. 32 DSGVO voneinander abgrenzen lassen.

a. Keine eindeutige Differenzierung nach voluntativem Element und Quelle

Zunächst lässt sich zunächst negativ festhalten, dass sich die Normen nicht eindeutig anhand der Einwirkungen auf Schutzziele mit Blick auf das voluntative Element unterscheiden lassen, sondern dass sich diese zumindest teilweise überschneiden.

182 Vgl. *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 8.

Tabelle 2: Schutzziele in Art. 25 Abs. 1 i.V.m. 5 Abs. 1 lit f) und 32 Abs. 2 DSGVO

	Vertraulichkeit	**Verfügbarkeit/Integrität**
Art. 25 Abs. 1 i.V.m. Art. 5 lit f)	unbefugte oder unrechtmäßige Verarbeitung	Unbeabsichtige(r) Verlust, Zerstörung oder Schädigung
	durch Verantwortlichen oder Dritte (unzuständige Personen, externe Dienstleister)	
Art. 32 Abs. 2	unbefugte Offenlegung unbefugter Zugang	unbeabsichtigte oder unrechtmäßige(r) Vernichtung, Verlust oder Veränderung
	durch Dritte oder, wenn unbeabsichtigt, auch durch Verantwortlichen oder Auftragsverarbeiter	

Sowohl Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) als auch Art. 32 Abs. 2 DSGVO adressieren ausdrücklich sowohl unbefugte bzw. unrechtmäßige (d.h. *vorsätzliche*) als auch unbeabsichtigte, mithin jedenfalls *fahrlässige Ereignisse*. Nach obiger Wortlautauslegung erfasst „unbeabsichtigt" auch zufällige Ereignisse, allerdings erscheint schwer vorstellbar wie *zufälligen Ereignissen* (insbesondere Naturkatastrophen) auf Ebene der Gestaltung der Verarbeitung begegnet werden kann. Der Begriff ist daher für den Bereich des Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) teleologisch zu reduzieren.

Auch bei der Einwirkungsquelle besteht keine stringente Differenzierung: Sowohl Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO als auch Art. 32 DSGVO adressieren interne Ereignisse beim *Verantwortlichen* wie etwa versehentliches Löschen durch Mitarbeitende oder Datenverlust aufgrund von „zufälligen" Hardware-Versagen[183]. Weiterhin werden, wenn auch differenzierend, externe Ereignisse sowohl von Art. 25 Abs. 1 (Verhalten *externer Dienstleister*) als auch von Art. 32 DSGVO (Angriffe von *Dritten,* d.h. wie beschrieben sowohl Innen- als auch Außentäter:innen) adressiert.

Die Abgrenzung ergibt sich aus der besonderen, datenschutzrechtlich geprägten Perspektive mit ihrer eigenen Methodik. Es handelt sich letztlich um eine Abgrenzung anhand von Sphären: Die Verarbeitungssphäre des Verantwortlichen mit allen internen und externen Stellen muss einerseits präventiv und fortlaufend im Sinne der Datenschutzgrundsätze nach Art. 25 Abs. 1 DSGVO ausgestaltet sein. Andererseits besteht eine Sphäre

183 *Schultze-Melling*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 32, Rn. 21.

jenseits dieses verarbeitungsbezogenen Planungshorizonts, in der die so gestaltete Verarbeitung vor „unerwünschten Ereignissen“[184] geschützt werden soll. Hierzu zählen fahrlässige Ereignisse, die sich aber anders als zuvor nicht durch eine Gestaltung der Verarbeitung verhindern lassen als zusätzlich auch zufällige Ereignisse sowie vorsätzlich durch Dritte hervorgerufene Ereignisse. Insgesamt ist somit vor allem nach den jeweiligen Sphären zu unterscheiden, d.h. welche Ereignisse können schon durch die Gestaltung der Verarbeitung vermieden werden und welche erst im Rahmen der Sicherung der Verarbeitung mit ihren Systemen bzw. Diensten.

b. Art. 25 Abs. 1 DSGVO

Nach Art. 25 Abs. 1 DSGVO soll die Verarbeitung im Kontrollbereich des Verantwortlichen zunächst möglichst frühzeitig anhand der Datenschutzgrundsätze (Art. 5 Abs. 1 DSGVO) gestaltet werden.[185]

Hinsichtlich des *Grundsatzes der Integrität und Vertraulichkeit* (und Verfügbarkeit) nach Art. 5 Abs. 1 lit f)[186] soll dabei zunächst sichergestellt werden, dass es nicht zu unbefugten und unrechtmäßige Verarbeitungen (Eingriffe in die „Vertraulichkeit“) kommt.

Eine *unbefugte Verarbeitung* läge beispielsweise in der Verarbeitung personenbezogener Daten durch einen externen IT-Dienstleister zu eigenen Zwecken, etwa um die Nutzung der von ihm implementierten IT-Produkte zu überwachen, ohne dafür einen eigenen Rechtmäßigkeitstatbestand nach Art. 6 DSGVO zu erfüllen oder in einer Verarbeitung durch einen unbefugten Mitarbeitenden.

Unrechtmäßig ist dagegen jede Verarbeitung des Verantwortlichen oder Auftragsverarbeiters, die über den eigentlichen Zweck hinausgeht. Etwa

184 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 59.

185 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 25, Rn. 16, 18.

186 Soll dagegen beispielsweise der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit b) DSGVO) umgesetzt werden, muss die Verarbeitung bei Verfolgung mehrerer Zwecke technisch so ausgestaltet werden, dass für jeden Zweck (z.B. Vertragserfüllung und Werbung) ein separater Einzelprozess vorliegt, so dass diese insbesondere mit ihren Zugriffsrechten unabhängig voneinander beendet werden können. Auch könnten Daten entsprechend gekennzeichnet werden [Tagging]. *Hartung*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 25, Rn. 16; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 25, Rn. 30.

wenn die Daten von dem Verantwortlichen nur zur Abrechnung eines Dienstens erhoben wurden, dann aber auch zur personalisierten Werbung genutzt werden.

Insoweit muss als technische Maßnahme u.a. durch ein *differenziertes Zugriffsmanagement* sichergestellt werden, dass nur so wenig Personen wie möglich und diese auch nur im notwendigen Umfang an der Verarbeitung beteiligt sind und somit auf die Daten zugreifen können.[187] Außerdem ist ein effektives Kontroll- und Aufsichtssystem (Controlling, organisatorische Maßnahme) erforderlich, dass die erlaubten Verarbeitungsumfänge auch tatsächlich nicht überschritten werden.

Weiterhin sind *eine unbeabsichtigte Zerstörung bzw. Schädigung oder ein unbeabsichtigter Verlust der Daten* (Verfügbarkeit und Integrität) im Rahmen der Verarbeitung zu vermeiden. Gegen ein solches fahrlässiges Verhalten kann wieder durch ein differenziertes Zugriffsmanagement vorgegangen werden, z.B. dass nur bestimmte Personen oder mehrere Personen (Vier-Augen-Prinzip) berechtigt sind, insbesondere besonders sensible Daten zu löschen oder zu verändern.

Vorsätzliche Ereignisse werden hinsichtlich der Verfügbarkeit bzw. Integrität in der Verarbeitungsperspektive des Art. 25 Abs. 1 DSGVO hingegen nicht berücksichtigt. Insofern geht der Schutzzweck des Art. 25 Abs. 1 DSGVO erkennbar davon aus, dass die an der Verarbeitung Beteiligten im wohlverstandenen Eigeninteresse solche destruktiven Eingriffe in die Verarbeitung nicht vornehmen, sondern wie zuvor beschrieben viel mehr vorsätzlich eine zu weitgehende, d.h. *überschießende Verarbeitung* durchführen. Destruktives, vorsätzliches Handeln Dritter fällt insofern unter Art. 32 DSGVO.

c. Art. 32 DSGVO

In einem zweiten Schritt soll die wie zuvor beschrieben ausgestaltete Verarbeitung (insbesondere auch gegenüber Dritten) gesichert werden, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Hierbei sind technische und organisatorische Maßnahmen zu treffen, die ein angesichts der Risiken angemessenes Schutzniveau gewährleisten. In Abgrenzung zu Art. 25 Abs. 1 i.V.m. Art 5 Abs. 1 lit f) DSGVO sind somit die Maßnahmen

187 EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, S. 32.

auf die Abwehr unerwünschter Ereignisse gerichtet,[188] die *außerhalb des Planungsbereichs des Verantwortlichen liegen* und somit nicht durch die Gestaltung der Verarbeitung (Art. 25 Abs. 1 DSGVO) verhindert werden können.

Ein solches fahrlässiges (*unbeabsichtiges)* Ereignis könnte etwa durch den unsachgemäßen Umgang des Personals mit der Informationstechnik (Hard- und Software) ausgelöst werden[189] (z.B. das Verlieren von Datenträgern, fahrlässige Nichtbefolgung von Richtlinien zur Bedienung oder auch Flüssigkeitsschäden an informationstechnischen Systemen). Fahrlässige Ereignisse können in diesem Bereich auch durch Dritte verursacht werden, etwa wenn die verwendete Hard- und Software Fehler aufweist, die dann zur *Vernichtung* oder *Veränderung* von Daten führen können.[190] Außerdem sind alle *unrechtmäßigen* bzw. *unbefugten*, d.h. vorsätzlichen Angriffe zu berücksichtigen, die entweder von Innen-[191] als insbesondere auch von Außentäter:innen verübt werden können, etwa in Form von Ransomware (*unrechtmäßiger Datenverlust*), Hackerangriffen (*ggf. unrechtmäßige Veränderung*) und Datendiebstahl (*unbefugter Zugang*). Schließlich sind auch zufällige Ereignisse wie etwa höhere Gewalt (Naturkatastrophen) erfasst (z.B. mit der *Folge eines unbeabsichtigten Datenverlusts* durch eine Überschwemmung).[192]

Dabei sollen insbesondere auch die „Systeme und Dienste" mit technischen und organisatorischen Maßnahmen ausgestattet werden, so dass sie eine Datensicherheit gewährleisten, die Einwirkungen unbefugter Dritter auf das System ausschließt als auch dem System ermöglicht, auf interne Störungen wie z.B. Datenverlust oder -veränderung zu reagieren.

---

188 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 59.

189 Vgl. *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 99.

190 Vgl. *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 104.

191 Der Schutz vor Innentäter:innen, die etwa personenbezogene Daten entwenden und veräußern wollen, wird zwar z.T. auch schon dadurch gewährleistet, dass diese beispielsweise als Mitarbeitende einer anderen Abteilung schon aus der Perspektive des Art. 25 i.V.m. Art. 5 Abs. 1 lit f) DSGVO (siehe voranstehendes Kapitel b.) keinen Zugriff auf diese Daten hat. Zusätzlich sind aber ggf. auch Sicherheitsmaßnahmen zu etablieren, dass er sich diesen Zugriff auch nicht durch einen „Innenangriff" verschaffen kann.

192 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 59.

Insgesamt zielt Art. 32 DSGVO somit darauf ab, vorsätzliche, fahrlässige als auch zufällig hervorgerufene, unerwünschte Ereignisse abzuwehren, deren Ursprung intern als auch extern liegen kann und die sich in Abgrenzung zu Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO nicht durch die Gestaltung der Verarbeitung verhindern lassen. Dieser Anwendungsbereich des Art. 32 DSGVO ist somit auch für die weitere Untersuchung der Resilienz maßgeblich.

Zum Abschluss soll das Ergebnis mit den jeweiligen Normadressaten, den unterschiedlichen Perspektiven und den Schutzrichtungen nochmal in folgender Abbildung zusammengefasst werden:

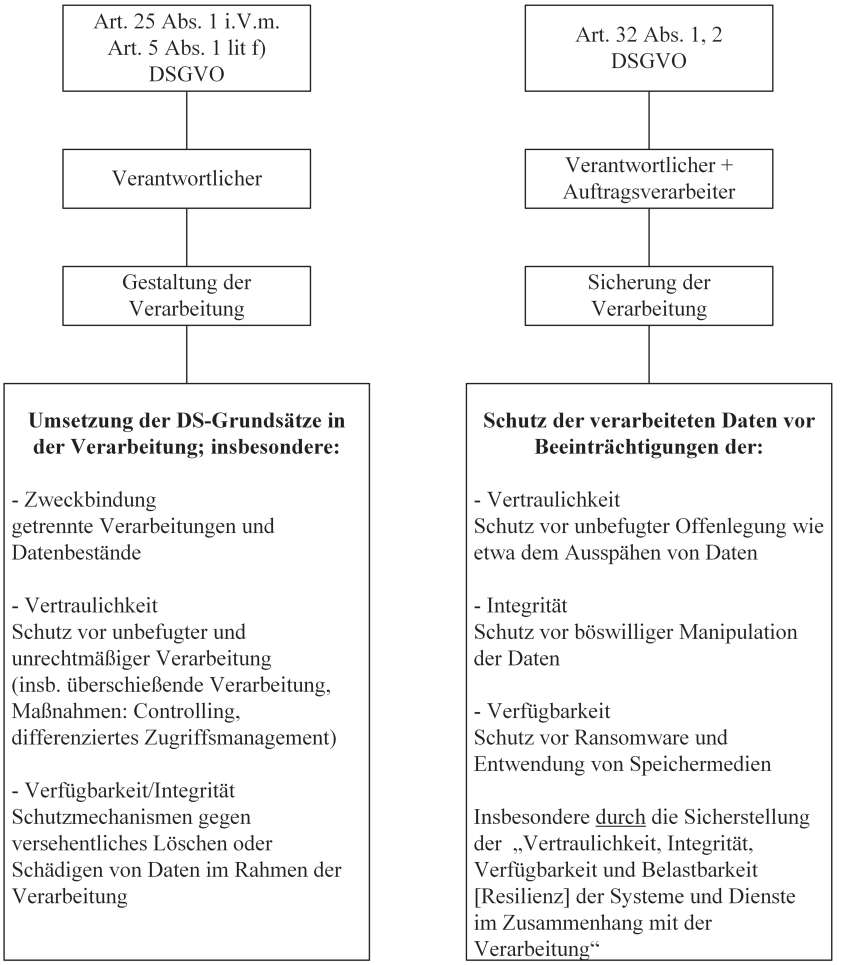

Abbildung 3: Abgrenzung Art. 25/32 DSGVO

B. Schutzgüter

In diesem Kapitel sollen die Schutzgüter der DSGVO ermittelt werden. Zunächst wird hierfür der Begriff des Schutzgutes, seine Bedeutung für das Daten- und IT-Sicherheitsrecht und damit auch für das Merkmal der Resilienz erläutert (I.). Im Anschluss werden spezifischer die Schutzgüter

der DSGVO herausgearbeitet (II.) Sodann wird unter III. erläutert, wie diese Schutzgüter in Art. 32 DSGVO eingebunden werden.

I. Terminologie und normative Bedeutung

Der Begriff des Schutzgutes wird nicht einheitlich verwendet; als Kompositum sagt er zumindest aus, dass ein bestimmtes Gut mit einem rechtlichen Schutz versehen wird.[193] Ähnlich wird auch der Begriff des „Rechtsgutes" etwa im Strafrecht definiert als ein „rechtlich geschütztes Interesse"[194] oder ein „rechtlich geschützter abstrakter Wert der Sozialordnung."[195] In dieser Untersuchung werden jene Rechtsgüter als *Schutzgüter* bezeichnet, die gerade durch das Daten- bzw. IT-Sicherheitsrecht geschützt werden sollen. In *andere Rechtsgüter* - insbesondere die berufliche bzw. unternehmerische Freiheit der Normadressaten - wird hingegen eingegriffen, um jene Schutzgüter zu sichern (dazu sogleich).

Zu den Schutzgütern können zunächst insbesondere Grundrechte mit ihren jeweiligen Schutzbereichen gehören.[196] Als Schutzgüter in diesem Sinne verpflichten die Grundrechte in ihrer objektiv-rechtlichen Dimension den Staat, die jeweiligen Grundrechtsträger:innen auch vor den von anderen Privatpersonen ausgehenden Bedrohungen ihrer Grundrechte zu schützen.[197] Die Erfüllung dieser sog. Schutzpflichten stellt zugleich eine Staatsaufgabe dar,[198] welche vom Staat in Gestalt des Gesetzgebers verlangt, diese Schutzpflichten durch entsprechende Gesetze auszugestalten.[199]

193 Siehe etwa *Calliess*, in: Dürig/Herzog/Scholz, Grundgesetz, 103. EL 2024, Art. 20a, Rn 71.

194 *Liszt*, ZStW 1886, 663 (672 f.).

195 *Jescheck/Weigend*, Lehrbuch des Strafrechts, S. 257 f.; Zur Übersicht mit weiteren Definitionsversuchen: *Engländer*, ZStW 2015, 616 (620).

196 Vgl. *Isensee*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IX, 413 (436), Rn. 48, der generell den Schutzbereich eines Grundrechts als „Schutzgut" bezeichnet.

197 *Epping/Lenz/Leydecker*, Grundrechte, Rn. 23 [neu]; *Stinner*, Staatliche Schutzpflichten im Rahmen informationstechnischer Systeme, S. 52.

198 *Isensee*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IV, 3, S. 37, Rn. 70; *Herzog*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IV, 81 (92), Rn. 26.

199 *Bethge*, in: Schmidt-Bleibtreu/Klein/Bethge, Bundesverfassungsgerichtsgesetz, 63. EL 2023, § 90, Rn. 108.

Genauer beschreibt das BVerfG[200] den inhaltlichen Rechtscharakter einer Schutzpflicht mit Blick auf das Grundrecht „Leben und körperliche Unversehrtheit" (Art. 2 Abs. 2 Satz 1 GG) dergestalt, dass die Schutzpflicht dem Staat gebiete „sich schützend und fördernd vor dieses Leben [oder jedes andere Grundrecht] zu stellen, das heißt vor allem, es auch vor rechtswidrigen Eingriffen vonseiten anderer zu bewahren." Entsprechend müsse sich die Rechtsordnung an diesem Gebot ausrichten.

Die Schutzpflicht wirke außerdem umso stärker, „je höher der Rang des in Frage stehenden Rechtsgutes innerhalb der Wertordnung des Grundgesetzes anzusetzen ist."[201] In dem hier vorliegenden Kontext des Daten- bzw. IT-Sicherheitsrechts kommt der Staat dieser Pflicht nach, indem er zur Sicherung der jeweiligen Schutzgüter Dritter (etwa betroffener Personen nach der DSGVO) den eigentlichen Normadressaten Vorgaben zur Gewährleistung der Daten- und IT-Sicherheit auferlegt.

Diese Vorgaben mit mehr oder minder konkreten Handlungspflichten stellen sich indes aus Sicht der Normadressaten, sofern es sich hierbei nicht um öffentlich-rechtliche Einrichtungen handelt, als staatliche Grundrechtseingriffe dar, sei es in ihre allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) oder ggf. auch ihre Berufsfreiheit (Art. 12 GG, Art. 15 GRC)[202] bzw. ihre unternehmerische Freiheit (Art. 16 GRC). Insofern wirken die Grundrechte hier in ihrer subjektiv-rechtlichen Abwehrdimension gegen den Staat („status negativus").[203] Der Grundrechtsträger und Normadressat kann insofern grundsätzlich vom Staat ein Unterlassen[204] dieses Eingriffs verlangen.

Damit der Eingriff gleichwohl gerechtfertigt ist, muss er insbesondere verhältnismäßig sein, d.h. zwischen den konkurrierenden Positionen muss -nach den Grundsätzen praktischer Konkordanz-[205] ein angemessenes Verhältnis hergestellt werden:

Dabei steht der durch die jeweiligen Pflichtennormen vorgegebene Aufwand (hier Art. 32 Abs. 1 DSGVO: Implementierungskosten, i.Ü. auch in

200 *BVerfG*, Urt. v. 25. 2. 1975 – 1 BvF 1 - 6/74, NJW 1975, 573 (575).
201 Wie zuvor.
202 *Poscher/Lassahn*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 133 (149), Rn. 46; *Wischmeyer*, Informationssicherheit, S. 123.
203 *Starck*, in: Mangoldt/Klein/Starck, Grundgesetz, 7. Auflage 2018, Art. 1, Rn. 183; *Isensee*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band IX, 413 (435 ff.), Rn. 47 ff.
204 Wie zuvor.
205 *BVerfG*, Beschluss v. 06.10.2009 – 2 BvR 693/09, NJW 2010, 220 (221 f.), Rn. 24; *BVerfG*, Beschluss v. 24.03.1998 – 1 BvR 131-96, NJW 1998, 2889 (2890); auch mit kritischen Stimmen siehe *Schladebach*, Der Staat 2014, 263 (266, 274 ff.).

§ 30 RegE BSIG (sowie § 19 Abs. 4 TDDDG: „wirtschaftlich zumutbar") für den Adressaten als Eingriff dem hierdurch erreichten Zuwachs bei der Sicherung der Schutzgüter gegenüber. Nachfolgend werden die genannten Aspekte zur Verdeutlichung noch einmal grafisch dargestellt:

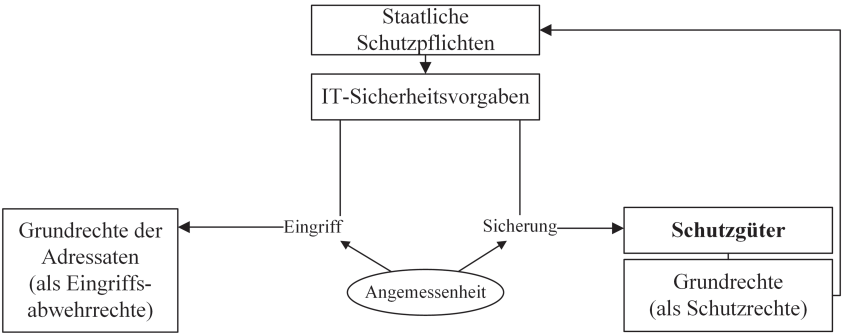

Abbildung 4: Abwägung zwischen Schutzgütern und Grundrechten der Adressaten

Der Gesetzgeber nimmt diese Abwägung zwischen den genannten Positionen dabei nicht unmittelbar und abschließend selbst vor. Vielmehr verfolgen die Pflichtennormen der Daten- und IT-Sicherheit einen sog. risikobasierten Ansatz[206], wonach es zunächst dem Adressaten obliegt, zu ermitteln, welchen Aufwand er betreiben muss, um den Risiken für die Schutzgüter angemessen zu begegnen. Genauer muss er insofern die Risiken bestimmen, d.h. analysieren mit welcher Wahrscheinlichkeit und in welchen Umfang (Folgenschwere) die Schutzgüter betroffen sein können. Anschließend muss er Maßnahmen ergreifen, die Eintrittswahrscheinlichkeit und/oder Folgenschwere angemessen reduzieren. Ob ihm das gelungen ist, ist entsprechend gerichtlich überprüfbar, so dass die Durchsetzung der Vorschriften gesichert ist und die Gesetze, die die o.g. Schutzpflicht ausfüllen insofern auch ihre Wirkung nicht verfehlen.

206 Für Art. 32 DSGVO: *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 22; *BSG*, Urt. v. 20.01.2021 – B 1 KR 15/20 R, BeckRS 2021, 13884, Rn. 79; für § 8a BSIG: *Bussche/Schelinski*, in: Leupold/Wiebe/Glossner, IT-Recht, Teil 7.1, Rn. 27.

Zusammenfassend wird mit dem Begriff des Schutzgutes in dieser Untersuchung

> *jenes rechtlich zu schützende Interesse bezeichnet, zu dessen Zweck der Gesetzgeber den Normadressaten Pflichten zur Gewährleistung einer angemessenen Daten- oder IT-Sicherheit auferlegt.*

Es zeigt sich, dass Daten- und IT-Sicherheitsnormen nicht im luftleeren Raum stehen, sondern eingebettet sind in einen spezifischen Ausgleich von grundrechtlichen und anderen Positionen mit Verfassungsrang in den jeweils bereichsspezifischen Normen. Dabei ist das Schutzgut von besonderer Bedeutung, da sich hieran zeigt wofür, also zum Schutz welchen Gutes Daten- oder IT-Sicherheit gewährleistet werden soll. Dieser Hintergrund ist entscheidend um den Inhalt der Resilienz als spezifische Anforderung der Datensicherheit (und ggf. auch später der IT-Sicherheit) in ihrer Funktion und Reichweite begründen zu können.

Neben dem hier skizzierten Unterfall, dass die Schutzgüter Ausprägungen von Grundrechten mit entsprechenden staatlichen Schutzpflichten darstellen, können auch andere rechtliche Interessen Schutzgüter sein. Dieser Frage wird ausführlich im Kapitel zu den Schutzgütern im IT-Sicherheitsrecht nachgegangen, in dem insbesondere auch öffentliche Interessen als sog. *Gemeinschaftsrechtsgüter* von Bedeutung sind, etwa im Rahmen der Dienstleistungen aus dem Bereich der Daseinsvorsorge.[207]

II. Die Schutzgüter der DSGVO

Nach Art. 1 Abs. 2, EG 2 der DSGVO ist Zweck der „Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten" die Wahrung ihrer "Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten", mithin liegen die Schutzgüter der DSGVO[208] in eben diesem soeben beschriebenen Bereich des Individualgüterschutzes.

Im vorliegenden Kontext der Datensicherheit muss sich der Staat aufgrund der bestehenden objektiven Schutzpflichten schützend vor die Betroffenen stellen, so dass auf deren personenbezogene Daten nicht durch Dritte unerlaubt zugegriffen werden kann. Um dies zu erreichen, muss er

207 S. 222 ff.
208 Kritisch hierzu: *Veil*, NVwZ 2018, 686 (690 ff.).

in die Grundrechte derjenigen eingreifen, die diese Daten (rechtmäßig) verarbeiten (Verantwortliche) und sie verpflichten, für eine angemessene Sicherheit der verarbeiteten Daten zu sorgen.

Dies gilt im Übrigen nicht nur für die Datensicherheit, sondern auch für den gesamten Datenschutz nach der DSGVO: Auch hier wird insbesondere in die unternehmerische Freiheit (Art. 16 GRC, EG 4 DSGVO) des Verantwortlichen eingegriffen, indem ihm nur innerhalb festgelegter Regeln gestattet wird, die personenbezogenen Daten z.B. seiner Kund:innen zu verarbeiten, um eben diese in ihren Grundrechten, insbesondere ihrem Datenschutzgrundrecht bzw. Recht auf informationelle Selbstbestimmung zu schützen. Es liegt mithin auch im Datenschutz stets ein Konflikt zwischen widerstreitenden Grundrechtspositionen vor, der durch den Staat in ausgleicher Weise geregelt werden muss.[209]

1. Sachliche Bestimmung der „Grundrechte und Grundfreiheiten"

Im Weiteren sollen diese als „Grundrechte und Grundfreiheiten" bezeichneten Schutzgüter näher untersucht werden. Die Bezeichnung „Rechte und Freiheiten" geht dabei auf Art 52 GRC, von dort wiederum auf die EMRK und die französische Rechtstradition zurück und bezeichnet -ohne qualitativen Unterschied zwischen Rechten und Freiheiten- die Individualgrundrechte.[210]

Inhaltlich umfasst dies nach Art. 2 Abs. 1 und EG 2 DSGVO deutlich mehr als nur das ausdrücklich genannte Datenschutzgrundrecht nach Art. 8 GRC und Art. 16 AEUV. Es kann hieraus geschlossen werden, dass dieses Grundrecht zwar das zentrale -„insbesondere"-, aber jedenfalls nicht

209 *Masing*, NJW 2012, 2305 (2306).

210 *Bieker/M. Hansen/Friedewald*, RDV 2016, 188 (188), *Schwerdtfeger*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Auflage 2019, Art. 52, Rn. 25; *Becker*, in: Schwarze/Becker/Hatje/Schoo, EU-Kommentar, 4. Auflage 2019, Art. 52 GRC, Rn. 2; nach a.A. bezieht sich der Begriff der Grundfreiheiten nicht auf die GRC, sondern auf die Grundfreiheiten der europäischen Union (z.B. Warenverkehrsfreiheit): *Veil*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018, Art. 24, Rn. 117; dagegen spricht aber systematisch, dass insbesondere die hier relevante Freiheit des Datenverkehrs als Voraussetzung für den europäischen Binnenmarkt, dem auch die anderen Grundfreiheiten in diesem Sinne dienen, gesondert in Art. 1 Abs. 3 DSGVO adressiert wird, siehe hierzu: *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 1, Rn. 41 ff.

das einzige Grundrecht darstellt, das durch die DSGVO geschützt werden soll. Vielmehr erkennt die DSGVO mit der weiten Formulierung der „Grundrechte und Grundfreiheiten" an, dass auch andere Grundrechte und Grundfreiheiten durch eine Verletzung des Datenschutzgrundrechts beeinträchtigt oder umgekehrt erst durch den Schutz desselben ermöglicht werden können.[211] Damit unterscheidet sich die DSGVO wie schon die DS-RL von dem BDSG a.F., dessen Gesetzeszweck in § 1 Abs. 1 BDSG a.F. sich auf den Schutz des allgemeinen Persönlichkeitsrechts sowie daraus insbesondere dem Recht auf informationelle Selbstbestimmung beschränkte.[212]

Andere in Betracht kommende Grundrechte sind insbesondere der Schutz des Privat- und Familienlebens, der Wohnung sowie der Kommunikation gemäß Art. 7 GRC,[213] die Gedanken-, Gewissens- und Religionsfreiheit und die Meinungs- (Art. 10 Abs. 1, 11 Abs. 1 GRC, Art. 4 Abs. 1, 5 Abs. 1 S. 1 Alt. 1 GG)[214] sowie die Informationsfreiheit (Art. 11 GRC, Art. 5 Abs. 1 S. 1 Alt. 2 GG).[215] Daneben ist auch das Diskriminierungsverbot geschützt, was insbesondere in dem Schutz besonderer Kategorien personenbezogener Daten in Art. 9 DSGVO zum Ausdruck kommt, die zumindest teilweise zugleich dem Diskriminierungsverbot unterliegende Merkmale nach Art. 21 Abs. 1 GRC darstellen.[216] Im Ergebnis beschreibt das Datenschutzrecht mit der Adressierung der genannten Schutzgüter „individuellen und unmittelbaren Grundrechtsschutz".[217] Im Rahmen der risikobezogenen Normen werden die Schutzgüter in der DSGVO geringfügig modifiziert, indem der Terminus abstrahierend auf „Rechte und Freiheiten natürlicher Personen"

211 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 1, Rn. 13 f.; *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 1, Rn. 36, 40; nach *Buchner* kann durch einen Datenschutzverstoß in Form der Offenlegung personenbezogener Daten etwa das Recht auf Nichtdiskriminierung verletzt werden; umgekehrt ermöglicht wirksamer Datenschutz erst eine freie Meinungsbildung und -äußerung; zu letzterem auch *Tinnefeld*, ZD 2015, 22 (25).

212 Vgl. § 1 Abs. 1 BDSG a.F., siehe ausführlicher: *Plath*, in: Plath, BDSG Kommentar 2013, § 1, Rn 8 f.

213 *Zerdick*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 1, Rn. 7.

214 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 1, Rn. 13.

215 *Ernst*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 1, Rn. 11.

216 *Buchner*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 1, Rn. 14.

217 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (399), Rn. 21.

ausgedehnt wird, was nach dem Wortlaut auch einfachgesetzliche Rechtspositionen einschließen könnte.[218]

2. Kreis der geschützten „natürliche Personen"

Fraglich ist weiterhin die Reichweite des Begriffs „natürliche Personen" und damit der Kreis der geschützten Grundrechtsträger. Hier ist bemerkenswert, dass auch Art. 32, EG 75 diesen in Art. 1 Abs. 2 DSGVO niedergelegten Terminus verwenden und nicht etwa den der „betroffenen Person", wie er in Art. 4 Nr. 1 DSGVO legaldefiniert wird. Es stellt sich daher die Frage, ob nur die Risiken für die jeweils von den Informationen betroffene Person oder für jede natürliche Person erfasst werden, die ggf. auch nur mittelbar von der Datenverarbeitung betroffen ist.

Der Wortlaut des Art. 32 DSGVO gibt hierauf zunächst keine klare Antwort. Blickt man in EG 75 DSGVO in den ersten Halbsatz, so spricht zunächst viel für eine weite Auslegung, denn dort heißt es die Risken für Rechte und Freiheiten natürlicher Person können aus einer „Verarbeitung personenbezogener Daten" und nicht etwa „Verarbeitung ihrer/der sie betreffenden personenbezogenen Daten" hervorgehen. Dieses Ergebnis wird durch die weiteren Ausführungen in EG 75 gestützt, in denen es als *weitere Schadenskategorie* heißt, dass „die betroffenen Personen" um ihre Rechte und Freiheiten gebracht werden. Dies spricht dafür, dass der Gesetzgeber sich der unterschiedlichen Bedeutung der so bezeichneten Personengruppen durchaus bewusst war und die erfassten Schutzgüter auch in personaler Hinsicht weit ausgestaltet hat.

Damit sind auch mittelbare Auswirkungen auf Dritte erfasst.[219] Denkbar sind z.B. Auswirkungen in engen sozialen Beziehungen wie Familie und Freundeskreise, in denen etwa die unzulässige Veröffentlichung von per-

218 *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 24, Rn. 31; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 27.

219 Vgl. *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 29; häufig wird in der Kommentarliteratur hingegen ohne Erläuterung nur auf betroffene Personen abgestellt, so etwa: *Hladjk*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 32, Rn. 4; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 27; teilweise wird auch EG 76 ins Feld geführt (*Kipker*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 24 DSGVO, Rn. 19) der tatsächlich von den Risiken für betroffene Personen spricht. Allerdings bleibt es dann zumindest begründungsbedürftig, warum dieser EG den eindeutigen Wortlaut in Art. 24, 25 und 32 DSGVO überlagern sollte.

sönlichen Informationen des einen auch die freie Persönlichkeitsentfaltung oder andere Grundrechte des oder der anderen beeinträchtigt.

III. Bestimmung in Art. 32 DSGVO

Nach der amtlichen Überschrift verpflichtet Art. 32 DSGVO den Verantwortlichen zwar wie schon Art. 17 der DS-RL dazu, die „*Sicherheit der Verarbeitung*" zu gewährleisten. Dies wird in Absatz 1 näher konkretisiert, nach dem ein „dem Risiko angemessenes Schutzniveau" zu gewährleisten ist. Dieses Risiko bezieht sich wie auch aus EG 75 ersichtlich auf die *Rechte und Freiheiten natürlicher Personen* und wird dort auch mit verschiedenen Schadens- und Risikokategorien näher umschrieben. Das Risiko muss dabei gerade aus „einer Verarbeitung personenbezogener Daten" hervorgehen.

Fraglich ist insoweit, ob nun nur die „Sicherheit der Verarbeitung" gewährleistet werden muss oder aber ob die „Rechte und Freiheiten natürlicher Personen" unmittelbar geschützt werden müssen.

Nach dem Wortlaut des Art. 32 Abs. 1 kann zunächst abgeleitet werden, dass die „Sicherheit der Verarbeitung" zwar den Handlungsauftrag umschreibt, nicht aber das eigentliche Schutzgut darstellt. Die Schutzgüter bestehen demnach in den „Rechten und Freiheiten natürlicher Personen" bei der Verarbeitung, denn der Kernzweck der Norm ist es, das Risiko für ebendiese zu reduzieren. Dies umfasst wie beschrieben sowohl deren Grundrechte als auch deren einfach-rechtliche Rechtsposition, die durch eine fehlende Datensicherheit beeinträchtigt werden können.

Auf der anderen Seite spricht die Überschrift dafür, dass aus Sicht des Verarbeiters die „sichere Verarbeitung" an sich und nicht unmittelbar die Unversehrtheit der Schutzgüter gewährleistet werden muss. Dafür streitet auch, dass das Risiko für die Rechte und Freiheiten natürlicher Personen im Rahmen der enumerativen Aufzählung nur ein Belang unter mehreren darstellt.

In Gegenüberstellung dieser Alternativen fällt auf, dass die erste Alternative zu einer originären Schutzverantwortung für die Rechte und Freiheiten natürlicher Personen führt, während die zweite Alternative mit dem beschränkten Blick auf die Sicherheit der Verarbeitung nur einer mittelbaren Verantwortung entspricht. Angesichts dessen, dass das Datenschutzrecht aber gemäß Art. 1 Abs. 2 DSGVO ausdrücklich auch die Grundrechte und insbesondere das Recht auf Schutz personenbezogener Daten schützen

will, spricht mehr dafür es hier nicht bei einer mittelbaren Verantwortung zu belassen, sondern den Verantwortlichen (und den Auftragsverarbeiter) unmittelbar zu verpflichten, die Grundrechte und einfachrechtlichen Positionen der natürlichen Personen risikoadäquat schützen.[220]

C. Auslegung der Resilienz

Im nun folgenden Abschnitt soll die Bedeutung der Resilienz von Systemen und Diensten zur Gewährleistung der Datensicherheit und damit zur Sicherung der zuvor beschriebenen Schutzgüter durch Auslegung ermittelt werden. Die Einführung der Resilienz (en: resilience) als *explizite Anforderung in der Datensicherheit* neben den bisherigen Schutzzielen (Verfügbarkeit, Vertraulichkeit, Integrität) stellt dabei ein Novum in der europäischen Gesetzgebung dar. Dementsprechend zeigt sich die inhaltliche Rezeption in der fachrechtlichen Literatur bislang sehr divers und mitunter eher oberflächlich ausgeprägt.

Nachdem zunächst einige Vorbegriffe des Art. 32 Abs. 1 lit b) DSGVO ausgelegt und erläutert werden (I.) folgt die eigentliche Auslegung des Resilienzbegriffs nach den vier juristischen Methoden der Auslegung.[221] Zunächst wird der *Wortlaut* Resilienz untersucht (II.). Als nächstes wird im Rahmen *der systematischen Auslegung* untersucht, wie sich die Resilienz zu dem Risikobegriff und der Risikomethodik des Art. 32 DSGVO sowie in die Regelungstechnik neben den anderen Schutzzielen positioniert. (III). In einem dritten Schritt wird in der *historischen und teleologischen Auslegung* untersucht, wie sich die Datensicherheitsvorgaben entwickelt haben und welche neuen Realweltphänomene aufgetreten sind, auf die der Gesetzgeber ggf. auch mit der Einführung der Resilienz reagieren wollte (IV.).

I. Vorbegriffe

Der zentrale Punkt der Auslegung im Rahmen dieser Untersuchung ist nur der Rechtsbegriff der Resilienz selbst. Somit sind, bevor zur Wortlautauslegung ebendieses Begriffs geschritten werden kann, zunächst noch einige Feststellungen zum übrigen Rechtssatz (Art. 32 Abs. 1 lit b) DSGVO) zu

220 So auch: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 28 ff.; *Bieker*, DuD 2018, 27 (27).

221 *Savigny*, System des heutigen Römischen Rechts, Band 1, S. 213 f.

treffen. Blendet man zunächst die bisherigen Schutzziele aus (zu diesen ausführlich in der systematischen Auslegung unter II.2.) und nimmt den Normauftrag des 1. Hs. auf, lautet der entsprechende Auszug des Rechtssatzes:

> „diese *Maßnahmen [zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus]* schließen gegebenenfalls unter anderem Folgendes ein: […] b) die Fähigkeit, die *Belastbarkeit [Resilienz]* der *Systeme und Dienste* im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;"

Um die nachfolgende Auslegung des schillernden Begriffs Resilienz zumindest grob einzugrenzen, ist deshalb zunächst zu klären, was unter den Begriffen „Maßnahmen", „Systeme" und „Dienste" zu verstehen ist, auf die die Resilienz hier bezogen wird. Darüber hinaus dienen diese Maßnahmen der Gewährleistung der „Sicherheit der Verarbeitung", so dass dieser Begriff zuerst beschrieben werden soll.

1. Datensicherheit / Sicherheit der Verarbeitung

Die Sicherheit der Verarbeitung ergibt sich als Erfordernis zunächst aus der Überschrift des Art. 32 DSGVO. Auch soll durch die Maßnahmen ein „*dem Risiko angemessenes Schutzniveau*" erreicht werden. In anderen Sprachfassungen[222] wird hier jedoch einheitlich von „Sicherheit" und „Sicherheitsniveau" gesprochen, so dass auch der deutsche Begriff des Schutzniveaus in diesem Sinne ausgelegt werden sollte. Normzweck unter der Überschrift „Sicherheit der Verarbeitung" ist es mithin ein „dem Risiko angemessenes Sicherheitsniveau" zu gewährleisten.[223]

Die Sicherheit der Verarbeitung kann bejaht werden, wenn sie die Sicherheit der personenbezogenen Daten (*Datensicherheit*) gewährleistet,[224] was sich insbesondere auch systematisch aus den Meldepflichten (Art. 33

222 Englisch: „Security of Processing/level of security"; Französisch: „Sécurité du traitement/niveau de sécurité"; spanisch „Seguridad del tratamiento/nivel de seguridad"; italienisch: „Sicurezza del trattamento, livello di sicurezza;"; zur Auslegung bei unterschiedlichen Sprachfassungen sogleich: S. 121 f.

223 Ebenso: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 30.

224 *Seufert*, ZD 2023, 256 (257); *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 1b; als "Daten- und Systemsicherheit", *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 1.

Abs. 1, 34 Abs. 1 DSGVO: „Verletzung des Schutzes personenbezogener Daten") ergibt. Die Datensicherheit lässt sich aus Art. 32 Abs. 2 DSGVO und im Umkehrschluss aus Art. 4 Nr. 12 DSGVO zunächst definieren als die Verfügbarkeit, Vertraulichkeit und Integrität personenbezogener Daten.[225] Dies stellt das Herzstück der Datensicherheit dar, an dem sich am Ende auch stets der „Verletzungserfolg" realisiert.[226]

Aber auch die Anforderungen an die Systeme und Dienste, namentlich die Resilienz sind wichtige Bestandteile einer umfassenden Datensicherheit.[227] Sie wirken zunächst im Vorfeld zum Schutz bestehender personenbezogener Daten, da eine Beeinträchtigung der Sicherheit der Systeme und Dienste häufig eine Verletzung des Schutzes personenbezogener Daten (Art. 4 Nr. 12 DSGVO) zur Folge haben kann.[228] Außerdem wirken sie auch dahingehend ergänzend, dass durch die Verarbeitung kein manipuliertes Personenwissen (und damit wiederrum personenbezogenen Daten) erzeugt wird. Datensicherheit kann somit umfassend 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.*

Zur Schutzrichtung wurde bereits erläutert, dass Art. 32 DSGVO auf alle unerwünschten Ereignisse abzielt, d.h. vorsätzliche, fahrlässige und zufällige Ereignisse, die sowohl von internen als auch von externen Quellen ausgelöst werden können.[229]

2. Maßnahmen

Die Sicherheit der Verarbeitung wird durch die Vornahme von Maßnahmen erreicht. Als Maßnahmen werden alle Handlungen definiert, die ge-

225 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (403), Rn. 30.
226 Wie zuvor.
227 So mit Blick auf die „Sicherung der Hard- und Software" auch schon *Gola/Klug/Körffer*, in: Gola/Schomerus, Bundesdatenschutzgesetz [a.F.], 12. Auflage 2015, § 9, Rn. 1.
228 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (403), Rn. 30.
229 Soweit sie in Abgrenzung zu Art 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f) DSGVO nicht bereits durch die Gestaltung der Verarbeitung verhindert werden können, siehe oben, S. 98 f.

eignet sind auf den entsprechenden Schutzzweck, im Kontext des Art. 32 DSGVO, mithin die „Gewährleistung eines risikoangemessenen Schutzniveaus", hinzuwirken.[230] Dabei unterscheidet der Gesetzeswortlaut zwischen technischen und organisatorischen Maßnahmen.

Die *technischen Maßnahmen* zeichnen sich dadurch aus, dass sie unmittelbar in bzw. an der verwendeten Technik, also der verwendeten Hard- und Software,[231] implementiert werden: Hierzu gehören neben informationstechnischen Maßnahmen wie der Verschlüsselung und der Verwendung sicherer Passwörter auch bauliche Maßnahmen, die den Zutritt Unbefugter z.B. zu Serverräumen ausschließen.[232]

Organisatorische Maßnahmen betreffen hingegen die Prozesse außerhalb der Technik und setzen somit insbesondere am Personal an.[233] Beispiele für organisatorische Maßnahmen sind etwa das Vier-Augen-Prinzip, Mitarbeiterschulungen und Protokollierungsvorgaben.

Da viele organisatorische Maßnahmen wie etwa das Vier-Augen-Prinzip eine technische Entsprechung haben müssen, also das etwa eine Aktion erst von den jeweiligen zwei Benutzer-Accounts freigegeben werden muss, wird die Möglichkeit einer klaren Unterscheidung zwischen technischen und organisatorischen Maßnahmen mitunter bezweifelt.[234] Rechtlich besteht insoweit auch keine Notwendigkeit zur Unterscheidung;[235] für den Normanwender kann jedenfalls festgehalten werden, dass sich der Handlungsauftrag nicht nur auf technische Maßnahmen beschränkt, sondern durch organisatorische Maßnahmen auch das Personal mit in den Blick genommen werden muss.

230 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 20a.

231 *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 37; *M. Lang*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 24, Rn 24.

232 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 24, Rn. 21; nur informationstechnische Maßnahmen nennend: *M. Lang*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 24, Rn. 24; *Cherdantseva/Hilton*, in: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), A Reference Model of Information Assurance & Security, 546 (552).

233 *Freund*, in: Schuster/Grützmacher, IT-Recht 2020, Art. 32 DSGVO, Rn. 16.

234 *M. Lang*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 24, Rn. 24 f.; *Hartung*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 24, Rn. 17; *Kipker*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 24 DSGVO, Rn. 16.

235 Wie zuvor.

3. Systeme

Im nachfolgenden Abschnitt soll der Begriff der „Systeme“ im Kontext des Art. 32 DSGVO beleuchtet werden. Nach der sogleich folgenden Darstellung der konsensfähigen Erfassung informationstechnischer Systeme wird auf zwei weitere Fragestellungen eingegangen: Zum einen ob Art. 32 DSGVO an dieser Stelle auch die jeweils enthaltenen Daten in den Systembegriff mit einschließt (a.) und zum anderen ob auch die jeweiligen Personen, die mit dem informationstechnischen System interagieren, im Sinne eines soziotechnischen Verständnisses von dem Systembegriff erfasst werden müssen (b.).

In der Literatur zu Art. 32 DSGVO wird zunächst ein technisches Systemverständnis zugrunde gelegt. Der Begriff des Systems sei insofern weit auszulegen und umfasse somit die Computersysteme wie Server, Arbeitsplatzcomputer sowie die verwendete Netzwerktechnik jeweils sowohl mit ihren *Hard- als auch ihren Softwarekomponenten*.[236] Somit wird deutlich, dass sich der Begriff des Systems in Art. 32 Abs. 1 lit b) DSGVO jedenfalls auf die verwendete Informationstechnik[237] bezieht.[238]

In der Rechtsinformatik definiert *Steinmüller* ein System sehr abstrakt als eine Menge von Elementen und den Relationen zwischen ihnen.[239] Diese Grunddefinition lässt sich dahingehend für die Datensicherheit konkretisieren und erweitern, dass ein System mit seinen Komponenten (Elementen) und deren Relationen so konzipiert ist, dass es einen spezifischen

236 *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 51; *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 43; *Piltz*, in: Gola/Heckmann, DSGVO, 3. Auflage 2022, Art. 32, Rn. 30; *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn 22.

237 Vgl. *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 43 „praktisch jede Form der Informationstechnik“. Daneben sind auch Systeme zur „papiergebundenen Verarbeitung“ erfasst: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 57.

238 Es sei an dieser Stelle darauf hingewiesen, dass die Begriffe Systeme und Komponenten skalierbar sind. So kann etwa ein Netzwerk von mehreren Computern auch als ein „System“ definiert werden, in dem dann diese Computer wiederrum „Komponenten“ bilden. Gerade um eine Technologieoffenheit des Rechts sicherzustellen, erscheint es auch sinnvoll eine Entwicklung der Begriffe in diesem Sinne zuzulassen. Teilweise wird auch von einem „System von Systemen“ gesprochen, wobei letztere dann auch als Subsysteme bezeichnet werden können: *Steinmüller et al.,* JA-Sonderheft 6: ADV und Recht, 1976, S. 10.

239 *Steinmüller et al.,* JA-Sonderheft 6: ADV und Recht, 1976, S. 9.

Dienst erbringt (dazu sogleich).[240] Außerdem lässt sich ein System durch sog. *Systemgrenzen* beschreiben, die das System von der Umwelt abgrenzen und insbesondere für die Bestimmung der Reichweite der Sicherheitsgewähr eine entscheidende Rolle spielen.[241] Zur Verdeutlichung nachfolgende Grafik:[242]

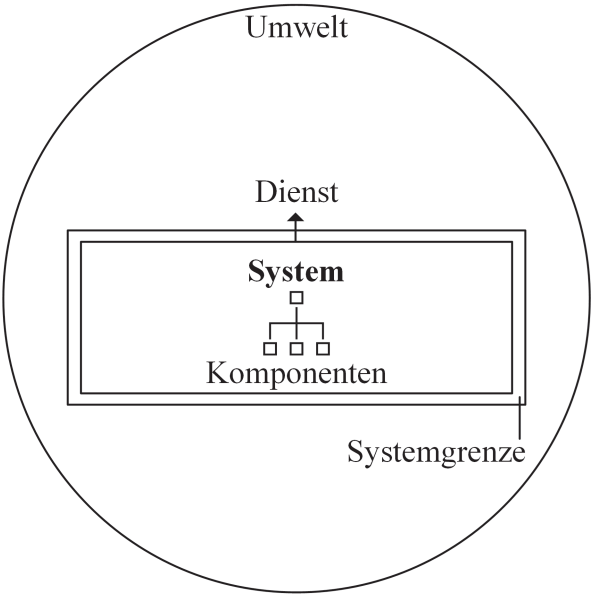

Abbildung 5: IT-System

a. Erfassung personenbezogener Daten

Als Komponenten eines Systems kommen wie o.g. insbesondere die verwendete Hard- und Software in Betracht. Fraglich ist hingegen, ob der Begriff des Systems als weitere Komponente auch die in dem System enthaltenen personenbezogenen Daten umfasst.

240 So in der technischen Literatur auch: *B. Randell/P. Lee/Treleaven*, ACM CSUR 1978, 123 (125).

241 *Aebi*, Praxishandbuch Sicherer IT-Betrieb, S. 5; *Steinmüller et al.,* JA-Sonderheft 6: ADV und Recht, 1976, S. 10.

242 Siehe zu den entsprechenden Definitionen auch *Avizienis et al.*, IEEE TDSC 2004, 11 (11 f.).

Entscheidend ist diese Frage insbesondere für die Auslegung von Art. 32 Abs. 1 lit b) DSGVO. Werden die personenbezogenen Daten als Systembestandteil definiert, sind die dort genannten Schutzziele auch hier auf die personenbezogenen Daten zu beziehen.

Dies wird teilweise mit der Begründung angenommen, dass insbesondere das Schutzziel der Vertraulichkeit nicht auf die Systeme mit ihrem Hardware-Design oder ihrem Software-Code zu beziehen sei, sondern nur die Vertraulichkeit der Daten selbst garantiert werden solle.[243]

Dagegen sprechen jedoch eine Reihe von Gründen: Zuvörderst ist hier der *eindeutige Wortlaut* zu nennen, mit dem die Schutzziele in Art. 32 Abs. 1 lit b) DSGVO auf Systeme und Dienste bezogen werden. Dagegen werden die Schutzziele an anderer Stelle, nämlich in Art. 32 Abs. 1 lit a) und c), Abs. 2 DSGVO explizit oder zumindest sinngemäß auf personenbezogene Daten bezogen.[244] Da somit *alle Schutzziele bereits an anderer Stelle in Art. 32 auf personenbezogene Daten* bezogen werden, entsteht durch die Nichtfassung der personenbezogenen Daten unter den Systembegriff auch keine Schutzlücke. Drittens verkennt die Gegenansicht, dass die explizite Adressierung der Sicherheit von Systemen und Diensten teleologisch wie bereits beschrieben *einen Vorfeldschutz bzw. eine Ergänzung* beschreibt, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Wortlaut und auch Telos sprechen insofern an dieser Stelle für eine spezifische Adressierung der Systeme ohne die darin enthaltenen personenbezogenen Daten.

Es spricht somit insgesamt viel dafür, dass der Gesetzgeber bei der Bezugnahme der Schutzziele auf die Schutzobjekte der Systeme und Dienste anstelle der Daten absichtsvoll handelte und ein eigenständiges Schutzerfordernis normiert hat.[245] Im Ergebnis fallen die personenbezogenen Daten somit nicht unter den Systembegriff des Art. 32 Abs. 1 lit b) DSGVO.

243 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 38.

244 Vgl. *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 23, Fn. 73.

245 Andernfalls würden sich Art. 32 Abs. 1 lit b einerseits sowie Art. 32 Abs. 1 lit c, Abs. 2 in ihrem Schutzgehalt überschneiden. In diesem Sinne die Schutzziele eigenständig für Systeme und Dienste auslegend auch: *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 22 ff.

b. Soziotechnisches Systemverständnis

Klärungsbedürftig ist weiterhin, ob auch die *Personen, die die informationstechnischen Systeme bedienen*, also etwa die Mitarbeitenden des Verantwortlichen im Sinne eines soziotechnischen Systemverständnisses in den Systembegriff einzubeziehen sind; womit sich in der Folge auch die Resilienz auf ein soziotechnisches System beziehen würde.

Für ein soziotechnisches Systemverständnis spricht zunächst, dass die informationstechnischen Systeme ohne die bedienenden natürlichen Personen regelmäßig unvollständig betrachtet werden. Die Mitarbeitenden sind oft eng in die Verarbeitung eingebunden,[246] indem sie etwa einen Verarbeitungsvorgang auslösen, gestalten oder beenden. Sie geben neue Informationen als Daten in das System ein, legen fest ob und wie diese verarbeitet werden sollen und nutzen die entsprechenden Ergebnisse.[247] Dies greift Art. 32 Abs. 4 DSGVO auch auf, indem er den Verantwortlichen verpflichtet sicherzustellen, dass seine Mitarbeitenden die personenbezogenen Daten nur auf seine Weisung hin verarbeiten.

Aufgrund dieser zentralen Stellung sind die Mitarbeitenden oft auch für die Gewährleistung der Sicherheit der Verarbeitung ein wesentlicher Bestandteil. Damit sie die insoweit an sie gestellten Anforderungen erfüllen können, sind insbesondere organisatorische Maßnahmen wie Schulungen im Umgang mit den Sicherheitsmaßnahmen (Nutzbarkeit), verbindliche Regelungen (Policies) und entsprechende auf Akzeptanz ausgerichtete Sensibilisierungen und Aufklärungsmaßnahmen erforderlich.[248] Außerdem müssen die Mitarbeitenden auch bei der Gestaltung der technischen Maßnahmen berücksichtigt werden, da nur eine hohe Nutzbarkeit der Maßnahmen wie etwa bei Authentifizierungsmechanismen einen tatsächlichen Sicherheitsgewinn verspricht. Die o.g. organisatorischen Maßnahmen lassen sich somit auch nicht isoliert von den technischen Maßnahmen betrachten, da sie nur gemeinsam gedacht eine entsprechende Schutzwirkung entfalten können.

246 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 37.

247 So auch bereits *Steinmüller:* Menschen sind als „Bedienungspersonal, Datenlieferanten und Benutzer" Teile (Elemente) eines Informationssystems, *Steinmüller*, Leviathan 1975, 508 (521).

248 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 37; *Eckert*, IT-Sicherheit, S. 3 f.

Spezifisch im Telos der Datensicherheit ist das Ziel eines umfassenden Schutzes der Daten und der daraus ableitbaren persönlichen Informationen hervorzuheben. Hierfür sind auch die Mitarbeitenden und die zugehörigen organisatorische Maßnahmen essenziell. So hilft es für diesen Schutz wenig, wenn die personenbezogenen Daten zwar von dem informationstechnischen System verschlüsselt werden, die Mitarbeitenden mit dem zugehörigen Schlüssel aber nicht sorgsam umgehen oder die persönlichen Informationen in nicht-technischer Weise, etwa mündlich, offenlegen.

Insgesamt sprechen somit einige Argumente dafür, von einem soziotechnischen Systemverständnis auszugehen und die Mitarbeitenden entsprechend mit einzubeziehen.[249]

Allerdings sprechen systematische Gründe gegen ein solches soziotechnisches Systemverständnis. Zunächst ist hier zu beachten, dass die technischen Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität auf das System bezogen werden. Insbesondere die Sicherstellung der Integrität und der Vertraulichkeit der Mitarbeitenden zu verlangen, erscheint nicht sachgerecht. Bei den Schutzzielen handelt es sich um in der Informationstechnik tradierte, technische Eigenschaften.[250] Eine Übertragung auf die soziale Ebene der Mitarbeitenden erscheint daher unpassend. Auch lässt sich argumentieren, dass die Einbeziehung der Mitarbeitenden in das Datensicherheitskonzept des Art. 32 Abs. 1 DSGVO zumindest nicht als Automatismus erfordert, dass diese auch unter den Begriff des Systems subsumiert werden, sondern bereits über das Erfordernis der Vornahme „organisatorischer Maßnahmen" abgedeckt ist.

Insgesamt kann die Frage, ob der Systembegriff in der DSGVO technisch oder soziotechnisch zu verstehen ist, an dieser Stelle noch nicht abschließend beantwortet werden. Für die Resilienz als umfassendes Prinzip könnte ein soziotechnisches Verständnis geboten sein, während die klassischen Schutzziele nur auf ein technisches System angewendet werden können. Mangels einer eindeutigen, abstrakten Festlegung müssen somit beide Aspekte im Verlauf der Untersuchung noch näher beleuchtet werden.[251]

---

249 Für ein Informationssystem in der Informationssicherheit ebenso: *Cherdantseva/Hilton*, in: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), A Reference Model of Information Assurance & Security, 546 (547).

250 *Samonas/Coss*, JISSec, Vol. 10 (2014), Heft 3, 21 (23 ff.); hierzu später ausführlich ab S. 187 ff.

251 Siehe im Ergebnis S. 201.

4. Dienste

Als weiteres Schutzobjekt neben den Systemen nennt Art. 32 Abs. 1 lit b) DSGVO die Dienste. Fraglich ist, wie der Begriff des Dienstes im Kontext der „Sicherheit der Verarbeitung" auszulegen ist. Im IT-Recht kann der Dienst technisch, ökonomisch als auch rechtlich verstanden werden.

a. Ökonomische Betrachtung

Zunächst kommt dem Dienstbegriff in einer *ökonomischen Betrachtung* Bedeutung zu: So beschreibt der Dienst der Informationsgesellschaft (Art. 4 Nr. 25 DSGVO mit Verweis auf Art. 1 Nr. 1 lit b) RL 2015/1535) „eine Dienstleistung der Informationsgesellschaft, d.h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung." Charakterisierend für den Dienstbegriff ist somit insbesondere das regelmäßig entgeltliche Leistungsangebot an einen Dritten.

Die Anwendung der ökonomischen Betrachtung auf den Dienst in Art. 32 Abs. 1 lit b) DSGVO ist indes zweifelhaft. Die Datensicherheitsvorgaben des Art. 32 DSGVO dienen anders als die Vorgaben des IT-Sicherheitsrechts nicht der gesicherten Erbringung einer ökonomisch relevanten Dienstleistung wie etwa der Bereitstellung einer Online-Suchmaschine oder eines Online-Marktplatzes. Vielmehr liegen wie zuvor beschrieben die Schutzgüter in den Rechten und Freiheiten natürlicher Personen, welche durch die Verarbeitung personenbezogener Daten gefährdet sein können.

b. Rechtliche Betrachtung

Bei einer *rechtlichen Betrachtung* hat der Dienst eine Gruppierungs- und Verantwortungszuweisungsfunktion, etwa im IT-Sicherheitsrecht, indem an den Dienst anknüpfend der Anbieter desselben alle hierfür notwendigen Systeme in seinen Anwendungsbereich einzubeziehen hat.[252]

In der DSGVO erscheint die rechtliche Betrachtungsweise dagegen nicht angezeigt, da die Verantwortung durch die Entscheidungsbefugnis über die Verarbeitung personenbezogener Daten begründet wird (Art. 4 Nr. 7

252 So etwa in Art. 21 Abs. 1 NIS2-RL und § 165 Abs. 1 TKG.

DSGVO) und nicht durch die Erbringung eines spezifischen Dienstes wie etwa den zuvor genannten.

c. Technische Betrachtung

Schließlich lässt sich bei einer *technischen Betrachtung* festhalten, dass Dienste von Systemen bereitgestellt bzw. erbracht werden.[253] In dem Dienst drückt sich das Verhalten des Systems nach außen, mithin an seine Umwelt aus; er wird wie bereits beschrieben[254] über eine Schnittstelle an der jeweiligen Systemgrenze an eine(n) oder mehrere Nutzer:innen erbracht.[255] Der Dienst stellt somit die spezifische Funktionalität eines Systems dar.

Im Kontext der Verarbeitung personenbezogener Daten kann der Dienst als die spezifizierte Funktionalität des Systems insbesondere auf die Verarbeitungsergebnisse personenbezogener Daten bezogen werden.[256] Somit kann hierunter vor allem das Generieren von *Personenwissen* aus personenbezogenen Einzelinformationen nach dem bereits dargestellten DIW-Modell gefasst werden. Praktisch schließt dies insbesondere die Bewertung persönlicher Aspekte im Rahmen des Profilings mit ein (Art. 4 Nr. 4 DSGVO). Insofern erscheint für den Dienstbegriff der DSGVO die technische Betrachtung am geeignetsten.

Zu beachten ist dabei auch, dass der Dienstbegriff durch den jeweiligen Zweck der Verarbeitung determiniert wird, d.h. ein Dienst darf nur darin bestehen, was vom jeweiligen Zweck (Art. 5 Abs. 1 lit. b) DSGVO) erfasst ist. Liegt der Zweck z.B. in der Reichweitenmessung eines Webangebots, muss sich der zugehörige technische Dienst des jeweiligen Systems auch in dieser Funktionalität erschöpfen.

---

253 *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 43.

254 Siehe oben, S. 115.

255 *Avizienis et al.*, IEEE TDSC 2004, 11 (11 ff.), Nutzer:in muss demnach auch nicht zwingend eine natürliche Person, sondern kann auch ein anderes System sein.

256 Außerdem kann ein technischer Dienst (ohne im hier dargestellten Sinn an der Verarbeitung mitzuwirken) die Zugriffs- (für den Auskunftsanspruch, Art. 15 DSGVO), Änderungs- und Löschungsfunktionen (Art. 16, 17 DSGVO) an den personenbezogenen Daten bereitstellen, die dem Betroffenen zur Wahrnehmung seiner Rechte zustehen; Vgl. *Kramer/Meints*, in: Auernhammer, DSGVO BDSG, 7. Auflage 2020, Art. 32, Rn. 43; *Sattler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 197 (214).

Diese technische Unterscheidung zwischen dem System an sich und der von ihm bereitgestellten, spezifizierten Funktionalität (Dienst) ist, wie im weiteren Verlauf gezeigt werden wird, für die Resilienz von nicht zu unterschätzender Bedeutung. Ob die Unterscheidung sich hingegen auch auf die Schutzziele dergestalt auswirkt, dass sich diese mit Blick auf Systeme oder Dienste sinnvoll voneinander abgrenzen lassen, ist zweifelhaft. Einzelheiten dazu werden ebenfalls an späterer Stelle erläutert, wenn die Schutzziele der Resilienz systematisch gegenübergestellt werden.

II. Auslegung nach dem Wortlaut

Nach Bestimmung der soeben dargestellten Vorbegriffe folgt nun die Auslegung des Begriffs der Resilienz. Ausgangspunkt einer jeden Auslegung ist zunächst der Wortlaut des Gesetzes.[257] Dieser Umstand ist zu trennen von der Auslegungsmethodik „nach dem Wortlaut" (auch grammatische Auslegung)[258], die den allgemeinen oder auch den spezifischen Sprachgebrauch der adressierten Fachdomäne ermittelt.[259] Im ersten Schritt (1) soll daher unmittelbar auf den deutschen Wortlaut „Belastbarkeit" eingegangen und diese Begrifflichkeit mit den anderen Sprachfassungen verglichen werden. Im zweiten Abschnitt dieses Kapitels wird sodann das allgemeine sowie das domänenspezifische Verständnis der „Resilienz" untersucht. Daran schließen sich die Synthese der domänenspezifischen Verständnisse (3.) und das Fazit für die Wortlautauslegung (4.) an.

1. „Belastbarkeit" oder Resilienz

Im europäischen Recht kommt den unterschiedlichen Sprachfassungen im Rahmen der Wortlautauslegung eine hohe Bedeutung zu.[260] Nach dem EuGH sind „die *verschiedenen sprachlichen Fassungen gleichermaßen verbindlich* […]; die Auslegung einer gemeinschaftsrechtlichen Vorschrift erfordert somit einen Vergleich ihrer sprachlichen Fassungen."[261]

257 *Herdegen*, Europarecht, S. 226, Rn. 92; *EuGH*, Urt. v. 17.04.2018 – C-414/16, NZA 2018, 569 (570), Rn. 44. *Honsell*, ZfPW 2016, 106 (120).
258 *Honsell*, ZfPW 2016, 106 (120 f.).
259 *Bydlinski*, Grundzüge der juristischen Methodenlehre, S. 27.
260 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (293 f.), Rn. 14.
261 *EuGH*, Urt. v. 06.10.1982 – Rs 283/81, NJW 1983, 1257 (1258).

Wie bereits angedeutet ist in der deutschen Fassung der DSGVO von „Resilienz" zunächst keine Rede. Vielmehr findet sich hier das Merkmal der „Belastbarkeit". Belastbarkeit ist nach dem *Duden* die Fähigkeit, eine Materialbeanspruchung auszuhalten, also z.B. die Belastbarkeit eines Drahtseils, aber auch körperliche und seelische Inanspruchnahme auszuhalten oder zu verkraften.[262]

In der Literatur wird zumeist die Auffassung vertreten, dass der deutsche Begriff „Belastbarkeit" verkürzt sei und daher sachgerechter und näher am englischen Original von Resilienz gesprochen werden sollte.[263] Da ein pauschaler Vorrang insbesondere der englischen Sprachfassung („resilience") im europäischen Recht aber nicht besteht, gilt es nun auch die anderen Sprachfassungen zu vergleichen.

Allerdings wird auch in der französischen („la résilience"), der italienischen („la resilienza") und der spanischen („la resiliencia") Sprachfassung von „Resilienz" gesprochen. Dies spricht bei einer vergleichenden Betrachtung dafür, auch im Deutschen eher dem lateinischen Wortstamm „resilire" (übersetzt als: zurückspringen, abprallen)[264] folgend von Resilienz als von „Belastbarkeit" zu sprechen. Im Übrigen ist die Übersetzung von „resilience" mit „Belastbarkeit" in die deutsche Rechtssprache nicht durchgängig. In EG 13 der NIS-RL wurde „resilience" dagegen mit „Robustheit" übersetzt, auch im Spanischen findet mit „la resistencia" eine abweichende Übersetzung statt. Im Französischen sowie im Italienischen stimmt die Übersetzung hingegen mit der DSGVO überein. In dem EU Cyber-Security-Act wird neben „Security" auch "Resilience" von (elektronischen) Geräten gefordert; in der deutschen Fassung wird es hier mit „Abwehrfähigkeit" übersetzt, während in den französischen, italienischen und spanischen Fassungen erneut o.g. Pendants der „Resilienz" verwendet werden.[265]

Auch aus der Sicht insbesondere der deutschen Rechtsanwender wäre eine einheitliche Übersetzung dringend geboten, um sowohl auf nationaler wie auch auf europäischer Ebene Missverständnissen und Fehlinterpre-

262 *Duden*, https://www.duden.de/rechtschreibung/Belastbarkeit, zuletzt abgerufen am 20.03.2024.

263 *Gonscherowski/M. Hansen/Rost*, DuD 2018, 442 (442), Fn. 1; *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn 42; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39; wohl auch: DSK, Standard-Datenschutzmodell, Teil B1.19, S. 22.

264 *Langenscheidt Wörterbuch*, https://de.langenscheidt.com/latein-deutsch/resilire, zuletzt abgerufen am 20.03.2024.

265 EU Cybersecurity-Act, VO 2019/991, EG. 2, Satz 2, EG. 5 sowie Art. 1 Abs. 1; in letztgenanntem Fall: "Fähigkeit zur Abwehr gegen Cyberangriffe"

tationen vorzubeugen. In der nachfolgenden Tabelle wird eine Auswahl von Übersetzungen von *„resilience"* aus EU-Dokumenten (Gesetzen sowie Kommissionsmitteilungen) aus der Sicherheit in der Informationstechnik aufgezeigt, um die Problematik zu verdeutlichen:

Tabelle 3: Übersetzungen von Resilienz im Daten- und IT-Sicherheitsrecht

Übersetzung	**Quelle**
Stabilität	Mitteilung der Kommission zum Schutz kritischer Informationsinfrastrukturen (Titel);[266] Entwurf DORA[267]
Robustheit	Mitteilung der Kommission zum Schutz kritischer Informationsinfrastrukturen (Text)[268]; EG 13 NIS-RL (s.o.)
Abwehrfähigkeit	EU Cybersecurity-Act[269]
Widerstandsfähigkeit	EU Cybersicherheitsstrategie 2013[270]
Resilienz	Mitteilung der Kommission zur Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit […][271]
Belastbarkeit	Art. 32 DSGVO (s.o.)

Diese Bandbreite an Übersetzungen ist kritisch zu bewerten. Zwar ist es nicht per se schädlich, dass ein Begriff in unterschiedlichen Gesetzen unterschiedlich übersetzt wird, da selbst identische Begriffe in unterschiedlichen Gesetzen nicht stets dieselbe Bedeutung haben müssen (sog. „Relativität der Rechtsbegriffe").[272] Da alle diese Gesetze aber zum Daten- und IT-Sicherheitsrecht i.w.S. gehören, legt der zuvor dargestellte Befund eher eine unsystematische, quasi willkürliche Übersetzungsweise nahe.

Für die Auslegung der deutschen Fassungen der Gesetze aus dem Bereich der IT-Sicherheit sollte daher sowohl aus vergleichender Betrachtung mit den anderen Sprachfassungen als auch angesichts der uneinheitlichen

266 EU KOM 2009 149 endgültig.
267 EU COM 2020 595 final, 24.9.2020; in der verabschiedeten Gesetzesfassung (EU-VO 2022/2554) wurde aber erfreulicherweise der Begriff „Resilienz" in der deutschen Fassung verwendet.
268 EU KOM 2009 149 endgültig, u.a. S. 2 f.
269 Siehe Fn. 265.
270 EU KOM, 2013/01 final, S. 5; ebenso: Strategie für eine sichere Informationsgesellschaft, EU KOM 2006/251 final, S. 7.
271 EU KOM, 2016/410 final, S. 3; aber auch häufig wieder als „Abwehrfähigkeit" übersetzt.
272 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (296 f.), Rn. 20.

Übersetzung in die deutschsprachigen, europäischen Rechtsvorgaben zur IT-Sicherheit der Begriff „Resilienz" als vorzugswürdig angesehen werden. Dies ermöglicht ein einheitliches Verständnis und vermeidet insbesondere mit Blick auf die „Belastbarkeit" und andere „behelfsmäßige Übersetzungen"[273] eine unsachgemäße, semantische Reduktion des Begriffs. Insbesondere die Übersetzung „Belastbarkeit" legt v.a. das reduzierte Verständnis einer „besseren Verfügbarkeit"[274] nahe und kann somit gerade nicht die Inhalte der weitergehenden „Resilienz" vollständig erfassen (dazu in den folgenden Abschnitten ausführlich).

2. Allgemeine Wortbedeutung und domänenspezifische Verwendung

Allerdings ist diese Diversität der Übersetzungen auf europäischer Ebene auch nicht völlig unerklärlich. Als Ausgangspunkt für die Wortlautauslegung ist zunächst auf den gewöhnlichen Sprachgebrauch abzustellen.[275] Ein solcher gewöhnliche Sprachgebrauch im Sinne eines allgemeinen, disziplinübergreifenden Verständnisses des Begriffs ist indes für die Resilienz nur schwerlich auszumachen.

Bezüglich des lateinischen Ursprungs des Begriffs „resilire" ist festzuhalten, dass dieser zunächst mit „zurückspringen" oder „abprallen" übersetzt werden kann.[276] Darauf folgte aber eine sehr bewegte Etymologie des Begriffs, die von „springenden" Fröschen im antiken Rom, über den Rückzug der Königin in England bis hin zu den Anforderungen an Stahlträger im Zeitalter der Industrialisierung reicht.[277] Und auch heute finden sich in den Lexika zumeist nur domänenspezifische Definitionen: So beschreibt der *Brockhaus* die Resilienz mit Blick auf die Psychologie und zwar als „die psychische Widerstandsfähigkeit von Menschen, die es ermöglicht,

273 *Scharte*, Resilience Engineering, S. 37.

274 Derart verkürzend: *Jergl*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018, Art. 32, Rn. 32; *Voskamp/D. Klein*, in: Kipker, Cybersecurity, S. 279, Rn. 19b; *Karg*, in: Lang/Löhr, IT-Sicherheit, 99 (111).

275 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (295), Rn. 17; *EuGH*, Urt. v. 05.07.2012 – C-49/11, EuZW 2012, 638 (639), Rn. 32; *EuGH*, Urt. v. 10.03.2005 – C-336/03, NJW 2005, 3055 (3055), Rn. 21.

276 *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (754); *Gonscherowski/M. Hansen/Rost*, DuD 2018, 442 (442); en: bounce back: *Alexander*, NHESS 2013, 2707 (2708); *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9.

277 *Alexander*, NHESS 2013, 2707 (2708 ff.).

selbst widrigste Lebenssituationen und hohe Belastungen ohne nachhaltige psychische Schäden zu bewältigen."[278] Das englische Oxford Lexikon nennt dagegen zwei Definitionen aus anderen Domänen: (1) „The capacity to recover quickly from difficulties; toughness, e.g. the often remarkable resilience of so many British institutions" sowie (2) „The ability of a substance or object to spring back into shape; elasticity., e.g. nylon is excellent in wearability, abrasion resistance and resilience". Während die erste Definition auf die Resilienz soziotechnischer Systeme wie (staatlicher) Institutionen abstellt, entstammt die zweite Definition offensichtlich aus der Materialwissenschaft. Zusammen mit der Psychologie-Definition aus dem *Brockhaus* lassen sich mithin allein in den beiden wohl bekanntesten, englischen und deutschen Lexika drei Definitionen aus unterschiedlichen Fachdomänen finden. Zugleich lässt sich aus diesen Definitionen allerdings eine erste Gemeinsamkeit extrahieren: In allen Fällen wird eine Entität mit einer Einwirkung konfrontiert und die Resilienz bezieht sich insoweit auf die Reaktion bzw. die Reaktionsfähigkeit dieser Entität.

Da sich aber ein darüber hinaus konkretisierender, gewöhnlicher Sprachgebrauch nicht fixieren lässt, ist nun in einem zweiten Schritt der spezifische Sprachgebrauch in ausgewählten Fachdisziplinen zu untersuchen.[279] Für eine intensivierte Analyse werden zunächst die Psychologie (a.), die Ökologie-, Klima- und Umweltforschung (b.) sowie aus der Technikdomäne die Material- und Ingenieurswissenschaft (c.i.), die Informationstechnik (c.ii.) und die kritischen Infrastrukturen (c.iii.) betrachtet. Weiterhin wird das Verständnis gesellschaftlicher Resilienz insbesondere angesichts von Katastrophen untersucht (d.).

Mit diesen Vorkenntnissen wird dann schließlich noch das dem Datensicherheitsrecht nahestehende IT-Sicherheitsrecht untersucht (e.). Dieses enthält zwar noch keine spezifisch IT-Sicherheitsrechtliche Definition, aber zumindest allgemeinere Definitionen sowie verschiedene weitere Anhaltspunkte. Neben deutschen und europäischen Regelungen werden auch solche aus der Schweiz und den USA berücksichtigt.

278 Daneben wird auch „digitale Resilienz" genannt, die aber sehr reduziert nur als „Fähigkeit, Herausforderungen der digitalen Welt zu bewältigen" definiert wird; *Brockhaus,* https://brockhaus.de/ecs/enzy/article/resilienz-psychologie, und https://brockhaus.de/ecs/enzy/article/digitale-resilienz, zuletzt abgerufen am 20.03.2024.

279 Siehe für eine erste Übersicht an Definitionen: Meridan Institute, Definitions of Community Resilience: An Analysis.

Die in den jeweiligen Fachdisziplinen gefundenen Ergebnisse werden im Anschluss an diesen Abschnitt (2.) für die Auslegung der Resilienz als Rechtsbegriff im Datensicherheitsrecht synthetisiert (3.).

a. Psychologie

Der Begriff hat hier bereits eine längere Tradition.[280] Erste Ursprünge finden sich in der Stressforschung, in der *Hans Selye*[281] das allgemeine Anpassungs-Syndrom (ASP) als eine „selbstständige, unspezifische Reaktion des Körpers auf jede Art von Schädigung" beschrieb und dabei in drei Phasen unterteilte: Eine Alarmreaktion als eine Art allgemeine Mobilmachung des Körpers, z.B. durch die Ausschüttung von Stresshormonen. In der sich anschließenden Widerstandsphase versucht der Körper sich mittels einer Gegenreaktion anzupassen, die Stresshormone abzubauen und wieder einen zumindest temporär stabilen Zustand zu erreichen. Nimmt die Belastung aber nicht ab, fällt der Körper danach in eine Erschöpfungsphase, da die Anpassungsenergie während der Widerstandsphase verbraucht wird. Zum besseren Verständnis umschreibt er die Phasen anhand des einfachen Beispiels des Hell-/Dunkel-Sehvermögens wie folgt: Tritt eine Person aus dem Dunkel in eine helle Umgebung, wird sie zunächst geblendet (Alarmreaktion). Daraufhin folgt die Anpassung an die neuen Lichtverhältnisse (Widerstandsphase), wodurch die Person ihre Umgebung wiedererkennen kann. Ist das Licht aber zu hell, etwa weil die Person in die Sonne blickt, erschöpft sich die Sehfähigkeit (Erschöpfungsphase).[282]

Während und nach dem zweiten Weltkrieg richtete sich der Blick spezifischer auf den Bereich der Psychologie, d.h. konkret auf die Frage des menschlichen Umgangs mit widrigen Ereignissen. Der Holocaust-Überlebende und spätere Professor für Neurologie und Psychiatrie an der Universität Wien *Viktor Frankl* stellte mit seinem Konzept der *„Trotzmacht des Geistes"* v.a. auf die innere Einstellung im Sinne einer *positiven Zukunftsorientierung* ab, die insbesondere einen über das Ertragen bzw. das Über-

280 Vgl. zu der nachfolgend dargestellten Entwicklung statt vieler: *Hoffmann*, Organisationale Resilienz, S. 49.

281 *Selye*, Stress beherrscht unser Leben, S. 38, 44 f., 82 ff., 146 ff.; vgl. *Nerdinger/Blickle/Schaper*, Arbeits- und Organisationspsychologie, S. 528 f. mit einer Zusammenfassung.

282 *Selye*, a.a.O., S. 84 f.

winden des eigenen Leids hinausgehenden, konkreten Sinn des Lebens voraussetze, der die Frage nach dem „Warum" des Überlebens/Leidens beantwortet.[283]

Daneben nahm auch die Entwicklungspsychologie einen zunehmend großen Raum ein. Impetus der Forschung war hier die Frage, ob, inwieweit und aus welchen Gründen kindliche Entwicklungen angesichts von Konfrontationen mit widrigen Ereignissen unterschiedlich (erfolgreich) verlaufen. Hierzu fand ab den 1950er Jahren auf der Insel Kauai (Hawaii) eine groß angelegte und viel zitierte Studie der Entwicklungspsychologin *Emmy Werner* statt, die mit ihrem Team der University of California knapp 700 Jungen und Mädchen beobachtete, die im Jahr 1955 auf besagter Insel geboren wurden.[284] Im Ergebnis wurde dabei festgestellt, dass von den 201 Kindern, die unter besonders schwierigen Bedingungen -wie etwa psychisch kranke oder alkoholsüchtige Eltern- aufwuchsen, 72 Kinder im Rahmen der 40 Jahre andauernden Beobachtung keine besonderen Auffälligkeiten aufwiesen. Sie erwiesen sich mithin als resilient gegenüber den widrigen Bedingungen, denen sie ausgesetzt waren. Im Rahmen weiterer Untersuchungen konnte dies u.a. darauf zurückgeführt werden, dass diese Kinder mindestens eine besonders enge Bezugsperson hatten und eine solche *soziale Bindung* folglich einen Resilienzfaktor darstellt.[285] Später wurde eine solche enge, soziale Bindung auch als Resilienzfaktor zur Prävention von Jugendgewalt nachgewiesen.[286]

Es folgten weitere Studien im Kinder- und Jugendbereich wie z.B. die in den 1990er Jahren durchgeführte „Bielefelder Invulnerabilitätsstudie", die sich mit Jugendlichen aus schwierigen Verhältnissen beschäftigte. Hierbei konnte auch eine *emotionale Ausgeglichenheit bzw. Robustheit* als Resilienzfaktor identifiziert werden; umgekehrt erwiesen sich Impulsivität und eine geringe Frusttoleranz als schädlich.[287]

Heute kann die Resilienz in der Psychologie[288] ergebnisorientiert definiert werden als „die Fähigkeit einer Person […], erfolgreich mit belasten-

283 *Frankl/Batthyány*, Wer ein Warum zu leben hat, S. 102 f., 117 f., 143., 212 ff.
284 Vgl. *Berndt*, Resilienz, S. 65 f.
285 *Berndt*, Resilienz, S. 67 f.
286 *Lösel/Farrington*, AJPM, Vol. 43 (2012), 8-23.
287 *Berndt*, Resilienz, S. 70.
288 Als Synonyme werden mitunter auch die Begriffe „Stressresistenz, psychische Robustheit oder psychische Elastizität" verwendet, *Wustmann*, Resilienz, S. 18.

den Lebensumständen und negativen Folgen von Stress umzugehen."[289] Bei belastenden oder widrigen Lebensumständen, fachsprachlich auch „Stressor" genannt, kann insbesondere zwischen chronischen Zuständen und singulären traumatischen Ereignissen unterschieden werden.[290]

Dabei sollte der Begriff „Fähigkeit" nicht dahingehend missverstanden werden, dass es sich um ein einer Person etwa genetisch oder aufgrund ihrer Erziehung statisch anhaftendes Attribut handelt. Vielmehr stellt die Resilienz einen „dynamischen Anpassungsprozess" i.S. einer „Auseinandersetzung mit dem Stressor" dar,[291] der bzw. die je nach Grad der Resilienz unterschiedlich erfolgreich verlaufen kann. Der Prozess umfasst chronologisch sowohl die Anpassung während als auch die Regeneration nach entsprechenden widrigen Lebensereignissen.[292] Aus der inhärenten Notwendigkeit der individuellen Anpassung an den jeweiligen Stressor folgt außerdem, dass die Resilienz einer Person über ihre Lebenszeit und angesichts der Konfrontation mit unterschiedlichen Stressoren variabel ist.[293]

Im Sinne eines präventiven Konzepts wird dabei davon ausgegangen, dass die Resilienz einer Person von verschiedenen, z.T. auch miteinander verschränkten Einzelaspekten („Resilienzfaktoren")[294] abhängig ist, deren bisherige Aufzählung in diesem Abschnitt auch lediglich als exemplarisch anzusehen ist.[295] Weiterhin ist zu beachten, dass diese Faktoren nicht einfach summarisch addiert werden können, sondern oft „miteinander assoziiert sind und interagieren".[296] Neben diesen Resilienzfaktoren wird außerdem erforscht, inwieweit die bisherige Erfahrung von widrigen Lebensereignissen ihrerseits die Resilienz für die Zukunft erhöht, mithin

289 *Wustmann*, Resilienz, S. 18 m.w.N.; *Fröhlich-Gildhoff/Rönnau-Böse*, Resilienz, S. 9; *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (754 f.).

290 Forschungsergebnisse beziehen sich häufiger auf die letztgenannte Gruppe, *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (754).

291 *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (754); *Rutter*, Development and psychopathology 2012, 335 (335).

292 *Helmreich/A. Kunzler/Lieb*, Im OP 2016, 270 (271).

293 *Wustmann*, Psychotherapie Forum, Vol. 17 (2009), Heft 2, 71 (73).

294 Als weitere Resilienzfaktoren werden u.a. der sozioökonomische Status (extern) sowie die kognitive Fähigkeiten und die (Epi-)Genetik des Betroffenen (intern) genannt *Kunzler et al.*, Nervenarzt 2018, 747 (747 f.); *R. Kalisch/Müller/Tüscher*, Behavioral and Brain Sciences 2015, AS-Nr. e128 (nur online); *Wright/Masten/Narayan*, in: Goldstein/Brooks, Handbook of Resilience in Children, 15 (17, 20 f.).

295 Siehe zu weiteren Resilienzfaktoren (dort: „Prädiktoren): *Kleim/R. Kalisch*, Nervenarzt 2018, 754 (755 ff).

296 *Kunzler et al.*, Nervenarzt 2018, 747 (748).

einen „abhärtenden Effekt“[297] hat. Dies betrifft v.a. die Erholungsphase mit der Frage, welche Begleitumstände nach einem widrigen Lebensereignis vorliegen müssen, damit aus einem solchen ein Gewinn an Resilienz und nicht im schlimmsten Fall sogar eine stärkere Anfälligkeit für künftige, widrige Lebensereignisse erwächst.[298]

Exemplarisch sei hier abschließend auf die Arbeit des *Leibniz-Instituts für Resilienzforschung* in Mainz verwiesen, das seit 2014 die neurowissenschaftlichen und psychologischen Mechanismen der Resilienz erforscht und darauf aufbauend auch versucht, resilienzfördernde Interventionen wie etwa psychologische Trainingsmethoden zu entwickeln.[299]

b. Ökologie, Umwelt- und Klimaforschung

Auch in der Ökologie ist der Resilienzbegriff schon länger gebräuchlich. Er wurde hier v.a. durch *Holling* geprägt, der Resilienz definierte als die Beständigkeit von Beziehungen innerhalb eines Ökosystems sowie als Maß für die Fähigkeit eines solchen, die Veränderung von Zustands- oder Antriebsvariablen aufzunehmen und weiterhin zu bestehen.[300] Damit legte sein Ansatz erstmals ein systembezogenes Verständnis von Resilienz zugrunde.[301]

Entscheidend für *Hollings* Verständnis von Resilienz ist v.a. der Gegenbegriff der Stabilität. Ein resilientes System zeichnet sich demnach durch seine Möglichkeit zu starken Schwankungen aus, etwa Insektenpopulationen, die zwar bei einer äußeren Veränderung sehr stark dezimiert werden, sich aber danach auch sehr schnell wieder erholen.[302] Demgegenüber stehen nicht resiliente Populationen, die zwar an sich eine sehr stabile Größe aufweisen, bei einer Veränderung aber ggf. schneller aussterben können.[303]

---

297 „Steeling or Strengthening Effect“, *Rutter*, Development and psychopathology 2012, 335 (335).

298 *Rutter*, Development and psychopathology 2012, 335 (337 ff).

299 Siehe Webseite der Institution: https://lir-mainz.de/strategie, zuletzt abgerufen am 30.08.2024; *Helmreich/A. Kunzler/Lieb*, Im OP 2016, 270 (271).

300 *S. Kaufmann/Blum*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 235 (238); *Holling*, Annual Review of Ecology and Systematics 1973, 1 (17).

301 *Alsubaie/Alutaibi/Martí*, in: Rome/Theocharidou/Wolthusen, Critical Information Infrastructures Security, 43 (44).

302 *Holling*, Annual Review of Ecology and Systematics 1973, 1 (17 f.).

303 Wie zuvor.

Neben dieser quantitativen Resilienz können ökologische Systeme außerdem auch in qualitativer Hinsicht verschiedene komplexere Zustände einnehmen, z.B. Flachwasserseen, die „in Abhängigkeit von Variablen wie Nährstoffgehalt, Seegröße und Temperatur – zwischen einem Klarwasserzustand und einem eutrophierten, trüben Zustand wechseln" können.[304]

Zusammenfassend als maßgeblich festzuhalten ist daher, dass in der Ökologie ein resilientes System durch die Fähigkeit zur Einnahme unterschiedlicher quantitativer und qualitativer Zustände zwar nicht in einem Sinne stabil ist, dass es einen Gleichgewichtszustand kontinuierlich beibehält, aber sich gleichwohl bzw. gerade deshalb als besonders überlebensfähig und mithin resilient auszeichnet.[305] Auch ist es ökologischen Systemen möglich, sich dauerhaft anzupassen[306] und nicht mehr in einen bereits bekannten Zustand zurückzukehren. Hierin wird der wesentliche Unterschied zwischen technischer und ökologischer Resilienz gesehen, da technische Resilienz in der Regel (nur) darauf zielt in einen ursprünglich vorgesehenen „Normal-Betriebszustand" zurückzukehren.[307]

Eine etwas andere Dimension entwickelt der ökologische Resilienzbegriff, soweit der Mensch als Teil des ökologischen Systems berücksichtigt wird. So untersucht etwa das *Stockholm Resilience Centre*[308] die Resilienz mit Blick darauf, dass die Menschen und die Natur auf der Erde ein einheitliches sozio-ökologisches System bilden. Dieses soll resilient sein, d.h. in die Lage versetzt werden mit Veränderungen umzugehen und sich fortwährend weiterzuentwickeln. Maßgeblich soll dies durch die Gestaltung der Beziehung zwischen Menschen (untereinander) sowie zwischen Menschen und Natur erreicht werden. Zur Erreichung von Resilienz werden dabei sieben Prinzipen genannt,[309] von denen zumindest die ersten fünf für die vorliegende Auslegung relevant erscheinen:

304 *Brand/Hoheisel/Kirchhoff*, in: Bayerische Akademie für Naturschutz und Landschaftsplege (ANL), Landschaftsökologie. Grundlagen, Methoden, Anwendungen, 78 (80) m.w.N.

305 *Holling*, Annual Review of Ecology and Systematics 1973, 1 (17 f.); siehe aber auch kritisch zur Frage der Allgemeingültigkeit dieses Konzepts: Fn. 304.

306 Ähnlich auch: *Longstaff*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 259 (266).

307 *Longstaff*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 259 (265 f.); *Zampieri*, Ecosphere, Vol. 12 (2021), Heft 2, S. 1.

308 https://www.stockholmresilience.org/research/research-news/2015-02-19-what-is-resilience.html, zuletzt abgerufen am 30.08.2024.

309 *R. Biggs et al.*, ARER 2012, 421 (425 ff.); hier nicht mit aufgenommen wurden die „breite Beteiligung anderer Personen" sowie „polyzentrale Regierungssysteme".

1. Diversität bzw. Redundanz:
   Nur ‚diverse' Systeme mit *vielen (unterschiedlichen) Komponenten* wie etwa Tierarten besitzen die Fähigkeit der Kompensation von ausfallenden Komponenten. Umgekehrt bedeutet dies auch, dass nicht redundante Komponenten besonders geschützt werden sollten.
2. Verbundenheit
   Kann in positiver Hinsicht die Regeneration beschleunigen, in negativer Hinsicht aber auch zur schnelleren Ausbreitungen von Störungen führen (Domino-Effekt).
3. Langsame Variablen und Rückkopplungen
   Gewisse Variablen wie etwa *Sättigungsfaktoren* in Flüssigkeiten (Gewässern) oder Gasen (Atmosphäre) werden lange ‚absorbiert', ohne dass es zu einer qualitativen Auswirkung kommt; ab gewissen Sättigungswerten werden aber *Kipppunkte* erreicht, die nur schwer kontrollier- oder umkehrbare Folgen haben, da es ab diesem Moment zu weiteren Rückkopplungen kommt.
4. CAS-Ansatz
   Der komplexe adaptive Systemansatz (CAS) bedeutet, dass innerhalb eines sozio-ökologischen Systems mehrere Zusammenhänge auf verschiedenen Ebenen gleichzeitig auftreten. Damit gehen eine *gewisse Unvorhersehbarkeit* und Unsicherheit einher, die akzeptiert werden müssen. Weiterhin muss dabei stets eine Vielzahl von Perspektiven berücksichtigt werden.
5. Aktives Lernen
   Sozio-ökologische Systeme befinden sich in einem Zustand der ständigen, dynamischen Entwicklung. Daher besteht die Notwendigkeit, das *vorhandene, aber stets unvollständige und unsichere Wissen zu ergänzen* und ggf. auch zu revidieren.

Neben den bislang dargestellten positiven Resilienzaspekten werden im Klimaschutz auch wie soeben in Ziff. 3 angedeutet die *Grenzen der Resilienz* aufgezeigt, d.h. Kipppunkte bestimmter Parameter wie z.B. der CO_2-Konzentration, bei deren Erreichen nichtlineare, abrupte Umweltveränderungen auftreten, die das Leben auf der Erde für die Menschheit deutlich erschweren würden.[310] Insgesamt wird nach diesem sozio-ökologischen Resilienzverständnis somit anders als bei einer rein ökologischen Betrachtung und ähnlich der technischen Resilienz (dazu sogleich) ein erhaltenswerter

310 *Rockström et al.*, E&S, Vol. 14 (2009), Heft 2, S. 1 ff.

Zustand umschrieben, der sich in diesem Fall durch den Fortbestand der für den Menschen notwendigen Lebensgrundlagen auszeichnet.

c. Technische Resilienz

Im nachfolgenden wird das technische Verständnis von Resilienz behandelt. Da sich dieses Verständnis wesensmäßig von den Fragen der Psychologie oder der Ökologie unterscheidet, wird es in diesem Absatz als „dritte Strömung" zusammengefasst. Aufgrund der Nähe zur hier gegenständlichen, ebenfalls im Kern technischen „Sicherheit der Verarbeitung" fand hier eine besonders umfangreiche Erhebung statt. Sie wird weiter unterteilt in die Unterbereiche Material- und Ingenieurswissenschaft (i.), Informationstechnik (ii.) und den Schutz kritischer Infrastrukturen (iii.).

i. Material- und Ingenieurswissenschaft

In der Materialwissenschaft wird die Resilienz wie schon in der obigen Definition des Oxford-Lexikons aufgezeigt als Elastizität von Materialien wie z.B. Nylon verstanden. Wissenschaftlich formuliert beschreibt Resilienz demnach „die Fähigkeit eines Materials, sich durch Energieeinwirkung elastisch zu verformen. Das Maß für Resilienz ist hier die maximale Energie, die das Material pro Volumeneinheit aufnehmen kann, ohne sich permanent (also plastisch bzw. spröde) zu verformen"[311], d.h. unbeschadet zu bleiben.[312]

In der Ingenieurswissenschaft lässt sich die Resilienz komplexer Systeme implementieren bzw. erhöhen, indem man bereits bei der Entwicklung des Systems den möglichen Ausfall von einzelnen Systemkomponenten wie etwa Lüftern, Ventilen oder Rohren berücksichtigt und entsprechende Techniken etabliert, die eine minimale Funktionsfähigkeit des Systems trotz des Ausfalls beliebiger Komponenten garantieren und die Möglichkeit bietet, die Funktionalität im Nachhinein vollständig wiederherzustellen.[313]

311 *Scharte/K. Thoma*, in: Wink, Multidisziplinäre Perspektiven der Resilienzforschung, 82-98, S. 83.

312 *Fooken*, in: Wink, Multidisziplinäre Perspektiven der Resilienzforschung, 13 (24 f.); vgl. auch: *Sheridan*, Hum Factors 2008, 418 (423).

313 *Altherr et al.*, AMM, Vol. 885 (2018), 240 (242).

ii. Informationstechnik

In der Informationstechnik ist der Diskurs zur Resilienz gemessen an der Bedeutung des Begriffs in anderen Domänen bislang noch eher klein.[314] Überwiegend wird Resilienz hier als die Fähigkeit eines Informationssystems gesehen, Veränderungen in seiner externen Umgebung zu bewältigen.[315] Diese recht allgemeine Definition soll im Weiteren geschärft und dabei die unterschiedlichen Konnotationen der Resilienz in den Bereichen Verlässlichkeit (1) und IT-Sicherheit (2) berücksichtigt werden. Diese großen Bereiche gegenüberstellend und zusätzlich die Bereiche Netzwerktechnik und Software-Entwicklung berücksichtigend wird unter (3) ein abschließendes Fazit für den Bereich der Informationstechnik gebildet.

(1) Verlässlichkeit

In der Forschung der Verlässlichkeit von informationstechnischen Systemen meint *Verlässlichkeit* (en: Dependability)[316] selbst zunächst die Fähigkeit eines Systems einen berechtigt vertrauenswürdigen Dienst anzubieten; ein berechtigt vertrauenswürdiger Dienst liegt wiederrum dann vor, wenn Ausfälle desselben nicht über ein akzeptables Maß an Häufigkeit und Schwere hinaus gehen.[317]

Die Resilienz wurde hier von *Avizienis/Laprie* als ein Synonym für Fehlertoleranz (en: Fault Tolerance) verstanden.[318] Dem Konzept der Fehlertoleranz liegt eine im Englischen sprachlich ausdifferenzierte Fehlerkette zugrunde, die nachfolgend illustriert wird.[319]

314 *Heeks/Ospina*, ISJ (Information Systems Journal) 2019, 70 (71 ff.)
315 Wie zuvor.
316 Ebenso übersetzend und kritisch zur Übersetzung als „Zuverlässigkeit": *Pfitzmann*, DuD 1993, 539 (540).
317 Das Erfordernis der Vertrauenswürdigkeit ergibt sich aus der Abhängigkeit von einem System, d.h. aufgrund der Abhängigkeit von einem System bzw. einem Dienst muss auf dessen Verlässlichkeit vertraut werden (können); *Avizienis et al.*, IEEE TDSC 2004, 11 (13, 22)
318 *Avizienis et al.*, IEEE TDSC 2004, 11 (14, 27).
319 *Avizienis et al.*, IEEE TDSC 2004, 11 (15 ff.); *B. Randell/P. Lee/Treleaven*, ACM CSUR 1978, 123 (125 f.); *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (8 f.); in der Netzwerktechnik auch: *Sterbenz et al.*, Computer Networks 2010, 1245 (1246).

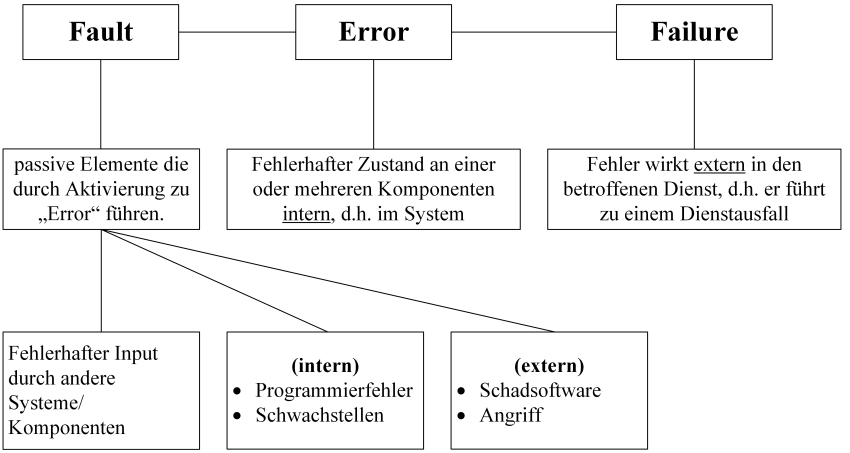

Abbildung 6: Fehlerkette in der Verlässlichkeit

Die Fehlertoleranz wird definiert als das Vermeiden eines Dienstausfalls (en: Service Failure) angesichts von Fehlern (en: Faults).[320] Ein Dienstausfall liegt vor, wenn der tatsächlich erbrachte Dienst von dem korrekten Dienst abweicht, d.h. die entsprechende Systemfunktion nicht erfüllt wird.[321]

Sie umfasst hierfür zunächst die Erkennung des fehlerhaften Zustands (en: Error detection) sowie die anschließende Wiederherstellung (en: Recovery).[322] Letztere bezieht sich sowohl auf die Beseitigung des fehlerhaften Zustands (en: Error Handling) als auch auf die Beseitigung bzw. das dauerhafte Verhindern der Reaktivierung der diesen Zustand auslösenden Elemente (Fault Handling).[323] Entsprechend o.g. Definition soll somit durch die Fehlertoleranz das Versagen des Dienstes und im Ergebnis eine Beeinträchtigung der Verlässlichkeit vermieden werden.[324]

320 *Avizienis et al.*, IEEE TDSC 2004, 11 (14).
321 Dies schließt sowohl die vollständig als auch teilweise fehlende, zeitliche Verfügbarkeit des Dienstes als auch die die inhaltlich fehlerhafte Diensterbringung ein: *Avizienis et al.*, IEEE TDSC 2004, 11 (13, 18 f.).
322 *Avizienis et al.*, IEEE TDSC 2004, 11 (24 ff.).
323 Wie zuvor.
324 *Avizienis et al.*, IEEE TDSC 2004, 11 (14).

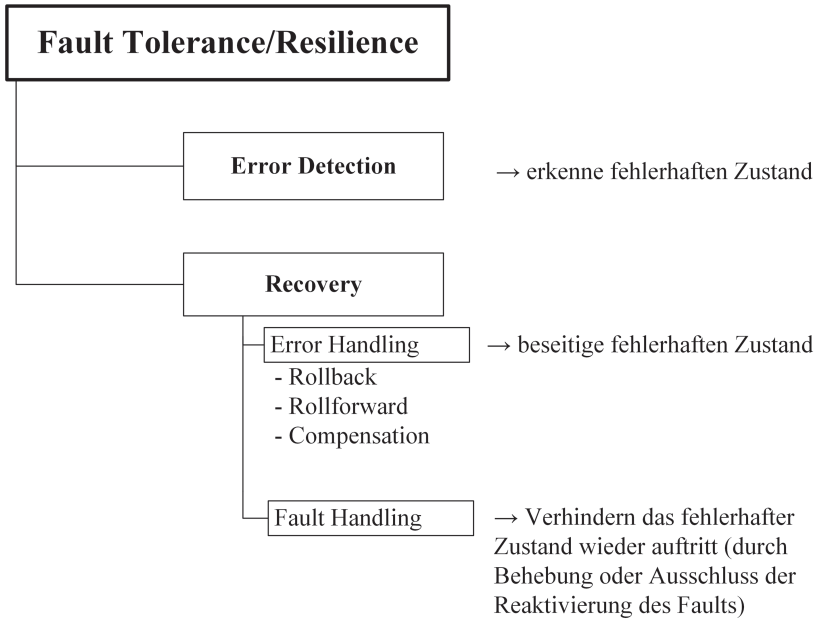

Abbildung 7: Fault Tolerance/Resilience

In dieser Methodik ist besonders das reaktive Element der Resilienz erkennbar: Falls ein fehlerhafter Zustand eingetreten ist, soll dieser erkannt und sodann beseitigt werden. An Beseitigungsmethoden[325] steht zunächst der sog. Rollback zur Verfügung, d.h. das System wird in einen vorherigen, fehlerfreien Zustand zurückversetzt. Beim Rollforward hingegen wird ein neuer, fehlerfreier Zustand hergestellt. Schließlich besteht die Möglichkeit der Kompensation, d.h. der fehlerhafte Zustand wird durch den Einsatz von Redundanzen gewissermaßen „maskiert", so dass er sich nicht mehr als Dienstausfall auswirkt.

Später wurde Resilienz von *Laprie* mit Blick auf die Verlässlichkeit umfassender definiert als „die Beständigkeit von Verlässlichkeit bei Veränderungen.[326] Damit bezieht sich die Resilienz nicht nur auf die Fehlertoleranz,

325 *Avizienis et al.*, IEEE TDSC 2004, 11 (25).

326 En: "Resilience is defined as the persistence of dependability when facing changes"; *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9. *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (13).

sondern auch auf die Fehlerprävention, die (nicht akute) Fehlerentfernung und die Fehlervorhersage.[327] Diese Verschiebung des Fokus‘ auf Veränderungen war und ist demnach geboten, da die modernen großen und vernetzten Informationsinfrastrukturen als ubiquitäre Systeme ständig mit Veränderungen, insbesondere hinsichtlich der Bedrohungslage, konfrontiert sind. Um Resilienz zu gewährleisten, müssen sich Systeme somit insbesondere an diese Veränderungen anpassen können (en: evolvability);[328] die Veränderungen lassen sich dabei in funktionale und strukturelle Veränderungen unterteilen. Funktionale Veränderungen meinen in diesem Kontext veränderte Anforderungen der Nutzer:innen an das System.[329] Dagegen beziehen sich strukturelle Veränderungen auf die eingesetzte Technologie und die Umwelt, z.B. ein Fehler in einer Komponente oder auch eine veränderte Bedrohungslage durch Angreifer:innen.[330] Diese Veränderungen, gegen die das informationstechnische System resilient sein soll, können dabei insbesondere auch unvorhergesehen auftreten.[331]

Neben den zuvor dargestellten Anpassungen im Rahmen der *Fault Tolerance* einschließlich der Wiederherstellung haben andere Forschende auch weitere Resilienzaspekte entwickelt, etwa die maßvolle Degradation, d.h. dass ein Dienstlevel reduziert wird, ohne einen kompletten Ausfall zuzulassen (z.B. ein geringerer Funktionsumfang).[332] Soweit die entsprechenden Anpassungen von den informationstechnischen Systemen autonom erfolgen, wird auch von „selbst-adaptiven Systemen“ gesprochen.[333] Als

327 *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9; ausführlich zu diesen Begriffen: *Avizienis et al.*, IEEE TDSC 2004, 11 (24 ff.)

328 *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9.

329 Z.b. gestiegene Lastanforderungen: *Laprie*, in: Fourth IEEE International Symposium on Network Computing and Applications, Resilience for the Scalability of Dependability, 5 (5); *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (15); zum holistischen Verständnis von „Funktion“ (d.h. nicht nur wie hier Nutzeranforderungen, sondern auch Sicherheitsanforderungen) in dieser Untersuchung: S. 202.

330 Wie zuvor.

331 *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9; *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (11); *Cámara et al.*, Computing 2013, 689 (689).

332 *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (16).

333 *Cámara et al.*, Computing 2013, 689 (690).

weitere Aspekte der Resilienz neben den skizzierten Kernelementen werden auch genannt:[334] Erstens die Bewertbarkeit in Bezug auf die Effektivität der Resilienz. Zweitens die Nutzbarkeit von Resilienztechniken sowohl für Administrator:innen als auch mit Blick auf die Anforderungen der Nutzer:innen. Und schließlich die Diversität des Systems, um sog. Single Points of Failure (SPOF) zu vermeiden, d.h. dass ein singuläres Ereignis alle (redundant vorgehaltenen) Komponenten gleichermaßen betrifft.

(2) IT-Sicherheit

Ob und inwieweit die o.g. Verlässlichkeit auch die IT-Sicherheit bereits mit einschließt, ist zweifelhaft. IT-Sicherheit lässt sich als der Schutz eines informationstechnischen Systems vor unautorisierten Eingriffen verstehen.[335] Dabei sind die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen[336] und Informationstechnik[337] angesichts solcher Eingriffe zu wahren.

Auch bei *Avizienis/Laprie et al.* wurde die IT-Sicherheit im Rahmen der Verlässlichkeit nicht von Anfang an berücksichtigt, sondern erst zu einem späteren Zeitpunkt einbezogen[338] und auch die Fehlertoleranz bzw. Resilienz wie oben dargestellt hierauf erstreckt.[339] Diese Integration der IT-Sicherheit in die Verlässlichkeit wird teilweise insbesondere mit Blick auf die sehr unterschiedlichen Terminologien kritisch gesehen.[340]

334 *Laprie*, in: 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), From Dependability to Resilience, G8-G9.

335 Vgl. *Eckert*, IT-Sicherheit, S. 6; *Avizienis/Laprie/Randell,* Fundamental Concepts of Dependability, 2001, S. 3; *L. Fischer/Lehnhoff*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 316 (318).

336 DIN, ISO/IEC 27000:2017, S. 12, Ziff. 2.33 (Definition: Informationssicherheit); BSI, IT-Grundschutz-Kompendium, 2023, Glossar, S. 3.

337 *Solms/van Niekerk*, Computers & Security, Vol. 38 (2013), 97 (98); *Whitman/Mattord*, Principles of Information Security, S. 8.

338 Folglich wurden in der sehr weiten Definition des Fehlers (fault) sowohl intern als auch extern ausgelöste sowie fahrlässige ebenso wie absichtlich, böswillig ausgelöste Fehler umfasst; *Avizienis et al.*, IEEE TDSC 2004, 11 (15); Ähnlich zur Resilienz als Eigenschaft sowohl für Verlässlichkeit als auch IT-Sicherheit: *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (8).

339 Wohl zustimmend, da auch auf „Angriffe" abstellend: *W. J. Zhang/Lin*, Enterprise Information Systems, Vol. 4 (2010), Heft 2, 99 (102).

340 Mit einem alternativen Vorschlag zur Integration: *Jonsson/Olovsson*, in: Pham/Hamza, Proceedings of the IASTED International Conference on Reliability, Quality Control and Risk Assessment, 93 (93 ff.).

Jedenfalls hat die IT-Sicherheit auch eine eigene historische Entwicklung hinter sich, die sich zumeist auch unabhängig von der Verlässlichkeit vollzog.[341] Auch hier wurde die Resilienz als wichtiges Merkmal erkannt und definiert. Dabei wird sie mitunter auch ausdrücklich neben den klassischen Schutzzielen genannt.[342] Für die Bestimmung der Resilienz ist demnach im Ausgangspunkt anzuerkennen, dass *Bedrohungssituationen unvermeidbar sind*, ständig wiederkehren und es dabei auch zumindest zu partiellen Fehlfunktionen der Verteidigung kommen wird. Dies ist insbesondere auf eine starke Ungewissheit bezüglich der drohenden Ereignisse zurückzuführen, da sich die Angriffsformen schnell weiterentwickeln.[343] Im Falle eines solchen unvorhergesehenen, durchbrechenden Angriffs müsse es das Ziel sein, „Ressourcen und [auszuführende] Operationen zu priorisieren, besonders wichtige Schlüsselwerte und Systeme vor den Angriffen zu beschützen und am Ende einen normalen operativen Zustand wiederherstellen zu können".[344] Dazu gehört *auch die soziotechnische Komponente*, also die Mitarbeitenden, einzubeziehen.[345]

Zur Resilienz in der IT-Sicherheit gehören laut *Singer/Friedman* im Ergebnis drei Elemente:[346] Das erste Element ist die Fähigkeit [durch flexible Anpassung] die beabsichtigte Leistungsfähigkeit auch unter verschlechterten Bedingungen (Ereignis) erbringen zu können.[347] Dazu muss indes auch (vorgelagert) die Erkennung dieses Ereignisses gehören, da andernfalls eine Anpassung nicht möglich ist. Zweitens muss schnellstmöglich die schon angesprochene Wiederherstellung stattfinden. Und drittens muss aus den Ereignissen gelernt werden, um in Zukunft besser mit Angriffen umgehen zu können.

341 *Avizienis et al.*, IEEE TDSC 2004, 11 (22); grundlegend zur Information Security: *Saltzer/Schroeder*, Proc. IEEE 1975, 1278 (1278 ff.).
342 *Singer/Friedman*, Cybersecurity and cyberwar, S. 36.
343 *Collier et al.*, Computer 2014, 70 (70); *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (2).
344 *Singer/Friedman*, Cybersecurity and cyberwar, S. 35.
345 *Collier et al.*, Computer 2014, 70 (75); *Singer/Friedman*, Cybersecurity and cyberwar, S. 171.
346 *Singer/Friedman*, Cybersecurity and cyberwar, S. 170 f.; ähnlich auch: "ability of the system to prepare, absorb, recover and adapt to adverse effects": *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (12).
347 Vgl. *Alt*, Die Sachverständigen 2020, 169 (170).

(3) Weitere Teilbereiche und Fazit

Ob Resilienz im Kontext der spezifischen IT-Sicherheit begrifflich anders verstanden werden muss als im klassischen Bereich der Verlässlichkeit, ist zweifelhaft. Methodisch zeigen sich zumindest starke Überschneidungen wie die Erkennung des fehlerhaften Zustands sowie die anschließende Behebung bzw. Abwehr desselben. Danach soll in beiden Fällen aus dem Ereignis „gelernt" werden, indem die auslösenden Elemente dauerhaft deaktiviert bzw. die entsprechenden Angriffspfade geschlossen werden.

Auf sachlicher Ebene können sich indes Unterschiede ergeben, insbesondere bei der Betrachtung von typischerweise in der Verlässlichkeit adressierten, fahrlässig oder zufällig ausgelösten Ereignissen einerseits und andererseits die für die IT-Sicherheit prägenden, absichtlich agierenden Akteure, was zu unterschiedlichen Ausgestaltungsanforderungen führen kann:[348] Soweit es z.B. bei zufälligen Fehlern wie etwa Hardware-Defekten oder Naturkatastrophen zu Ausfällen kommen kann, reicht zur Herstellung der Resilienz im Sinne der Verlässlichkeit unter Umständen bereits eine bloße Redundanz der jeweiligen Komponenten oder Systeme. Ein(e) Angreifer:in, welche(r) diese Struktur kennt, könnte dann aber mit nur einer Schadsoftware die identischen, redundanten Systeme und Komponenten ausschalten und so diese Backup-Sicherung leicht überwinden.[349] Somit sind für die Resilienz in der IT-Sicherheit zumindest eine heterogene Redundanz[350] (Diversität) oder sogar gänzlich andere Resilienzmechanismen erforderlich. Für die abstrakte begriffliche Bestimmung der Resilienz im vorliegenden Kontext erscheinen aber sowohl das Verständnis der IT-Sicherheit als auch der Verlässlichkeit zumindest als Ausgangsbasis nutzbar.

Neben den bereits genannten großen Strömungen der Verlässlichkeit und der IT-Sicherheit sind noch zwei konkretere Teilbereiche zu nennen, die bezüglich der Resilienz im Bereich der Informationstechnik Hinweise geben können:

Zum einen die Netzwerktechnik[351], in der Resilienz v.a. die Fähigkeit betrifft mit stark schwankenden Lasten umgehen zu können. Eine hohe Last-

348 *Singer/Friedman*, Cybersecurity and cyberwar, S. 171.

349 *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (13); *Singer/Friedman*, Cybersecurity and cyberwar, S. 170.

350 *L. Fischer/Lehnhoff*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 316 (337).

351 Vgl. *L. Xie et al.*, in: Hutchison/Denazis/Lefevre/Minden, Active and Programmable Networks, 83 (83 f.).

phase kann einerseits durch sog. flash crowd events, also einem plötzlichen Anstieg legitimen Datenverkehrs (en: Traffic) entstehen,[352] z.B. eine hohe Last auf den Servern, die VoIP-Dienste anbieten, infolge der Ausgangsbeschränkungen im Rahmen der Corona-Krise. Andererseits kann eine solche Lastphase auch böswillig durch sog. DDoS-Angriffe ausgelöst werden, bei denen ein Botnetz unerwünschten Traffic in Form von „sinnlosen" Anfragen durchführt, mit dem expliziten Ziel die Server und Netzwerke zu überlasten.[353] Mitunter sind ausgeklügelte DDoS-Angriffe aber gar nicht ohne Weiteres von legitimem Datenverkehr zu unterscheiden.[354] Folglich muss „Resilienz" hier sowohl auf angriffsbedingte als auch auf an sich legitime Lastspitzen eine Antwort bieten. Gleiches gilt generell bei lokalen Ausfällen von Knotenpunkten in einem Netzwerk, bei denen es ebenfalls nicht darauf ankommt, ob dies durch einen Angriff oder einen Fehler geschieht.[355] Ein resilientes Netzwerk bietet und erhält trotz solcher Einwirkungen zumindest noch ein „akzeptables Dienstniveau".[356]

In der Softwareentwicklung kann man auch von „Resilient Software Development" sprechen, wobei Software-Resilienz ganz ähnlich, wenn auch detaillierter definiert wird als „die Fähigkeit, das Ausmaß und/oder die Dauer von Störungsereignissen zu reduzieren. Die Effektivität einer resilienten Anwendungs- oder Infrastruktursoftware hängt von ihrer Fähigkeit ab, ein potenziell störendes Ereignis zu erkennen, zu absorbieren, sich anzupassen und/oder sich schnell davon zu erholen."[357]

Insgesamt bleibt festzuhalten, dass die Resilienz in der Informationstechnik die Reaktion auf verschiedene Ereignisse wie Angriffe, fehlerhafte Systemzustände, Lastspitzen in Netzwerken oder Programmstörungen beschreibt. Dabei soll das in Rede stehende Ereignis zunächst in einer akuten

352 Vgl. *Andersson et al.*, in: Calinescu/Di Giandomenico, Software Engineering for Resilient Systems, 11 (13).

353 *R. Grimm/Waidner*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 33 (44, 49), Rn. 44, 73 ff.; *LG Düsseldorf*, Urt. v. 22.03.2011 – 3 KLs 1/11, MMR 2011, 624 (624), mit Anmerkung *Bär*, S. 625 f.

354 Vgl. *Eckert*, IT-Sicherheit, S. 12.

355 *Bishop et al.*, in: Proceedings of the 2011 workshop on New security paradigms workshop (NSPW), Resilience is more than availability, 95 (95).

356 *L. Xie et al.*, in: Hutchison/Denazis/Lefevre/Minden, Active and Programmable Networks, 83 (84). *Sterbenz et al.*, Computer Networks 2010, 1245 (1246).

357 Englisches Original: "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient application or infrastructure software depends on its ability to anticipate, absorb, adapt do and/or recover rapidly from a potentially disruptive event." In: *Merkow/Raghavan*, Secure and resilient software, S. 1 f.

Phase erkannt und bewältigt werden, um eine Beeinträchtigung des jeweiligen Dienstes möglichst zu verhindern oder andernfalls die Funktionsfähigkeit des Dienstes schnellstmöglich wiederherzustellen. Außerdem soll eine Reaktivierung der Elemente, die das Ereignis ausgelöst haben für die Zukunft möglichst ausgeschlossen werden.

Ungeachtet dessen, dass sich fahrlässige und zufällige Ereignisse, wie sie tradiert von der Verlässlichkeit erfasst werden, einerseits und vorsätzliche Sicherheits-Ereignisse andererseits, oft ohnehin nicht unterscheiden lassen (wie etwa in der Netzwerktechnik), so ist eine Differenzierung auf definitorischer Ebene der Resilienz jedenfalls auch nicht erforderlich. Allein auf der Maßnahmenseite können sich insoweit Unterschiede ergeben.

iii. Kritische Infrastrukturen

Einen weiteren Referenzbereich für die technische Resilienz bilden die kritischen Infrastrukturen. Kritische Infrastrukturen sind „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 eintreten würden."[358] Im RegE BSIG wird nun in § 2 Nr. 22 stattdessen der Begriff „kritische Anlagen" verwendet.[359] Erfasst werden u.a. Einrichtungen aus den Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation.

In der bereits untersuchten Informationstechnik steht die Resilienz von IT-Systemen im Fokus. Der Resilienzbegriff geht im Bereich kritischer Infrastrukturen notwendigerweise noch darüber hinaus, da etwa bei Energieerzeugungsanlagen eingebettete IT-Systeme (Embedded Systems) vorliegen, die mit den übrigen Bestandteilen ein *cyber-physisches sowie ein soziotechnisches Gesamtsystem* bilden.[360] Kernziel der Resilienz ist hier, dass die von der kritischen Infrastruktur erbrachte Dienstleistung nicht unterbrochen wird.

358 BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen, 2009, S. 3.

359 *Kipker/Dittrich*, MMR 2023, 481 (481 f.).

360 Vgl. *Alsubaie/Alutaibi/Martí*, in: Rome/Theocharidou/Wolthusen, Critical Information Infrastructures Security, 43 (50); *Gazos*, in: Polarisierte Welten: Verhandlungen des 41. Kongresses der Deutschen Gesellschaft für Soziologie, Die soziomaterielle Konstitution von Cybersicherheit in der Dynamik kritischer Informationsinfrastrukturen, S. 1, 3.

Dieses Ziel ist weiter gefasst als das Verständnis der Informationstechnik, soweit diese nur auf die Funktionalität der IT-Systeme abstellt. Durch die Einbettung sind die IT-Systeme nicht mehr isoliert, sondern im Kontext des Gesamtsystems zu betrachten, etwa bei der Frage wie ein IT-System bei Ausfall einer physischen Komponente reagiert. Umgekehrt kann ein defekter Steuerungsdienst in einem Kraftwerk den Generator schädigen und so einen Abbruch der Stromerzeugung herbeiführen. Auch die soziale Komponente (mithin das Personal) ist bei kritischen Infrastrukturen ergänzend zu berücksichtigen, hier jedoch nicht nur bezüglich der Informationstechnik, sondern bezüglich des ganzen cyber-physischen Systems.

In der wissenschaftlichen Literatur[361] lässt sich zwar keine feststehende Definition, aber zumindest ein grober Konsens dahingehend feststellen, dass unter Resilienz die Fähigkeit eines Systems verstanden werden kann, „internen/externen Belastungen standzuhalten und sich von ihnen zu erholen."[362] Das Ziel der Resilienz liegt somit in der Gewährleistung einer möglichst kontinuierlichen bzw. schnell wiederherstellbaren Funktionalität[363] dieses Gesamtsystems angesichts solcher Belastungen.

d. Gesellschaftliche Resilienz / Katastrophenschutz

Die gesellschaftliche oder auch „soziale Resilienz"[364] ist vor allem mit Blick auf zwei Kategorien von Ereignissen bedeutsam: Einerseits schleichende, längerfristige Ereignisse bzw. Veränderungen wie z.B. der Klimawandel und andererseits abrupte Störereignisse in Gestalt von Katastrophen.[365]

Aufgrund der höheren Vergleichbarkeit mit Daten- und IT-Sicherheitsvorfällen wird nachfolgend nur auf letzteres eingegangen. Unter Katastrophenschutz werden somit im hiesigen Kontext alle Maßnahmen verstanden, die (ggf. schon vorher vorbereitet) auf den Eintritt einer Katastro-

361 Eine exemplarische Übersicht findet sich bei: *Alsubaie/Alutaibi/Martí*, in: Rome/Theocharidou/Wolthusen, Critical Information Infrastructures Security, 43 (45).

362 *Y. Fang/Zio*, in: Gritzalis/Theocharidou/Stergiopoulos, Critical Infrastructure Security and Resilience, 97 (98 f.) m.w.N.

363 Ebd.

364 Definiert als „Widerständigkeit sozialer Gemeinschaften": *Bonß*, in: Endreß/Maurer, Resilienz im Sozialen, 15 (26).

365 Wie zuvor; Vgl. OECD, Concepts and dilemmas of State building in fragile situations, 2009, S. 17.

phe[366] reagieren und versuchen diese zu bewältigen. Insofern ist er dem (technischen) IT-Sicherheitsrecht ereignis-chronologisch nachgelagert, etwa wenn die Katastrophe in Form eines großflächigen Stromausfalls infolge des Versagens ein oder mehrerer kritischer Energieerzeugungsanlagen vorliegt.[367]

Da Katastrophen trotz aller Bemühungen nicht immer vorherhergesehen und damit auch nicht durch „planende Vorausschau" verhindert werden können,[368] kommt der Resilienz mit ihren Aspekten der Anpassung während der Katastrophe bzw. der Regeneration nach einer solchen eine besondere Bedeutung zu.[369] Dementsprechend lässt sich als Kerngedanke hier „die Möglichkeit, mit negativen Folgen von Ereignissen durch unterschiedlichste Strategien fertigzuwerden"[370] identifizieren. Dass der Resilienz in diesem Sinne heute große Bedeutung zukommt ist auch Ausdruck einer Verlagerung, mit der der Fokus sich nicht mehr nur auf die präventive Reduktion der Verletzlichkeit (auch Resistenz genannt)[371] beschränkt, sondern insbesondere auch darauf bezogen wird, eine starke Resilienz im Katastrophenfall zu gewährleisten.[372]

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) definiert Resilienz noch recht abstrakt als „Fähigkeit eines Systems, Ereignissen zu widerstehen bzw. sich daran anzupassen und dabei seine Funktionsfähigkeit zu erhalten oder möglichst schnell wieder zu erlangen".[373] Das *USA National Research Council* ist in seiner Definition hingegen deutlich detaillierter: „Die Fähigkeit, widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen." Auch das *United Nations Office for Disaster Risk Reduction (UNDRR)* verfolgt einen solch umfassenden Ansatz, indem es Resilienz definiert als die „Fähigkeit eines Systems, einer Gemeinschaft oder Gesellschaft, die Gefahren ausgesetzt ist, den

366 BBK, Online-Glossar des BBK, 2024, Definition Katastrophe.
367 Dies gilt umgekehrt aber nicht für Katastrophen, die etwa durch Naturereignisse ausgelöst werden.
368 *Würtenberger*, in: Baumeister, Staat, Verwaltung und Rechtsschutz, 561 (564).
369 Vgl. *Bonß*, in: Endreß/Maurer, Resilienz im Sozialen, 15 (19f.); ähnlich auch: *Häfele/Renn/Erdmann*, in: Häfele, Energiesysteme im Übergang, 375 (408).
370 *Krüger/Max*, Resilienz im Katastrophenfall, S. 31.
371 *Longstaff*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 259 (263 ff.).
372 *Korff*, in: Lewinski, Resilienz des Rechts, 23 (23).
373 BBK, Online-Glossar des BBK, 2024, Definition Resilienz.

Auswirkungen einer Gefahr rechtzeitig und effizient zu widerstehen, sie zu absorbieren, sie aufzunehmen, sich an sie anzupassen, sie zu transformieren und sich von ihnen zu erholen, auch durch die Erhaltung und Wiederherstellung ihrer wesentlichen Grundstrukturen und -funktionen durch Risikomanagement."[374]

Spezifischer auf die Fragen sozialer Aspekte bei Katastrophen lässt sich auch die soziale Resilienz in drei inzwischen bereits vertraut erscheinende Aspekte unterteilen:[375] Als erstes die Fähigkeit der Gesellschaft eine Katastrophe durch Anpassung einzudämmen und sie durch flexible Reaktion zu ertragen. Zweitens sich von einem durch die Katastrophe ausgelösten Tiefpunkt der Funktionalität der Gesellschaft wieder zu erholen. Und schließlich aus der Katastrophe und den Konsequenzen in konstruktiver Weise zu lernen um künftig (noch) resilienter zu werden.[376] Als wesentliche (positive) Resilienzfaktoren werden insoweit ein starkes Zusammengehörigkeitsgefühl der Gesellschaft, eine gemeinsame Weltanschauung, vertrauensgetragene Führung sowie ziviles Engagement und aktive Öffentlichkeitsbeteiligung genannt.[377]

Zunehmend verbreitet sind auch sehr übergreifende Ansätze, eine Nation bzw. eine Gesellschaft als Gesamtsystem möglichst resilient zu gestalten, indem sie (präventiv) so gestaltet wird, dass menschliche, ökonomische und ökologische Schäden durch widrige Ereignisse bestmöglich vermieden werden können.[378]

374 UNDRR (vormals: UNISDR), https://www.undrr.org/terminology/resilience, zuletzt abgerufen am 12.04.2024.

375 *Elran*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 291 (294 f.).

376 Siehe hierzu auch *Berkes*, Nat Hazards, Vol. 41 (2007), 283 (287).

377 *Elran*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 291 (295 f.).

378 *Cutter et al.*, Environment: Science and Policy for Sustainable Development 2013, 25; ähnlich auch: Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022, 08.12.2017, S. 516, Kap. 6.2; vgl. auch: OECD, Concepts and dilemmas of State building in fragile situations, 2009, S. 17 f, wobei der resiliente Staat hier als positiver Gegenpol zum fragilen Staat angesehen und sich vor allem durch einen funktionierenden Gesellschaftsvertrag (en: social contract) zwischen Staat und Gesellschaft auszeichnet. Letzteres wird insbesondere dann angenommen, wenn der Staat in der Lage ist die gesellschaftlichen Erwartungen an ihn zu erfüllen.

e. IT-Sicherheitsrecht

Im Nachfolgenden soll auf Anforderungen aus dem IT-Sicherheitsrecht i.w.S. eingegangen werden. Dabei wird zunächst eine allgemeine Einführung mit der Verwendung des Resilienzbegriffs nicht nur in europäischen Gesetzen, sondern insbesondere auch bereits zuvor in Politikansätzen und Strategien der EU-Kommission gegeben (i.). Anschließend wird konkret auf die (sofern vorhandenen) Definitionen der Resilienz im (RegE) BSIG und der NIS(2)-RL, dem RefE KRITIS-DachG, dem IT-Sicherheitsgesetz für Banken: DORA[379] und dem die Agentur der EU für Cybersicherhit (ENISA) einrichtenden CSA[380] eingegangen (ii-v). Schließlich folgt noch ein internationaler Blick auf die Definitionen in (IT-)Sicherheitsstrategien aus der Schweiz und den USA (vi.-vii.).

i. Einführung

Der Begriff der Resilienz ist zumindest im europäischen Kontext der IT-Sicherheit an sich nicht unbekannt. Bereits seit 2007 wird der Begriff „Resilienz" von der EU-Kommission in diesem Kontext regelmäßig verwendet.[381] Die Tätigkeit der EU-Kommission in dem Bereich der europäischen IT-Sicherheit lässt sich schon auf das Jahr 2001 zurückführen,[382] in der die Europäische Kommission einen Vorschlag für einen europäischen Politikansatz im Bereich der Sicherheit der Netz- und Informationssysteme einbrachte.[383] Das Ziel der „Erhöhung der Sicherheit und der Widerstandsfähigkeit" (en: resilience) wurde dann 2006 mit der Strategie für eine sichere Informationsgesellschaft noch wenig prominent eingeführt.[384] Die darauf folgende, stärkere Positionierung des Resilienzbegriffs wird u.a. auf die Cyber-Angriffe in Estland 2007 zurückgeführt, die gewissermaßen zu einem Weckruf in der EU geführt haben.[385] Denn an diesem jenseits der finanziellen Schä-

379 EU-VO 2022/2554, Digital Operational Resilience Act.
380 EU-VO 2019/881, Cyber Security Act, Cybersecurity Act.
381 *Dewar*, The European Union and Cybersecurity, S. 173.
382 *Dewar/Dunn Cavelty*, in: Schünemann/Kneuer, E-Government und Netzpolitik im europäischen Vergleich, 281 (283).
383 EU-Kommission, KOM (2001) 298 endgültig, 06.06.2001.
384 EU-Kommission, KOM(2006) 251 endgültig, 31.05.2006, S. 7; s. auch Entschließung d. europäischen Rates, EU-ABl. 2007 C 68/3.
385 *Dewar*, The European Union and Cybersecurity, S. 166 ff.

den[386] an sich nicht sehr folgenschweren Angriff zeigte sich exemplarisch die immer stärker werdende Abhängigkeit von Netz- und Informationssystemen und zwar sowohl mit Blick darauf, dass die Auswirkungen eines Ausfalls mit der wachsenden Zahl der digitalisierten Lebensbereiche immer größer werden, als auch, dass aufgrund der technischen Interdependenz entsprechende Ausfälle in einzelnen Mitgliedsstaaten potenziell kaskadenartige Ausfälle in ganz Europa auslösen können.[387]

Zum Schutz des europäischen Binnenmarktes[388] sollten die entsprechenden Infrastrukturen in Anbetracht solcher Ereignisse daher möglichst resilient ausgestaltet sein. Ausdrücklich definiert wird „Resilienz" in diesem Zusammenhang jedoch nicht. Zumindest Anhaltspunkte liefert die Cybersecurity-Strategie 2013, die der „Cyber Resilience" einen eigenen Abschnitt widmet:[389] Demnach kann diese insbesondere dazu dienen, „grenzübergreifende Risiken und Bedrohungen einzudämmen und in Notfällen auf koordinierte Weise zu reagieren." Besonders hervorgehoben werden mit Blick auf Sicherheitsvorfälle koordinierte Prozesse zur „Prävention, Erkennung, Folgenminderung und Reaktion", einschließlich der Ermöglichung eines europaweiten Informationsaustauschs. Auch der private Sektor selbst sollte seine Resilienz gegenüber Cyberangriffen stärken. In diesem Zusammenhang wird die „Reaktion auf Sicherheitsvorfälle, die Ermittlung der Ursachen und die Durchführung [retrospektiver] cyberforensischer Untersuchungen" genannt. Im Kontext der Cyberverteidigungspolitik wird die Resilienz von Kommunikations- und Informationssystemen in diesem Dokument außerdem mit der „Erkennung komplexer Cyberbedrohungen, der Reaktion darauf und der Wiederherstellung danach" assoziiert.[390]

An diesem Punkt lässt sich bereits festhalten, dass Resilienz Bewältigungsmethoden für Sicherheitsvorfälle umschreibt: Hierzu können insbesondere deren möglichst frühzeitige Erkennung, die Reaktion während des Vorfalls sowie die Minimierung der Folgen bzw. die Wiederherstellung

386 *M. Schmidt*, Cyberkrieg gegen Estland macht Westen ratlos, Tagesspiegel vom 30.05.2007 in: Tagesspiegel, 30.05.2007.

387 *Dewar*, The European Union and Cybersecurity, S. 172.

388 Für den Bereich der nationalen Sicherheit, zu der man diese Frage sicherlich auch zählen könnte, fehlte der EU die Kompetenz; der EU-Cybersicherheit liegt daher ein sozio-ökonomisches Verständnis mit Fokus auf den Schutz der europäischen Wirtschaft zugrunde. s. *Dewar*, The European Union and Cybersecurity, S. 175 ff.

389 EU-Kommission, JOIN(2013) 1 final, 07.02.2013, Kap. 2.1, S. 5 ff; in der deutschen Fassung: „Widerstandsfähigkeit".

390 EU-Kommission, JOIN(2013) 1 final, 07.02.2013, Kap. 2.3, S. 13; in der deutschen Fassung: „Robustheit".

gezählt werden. Ein hoher Stellenwert wird dabei auch organisatorischen Aspekten wie der Zusammenarbeit der beteiligten Akteure zur Vermeidung der Ausbreitung von Sicherheitsvorfällen eingeräumt, so dass der Begriff auf das soziotechnische Gesamtsystem abzielt und nicht auf (einzelne) IT-Systeme beschränkt bleibt.

ii. RegE BSIG und NIS2-RL

Im deutschen IT-Sicherheitsrecht, insbesondere in § 30 RegE BSIG (wie auch dem damit umgesetzten Art. 21 NIS2-RL) ist das Erfordernis der Resilienz noch nicht eingeführt. Gleiches gilt für die Sicherheitsdefinitionen nach § 2 Nr. 36 RegE BSIG, Art. 6 Nr. 1 NIS2-RL.

Allerdings finden sich einige Erwähnungen der Resilienz: So findet sich z.B. in § 51 RegE BSIG die aus Art. 28 der NIS2-RL übernommene Vorgabe: „Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domain Name Systems zu leisten, sind Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister verpflichtet, genaue und vollständige Domain-Namen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt zu sammeln und zu pflegen."

Daneben findet sich v.a. in der NIS2-RL noch eine Vielzahl weiterer Erwähnungen, allerdings ohne ein definiertes Begriffsverständnis zu ermöglichen: So würde etwa die Schwachstellendatenbank der ENISA die Resilienz erhöhen (EG 63), die Resilienz der Lieferkette von IKT-Diensten, -Systemen und -Produkten müsse sichergestellt werden (EG 91) und Meldungen über Vorfälle müssten hinreichend detailliert sein, damit andere Einrichtungen daraus wichtige Lehren ziehen und ihre Resilienz erhöhen könnten (EG 101).[391]

Diese inhaltlich wenig detaillierte Verwendung des Resilienzbegriffs in der NIS2-RL überrascht insoweit besonders, da laut EG 2 derselben seit Inkrafttreten der NIS-RL „erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden."

391 Weitere Erwähnungen finden sich in EG 2, 5, 55, 85, 100, 109 sowie Art. 7 Abs. 2 lit i) NIS2-RL. Auch in der NIS-RL wurde die Resilienz bereits in EG 13 und Art. 9 Abs. 3 genannt; im BSIG hingegen bislang nicht.

iii. RefE KRITIS-DachG

Weiterhin ist der Referentenentwurf des KRITIS-DachG, mit dem die europäische RL 2022/2557 über die „Resilienz kritischer Einrichtungen" (RKE-RL) umgesetzt werden soll, zu berücksichtigen. Dieses Gesetz soll zwar nicht der Gewährleistung der IT-Sicherheit, sondern der physischen Sicherheit dienen – dabei aber gleichwohl zu den Regelungen der IT-Sicherheit eine „größtmögliche Kohärenz" erreichen,[392] so dass sich dieses Gesetz hier als weiterer Ansatzpunkt auch für die Auslegung der Resilienz in der Datensicherheit anbietet.

Nach § 2 Nr. 5 RefE KRITIS-DachG umfasst Resilienz „die Fähigkeit eines Betreibers kritischer Anlagen, einen Vorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Vorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen;" Ein Vorfall ist nach § 2 Nr. 9 RefE KRITIS-DachG „ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich stört oder stören könnte."

In § 10 Abs. 1 RefE KRITIS-DachG werden die einzelnen Resilienzmaßnahmen genannt, wobei die Elemente nach § 2 Nr. 5 konkretisiert und ergänzt werden. Darüber hinaus enthält Anhang 1 praktische Resilienzmaßnahmen und nennt unter anderem Notfallvorsorge, Maßnahmen des Objektschutzes (Zäune, Sperren), Zugangskontrollen i.V.m. Personaleinteilungen nach Kritikalität der wahrgenommenen Funktion und entsprechenden Zugangsrechten sowie Sensibilisierungen des Personals.

Im Ergebnis soll Resilienz demnach Störungen der kritischen Dienstleistung (etwa der Wasserversorgung) mit Blick auf die Sicherheit der Anlagen (jenseits der IT-Sicherheit) möglichst ausschließen. Dabei wird laut Entwurfsbegründung mit der Pflichtennorm des § 10 RefE KRITIS-DachG ein „risikobasierter All-Gefahren-Ansatz beim Ergreifen von Maßnahmen zur Stärkung der Resilienz verfolgt."[393]

392 BMI, Referentenentwurf zum KRITIS-DachG, 21.12.2023, S. 1 f.
393 BMI, Referentenentwurf zum KRITIS-DachG, 21.12.2023, S. 60 f.

iv. Digital Operational Resilience Act (DORA)

Im Finanzsektor besteht innerhalb des IT-Sicherheitsrechts der Digital Operational Resilience Acts (DORA) als lex specials gegenüber dem RegE BSIG bzw. der NIS2-RL.[394]

Im DORA ist „digitale operationale Resilienz" in Art. 3 Nr. 1 definiert als „die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es […] das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, zu unterstützen."

Festzuhalten ist zunächst, dass Resilienz auch hier als (aktive) Fähigkeit verstanden wird. Inhaltlich werden hierunter alle IKT-bezogenen Fähigkeiten zur Gewährleistung der Sicherheit der Netzwerk- und Informationssysteme erfasst. Damit ermöglicht diese Definition allerdings keine inhaltliche Konturierung der Resilienz; vielmehr wird insofern eher ein Gleichlauf mit dem IT-Sicherheitsbegriff in dem Sinne geschaffen, dass alle Maßnahmen (insbesondere auch das IKT-Risikomanagement, Art. 5 Abs. 1 DORA) auf eine Erhöhung der Resilienz und auf die Gewährleistung von IT-Sicherheit einzahlen, so dass kein eigenständiger Anwendungsbereich für die Resilienz verbleibt. Allerdings werden in den Art. 10 (Erkennung) Art. 11 (Reaktion und Wiederherstellung) und Art. 13 (Lernprozess und Weiterentwicklung) auch spezifische, dem Resilienzkonzept zuordnungsfähige Aspekte beschrieben.

v. Cybersecurity-Act (CSA)

Eine weitere wesentliche Entwicklung der Resilienz findet sich im Cyber-Security-Act (CSA), der ebenfalls zum IT-Sicherheitsrecht gezählt werden kann.[395] In EG 2 wird festgestellt, dass insbesondere im Bereich IoT „die Sicherheit und Abwehrfähigkeit [eng.: security and resilience] dieser Geräte

394 Siehe EG 28 NIS2-RL.

395 Diese europäische Verordnung (2019/881) regelt die Befugnisse der Agentur der Europäischen Union für Cybersicherheit (ENISA). Zu deren Aufgaben gehört es nach EG 24, 25 insbesondere die Umsetzung der NIS-RL zu unterstützen.

schon bei der Konzeption [bislang] nicht ausreichend berücksichtigt wurden". Mithin wird Resilienz hier nun auch von der Makroebene komplexer Netz- und Informationssysteme auf einzelne IoT-Geräte herunterskaliert. Ungeachtet dessen wird der Resilienzbegriff aber auch hier auf höherer Ebene verwendet, etwa in Bezug auf einzelne Mitgliedsstaaten oder die europäische Union; auf dieser Makroebene sollen die Mitgliedsstaaten demnach insbesondere einen strukturierten Informationsaustausch über Cybersicherheitsrisiken und Maßnahmen pflegen, um nationale Kapazitäten und abgestimmte Verfahren aufzubauen und so im Ergebnis die Resilienz insgesamt zu stärken.[396]

vi. Strategie zum Schutz kritischer Infrastrukturen (Schweiz)

Auch in anderen Ländern wird Resilienz bereits im Kontext der Sicherheit einschließlich der IT-Sicherheit kritischer Infrastrukturen als regulatorischer Begriff verwendet: In der Schweiz ist Resilienz als Bestandteil der vom Schweizerischen Bundesrat beschlossenen „Nationale[n] Strategie zum Schutz Kritischer Infrastrukturen" genannt und anders als im europäischen Rechtsrahmen auch schon mit einer feststehenden Definition ausdifferenziert: Demnach seien kritische Infrastrukturen in der Zielvorstellung resilient, wenn „großflächige und schwerwiegende Ausfälle möglichst verhindert und die Funktionsfähigkeit im Ereignisfall möglichst rasch wieder gewährleistet werden kann."[397] Hierfür wird Resilienz definiert als „die Fähigkeit eines Systems, […] intern oder extern verursachten Störungen zu widerstehen (Widerstandsfähigkeit) und die Funktionsfähigkeit möglichst zu erhalten (Anpassungsfähigkeit) respektive möglichst schnell und vollständig wiederzuerlangen (Regenerationsfähigkeit)."[398]

396 EG 39 CSA; siehe zur Skalierbarkeit des Resilienzbegriffs auch: *Björck et al.*, in: New Contributions in Information Systems and Technologies, Cyber Resilience - Fundamentals for a Definition, 311 (312); *Bodeau/Graubart,* Cyber Resiliency Engineering Framework, Sep. 2011, S. 37.

397 Grundlegend: Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022, 08.12.2017, S. 515 f.

398 Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen, 16.06.2023, S. 3; Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022, 08.12.2017, S. 515 f.

vii. Strategic Plan 2023-2025 (USA)

In den USA hat sich der Begriff seit mehreren Jahren als prominenter Begriff im Bereich des Schutzes kritischer Infrastrukturen etabliert.[399] So spricht auch die Strategie der Cybersecurity and Infrastructure Security Agency (CISA)[400] für die Jahre 2023-2025 von Risikoreduktion und Resilienzstärkung an Amerikas kritischer Infrastruktur.[401] „Dabei wird Resilienz als die Fähigkeit definiert, sich auf veränderte Bedingungen vorzubereiten und sich an sie anzupassen. Das bedeutet, dass die kritische Infrastruktur in der Lage sein muss, Störungen, vorsätzlichen Angriffen, Unfällen oder natürlich auftretenden Bedrohungen oder Zwischenfällen standzuhalten und sich schnell davon zu erholen. Eine resiliente Infrastruktur muss demnach auch robust, agil und anpassungsfähig sein."[402] Demgegenüber wird Sicherheit (Security) definiert als die „Reduktion von Risiken für kritische Infrastrukturen durch Eindringen, Angriffe oder die Auswirkungen von Naturkatastrophen oder vom Menschen verursachten Katastrophen durch den Einsatz von physischen Mitteln oder defensiven Cyber-Maßnahmen."[403]

Hieran zeigt sich, dass die Gewährleistung von Resilienz von der Risikoreduktion im Rahmen der IT-Sicherheit zu unterscheiden ist. Dieser Differenzierung wird später im Rahmen der systematischen Auslegung noch weiter nachgegangen. Im Übrigen lassen sich auch hier ähnlich der Schweizer KRITIS-Strategie die Elemente des Widerstands, der Anpassung an und der Erholung nach einem Ereignis isolieren.[404]

---

399 Teilweise wird er auch als „Ersatz" für den Begriff des Schutzes kritischer Infrastrukturen verstanden: *Fekete/Grinda/Norf*, in: Wink, Multidisziplinäre Perspektiven der Resilienzforschung, 215 (222).

400 Die CISA ist in den USA eine Bundesbehörde und zugleich Teil des Ministeriums für innere Sicherheit (en: Department of Homeland Security), siehe auch: https://www.dhs.gov/topics/cybersecurity, zuletzt abgerufen: 19.04.2024.

401 CISA, Strategic Plan 2023-2025, Sep. 2022, S. 16 ff.

402 Original (en): "Resilience may be defined as the ability to prepare for and adapt to changing conditions. This means being able to withstand and recover rapidly from disruptions, deliberate attacks, accidents, or naturally-occurring threats or incidents. Resilient infrastructure must also be robust, agile, and adaptable."; CISA, A Guide to Critical Infrastructure Security and Resilience, Nov. 2019, S. 11.

403 Original (en): "Security may be defined as reducing the risk to critical infrastructure from intrusions, attacks, or the effects of natural or man-made disasters, through the application of physical means or defensive cyber measures." CISA, A Guide to Critical Infrastructure Security and Resilience, Nov. 2019, S. 11.

404 Siehe zu diesen Elementen ausführlicher auch schon: NIAC, Critical Infrastructure Resilience, 08.09.2009, S. 12 f.

viii. Fazit

Insgesamt bleibt der Begriff Resilienz im europäischen und nationalen IT-Sicherheitsrecht eher unscharf und für die Ermittlung eines präzisen Wortlautverständnisses ungeeignet. Zu häufig wird er als Schlagwort im Rahmen der Gewährleistung von IT-Sicherheit und (Cyber)resilienz verwendet.

In der DORA zeigt sich mit der Definition der „digitalen operationalen Resilienz" eine weitgehende Gleichsetzung von Resilienz und IT-Sicherheit. Gleichzeitig werden aber zumindest auch resilienzspezifische Maßnahmen (Erkennung, Reaktion und Wiederherstellung sowie einen Lernprozess) verlangt. Der CSA fordert in Art. 1 Abs. 1 zwar sowohl „ein hohes Niveau" der Cybersicherheit als auch der Cyber-Resilienz (zit: „Fähigkeit zur Abwehr von Cyberangriffen", eng.: cyber resilience), definiert letztere aber nicht. Mit diesem Schlagwort bestimmt der EU-Gesetzgeber folglich nur ein übergreifendes Ziel, das anzustreben und bei dessen Erreichen gleichsam die Sicherheit gewährleistet sei. In eben diese Richtung weist auch der CRA-E, der eine horizontale Regelung zur IT-Sicherheit von Produkten darstellt, aber trotz der Resilienz im vorgesehenen Gesetzestitel und mehrfacher Nennung im Gesetzestext als auch in den Erwägungsgründen diesen Begriff in keiner Weise inhaltlich nutzbar macht.

Ähnlich verhält es sich auch mit der NIS2-RL, dem RegE BSIG und dem RefE KRITIS-DachG. Letzterer liefert zwar eine Methodendefinition, die erneut auch mögliche Resilienzelemente wie die Reaktion auf Vorfälle oder die Folgenbegrenzung sowie die Erholung von Vorfällen beinhaltet; sie bezieht sich aber im Übrigen v.a. auf ein klassisches, risikobasiertes Vorgehen (§ 10 Abs. 1 S. 2 RefE KRITIS-DachG) und umfasst insbesondere auch typische Sicherheitsaspekte wie etwa den Objektschutz durch Zäune und Sperren. Dadurch schafft diese Definition nicht die nötige Abgrenzung zum bisherigen Sicherheits- oder Schutzbegriff. Stattdessen wird Resilienz hier erneut als konsumierender Oberbegriff -in diesem Fall für die physische Sicherheit- verwendet.

Einen etwas anderen Blickwinkel liefert hingegen die Schweizer KRITIS-Strategie sowie der Strategieplan der US-amerikanischen CISA. Hier wird zum einen eine präzise Definition mit unterschiedlichen Teilaspekten der Resilienz als auch im Strategieplan der CISA sogar eine definitorische Abgrenzung zur IT-Sicherheit geliefert. Diese Aspekte können die Wortlautauslegung somit entscheidend bereichern.

3. Synthese

Auf Basis der beschriebenen Begriffsverständnisse und den dahinterstehenden Konzepten der Resilienz in den unterschiedlichen Domänen erfolgt nun die Synthese derselben für das Wortlautverständnis der Resilienz als Rechtsbegriff in der Datensicherheit. Insgesamt zeigte sich die Resilienz als Begriff sehr universell und lässt sich auf verschiedenste Objekte (Materialien, Menschen, Ökosysteme, kritische Infrastrukturen) beziehen. Das Nationale Institute of Standards and Technologie (NIST) weist dementsprechend verschiedene Definitionen für Resilienz aus, je nachdem auf welches Objekt sie sich bezieht.[405] Für die Auslegung des Resilienzbegriffs ist folglich zu beachten, dass dieser nach Art. 32 Abs. 1 lit b) DSGVO neben Diensten insbesondere auf Systeme bezogen wird. Insofern liegt es nahe jenen Verständnissen der Resilienz ein gesteigertes Gewicht in der Synthese einzuräumen, die sich ebenfalls auf die Resilienz von Systemen beziehen.

In den Bereichen der IT-Sicherheit, der kritischen Infrastrukturen sowie dem Katastrophenschutz zeigte sich außerdem spezifischer, dass die entsprechenden Verständnisse und Definitionen ein *soziotechnisches System* voraussetzen. Dabei war insbesondere festzuhalten, dass die Resilienz sich hier nicht auf das technische System beschränken darf, sondern die Mitarbeitenden miteinbezogen werden müssen, um etwa nach einem technischen Zwischenfall eine gewisse Ordnung aufrechtzuerhalten, die Schadensausbreitung zu vermindern oder ggf. auch Maßnahmen zur Wiederherstellung einzuleiten.[406] Ihnen kommt insoweit anders als den meisten technischen Systemen die Fähigkeit zu, sich angesichts von überraschenden Vorfällen adaptiv zu verhalten.[407] Auf den Aspekt des soziotechnischen Systemverständnisses der Resilienz wird in der systematischen Auslegung mit Blick auf den Systembegriff in Art. 32 Abs. 1 lit b) DSGVO noch zurückzukommen sein.

Hinsichtlich der Auslegung des Resilienzbegriffs als solchem bildet zunächst gleichwohl der psychologische Resilienzbegriff als die prägende

405 Dort u.a. für Systeme, Organisationen oder Nationen; *Ross et al.,* Developing cyber resilient systems, 2019, S. 71 f.; ähnlich auch: *Björck et al.*, in: New Contributions in Information Systems and Technologies, Cyber Resilience - Fundamentals for a Definition, 311 (312).

406 Vgl. auch: *Gazos*, in: Polarisierte Welten: Verhandlungen des 41. Kongresses der Deutschen Gesellschaft für Soziologie, Die soziomaterielle Konstitution von Cybersicherheit in der Dynamik kritischer Informationsinfrastrukturen, S. 4.

407 Wie zuvor.

Domäne das Fundament für die weitere Bestimmung. Er offeriert ein grundlegendes Verständnis, indem er die erfolgreiche Anpassung an bzw. die Erholung nach widrigen Lebensumständen adressiert. Mit Blick auf die Unabdingbarkeit der Konfrontation mit widrigen Lebensumständen wird der Charakter des Konzepts deutlich, nachdem Gegenstand der Resilienz jedenfalls nicht die Vermeidung bzw. der Ausschluss der schädigenden Ereignisse als solcher sein kann. Vielmehr gilt es nach diesem Verständnis der Resilienz solche unvermeidbaren, „umweltbedingten Risikoerfahrungen" und insbesondere deren „erwartete Folgen" möglichst gut zu bewältigen.[408] Dieses Definitionsmerkmal als *Umgang mit unvermeidbaren, widrigen Ereignissen*[409] ließe sich auch uneingeschränkt auf die deutsche Übersetzung „Belastbarkeit" übertragen, da dieser Begriff impliziert, dass das Auftreten von Belastungen nicht verhindert werden kann und diese somit ausgehalten werden müssen.[410] Weiterhin lässt sich abstrahierend festhalten, dass bestimmte Faktoren die entweder an dem Subjekt (hier dem System) ansetzen oder sich aus dessen Verhältnis zu seiner Umgebung ergeben, die Resilienz als Ergebnis begünstigen oder schwächen. Diese Faktoren könnten in der Datensicherheit durch Maßnahmen beschrieben bzw. ausgefüllt werden. Gleichzeitig sollte wie in der Psychologie davon ausgegangen werden, dass die Resilienz stets nur eine Momentaufnahme ist und nicht als statische Eigenschaft einem Subjekt per se anhaftet.[411] Schließlich dürfte auch die Steigerung der Resilienz durch einen „Abhärtungseffekt" in der Erholungsphase, bei dem aus den bisherigen Ereignissen gelernt wird, für die Datensicherheit ein wesentlicher Baustein sein.

Weiterhin gibt der ökologische Resilienzbegriff entscheidende Impulse für das Verständnis von Resilienz: Zunächst ist die Anpassungsphase in der Ökologie besonders charakteristisch. Hierbei wird auf die Fähigkeit zur Einnahme *qualitativ verschiedener Zustände* abgestellt und weniger auf eine Rückkehr zu einem primären, stabilen Zustand, wie es das technische Verständnis propagiert.[412] Dies lässt sich auf informationstechnische Systeme und Dienste allerdings nur bedingt übertragen, da auch hier zwar ein

408 *Rutter*, Development and psychopathology 2012, 335 (336); *Bröckling*, Resilienz: Über einen Schlüsselbegriff des 21. Jahrhunderts, 2017, S. 8.

409 Vgl. in diesem Sinne im Datenschutzrecht bereits: DSK, Standard-Datenschutzmodell, B.1.19, S. 22; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39.

410 *Bröckling*, Resilienz: Über einen Schlüsselbegriff des 21. Jahrhunderts, 2017, S. 8.

411 *Park et al.*, Risk analysis 2013, 356 (359).

412 Vgl. *Davoudi*, Planning Theory & Practice 2012, 299 (300 f.).

abweichender Zustand z.B. in Form eines Notfallmodus möglich und ggf. sogar sinnvoll erscheint, das mittel- bis langfristige Ziel aber in der Regel die Rückkehr zu einem „Normalzustand" und dem eigentlichen Leistungsprogramm ist.[413] Eine gewissermaßen freie evolutionäre Anpassung ist bei IT-Systemen und Diensten insoweit kaum möglich. Technische Systeme sind anders als ökologische Systeme Ausdruck einer menschlichen Intention und sind somit dahingehend konzipiert einen bestimmten Dienst zu erbringen,[414] wovon sie nicht ohne weiteres transformatorisch abweichen können und sollen.[415] Somit ist insgesamt ein Verständnis der Resilienz anzuwenden, wie es in anthropozentrischen Resilienzverständnissen wie der technischen Resilienz (mit Blick auf den Menschen auch in der Psychologie) und innerhalb der Ökologie allenfalls noch in der Klima(schutz)forschung zugrunde liegt, bei dem nur ein intendierter, stabiler Zustand des Systems bzw. des Dienstes als Maßstab für die Resilienz vorliegt. Eine evolutionäre Anpassung ist bei der Resilienz als Datensicherheitsprinzip nur insoweit möglich, als dass moderne IT-Systeme möglichst autonom aus Ereignissen lernen und sich optimierend anpassen sollen, um künftig besser auf solche vorbereitet zu sein.[416] Aber dieser Prozess bleibt auf die Sicherheit der Systeme und Dienste beschränkt. Dass sich IT davon unabhängig z.B. an geänderte Nutzeranforderungen anpassen soll, ist jedenfalls kein Aspekt der Resilienz im Kontext der Datensicherheit.

Darüber hinaus ist der Aspekt der *quantitativen Resilienz* zu beachten, der in der Ökologie in Form von schwankenden Populationsgrößen auftritt. Dieser Aspekt lässt sich für die Informationstechnik in dem Sinne nutzbar machen, dass ein System in der Lage sein soll bei einem widrigen

413 „You want your computer to bounce back and do what it was designed to do." *Longstaff*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 259 (265 f.). Gleichzeitig weist *Longstaff* aber auch auf die bestehende Tendenz hin, technische Systeme stärker nach ökologischem Vorbild zu gestalten.

414 Vgl. *Park et al.*, Risk analysis 2013, 356 (357), die insoweit ebenfalls attestieren, dass zwischen der Anwendung des Resilienzbegriffs auf ökologische bzw. technische Systeme differenziert werden muss, da nur letztere eine Intentionalität (nach hiesigem Verständnis: die Erbringung eines bestimmten Dienstes) aufweisen.

415 Vgl. *Heeks/Ospina*, ISJ (Information Systems Journal) 2019, 70 (72) mit Verweis auf ihre Literaturrecherche zur Resilienz bei Informationssystemen, nach der die überwiegende Mehrheit der untersuchten Literatur eine Wiederherstellung der Systemleistung (bounce back) anstrebt, eine fortentwickelnde Anpassung (bounce forward) konnte hingegen nur in 3 Literaturquellen gefunden werden.

416 Vgl. mit englischer Bezeichnung „Evolvability", welche als Teil der Resilienz kontinuierliches Lernen und Optimieren beschreibt: *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (11); *Ratasich et al.*, IEEE Access 2019, 13260 (13271).

Ereignis zu schwanken, d.h. seine Leistung in Form des Dienstangebots graduell abzusenken, aber nach Möglichkeit ein schlagartiges und vollständiges Ausfallen des Dienstes zu verhindern.

Ebenso ist die Vorstellung von *Grenzen der Resilienz* sowohl aus dem ökologischen als auch dem technischen Verständnis transferfähig: Unabhängig davon ob es nun um das Aussterben eines multistabilen Ökosystems oder die Unmöglichkeit zur Rückkehr eines Ausgangszustands nach dem technischen Verständnis geht: Die abzuleitende Erkenntnis ist, dass das Maß an Belastungen beschrieben werden muss, mit dem ein (hier informationstechnisches) System trotz vorhandener Resilienz möglicherweise nicht mehr umgehen kann.[417] Dies wirft zugleich die noch ungeklärte Frage nach der Messbarkeit von Resilienz[418] auf, die an dieser Stelle aber nicht vertieft werden soll.

In der Informationstechnik begründen *Avizienis/Laprie u.a.* ein methodisch solides Verständnis des Resilienzbegriffs als Fehlertoleranz, d.h. dass aktiv werdende Fehler erkannt und bewältigt werden müssen, so dass sie nicht zu einem (vollständigen) Ausfall der Systemfunktion in Gestalt des Dienstes führen. Die später von *Laprie* vorgenommene Ausdehnung des Resilienzbegriffs u.a. auf die Fehlerprävention ist dagegen geeignet diese methodische Klarheit zu konterkarieren; allerdings setzt diese Ausdehnung mit der Hervorhebung einer sich verändernden Umgebung und den deshalb notwendigen Merkmalen insbesondere der Entwicklungsfähigkeit als auch der Diversität von Systemen auch für die Datensicherheit wichtige Akzente. Mit Blick auf die IT-Sicherheit erscheinen insbesondere die Merkmale der Erkennung eines Ereignisses (hier v.a. eines Angriffs), der Anpassungsfähigkeit an ein solches sowie ggf. der Wiederherstellung nach einem solchen einschließlich eines Lerneffekts zentral auch für das Verständnis in der Datensicherheit. Aus der Netzwerktechnik kann ergänzend abgeleitet werden, dass Resilienz auch bedeutet mit Ereignissen umzugehen, bei denen gar nicht bekannt ist, ob es sich um einen vorsätzlichen Angriff oder ein sonstiges Ereignis handelt (etwa im Falle des Erhalts (vermeintlich) korrumpierter Daten). Darüber hinaus folgt aus der IT-Sicherheit auch die Erkenntnis, dass Resilienz gegen ungewisse Ereignisse wie etwa neue, bislang unbekannte Angriffsformen gerichtet ist.

417 Resilienzmaßnahmen werden im Datensicherheitsrecht insbesondere auch durch das Merkmal der Angemessenheit beschränkt, siehe dazu später: S. 182 f.

418 *Heeks/Ospina*, ISJ (Information Systems Journal) 2019, 70 (72); *Zobel/Khansa*, Decision Sciences 2012, 687 (687 ff.).

Das IT-Sicherheitsrecht bietet sich als Pate für das Datensicherheitsrecht insofern an, als dass es dort ebenfalls um die staatlich vorgegebene Gewährleistung von Sicherheit in informationstechnischen Systemen zum Schutz von zumindest auch grundrechtlich geprägten Schutzgütern geht. Allerdings besteht auch hier zumeist noch keine eindeutige Legaldefinition. Als prägend für den Resilienzbegriff kann zumindest identifiziert werden, dass er Bewältigungsmethoden wie die Erkennung, die Reaktion, die Folgenminderung und die Erholung von bzw. auf Ereignisse(n) umschreibt. Dabei sind insbesondere auch die Schweizer Strategie zum Schutz kritischer Infrastrukturen sowie der Strategic Plan der *CISA* hervorzuheben, die recht eindeutig die drei Elemente der (Widerstandsfähigkeit, Anpassungsfähigkeit und Regenerationsfähigkeit) beschreiben und damit ein hohes Maß an Operationalität versprechen. Aus den Definitionen der CISA ist weiterhin zu entnehmen, dass Resilienz anders als „klassische Sicherheitsgewährleistung" nicht (unmittelbar) auf die Reduktion von Risiken gerichtet ist (ausführlich dazu auf S. 169 ff.).

Im Katastrophenschutz verdeutlicht sich schließlich noch einmal die schon in der Psychologie identifizierte Differenzierung zur Resistenz: So geht es bei Resilienz nicht mehr vorrangig darum, widrige Ereignisse zu verhindern (was insbesondere bei Naturkatastrophen oder auch Terroranschlägen naturgemäß nur begrenzt möglich ist), sondern v.a. um die Strategie im Umgang mit einem eingetretenen Ereignis.

Aus vielen der untersuchten Begriffsverständnissen wird außerdem deutlich, dass sich die Resilienz i.d.R. nicht auf die Bewältigung spezifischer Ereignisse richtet, sondern vielmehr den Blick auf das zu schützende Objekt (in der Psychologie eine Person, bei Ökologie und technischer Resilienz ein System) selbst richtet, um dieses in seiner (generellen) Bewältigungsfähigkeit gegenüber unterschiedlichsten und zumeist auch ungewissen, widrigen Ereignissen zu stärken.[419] Dieser Aspekt wird in der systematischen Auslegung bei der Abgrenzung gegenüber den klassischen, spezifischen Schutzzielen (Verfügbarkeit, Vertraulichkeit und Integrität) nochmals vertieft.

419 So mit Blick auf Ökologie, Ingenieurswissenschaft und Psychologie zur Ableitung der Resilienz im Katastrophenschutz: *Krüger/Max*, Resilienz im Katastrophenfall, S. 66.

4. Fazit

Ausgehend von der zuvor dargestellten Synthese ergibt sich für die Wortlautauslegung der Resilienz in der Datensicherheit folgendes Fazit und die am Ende dieses Abschnitts dargestellte Arbeitsdefinition für die weitere Auslegung.

Aus der Synthese lassen sich insbesondere drei für die Resilienz konstituierenden Elemente identifizieren: Es wurde gezeigt, dass für die Resilienz die Fähigkeit zur Anpassung an ein (widriges) Ereignis als auch zur Regeneration nach einem solchen entscheidend sind. Beides setzt jedoch, wie auch einige der untersuchten Resilienzansätze zeigten, zunächst voraus, dass das Auftreten eines nicht vorhergesehenen (ungewissen) Ereignisses zunächst einmal von dem System möglichst frühzeitig erkannt wird („*Ereigniserkennung*").[420]

Die „*Anpassungsfähigkeit*" an ein Ereignis verfolgt das Ziel, die Auswirkungen des Ereignisses auf die Datensicherheit (z.B. auch durch manipulierte Dienste) durch adaptive Maßnahmen möglichst gering zu halten.[421] In diesem Zusammenhang ist insbesondere auch die nach dem ökologischen Verständnis wichtige Schwankungsfähigkeit zu sehen, d.h. die Möglichkeit zur graduellen Absenkung anstelle eines Totalausfalls. Die ebenfalls immer wieder genannte *Widerstandsfähigkeit* dürfte sich zumindest zum Teil als Aktives widerstehen (z.B. durch die Aktivierung redundanter Strukturen) als Unterfall bzw. Synonym der Anpassung verstehen lassen.

Schließlich erwies sich die *Fähigkeit zur Erholung* als essenziell. Dies umfasst sowohl die Wiederherstellung des ordnungsgemäßen Zustandes

420 So insbesondere bereits in der Informationstechnik, sowohl Fehler- (Verlässlichkeit) als auch Ereigniserkennung (IT-Sicherheit): Informationstechnik, S. 133 ff. ; als Merkmal der Resilienz auch bei *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 45, *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 61; als Angriffserkennungssysteme: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39; unabhängig von der Resilienz als beispielhafte Maßnahme nach Art. 25 Abs. 1 i.V.m. Art. 5 Abs. 1 lit f): EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, S. 33.

421 Vgl. *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 42, 45; ähnlich auch: *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 26; mit in vorheriger Fußnote genannten Einschränkungen *EDSA,* wie zuvor.

(z.B. bei der Diensterbringung) als auch die Analyse und das Lernen aus dem Ereignis,[422] um die Resilienz für die Zukunft zu verbessern.

Insgesamt lässt sich damit als Arbeitsdefinition aus der Wortlautauslegung festhalten, dass Resilienz nach dem Wortlaut *die Fähigkeit eines soziotechnischen Systems beschreibt, ungewisse Ereignisse zu erkennen, sich an diese anzupassen und sich nach einem solchen unter lernender Verbesserung schnellstmöglich zu erholen.*

III. Systematische Auslegung

Im Rahmen der systematischen Auslegung gilt es den Begriff der Resilienz gegenüber dem übrigen Art. 32 DSGVO rechtlich einzuordnen. Nach Art. 32 Abs. 1 DSGVO sind alle Maßnahmen und somit auch jene zur Gewährleistung der Resilienz auf ein „dem Risiko angemessenes Schutzniveau" auszurichten, so dass sich für die systematische Auslegung zunächst die Frage stellt, wie sich die Resilienz mit dem schon angedeuteten Fokus auf ungewisse Ereignisse gegenüber dem Begriff sowie der Methodik des Risikos positioniert (1.). Nach Art. 32 Abs. 1 lit b) DSGVO soll aber nicht nur die Resilienz, sondern auch die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sichergestellt werden. In einem zweiten Schritt ist daher die Resilienz diesen Schutzzielen gegenüberzustellen (2.)

1. Risiko

Der Risikobegriff bezieht sich nach Art. 32 Abs. 1 DSGVO auf die Schutzgüter der „Rechte und Freiheiten natürlicher Personen". Nach einer Einleitung soll der Begriff des Risikos (b.) sowie die Risikomethodik (c.) näher erläutert werden.

a. Einleitung

Das Risiko ist ein essenzieller Abwägungsfaktor bei der Wahl von toM, wozu auch die Resilienzmaßnahmen gehören. Der Normadressat hat insofern eine Entscheidung zu treffen, welche toM er auswählt, um den Norm-

422 Mit den in Fn. 420 genannten Einschränken: *EDSA,* wie zuvor.

auftrag der Gewährleistung eines risikoangemessenen Schutzniveaus zu erfüllen. Bei dieser Entscheidung ist eine Abwägung zwischen der Risikominderung der zu ergreifenden toM und dem hierfür nötigen Aufwand (Implementierungskosten) vorzunehmen.[423] Aufgrund des zentralen Elements der Entscheidung im Rahmen dieses Normauftrags wird der Normadressat in diesem Abschnitt (1. Risiko) als *Entscheider* bezeichnet.

b. Begriffsdefinition

Eine gesetzliche Definition des Risikos enthält die DSGVO nicht. Allerdings wird der Begriff in der DSGVO in EG 75 zumindest durch die zwei Dimensionen der „Eintrittswahrscheinlichkeit" und „Schadensschwere" konturiert.[424] Auch ergibt sich aus EG 75, dass die Risiken initial stets „aus einer Verarbeitung personenbezogener Daten hervorgehe[n]". Die Eintrittswahrscheinlichkeit bezieht sich im Kontext des Art. 32 DSGVO auf den Eintritt von im Sinne der Datensicherheit unerwünschten Ereignissen und die Schadensschwere auf dessen Folgen.[425]

Für einen Risikoeintritt müssen weitere Umstände, namentlich Angriffe oder sonstige Ereignisse, das Vorhandensein von Sicherheitslücken[426] sowie ggf. das Fehlen bzw. die Unvollständigkeit von Schutzmaßnahmen[427] gegeben sein, die zu einer Beeinträchtigung von Rechten und Freiheiten natürlicher Personen führen. Da der Eintritt dieser Umstände abhängig von der oder den Eintrittswahrscheinlichkeit(en) aber nicht sicher ist, stellt der Risikobegriff stets nur eine beschreibende, antizipierende Annäherung an eine unsichere Zukunft dar.[428]

---

423 Vgl. *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 95, wonach zumindest kein „eklatantes Missverhältnis" bestehen darf.

424 *Bieker/Bremert*, ZD 2020, 7 (8).

425 *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 13; als „Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung" *Grages*, in: Plath, DSGVO, BDSG, TTDSG Kommentar, 4. Auflage 2023, Art. 32, Rn. 4.

426 *Grages*, in: Plath, DSGVO, BDSG, TTDSG Kommentar, 4. Auflage 2023, Art. 32, Rn. 4.

427 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (401 f.), Rn. 26.

428 Vgl. *Scherzberg*, in: Engel/Halfmann/Schulte, Wissen, Nichtwissen, unsicheres Wissen, 113 (136).

Die Datenschutzkonferenz (DSK) definiert das Risiko als

> *„das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.*"[429]

Dies deckt sich zumindest teilweise mit den rechtlichen Vorgaben. Zutreffend ist zunächst, „das Bestehen der Möglichkeit" als Ausdruck der unsicheren Zukunft an den Anfang zu stellen und insoweit mit dem Begriff der *Eintrittswahrscheinlichkeit* zu beschreiben.

Das „Ereignis" selbst sollte indes vom Schaden sprachlich getrennt bleiben. Zutreffend ist zwar, dass Ereignis und Schaden unmittelbar zusammenfallen können, etwa wenn persönliche Daten unbefugt offengelegt wurden. Nichtsdestotrotz sollte zwischen dem technischen Ereignis (also insbesondere, aber nicht ausschließlich dem „Sicherheitsvorfall") und seinen rechtlichen Auswirkungen bzw. Schäden konsequent differenziert werden. Auch ist zu beachten, dass nicht jedes Ereignis auch zu einem Schaden führt, d.h. es ist unzureichend hier nur von einer Eintrittswahrscheinlichkeit auszugehen. Vielmehr besteht eine weitere Eintrittswahrscheinlichkeit (an der ggf. auch mit Maßnahmen angesetzt werden kann), wonach das Ereignis auch einen Schaden nach sich zieht.[430]

Den Komplementärbegriff zum Risiko bildet aus soziologischer Perspektive die „Sicherheit".[431] Nach der Überschrift des Art. 32 DSGVO soll die „Sicherheit der Verarbeitung" gewährleistet werden. Da eine absolute Sicherheit im Sinne einer vollständigen Risikofreiheit per se nicht erreicht, sondern allenfalls eine (soziale) Fiktion darstellen kann,[432] reduziert Art. 32 DSGVO die Gewährleistungsanforderung sachgemäß hin zu einem risikoangemessenen Schutzniveau; d.h. die Risiken müssen um ein angemessenes Maß gemindert werden.[433]

---

429 DSK, Kurzpapier Nr. 18, 26.04.2018, S. 1.

430 Wohl ebenfalls (aber ausschließlich) auf die Eintrittswahrscheinlichkeit des Schadenseintritts abstellend: *Bieker*, DuD 2018, 27 (30 f.); vgl. außerdem: DIN, ISO/IEC 27005:2022 (EN), S. 16.

431 *Luhmann*, Soziologische Aufklärung 5, S. 128.

432 Wie zuvor.

433 Ausführlich dazu sogleich auf S. 167.

Insgesamt sollte Risiko darum definiert werden als

„die Eintrittswahrscheinlichkeit eines Ereignisses sowie eines Schadens an den Rechten und Freiheiten natürlicher Personen und dessen Schwere."

Diese Definition soll anhand der nachfolgenden Grafik noch einmal illustriert werden:

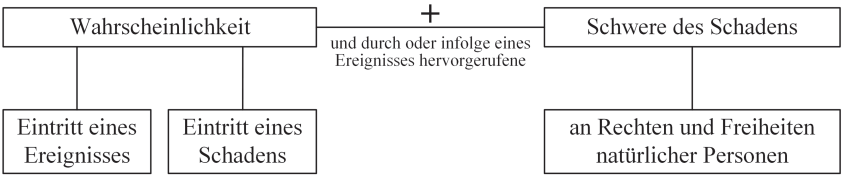

Abbildung 8: Risiko aus Wahrscheinlichkeit und Schadensschwere

Der *Begriff des Ereignisses* sollte dabei möglichst generisch verstanden werden. Er kann zwar die Verletzung des Schutzes personenbezogener Daten i.S.d. Art. 4 Nr. 12 DSGVO darstellen. Auch dieser kann aber noch ein Ereignis vorausgegangen sein, z.B. ein Fehler und damit ein Verfügbarkeitsverlust in einem System. Insofern normiert die DSGVO mit der Verletzung des Schutzes personenbezogener Daten nur einen „datenbezogenen Sicherheitsvorfall"; der system- oder dienstbezogene Sicherheitsvorfall, also eine Verletzung der diesbezüglichen Schutzziele, ist hingegen nicht ausdrücklich benannt. Seine Bedeutung als Ursache für eine Verletzung personenbezogener Daten ergibt sich aber systematisch aus Art. 32 Abs. 1 lit b) DSGVO.[434]

Entsprechend kann die voranstehend beschriebene *Kette von Ereignissen* und dem schlussendlichen Schaden erweitert werden, z.B. Manipulation im System (Wahrscheinlichkeit a) führt mit Wahrscheinlichkeit b) zu einer Veränderung personenbezogener Daten, was mit Wahrscheinlichkeit c) zu bestimmten Schäden an den Rechten und Freiheiten natürlicher Personen (EG 75, z.B. finanzieller Verlust) führt. Somit können Risiken tiefgreifend antizipiert und abgeschätzt werden. In der Praxis werden insbesondere auch für eine granularere Darstellung der Eingriffe in informationstechnische Systeme sog. Angriffsbäume verwendet.[435]

434 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (403), Rn. 30.
435 *Liedtke*, Informationssicherheit, S. 176; *Schneier*, Dr. Dobb's journal, Vol. 24 (1999), Heft 12, 21 (21 ff.).

Daraus wird außerdem deutlich, dass sich das Risiko mit dem Eintritt des Ereignisses der Verletzung des Schutzes personenbezogene Daten häufig noch nicht endgültig realisiert hat. Vielmehr führt die extensive Auslegung des Risikobegriffs dazu, dass sich das Risiko erst dann endgültig verwirklicht hat, wenn infolge des Ereignisses auch ein Schaden in seiner finalen Ausprägung an den Rechten und Freiheiten natürlicher Personen eingetreten ist.

c. Methodik

Die Identifikation, die Analyse und die ggf. vorzunehmende Behandlung von Risiken bedarf weiterhin einer bestimmten Methodik, die als „Risikomanagement" bezeichnet wird.[436]

i. Einleitung

In Art. 32 DSGVO ist ein Risikomanagement zunächst nicht explizit vorgeschrieben.[437] Allerdings ist es im Rahmen einer sog. Risikofolgenabschät-

436 *Bieker/Bremert*, ZD 2020, 7 (8); ähnlich auch DSK, Standard-Datenschutzmodell, S. 49; weisen insofern daraufhin, dass der Begriff „Risikomanagement" im Unternehmensbereich an sich eine Methodik meint, um Risiken für ein Unternehmen auf ein aus dessen Sicht annehmbares Maß zu reduzieren, was insbesondere von der jeweiligen Risikoaffinität des Unternehmens abhängt. Der Begriff wird in dieser Untersuchung davon insofern abweichend verwendet, als dass die Methodik nach hiesigem Verständnis stets auf das Ziel einer rechtlich unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes angemessenen Risikoreduktion gerichtet ist. Außerdem ist Risikoobjekt insofern nicht das ggf. als Verantwortlicher operierende Unternehmen, sondern die durch die DSGVO geschützte betroffene Person; vgl. *F. Thoma*, ZD 2013, 578 (578 f.); ähnlich auch *Heinemann*, in: Moos/Arning/Schefzig, Die neue Datenschutz-Grundverordnung, 463 (466 f.), Rn. 10-13.

437 Ob ein solches Risikomanagement insbesondere auch mit Blick auf die erforderliche Risikobeurteilung (siehe hierzu: *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 24 ff.) sowie das Erfordernis der regelmäßigen Überprüfung, Bewertung und Evaluierung nach Art. 32 Abs. 1 lit d) DSGVO trotzdem bei Anwendung des Art. 32 Abs. 1 stets erforderlich ist, kann an dieser Stelle dahingestellt bleiben. Es spricht jedoch aufgrund der genannten Anforderungen einerseits viel dafür; mit Blick auf die Verhältnismäßigkeit gerade bei sehr kleinen Unternehmen oder Selbstständigen sind jedoch andererseits auch Zweifel angezeigt, ob wirklich ein Risikomanagement im hier verstandenen Sinne durchgeführt werden muss (oder ob es ggf. nicht auch hinreichend ist, wenn nur

zung nach Art. 35 DSGVO auch hinsichtlich der Datensicherheit vorgesehen.[438] Somit findet ein Risikomanagement (auch) hinsichtlich der Datensicherheit jedenfalls dann statt, wenn die Voraussetzungen einer Risikofolgenabschätzung nach Art. 35 DSGVO (voraussichtlich hohes Risiko der Verarbeitung (Art. 35 Abs. 1) oder Erfüllung eines Regelbeispiels nach Art. 35 Abs. 3) gegeben sind. Bei den hier gegenständlichen digitalen Diensten dürfte dies regelmäßig bereits aufgrund des für die Personalisierung vorgenommenen Profilings der Fall sein.[439]

Inhaltlich wird das Risikomanagement wie folgt konturiert: Nach Art 35 Abs. 7 DSGVO sind insbesondere die Verarbeitungsvorgänge zu beschreiben, die daraus resultierenden Risiken zu bewerten und durch entsprechend vorzusehende Abhilfemaßnahmen zu bewältigen. Auch die Erwägungsgründe 77 und 90 DSGVO zeichnen ein solches Risikomanagement vor, in denen u.a. dem europäischen Datenschutzausschuss (EDPB)[440] die Verfassung entsprechender Leitlinien nahegelegt wird. Demnach ist das mit der Verarbeitung verbundene Risiko zunächst zu *ermitteln*, anschließend in Bezug auf Ursache, Art, Eintrittswahrscheinlichkeit und Schwere *abzuschätzen* und schließlich entsprechend *einzudämmen*.

Darüberhinausgehend lässt die DSGVO offen, anhand welcher konkreten methodischen Ausgestaltung das Risikomanagement vorgenommen werden soll. Die dargestellten Ansätze weisen aber bereits Ähnlichkeiten mit dem aus der Informationssicherheit bekannten Informationssicherheitsmanagementsystem (ISMS) nach der ISO/IEC 27000-Familie bzw. dem allgemeinen Risikomanagement nach ISO 31000[441] auf. Spezifisch für das Datenschutzrecht existiert weiterhin eine Norm zur Datenschutzfolgen-

---

generell risikoangemessene Maßnahmen nach dem Stand der Technik getroffen werden, z.B. auf Basis eines Branchenleitfadens zur Datensicherheit).

438 *Baumgartner*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 35, Rn. 54; *Syckor/Strufe/Lauber-Rönsberg*, ZD 2019, 390 (392).

439 Die „Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen" wird auch in der Liste der Verarbeitungsvorgänge, für die eine Datenschutzfolgenabschätzung gemäß Art. 35 Abs. 4 DSGVO durchzuführen ist genannt; der „Betrieb von großen sozialen Netzwerken" wird hierzu als typisches Einsatzfeld bezeichnet, DSK, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, 17.10.2018, S. 3, Ziff. 9.

440 Zum europäischen Datenschutzausschuss siehe Art. 68 DSGVO. Im Englischen: European Data Protection Board (EDPB), wobei diese Abkürzung auch im Rahmen dieser Untersuchung verwendet wird.

441 Ebenfalls auf eine „Überschneidung" hinweisend: Art.-29 Datenschutzgruppe, WP 248 Rev. 01, 04.10.2017, S. 21.

abschätzung (ISO/IEC 29134), die auch die Datensicherheit abdeckt[442] und auf die vom EDPB verwiesen wird.[443] Auf nationaler Ebene existiert daneben noch das sog. Standard-Datenschutzmodell der DSK.[444]

Aufgrund der internationalen Ausrichtung, die insbesondere für Anbieter der global angebotenen digitalen Dienste entscheidend sein dürfte und des ausdrücklichen Verweises durch den EDPB wird nachfolgend die Methodik der ISO/IEC 29134 dargestellt, die grundlegenden Bausteine finden sich aber in allen genannten Normen wieder.[445]

Die ISO/IEC 29134 enthält mit Blick auf die Risikobeurteilung insbesondere folgende methodische Schritte, die Ermittlung" und „Abschätzung" von Risiken aus der DSGVO entsprechen:[446]

1. Identifizieren von Datenschutzrisiken (ii.)
2. Analysieren der Datenschutzrisiken (iii.)
3. Bewertung der Datenschutzrisiken (iv.)
4. (Angemessene) Behandlung von Datenschutzrisiken (v.)
5. Iteration (vi.)

ii. Identifizieren von Datenschutzrisiken[447]

Im Rahmen der Identifikation sind insbesondere die technisch möglichen Sicherheitsvorfälle zu umschreiben, d.h. von welchen Risikoquellen die Schutzziele in Bezug auf die personenbezogenen Daten verletzt werden könnten.[448] Dabei sind auch die entsprechenden Szenarien wie Angriffe, eine missbräuchliche Nutzung oder technische sowie umweltbezogene Stö-

442 Hier findet sich die Datensicherheit in Form der Schutzziele der Risikoidentifikation: Verfügbarkeit, Vertraulichkeit, Integrität sowie bei den Maßnahmen u.a. mit dem Zugangsschutz, der Reduktion von Schwachstellen und dem Schutz vor Schadsoftware, DIN, ISO/IEC 29134:2020, S. 27, 34; siehe hierzu auch: *Trautwein/Kurpierz*, PinG 2018, 26 (29).

443 Art.-29 Datenschutzgruppe, WP 248 Rev. 01, 04.10.2017, Anhang 1, S. 27.

444 DSK, Standard-Datenschutzmodell, S. 5 f., das auch ausdrücklich auf die Anforderungen nach Art. 32 DSGVO, also der Datensicherheit Bezug nimmt.

445 Ein ähnlicher methodischer Ansatz auch u.a. auf ISO 29134 aufbauend findet sich bei: *F. Ritter/Reibach/Lee*, ZD 2019, 531 (531 ff.).

446 Zur Anwendung diese Schritte unter der DSGVO wohl ebenso: *Alt*, Die Sachverständigen 2020, 169 (170).

447 DIN, ISO/IEC 29134:2020, S. 26 f.

448 *Bieker*, DuD 2018, 27 (30).

rungen zu berücksichtigen. Hinsichtlich der möglichen Angriffe kann auch eine Modellierung typischer Angreifer:innen vorzunehmen sein.[449]

iii. Analysieren der Datenschutzrisiken[450]

Bei der darauffolgenden Analyse werden die identifizierten Datenschutzrisiken genauer untersucht. Dies umfasst neben den Kategorien personenbezogener Daten (und damit ihrer Sensibilität sowie den drohenden Schäden bei Datensicherheitsverletzungen) auch die möglichen oder bekannten Schwachstellen sowie die Bedrohungen, die diese Schwachstellen ausnutzen können. Daraus sind die für das Risiko konstituierenden Eintrittswahrscheinlichkeiten (ggf. anhand zuvor beschriebener Kette von Ereignissen) sowie die Folgenschwere zu bestimmen, d.h. ihnen werden bestimmte Werte zugewiesen. Die Analyse kann dabei insbesondere qualitativ (d.h. durch bestimmte, deskriptive Kategorien (hoch, mittel, gering) als auch quantitativ, insbesondere auf Basis von empirischen Daten oder spieltheoretischen Berechnungen erfolgen.[451]

Wie bei der Auswahl von toM ist auch schon bezüglich des Risikomanagements als Verfahren der Grundsatz der Verhältnismäßigkeit zu wahren. Insofern muss der Normauftrag dahingehend restriktiv ausgelegt werden, dass nicht jedes noch so versteckte Risiko identifiziert und analysiert werden muss, sondern nur soweit sich dies im Rahmen eines *„vernünftigen Aufwands"*[452] bewegt.

iv. Bewerten von Datenschutzrisiken[453]

Im Rahmen der Bewertung der Datenschutzrisiken werden diese anhand der analysierten Eintrittswahrscheinlichkeiten und Schadensschwere priorisiert, d.h. es wird festgelegt welche Risiken in welcher Reihenfolge behandelt werden sollen. Dafür wird eine „Datenschutzrisikokarte" erstellt, in der die Risiken mit *Eintrittswahrscheinlichkeit* und *Auswirkungsgrad*

449 *Bieker*, DuD 2018, 27 (30).
450 DIN, ISO/IEC 29134:2020, S. 27 ff.
451 *Werner*, in: Baumgärtel/Kiparski, DGRI-Jahrbuch 2021/2022, 161 (169 f.), Rn 33 f.
452 Zu dem Begriff später noch vertieft: S. 170 ff.
453 DIN, ISO/IEC 29134:2020, S. 29 f.

gekennzeichnet werden (sind beide Faktoren als „hoch" zu bewerten, hat die Behandlung eine höhere Priorität als wenn einer oder beide Faktoren als „mittel" oder als „niedrig" zu bewerten sind).[454]

v. (Angemessene) Behandlung von Datenschutzrisiken

Für die Risikobehandlung stehen vier Optionen zur Auswahl: Risikoreduktion,[455] Risikobeibehaltung, Risikovermeidung und Risikoübertragung,[456] wobei Art. 32 DSGVO regelmäßig eine Risikoreduktion oder notfalls eine -vermeidung (keine oder zumindest eine eingeschränkte Verarbeitung personenbezogener Daten) fordern dürfte.[457]

Soweit eine Risikoreduktion erforderlich ist, müssen so lange technische und organisatorische Maßnahmen getroffen werden, bis das verbleibende Restrisiko „akzeptabel" ist[458] bzw. bis nach dem Wortlaut der DSGVO ein „dem Risiko angemessenes Schutzniveau" hergestellt wurde.

Hierfür ist eine Abwägung zwischen dem Aufwand („Implementierungskosten") der Maßnahmen und dem hierdurch erreichten Nutzen in Form der Risikoreduktion (Eintrittswahrscheinlichkeit x Folgenschwere vor/nach Maßnahme) erforderlich.[459] Diese Risikoreduktion kann quantitativ auch

454 Vgl. DIN, ISO/IEC 29134:2020, S. 29 f., S. S. 56 f.; eine solche „Risikokarte" findet sich auch als „Risikomatrix" in: DSK, Kurzpapier Nr. 18, 26.04.2018, S. 5.

455 Zu beachten ist, dass der Begriff Risikoreduktion missverständlich sein kann, da (geeignete) Maßnahmen das Risiko zwar insgesamt reduzieren, aber z.T. auch andere Risiken schaffen oder erhöhen könnten; Vgl. *Bieker*, DuD 2018, 27 (31); so könnte etwa eine Maßnahme zur Erkennung von manipulierten Informationen das Risiko erhöhen, dass aufgrund der Fehlerquote (false-positive) „zutreffende Informationen" aussortiert werden.

456 DIN, ISO/IEC 29134:2020, S. 31.

457 Eine Risikobeibehaltung ist nur möglich, wenn die bereits vorhandenen Maßnahmen ausreichen, etwa wenn die Methodik als Iteration (dazu sogleich) durchgeführt wird. Eine Risikoübertragung etwa durch eine Versicherung (so ausdrücklich in: DIN, ISO/IEC 29134:2020, S. 32) ist hingegen im Sinne der DSGVO keine rechtlich adäquate Option, da der Verantwortliche die Risiken tatsächlich angemessen mindern muss; vgl. zu diesem Rechtsgedanken im KRITIS-Recht: *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 8a BSIG, Rn. 20.

458 Vgl. DIN, ISO/IEC 29134:2020, S. 32.

459 Zumeist bleibt die Beschreibung der Abwägungspunkte sehr vage, so z.B. auch das DIN, ISO/IEC 29134:2020, S. 30; sowie das EDSA, Leitlinien 4/2019 zu Artikel 25, 20.10.2020, Rn. 24. Im dargestellten Sinne neben *Werner*, in: Baumgärtel/Kiparski, DGRI-Jahrbuch 2021/2022, 161 (168 ff.), Rn. 29 ff.; bereits ähnlich: *Jergl*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018,

wiederrum als Differenz der Risikokosten (vor/nach Maßnahme) und somit als Kostenwert ausgedrückt werden.

Die daraus resultierende *Kosten-Nutzen-Abwägung* verhilft auch dem grundrechtlichen Verhältnismäßigkeitsprinzip zur Geltung.[460] Dabei werden die Maßnahmen in der Datensicherheit nach Art. 32 Abs. 1 DSGVO zumeist die Eintrittswahrscheinlichkeit eines Ereignisses (und damit auch eines Schadenseintritts) reduzieren, z.B. durch das Schließen einer Schwachstelle bzw. durch den Aufbau größerer und besserer Sicherheitsmechanismen, die bei einem Angriff überwunden werden müssen.

Im Ergebnis sind die zur Risikoreduktion getroffenen Maßnahmen angemessen und das verbleibende Restrisiko „akzeptabel", wenn die Vornahme weiterer Maßnahmen einen im Vergleich zur damit zu erreichenden Risikoreduktion unverhältnismäßigen Aufwand begründen würde,[461] also insbesondere hohe Kosten aufweisen würde ohne die Eintrittswahrscheinlichkeit signifikant zu senken.

vi. Iteration

Dieser in ISO/IEC 29134 als „Reflektieren von Prozessänderungen" bezeichnete[462] und in Art. 32 Abs. 1 lit d) und Art. 35 Abs. 11 DSGVO niedergelegte Schritt enthält Vorgaben zur Iteration des Risikomanagements. So ist das Risikomanagement zum einen zu aktualisieren, wenn sich die Sachlage hinsichtlich der Datenverarbeitungsprozesse ändert,[463] was als *anlassbezogene Iteration* bezeichnet werden kann. Demgegenüber steht die - in ISO/IEC 29134 vorgesehene, aber gesetzlich nicht vorgeschriebene- *turnusmäßige Iteration*, wonach das Risikomanagement in festen Zeitabständen

---

Art. 32, Rn. 52 ff.; nach a.A. wird nur auf die absolute Höhe der Risiken abgestellt, so wohl *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 95, insofern dürfe kein „eklatantes Missverhältnis" zu den Kosten bestehen. Das Abstellen auf die Risikoreduktion ermöglicht hingegen eine präzisere Anknüpfung an die Maßnahmen, die gerade nach ihrem Nutzen, also ihrer Risikoreduktion ausgewählt und vorgenommen werden müssen.

460 *Werner*, in: Baumgärtel/Kiparski, DGRI-Jahrbuch 2021/2022, 161 (165), Rn. 17; vgl. auch: *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 20.

461 Vgl. auch *M. Lang*, in: Taeger/Gabel, DSGVO - BDSG, 4. Auflage 2022, Art. 24, Rn. 63 wonach Maßnahmen das Risiko auf ein angemessenes Maß reduzieren müssen.

462 DIN, ISO/IEC 29134:2020, S. 39.

463 Wie zuvor.

überprüft werden soll.[464] Ungeachtet dessen wird zumindest ein „stetig laufendes Verfahren zur Überwachung datenschutzrechtlicher Risiken" vorgegeben.[465]

Mit Blick auf die Datensicherheit müssen dabei nicht nur Prozessänderungen, sondern auch Änderungen in der Datensicherheitslage, d.h. insbesondere das Auftauchen neuer Sicherheitsrisiken, berücksichtigt werden.[466] Steht mithin neues Wissen über Risiken zur Verfügung, etwa durch neu bekannt gewordene Schwachstellen, ist das Risikomanagement diesbezüglich zu aktualisieren und ggf. die Risikobehandlung dementsprechend anzupassen. Insofern wird hier *explizites Wissen* über neue spezifische Risiken (Risikowissen) verfügbar.[467]

d. Gegenüberstellung der Resilienz

Fraglich ist, wie sich die Resilienz in Begriff und Methodik des Risikos nach der DSGVO bzw. der ISO/IEC 29134 einfügt. Dabei wird zunächst herausgearbeitet, dass sich die Resilienz, wie schon in der Wortlautauslegung angedeutet, anders als das Risiko definitorisch mit der Bewältigung von Ungewissheit befasst (i.). In einem weiteren Schritt wird dann das Verhältnis der Resilienz zum Risikomanagement geklärt (ii.).

i. Resilienz als Umgang mit Ungewissheit

Das Risiko befasst sich nach seiner Definition und wie auch in der Methodik gezeigt wurde mit hinreichend bekannten und beschreibbaren Vorgängen (Einwirkungen, die auf Schwachstellen treffen, führen zu Ereignissen, bei denen Schutzziele verletzt werden (Sicherheitsvorfälle), welche ihrerseits Auswirkungen auf Schutzgüter haben können). Risiken beschreiben mithin Vorgänge, die sich im Vorfeld antizipieren bzw. kalkulieren lassen[468]

464 DIN, ISO/IEC 29134:2020, S. 39; *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 35, Rn. 73.
465 *Rath/Feuerherdt*, CR 2017, 500 (503); *Baumgartner*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 35, Rn. 77.
466 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 35, Rn 73.
467 Zur Abgrenzung des impliziten Wissens siehe: S. 183 f.
468 *Luhmann*, Soziologische Aufklärung 5, S. 129; *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (52).

und denen daher im Rahmen der Angemessenheit mit spezifischen Gegenmaßnahmen begegnet werden kann.

Nachfolgend soll die Ungewissheit zunächst genauer beschrieben werden. So lassen sich verschiedene Formen von Ungewissheit ausmachen (1) und die Ungewissheit kann sich auf unterschiedliche Aspekte, namentlich die Eintrittswahrscheinlichkeiten und/oder die Schwere von Ereignissen beziehen (2). Unter (3) wird dann dargestellt, ob und inwieweit die Resilienz eine Antwort auf diese Ungewissheit geben kann. Schließlich (4) wird beschrieben, wie sich die Resilienz mit der Adressierung der Ungewissheit zum Risikobegriff in Art. 32 DSGVO verhält, dem dort wie gezeigt eine übergeordnete Rolle (Schutzzweck des Art. 32 DSGVO: Gewährleistung eines dem Risiko angemessenen Schutzniveaus) zukommt.

(1) Ungewissheit als (Un)bekanntheit und (Nicht)-Wissen

Allerdings gibt es insbesondere in der Daten- und IT-Sicherheit Situationen, die nicht hinreichend als Risiken antizipiert werden können und die tradierte Risikomethodik somit an ihre Grenzen bringen.[469] Basierend auf einer Differenzierung in der *Entscheidungstheorie* kann man diesbezüglich in Abgrenzung zu den soeben skizzierten Entscheidungen unter Risiko (Entscheidung unter Unsicherheit)[470] von Entscheidungen unter Ungewissheit sprechen.[471] Die Ungewissheit drückt dabei aus, dass der *Entscheider*

469 *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (2); *Collier et al.*, Computer 2014, 70 (70).

470 *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (51 f.).

471 *G. Menges*, Statistische Hefte 1963, 151 (152); *Boeckelmann/Mildner*, SWP-Zeitschriftenschau Sep. 2011, 1 (1 f.); *Gigerenzer*, in: Fleischer, Rationale Entscheidungen unter Unsicherheit, 1 (2 ff.); *Knight*, Risk, Uncertainty and Profit, S. 19 f.; *Nell*, Wahrscheinlichkeitsurteile in juristischen Entscheidungen, S. 127 f.; *Bamberg/Coenenberg/Krapp*, Betriebswirtschaftliche Entscheidungslehre, S. 19; die Verwendung des Terminus „Ungewissheit" in hier vertretener Abgrenzung zur „Unsicherheit/Risiko wird in der Literatur zur Sicherheitsforschung uneinheitlich bewertet. Nicht abschließend zu nennen sind insoweit: *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (46 f.), der Ungewissheit als Unterfall von Unsicherheit definiert oder *Schmid*, in: Pelizäus/Nieder, Das Risiko – Gedanken übers und ins Ungewisse, 31 (55) der von Ungewissheit spricht, wenn nur Wissen über die Eintrittswahrscheinlichkeit fehlt und von Unsicherheit spricht, wenn das Wissen sowohl über Eintrittswahrscheinlichkeit als auch Folgen fehlt; *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (61 ff.) unterscheidet mit grundlegendem Verweis auf *Beck*, Risikogesellschaft, S. 17, 28 f. zwischen alten, bekannten und beherrschbaren Risiken einerseits sowie neuen, teilweise unbekannten und unbeherrschbaren Risi-

– also hier der zur Gewährleistung der Datensicherheit verpflichtete Verantwortliche - kein (vollständiges) Bild der Realität hat,[472] also dass kein Wissen vorhanden ist bzw. er keinen Zugang zu vorhandenem Wissen hat.[473] Konkret fehlt ihm hier das Wissen darüber, ob, weshalb und mit welcher Wahrscheinlichkeit es zu einem schädigenden Ereignis kommt und welche Auswirkungen dieses hat.[474] In Abgrenzung zum Risiko liegt Ungewissheit mithin vor, wenn sich die Eintrittswahrscheinlichkeit und/oder die Folgenschwere eines Ereignisses nicht mehr qualitativ oder quantitativ analysieren lassen[475] oder bereits das Ereignis selbst nicht als mögliches Risiko identifiziert werden konnte. Rechtlich maßgeblicher Zeitpunkt für die Frage der Ungewissheit ist dabei der Zeitpunkt der Maßnahmenwahl. Im Weiteren ist außerdem zwischen zwei Formen oder *Ordnungen von Ungewissheit* zu differenzieren:[476]

Als (Un)gewissheit erster Ordnung wird hier das abstrakte Vorhandensein bzw. Nichtvorhandensein von Wissen über den Sachgegenstand, also Ereignisse und Umstände, welche für die Gewährleistung der Datensicherheit von Bedeutung sind, definiert. Diese (Un)gewissheit erster Ordnung wird für diese Untersuchung als *Wissen*[477] *bzw. Nicht-Wissen* bezeichnet.

---

ken andererseits; *Scherzberg*, in: Engel/Halfmann/Schulte, Wissen, Nichtwissen, unsicheres Wissen, 113 (117), bezeichnet Ungewissheit im hier verwendeten Sinn als „unkalkulierbarer Ungewissheit" und Unsicherheit/Risiko als „kalkulierbare Ungewissheit". Jedenfalls zum Teil mag diese Uneinheitlichkeit auch auf unterschiedliche Übersetzungen des englischen Worts „uncertainty" (Unsicherheit/Ungewissheit) zurückzuführen sein, wobei die Übersetzung mit „Ungewissheit" den Kern des mangelnden Wissens besser beschreibt, *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 20.

472 *G. Menges*, ebd.; *Nell,* ebd.; vgl. auch weiter ausdifferenzierend: *W. Walker et al.*, Integrated Assessment 2003, 5 (8 ff.).

473 Vgl. *Wollenschläger*, Wissensgenerierung im Verfahren, S. 33; als „Mangel an Information zur Ausgangslage oder zu zukünftigen Entwicklungen" *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 19.

474 Vgl. *Kolliarakis*, in: Jeschke/Jakobs/Dröge, Exploring Uncertainty, 313 (317); *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (118 f., 122).

475 *Lamker*, Unsicherheit und Komplexität in Planungsprozessen, S. 85.

476 Grundlegend wurde diese Unterscheidung in (un)known (un)knowns vom US-Verteidigungsminister Donald Rumsfeld populär gemacht, DoD, News Briefing - Secretary Rumsfeld and Gen. Myers, 12.02.2002; als Konzept bestand sie allerdings bereits zuvor und wurde u.a. von der NASA verwendet: NASA, Program Management and Procurement Procedures and Practices, 24.06.1981, S. 73 f.

477 Klarstellend sei an dieser Stelle darauf hingewiesen, dass der Begriff des Wissens sich hier auf das Wissen über die Datensicherheitsgewährleistung bezieht, nicht auf

Im Falle des Nicht-Wissens ist weiter zu differenzieren: Das Wissen ist entweder nicht vorhanden, weil es jeweils zum Zeitpunkt der Entscheidung absolut nicht existiert oder aber die Hebung dieses Wissens ist nicht mehr mit *vernünftigem Aufwand* möglich. Diese Einschränkung des Wissensbegriffs ergibt sich aus dem Kontext des Datensicherheitsrechts, der somit einen relativen und keinen absoluten Wissensbegriff fordert: Denn der Normauftrag muss den Adressaten als Entscheider zum Ausgangspunkt nehmen und dieser kann Wissen nur insoweit innehaben, als dieses objektiv existiert und er dieses auch mit vernünftigem Aufwand erlangen kann. Der vernünftige Aufwand ist insofern Ausdruck des Verhältnismäßigkeitsprinzips und richtet sich nach der Bedeutung der jeweils zu sichernden Schutzgüter.[478]

Die Ungewissheit zweiter Ordnung beschreibt den subjektiven Erkenntniszustand des Entscheiders bzgl. dieses Wissens.[479] Sie beschreibt spezifischer die subjektive Kenntnis des Entscheiders von dem objektiv vorhandenen und mit verhältnismäßigen Aufwand erreichbaren Wissen und wird nachfolgend als *(Un)bekanntheit* bezeichnet. Es adressiert somit insbesondere auch den Fall, dass an sich mit vernünftigem Aufwand zu hebendes Wissen dem Entscheider gleichwohl nicht vorliegt. In welchen praktischen Fällen dies gegeben ist, wird sogleich bei den einzelnen Kategorien erläutert.

Entsprechend dieser Definition lassen sich folgende Kategorien unterscheiden, wobei hier zusätzlich die verbreiteteren englischen Entsprechungen genannt werden:[480]

---

das Wissen über natürliche Personen, welches die personalisierten Dienste verwenden.

478 Der vernünftige Aufwand hat insoweit den gleichen Bezugspunkt wie die abstrakte Angemessenheit (S. 182 f.). Da auf der anderen Seite der Abwägung aber hier nicht der Aufwand für konkrete toM zur Sicherheitsgewähr, sondern die Reichweite des Verfahrens der Risikoidentifikation und -analyse steht erscheint es sinnvoll, hier zwei unterschiedliche Begriffe zu nutzen.

479 Dies wird auch als „epistemologischer Status" bezeichnet: *Daase/Kessler*, Security Dialogue 2007, 411 (413); *Wollenschläger*, Wissensgenerierung im Verfahren, S. 33 spricht insoweit von einem „bewussten oder unbewussten Mangel an Wissen" .

480 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 57 ff; diese sprechen sprachlich nur von „Bekanntheit"; mit von hiesiger Verwendung teilweise abweichender inhaltlicher Ausgestaltung der Kategorien: *Daase/Kessler*, Security Dialogue 2007, 411 (413 ff.); *Boeckelmann/Mildner*, SWP-Zeitschriftenschau Sep. 2011, 1 (2 f.).

Known	Knowns	=	bekanntes	Wissen (Risiko)
Known	Unknowns	=	bekanntes	Nicht-Wissen
Unknown	Knowns	=	unbekanntes	Wissen
Unkown	Unknowns	=	unbekanntes	Nicht-Wissen

Zunächst beschreibt die Kategorie des *bekannten Wissens* (Known Knowns) die Risiken und gehört somit mangels Vorliegens eines Wissensdefizits gerade nicht zur Ungewissheit. Das Wissen über Risiken ist durch Empirie oder fundierte Schätzung objektiv vorhanden bzw. erzeugbar und dieses Wissen ist dem Entscheider auch bekannt. Es handelt sich somit zwar immer noch um eine Entscheidung unter Unsicherheit, da der Eintritt des Ereignisses nicht sicher feststeht; der Entscheider verfügt aber vollständig über das Wissen, was er zum Zeitpunkt der Entscheidung (Maßnahmenwahl) haben kann.[481]

Die Kategorie des *bekannten Nicht-Wissens* (Known Unknowns) beschreibt den Zustand, bei welchem der Entscheider Kenntnis davon hat, dass ihm über bestimmte Umstände kein Wissen vorliegt.[482] Dies kann zum einen daran liegen, dass die zum gegenwärtigen Zeitpunkt bestehenden *absoluten Grenzen der wissenschaftlichen Erkenntnisfähigkeit* erreicht sind (exemplarisch bei dem Blackbox-Charakter von KI-Systemen, der zumindest in Ansätzen versucht wird durch sog. erklärbare, künstliche Intelligenz (en: explainable AI) zu durchbrechen[483]).

Zum anderen muss Wissen (über Risiken), wie bereits angerissen, nur im Rahmen des *vernünftigen Aufwands* gehoben werden: Diese Grenze kann etwa bei sehr hoher Komplexität von Systemen[484] erreicht werden, da diese Systeme bei einer antizipierten Betrachtung nur stark vereinfacht modelliert werden können und dabei bestimmte Annahmen getroffen werden müssen, wie etwa dass Wechselwirkungen zwischen den Komponenten nur schwach ausgeprägt sind und das Verhalten der Komponenten

481 Teilweise gleichwohl auch als Entscheidungen unter Ungewissheit bezeichnet: *Schneeweiß*, Entscheidungskriterien bei Risiko, S. 1, 12, 27. Zur begrifflichen Vielfalt bei Unsicherheit/Ungewissheit: siehe Fn. 471.

482 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 59.

483 *Adadi/Berrada*, IEEE Access 2018, 52138 (52138 ff.).

484 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 59; zur Resilienz als Antwort Vgl. *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (12); *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (12).

linear ist.[485] Solche komplexen Systeme weisen mitunter sogar Eigenschaften auf, die über die Eigenschaften ihrer Komponenten hinausgehen (sog. Emergenz)[486] und folglich auch nicht alleine durch eine Betrachtung ihrer Komponenten erklärt werden können. Somit ist das Wissen über komplexe Systeme und ihr zukünftiges Verhalten zumeist unvollständig.[487] Unter diese Fallgruppe dürften auch Situationen fallen, in denen (auch) Dienste oder Informationen von Dritten genutzt werden und der Entscheider keinen Einblick in die Funktionsweise sowie die Sicherheit der Systeme des Dritten hat. Diese Systeme liegen mithin außerhalb seiner *Systemgrenzen*,[488] die den Kontrollbereich des Entscheiders umschreiben.

Die nächste Kategorie ist jene des *unbekannten Wissens* (Unknown Knowns). Charakteristisch ist hier, dass das Wissen über bestimmte Umstände an sich verfügbar bzw. mit vernünftigem Aufwand zu heben wäre. Das Wissen ist dem Adressaten aber jedenfalls unbekannt, d.h. es wurde subjektiv nicht erhoben bzw. zur Kenntnis genommen. Theoretisch ist dieses Defizit somit vermeidbar[489] und wird z.T. mit dem Schlagwort „Ignoranz" umschrieben.[490]

In Erscheinung treten kann diese Kategorie insbesondere bei Fehlern bzw. Schwachstellen in Systemen. Es ist nicht anzunehmen, dass jede Software bereits herstellerseitig fehlerfrei zur Verfügung gestellt wird.[491] Ebenso wenig kann davon ausgegangen werden, dass der Verwender einer solchen Software wie etwa der Verantwortliche all diese Fehler einschließlich insbesondere der Schwachstellen finden und beheben kann; außerdem ist insoweit zu berücksichtigen, dass durch die Behebung mitunter auch unbemerkt andere, neue Fehler in das System eingefügt werden können.[492] Verschuldenstechnisch kann hier ein fahrlässiges Verhalten vorliegen, da

485 *Park et al.*, Risk analysis 2013, 356 (362); *Beckerman*, Systems Engineering 2000, 96 (97).

486 *Hiermaier/Scharte/Fischer*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 155 (156); *Holland*, Complexity, S. 49 ff.

487 *Park et al.*, Risk analysis 2013, 356 (362); *Funtowicz/Ravetz*, Futures 1994, 568 (578); *Berkes*, Nat Hazards, Vol. 41 (2007), 283 (284 f.); *W. Walker et al.*, Integrated Assessment 2003, 5 (9 f.).

488 Dazu bereits S. 114 f.

489 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 61.

490 *Daase/Kessler*, Security Dialogue 2007, 411 (414 f.); *Boeckelmann/Mildner*, SWP-Zeitschriftenschau Sep. 2011, 1 (3).

491 FZI, Wirksame Sicherheitsmaßnahmen für IoT-Produkte, 25.01.2021, S. 10.

492 *Avizienis et al.*, IEEE TDSC 2004, 11 (29).

entweder vorhandenes Wissen oder zumindest mit vernünftigem Aufwand erzeugbares Wissen nicht genutzt wurde.[493] Allerdings liegt dieses Verschulden nicht zwangsläufig beim Verantwortlichen, z.B. wenn er eine fehlerhafte (Soft- oder Hardware-) Komponente einkauft, den Fehler in derselben aber selbst nicht erkennen konnte.

Schließlich verbleibt sog. *unbekanntes Nicht-Wissen* (*Unknown Unknowns),* d.h. drohende Ereignisse, die unvorhersehbar und unerwartet auftreten.[494] Entscheidend ist insoweit insbesondere in Abgrenzung zu dem bekannten Nicht-Wissen*,* dass dem Entscheider nun auch nicht bekannt ist, dass ihm das Wissen über Ereignisse fehlt. Es handelt sich mithin um Ereignisse, von denen er „nicht einmal träumt",[495] d.h. die als solche gänzlich außerhalb seines Erkenntnishorizonts liegen. Sie werden teilweise auch als *Black Swans* bezeichnet; was genauer Ereignisse beschreibt, die aufgrund ihrer (erst im Nachgang feststellbaren und dies ggf. auch rückblickend mit vernünftigem Aufwand) sehr geringen Eintrittswahrscheinlichkeit auch objektiv nicht antizipiert wurden, die aber hohe Schäden zur Folge hatten.[496] Hierunter können etwa global wirkende Sicherheitslücken wie *Heartbleed*[497] in der zur Transportverschlüsselung im Internet weit verbreiteten Software OpenSSL oder *Meltdown*[498] als Hardware-Sicherheitslücke in Mikroprozessoren gefasst werden. Aus Sicht eines Entscheiders außerhalb der mit den jeweiligen IT-Produkten befassten Organisationen[499] handelt es sich hierbei um Nicht-Wissen, da er das Wissen hierüber nicht mit vernünftigem Aufwand hätte erlangen können. Es traf diese Entscheider auch völlig unerwartet (Unbekanntheit), da sie nicht mit einer solch

493 Ist eine Sicherheitslücke hingegen so versteckt (weil sie etwa nur bei beim gleichzeitigen Zusammentreffen vieler Programmzustände eintritt), dass sie mit vernünftigem Aufwand nicht gefunden werden konnte, liegt ein Fall des *bekannten oder unbekannten Nicht-Wissens* vor.

494 *Sharkov*, in: Multari/Singhal/Manz, Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense - SafeConfig'16, 3 (4).

495 *Daase/Kessler*, Security Dialogue 2007, 411 (413).

496 Vgl. *Kolliarakis*, in: Jeschke/Jakobs/Dröge, Exploring Uncertainty, 313 (320); *Hiermaier/Scharte/Fischer*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 155 (156); *Taleb*, Der Schwarze Schwan, S. 1 f.

497 *Ghafoor et al.*, in: 17th IEEE International Multi Topic Conference 2014, Analysis of OpenSSL Heartbleed vulnerability for embedded systems, 314 (314 ff).

498 *Lipp et al.*, CACM, Vol. 63 (2020), Heft 6, 46 (46 ff.).

499 Aus deren Sicht mag es sich hingegen um *unbekanntes Wissen* gehandelt haben, da die Sicherheitslücken möglicherweise auch mit vernünftigem Aufwand hätten festgestellt werden können; wird dies verneint, wäre es auch aus deren Sicht ein Fall *unbekannten Nicht-Wissens.*

schweren und übergreifenden Sicherheitslücke in einer global eingesetzten (open-source) Komponente rechneten.[500]

Alle drei Kategorien die sich mit Unbekanntheit und/oder Nicht-Wissen befassen, sind dem Oberbegriff des „Entscheidens unter Ungewissheit" (en: unknown) zuzuordnen, da in jedem Falle ein Mangel im Erkenntniszustand vorliegt. Im Ergebnis ergibt sich somit folgende Matrix:[501]

Tabelle 4: Kategorien von Ungewissheit

	Wissen	Nicht-Wissen
bekannt	**Bekanntes Wissen** ***Entscheiden unter*** Risiko ***(Unsicherheit)*** Dem Entscheider ist vorhandenes Wissen bekannt.	**bekanntes Nicht-Wissen** ***Entscheiden unter Ungewissheit*** Dem Entscheider ist das Nicht-Wissen bekannt.
unbekannt	**unbekanntes Wissen** ***Entscheiden unter Ungewissheit*** Dem Entscheider ist vorhandenes Wissen unbekannt.	**unbekanntes Nicht-Wissen** ***Entscheiden unter Ungewissheit*** Selbst das Nicht-Wissen ist dem Entscheider nicht bekannt.

(2) Was ist unbekannt und worüber besteht kein Wissen?

In einem weiteren Schritt soll genauer beschrieben werden, worauf sich die (*Un)bekanntheit* sowie das *(Nicht-)Wissen* beziehen können. Ausgehend von den Dimensionen des Risikos ist nur dann von *bekanntem Wissen* also einem antizipationsfähigen Risiko zu sprechen, wenn sowohl Wissen zur Eintrittswahrscheinlichkeit als auch zur Folgenschwere beim Entscheider vorliegt oder zumindest (mit vernünftigem Aufwand) gehoben werden kann. Bezüglich der Unbekanntheit bzw. des Nicht-Wissens lassen sich somit drei Kategorien zusammenfassen:

Zunächst kann das Ereignis *gänzlich unbekannt sein bzw. keinerlei Wissen darüber existieren*. Hierunter fallen insbesondere Ereignisse im Bereich

500 Geht man hier (abweichend von den genannten Beispielen) von einem schuldhaften Verkennen aus, d.h. dass dem Normadressaten der Umstand des Nicht-Wissens hätte bekannt sein müssen (bekanntes Nicht-Wissen), kann ihm das Unterlassen entsprechender spezifischer Resilienzmaßnahmen als unzureichende Sicherheitsgewährleistung vorgehalten werden.

501 Vgl. *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, Abb. 3, S. 57.

das sog. *unbekannten Nicht-Wissens*. Auch in Fällen unbekannten Wissens fehlt dem Entscheider jegliche *Kenntnis, wenn Schwachstellen vollständig übersehen wurden* (theoretisch aber hätten erkannt werden können). Schließlich könnten auch Fälle des *bekannten Nicht-Wissens* hierunterfallen, etwa beim bereits angesprochenen Einsatz von ML-Systemen, bei dem sich aufgrund des Blackbox-Charakters weder die Wahrscheinlichkeit noch der Grad möglicher Abweichungen (und damit auch die Folgenschwere) der Ergebnisse sicher vorhersagen lässt.

Zweitens kann Wissen *nur bezüglich der Eintrittswahrscheinlichkeiten* eines Ereignisses nicht aber bzgl. der Folgenschwere bestehen bzw. bekannt sein.[502] Beispielsweise kann in Fällen des *bekannten Nicht-Wissens* zwar die Eintrittswahrscheinlichkeit eines Ereignisses (z.B. der Ausfall bzw. die Manipulation eines Dienstes bekannt sein, allerdings kann die Folgenschwere in einem sehr komplexen, offenen System nicht vorher antizipiert werden, etwa wenn Dienstergebnisse später auch von unbekannten Drittdiensten genutzt werden.[503]

Drittens kann das Wissen umgekehrt *nur bezüglich der Folgenschwere* bestehen, nicht aber bzgl. der Eintrittswahrscheinlichkeit. Dies ist anzunehmen, soweit das Wissen über ein mögliches Ereignis und seine Folgen (z.B. die Folgen des Ausfalls einer Komponente) besteht, nicht aber darüber, wie wahrscheinlich es ist, dass es zu diesem Ereignis kommt. Dies ist besonders häufig bei Ereignissen anzutreffen, die durch menschliche Angreifer:innen verursacht werden, da häufig kein Wissen über deren Anzahl, Motivation und Fähigkeiten vorhanden ist. Spieltheoretische Berechnungen[504] können dabei die Ungewissheit zwar reduzieren, aber zumeist nicht vollständig ausschließen. Da dieses Wissensdefizit dem Entscheider bekannt ist, handelt es sich um einen Fall des *bekannten Nicht-Wissens*.

---

502 *A. Eckhardt/Rippe*, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, S. 33 vertreten hierzu die Auffassung, man könne in diesen Fällen auch von einem sehr hohen oder sogar dem höchstmöglichen Schadensausmaß ausgehen. Dies ebnet den Weg zurück in das Risikomanagement.

503 Der soeben genannte Fall unbekannten Wissens mit den übersehenen Schwachstellen kann hierunter hingegen nur selten fallen: Denkbar ist zwar die Eintrittswahrscheinlichkeit aus Statistiken über die generelle Häufigkeit von Schwachstellen abzuleiten; mangels konkreter Kenntnis der Schwachstelle kann aber die ebenso wichtige Ausnutzungswahrscheinlichkeit derselben nicht bestimmt werden und damit bleibt am Ende (auch) die Eintrittswahrscheinlichkeit eines Ereignisses infolge übersehener Schwachstellen ungewiss.

504 *Beyerer/Geisler*, EJSR 2016, 135 (138 f.).

Soweit Eintrittswahrscheinlichkeit und Folgenschwere ungewiss sind, können somit im Ergebnis alle drei Formen der Ungewissheit vorliegen. Ist hingegen nur die Eintrittswahrscheinlichkeit oder Folgenschwere ungewiss, ist stets ein Fall des bekannten Nicht-Wissens gegeben.

(3) Resilienz als spezifische Antwort

Insgesamt zeigt sich somit, dass ein großer Bereich besteht, in dem das Wissen des Entscheiders über Risiken gänzlich fehlt oder unvollständig bleibt und er mit dem Risikomanagement somit nicht alle drohenden Einwirkungen behandeln kann. Die Resilienz kann nun eben diesen ungewissen Ereignissen entgegengesetzt werden, die sich infolgedessen, dass sie sich nicht vorher als Risiko antizipieren und verhindern lassen, manifestieren können.[505] Umgekehrt kann zur Abgrenzung auch formuliert werden: Um antizipationsfähigen Ereignissen (Risiken) zu begegnen, ist keine Resilienz erforderlich,[506] dies ist vielmehr tradierter Bestandteil bei der Gewährleistung von Datensicherheit (und Sicherheit im Allgemeinen). Die Resilienz tritt vielmehr als Komplementär zum klassischen Risikomanagement auf,[507] welches bei ungewissen, d.h. unbekannten Ereignissen und solchen bei denen es an dem notwendigen Wissen fehlt, an seine Grenzen stößt.

Eine weitere Unterscheidung ergibt sich aus dem Betrachtungsraum: Durch seine Beschränkung auf Risiken ist das Risikomanagement auf die Betrachtung singulärer Vorgänge beschränkt, die sich als Ketten von Einwirkung, Schwachstelle und Ereignis bis hin zum Schaden beschreiben lassen. Insbesondere die Analyse der informationstechnischen Systeme hinsichtlich der möglichen Einwirkungen und Schwachstellen bis zum (zu verhindernden) Ereignis wird bereits seit langem durch sog. Angriffs-

505 Vgl. *Wildavsky*, Searching for safety, S. 85; *Fritz*, Resilienz als sicherheitspolitisches Gestaltungsbild, S. 102; *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (118); Resilienz als Antwort insbesondere auf „unvorhergesehene Störungen" bei *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39 bzw. „nicht vorhergesehene Änderungen in den Abläufen" bei *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 43.

506 *Scharte*, Resilience Engineering, S. 453.

507 Vgl. *Fritz*, Resilienz als sicherheitspolitisches Gestaltungsbild, S. 23; *Park et al.*, Risk analysis 2013, 356 (357); *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (121).

bäume beschrieben.[508] Oft besteht wie dargestellt bereits kein (vollständiges) Wissen über diese singuläre Ereignisketten (etwa die Existenz von Schwachstellen oder die Motivation möglicher Angreifer:innen). Daneben ist die Beschränkung auf singuläre Ereignisketten auch für die vollständige Sicherheitsgewähr unzureichend,[509] da in komplexen Systemen zusätzlich betrachtet werden muss, welche Auswirkungen daraus resultieren, wenn mehrere betrachtete Ereignisse gleichzeitig eintreten. Da dies aber häufig zu einer unüberschaubaren Anzahl von Kombinationsmöglichkeiten führt, kann dies mitunter nicht mehr mit vernünftigem Aufwand durchgeführt werden. Auch insoweit greift die Resilienz ein und adressiert explizit den Umgang mit dem *Unbekanntem* und der *Ungewissheit*,[510] so dass die Resilienz das Risikomanagement ergänzt und beide Ansätze gemeinsam einen angemessenen Schutz gewährleisten können.[511]

Schließlich ist anzumerken, dass das Risikomanagement wie die Resilienz (nur) eine Methodik bietet (dazu sogleich), welche allein aber noch keine Vorgabe hinsichtlich bestimmter zu wählender Maßnahmen beinhaltet.[512]

(4) Folgen für die Risikodefinition

Wie oben bereits dargestellt ist die Definition des Risikobegriffs in der DSGVO sehr weit gefasst und erstreckt sich von den Einwirkungen auf die Verarbeitung, die zu einer „Verletzung des Schutzes personenbezogener Daten" (Art. 4 Nr. 12 DSGVO) führen können bis zu den finalen Schäden an den Rechten und Freiheiten natürlicher Personen.

Insofern scheint es zunächst auch nachvollziehbar, dass nach Art. 32 Abs. 1 DSGVO die Resilienz nur einen Aspekt darstellt, um diese Risiken im Sinne der Gewährleistung eines „angemessenen Schutzniveaus" zu bewälti-

508 Grundlegend: *Schneier*, Dr. Dobb's journal, Vol. 24 (1999), Heft 12, 21 (21 ff.).

509 *Sheridan, Hum Factors 2008, 418* (421).

510 Nur abstellend auf „Ungewissheit" (en: uncertainties): *Wildavsky*, Searching for safety, S. 85; ähnlich auch *Bröckling*, Resilienz: Über einen Schlüsselbegriff des 21. Jahrhunderts, 2017, S. 14; *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 (2044 f.).

511 *Park et al.*, Risk analysis 2013, 356 (359, 366).

512 Ähnlich auch: *Fritz*, Resilienz als sicherheitspolitisches Gestaltungsbild, S. 90, der insoweit von einem „Formalismus" spricht.

gen. Die Resilienz steht nach diesem Verständnis somit nicht neben dem (antizipationsfähigen) Risiko, sondern ist ein Teil der Risikobewältigungsstrategie.

Allerdings führt dies zu einem Widerspruch, sofern man es für „Risiken" im Sinne der Entscheidungstheorie wie bereits zuvor dargestellt als konstitutiv erachtet, dass sie in Eintrittswahrscheinlichkeit und Folgenschwere im Vorfeld mess- und kalkulierbar[513], also anders als die Ungewissheit gerade antizipierbar sind[514] und so im Sinne der Risikomethodik identifiziert, analysiert, bewertet und behandelt werden können. Die Resilienz als Antwort auf Ungewissheit kann in diesem Fall somit nicht als Teil der Risikomethodik gesehen werden, sondern ist wie bereits dargestellt ein Komplementär hierzu.

Auflösen lässt sich dieses Dilemma mit einer Begriffsauslegung des Risikos, die auch die Ungewissheit einschließt, d.h. auch objektiv unbekannte, mit vernünftigem Aufwand nicht erkennbare und somit weder durch Empirie noch durch Schätzungen hinsichtlich Eintrittswahrscheinlichkeit und Schadensschwere bezifferbare Risiken umfasst. Man kann dies als eine *naturalistische Betrachtungsweise* bezeichnen, mit der anerkannt wird, dass Risiken objektiv nicht ihre Existenz einbüßen, nur weil sie nicht erkannt und infolgedessen auch nicht behandelt werden (können).

Dies entspricht auch der teleologischen und historischen Zielsetzung der DSGVO. Es erscheint zweckwidrig anzunehmen, dass mit der DSGVO nur solche antizipationsfähigen Risiken adressiert und der Verantwortliche bzw. der Auftragsverarbeiter im Übrigen vollständig freigestellt werden sollte, zumal für die Resilienz dann nach dem dargestellten Verständnis kein Raum verbliebe.

ii. Methodische Einordnung

Für die methodische Implementierung gilt aber gleichwohl, dass es bei der Gewährleistung von Resilienz nicht um die Beurteilung und Behandlung antizipierter Risiken gehen kann. Mithin ist die Resilienz auch nicht durch das Risikomanagement abgedeckt, sondern es bedarf insoweit ergänzender bzw. modifizierende Methodiken für den resilienten Umgang mit Ungewissheit.

513 *Luhmann*, Soziologische Aufklärung 5, S. 129; *Bonß*, in: Zoche/Kaufmann/Haverkamp, Zivile Sicherheit, 43 (52).

514 *G. Menges*, Statistische Hefte 1963, 151 (152).

Dabei ist in einem ersten Schritt zu beachten, dass sich die Methodik zur Gewährleistung der Resilienz in Abhängigkeit von den Formen der Ungewissheit unterscheidet (1). Zweitens: Die zu treffenden Resilienzmaßnahmen müssen zwar angemessen sein, allerdings kann die Angemessenheit aufgrund der Ungewissheit gerade nicht auf die Risikoreduktion bezogen werden; auch hier ergeben sich insoweit methodische Unterschiede (2). Weiterhin stellt sich die Frage, wie bei einem Wissenszuwachs zwischen Risikomanagement (Iteration) und Resilienzmethodik (Lernen) zu differenzieren ist (3). Am Ende schließt dieser Abschnitt mit einer Zusammenfassung von Risikomanagement und Resilienzmethodik (4).

(1) Adressierung unterschiedlicher Formen der Ungewissheit

Hinsichtlich der Entwicklung einer Resilienzmethodik muss zunächst zwischen den unterschiedlichen Formen der Ungewissheit wie sie in Abschnitt i.(1)[515] dargestellt wurden, differenziert werden. Hierfür sind im Ergebnis zwei unterschiedliche methodische Ansätze erforderlich:

Mit dem ersten Ansatz ist mit Blick auf das *unbekannte Wissen* und das *unbekannte Nicht-Wissen* zu untersuchen, welche Beeinträchtigungen wesentlicher Schutzobjekte (etwa Daten oder Systeme sowie deren Komponenten und Schnittstellen) unabhängig von den ungewissen Ursachen eines Ereignisses zu hohen Auswirkungen für die Schutzgüter führen können, mithin kritisch sind.[516] In Abhängigkeit von dieser Kritikalität sind dann im Rahmen der abstrakten Angemessenheit (dazu sogleich) entsprechende Resilienzmaßnahmen zu ergreifen, um diese Schutzobjekte besonders zu sichern.

Der zweite methodische Ansatz der Resilienz richtet sich auf das *bekannte Nicht-Wissen*. Die klassische Risikomethodik steht insoweit nach wie vor an erster Stelle: Zunächst sind die Risiken, die als solche antizipiert werden können, d.h. über die Wissen vorliegt oder zumindest erzeugt werden kann, im Rahmen der „klassischen" Risikomethodik zu bewältigen. Soweit sich im Rahmen der Risikoidentifikation und -analyse aber herausstellt, dass ein

515 S. 170 ff.

516 Vgl. *Sharkov*, in: Multari/Singhal/Manz, Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense - SafeConfig'16, 3 (5); *Alderson*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 66 (71).; *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (126).

Bereich des bekannten Nicht-Wissens besteht[517] sind hierfür entsprechende Resilienzmaßnahmen vorzusehen. Für den Umfang der Maßnahmen ist wiederrum auf die Kritikalität des jeweiligen, mit Ungewissheit behafteten Schutzobjekts[518] im Rahmen der abstrakten Angemessenheit (dazu sogleich) abzustellen. Der Unterschied zum ersten Ansatz liegt darin, dass sich anhand der Risikomethodik der Bereich der Ungewissheit bereits entsprechend als bekanntes Nicht-Wissen eingrenzen lässt.

Als Zwischenfazit lässt sich insoweit festhalten: Die Resilienz steht nicht losgelöst von der klassischen Risikomethodik, sondern ergänzt diese hinsichtlich bestehender Ungewissheit. Sowohl mit der Resilienz als auch der Risikomethodik wird eine Reduktion der naturalistischen Risiken für die jeweiligen Schutzgüter angestrebt. Der Unterschied besteht darin, dass die Resilienz kein Wissen über die spezifischen Einzelrisiken voraussetzt. Sofern ein Fall des bekannten Nicht-Wissens vorliegt, ergibt sich bereits aus der Risikoidentifikation und -analyse hinsichtlich welcher Schutzobjekte Ungewissheit besteht. Hinsichtlich unbekannten Wissens und unbekannten Nicht-Wissens ist hingegen eine selbstständige Kritikalitätsanalyse durchzuführen, d.h. welche Schutzobjekte für die jeweiligen Schutzgüter von besonderer Bedeutung sind und somit auch in Ungewissheit konkreter Risiken besonders geschützt werden müssen.

(2) Angemessenheit von Resilienzmaßnahmen

Im Ergebnis zielt die Risikomethodik der DSGVO wie bereits voranstehend beschrieben auf die Herstellung eines „angemessenen Schutzniveaus". Die Angemessenheit ist dabei ein Ausdruck des Verhältnisses von Aufwand bzw. Kosten der Maßnahmen und der damit erreichten Risikoreduktion.[519]

Das Verhältnismäßigkeitsprinzip muss an sich auch für die Resilienzmaßnahmen gelten. Allerdings kann der Nutzen von Resilienzmaßnahmen nicht in Form der Risikoreduktion bemessen werden, da diese wie die Risiken selbst unbekannt bzw. ungewiss ist. Um den Auftrag zu Resilienzmaßnahmen auch mit Blick auf die kritischen Schutzobjekte nicht grenzenlos

517 Vgl. *Scherzberg*, in: Engel/Halfmann/Schulte, Wissen, Nichtwissen, unsicheres Wissen, 113 (137), der fordert, dass „erkennbare Ausmaß des Nichtwissens" im Risikomanagement zu berücksichtigen.

518 Je nach Einwirkungsmöglichkeit des Schutzobjekts, bei dem ein Nicht-Wissen erkannt wurde sind mehr oder weniger Resilienzmaßnahmen erforderlich.

519 Siehe hierzu bereits S. 167.

werden zu lassen, muss dem Aufwand folglich ein anderer Anknüpfungspunkt zur Abwägung gegenübergestellt werden.

Als Alternative zur Bemessung des Nutzens in Form der konkreten Risikoreduktion bietet es sich insofern an auf die Schutzgüter, mithin die Rechte und Freiheiten natürlicher Personen an sich abzustellen. Insoweit ist zu untersuchen, welche (Kategorien von) Schutzgüter(n) betroffen sind (in der DSGVO stets Grundrechte, z.B. das Datenschutzgrundrecht oder das Diskriminierungsverbot)[520] und welche Beeinträchtigungen an diesen drohen. Dies ergibt sich gemäß Art. 32 Abs. 1 DSGVO aus *der Art, dem Umfang, der Umstände und der Zwecke der Verarbeitung*.[521] Dabei ist bei personalisierten Diensten auch auf die jeweiligen Entscheidungen abzustellen (z.B. Personalisierung von Produktwerbung oder aber die Personalisierung eines politischen Informationsangebots). Es kann außerdem angenommen werden, dass die Bedrohung der Schutzgüter umso intensiver ist, je mehr und je sensiblere Daten verarbeitet werden bzw. je weiter der als Verarbeitungszweck erbrachte Dienst in die persönliche Lebenssphäre der betroffenen Personen hineinreicht.[522] Dabei sind auch die aus der Verarbeitung allgemein resultierenden *Schäden bzw. Schadkategorien* (EG 75 DSGVO) zu berücksichtigen.

Diese Betrachtung, in der die Kosten für Resilienzmaßnahmen zu der abstrakten Exposition ins Verhältnis gesetzt werden, kann als *„abstrakte Angemessenheit"* bezeichnet werden. Demgegenüber steht die schon beschriebene *risikobezogene Angemessenheit,* die sich mit den Kosten für Maßnahmen befasst, mit denen die Risiken für antizipierte Ereignisse mit deren Eintrittswahrscheinlichkeiten und Folgen gesenkt werden sollen.

(3) Resilienzlernen und Risikomanagement-Iteration

Wie im Rahmen der Wortlautdefinition herausgearbeitet, umfasst die Resilienz auch die lernende Verbesserung in der Erholungsphase. In Abgrenzung der Resilienz als Antwort auf Ungewissheit zum Risikomanagement ist hierbei besonders zu differenzieren: Das Risikomanagement geht

520 Siehe hierzu bereits S. 106.

521 Als „Steuerungsvariablen der Sicherheitsrelevanz" bezeichnet von: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn 55.

522 Vgl. *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 27; *Freund*, in: Schuster/Grützmacher, IT-Recht 2020, Art. 32 DSGVO, Rn. 20.

zwangsläufig von einem begrenzten Wissen aus, auf dessen Basis die Risiken zunächst identifiziert und anschließend analysiert, bewertet und behandelt werden. Dies ist jedoch kein statischer Zustand: Wird neues Wissen über neue Ereignisse und damit Einzelrisiken verfügbar, so ist das Risikomanagement zu wiederholen (Iteration, s.o.: S. 168). Dieses Lernen (etwa beim Auftauchen und ggf. auch der Ausnutzung einer bislang unbekannten Schwachstelle) durch Schließung derselben ist bereits methodischer Bestandteil des Risikomanagements in Form der Iteration.

Soweit es die Resilienz betrifft, ist das Lernen mithin in systematischer Abgrenzung nur auf die eigentlichen Resilienzmaßnahmen zu beziehen, d.h. auf einen künftigen besseren Umgang mit (weiterhin verbleibender) Ungewissheit (lernende Verbesserung). Es wird insoweit kein *explizites Wissen* über neue Einzelrisiken wie in der Iteration des Risikomanagements genutzt, sondern die Resilienzmaßnahmen werden durch *implizites Wissen* für den Umgang mit Ungewissheit weiter optimiert und verbessert. Implizites Wissen meint im Umkehrschluss kein Wissen über Einzelrisiken, sondern vielmehr übergeordnetes Wissen über Bewältigungsstrategien, die v.a. auf Erfahrung und Intuition basieren.[523]

Kondensiert auf die einzelnen Elemente der Resilienz betrifft dies zunächst die (fortlaufende) Verbesserung der Ereigniserkennung. Heutige ML-basierte Anomalie-[524] und Angriffserkennungssysteme bewältigen ständig Ungewissheit, indem sie die eingehenden Datenflüsse fortlaufend auswerten und sich dabei kontinuierlich verbessern (inkrementelles bzw. online Lernen).[525] Damit sind sie auch für künftige ungewisse Angriffe, etwa durch noch subtiler manipulierte Daten, besser gerüstet. Hier wird insofern auch gerade kein explizites Wissen erzeugt, vielmehr beruhen sie auf der „Erfahrung" des ML-Systems und sind aufgrund des Blackbox-Charakters solcher Systeme auch nicht als explizites Wissen erklärbar. Weiterhin ist eine Verbesserung der Anpassungsmöglichkeiten denkbar, etwa in Form besserer Strategien der Resilienzsysteme (z.B. bei der Netzwerksegmentierung). Schließlich können auch die Erholungsfähigkeiten optimiert werden, etwa in Form einer schnelleren Wiederherstellung des Normalzustandes.

523 Vgl. *Scherzberg*, in: Schuppert/Voßkuhle, Governance von und durch Wissen, 240 (242, 244).

524 Siehe in einem Überblick: *Nassif et al.*, IEEE Access, Vol. 9 (2021), 78658 (78658 ff.).

525 Vgl. *Müller-Quade et al.,* Whitepaper: Künstliche Intelligenz und IT-Sicherheit, April 2019, S. 6 f.

(4) Zusammenfassung der Methodik

Die Resilienz gibt somit insgesamt eine Antwort auf ungewisse Ereignisse, indem sie abstrakt angemessene Maßnahmen zur Sicherung verlangt, mit denen ein Ereignis erkannt, sich daran angepasst oder sich schnellstmöglich davon erholt werden kann.

Resilienz setzt nicht an Einzelrisiken an, sondern auf einer höheren Ebene. Man könnte auch formulieren, dass im Sinne von verketteten Ereignissen die *Resilienz* nicht am Anfang einer oder mehrerer Kausalketten ansetzt, sondern bei einem auf ungewissen Ursachen beruhenden, höherrangigen Ereignis sicherstellt, dass angesichts dessen die Schutzgüter gleichwohl noch gesichert werden. Dies gilt sowohl für die Ungewissheit, die im Rahmen der Risikomethodik zumindest erkannt und eingegrenzt werden kann (bekanntes Nicht-Wissen) als auch für vollständig ungewisse Ereignisse an kritischen Schutzobjekten (unbekanntes Wissen, unbekanntes Nicht-Wissen).

Die Ergebnisse werden in der nachfolgenden Grafik zusammengefasst:

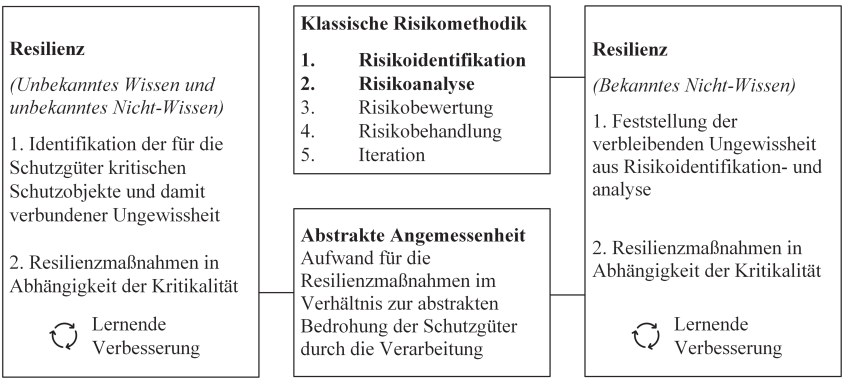

Abbildung 9: Risiko- und Resilienzmethodik

iii. Ergebnis und Folgen für den Resilienzbegriff

Im Ergebnis sind aus der Gegenüberstellung der Resilienz zum Risiko folgende systematische Auslegungsergebnisse festzuhalten:

Zunächst adressiert die Resilienz anders als das Risiko im entscheidungstheoretischen Sinn die Bewältigung von Ungewissheit.[526] Die Ungewissheit besteht dabei aus den Komponenten der (Un)Bekanntheit und des (Nicht-)Wissens: In der Folge bestehen drei Kategorien, namentlich: *bekanntes Nicht-Wissen*, *unbekanntes Wissen* und *unbekanntes Nicht-Wissen*. Bekanntes Nicht-Wissen ist gegeben, wenn Wissen entweder absolut nicht verfügbar ist oder zumindest nicht mit vernünftigem Aufwand gehoben werden kann (Nicht-Wissen) und dies dem Entscheider bekannt ist (z.B. bei Einsatz einer KI-Komponente). Unbekanntes Wissen besteht dabei in den Fällen, in denen an sich vorhandenes Wissen nicht genutzt wird (z.B. wenn unbemerkt Konfigurations- oder Programmierfehler auftreten). Unbekanntes Nicht-Wissen liegt schließlich vor, wenn dem Entscheider das Nicht-Wissen nicht mal bekannt ist, weil er mit dem zugehörigen Ereignis in keiner Weise rechnet (z.B. global wirkende Sicherheitslücken wie *Heartbleed* in OpenSSL).

Die Ungewissheit kann sich dabei sowohl vollständig auf Ereignisse und damit verbundene Risiken erstrecken als auch nur auf die Eintrittswahrscheinlichkeit oder die Folgenschwere. Soweit Eintrittswahrscheinlichkeit und Folgenschwere ungewiss sind, können alle drei Kategorien der Ungewissheit vorliegen. Ist hingegen nur die Eintrittswahrscheinlichkeit oder die Folgenschwere ungewiss, liegt ein Fall des bekannten Nicht-Wissens vor.

Methodisch steht die Resilienz *komplementär neben der Risikomethodik*, indem sie entweder die verbleibende, bekannte Ungewissheit aus Risikoidentifikation und -analyse oder das unbekannte Wissen- bzw. Nicht-Wissen bzgl. der für die Schutzgüter besonders kritischen Schutzobjekte adressiert. Insofern ist bei der Vornahme von Resilienzmaßnahmen entweder an der bekannten Stelle der Ungewissheit (bekanntes Nicht-Wissen) anzusetzen, oder es sind, in Unkenntnis woher die Ungewissheit droht, von den Schutzgütern her gedacht die besonders kritischen Schutzobjekte zu sichern. Sachlich setzt die Resilienz in beiden Fällen nicht an dem Beginn einer Ereigniskette (einem Einzelrisiko wie etwa einem Angriff), sondern an einem i.d.R. höherrangigen Ereignis an, dessen Ursachen ungewiss sind.

Um trotz der Ungewissheit eine Angemessenheit der Resilienzmaßnahmen zu gewährleisten, ist der damit verbundene Aufwand methodisch statt mit der Risikoreduktion mit der aus der Verarbeitung resultierenden abstrakten Bedrohung der zu sichernden Schutzgüter abzuwägen. Schließlich

526 Zur Cyberresilienz als Antwort auf Ungewissheit (en: uncertainty) vgl. auch: *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (2, 7 ff.).

ist das Lernen in der Erholungsphase der Resilienz als Optimierung von Resilienzmaßnahmen von der fortwährenden Erweiterung der Wissensbasis über Einzelrisiken innerhalb der Iteration des Risikomanagements zu unterscheiden.

2. Schutzziele nach Art. 32 Abs. 1 lit b) DSGVO

Im nun folgenden Abschnitt der systematischen Auslegung soll zweitens untersucht werden, wie sich die Resilienz zu der bestehenden Trias der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) verhält, die in Art. 32 Abs. 1 lit b) DSGVO neben der Resilienz und bezogen auf Systeme und Dienste genannt werden.

Hierfür wird zunächst eine historische Herleitung der Schutzziele in der Informationssicherheit vorgenommen (a.). Anschließend folgt eine Betrachtung der Entwicklung der Schutzziele im Datenschutzrecht (b.) und schließlich eine Beschreibung der Schutzziele in Art. 32 Abs. 1 lit b) DSGVO mit Blick auf die neuen Schutzobjekte Systeme und Dienste (c.) Nach einem Zwischenfazit zu den Schutzzielen (d.) wird erläutert, wie sich die Resilienz demgegenüber einordnet (e.).

a. Historische Entwicklung

Wesensmäßig taucht der Dreiklang dieser Schutzziele in der Informationssicherheit bereits in den 1970er Jahren als drei Kategorien „potenzieller Sicherheitsverletzungen" in informationstechnischen Systemen auf:[527]

1. Die unautorisierte Informationsfreigabe: Die Informationen können von einer nicht autorisierten Person gelesen und ausgenutzt werden. Auch die entsprechende Beobachtung des Informationsflusses sowie die unautorisierte Nutzung von Programmen wird hierunter gefasst (entspricht: Vertraulichkeit).
2. Die unautorisierte Informationsveränderung: Eine unautorisierte Person kann Änderungen an gespeicherten Informationen vornehmen (entspricht: Integrität).

527 *Saltzer/Schroeder*, Proc. IEEE 1975, 1278 (1280); *Cherdantseva/Hilton*, in: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), A Reference Model of Information Assurance & Security, 546 (547 f.)

3. Die unautorisierte Nutzungsverweigerung: Eine nicht autorisierte Person kann autorisierte Benutzer daran hindern, Informationen zu nutzen oder zu verändern (entspricht: Verfügbarkeit).

Zu beachten ist, dass die Schutzziele hier noch ausschließlich auf „Informationen" bezogen wurden und nicht etwa auf Systeme oder Dienste. Allerdings bezog die Definition von Sicherheit (en: Security) auch hier schon sowohl Maßnahmen zur Kontrolle der Nutzung oder Modifikation der gespeicherten Informationen als auch „des Computers" selbst mit ein.[528]

Auch in der Netzwerk-Sicherheit wurden die Schutzziele bald aufgegriffen. Angriffe auf die Vertraulichkeit und Integrität wurden dabei als (aktive) Sabotageakte klassifiziert. Umgekehrt wurden bloße Angriffe auf die Vertraulichkeit mitunter auch als „passive Angriffe" bezeichnet, da sie die Informationsverarbeitung bzw. den Informationsfluss nicht stören.[529] Im Weiteren wurden außerdem Angriffe auf die Authentizität etwa durch Veränderung der Metadaten aufgeführt,[530] wodurch eine falsche Zuordnung der Inhalte bewirkt werden kann. Umgekehrt werden Änderungen der Inhaltsdaten als Angriffe auf die Integrität von Informationen qualifiziert.[531]

Wenig später im Jahr 1985 schuf das US-Verteidigungsministerium einen Katalog von sog. „Trusted Computer System Evaluation Criteria". Auch hier galt als grundlegende Anforderung für die „Computersicherheit" die „*Verwendung spezifischer Sicherheitsfunktionen, so dass nur ordnungsgemäß autorisierte Personen oder Prozesse, die in ihrem Namen arbeiten, Zugriff auf Informationen haben und diese Lesen, Schreiben, Erstellen oder Löschen können.*"[532] Durch die Beschränkung des Zugriffs auf einen autorisierten Personenkreis steht dabei zunächst die Vertraulichkeit im Vordergrund. Die Nennung der unterschiedlichen Berechtigungen, insbesondere des Schreibens und Löschens legt daneben auch die Integrität und Verfügbarkeit von Informationen mit an.

528 *Saltzer/Schroeder*, Proc. IEEE 1975, 1278 (1279).
529 *Voydock/Kent*, ACM CSUR 1983, 135 (140, 142).
530 Dort statt „Metadaten" „protocol control information": *Voydock/Kent*, ACM CSUR 1983, 135 (142).
531 Wie zuvor.
532 En: "In general, secure systems will control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information." DoD, Trusted Computer System Evaluation Criteria, 26.12.1985, S. 9.

b. Einführung im deutschen und europäischen Datenschutzrecht

Im BDSG a.F.[533] war die Datensicherheit in § 9 und der zugehörigen Anlage geregelt. Die zwischenzeitlich weltweit standardisierten klassischen Schutzziele „Verfügbarkeit, Vertraulichkeit und Integrität" wurden dort, trotz intensiver Kritik,[534] bis zuletzt nicht ausdrücklich implementiert. Teilweise wurden die Schutzziele von der Literatur aber gleichwohl in die Anforderungen hineingelesen.[535]

Die Landesdatenschutzgesetze (LDSG) waren dagegen zum Teil schon weiter fortgeschritten. So setzte das LDSG in Schleswig-Holstein (SH)[536] in „§ 5 - Allgemeine Maßnahmen zur Datensicherheit" fest, dass im Rahmen der Datensicherheit durch technisch-organisatorische Maßnahmen u.a. Folgendes zu gewährleisten ist:

1. „Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (Verfügbarkeit),
2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (Integrität),
3. nur befugt auf Verfahren und Daten zugegriffen werden kann (Vertraulichkeit)."

Auch die DS-RL nannte die Trias der klassischen Schutzziele noch nicht ausdrücklich. Art. 16 stellte nach seiner Überschrift auf die „Vertraulichkeit der Verarbeitung" ab, beschränkte dies aber inhaltlich auf die interne Vertraulichkeit in der Form, dass nach dieser Vorschrift dem Verantwortlichem oder Auftragsverarbeiter unterstellte Personen die personenbezogenen Daten „nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten" dürfen.

533 bis zum 24.05.2018, aufgehoben durch das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU).

534 *Ernestus*, in: Simitis/Dammann/Arendt, Bundesdatenschutzgesetz, § 9 Rn. 1; *Melling-Schultze*, in: Taeger/Gabel, Kommentar zum BDSG [a.F.], 2. Auflage 2013, § 9, Rn. 42; *Wedde*, in: Däubler, Bundesdatenschutzgesetz [a.F.], 5. Auflage 2016, § 9, Rn. 7.

535 *Bizer*, DuD 2007, 350 (355); als „Verfügbarkeit, Authentizität und Integrität": *Gola/Klug/Körffer*, in: Gola/Schomerus, Bundesdatenschutzgesetz [a.F.], 12. Auflage 2015, § 9, Rn. 2.

536 LDSG SH a.F. vom 09.02.2000 (zuletzt geändert am 16.03.2015), gültig bis zum 23.05.2018.

In Art. 17 DS-RL „Sicherheit der Verarbeitung" hieß es weiterhin, dass

> *„der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muß [sic!], die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang […] und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind."*

In dieser Vorgabe sind bereits die drei klassischen Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität zu erkennen, ohne dabei jedoch (was seinerzeit wie auch im BDSG kritisiert wurde) ausdrücklich benannt zu sein.[537]

Mit der DSGVO ist der Gesetzgeber dieser Forderung erfreulicherweise nachgekommen und hat die Schutzziele darüber hinaus auch noch wie bereits beschrieben in ihrer Bedeutung zwischen Art. 25 und 32 DSGVO weiter konturiert.[538] Außerdem hat er sich dazu entschieden, die Schutzziele nun in Art. 32 Abs. 1 lit b) DSGVO auch mit Bezug auf „Systeme und Dienste" in seine Sicherheitsanforderungen aufzunehmen (dazu sogleich ausführlich).

c. Vorkommen und Auslegung in der DSGVO

Die genannten Schutzziele „Verfügbarkeit, Vertraulichkeit und Integrität" werden in der DSGVO in Art 25 i.V.m. Art 5 Abs. 1 lit f. sowie in Art 32 Abs. 1 lit b), lit c), Abs. 2 ausdrücklich genannt.

Der Gesetzgeber hat die Schutzziele in der DSGVO nicht nur das erste Mal ausdrücklich normiert, sondern sie nun auch auf neue Schutzobjekte ausgedehnt. Wie voranstehend gezeigt, wurden die Schutzziele bis dahin wie etwa im LDSG SH überwiegend auf Daten bezogen; § 5 LDSG SH erstreckte die Verfügbarkeit und Vertraulichkeit zumindest noch auf „Verfahren".

Nun bezieht Art. 32 Abs. 1 lit b) DSGVO die klassischen Schutzziele im Kontext der Datensicherheit auf „Systeme und Dienste" im Zusammenhang mit der Verarbeitung. Diese Begriffe wurden bereits eingangs grundlegend

537 *Bock/Meissner*, DuD 2012, 425 (427, 432), verbunden mit der Forderung an den europäischen Gesetzgeber die Schutzziele ausdrücklich zu normieren.

538 Siehe oben: S. 90 ff.

definiert, wobei die Frage einer soziotechnischen Auslegung des Systembegriffs für die Resilienz zwar im Rahmen der Auslegung nach dem Wortlaut bejaht wurde, für die Schutzziele aber bislang offen ist. Im Rahmen der Definition des Systems wurde auch erläutert, dass die personenbezogenen Daten im Sinne des Art. 32 DSGVO nicht als Teil des Systems zu verstehen sind[539] und die Schutzziele sich an dieser Stelle somit auch nicht auf die personenbezogenen Daten beziehen. Nach anderer Ansicht sind hingegen alle Schutzziele[540] und v.a. die Vertraulichkeit[541] in Art. 32 Abs. 1 lit b) DSGVO (auch) auf die Daten zu beziehen. Allerdings sind alle Schutzziele durch Art. 32 Abs. 1 lit c), Abs. 2 DSGVO schon auf die personenbezogenen Daten bezogen, so dass sich durch eine solche Ausdehnung in der Sache kein Unterschied ergibt. Zu Unterschieden kommt es nur dann, wenn einzelne Schutzziele wie etwa die Vertraulichkeit (dazu sogleich) nur auf Daten und nicht eigenständig auf Systeme bezogen werden.

Im Weiteren wird deshalb auf den Inhalt der Schutzziele in Bezug auf Systeme und Dienste eingegangen und an geeigneter Stelle auch auf die unterschiedliche Bedeutung der Schutzziele bei der Anwendung auf personenbezogene Daten hingewiesen. Die Neuausrichtung der klassischen Schutzziele auch auf Systeme und Dienste verdient auch deshalb besondere Beachtung, weil im Datenschutzrecht die Sicherheit von Systemen und Diensten nach den Schutzgütern traditionell eine geringere Rolle einnimmt als etwa im IT-Sicherheitsrecht. Bei letzterem ist die Funktionsfähigkeit auch der Systeme und Dienste selbst von besonderer Bedeutung, weil deren informationsverarbeitende Tätigkeit für die Erbringung einer kritischen Versorgungsleistung benötigt werden.

Im Datenschutzrecht hingegen liegt der Fokus bei der Verarbeitung stärker auf den dabei genutzten personenbezogenen Daten. Durch die Verarbeitung sollen die Rechte und Freiheiten natürlicher Personen nicht beeinträchtigt werden; so sollen etwa insbesondere unbefugte Offenlegungen der personenbezogenen Daten verhindert werden. Die fehlende Funktionalität eines Systems oder eines Dienstes führt hingegen nicht per se zu einer Beeinträchtigung der Schutzgüter, sondern diesen kommt wie bereits zuvor dargestellt eine Vorfeldschutzfunktion zu.[542]

539 Siehe oben: S. 115.
540 *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 35d ff.
541 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 38.
542 Siehe oben, S. 111.

Entsprechende Ausnahmen und die damit verbundenen Bedeutung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit (i. – iii.) an Systemen und Diensten werden im Folgenden dargestellt.

i. Verfügbarkeit

Die Verfügbarkeit von Systemen beschreibt pointiert deren „jederzeitige Nutzungsmöglichkeit".[543] Für das Datenschutzgrundrecht ist die Verfügbarkeit von Systemen insbesondere aus Gründen der Transparenz[544] geboten:

Die Systeme und Dienste ermöglichen den Zugriff auf die erhobenen personenbezogenen Daten sowie die daraus erzeugten Informationen. Ist der Zugriff nicht mehr möglich, kann der betroffenen Person keine Auskunft mehr erteilt werden bzw. sie kann die Daten auch nicht mehr einsehen. Dies ist zur aktiven Wahrnehmung des Rechts auf informationelle Selbstbestimmung bzw. des Datenschutzgrundrechts und damit zur Verwirklichung dieses Schutzgutes indes erforderlich, etwa um zu prüfen, ob die personenbezogenen Daten rechtmäßig auf Basis eines Erlaubnistatbestandes sowie entsprechend der Datenschutzgrundsätze verarbeitet wurden.[545] Konkret kann beispielsweise nur so überprüft werden, ob nur die für den Zweck tatsächlich erforderlichen Daten erhoben wurden (Grundsatz der Datenminimierung, Art. 5 Abs. 1 lit c) DSGVO). Dasselbe gilt für die Verfügbarkeit von Diensten, die etwa für die o.g. Auskunftserteilung erforderlich sind.

Wenn ein Dienst verfügbar sein soll, schließt dies notwendigerweise auch die Verfügbarkeit des Systems mit ein. Denkbar ist umgekehrt aber, dass ein System noch verfügbar ist und nur ein von diesem System bereitgestellter Dienst ausgefallen ist. Ob die Verfügbarkeit (auch) die ordnungsge-

543 *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn 25; ähnlich auch *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 31.

544 Vgl. mit Verweis auf die Nachweispflichten der DSGVO: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 38b.

545 Vgl. *Sattler*, in: Ebers/Steinrötter, Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 197 (214); *Kramer/Meints*, in: Auernhammer, DSGVO BDSG, 7. Auflage 2020, Art. 32, Rn. 43.

mäße Funktionsweise[546] (also das „Wie") erfasst oder nur wie hier zunächst beschrieben das „Ob" der Funktionsfähigkeit, ist zweifelhaft. Dies erscheint insbesondere in Abgrenzung zur Integrität problematisch (dazu sogleich).

ii. Integrität

Die Integrität von Systemen ist im IT-Recht bereits durch das BVerfG bekannt, soweit dieses im Rahmen seiner Entscheidung zur sog. „Online-Durchsuchung"[547] die Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in Form des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelte. Diese nationale grundrechtliche Definition kann zumindest als indizielle Auslegungshilfe für den Begriff der „Integrität" in der DSGVO herangezogen werden.

Die Integrität eines IT-Systems ist nach dem BVerfG beeinträchtigt, sobald „auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können" und so die „entscheidende technische Hürde für die Ausspähung, Überwachung oder Manipulation des Systems" genommen ist.[548] Die Schutzziele Vertraulichkeit und Integrität stehen hier insofern in einer sehr engen Verknüpfung, da die Vertraulichkeit der im System enthaltenen Daten nicht mehr gewährleistet werden kann, wenn das System etwa durch eingebrachte *Spyware*[549] in seiner Integrität verletzt ist.

546 *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 58; zu § 9 BDSG a.F. bereits *Hennrich*, Cloud Computing, S. 208 m.w.N.

547 *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (822 ff.).

548 *BVerfG,* a.a.O., S. 827, Rn. 204. Deutlich erkennbar wird aus dieser Definition die korrespondierende Angriffssicht, die sich daraus ergibt, dass mit dem Urteil das o.g. Grundrecht in seiner Abwehrdimension gegen einen staatlichen Zugriff auf das IT-System durch den sog. „Staatstrojaner" beschrieben wurde, siehe auch: *Stadler*, MMR 2012, 18 (18, 20).

549 Spyware ist eine client-seitige, d.h. auf einem Endgerät installierte Schadsoftware, die unautorisiert Informationen auf diesem Endgerät aufzeichnet und an ein externes System übermittelt, Vgl. *Stamminger et al.*, in: Samarati, Information Security, 202 (205).

Die so beschriebene *Systemintegrität* ist somit auch strikt zu unterscheiden von der Integrität der personenbezogenen Daten.[550] Letztere wird gesondert in Art. 32 Abs. 2 DSGVO adressiert.[551] Hinsichtlich des Schutzzwecks der Systemintegrität greift erneut die schon angesprochene Perspektive des Vorfeldschutzes: Sind die Systeme selbst integer, also insbesondere frei von Schadsoftware, können sie die Vertraulichkeit sowie die anderen Schutzziele an den personenbezogenen Daten sicherstellen.[552] Z.T. wird unter Integrität von Systemen auch (nur) deren „korrekte Funktionsweise"[553] verstanden, die durch eine (etwa nur ausspähende Korrumpierung) abhängig vom Verständnis dieser Anforderung zumindest noch nicht zwingend beeinträchtigt ist. Dieses Verständnis dürfte daher (insbesondere in Abgrenzung zur Verfügbarkeit) zu kurz greifen.

In der Gesamtschau auch mit Blick auf die Erkenntnisse aus dem genannten Urteil des BVerfGs sollte die Integrität als Anforderung verstanden werden, wonach der Zustand des Systems frei von allen Manipulationen sein soll, die sich auf den Schutz der personenbezogenen Daten auswirken können. Andere Beeinträchtigungen, die sich auf die Funktion auswirken können, etwa technisches Versagen von Komponenten (Hardware-Defekte) sind dagegen mangels Manipulationstatbestand *dem Schutzziel der Verfügbarkeit* (des Systems bzw. des Dienstes) zuzuordnen.

Die *Integrität des Dienstes*, also die Integrität der Funktionalität eines Systems, kann als die Manipulationsfreiheit des erzeugten Ergebnisses verstanden werden. Dies umfasst nach dem im 2. Kapitel, A. vorgestellten Modell sowohl die Erzeugung unrichtigen Personenwissens (etwa einer tatsächlich nicht bestehenden Präferenz) als auch im Folgeschritt eine vom Dienst getroffene Entscheidung im Rahmen einer Personalisierung (ein individuelles Preisangebot, eine Empfehlung eines bestimmten Produkts oder Posts).

---

550 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (406), Rn. 40; *Bedner/Ackermann*, DuD 2010, 323 (326); a.A. *Mantz*, in: Sydow/Marsch, DS-GVO, BDSG, 3. Auflage 2022, Art. 32, Rn 14, der hinsichtlich der Nichterfassung der personenbezogenen Daten von einer „sprachlichen Ungenauigkeit" des Gesetzes ausgeht.

551 Vgl. *Piltz/Zwerschke*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, Art. 32 DSGVO, Rn. 61.

552 Vgl. *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (406), Rn. 40.

553 *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 31.

iii. Vertraulichkeit

Die Vertraulichkeit von Daten stellt wohl das bedeutendste Element der Datensicherheit dar. Umso wichtiger ist es, die Vertraulichkeit des Systems hiervon sauber abzugrenzen.[554] Als erster Anhaltspunkt für das Verständnis der Vertraulichkeit kann wiederrum auf das vom BVerfG geprägte „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" abgestellt werden. Allerdings betrifft auch dieses Grundrecht im Detail mit der Vertraulichkeit die im „informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten".[555] Anders als bei dem Recht auf informationelle Selbstbestimmung geht es dabei allerdings noch nicht um ein konkretes personenbezogenes Datum, sondern übergreifend um alle personenbezogenen Daten, die einem informationstechnischen System „anvertraut" werden oder allein schon durch dessen Nutzung erzeugt werden.[556] Die „Vertraulichkeit des informationstechnischen Systems" stellt mithin hier im Ergebnis auf die Gesamtheit bzw. das Potential an darin verarbeiteten personenbezogenen Daten und nicht auf das System selbst ab. Dies entspricht auch den datensicherheitsrechtlichen Definitionen von Vertraulichkeit, in dem diese als der Schutz vor unbefugter Preisgabe von Informationen beschrieben wird.[557]

Insofern ist festzustellen, dass der Vertraulichkeitsbegriff auch hier stark mit Daten verknüpft ist; die Frage der Vertraulichkeitsanforderung an Systeme ist damit aber noch nicht beantwortet. In Anknüpfung an den Wortlaut und die Systematik von Art. 32 Abs. 1 lit b), Abs. 2 DSGVO sollte die Trennung zwischen Schutzzielen an personenbezogenen Daten einerseits und an Systemen und Diensten andererseits aufrechterhalten werden.

Zur Auflösung des Widerspruchs zwischen dem Wortlaut der Vertraulichkeit des Systems und der definitorischen Bindung der Vertraulichkeit an die Daten können hier anstelle der bereits adressierten personenbezogenen Daten die *systembezogenen Daten* zugrunde gelegt werden. Zu schützen sind damit jene Daten über die innere Struktur des Systems, die entsprechende Zustände oder Eigenschaften des Systems beschreiben. Beispiele sind etwa Daten über Versionen von Betriebssystemen, installier-

554 a.A. erneut *Mantz*, Fn. 550.
555 *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822 (827), Rn. 204.
556 *BVerfG*, a.a.O., Rn. 200.
557 *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 31.

te Software, Update-Zustände sowie über die verwendete Hardware. Die rechtliche Anforderung der Vertraulichkeit dieser systembezogenen Daten lässt sich telelogisch wiederrum durch den Vorfeldschutz erklären. So könnte beispielsweise das Datum einer veralteten Softwareversion entsprechend für Angriffe ausgenutzt werden und somit im Ergebnis den Schutz personenbezogener Daten gefährden. Aus dieser Sicht heraus kann dem Schutzziel der Vertraulichkeit ein sinnvoller Anwendungsbereich bezüglich der Systeme zugewiesen werden. Die Vertraulichkeit umfasst insoweit den Schutz vor einem Ausspähen des Hardware-Designs oder des Software-Codes,[558] denn ebendies könnte spätere Angriffe zur Offenlegung, Manipulation oder Vernichtung personenbezogener Daten erleichtern.

Die *Vertraulichkeit des Dienstes* ist nur insofern abgrenzungsfähig, als dass es bei dem Dienstergebnis wie einer personalisierten Empfehlung um das Verarbeitungsergebnis handelt, dass ggf. in besonderer Weise schutzwürdig ist. Gleichwohl wird dieses Ergebnis als personenbezogenes Datum ausgedrückt, so dass keine kategorische Abgrenzung möglich ist. Insgesamt spricht somit in der Auslegung viel dafür, der Vertraulichkeit des Dienstes hier (anders als bei dem System) keinen eigenen Anwendungsbereich zuzugestehen.

d. Zusammenfassung

Ausgangspunkt war die Frage, wie die Schutzziele an Systemen und Diensten in Art. 32 Abs. 1 lit b) DSGVO zu beschreiben sind.

Diese Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität werden heute als die „klassischen Schutzziele der Datensicherheit" verstanden.[559] Aus der historischen, technischen Betrachtung heraus lassen sie sich allgemein definieren als „die erwünschte Fähigkeit eines Informationssystems einer bestimmten Kategorie von Bedrohungen zu widerstehen."[560] Juristisch zugeschnitten sind sie als Anforderungen an ein System oder einen Dienst zu verstehen, die zur Sicherung bestimmter Schutzgüter eingehalten wer-

558 Ebendies explizit ablehnend: *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 38.

559 *F. Ritter/Reibach/Lee*, ZD 2019, 531 (532); *M. Rost*, DuD 2018, 13 (13 f.); *Trautwein/Kurpierz*, PinG 2018, 26 (29).

560 Vom Verfasser übersetzt aus *Cherdantseva/Hilton*, in: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), A Reference Model of Information Assurance & Security, 546 (548).

den müssen.[561] Als eine solche erwünschte Fähigkeit bzw. zu erfüllende Anforderung drücken sie zugleich einen bestimmten „Sollzustand“[562] aus, der angestrebt und möglichst erhalten werden soll.[563]

Insoweit stellen Schutzziele auch ein Maß für die gewährleistete Sicherheit dar. Umgekehrt folgt aus dem Zuschnitt auf „bestimmte Kategorien von Bedrohungen“ zugleich eine gewisse Bündelung von Maßnahmentypen, ohne allerdings ein exklusives Maßnahme-Schutzziel-Verhältnis zu begründen. Vielmehr existieren auch Maßnahmen, die mehreren Schutzzielen zugleich dienen (z.B. dient die in Art. 32 Abs. 1 lit a) DSGVO geforderte Verschlüsselung von Daten sowohl deren Integrität als auch deren Vertraulichkeit).[564]

Die Schutzziele in Art. 32 Abs. 1 lit b) DSGVO beziehen sich nur auf das technische System mit seinen Bestandteilen, d.h. auf die IT-Infrastruktur im engeren Sinn in Form der Hard- und Software.[565] Dies umfasst sowohl das System als auch den vom System erbrachten Dienst. Es wurden gegenüber den Schutzzielen an personenbezogenen Daten eigenständige Definitionen für die Verfügbarkeit und Integrität von Systemen und Diensten sowie die Vertraulichkeit von Systemen ermittelt.

Hingegen können die Schutzziele und insoweit auch der Systembegriff nicht auf die mitwirkenden natürlichen Personen erstreckt werden,[566] da die technischen Schutzziele auf diese keine definitorisch sachgerechte Anwendung finden können. Gleichwohl sind zur Gewährleistung der Schutzziele an dieser IT-Infrastruktur neben baulichen Maßnahmen (Zutrittskontrolle) auch Maßnahmen „an den“ bzw. für die Mitarbeitenden (z.B.

561 *Schmitz/Dall'Armi*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Rn. 32.

562 *Jandt*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 391 (404), Rn. 33; Als „Zielbestimmungen“: *Bock/Meissner*, DuD 2012, 425 (426).

563 Soweit die Schutzziele auf Daten bezogen sind, lassen sie sich entsprechend definieren als eine erwünschte Eigenschaft von Daten mit Blick auf eine bestimmte Kategorie von Bedrohungen.

564 Vgl. *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 20; Auf der anderen Seite können Maßnahmen für ein Schutzziel auch andere Schutzziele gefährden: So gefährdet etwa die genannte Verschlüsselung von Daten deren Verfügbarkeit, insbesondere wenn es bei der Verschlüsselung zu Fehlfunktionen kommen sollte, *Jergl*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018, Art. 32, Rn 30.

565 *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 22; siehe im Übrigen bereits zuvor: S. 114 ff.

566 So aber wohl *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 37.

entsprechende Schulungen und Sensibilisierungsmaßnahmen) erforderlich. Mitarbeitende müssen etwa geschult werden, um die Integrität der Systeme zu sichern, indem sie beispielsweise keine privaten, externen Speichergeräte in der betrieblichen Umgebung einsetzen. Dabei werden die Mitarbeitenden aber nicht Teil des Systems in dem Sinne, dass sie selbst die Schutzziele wie etwa das technische Erfordernis der „Integrität" erfüllen müssten.

e. Einordnung der Resilienz

Zu untersuchen ist nun, wie sich die Resilienz gegenüber den so beschriebenen Schutzzielen systematisch einordnet. Die Resilienz wird vom europäischen Gesetzgeber in der DSGVO grammatikalisch neben den klassischen Schutzzielen implementiert, die als historisch gewachsene Trias den anzustrebenden Zustand der Daten- und IT-Sicherheit auch heute noch vollständig abzubilden vermag.[567] Insoweit ist fraglich, ob sich die Resilienz als Erweiterung in die Systematik der Schutzziele einfügen und daher ebenfalls als Schutzziel qualifiziert werden kann. Wie die Schutzziele wird die Resilienz dabei auf Systeme und Dienste bezogen.

Teilweise wird die Resilienz als weiteres Schutzziel klassifiziert.[568] Auch inhaltlich wird der Resilienz ein Sollzustand zugewiesen, wie etwa dass ein System oder ein Dienst „auch unter hoher Inanspruchnahmefrequenz ordnungsgemäß funktionieren" können müsste.[569] Damit wird die Resilienz als eine besondere Ausprägung der Verfügbarkeit verstanden.[570] Dem ist jedoch entschieden entgegenzutreten: Die Resilienz stellt weder eine Ausprägung der Verfügbarkeit – dagegen spricht bereits historisch, dass der Gesetzgeber hierfür die Trias der tradierten Schutzziele gerade nicht hätte erweitern müssen – noch ein weiteres, neues Schutzziel dar.

---

567 Vgl. *Samonas/Coss*, JISSec, Vol. 10 (2014), Heft 3, 21 (37 f.).

568 Als weiteres „Sicherheitsziel": *Hladjk*, in: Ehmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 32, Rn. 8; im IT-Sicherheitsrecht außerdem: *Klaus et al.*, DuD 2021, 738 (739).

569 So allerdings ohne Verwendung des Schutzzielbegriffs: *Piltz*, in: Gola/Heckmann, DS-GVO, 3. Auflage 2022, Art. 32, Rn. 31.

570 *Jergl*, in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung 2018, Art. 32, Rn. 32; *Voskamp/D. Klein*, in: Kipker, Cybersecurity, S. 279, Rn. 19b; *Karg*, in: Lang/Löhr, IT-Sicherheit, 99 (111).

Vielmehr geht die Gegenansicht zu Recht von einer Sonderstellung dieses Merkmals aus und verneint die Klassifikation als viertes Schutzziel.[571] Betont wird dabei insbesondere der dynamische, funktionale Charakter der Resilienz als die Fähigkeit mit Störungen umgehen zu können.[572] Auch in der technischen Fachliteratur ist dieser Gedanke zu finden, wonach Resilienz keine intrinsische Eigenschaft, sondern eine (aktive) Fähigkeit eines Systems darstellt.[573]

Für letztere Ansicht streitet nach hiesiger Untersuchung neben der Wortlautauslegung in diesem Sinne auch der hier vorgenommene, systematische Vergleich der Resilienz mit den skizzierten Schutzzielen: Hier zeigt sich, dass die Resilienz als funktionale Anforderung den Schutzzielen nachgelagert ist. Die Schutzziele bilden wie beschrieben einen technischen Sollzustand ab,[574] der v.a. die gewährleistete Resistenz eines Systems sowie die Beeinträchtigungslosigkeit der personenbezogenen Daten sowie der Systeme und der Dienste umschreibt. Dieser Sollzustand soll durch die Härtung der Systeme erreicht und gehalten werden. Somit sollen Sicherheitsvorfälle in Form von Schutzzielverletzungen vermieden werden, die zunächst system- bzw. dienstbezogen sind und sodann eine Verletzung des Schutzes personenbezogener Daten (datenbezogener Sicherheitsvorfall) nach sich ziehen können.

Die Resilienz soll neben der Vermeidung von ungewissen Ereignissen insbesondere auch dann durch Anpassung des Systems eingreifen, wenn es bereits zu einem Sicherheitsvorfall gekommen und die Resistenz bzw. der Sollzustand somit bereits durchbrochen ist. Es kommt in diesem Fall auf die Fähigkeit des Systems an, mit diesem Ereignis umgehen zu können und so trotz einer Verletzung der Datensicherheit die Entstehung eines Scha-

571 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn 42; *Gonscherowski/M. Hansen/Rost*, DuD 2018, 442 (446); *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 26; *Laue*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Auflage 2019, Art. 32 DSGVO, Rn. 14; ähnl. von einem „Prinzip" sprechend: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39.

572 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 42 ff.; *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 26; *Heitmann*, IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie, S. 13.

573 *Alderson*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 66 (74); *Hollnagel/Woods*, in: Hollnagel/Woods/Leveson, Resilience engineering, 347 (347 f.).

574 Siehe Fn. 562.

dens an den Schutzgütern (Rechte und Freiheiten natürlicher Personen) zu vermeiden. Die Resilienz beschreibt somit gerade keinen sicherheitstechnischen Sollzustand (wie die Schutzziele), sondern eine funktionale Eigenschaft des Systems insbesondere im Umgang mit Sicherheitsvorfällen.

Weiterhin ergibt sich hinsichtlich der *Bedrohungssicht* auf Schutzziele ein gravierender Unterschied. Schutzziele lassen sich auch unter Berücksichtigung der historischen Betrachtung als Spiegelbild von bestimmten Bedrohungen bzw. Angriffen verstehen.[575] Ein Angriff auf die „Resilienz" von Systemen und Diensten ist aber jedenfalls strukturell kein finales Angriffsziel wie etwa auf deren Verfügbarkeit oder Integrität. Ein Angriff auf die Resilienz etwa durch Beeinträchtigung der Anpassungsfähigkeit kann vielmehr nur ein Hilfsmittel sein, um den eigentlich von dem/der Angreifer:in erstrebten Erfolg einer Schutzzielverletzung an dem System, dem Dienst oder den verarbeiteten Daten zu erreichen. Umgekehrt dient die Resilienz als Abwehrmechanismus auch nicht wie die anderen schutzzielbezogenen Maßnahmen der Abwehr spezifischer Risiken, sondern entspricht, wie im Rahmen der bisherigen Auslegung herausgearbeitet wurde, eher einer universalen Fähigkeit mit ungewissen, widrigen Ereignissen umgehen zu können.

Ob eine hinreichende Resilienz durch Maßnahmen gewährleistet wurde, kann sich mitunter auch darin ausdrücken, wenn es in Folge eines Ereignisses gerade nicht zu einer Verletzung der Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität kommt.[576] Dabei ist allerdings genau zu differenzieren: Zunächst wird wie beschrieben im Regelfall aufgrund des ungewissen Charakters des Ereignisses ein Sicherheitsvorfall eintreten, etwa die Verletzung der Integrität eines Systems (z.B. Infiltration durch bislang unbekannte Schadsoftware). Gleichwohl kann die Resilienz etwa noch die Vertraulichkeit von Daten gewährleisten, d.h. sicherstellen, dass es trotz dieser der unerwarteten und deshalb nicht zu verhindernden Integritätsverletzung am Schutzobjekt System nicht zu einer Offenlegung, d.h. einer Vertraulichkeitsverletzung an den personenbezogenen Daten kommt (z.B. durch Erkennung der Schadsoftware und einer entsprechenden Zugriffsbegrenzung). Resilienz kann somit eine drohende oder bereits begonnene Kette von Sicherheitsvorfällen bzw. Schutzzielverletzungen unterbrechen. Sie ist jedoch insoweit kein Maß für den Schutz der initial verletzten

575 *Freimuth,* Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, S. 61.

576 Vgl. *Klaus et al.*, DuD 2021, 738 (739); *Gonscherowski/M. Hansen/Rost*, DuD 2018, 442 (444 f.); *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (12).

Schutzziele. Dies würde die Abgrenzung zwischen risiko- und schutzzielbezogenen Maßnahmen (z.B. Verschlüsselung von Daten) einerseits und den auf Ungewissheit abzielenden Resilienzmaßnahmen (z.B. Erkennung eines und Reaktion auf einen unautorisierten Datenabfluss) andererseits konterkarieren.

Im Ergebnis bestimmt Art. 32 Abs. 1 lit b) DSGVO damit die drei klassischen Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit sowie zusätzlich die funktionale Anforderung der Resilienz. Die spezifische Systematik des Art. 32 Abs. 1 lit b) DSGVO ist insoweit zu kritisieren, als dass sie diesen Unterschied zwischen den Schutzzielen und der Resilienz nicht deutlich kennzeichnet und darüber hinaus auch eine zweigeteilte Auslegung des Systembegriffs (dazu sogleich ausführlich) notwendig macht.

3. Systeme und Dienste

Nach Art. 32 Abs. 1 lit b) DSGVO bezieht sich die Resilienz sowohl auf *Systeme* als auch auf *Dienste*.

Hinsichtlich der Systeme bestätigt sich als Folge der systematischen Auslegung der Schutzziele die Hypothese, dass der Systembegriff für diese zwar informationstechnisch, *für die andersartige Resilienz aber soziotechnisch zu verstehen ist.* Gerade der Umgang mit bereits eingetretenen Sicherheitsvorfällen verlangt ggf. ein menschliches Eingreifen, um die Resilienz etwa in Form einer Anpassung der Systeme zu gewährleisten.[577] Dagegen sind die Schutzziele selbst aufgrund ihrer technischen Ausrichtung wie bereits dargestellt auf ein technisches Systemverständnis ausgerichtet. Der Begriff der Systeme ist in Art. 32 Abs. 1 lit b) DSGVO mithin zweigeteilt auszulegen – als informationstechnisches System hinsichtlich der Schutzziele und als soziotechnisches System hinsichtlich der Resilienz.

Zum Begriff des Dienstes wurde bei der Darstellung der Vorbegriffe festgestellt, dass ein technisches Verständnis des Dienstbegriffs zugrunde zu legen ist, nach welchem der Dienst *die Funktionalität eines Systems* darstellt. Als Funktion steht etwa ein bestimmtes Ergebnis wie die Erzeugung bestimmten Wissens oder das Treffen einer Entscheidung. Daneben erfüllen die *Dienste* (und damit auch die Systeme) wie bereits beschrieben

577 Vgl. *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (2, 14 f.).

eine Funktion bei der Erfüllung der Betroffenenrechte; ihre Verfügbarkeit ist etwa von Bedeutung, um Auskunftsrechte zu erfüllen.[578]

Für die Resilienz wurde aus dem Wortlaut zunächst herausgearbeitet, dass sie die *Fähigkeit eines soziotechnischen Systems beschreibt, ungewisse Ereignisse zu erkennen, sich an diese möglichst folgenmindernd anzupassen und sich nach einem solchen unter lernender Verbesserung schnellstmöglich zu erholen.*

Die einzelnen Leistungen der Resilienz können insofern nur durch das System selbst gewährleistet werden, etwa indem hier Maßnahmen zur Erkennung, Anpassung und anschließenden Erholung einschließlich der lernenden Verbesserung implementiert werden. Der Dienst selbst kann zwar in dem Sinne als resilient verstanden werden, als dass das durch ihn erbrachte funktionale Angebot trotz des Vorliegens ungewisser Ereignisse unbeeinträchtigt bleibt.[579] Dies divergiert aber vom inhaltlichen Kern der Resilienz, der gerade die Maßnahmen am System und damit dessen (weitere) Funktionen im Umgang mit Ungewissheit umschreibt, damit der Dienst im Ergebnis resilient ist:

> *Die Resilienz des Dienstes liegt vor, wenn das durch ihn erbrachte funktionale Angebot des Systems angesichts ungewisser Ereignisse unbeeinträchtigt bleibt.*

Im vorliegenden Szenario ist der (resiliente) Dienst die Personalisierung in Form der Erzeugung personalisierten Wissens und den daraus abgeleiteten Entscheidungen. Für die weitere Untersuchung steht gleichwohl die Resilienz des Systems im Vordergrund, die aus den genannten Gründen die entscheidende Rolle einnimmt.

Es sei an dieser Stelle ergänzend darauf hingewiesen, dass teilweise auch zwischen der eigentlichen Funktionalität eines Systems (hier: der Dienst) einerseits und nicht-funktionalen Eigenschaften wie der Gewährleistung der IT- bzw. Datensicherheit und damit auch der Resilienz andererseits, unterschieden wird.[580] In dieser Untersuchung wird der Funktionsbegriff hingegen holistisch für alle Funktionen eines Systems verwendet, d.h. so-

578 Siehe Fn. 545.

579 Vgl. hierzu die Definition von Fehlertoleranz/Resilienz in der Verlässlichkeitsforschung als das Vermeiden von Dienstausfällen: S. 133 ff.

580 Statt vieler: *Balzert*, Lehrbuch der Softwaretechnik, S. 109 f.

wohl für Sicherheitsfunktionen (einschließlich der Resilienz) als auch für den Dienst als das eigentliche funktionale Leistungsangebot des Systems.[581]

4. Fazit

Für die systematische Auslegung konnten in Gegenüberstellung mit dem Risikoverständnis der DSGVO folgende Ergebnisse gefunden werden:

Hinsichtlich des Risikos wurde herausgearbeitet, dass die Resilienz sich anders als die Risikomethodik mit der Bewältigung von Ungewissheit befasst. Sie hat insoweit eine Komplementärfunktion zur Bewältigung der Ereignisse, die sich nicht als Risiken antizipieren lassen, mithin ungewiss sind. Dabei wurden die Kategorien *bekanntes Nicht-Wissen*, *unbekanntes Wissen* und *unbekanntes Nicht-Wissen* bestimmt, die jeweils unterschiedliche Formen der Ungewissheit beschreiben. Dabei wird bekanntes Nicht-Wissen in der Risikoidentifikation und -analyse sichtbar, so dass hier an der entsprechenden Stelle mit Resilienzmaßnahmen reagiert werden kann. Für die übrigen Kategorien der Ungewissheit kann hingegen nur an den bekanntermaßen besonders kritischen Schutzobjekten (z.B. besonders sensible Daten, zentrale Schnittstellen oder andere wichtige Komponenten) angesetzt werden.

Methodisch ist im Ergebnis weiterhin zwischen der abstrakten Angemessenheit der Resilienzmaßnahmen, welche den Aufwand gegenüber der abstrakten Bedrohung der Schutzgüter durch die (unsichere) Verarbeitung abwägt einerseits und der bisher im Gesetz verankerten risikobezogenen Angemessenheit andererseits zu unterscheiden. Bei letzterer ist der Aufwand der risikospezifischen Maßnahmen gegenüber der damit zu erreichenden Risikoreduktion abzuwägen. Schließlich wurde dargestellt, dass bei dem Risikomanagement im Rahmen der Iteration neues, explizites Wissen über Risiken genutzt werden kann (z.B. eine neu bekannt gewordene Schwachstelle zu schließen). Dagegen bezieht sich das Lernen in der Erholungsphase der Resilienz auf die Nutzung impliziten Wissens, also kein Wissen über neue Einzelrisiken, sondern Wissen über neue Bewältigungsstrategien im Umgang mit Ungewissheit.

581 Ebenfalls kritisch zur Unterscheidung von funktionalen und nicht-funktionalen Eigenschaften: *Glinz*, in: 15th IEEE International Requirements Engineering Conference (RE '07), On Non-Functional Requirements, 21 (22 ff.).

Gegenüber den Schutzzielen erweist sich die Resilienz als grundlegend andersartig. Bei den Schutzzielen handelt es sich um Anforderungen an technische Systeme und Dienste (oder in Art. 32 Abs. 2 DSGVO auch Daten) die zur Sicherung der Schutzgüter der DSGVO erfüllt sein müssen.[582] In dieser Funktion lassen sie sich als „Sollzustände" beschreiben: Die Vertraulichkeit eines Systems[583] ist dann gewahrt, wenn kein unbefugter Zugriff auf dieses stattfindet. Die Integrität ist gewahrt, solange das System oder der Dienst unversehrt, d.h. frei von Manipulationen ist. Schließlich ist ein System oder ein Dienst verfügbar, wenn es für den jeweiligen Nutzer jederzeit verwendbar ist.[584] Demgegenüber spezifiziert die Resilienz eine funktionale Anforderung an soziotechnische Systeme, die diese befähigt mit ungewissen Ereignissen, d.h. unmittelbar bevorstehenden oder bereits eingetretenen Sicherheitsvorfällen (mit entsprechenden Schutzzielverletzungen) umzugehen. Diese funktionale Anforderung ist in der Bedrohungssicht anders als die Schutzziele auch kein eigenständiges Angriffsziel.[585]

Aus der Positionierung der Resilienz als einem weiteren Merkmal neben den Schutzzielen folgt weiterhin, dass die Resilienz nur ein Bestandteil zur Gewähr der Sicherheit der Verarbeitung ist. Damit wird die Resilienz hier anders eingeordnet als etwa im CSA, bei dem die Resilienz als weiteres Prinzip neben der Sicherheitsgewähr verstanden wird oder etwa der DORA, bei der alle (Sicherheits-)Maßnahmen per se Resilienzmaßnahmen sind.

Schließlich wurde herausgearbeitet, dass die Resilienz mit Blick auf Systeme und Dienste unterschiedlich zu verstehen ist, wobei der zentrale Anknüpfungspunkt in der Resilienz der soziotechnischen Systeme zu sehen ist und der „resiliente Dienst" vielmehr ein Ergebnis der Resilienz der Systeme ist.

Ergänzend sei an dieser Stelle darauf hingewiesen, dass Art. 32 Abs. 1 lit c) DSGVO explizit die rasche Wiederherstellung der Verfügbarkeit der Daten nach einem Zwischenfall verlangt. Dies ist ebenfalls eine (in sozio-

582 Vgl. *Schmitz/Dall'Armi*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil XII, Kapitel 1, Rn. 32, welche aber nur auf das „System" abstellen.

583 Für die Vertraulichkeit des Dienstes konnte demgegenüber kein eigenständiger Anwendungsbereich identifiziert werden, siehe oben, S. 195 ff.

584 Genannte Definitionen nach: *Jandt*, in: Kühling/Buchner, Datenschutz-Grundverordnung/BDSG, 4. Auflage 2024, Art. 32, Rn. 23 ff.

585 Allenfalls können diese Resilienzmaßnahmen im Falle eines Angriffs umgangen werden und so ggf. ihre vollständige Schutzwirkung nicht ausspielen.

technischen Systemen zu implementierende) Maßnahme zur Bewältigung eines ungewissen Ereignisses[586] und fällt folglich auch unter die Erholung im Rahmen der Resilienz, wie sie in der Arbeitsdefinition nach der Wortlautauslegung bestimmt wurde. Für die systematische Auslegung ist somit anzunehmen, dass in Art. 32 Abs. 1 lit c) ein Aspekt der Resilienz gesondert hervorgehoben wird.

IV. Historische Auslegung

Im Rahmen der historischen Auslegung gilt es anhand der Entstehungsgeschichte den Willen des Gesetzgebers zu ermitteln; als „Gesetzgeber" sind alle Gesetzgebungsorgane zu zählen, „deren Zustimmung der Rechtsakt im konkreten Fall trägt".[587] Dies ist bei der DSGVO jedenfalls das Europäische Parlament. Die EU-Kommission fällt hingegen nicht unmittelbar darunter, da ihr lediglich ein Initiativrecht zukommt und ihre Gesetzesvorschläge durch das Parlament nach Belieben verändert werden können.[588] Allerdings kann nach der sog. „Paktentheorie" auch schon der Kommissionsvorschlag berücksichtigt werden, soweit das Parlament dessen Inhalte in seinen Willen aufgenommen hat.[589] Die Bedeutung der historischen Auslegung wird im europäischen Recht aber tendenziell eher als gering angesehen.[590]

Normativ können sowohl Vorgängervorschriften als auch vorangegangene Entwürfe eines Gesetzes betrachtet werden.[591] Im Folgenden sollen somit als Vorgängervorschrift[592] des Art. 32 DSGVO der Art. 17 DS-RL sowie die Entwicklung der DSGVO betrachtet werden.

---

586 So bezeichnet *S. Ritter*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2. Auflage 2020, Art. 32, Rn. 65 ff. diese Maßnahme als Teil der Disaster-Recovery nach einem Vorfall. Insofern sei insbesondere auch ein Business-Continuity-Management bzw. ein Notfallmanagement auch unter Einbeziehung des Personals vorzusehen, um die Daten rasch wiederherzustellen zu können.

587 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (303), Rn. 33.

588 Wie zuvor.

589 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285, Rn. 34 m.w.N.

590 *Herdegen*, Europarecht, S. 226, Rn. 92; *Classen/Nettesheim*, Europarecht, § 9, Rn. 174; a.A. *Leisner*, EuR 2007, 689-706 (706).

591 *Pieper*, in: Dauses/Ludwigs, Handbuch des EU-Wirtschaftsrechts, Rn. 48; *GA Mayras,* Schlussanträge EuGH Urt. v. 23.10.1974 – Rs. 32/74, S. 1215.

592 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn. 4.

1. Vorgängervorschrift Art. 17 DS-RL

Bisher war die Sicherheit der Verarbeitung in Art. 17 der DS-RL normiert. Diese enthielt weder die Resilienz noch nannte sie die vorangehend skizzierten Schutzziele ausdrücklich. Allerdings wurde bereits der „Schutz [der personenbezogenen Daten] gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang […] und gegen jede andere Form der unrechtmäßigen Verarbeitung." erfasst. Mit diesen Begrifflichkeiten lassen sich wie gezeigt die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit assoziieren.

Vergleicht man nun diese Vorschrift mit Art. 32 Abs. 1 und 2 DSGVO, so ist festzustellen, dass der Gesetzgeber offensichtlich in zweifacher Hinsicht einen Handlungsbedarf identifizierte: Zum einen, dass diese Schutzziele auch explizit auf Systeme und Dienste bezogen und der Schutzumfang somit erweitert werden müssten und zum zweiten, dass die Schutzziele an dieser Stelle aber nicht hinreichend seien, sondern mit der „Resilienz" eine weitere spezifische Anforderung an die Systeme und Dienste gestellt werden müsste.

2. Entwicklung der DSGVO

Im Kommissionsentwurf zur DSGVO vom 25.01.2012 waren die Datensicherheitsvorgaben noch nicht weiter konkretisiert. Vielmehr hieß es in Art. 30 Abs. 1 (später Art. 32 Abs. 1 DSGVO) ähnlich zur finalen Fassung lediglich: „Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung des Stands der Technik und der Implementierungskosten technische und organisatorische Maßnahmen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist."[593] Der 2. Hs. mit den Listenpunkten a) bis d) war noch nicht vorhanden.

Der europäische Datenschutzbeauftragte forderte in seiner Stellungnahme vom 07.03.2012 zu diesem Entwurf eine Klarstellung der Gesamtverant-

593 EU KOM (2012) 11 endgültig, Art. 30, S. 68.

wortung des Verantwortlichen für die Datensicherheit und die Ergänzung einer Pflicht zur Durchführung einer Informationssicherheitsstrategie.[594]

Dem scheint das Parlament in seiner Konkretisierung (Beschluss vom 12.03.2014) gefolgt zu sein, die sich heute noch in leicht veränderter Form in S. 2 findet: „Eine solche Sicherheitspolitik umfasst – unter Berücksichtigung des Stands der Technik und der Implementierungskosten – Folgendes: […] b.) die Fähigkeit, die Vertraulichkeit, Vollständigkeit, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen;".[595]

3. Fazit

Insgesamt zeigt sich, dass konkrete Vorgaben zur Datensicherheit erst spät Eingang in das europäische Datenschutzrecht gefunden haben. Weder in der Vorgängervorschrift noch in den ersten Entwürfen wurden die Schutzziele oder die Resilienz (ausdrücklich) genannt und das obwohl die maßgeblich durch die Schutzziele beschriebene Datensicherheit an sich schon eine lange Geschichte aufweist.[596]

Hieraus lässt sich schließen, dass der Gesetzgeber auf erst in jüngster Zukunft vermehrt aufgetretene Phänomene in der Datensicherheit reagiert hat, denen mit dem bisherigen Regelungskonzept (Risiken und Schutzziele) nicht (mehr) beizukommen war. Somit ist auch für die Resilienz im Rahmen der sich anschließenden teleologischen Auslegung nach neuen Sachphänomen zu suchen, auf die das Prinzip der Resilienz eine Antwort geben könnte. Es stellt sich somit pointiert die Frage, warum die Resilienz (erst) jetzt vom Gesetzgeber gesondert normiert wurden.

---

594 EDSB, Zusammenfassung der Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket, S. 4.

595 Siehe hierzu: EU-Parlament, P7_TA(2014)0212 - Legislative Entschließung zum Vorschlag zur allgemeinen Datenschutzverordnung [später DSGVO], 12.03.2014, ABl. 2017 C 378/399 (445 f), Abänderung 124.

596 Exemplarisch im deutschsprachigen Raum als „Datensicherung" bereits: *Weck*, DuD 1989, 386 (386).

V. Teleologische Auslegung

Für die teleologische Auslegung ist nach dem EuGH auf den „Sinn und Zweck" oder auch den „Geist" der jeweiligen Norm abzustellen.[597] Dabei kann bei der Auslegung des Sekundärrechts wie der DSGVO der dort in den Erwägungsgründen oder der Präambel niedergelegte Zweck herangezogen werden und dieser ggf. mit Blick auf das europäische Primärrecht und damit insbesondere auch die europäische Grundrechtecharta (Art. 6 Abs. 1 EUV) korrigiert werden.[598] Daneben kann jedenfalls nach einer Literaturauffassung auch auf den spezifischen Zweck einzelner Regelungen abgestellt werden.[599]

Der Zweck der DSGVO liegt wie bereits dargestellt insbesondere in der Sicherung der in Art. 1 Abs. 2 DSGVO niederlegten Schutzgüter, namentlich der Rechte und Freiheiten natürlicher Personen, insbesondere des Datenschutzgrundrechts nach Art. 8 Abs. 1 GRC (EG 1 DSGVO). Art. 32 DSGVO regelt mit der Datensicherheit hierfür einen Teilaspekt und die Resilienz stellt wiederrum eine spezifische Datensicherheitsvorgabe dar. In Umkehr dieser Ableitung ist mithin zu fragen, wie die Resilienz der Sicherung des Datenschutzgrundrechts und anderer Rechte und Freiheiten natürlicher Personen dienen kann und somit gegenüber welchen neuen Realweltphänomenen die Resilienz diese Schutzgüter sichern soll.

Systematisch wurde bereits dargelegt, dass Resilienz nicht unmittelbar auf den Umgang mit antizipationsfähigen Risiken, sondern auf den Umgang mit Ungewissheit gerichtet ist. Im Rahmen dessen wurden bereits auch einzelne Fallgruppen von Ungewissheit (*bekanntes Nicht-Wissen, unbekanntes Wissen, unbekanntes Nicht-Wissen)* aufgezeigt. Historisch konnte weiterhin gezeigt werden, dass es sich um eine in der Datensicherheit gänzlich neue Anforderung handelt und diese auch erst spät in das Gesetzgebungsverfahren aufgenommen wurde.

Entsprechend liegt teleologisch die These nahe, dass Resilienz als funktionale Anforderung soziotechnischer Systeme eine Antwort auf zuletzt stark zunehmende Ungewissheitssituationen in der Sicherheitsgewährleis-

597 *Pieper*, in: Dauses/Ludwigs, Handbuch des EU-Wirtschaftsrechts, Rn 33; *EuGH*, Urt. v. 09.12.1965 – 44/65, BeckRS 2004, 71198.

598 *Pieper*, in: Dauses/Ludwigs, Handbuch des EU-Wirtschaftsrechts, B. I. Rechtsquellen, Rn. 44.

599 *Riesenhuber*, in: Riesenhuber, Europäische Methodenlehre, 285 (308), Rn. 42; *Wank*, Juristische Methodenlehre, S. 445, Rn. 96 ff.

tung gibt. Solche Ungewissheitssituationen können sich insbesondere aus den nachfolgenden Gründen ergeben, die auch bereits in der systematischen Auslegung bei den Kategorien von Ungewissheit[600] angesprochen wurden.

1. Ungewissheit in komplexen, offenen Systemen

Zunächst haben sich die verwendeten Systeme stark verändert: Ursprünglich bestanden vor allem geschlossene, räumlich abgrenzbare und auf einen bestimmten Kreis von Teilnehmer:innen beschränkte Systeme.[601] Demgegenüber entwickelten sich zunehmend offene Systeme, *die räumlich verteilt und vernetzt sowie offen für die Kommunikation mit möglichst vielen anderen Systemen sind.*[602] Zu offenen Systemen zählen insbesondere jene zur Bereitstellung der hiesigen digitalen Dienste (Online-Marktplätze, Online-Suchmaschinen sowie soziale Netzwerke).[603] Die DSGVO enthält zwar keine expliziten Verweise auf diese neuen Ungewissheiten, verweist in EG 6 aber zumindest auch pauschal auf „rasche technologische Entwicklungen" und eine Datennutzung in „noch nie dagewesenem Umfang".

Solche neuen offenen Systeme weisen starke *Interdependenzen* und eine *hohe Komplexität* mit unüberschaubar zahlreichen und teilweise auch nur subtilen und damit schwer erkennbaren Kommunikationsbeziehungen auf.[604] Wie bereits dargestellt spricht man in diesem Zusammenhang auch von *Emergenz*, wenn sich das Verhalten eines offenen Systems nicht mehr anhand einer Betrachtung seiner Komponenten und seiner einzelnen Kommunikationsbeziehungen erklären lässt.[605] Im Ergebnis ist somit eine vollständige Risikoanalyse nicht möglich und folglich auch nicht mehr hinreichend, um die Datensicherheit zu gewährleisten.

Erschwerend kommt hinzu, dass Normadressaten mitunter auch nur Betreiber kleinerer Gruppen von Komponenten oder sogar nur einzelner

600 S. 170 ff.
601 *Eckert*, IT-Sicherheit, S. 3.
602 *Eckert,* a.a.O.; ähnlich auch *Hiermaier/Scharte/Fischer*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 155 (155), der insoweit von auf zunehmender Vernetzung beruhenden soziotechnischen Systemen spricht.
603 So bereits in der Einleitung, S. 34.
604 *Park et al.*, Risk analysis 2013, 356 (358); *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (8, 12); *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (12, 32).
605 Siehe oben, S. 174.

Komponenten in solchen komplexen Systemen sind, etwa eines Servers, der von Dritten eingehende Informationen verwaltet, aufbereitet und die Ergebnisse wiederrum Dritten zur Verfügung stellt. Solche Betreiber sehen sich daher sowohl für empfangende Informationen als auch z.T. für die Folgen der Ergebnisse ihrer Informationsverarbeitung einer starken Ungewissheit ausgesetzt.

2. KI als ungewisse Komponente

Eine zusätzliche Ungewissheit kann durch den Einsatz von KI entstehen. Aufgrund des typischen *Blackbox-Charakters* vieler KI-Systeme[606] lassen sich die Lernentwicklung und die damit verbundenen Entscheidungen dieser Systeme nicht sicher vorhersehen. Gleiches gilt für das Verhalten der KI-Systeme im Falle eines Angriffs durch Datenmanipulation (sog. Adversarial Examples, insbesondere Data Poisoning[607]).

Die EU-Kommission schreibt hierzu in ihrem Weißbuch zur Künstlichen Intelligenz, dass entsprechende KI-Systeme technisch solide und präzise sein müssten, um vertrauenswürdig zu sein. Zu treffende Maßnahmen umfassen demnach u.a. die Gewährleistung, dass KI-Systeme sowohl gegen offene Angriffe als auch gegen subtilere Versuche, Daten oder die Algorithmen selbst zu manipulieren, widerstandsfähig [en: resilient] sind und dass in solchen Fällen Abhilfemaßnahmen ergriffen werden.[608] Auch der KI-VO-E sieht in Art. 15 Abs. 4, 5 vor, dass Hochrisiko-KI-Systeme sowohl gegenüber Fehlern, Störungen oder Unstimmigkeiten als auch gegenüber den Versuchen unbefugter Dritter, ihre Verwendung oder Leistung durch

606 *Eigner et al.*, in: Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Towards Resilient Artificial Intelligence: Survey and Research Issues, 536 (536).

607 Adversarial Examples bezeichnet als Oberbegriff jeden Input in ein ML-System, den ein(e) Angreifer:in absichtlich darauf ausgerichtet hat, dass das ML-System Fehler macht. Beim Data Poisoning (oder auch Poisoning Attack) werden Trainingsdaten manipuliert mit dem Ziel, das ML-System „umzutrainieren", so dass es künftig andere Entscheidungen trifft; davon zu unterscheiden sind insbesondere sog. *Evasion Attacks*, die das System nicht umtrainieren, sondern nur täuschen, z.B. schwarze Aufkleber auf einem Stop-Schild, so dass dieses von einem bilderkennenden ML-System nicht mehr richtig erkannt wird; *H. Xu et al.*, IJAC (International Journal of Automation and Computing) 2020, 151 (151 f., 159).

608 EU-Kommission, COM(2020) 65 final, Weißbuch zur Künstlichen Intelligenz, 19.02.2020, S. 24 f.

Ausnutzung von Systemschwachstellen zu verändern, *widerstandsfähig [en: resilient]* sein müssen.

An dieser Stelle ist darauf hinzuweisen, dass in der DSGVO KI-Systeme (wie auch andere automatisierte Entscheidungssysteme) grundsätzlich von Art. 22 DSGVO erfasst werden, ohne jedoch spezifische Vorgaben an die Sicherheit dieser Entscheidungssysteme zu stellen. Jedenfalls in Fällen von o.g. Angriffen wäre hier auch unstreitig Art. 32 DSGVO einschlägig; für sich entwickelnde Fehler insbesondere bei KI-Systemen mit inkrementellem Lernen (Online Lernen) könnte man dies u.U. auch als Anforderung des Art. 22 Abs. 3 DSGVO verstehen. Insoweit erläutert EG 71 zur automatisierten Entscheidungsfindung, der Verantwortliche müsse „technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden und das Risiko von Fehlern minimiert wird". Systematisch dürfte dies aber eher auf Art. 32 DSGVO verweisen, der insofern neben vorsätzlichen Angriffen auch zufällige und fahrlässige Ereignisse erfasst.[609]

3. Ermöglichung von Resilienz durch Komplexität und Autonomie

Auf der Maßnahmenseite spielt die gestiegene Komplexität und Autonomie von IT-Systemen[610] ebenfalls eine tragende Rolle. Nach dem aus der Systemtheorie stammenden *ashby'schen Gesetz* benötigt ein System eine gewisse Eigenkomplexität, um flexibel auf Ereignisse reagieren zu können. Denkbar ist dies v.a. für den Ausfall einzelner und den entsprechenden Ausgleich durch andere Komponenten.[611] Somit ist jedenfalls hinsichtlich der technischen Systeme die Möglichkeit als auch die Notwendigkeit von solchen Resilienzmaßnahmen[612] erst durch die neuere Entwicklung besonders komplexer Systeme entstanden.

609 Siehe S. 98.

610 *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn 44.

611 *Fathi*, Resilienz im Spannungsfeld zwischen Entwicklung und Nachhaltigkeit, S. 68 mit Verweis auf *Ashby*, An introduction to cybernetics, S. 206 f.

612 Vgl. *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (12).

4. Fazit

Insgesamt kommt der Resilienz somit nach dem Telos eine Ergänzungsfunktion vor allem für neue Ungewissheitssituationen zu, die im Bereich des *bekannten Nicht-Wissens* zum einen in offenen Systemen und zum anderen durch den vermehrten Einsatz von KI auftreten. Daneben treten bereits bestehende Ungewissheitssituationen, die aber durch Einführung der Resilienz nun spezifisch mitadressiert werden können wie das Übersehen von Fehlern und Schwachstellen (*unbekanntes Wissen).* Auch das Auftreten von sog. Black Swans (*unbekanntes Nicht-Wissen)* insbesondere durch die Ereignisse infolge globaler und sektorübergreifender IT-Sicherheitslücken (z.B. die bereits genannten *HeartBleed* und *Meltdown*)[613] ist zwar an sich kein neues, zunehmendes Phänomen innerhalb der Informationstechnik wie die steigende Komplexität oder der vermehrte Einsatz von KI. Allerdings nimmt die Folgenschwere solcher zentralen Sicherheitslücken durch die immer breitere Verwendung digitaler Technologien, die auf zentralen IT-Strukturen und IT-Produkten beruhen, stark zu.

All diesen neuen bzw. in ihrer Bedeutung zunehmenden Ereignissen kann nicht mit klassischen, risikospezifischen „Resistenzmaßnahmen", sondern nur mit der Ergänzung der Resilienz begegnet werden. Zugleich wird die Einführung der Resilienz insbesondere in Form adaptiver Maßnahmen erst durch die Flexibilität moderner, komplexer Systeme ermöglicht.

VI. Ergebnis

Nachfolgend soll als Ergebnis der Auslegung nach dem Wortlaut, der systematischen Auslegung sowie der historischen und teleologischen Auslegung eine Definition für den Begriff der Resilienz im Kontext des Art. 32 Abs. 1 lit b) DSGVO gebildet werden. Dabei ist zu beachten, dass bei der auslegenden Definition eines Rechtsbegriffs das Augenmerk auf der *Zweckmäßigkeit* liegen muss. Die Bestimmung eines Fach- bzw. Rechtsbegriffs kann nicht nach absoluten Maßstäben richtig oder falsch, sondern nur mehr oder minder zweckmäßig sein, wobei eine hohe Zweckmäßigkeit eine entsprechend hohe Eindeutigkeit bzw. umgekehrt eine geringe Mehrdeutigkeit

613 Siehe hierzu bereits: S. 170 ff.

voraussetzt.[614] Insbesondere in eine falsche Richtung gehen demnach Begriffsbestimmungen, die bestehende sachliche Zusammenhänge verbergen oder nicht bestehende Zusammenhänge intendieren.[615]

Aus dem *Wortlaut* ergab sich die grundlegende Feststellung, dass Resilienz die Fähigkeit eines soziotechnischen Systems beschreibt, ungewisse Ereignisse zu erkennen, sich an diese zur Minderung der Folgen anzupassen und sich nach einem solchen unter lernender Verbesserung schnellstmöglich zu erholen.

Die *systematische Auslegung* konkretisierte in Gegenüberstellung mit dem Risiko und der Risikomethodik die Erkenntnis, dass Resilienz nicht auf als Risiken antizipierbare Ereignisse, sondern auf ungewisse Ereignisse gerichtet ist.[616] Ihr kommt somit neben der Risikomethodik eine Komplementärfunktion zu.

Die zu adressierende Ungewissheit konnte konkretisierend in die drei Kategorien des bekannten Nicht-Wissens, des unbekannten Wissens und des unbekannten Nicht-Wissens unterteilt werden. Das *bekannte Nicht-Wissen* wird im Rahmen der Risikoidentifikation und -analyse festgestellt (z.B. bei einer vereinfachten Modellierung von Systemen), so dass Resilienzmaßnahmen in dem erkannten Bereich der Ungewissheit ansetzen können. Zum Umgang mit *unbekanntem Wissen* (z.B. Konfigurations- oder Programmierfehler) und *unbekanntem Nicht-Wissen* können hingegen durch die Resilienz nur die bekanntermaßen für die Schutzgüter besonders kritischen Schutzobjekte (besonders sensible Daten oder zentrale IT-Komponenten) betrachtet und diese angesichts der Ungewissheit besonders gesichert werden.

Darüber hinaus wurde festgestellt, dass Resilienzmaßnahmen (nur) *abstrakt angemessen* sein können und müssen, d.h. dass die Angemessenheit sich daran orientiert, welche Schutzgüter betroffen sind und in welcher Höhe hieran Beeinträchtigungen drohen (und nicht etwa wie im Risikomanagement an der zu erreichenden Risikoreduktion, da eine solche bei ungewissen Ereignissen gerade nicht feststellbar ist). Außerdem wurden die Unterschiede zwischen dem Resilienzlernen (neues implizites Wissen über

614 *Bull*, Die Staatsaufgaben nach dem Grundgesetz, S. 43; *Quaritsch*, Staat und Souveränität, S. 21.

615 Wie zuvor.

616 Ähnlich auch auf „insbesondere unvorhergesehene Störungen" abstellend: *Martini*, in: Paal/Pauly, DSGVO, BDSG, 3. Auflage 2021, Art. 32, Rn. 39; „nicht vorhergesehene Änderungen": *M. Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2019, Art. 32, Rn 43.

Bewältigungsstrategien im Umgang mit Ungewissheit) und der Iteration im Risikomanagement (neues explizites Wissen, z.B. über neu entdeckte Schwachstellen, die nun geschlossen werden können) dargestellt.

Weiterhin konnte in der systematischen Auslegung gezeigt werden, dass sich die Resilienz als funktionale Anforderung insbesondere auch zur Reaktion auf bereits eingetretene Sicherheitsvorfälle wesensmäßig von den Schutzzielen unterscheidet und die Resilienz insofern insbesondere keinen solchen „Sollzustand" beschreibt und kein eigenständiges Angriffsziel darstellt.

Schließlich konnte in der *historischen Auslegung* herausgearbeitet werden, dass der Gesetzgeber mit dieser bislang unbekannten Anforderung auf neue Ungewissheitssituationen reagieren wollte, die dann in der *teleologischen Auslegung* insbesondere auf den vermehrten Auftritt offener, interdependenter Systeme sowie den Einsatz von KI exemplarisch verdichtet werden konnten.

Zusammenfassend ist die Resilienz wie folgt auszulegen:

> *Sie ist die Fähigkeit eines soziotechnischen Systems, unmittelbar bevorstehende oder bereits eingetretene Ereignisse, die aufgrund von Ungewissheit nicht vermeidbar sind, zu erkennen und sich an diese anzupassen sowie sich unter lernender Verbesserung schnellstmöglich davon zu erholen.*

Eingeordnet in Art. 32 Abs. 1 lit b) DSGVO muss der Verantwortliche oder der Auftragsverarbeiter somit die *Fähigkeit* der im Zusammenhang mit der Verarbeitung stehenden *(soziotechnischen) Systeme*[617] *unmittelbar bevorstehende oder bereits eingetretene Ereignisse, die aufgrund von Ungewissheit nicht vermeidbar sind, zu erkennen und sich an diese anzupassen sowie sich unter lernender Verbesserung schnellstmöglich davon zu erholen,* auf Dauer sicherstellen. Die Umsetzung erfolgt wie bei allen Punkten des Katalogs in Art. 32 Abs. 1 DSGVO durch technische und organisatorische Maßnahmen.

Die Resilienz als Fähigkeit eines soziotechnischen Systems zielt neben dem Schutz der personenbezogenen Daten insbesondere darauf ab, dass der diese Daten verarbeitende *Dienst*, der hieraus etwa *Personenwissen* erzeugt, trotz des Eintritts ungewisser Ereignisse unbeeinträchtigt bleibt, mithin „resilient" ist.

617 Der Dienst kann davon abweichend als resilient definiert werden, wenn das durch ihn erbrachte funktionale Angebot des Systems trotz Vorliegen ungewisser Ereignisse unbeeinträchtigt bleibt, siehe hierzu: S. 201 f.

D. Demonstration anhand personalisierter Dienste

In diesem Abschnitt soll die rechtspraktische Funktion und Umsetzung der Resilienz anhand des gewählten Szenarios mit dem Angriffsvektor der singulären Informationsmanipulation bei personalisierten Diensten demonstriert werden. Durch das hiermit verbundene Einbringen unrichtiger, personenbezogener Daten in das Persönlichkeitsprofil einer Person können die Rechte und Freiheiten derselben (Schutzgüter), allen voran das Datenschutzgrundrecht, beeinträchtigt werden. Darüber hinaus kann aber auch die Informationsfreiheit beeinträchtigt sein, beispielsweise wenn infolge dieser Manipulation des Profils auch unrichtige Empfehlungen auf z.B. in Online-Suchmaschinen oder sozialen Netzwerken erteilt werden und somit der (personalisierte) Informationsraum manipuliert wird.[618]

I. Ungewissheit

Die personalisierten Dienste werden wie bereits zuvor beschrieben von offenen Systemen erbracht, die einen offenen Kreis von Nutzer:innen aufweisen und von deren Systemen (Endgeräte) Daten empfangen, verarbeiten und an diese ausgeben. Der Verantwortliche und Dienstanbieter hat keine Kontrolle über die diese Daten übermittelnden Endgeräte; sie liegen außerhalb seiner Systemgrenzen.[619]

In den Kategorien der Ungewissheit liegt hier ein Fall des *bekannten Nicht-Wissens* vor, da dem Anbieter des personalisierten Dienstes das fehlende Wissen hinsichtlich der Daten aus dem offenen System bereits bekannt ist. Eine entsprechende Risikoidentifikation und -analyse würde ergeben, dass die Möglichkeit einer Daten- und in der Folge einer Informationsmanipulation existiert, die sich dann auch auf die Wissensgenerierung und die Entscheidung auswirken könnte. Aufgrund der offenen Systemarchitektur und der damit verbundenen fehlenden Kontrolle über die Endgeräte kann aber weder die Wahrscheinlichkeit für das Vorhandensein einer Schwachstelle noch die Ausnutzungswahrscheinlichkeit zum Zwecke der Manipulation (auch unter Berücksichtigung der Motivation des Angreifenden) hinreichend sicher bestimmt werden.

---

618 *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.).

619 Siehe S. 34.

Somit besteht auch Ungewissheit über Art, Umfang und das Ziel einer möglichen Manipulation, so dass auch die Auswirkungen auf das Persönlichkeitsprofil und die Entscheidungsfindung ungewiss sind. Anzumerken ist schließlich, dass bei den Empfehlungssystemen der personalisierten Dienste wie beschrieben häufig auch KI-Komponenten eingesetzt werden. Durch die nur *singuläre Datenmanipulation* werden diese aber im vorliegenden Szenario nicht beeinträchtigt.[620]

Ausgehend von einem der skizzierten personalisierten Dienste verlangt die Resilienz als Datensicherheitsanforderung in diesem Szenario nach den folgenden Gegenmaßnahmen:

II. Resilienzmaßnahmen

Auch die Resilienz wird in ihren einzelnen Ausprägungen durch technische und organisatorische Maßnahmen umgesetzt. Diese werden nachfolgend abstrakt beschrieben und durch einige Beispiele dargestellt.

1. Ereigniserkennung

Im Rahmen der Angriffserkennung müssen ungewisse Ereignisse zunächst durch *detektive Maßnahmen*[621] wie der Einführung sog. Angriffserkennungssysteme erkannt werden. Hierzu kann insbesondere auch eine Anomalieerkennung eingesetzt werden.[622] Sofern explizit das Verhalten der Nutzer:innen bzw. deren Endgeräte auf Anomalien überwacht wird, spricht man auch von User and Entitiy Behavior Analysis (UEBA).[623] Weiterhin können Plausibilitätsprüfungen angestellt werden um manipulierte Einga-

620 KI-Systeme lassen sich durch große, „vergiftete" Datenmengen umtrainieren, wie sie bei der *pluralen Informationsmanipulation* vorliegen, siehe zu diesem Szenario S. 318 ff.

621 Der Begriff „detektive Maßnahmen" findet sich ähnlich auch bei *Weber/Yildiz*, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, S. 16.

622 *Arzt et al.*, MMR 2022, 593 (610); man spricht hier im IT-Sicherheitsrecht (§ 8a Abs. 1a BSIG) auch von Angriffserkennungssystemen, die tradierte sowie KI-gestützte Muster- und Anomalieerkennung als auch heuristische Methoden zur Detektion eines Angriffs (hier Ereignis) einsetzen; *S. Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit 2023, § 8a BSIG, Rn 23 f.

623 Vgl. *Shashanka/Shen/Wang*, in: 2016 IEEE International Conference on Big Data (Big Data), User and entity behavior analytics for enterprise security, 1867 (1867 f.).

ben[624] oder auch unplausible Ergebnisse zu erkennen. Dabei können sehr plötzliche Veränderungen in den Verhaltensmustern oder den Ergebnissen auf eine Manipulation hindeuten.

Im vorliegenden Fall müssen die manipulierten Daten, die von den Endgeräten der Nutzer:innen kommen erkannt werden, so dass insbesondere eine UEBA in Betracht kommt. Nach Erkennung einer Anomalie kann zur Bestätigung derselben als Sicherheitsvorfall ggf. entweder Personal eingesetzt[625] und/oder mit entsprechendem Hinweis auf dieselbe *auch der/die Nutzer:in konsultiert* und zu einem entsprechenden Feedback zu der oder den Anomalie(n) aufgefordert werden, um ggf. schnelle Gewissheit über eine Manipulation der Daten zu erhalten.

2. Anpassungsfähigkeit

Das System muss sich weiterhin an das erkannte Ereignis anpassen, um die Auswirkungen möglichst gering zu halten.[626] Es sind mithin (vorher etablierte) *adaptive Maßnahmen* erforderlich, bei der insbesondere noch unbeeinträchtigte Daten und Komponenten geschützt werden. Dies kann allgemein sowohl technische Maßnahmen (z.B. bei Ausfall von Komponenten die Aktivierung von Redundanzen[627] oder bei Erkennen eines Angriffs das Aktivieren von (halb-)automatisierten Firewall-Regeln, so dass alles bis auf die wichtigsten Prozesse blockiert wird[628]) als auch organisatorische Maßnahmen (z.B. in Form von durch das Personal auszuführenden Notfallplänen[629]) einschließen.

Konkret im vorliegenden Szenario könnte, sofern noch manipulierte Daten eingehen, der Datenzufluss zunächst blockiert werden. Möglich ist dies je nach genauer Angriffskonstellation durch sog. CAPTCHAs, mit denen bei entsprechendem Verdacht geprüft werden kann, ob zumindest tatsäch-

624 Vgl. *Berger et al.*, ACM CSUR, Vol. 54 (2022), Heft 7, 1 (12, 25).
625 Vgl. *Sohr/Kemmerrich*, in: Kipker, Cybersecurity, 49 (102), Rn. 202.
626 Vgl. *Weber/Yildiz*, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, S. 24.
627 *Goessling-Reisemann/Thier*, in: Ruth/Goessling-Reisemann, Handbook on resilience of socio-technical systems, 117 (125).
628 *Pohlmann*, in: Lang/Löhr, IT-Sicherheit, 1 (11); ähnlich auch: Datenisolation und Blockierung von Schnittstellen, so dass die Angreifer:innen nicht weiter im System vordringen können: *Arzt et al.*, MMR 2022, 593 (610).
629 Vgl. hierzu auch aus der Praxis den Angriff auf die zum Sparkassenverbund gehörige „Deutsche Leasing": IT Finanzmagazin, Schwerwiegender Cyberangriff auf Deutsche Leasing, 05.06.2023, 05.06.2023.

lich ein Mensch die den Datenfluss auslösenden Eingaben durchführt.[630] Weiterhin sollten die bereits empfangenen Daten die möglicherweise manipuliert wurden, nicht ohne weiteres in die Personalisierung mit aufgenommen werden, um zu verhindern, dass sie das je nach Erkennungszeitpunkt noch unbeeinträchtigte Personenwissen verändern.

Im Zweifel sollten sie zunächst mit einem „Quarantäne-Status" versehen und deaktiviert werden, um ggf. auch bei einer False-Positive Erkennung noch reagieren zu können.[631] Die Daten können ggf. weiter in den Lernprozess einbezogen werden, die dadurch bedingte Veränderung des Personen- und Lernwissens muss aber jedenfalls reversibel sein, um das manipulationsfreie Profil im Falle des Nachweises eines Angriffs wiederherstellen zu können. Auch hierfür können sowohl technische Maßnahmen vorgesehen werden, also etwa entsprechende automatisierte Vorgänge nach Erkennung des Angriffs als auch organisatorische Maßnahmen wie etwa bei besonders zweifelhaften Fällen die manuelle Untersuchung einzelner Profile durch die Mitarbeitenden.

3. Erholung

Die Erholungsphase dient der Wiederherstellung des ordnungsgemäßen Zustandes (*wiederherstellende Maßnahmen*) der informationstechnischen Systeme, Dienste und Daten. Nach Möglichkeit soll hierbei auch eine lernende Verbesserung der Resilienzmaßnahmen stattfinden. Allgemein müssen in der Erholungsphase insbesondere ggf. gelöschte oder manipulierte Daten nach einem Ereignis aus vorab angelegten Backups wiederhergestellt werden und Systeme sowie Dienste wieder ihre ordnungsgemäße Funktion erbringen.[632] Hierbei können auch Priorisierungen angezeigt sein; etwa um besonders kritische Daten oder Dienste vorrangig wiederherzustellen.[633]

Vorliegend ist nach dem Ergebnis während der Anpassungsphase zu differenzieren: In jedem Fall sollte der personalisierte Dienst schnellstmöglich in den Normalzustand zurückkehren, d.h. entweder die verwendeten

630 *G. Yang/Gong/Cai*, in: Proceedings 2017 Network and Distributed System Security Symposium, Fake Co-visitation Injection Attacks to Recommender Systems, S. 13, der gleichzeitig aber auch auf die Umgehungsmöglichkeit hinweist. Man könnte diese Maßnahme auch als weitere detektive Maßnahme verstehen, sie weist insofern einen Doppelcharakter auf.

631 Vgl. *Arzt et al.*, MMR 2022, 593 (610).

632 Vgl. *Weber/Yildiz*, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, S. 17.

633 Vgl. *Weber/Yildiz*, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, S. 24.

Quarantäne-Daten dauerhaft von der Verarbeitung ausschließen oder die zu Unrecht nicht verwendeten Daten in die weitere Verarbeitung aufnehmen. Etwaige manipulative Veränderungen am Profil müssen umgehend revidiert werden.

Um künftigen Ereignissen besser begegnen zu können, sollte das aus den detektierten Angriffen zu erzielende Wissen genutzt werden (*Lernen*), um insbesondere die Anomalieerkennung sowie ggf. auch die Anpassungsfähigkeiten zu optimieren.

III. Abstrakte Angemessenheit

Für die Frage der abstrakten Angemessenheit und damit den Umfang der zu treffenden Resilienzmaßnahmen ist auf die Modalitäten der Verarbeitung abzustellen, um zu bestimmen welche Schutzgüter betroffen sind und wie stark diese infolge von zumindest teilweise ungewissen Sicherheitsverletzungen beeinträchtigt sein können.

Bei den für die Datensicherheit typischen Vertraulichkeitsfällen wird man insbesondere betrachten müssen, ob und inwieweit besonders sensible Daten (Art. 9 Abs. 1 DSGVO) verarbeitet werden, die ggf. auch ein lohnenswertes Ziel für Angreifer:innen (z.B. für Erpressung) darstellen und welche Schutzgüter bei einer Offenlegung betroffen werden (z.B. neben dem Datenschutzgrundrecht auch das Diskriminierungsverbot).[634]

Bei personalisierten Diensten können infolge der ungewissen Manipulationen der Daten und der insofern manipulierten Informationsinterpretation und Wissenserzeugung *(Personenwissen)* falsche Persönlichkeitsbilder entstehen. Auch die daraus folgenden falschen Dienstentscheidungen können gravierende Folgen haben: Bei sozialen Netzwerken und Online-Suchmaschinen kann dies die individuelle Persönlichkeitsentfaltung stark beeinträchtigen sowie insbesondere auch zu einer politischen Beeinflussung führen. Dies gilt in besonderem Maße soweit durch Manipulationen die ohnehin tendenziell bestehenden Filterblasen (Filter Bubbles)[635] verstärkt

634 Zur Veranschaulichung sei hier exemplarisch auf einen Sicherheitsvorfall verwiesen, bei dem Hacker in Finnland vertrauliche Gesprächsinformationen aus Psychotherapiesitzungen erlangten und die Patient:innen anschließend unter Androhung der Veröffentlichung erpressten: *Muth*, Cyber-Erpresser in Finnland, Süddeutsche Zeitung vom 29.10.2020.

635 *Jürgens/Stark/Magin*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 98 (110); *Pariser*, Filter Bubble, S. 17 ff., 24, 169 ff; welcher die durch ubi-

werden. Aus Sicht der Angreifenden dürften außerdem Journalist:innen[636] und Politiker:innen aufgrund ihres Einflusses auf politische Entscheidungen sowie die öffentliche Meinungsbildung[637] besonders attraktive Ziele darstellen, so dass diese möglicherweise auch individuell besonders gefährdet sind. Im Ergebnis dürfte die abstrakte Angemessenheit somit bei den genannten Diensten Resilienzmaßnahmen in großem Umfang rechtfertigen können.

IV. Fazit

Insgesamt zeigte die Demonstration anhand des konkreten Anwendungsbeispiels der personalisierten Dienste welche Ungewissheit konkret bestehen kann und wie dieser mit der Resilienz begegnet werden kann. Dabei wurde auch gezeigt, wie die einzelnen Elemente der Resilienz durch technische und organisatorische Maßnahmen umgesetzt werden können. Zuletzt wurde konkretisiert, wie der Umfang der angemessenen Resilienzmaßnahmen mit Blick auf die abstrakt drohenden Schutzgutverletzungen durch die Manipulation der personalisierten Dienste bestimmt werden kann.

---

quitäre Personalisierung geschaffene Filter Bubble als einen individuellen, fremdbestimmten und für den Nutzer nicht direkt wahrnehmbaren beschränkten Informationsraum im Internet beschreibt und auf dessen mögliche negative Folgen wie eine (unbemerkte) schwindende Selbstbestimmtheit und eine Beeinträchtigung des demokratischen Austauschs hinweist; Zur Filter Bubble in der Online-Suchmaschine auch: *Lewandowski/Kerkmann/Sünkler*, in: Stark/Dörr/Aufenanger, Die Googleisierung der Informationssuche, 75 (91).

636 Zum generellen Einfluss von sozialen Netzwerken, in diesem Fall X (vormals Twitter), auf die Tätigkeit von Journalist:innen: *McGregor/Molyneux*, Journalism 2020, 597 (597 ff., 607).

637 Hierzu später noch ausführlich: S. 259 ff.

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:

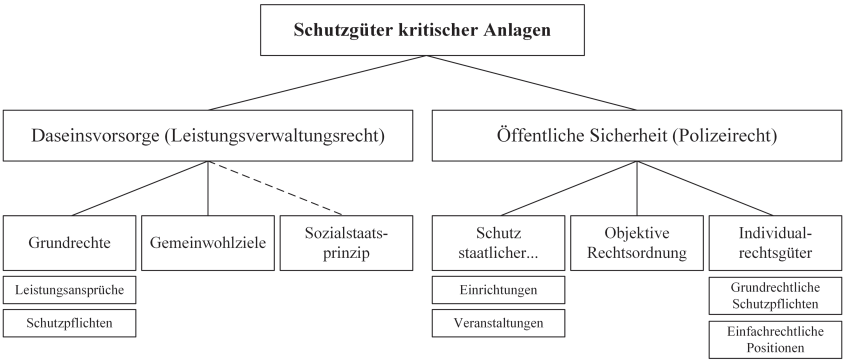

Abbildung 10: Schutzgüter kritischer Anlagen

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.

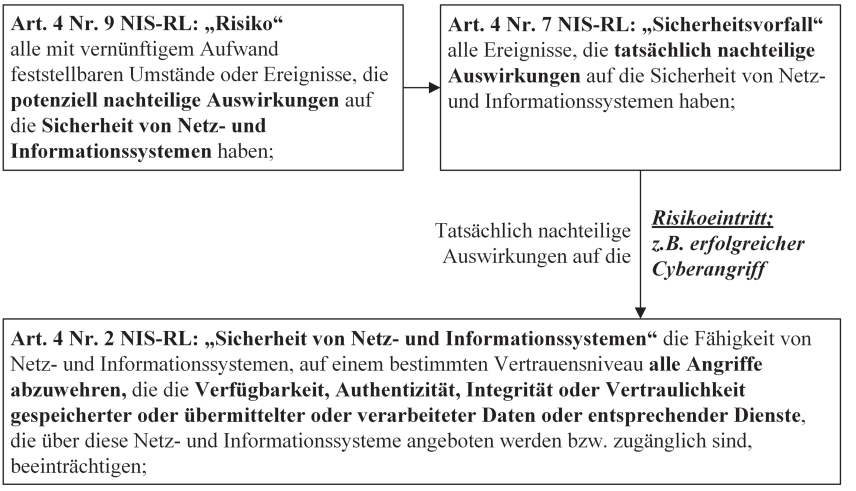

Abbildung 12: Bezugspunkt des Risikos nach NIS-RL

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.*

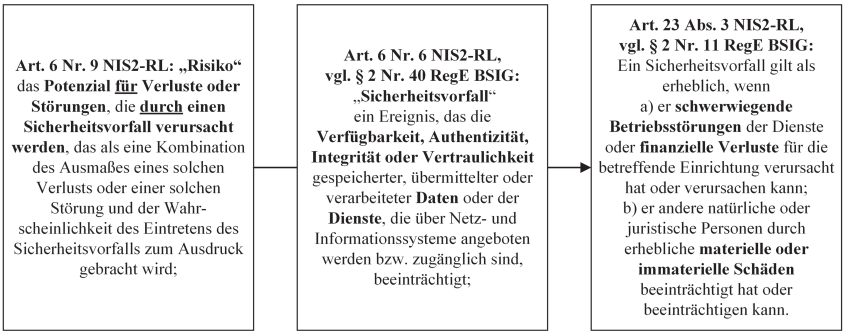

Abbildung 13: Bezugspunkt des Risikos nach NIS2-RL

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 „*Risikomanagementmaßnahmen*", 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.

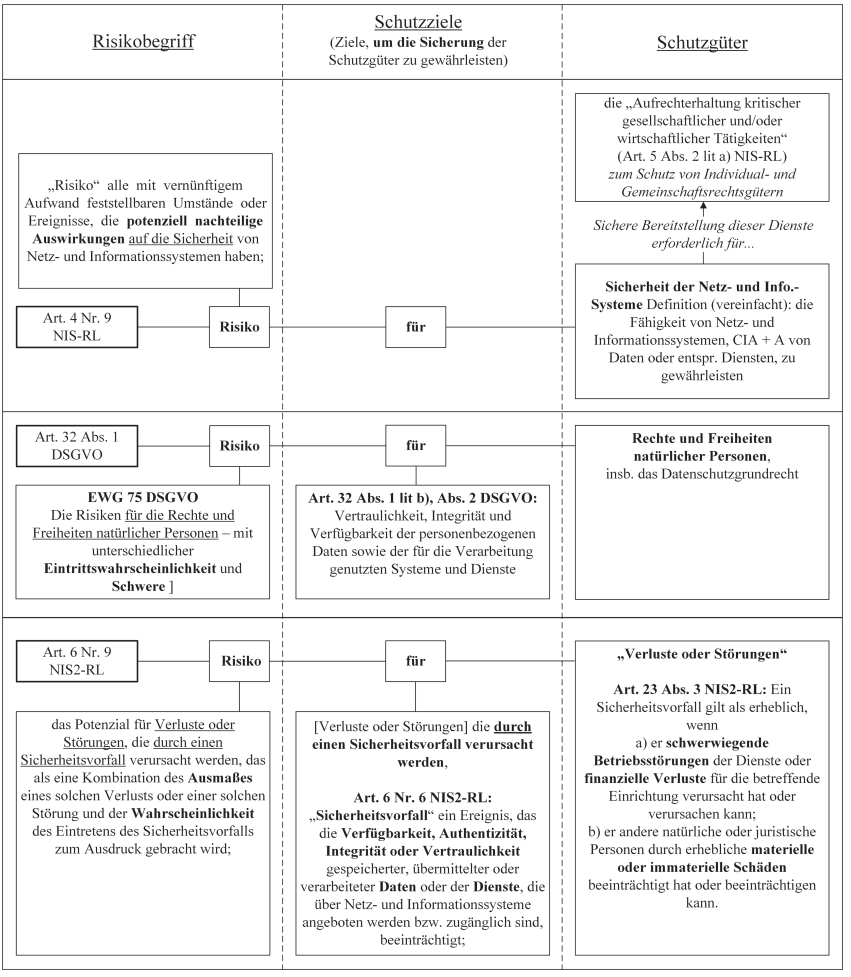

Abbildung 14: Risikobezugspunkte und -definitionen von NIS-RL, DSGVO und NIS2-RL

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.

5. Kapitel: Zusammenfassung und Implementierungsvorschlag

A. Zusammenfassung der Ergebnisse

Die in der Einleitung (1. Kapitel) aufgeworfene Forschungsfrage dieser Untersuchung zielte zunächst darauf zu ermitteln, was nach verständiger Auslegung unter der neuen Datensicherheitsanforderung *Resilienz* (deutscher Wortlaut: Belastbarkeit) nach Art. 32 Abs. 1 lit b) DSGVO zu verstehen ist (3. Kapitel). Weiterhin wurde untersucht, ob dieser Begriff mit seinen so ermittelten Inhalten darüber hinaus auch in das nahestehende IT-Sicherheitsrecht, hier in Gestalt des § 30 RegE BSIG übertragen werden könnte (4. Kapitel), um auf diesem Weg zum einen den regulatorischen Mehrwert der Resilienz auch im IT-Sicherheitsrecht zu nutzen und zum anderen eine größere rechtliche Kohärenz zwischen den beiden Gesetzen zu ermöglichen.

Als exemplarisches Szenario für die Bedeutung der Resilienz wurden personalisierte, digitale Dienste (Online-Suchmaschinen, Online-Marktplätze, soziale Netzwerke) betrachtet, deren Anbieter gerade beiden genannten Gesetzen unterfallen. Technisch wurde auf eine Manipulation dieser Dienste durch das Einbringen falscher Informationen (z.B. tatsächlich nicht durchgeführte Suchanfragen oder sonstiger Interaktionen mit dem jeweiligen Dienst wie Postings oder Likes) abgestellt (2. Kapitel). Dabei war zwischen zwei Manipulationsformen zu unterscheiden: Erstens die für das Datensicherheitsrecht relevante singuläre Informationsmanipulation, d.h. der Manipulation eines einzelnen Persönlichkeitsprofils mit dem Ziel, für eine individuelle, möglicherweise gesellschaftlich besonders wichtige Person falsche Empfehlungen zu erreichen. Und zweitens die für das IT-Sicherheitsrecht relevante plurale Informationsmanipulation, d.h. die großflächig, auch mit gefakten Accounts durchgeführte Manipulation personalisierter Dienste mit dem Ziel, diese in ihrem Empfehlungsverhalten gegenüber möglichst vielen Nutzer:innen zu beeinflussen.

Zum jeweiligen Abschluss der Kapitel 3 und 4 wurde dann auch anhand eben dieses Szenarios die rechtspraktische Bedeutung der Resilienz zur Beschreibung von Maßnahmen gegen diese Formen der Manipulation sowohl aus der Perspektive des Daten- als auch des IT-Sicherheitsrechts

demonstriert. Diese Untersuchung führte zu den nachfolgend dargestellten Ergebnissen:

I. Resilienz in der DSGVO

Die Resilienz i.S.d. Art. 32 Abs. 1 lit b) DSGVO wurde anhand der vier klassischen Auslegungsmethoden am Ende definiert als die

> *Fähigkeit eines soziotechnischen Systems, unmittelbar bevorstehende oder bereits eingetretene Ereignisse, die aufgrund von Ungewissheit nicht vermeidbar sind, zu erkennen und sich an diese anzupassen sowie sich unter lernender Verbesserung schnellstmöglich davon zu erholen.*

Zunächst wurde die *Auslegung nach dem Wortlaut*[950] vorgenommen. Hierfür wurden mangels eines einheitlichen, gewöhnlichen Sprachgebrauchs verschiedenste Fachdomänen untersucht, um hieraus in der Gesamtschau ein Auslegungsverständnis für die Resilienz in der Datensicherheit zu entwickeln: Aus der IT-Sicherheit, dem Katastrophenschutz und dem Schutz kritischer Infrastrukturen konnte zunächst abgeleitet werden, dass die Resilienz sich auch in der Datensicherheit auf ein *soziotechnisches System* beziehen muss. Die Psychologie lieferte dann inhaltlich eine erste Grundlage mit seinem Verständnis der Resilienz als *erfolgreiche Anpassung an bzw. der Erholung von widrigen Ereignissen*. Dabei soll sich die Resilienz gegenüber künftigen Ereignissen im Idealfall steigern, die Resilienz mithin *verbessert* werden. Die technische Resilienz zeigte in Abgrenzung zur Ökologie außerdem auf, dass Resilienz eine (möglichst schnelle) *Rückkehr zu einem bestimmten „Normalzustand"* (Erholung) ermöglichen soll.[951] Die Ökologie konnte statt dieser qualitativen Resilienz[952] aber den Aspekt der quantitativen Resilienz einbringen, nämlich Resilienz als Schwanken von Populationsgrößen, was in der Resilienz der Datensicherheit als das Schwanken des

950 Beginnend auf S. 121; Synthese und Ergebnis: S. 153 ff.

951 Bei der Resilienz von Ökosystemen bestehen hingegen keine vordefinierten Normalzustände, vielmehr können sie um fortzubestehen verschiedene qualitative (und quantitative) Zustände annehmen.

952 Qualitative Resilienz meint die Frage, welcher Zustand erhaltenswert ist. Dies ist in anthropozentrischen Verständnissen von Resilienz stets ein bestimmter, von Menschen angestrebter Zustand; in der Ökologie existiert ein solcher nicht, d.h. die Resilienz von Ökosystemen zielt nur darauf, dass das Ökosystem in irgendeinem Zustand fortbesteht und sich ggf. auch frei evolutionär verändert, ausführlich dazu: S. 153 ff.

Dienstangebots umgesetzt werden kann: Im Rahmen der Anpassung soll demnach ein Dienst (also die Funktionalität eines Systems, z.B. die Online-Suchmaschine) möglichst nicht vollständig ausfallen, sondern besser seine Leistung bei Eintritt eines Ereignisses nur graduell verringern („schwanken"). Die Informationstechnik und das IT-Sicherheitsrecht lieferten außerdem Hinweise auf die Notwendigkeit der vorgelagerten *Erkennung eines Ereignisses* (z.B. durch sog. Angriffserkennungssysteme). Weiterhin härteten diese informationstechnischen Fachdomänen die Resilienzelemente der Anpassungsfähigkeit und der Erholungsfähigkeit einschließlich einer *aus zurückliegenden Ereignissen lernenden Verbesserung* (entsprechende Beispiele folgen sogleich im Szenario). Die IT-Sicherheit zeigte außerdem, dass Resilienz gegen *ungewisse Ereignisse wie z.B. neue bislang unbekannte Angriffsformen* gerichtet ist. Insgesamt lieferte die Wortlautauslegung somit das Grundverständnis mit der Erkennung von ungewissen Ereignissen, die (folgenmindernde) Anpassung an solche sowie die Erholung unter lernender Verbesserung.

Die *systematische Auslegung* belegte zunächst die bisherige Feststellung aus dem Wortlaut, dass sich Resilienz anders als das ihr systematisch gegenüberzustellende Risiko tatsächlich auf ungewisse, d.h. im Gegensatz zum Risiko *nicht* im Vorfeld in ihrer Eintrittswahrscheinlichkeit und Folgenschwere antizipierbare Ereignisse bezieht. Diese Ungewissheit konnte dabei in drei Kategorien, namentlich das bekannte Nicht-Wissen, das unbekannte Wissen und das unbekannte Nicht-Wissen unterteilt werden.[953] Das *bekannte Nicht-Wissen* erfasst die Fälle, bei denen die Risikoidentifikation- und -analyse an ihre Grenzen kommt, z.B. weil offene Systeme vorliegen, die nicht der umfassenden Kontrolle des Normadressaten unterliegen,[954] komplexe Systeme nur vereinfacht modelliert werden können oder KI als nicht vollständig erklärbare Komponente (sog. Blackbox) eingesetzt wird. *Unbekanntes Wissen* liegt z.B. bei Fehlkonfigurationen von IT-Systemen vor, d.h. das richtige Wissen wäre an sich (leicht) vorhanden, wird aber (fahrlässig) nicht genutzt. Schließlich bestehen aus Sicht des Normadressaten gänzlich ungewisse Ereignisse, teilweise auch „Black Swans" genannt, d.h. solche zu denen er kein Wissen hat (Nicht-Wissen) und ihm darüber

953 S. 170 ff.

954 Z.B. ein soziales Netzwerk, bei dem auch alle Endgeräte der Nutzer zu dem System gehören. Der Anbieter des sozialen Netzwerks kontrolliert aber insbesondere die Sicherheit dieser Endgeräte nicht, erhält aber gleichwohl von diesen Daten, die er für die Erbringung seines Dienstes nutzt.

hinaus noch nicht mal bekannt ist, dass hier Ereignisse drohen, zu denen er kein Wissen hat (*Unbekanntes Nicht-Wissen)*. Hierzu gehören etwa Schwachstellen in allgemein verwendeten Sicherheitsprotokollen, z.B. HeartBleed in OpenSSL. Auf die Ungewissheit in all seinen Formen und die damit verbundenen Ereignisse kann die Risikomethodik (auch Risikomanagement) keine Antwort liefern und insofern zeigte sich, dass es sich bei der Resilienz um eine Anforderung für den Umgang mit solchen ungewissen Ereignissen handelt, dessen Implementierung das Risikomanagement insoweit an seinen „blinden Flecken" ergänzt.[955]

Umgekehrt deutete sich aus diesen Feststellungen bereits an, dass es sich, wie im zweiten Abschnitt der systematischen Auslegung dargestellt, bei der Resilienz nicht wie teilweise angenommen um ein weiteres Schutzziel oder gar nur eine Unterausprägung des Schutzziels der Verfügbarkeit handelt.[956] Die *Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität (und Authentizität)* beschreiben anzustrebende „Sollzustände" an Schutzobjekten wie Daten oder Systemen. Als solche gruppieren sie aus einer Bedrohungssicht heraus bestimmte Angriffe und entsprechende Gegenmaßnahmen (z.B. ein Angriff auf die Vertraulichkeit von Daten mit der Gegenmaßnahme der Verschlüsselung der Daten). Sie sind insofern Ausdruck eines durch Härtung der Systeme sicherzustellenden Nicht-Eintritts von als Risiken antizipierten Sicherheitsvorfällen. Die Resilienz ist hingegen eine übergeordnete, funktionale Anforderung an soziotechnische Systeme, die wie beschrieben den Umgang mit ungewissen Ereignissen betrifft, zu denen insbesondere auch die mangels Antizipation gleichwohl eintretenden Sicherheitsvorfälle zu zählen sind. Sie ist damit auch weder ein solcher Sollzustand (sondern soll gerade eingreifen, wenn der Sollzustand nicht mehr vorliegt) noch ein eigenständiges Angriffsziel mit entsprechenden Gegenmaßnahmen.

Schließlich bestätigte sich im dritten Abschnitt der systematischen Auslegung mit Blick auf die *Systeme und Dienste,*[957] auf die sich die Resilienz nach Art. 32 Abs. 1 lit b) DSGVO bezieht, dass *Systeme* anders als bei den nur informationstechnischen Schutzzielen für die Resilienz soziotechnisch zu verstehen sind, was insoweit in der Auslegung der besagten Vorschrift zu einem Auseinanderfallen des Systembegriffs (soziotechnisch für die Resilienz; (nur) informationstechnisch für die Schutzziele) führt.[958] Der *Dienst*

955 Zur methodischen Integration sogleich unter B. Implementierungsvorschlag, S. 333.
956 S. 187 ff.
957 S. 201 ff.
958 Siehe auch hierzu sogleich unter B. Implementierungsvorschlag, S. 333.

hingegen beschreibt das funktionale Angebot eines Systems (z.B. die Suchmaschine) und wird somit von der Resilienz als (weiterer) funktionaler Anforderung an das System nicht unmittelbar betroffen. Er profitiert indes in einer Schutzperspektive von der Resilienz, d.h. der Dienst ist resilient, wenn das durch ihn erbrachte funktionale Angebot des Systems angesichts ungewisser Ereignisse unbeeinträchtigt bleibt.

Aus der *historischen Auslegung*[959] folgte schließlich, dass der Gesetzgeber in der Novellierung des Datenschutzrechts durch die DSGVO mit der Resilienz auf neue Sachphänomene in der Datensicherheit reagieren wollte, für die die bisherige Regelungsmethodik mit Risiken und Schutzzielen nicht hinreichend war. Diese Sachphänomene konnten dann in der *teleologischen Auslegung*[960] insbesondere mit den schon genannten, mit Ungewissheit behafteten Entwicklungen der offenen Systemarchitektur, der gleichzeitig steigenden Komplexität der Systeme und dem zunehmenden Einsatz von KI umschrieben werden.

Anhand des Beispiels der singulären Informationsmanipulation bei personalisierten Diensten konnte die Bedeutung der Resilienz in der Datensicherheit auch rechtspraktisch demonstriert werden,[961] um die *Schutzgüter der DSGVO* zu sichern. Dies betrifft etwa das *Datenschutzgrundrecht* sowie die *Informationsfreiheit* des Betroffenen, die gegenüber der Manipulation ihrer Profile und infolgedessen auch der Dienstentscheidungen, z.B. in Form von falschen Empfehlungen von (einseitigen oder wahrheitswidrigen) Informationen in sozialen Netzwerken oder in Online-Suchmaschinen, gesichert werden müssen.

Die Ungewissheit (in der Kategorie des bekannten Nicht-Wissens) besteht hier darin, dass der Dienstanbieter nicht sicher weiß und auch nicht wissen kann, ob die Daten, die er von seinen (vermeintlichen) Nutzer:innen bekommt, manipuliert sind; insbesondere weil er die IT-Sicherheit der Endgeräte (z.B. Smartphones) dieser Nutzer:innen (in diesem „offenen System") nicht kennt. Um mit dieser Ungewissheit umzugehen, ist eine hinreichende Resilienz durch technische und organisatorische Maßnahmen sicherzustellen. Dies umfasst zunächst die *Erkennung* des Ereignisses, hier in Form der manipulierten Informationen z.B. durch eine Analyse des Nutzerverhaltens oder der Ergebnisse auf ungewöhnliche Ausschläge (Anomalien oder auch Plausibilitätsprüfungen); in Zweifelsfällen kann auch

959 S. 205 ff.
960 S. 208 ff.
961 S. 215 ff.

ein entsprechendes Nutzer-Feedback eingeholt werden. Im Rahmen der *Anpassung,* bei der allgemein gesprochen die Auswirkungen des erkannten Ereignisses möglichst gering gehalten werden sollen, muss der manipulierte Datenfluss unterbunden (z.B. durch CAPTCHAs, mit denen geprüft wird, ob die eingehenden Daten von einem Menschen oder einem Programm erzeugt werden) und mit den bereits eingegangen, ggf. manipulierten Daten umgegangen werden. Bestehen noch Zweifel am Vorliegen einer Manipulation (etwa bei ausbleibendem Feedback des/der Nutzer:in) können die Daten zwar weiter genutzt werden, die dadurch eintretenden Veränderungen müssen aber in jedem Fall reversibel gehalten werden. In der Phase der *Erholung,* d.h. der Wiederherstellung des Normalzustandes, sind dann ebendiese ggf. manipulativen Veränderungen am Persönlichkeitsprofil wieder zu korrigieren. Die Resilienzmaßnahmen sollten im Rahmen der Erholung außerdem soweit möglich aus den entsprechenden Erfahrungen heraus verbessert werden.[962]

Die genannten Maßnahmen müssen dabei *abstrakt angemessen*[963] sein, d.h. sie müssen in ihrem Aufwand gegenüber der abstrakten (aufgrund der Ungewissheit nicht der risikobezogenen) Bedrohung der oben genannten Schutzgüter durch die Verarbeitung verhältnismäßig sein. Hierbei kommt es insbesondere auf die generelle Sensibilität der Daten und der Bedeutung der Dienstscheidungen für die jeweiligen Personen mit ihren Grundrechten an.

II. Übertragbarkeit in den RegE BSIG

In einem zweiten Schritt wurde untersucht, ob die so ausgelegte und am Szenario geprüfte Resilienz in den RegE BSIG übertragen werden könnte. Hierfür wurden zunächst die *Unterschiede zwischen dem IT-Sicherheitsrecht des RegE BSIG (teilweise auch der NIS2-RL) und dem Datensicherheitsrecht nach der DSGVO* betrachtet, von denen die wichtigsten drei hier noch einmal zusammengefasst werden sollen:

Unterschied 1: Bei den Schutzgütern, d.h. den Rechtsgütern, die durch die Gewährleistung von Daten- bzw. IT-Sicherheit gesichert werden sollen,

962 Zur Abgrenzung zur Iteration im Risikomanagement sogleich in der dritten These des Implementierungsvorschlags, S. 333 f.

963 Siehe auch hierzu sogleich noch ausführlich, vierte These, S. 334.

bestehen erhebliche Differenzen:[964] Die DSGVO schützt Individualgrundrechte, insbesondere das *Datenschutzgrundrecht (Art. 8 GRC).* Dagegen schützt das IT-Sicherheitsrecht des RegE BSIG durch die entsprechende Gewährleistung der IT-Sicherheit der *kritischen Anlagen* (z.B. Kraftwerke) neben den Individualgrundrechten wie Leben und Gesundheit insbesondere auch *verschiedene Gemeinwohlziele* (insbesondere im Bereich der Daseinsvorsorge, z.B. sichere Energie- und Trinkwasserversorgung, öffentliche Gesundheit). Dieser Schutz kritischer Anlagen ist für das IT-Sicherheitsrecht historisch prägend und auch weiterhin ein Kernanliegen, daneben werden aber auch die hier gegenständlichen *digitalen Dienste* als sog. wichtige Einrichtungen erfasst. Hier konnten andere Schutzgüter festgestellt werden, so ergaben sich etwa bei Online-Suchmaschinen und sozialen Netzwerken andere Individualgrundrechte, etwa die *Meinungs- und Informationsgrundrechte* als auch andere Gemeinwohlziele wie die *öffentliche Meinungsbildung.*

Unterschied 2: Die *Definitionen von IT-Sicherheit und Datensicherheit* unterscheiden sich bei näherer Betrachtung maßgeblich:[965] Zwar zielen beide zunächst auf die Sicherung der Verfügbarkeit, Vertraulichkeit und Integrität der (personenbezogenen) Daten und Dienste (nur im Falle der Datensicherheit auch der Systeme, dazu sogleich). Mit der *Authentizität* besteht im IT-Sicherheitsrecht aber ein weiteres Schutzziel, welches v.a. in offenen Systemen relevant ist. Dabei bestehen außerdem tendenziell unterschiedliche, teleologische Gewichtungen der Schutzziele: Bei der Datensicherheit liegt dieses Gewicht v.a. in der *Vertraulichkeit der personenbezogenen Daten* und bei der IT-Sicherheit v.a. in der *Verfügbarkeit und Integrität der Dienste.*[966]

Unterschied 3: Das *informationstechnische System (IT-System)* ist ein wesentlicher Anknüpfungspunkt sowohl im Daten- als auch im IT-Sicherheitsrecht. In beiden Fällen ist das System der *Träger der technischen Maßnahmen* (z.B. einer Verschlüsselungsfunktion), die getroffen werden um die jeweilige Sicherheit zu gewährleisten. Darüber hinaus ist aber das System nur in der DSGVO auch selbst ein Schutzobjekt, d.h. auch an diesem sollen

964 Zu den Schutzgütern der DSGVO: S. 105 ff., zu jenen im BSIG bei kritischen Anlagen unter dem Begriff der Daseinsvorsorge, S. 230 ff. und zu jenen bei digitalen Diensten S.254 ff.

965 S. 298.

966 Sowohl mit Blick auf digitale Dienstleistungen als auch (vorgelagerte) IT-Dienste, zu den Unterschieden bei den Dienstbegriffen im IT-Sicherheitsrecht: S. 300 ff.

die Verfügbarkeit, Vertraulichkeit und Integrität sichergestellt werden. Im RegE BSIG ist es hingegen nur ein Maßnahmenträger. Insbesondere die damit fehlende Anforderung der „Integrität der Systeme" könnte wie dargestellt wurde insoweit eine Schutzlücke eröffnen.[967]

Ein ***Gleichlauf*** bzw. eine weitgehende Ähnlichkeit konnte zwischen DSGVO und RegE BSIG bzw. der hierdurch umzusetzenden NIS2-RL beim *Risiko* (sowohl bezüglich seiner Definitionen als auch der *rechtlichen Risikomethodik*[968]) wie auch der *Angemessenheit* festgestellt werden. Hervorzuheben ist an dieser Stelle auch, dass sich zwar nun die Risikobegriffe aus NIS2-RL (und RegE BSIG) auch wie in der DSGVO auf die Schutzgüter beziehen, nicht aber die Pflichtennormen (§ 30 Abs. 1 RegE BSIG, Art. 21 Abs. 1 NIS2-RL), die immer noch (nur) von Risiken bzw. Störungen für die IT-Sicherheit ausgehen. Für die rechtlich geforderte Gewährleistung der IT-Sicherheit (wie auch der Datensicherheit) ist es aber von nicht zu unterschätzender Bedeutung, dass stets auf die *Folgen für die rechtlich relevanten Schutzgüter* (s.o. Unterschied 1) und nicht nur auf die vorgelagerten Schutzziele der IT-Sicherheit (z.B. Integrität von Daten) abgestellt wird.[969]

Die **Übertragung der Resilienz in das IT-Sicherheitsrecht** schließen die dargestellten Unterschiede indes nicht aus:[970] Die Resilienz kann auch zur Sicherung der Schutzgüter des RegE BSIG bei digitalen Diensten einen wichtigen Beitrag leisten, wie sich insbesondere im Szenario (dazu gleich noch näher) zeigte. Sie kann somit nicht nur die Individualrechtsgüter der DSGVO, sondern insbesondere auch die Gemeinschaftsrechtsgüter nach dem RegE BSIG sichern.

Das Schutzziel der Authentizität aus der NIS2-RL adressiert einen weiteren, in offenen Systemen wichtigen Angriffsvektor (Täuschung über die Identität von Entitäten), der auch für die Resilienz bedeutsam sein kann. Dass die Schutzziele im RegE BSIG nicht auf das System bezogen werden, sorgt sogar für größere Kohärenz – da die Resilienz hier als funktionale Anforderung somit (anders als in der DSGVO) nicht neben den wesensmäßig andersartigen Schutzzielen als Sollzuständen am System positioniert werden müsste.

Hilfreich ist für eine Übertragung der Resilienz weiterhin, dass das System im RegE BSIG mit „Komponenten" und „Prozessen" weiter ausdif-

967 S. 303 f.
968 Etwas ausgeprägtere Unterschiede waren bei der privaten Normung festzustellen, siehe hierzu: S. 311 f.
969 S. 307 ff.
970 S. 311 ff.

ferenziert wird. Auf der Kehrseite steht, dass das System im IT-Sicherheitsrecht ausschließlich informationstechnisch (also als IT-System) definiert wird; für die Resilienz als Eigenschaft soziotechnischer Systeme fehlt es somit an einem Anknüpfungspunkt, der auch die soziale Komponente (d.h. das die IT bedienende Personal) einschließt.

Es konnten außerdem zahlreiche bereits im IT-Sicherheitsrecht *existente Ansatzpunkte* identifiziert werden, die in Richtung der Resilienz weisen, wie etwa die Vorgabe von Maßnahmen nach § 30 Abs. 2 Nr. 2 RegE BSIG, Art. 6 Nr. 8 NIS2-RL zur „Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon".[971] Aber es fehlt bislang an einer eigenständigen Definition[972] der Resilienz als übergreifendes Konzept für solche auf Ungewissheit gerichtete Maßnahmen im Bereich des IT-Sicherheitsrechts. Schließlich konnte mit Blick auf die Ungewissheit auch gezeigt werden, dass das IT-Sicherheitsrecht hier teleologisch vor im Vergleich zur DSGVO parallelen Ungewissheitssituationen steht: auch insoweit ist ein Wandel von geschlossenen hin zu offenen Systemen (wie den digitalen Diensten), eine zunehmende Komplexität der IT-Systeme und ein vermehrter Einsatz von KI festzustellen.

Das Resilienz eine Antwort auf diese Situationen nicht nur in der DSGVO, sondern auch im RegE BSIG liefern kann, wurde anhand des Szenarios der personalisierten Dienste noch einmal demonstriert:

Insofern zeigte sich im Vergleich zur DSGVO auch, dass die Resilienz je nach Rechtsgebiet und zu sichernden Schutzgütern z.T. auch unterschiedliche Maßnahmen verlangt: Mussten nach der DSGVO Resilienzmaßnahmen ergriffen werden, um Manipulationen am individuellen Persönlichkeitsprofil zu erkennen und entsprechend darauf zu reagieren, geht es hier um die plurale Informationsmanipulation, d.h. es müssen großflächige, manipulative Angriffe, u.a. auf ML-Systeme („Poisoning Attacks") erkannt und bewältigt werden, um beispielsweise Beeinträchtigungen des Gemeinschaftsrechtsguts der öffentlichen Meinungsbildung durch eine manipulationsbedingte Bevorzugung inhaltlich einseitiger oder sogar wahrheitswidriger Inhalte („Fake News") auf sozialen Netzwerken zu verhindern.

971 S. 313 ff.

972 Lediglich im Bereich der physischen Sicherheit kritischer Infrastrukturen in Art. 2 Nr. 2 RKE-RL, § 2 Nr. 5 RefE KritisDachG existiert eine Definition, die allerdings auch nicht dem hiesigen Verständnis als explizite Antwort auf Ungewissheit entspricht.

Konkret können beispielsweise bei der *Erkennung* statt die Aktivitäten der einzelnen Nutzer:innen z.B. auch bestimmte Elemente auf der Plattform (wie Postings) betrachtet werden, um an diesen starke Ausschläge (Anomalien) bei den Interaktionen (wie etwa den Likes oder den Kommentaren) festzustellen. Bei der *Anpassung* müssen erneut die manipulierten Datenflüsse unterbunden werden (z.B. wieder durch CAPTCHAs) als auch mit den bereits erhaltenen, ggf. manipulierten Daten umgegangen werden. Diese sind dann zu deaktivieren und dürfen insbesondere nicht ohne weiteres für das weitere Training von ML-Systemen verwendet werden, sondern müssen zunächst bereinigt werden.[973] Wenn die Trainingsdaten (gleichwohl) zumindest teilweise schon verwendet wurden, muss im Rahmen der *Erholung* das ML-System dieses ggf. in einen früheren Stand zurückgesetzt und dann mit bereinigten Daten neu trainiert werden. Schließlich sollten die Resilienzmaßnahmen soweit notwendig auch hier für die Zukunft verbessert werden.

Weiterhin müssen diese Resilienzmaßnahmen auch hier *abstrakt angemessen*[974] sein, jedoch nun im Verhältnis zu anderen Schutzgütern als in der DSGVO, d.h. insbesondere gegenüber dem eingangs genannten Gemeinwohlziel der öffentlichen Meinungsbildung. Hierbei kommt es insbesondere auch auf die Anzahl der Nutzer:innen und damit den (quantitativen) Einfluss des Dienstes auf dieses Gemeinwohlziel an.

Eine Übertragung und Implementierung der Resilienz ist im Ergebnis auch im IT-Sicherheitsrecht systematisch durchaus möglich, aufgrund der im IT-Sicherheitsrecht schon bestehenden Ansätze auch naheliegend sowie teleologisch zur Gewährleistung der IT-Sicherheit auch gegenüber neuen Ungewissheitssituationen angezeigt. Letzteres konnte auch noch einmal im konkreten Szenario gezeigt werden.

Die Übertragung würde zugleich zu einer stärkeren Kohärenz des Daten- und IT-Sicherheitsrechts führen. Im Folgenden wird für die gesetzliche Implementierung ein harmonisierender Vorschlag mit den notwendigen Folgeänderungen der Resilienz sowohl im RegE BSIG als auch in der DSGVO unterbreitet.

---

973 Um auch bei einer unbemerkten Nutzung manipulierter Daten für das Training gewappnet zu sein, können mehrere, unterschiedliche ML-Systeme parallel verwendet. Da diese folglich auch unterschiedlich auch auf Angriffe reagieren, kann bei Abweichungen ggf. der Mittelwert oder ein Ergebnis nach Mehrheitsentscheidung gewählt werden, um die Folgen zu minimieren. Für die Erholung gilt hier ebenso, dass ML-Systeme ggf. zurückgesetzt werden müssen.

974 Siehe hierzu sogleich noch ausführlich, S. 334.

B. Implementierungsvorschlag

Die Resilienz als Merkmal der DSGVO hat sich als hilfreiche Ergänzung für das IT-Sicherheitsrecht, jedenfalls im Rahmen des § 30 RegE BSIG, erwiesen und sollte daher auch *de lege ferenda* hierhin übertragen und implementiert werden. Darüber hinaus konnte die Untersuchung beider Rechtsgebiete zeigen, dass diese für die Einführung des Resilienzbegriffs noch nicht die optimalen Rahmenbedingungen bereithalten, die idealiter im Gesetz novellierend eingeführt, andernfalls aber zumindest im Wege der Auslegung mitberücksichtigt werden müssen. Hierfür werden folgende sechs Thesen für das Daten- und das IT-Sicherheitsrecht formuliert:

Erstens wurde festgestellt, dass bislang nicht präzise zwischen den Entscheidungsformen unter antizipierbarer Unsicherheit, namentlich der *Entscheidung unter Risiko* und der *Entscheidung unter Ungewissheit* differenziert wird.[975] Es ist für die Erfüllung des Normauftrags von nicht zu unterschätzender Bedeutung ob Maßnahmen gegenüber antizipierten Ereignissen und damit zur Minderung spezifischer Risiken ergriffen werden oder aber um ungewissen Ereignissen entgegenzutreten. Es wäre daher wünschenswert auch den Begriff der Ungewissheit direkt im Gesetz zu verankern.

Zweitens wurde in der Definition herausgearbeitet, dass Resilienz die Fähigkeit eines *soziotechnischen Systems* darstellt, d.h. auch die soziale Komponente miteinschließt.[976] Zwar erfolgt die Umsetzung der Resilienzmaßnahmen auch nach dem bisherigen Rechtsrahmen sowohl durch technische als auch organisatorische Maßnahmen und führt somit über letztere mittelbar zur Erfassung des soziotechnischen Systems. Trotzdem wäre es wünschenswert den Bezug der Resilienz auf das soziotechnische System insbesondere in Abgrenzung zu den nur auf informationstechnische Systeme und Daten abzielenden Schutzzielen (Verfügbarkeit, Vertraulichkeit, Integrität und ggf. Authentizität) im Gesetz eindeutig hervorzuheben.

Drittens ist es notwendig, dass auch die methodische Verschränkung[977] zwischen der Risikomethodik und der Ungewissheit gesetzlich ausdrücklich hergestellt wird. Es muss zum einen deutlich werden, dass der nach Risikoidentifikation und -analyse verbleibenden Ungewissheit (*bekanntes Nicht-Wissen)* durch entsprechende Resilienzmaßnahmen zu begegnen ist.

975 Ausführlich zu dieser Unterscheidung: S. 169 ff.
976 S. 153.
977 S. 180 ff.

Im Unterschied dazu ist aber auch die Methodik bei *unbekanntem Wissen* und *unbekanntem Nicht-Wissen* zu beachten, worauf nur ausgehend von der Kritikalität der (personenbezogenen) Daten bzw. der jeweils genutzten Informationstechnik (Schutzobjekte) für die Schutzgüter mit Resilienzmaßnahmen reagiert werden kann. Zur Methodik gehört schließlich auch, zwischen der Iteration im Rahmen des Risikomanagements, bei der Risiken für nun *gewisse* Ereignisse (explizites Wissen) minimiert werden (z.B. das Schließen einer nun bekannt gewordenen Schwachstelle) von der lernenden Verbesserung der Resilienzmaßnahmen zu unterscheiden. Letzteres meint die Optimierung der Bewältigungsstrategien (implizites Wissen) dahingehend, in Zukunft noch besser mit anderen *ungewissen* Ereignissen umgehen zu können, d.h. eine bessere Erkennung, eine effizientere Anpassung und eine schnellere, ggf. auch umfassendere Erholung.

Viertens wirken diese bislang bestehenden Defizite bei der Vorgabe der Methodik in einer fehlenden Konkretisierung der Angemessenheit fort. Im Rahmen der Risikomethodik wurde festgestellt, dass die zugehörigen Maßnahmen mit ihrem Aufwand zu der Höhe der mit diesen Maßnahmen zu erreichenden Risikoreduktion verhältnismäßig auszuwählen sind. Da letztere bei der Resilienz aber gerade ungewiss ist, muss statt dieser „Risikoangemessenheit" wie bereits bei dem Szenario angesprochen auf eine *„abstrakte Angemessenheit"* abgestellt werden, bei der statt auf die mit risikospezifischen Maßnahmen zu erreichende Risikoreduktion nur auf die abstrakte Bedrohung der Schutzgüter durch die Datenverarbeitung oder durch die kritische Dienstleistung Bezug genommen wird.[978] Dies bedarf idealiter eines eigenen Anknüpfungspunkts im Gesetzeswortlaut neben der bestehenden risikobezogenen Angemessenheit.

Fünftens beleuchtete diese Arbeit die begleitenden gesetzlichen Vorgaben zur Resilienz im Daten- sowie im IT-Sicherheitsrecht. Hierzu gehörten etwa die Begriffe des Risikos, der Schutzziele sowie der Systeme und Dienste. Es wurde herausgearbeitet, dass diese Begriffe in den jeweiligen Regelungen mitunter zwar unterschiedliche Gewichtungen und Konnotationen haben (insbesondere bei den Schutzzielen und dem Dienst),[979] gleichwohl erscheint aber eine stärkere, begriffliche Harmonisierung in diesen sich oft überschneidenden Regelungen durchaus möglich und sinnvoll.[980] In diesem Zusammenhang ist insbesondere auf die bislang völlig

978 S. 182 f.
979 S. 299 ff.
980 Dazu sogleich im Ausblick: S. 335 f.

unsystematisch erscheinende Umsetzung der IT-Sicherheitsdefinition aus der NIS2-RL in den RegE BSIG hinzuweisen, die insbesondere aufgrund einer kuriosen Vielfalt an Schutzobjekten (Systemen, Komponenten und Prozesse, Informationen, Daten und Dienste) derzeit zur Bestimmung der zu gewährleistenden IT-Sicherheit nur einen Rückgriff auf die Definition der NIS2-RL zulässt.[981] Es bleibt zu hoffen, dass diese gravierenden Widersprüche bis zur finalen Verabschiedung des NIS2UmsuCG und damit des novellierten BSIG noch behoben werden.

Sechstens ist abschließend hervorzuheben, dass diese eindeutige Definition der Resilienz als Fähigkeit eines soziotechnischen Systems im Umgang mit Ungewissheit und den zugehörigen methodischen Folgen zwingend erforderlich ist, damit dieser neue Rechtsbegriff tatsächlich einen Beitrag im Daten- und IT-Sicherheitsrecht leisten kann. Es ist abschließend noch einmal zu betonen, dass die Resilienz nur ein *weiteres, spezifisches Element zur Gewähr der Daten- und IT-Sicherheit* darstellt und diese Begriffe nicht etwa ablöst. Es wurden während der Untersuchung zahlreiche Gesetze im bestehenden IT-Sicherheitsrecht (RefE Kritis-DachG, CRA-E, DORA) analysiert, bei denen es der Resilienz an einer solchen notwendigen Konkretisierung fehlt.[982] Vielmehr zeichnet sich mit dieser Rechtsentwicklung und auch in der öffentlichen sowohl rechtlichen als auch technischen Debatte gegenwärtig eine Tendenz ab, bei der die Resilienz ähnlich wie vormals „*Cyber*sicherheit" zu einem inhaltsleeren Schlagwort verkommt.[983] Dies kann aber im Ergebnis für ein normbestimmtes Daten- und IT-Sicherheitsrecht nicht hingenommen werden.

C. Ausblick

Neben der DSGVO und dem (RegE) BSIG umfasst das Daten- und IT-Sicherheitsrecht auch weitere Gesetze, für welche die Resilienz von Bedeutung sein könnte. In dieser Arbeit wurden insbesondere das EnWG, das TKG, das TDDDG und der DORA im Finanzsektor angesprochen. Die Resilienz nach dem Ergebnis dieser Untersuchung könnte ggf. auch in solche sektoralen IT-Sicherheitsgesetze übernommen werden. Anstatt die

981 S. 263 ff.
982 S. 145 ff.
983 Exemplarisch zuletzt: BReg, Nationale Sicherheitsstrategie 2023, S. 46: „Resilient: Die Sicherung unserer Werte durch innere Stärke".

Resilienz in alle einzelnen Gesetze zu implementieren wäre langfristig aber die Entwicklung eines „IT-Sicherheitsrechts – Allgemeiner Teil," dass übergreifend für die gesamte IT-Infrastruktur die wichtigsten Grundbegriffe und -prinzipien enthält, um ein über die immer stärker vernetzten Teilbereiche reichendes, angemessenes Schutzniveau zu gewährleisten, ein sinnvolles Ziel.[984] Hier könnte die Resilienz somit übergreifend für das gesamte betreiberbezogene IT-Sicherheitsrecht definiert werden.

Weiterhin wurde bereits bei der Eingrenzung des Untersuchungsgegenstands darauf hingewiesen, dass sich die Gewährleistung von IT- und Datensicherheit nicht auf die Perspektive von Betreibern bzw. Verantwortlichen von komplexen, informationstechnischen Systemen wie in den zuvor genannten Gesetzen beschränkt. Zunehmend rückt zur Erhöhung der IT- und Datensicherheit auch eine produkt- und damit herstellerbezogene Regulierung in den Fokus. Der Gewähr der IT- und Datensicherheit durch Betreiber und Verantwortliche sind Grenzen gesetzt. Insbesondere Schwachstellen bzw. nicht vorhandene Sicherheitsfunktionen, die bereits in der Entwicklung der Produkte nicht berücksichtigt bzw. nicht nachträglich durch eine Softwareaktualisierung (Patch) der Hersteller korrigiert oder integriert werden, stellen die Betreiber und Verantwortlichen vor allein kaum zu lösende Herausforderungen. In §§ 41, 2 Nr. 23 RegE BSIG existieren solche Anforderungen deshalb bereits (mittelbar) mit Blick auf sog. „kritische Komponenten", d.h. solchen informationstechnischen Komponenten, die in kritischen Anlagen eingesetzt werden.[985] Eine horizontale Regulierung der IT-Sicherheit für grundsätzlich alle IT-Produkte liefert außerdem der ebenfalls bereits angesprochene CRA-E. Daneben existieren wie ebenfalls bereits genannt bereichsspezifische Regelungen wie die MedizinProdVO oder der RED.

Es erscheint insoweit folgerichtig, die Daten- und IT-Sicherheitsgewähr und somit auch die Resilienz in der Entwicklungs- und Aktualisierungsphase von Produkten und somit auch in diesen gesetzlichen Regelungen zu berücksichtigen. Mit der Produktentwicklung korrespondiert auch eine von

984 Siehe hierzu das Forschungsprojekt ITSR.sys, an dem der Verfasser während der Promotion beteiligt war: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/itsr_sys; Die Ergebnisse wurden insbesondere in *Werner/Brinker/Raabe*, CR 2022, 817 veröffentlicht.

985 Weiterhin müssen diese Komponenten auch in kritischer Funktion eingesetzt werden, d.h. eine Störung der Schutzziele an diesen Komponenten kann insbesondere zu einem Ausfall oder erheblichen Beeinträchtigung der kritischen Anlage führen und sie müssen gesetzlich als solche bestimmt werden (§ 2 Nr. 23 b, c RegE BSIG).

dieser Untersuchung abweichende Interpretation von Resilienz, nämlich in Form von *Resilience by Design*. Während der hier ausgelegte Resilienzbegriff sich auf die Fähigkeit zur adaptiven Reaktion auf eingetretene Ereignisse bezieht, kann auch eine intrinsische Resilienz bereits in der Entwurfsphase von Systemen berücksichtigt werden. Das bedeutet den Eintritt bzw. die Ausbreitung ungewisser Ereignisse bereits durch entsprechende Architektur- oder Designentscheidungen einzuschränken, indem z.B. die zur Ungewissheit führende übermäßige Komplexität soweit noch möglich vermieden wird[986] oder andernfalls komplexe Systeme zumindest segmentiert werden.[987] Neben den Herstellern einzelner Produkte müsste ein solches Prinzip auch bei der Planung der Architektur komplexerer Systeme durch den (künftigen) Betreiber Beachtung finden, um beispielsweise auch durch Diversität der Komponenten besser gegen ungewisse Ereignisse gewappnet zu sein.

Außerdem wurde der *KI-VO-E* angesprochen. Wie in dieser Untersuchung dargestellt, können Resilienzmaßnahmen insbesondere mit Blick auf ungewisse Manipulationen von ML-Systemen eine entscheidende Rolle spielen. Tatsächlich nennt der KI-VO-E auch den Begriff der Resilienz in Art. 15 Abs. 3 und 4. Nach Abs. 4 sollen ML-Systeme gegenüber Versuchen unbefugter Dritter resilient sein, ihre Nutzung, Ergebnisse oder Leistung durch Ausnutzung von Systemschwachstellen zu verändern. Auch die hier behandelten Aspekte der Datenmanipulation (in dem KI-VO-E: als „data poisoning" bzw. „model poisoning" bezeichnet) werden in diesem Kontext genannt. Allerdings ist wie so oft auch hier die Abgrenzung zwischen Resilienz und „Cybersicherheit" nicht eindeutig.[988] Insofern könnte es sich anbieten die hier gefundenen Auslegungsergebnisse zur Resilienz auf die kommende KI-VO zu übertragen, wobei auch hier der zuvor genannte Aspekt des Resilience by Design eine große Rolle spielen dürfte.

Schließlich könnte Resilienz im *organisatorischen bzw. betrieblichen Kontext* eine stärkere Rolle spielen. In dieser Untersuchung wurde dargestellt, dass die Resilienz als Anforderung der Daten- und der IT-Sicherheit zur Bewältigung ungewisser, informationstechnischer Ereignisse auf das soziotechnische System Bezug nimmt, mithin auch das Personal und die Unternehmensstruktur adressiert. Darüber hinaus könnte das Prinzip der

986 *I. Linkov/Kott*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 1 (12).
987 *Bodeau/Graubart*, in: Kott/Linkov, Cyber Resilience of Systems and Networks, 197 (208 f.).
988 Vgl. auch EG 51 KI-VO-E.

Resilienz aber auch zur Bewältigung unternehmerischer, ungewisser Ereignisse genutzt werden, etwa bei Unterbrechungen von Lieferketten oder der Personalverfügbarkeit. Hier könnte die Resilienz somit als Antwort auf ungewisse Ereignisse neben das unternehmerische Risikomanagement (wie es etwa für börsennotierte Unternehmen nach § 91 Abs. 3 AktG verlangt wird) treten.

Insgesamt bleibt damit noch erheblicher Raum für weitere rechtswissenschaftliche Forschung, um die Resilienz über die in dieser Untersuchung gelegten Grundlagen hinaus auf weitere gesetzliche Regelungen innerhalb und außerhalb des Daten- und IT-Sicherheitsrechts mit ggf. auch weiteren, spezifischeren Anforderungen zu erstrecken und fortzuentwickeln.

Literaturverzeichnis

Aamodt, Agnar/Nygård, Mads, Different roles and mutual dependencies of data, information, and knowledge — An AI perspective on their integration, Data & Knowledge Engineering, Vol. 16 (1995), S. 191–222.

Adadi, Amina/Berrada, Mohammed, Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI), IEEE Access 2018, S. 52138–52160.

Aebi, Daniel, Praxishandbuch Sicherer IT-Betrieb, Risiken erkennen Schwachstellen beseitigen IT-Infrastrukturen schützen, Wiesbaden 2004.

Aggarwal, Charu C., Recommender Systems, Cham 2016.

Albers, Marion, § 22 - Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem, Schmidt-Aßmann, Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts II, München 2008, S. 107–220.

Albers, Marion, Die Komplexität verfassungsrechtlicher Vorgaben für das Wissen der Verwaltung, Zugleich ein Beitrag zur Systembildung im Informationsrecht, in: Spiecker gen. Döhmann, Collin (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tagung vom September 2006, Neue Staatswissenschaften Bd. 10, Tübingen 2008, S. 50–69.

Alcorn, Wade, Cross-site scripting viruses and worms – a new attack vector, Network Security 2006, Heft 7, S. 7–8.

Alderson, David, Overcoming barriers to greater scientific understanding of critical infrastructure resilience, in: Ruth, Goessling-Reisemann (Hrsg.), Handbook on resilience of socio-technical systems, Cheltenham/Northampton, Großbritannien 2019, S. 66–88.

Alexander, D. E., Resilience and disaster risk reduction: an etymological journey, Natural Hazards and Earth System Sciences (NHESS) 2013, S. 2707–2716.

Alsubaie, Abdullah/Alutaibi, Khaled/Martí, José, Resilience Assessment of Interdependent Critical Infrastructure, in: Rome, Theocharidou, Wolthusen (Hrsg.), Critical Information Infrastructures Security Bd. 9578, Cham 2016, S. 43–55.

Alt, Ulrich, Datensicherheit, Datenschutz und Technik – ein risikoorientierter Ansatz, Die Sachverständigen 2020, S. 169–172.

Altherr, Lena C./Joggerst, Laura/Leise, Philipp/Pfetsch, Marc E./Schmitt, Andreas/Wendt, Janine, On Obligations in the Development Process of Resilient Systems with Algorithmic Design Methods, Applied Mechanics and Materials (AMM), Vol. 885 (2018), S. 240–252.

Andersson, Jesper/Grassi, Vincenzo/Mirandola, Raffaela/Perez-Palacin, Diego, A Distilled Characterization of Resilience and Its Embraced Properties Based on State-Spaces, in: Calinescu, Di Giandomenico (Hrsg.), Software Engineering for Resilient Systems, 11th International Workshop, SERENE 2019, 17.09.2019, Neapel, Italien, , S. 11–25.

Art.-29 Datenschutzgruppe, WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 16.02.2010.

Art.-29 Datenschutzgruppe, WP 248 Rev. 01, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", 04.10.2017.

Arzt, Clemens/Kleemann, Steven/Plappert, Christian/Rieke, Roland/Zelle, Daniel, Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung, Rechtliche und technische Anforderungen im Verbund, Multimedia und Recht (MMR) 2022, S. 593–614.

Ashby, William Ross, An introduction to cybernetics, New York 1956.

Auernhammer, Herbert, DSGVO BDSG, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze : Kommentar, 7. Aufl., hrsg. von Martin Eßer, Philipp Kramer, Kai von Lewinski, Köln 2020.

Avizienis, Algirdas/Laprie, Jean-Claude/Randell, B./Landwehr, C., Basic concepts and taxonomy of dependable and secure computing, IEEE Transactions on Dependable and Secure Computing (IEEE TDSC) 2004, S. 11–33.

Avizienis, Algirdas/Laprie, Jean-Claude/Randell, Brian, Fundamental Concepts of Dependability, Heft 010028, UCLA CSD Report 2001.

Badawy, Adam/Ferrara, Emilio/Lerman, Kristina, Analyzing the Digital Traces of Political Manipulation: The 2016 Russian Interference Twitter Campaign, in: 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 28.-31.08.2018, Barcelona, Spanien, S. 258–265.

Badriyah, Tessy/Wijayanto, Erry Tri/Syarif, Iwan/Kristalina, Prima, A hybrid recommendation system for E-commerce based on product description and user profile, in: Ariwa, Pichappan (Hrsg.), Seventh International Conference on Innovative Computing Technology (INTECH), 16.-18.08.2017, Luton, Großbritannien, S. 95–100.

Balzert, Helmut, Lehrbuch der Softwaretechnik, Entwurf, Implementierung, Installation und Betrieb, 3. Aufl., Heidelberg 2011.

Bamberg, Günter/Coenenberg, Adolf G./Krapp, Michael, Betriebswirtschaftliche Entscheidungslehre, München 2019.

Bauer, Hartmut, Privatisierung von Verwaltungsaufgaben, 3. Bericht von Prof. Dr. Hartmut Bauer, Dresden, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer (VVDStRL) 1995, S. 243–286.

Beck, Ulrich, Risikogesellschaft, Auf dem Weg in eine andere Moderne, 24. Aufl., Vol. 1365 = Neue Folge Band 365, Frankfurt am Main 2020.

Beckerman, Linda P., Application of complex systems science to systems engineering, Systems Engineering 2000, S. 96–102.

BeckOK Bauordnungsrecht Baden-Württemberg, 27. Aufl., hrsg. von Willy Spannowsky, Michael Uechtritz, 2024 (zit. als *Bearbeiter:in* in: BeckOK BauordnungsR BW).

BeckOK Datenschutzrecht, DS-GVO, DA, DGA, BDSG. Datenschutz und Datennutzung, 47. Aufl., hrsg. von Heinrich Amadeus Wolff, Stefan Brink, Antje von Ungern-Sternberg, 01.02.2024 (zit. als *Bearbeiter:in* in: BeckOK DatenschutzR).

BeckOK Grundgesetz, 57. Aufl., hrsg. von Volker Epping, Christian Hillgruber, 15.01.2024 (zit. als *Bearbeiter:in* in: BeckOK GG).

BeckOK Informations- und Medienrecht, 43. Aufl., hrsg. von Hubertus Gersdorf, Boris P. Paal, 2024 (zit. als *Bearbeiter:in* in: BeckOK InfoMedienR).

BeckOK Polizeirecht BW, 31. Aufl., hrsg. von Markus Möstl, Christoph Trurnit, 2023 (zit. als *Bearbeiter:in* in: BeckOK PolR BW).

Bedner, Mark/Ackermann, Tobias, Schutzziele der IT-Sicherheit, IT-Sicherheit hat den Schutz von elektronisch gespeicherten Informationen und deren Verarbeitung als Ziel. Abzusichernde Eigenschaften und Zustände dieser Informationen und Systeme werden in Form von Schutzzielen der IT-Sicherheit beschrieben., Datenschutz und Datensicherheit (DuD) 2010, S. 323–328.

Beierle, Christoph/Kern-Isberner, Gabriele, Methoden wissensbasierter Systeme, Grundlagen, Algorithmen, Anwendungen, 5. Aufl., Wiesbaden 2014.

Berger, Christian/Eichhammer, Philipp/Reiser, Hans P./Domaschka, Jörg/Hauck, Franz J./Habiger, Gerhard, A Survey on Resilience in the IoT, ACM Computing Surveys (ACM CSUR), Vol. 54 (2022), Heft 7, AS-Nr. 147, S. 1–39.

Berkes, Fikret, Understanding uncertainty and reducing vulnerability: lessons from resilience thinking, Natural Hazards (Nat Hazards), Vol. 41 (2007), S. 283–295.

Berndt, Christina, Resilienz, Das Geheimnis der psychischen Widerstandskraft, München 2015.

Beucher, Klaus/Ehlen, Theresa/Utzerath, Julia, Kap. 14 - Kritische Infrastrukturen, in: Kipker (Hrsg.), Cybersecurity, 2. Auflage, 2023, S. 499–578.

Beyerer, Jürgen/Geisler, Jürgen, A Framework for a Uniform Quantitative Description of Risk with Respect to Safety and Security, European Journal for Security Research (EJSR) 2016, S. 135–150.

Bieker, Felix, Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, Datenschutz und Datensicherheit (DuD) 2018, S. 27–31.

Bieker, Felix/Bremert, Benjamin, Identifizierung von Risiken für die Grundrechte von Individuen, Auslegung und Anwendung des Risikobegriffs der DS-GVO, Zeitschrift für Datenschutz (ZD) 2020, S. 7–14.

Bieker, Felix/Hansen, Marit/Friedewald, Michael, Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung, Recht der Datenverarbeitung (RDV) 2016, S. 188–197.

Bieresborn, Dirk, Teil X, Kap. 1 Umgang mit Patientendaten, in: Forgó, Helfrich, Schneider (Hrsg.), Betrieblicher Datenschutz, Rechtshandbuch, 3. Auflage, München, Wien 2019.

Biggio, Battista/Roli, Fabio, Wild patterns: Ten years after the rise of adversarial machine learning, Pattern Recognition, Vol. 84 (2018), S. 317–331.

Biggs, Reinette/Schlüter, Maja/Biggs, Duan/Bohensky, Erin L./BurnSilver, Shauna/Cundill, Georgina/Dakos, Vasilis/Daw, Tim M./Evans, Louisa S./Kotschy, Karen/Leitch, Anne M./Meek, Chanda/Quinlan, Allyson/Raudsepp-Hearne, Ciara/Robards, Martin D./Schoon, Michael L./Schultz, Lisen/West, Paul C., Toward Principles for Enhancing the Resilience of Ecosystem Services, Annual Review of Environment and Resources (ARER) 2012, S. 421–448.

Bishop, Matt/Carvalho, Marco/Ford, Richard/Mayron, Liam M., Resilience is more than availability, in: Peisert, Ford, Gates et al. (Hrsg.), Proceedings of the 2011 workshop on New security paradigms workshop (NSPW), 12.-15.09.2011, Marin County, USA, S. 95–103.

bitkom e.V., Umfrage: Cookie-Banner spalten Internetnutzer, 10.11.2020, https://www.bitkom.org/Presse/Presseinformation/Cookie-Banner-spalten-Internetnutzer (zugegriffen am 20.3.2024).

Bizer, Johann, Sieben Goldene Regeln des Datenschutzes, Datenschutz und Datensicherheit (DuD) 2007, S. 350–356.

Björck, Fredrik/Henkel, Martin/Stirna, Janis/Zdravkovic, Jelena, Cyber Resilience - Fundamentals for a Definition, in: Rocha, Correia, Costanzo et al. (Hrsg.), New Contributions in Information Systems and Technologies, S. 311–316.

Bock, Kirsten/Meissner, Sebastian, Datenschutz-Schutzziele im Recht, Datenschutz und Datensicherheit (DuD) 2012, S. 425–431.

Bodeau, Deborah/Graubart, Richard, Cyber Resiliency Engineering Framework, MITRE Technical Report, Sep. 2011.

Bodeau, Deborah/Graubart, Richard, Systems Engineering Approaches, in: Kott, Linkov (Hrsg.), Cyber Resilience of Systems and Networks, Cham 2019, S. 197–220.

Boeckelmann, Lukas/Mildner, Stormy-Annika, Unsicherheit, Ungewissheit, Risiko, Die aktuelle wissenschaftliche Diskussion über die Bestimmung von Risiken, SWP-Zeitschriftenschau Sep. 2011, Heft 2, S. 1–8.

Bonß, Wolfgang, Karriere und sozialwissenschaftliche Potenziale des Resilienzbegriffs, in: Endreß, Maurer (Hrsg.), Resilienz im Sozialen, Theoretische und empirische Analysen, Wiesbaden 2015, S. 15.

Bonß, Wolfgang, (Un-)Sicherheit in der Moderne, in: Zoche, Kaufmann, Haverkamp (Hrsg.), Zivile Sicherheit, Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken, Sozialtheorie, Berlin 2010, S. 43–69.

Börding, Andreas/Jülicher, Tim/Röttgen, Charlotte/Schönfeld, Max v., Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, Computer und Recht (CR) 2017, Heft 2, S. 134–140.

Bosse, Christian K./Dehling, Florian/Groen, Eduard C./Salemi, Simone/Schmitt, Hartmut, Auf dem Weg zu gebrauchstauglichen Datenschutzlösungen für digitale Ökosysteme, Datenschutz und Datensicherheit (DuD) 2024, S. 82–88.

Brand, Fridolin/Hoheisel, Deborah/Kirchhoff, Thomas, Der Resilienz-Ansatz auf dem Prüfstand: Herausforderungen, Probleme, Perspektiven, in: Bayerische Akademie für Naturschutz und Landschaftsplege (ANL) (Hrsg.), Landschaftsökologie. Grundlagen, Methoden, Anwendungen, 2011, S. 78–84.

Bräutigam, Peter, Die Weiterentwicklung des E-Commerce zum E-Commerce 2.0, in: Bräutigam, Rücker (Hrsg.), E-Commerce, Rechtshandbuch, München 2017, S. 1–44.

Bretthauer, Sebastian, Smart Meter im Spannungsfeld zwischen Europäischer Datenschutzgrundverordnung und Messstellenbetriebsgesetz, Zeitschrift für das gesamte Recht der Energiewirtschaft (EnWZ) 2017, S. 56–61.

Bröckling, Ulrich, Resilienz: Über einen Schlüsselbegriff des 21. Jahrhunderts, https://nbn-resolving.org/urn:nbn:de:0168-ssoar-80731-7, Soziopolis: Gesellschaft beobachten 2017 (zugegriffen am 20.3.2024).

Bull, Hans Peter, Daseinsvorsorge im Wandel der Staatsformen, Der Staat 2008, S. 1–19.

Bull, Hans Peter, Die Staatsaufgaben nach dem Grundgesetz, Zugl.: Hamburg, Univ., Habil.-Schr., 1972, 2. Aufl., Kronberg im Taunus 1977.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), Online-Glossar des BBK, 2024, https://www.bbk.bund.de/DE/Infothek/Glossar/glossar_node.html (zugegriffen am 17.4.2024).

Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kompendium, 2023, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html (zugegriffen am 17.4.2024).

Bundeskartellamt (BKartA), Beschluss vom 06.02.2019, Az.: B6-22/16, BeckRS 2019, 4895.

Bundeskartellamt (BKartA), Pressemitteilung vom 07.02.2019, Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen, 07.02.2019, https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07_02_2019_Facebook.html (zugegriffen am 17.4.2024).

Bundesministerium des Innern und für Heimat (BMI), Nationale Strategie zum Schutz Kritischer Infrastrukturen, 2009, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3 (zugegriffen am 17.4.2024).

Bundesministerium des Innern und für Heimat (BMI), Nationaler Plan zum Schutz der Informationsinfrastrukturen, Juli 2005, https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05-12-09/05-12-09-anlage-nr-16.pdf?__blob=publicationFile&v=2 (zugegriffen am 17.4.2024).

Bundesministerium des Innern und für Heimat (BMI), Referentenentwurf zum KRITIS-DachG, 21.12.2023.

Bundesministerium des Innern und für Heimat (BMI), Referentenentwurf zum NIS2UmsuCG, 22.12.2023.

Bundesministerium des Innern und für Heimat (BMI), Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden, Mai 2011, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis-leitfaden.pdf;jsessionid=2F83F24C91A35DD1925FBACA7A8FA67B.live872?__blob=publicationFile&v=7 (zugegriffen am 17.4.2024).

Bundesnetzagentur (BNetzA), IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG, Aug. 2015, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=1 (zugegriffen am 14.4.2024).

Bundesnetzagentur (BNetzA), Katalog von Sicherheitsanforderungen nach § 109 TKG, 2. Aufl., 29.04.2020, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=6.

Bundesregierung (BReg), Entwurf NIS2UmsuCG, 22.07.2024, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html (zugegriffen am 20.11.2024).

Bundesregierung (BReg), Nationale Sicherheitsstrategie 2023, Integrierte Sicherheit für Deutschland, https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf (zugegriffen am 17.4.2024).

Burke, Robin/Mobasher, Bamshad/Williams, Chad/Bhaumik, Runa, Classification features for attack detection in collaborative recommender systems, in: Eliassi-Rad, Ungar, Craven et al. (Hrsg.), Proceedings of the 12th ACM SIGKDD, 20.-23.08.2006, Philadelphia, USA, S. 542–547.

Bussche, Axel von dem/Schelinski, Tobias, 7.1 Rechtsgrundlagen und Haftungsfolgen in der IT-Sicherheit, in: Leupold, Wiebe, Glossner (Hrsg.), IT-Recht, Recht, Wirtschaft und Technik der digitalen Transformation, 4. Auflage, München 2021.

Buxmann, Peter/Schmidt, Holger, Grundlagen der Künstlichen Intelligenz und des Machinellen Lernens, in: Buxmann, Schmidt (Hrsg.), Künstliche Intelligenz, Berlin, Heidelberg 2021, S. 3–26.

Bydlinski, Franz, Grundzüge der juristischen Methodenlehre, 2. Aufl., Wien 2012.

Calliess, Christian/Ruffert, Matthias (Hrsg.), EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta : Kommentar, 6. Aufl., München 2022.

Cámara, Javier/Lemos, Rogério de/Vieira, Marco/Almeida, Raquel/Ventura, Rafael, Architecture-based resilience evaluation for self-adaptive systems, Computing 2013, S. 689–722.

Chen, Liang/Xu, Yangjun/Xie, Fenfang/Huang, Min/Zheng, Zibin, Data poisoning attacks on neighborhood-based recommender systems, Transactions on Emerging Telecommunications Technologies (Trans Emerging Tel Tech) 2021, Heft 6, AS-Nr. e3872.

Cherdantseva, Yulia/Hilton, Jeremy, A Reference Model of Information Assurance & Security, in: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), 02.-06.09.2013, Regensburg, S. 546–555.

Classen, Claus Dieter/Nettesheim, Martin, Europarecht, 9. Aufl., München 2021.

Collier, Zachary A./DiMase, Daniel/Walters, Steve/Tehranipoor, Mark Mohammad/Lambert, James H./Linkov, Igor, Cybersecurity Standards: Managing Risk and Creating Resilience, Computer 2014, Heft 9, S. 70–76.

Cornils, Matthias, Staatliche Infrastrukturverantwortung und kontingente Marktvoraussetzungen, Unter besonderer Berücksichtigung des Universaldienstes für Telekommunikationsleistungen, Archiv des öffentlichen Rechts (AöR) 2006, 378-422.

Cutter, Susan L./Ahearn, Joseph A./Amadei, Bernard/Crawford, Patrick/Eide, Elizabeth A./Galloway, Gerald E./Goodchild, Michael F./Kunreuther, Howard C./Li-Vollmer, Meredith/Schoch-Spana, Monica/Scrimshaw, Susan C./Stanley, Ellis M./Whitney, Gene/Zoback, Mary Lou, Disaster Resilience: A National Imperative, Environment: Science and Policy for Sustainable Development 2013, Heft 2, S. 25–29.

Cybersecurity and Infrastructure Security Agency (CISA), A Guide to Critical Infrastructure Security and Resilience, Nov. 2019, https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf (zugegriffen am 15.4.2024).

Cybersecurity and Infrastructure Security Agency (CISA), Strategic Plan 2023-2025, Sep. 2022, https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf (zugegriffen am 15.4.2024).

Daase, Christopher/Kessler, Oliver, Knowns and Unknowns in the `War on Terror': Uncertainty and the Political Construction of Danger, Security Dialogue 2007, S. 411–434.

Danwitz, Thomas von, Was ist eigentlich Regulierung?, Die Öffentliche Verwaltung (DÖV) 2004, S. 977–985.

Datenethikkommission (DEK), Gutachten der DEK, Oktober 2019, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission-kurzfassung.pdf?__blob=publicationFile&v=5 (zugegriffen am 8.4.2024).

Däubler, Wolfgang, Bundesdatenschutzgesetz [a.F.], Kompaktkommentar zum BDSG, 5. Aufl., hrsg. von Wolfgang Däubler, Thomas Klebe, Peter Wedde u.a., Frankfurt a.M. 2016.

Davoudi, Simin, Resilience: A Bridging Concept or a Dead End?, Planning Theory & Practice 2012, S. 299–307.

Deldjoo, Yashar/Di Noia, Tommaso/Merra, Felice Antonio, A Survey on Adversarial Recommender Systems, ACM Computing Surveys (ACM CSUR) 2022, Heft 2, AS-Nr. 35.

Department of Defense (DoD), Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 26.12.1985.

Deusch, Florian/Eggendorfer, Tobias, 50.1 IT-Sicherheit, in: Taeger, Pohle (Hrsg.), Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, 38. EL, München 2023.

Deutsches Institut für Normung e. V. (DIN), ISO/IEC 27000:2017, Informationssicherheits-Managementsysteme – Überblick und Terminologie.

Deutsches Institut für Normung e. V. (DIN), ISO/IEC 27005:2022 (EN), Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

Deutsches Institut für Normung e. V. (DIN), ISO/IEC 29134:2020, Informationstechnik – Sicherheitsverfahren – Leitlinien für die Datenschutz-Folgenabschätzung (ISO/IEC 29134:2017); Deutsche Fassung EN ISO/IEC 29134:2020.

Dewar, Robert, The European Union and Cybersecurity, A Historiography of an Emerging Actor's Response to a Global Security Concern, 2017.

Dewar, Robert/Dunn Cavelty, Myriam, Die Cybersicherheitspolitik der Europäischen Union, Die Cybersicherheitspolitik der Europäischen Union: Bollwerk gegen die Versicherheitlichung eines Politikbereichs, in: Schünemann, Kneuer (Hrsg.), E-Government und Netzpolitik im europäischen Vergleich, 2., aktualisierte und überarbeitete Auflage, E-Government und die Erneuerung des öffentlichen Sektors Band 19, Baden-Baden 2019, S. 281–299.

Diakopoulos, Nicholas, Algorithmic Accountability, Digital Journalism 2015, S. 398–415.

DoD, News Briefing - Secretary Rumsfeld and Gen. Myers, 12.02.2002, https://web.archive.org/web/20160406235718/http://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636 (zugegriffen am 17.3.2024).

Dürig, Günter/Herzog, Roman/Scholz, Rupert (Hrsg.), Grundgesetz, 103. Aufl., 2024.

Ebsen, Ingwer, Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, Deutsches Verwaltungsblatt (DVBl) 1997, S. 1039–1052.

Eckert, Claudia, IT-Sicherheit, 11. Aufl., Berlin, Boston 2023.

Eckhardt, Anne/Rippe, Klaus Peter, Risiko und Ungewissheit bei der Entsorgung hochradioaktiver Abfälle, Zürich 2016.

EDSA, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 02.09.2020, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en (zugegriffen am 15.4.2024).

EDSA, Guidelines 9/2022 on personal data breach notification under GDPR, 2. Aufl., 28.03.2023, https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf (zugegriffen am 23.3.2024).

EDSA, Leitlinien 4/2019 zu Artikel 25, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, 2.0, 20.10.2020.

EDSB, Zusammenfassung der Stellungnahme des EDSB vom 7. März 2012 zum Datenschutzreformpaket, ABl. C 192/7, 30.06.2012.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO, Datenschutz-Grundverordnung, 2. Aufl., München, Wien 2018.

Eigner, Oliver/Eresheim, Sebastian/Kieseberg, Peter/Klausner, Lukas Daniel/Pirker, Martin/Priebe, Torsten/Tjoa, Simon/Marulli, Fiammetta/Mercaldo, Francesco, Towards Resilient Artificial Intelligence: Survey and Research Issues, in: Clarke, Vassilakis (Hrsg.), Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 26-28.07.2021, Rhodos, Griechenland, S. 536–542.

Elran, Meir, Societal Resilience: A Key Response to Severe Terror, in: Gander, Perron, Poscher et al. (Hrsg.), Resilienz in der offenen Gesellschaft, Symposium des Centre for Security and Society, Sicherheit und Gesellschaft Bd. 1, Baden-Baden 2012, S. 291–299.

Emmert, Ulrich, Europäische und nationale Regulierungen, Konsequenzen für den Datenschutz nach dem Ende von Safe Harbor, Datenschutz und Datensicherheit (DuD) 2016, S. 34–37.

Engländer, Armin, Revitalisierung der materiellen Rechtsgutslehre durch das Verfassungsrecht?, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2015, S. 616–633.

ENISA, Glossary Risk Management, 24.07.2009, https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary (zugegriffen am 12.3.2024).

ENISA, Interoperable EU Risk Management Toolbox, 21.02.2023, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox (zugegriffen am 12.3.2024).

Epping, Volker/Lenz, Sebastian/Leydecker, Sebastian, Grundrechte, 10. Aufl., Berlin, Heidelberg 2024.

Ernestus, Walter, § 9, in: Simitis, Dammann, Arendt (Hrsg.), Bundesdatenschutzgesetz, 7., neu bearb. Aufl., Nomos-Kommentar, Baden-Baden 2011.

EU-Kommission, COM(2016) 410 final, Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche, 05.07.2016.

EU-Kommission, COM(2020) 65 final, Weißbuch zur Künstlichen Intelligenz, Ein europäisches Konzept für Exzellenz und Vertrauen, 19.02.2020.

EU-Kommission, JOIN(2013) 1 final, Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, 07.02.2013.

EU-Kommission, JOIN(2020) 18 final, The EU's Cybersecurity Strategy for the Digital Decade, 16.12.2020 (zugegriffen am 21.3.2024).

EU-Kommission, KOM (2001) 298 endgültig, Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz, 06.06.2001.

EU-Kommission, KOM(2003) 270 endgültig, Grünbuch zu Dienstleistungen von allgemeinem Interesse, 21.5.2003.

EU-Kommission, KOM(2004) 375 endgültig, Weißbuch zu Dienstleistungen von allgemeinem Interesse, 12.5.2004.

EU-Kommission, KOM(2006) 251 endgültig, Eine Strategie für eine sichere Informationsgesellschaft – „Dialog, Partnerschaft und Delegation der Verantwortung", 31.05.2006.

EU-Kommission, KOM(2007) 725 endgültig, Begleitdokument zu der Mitteilung „Ein Binnenmarkt für das Europa des 21. Jahrhunderts" - Dienstleistungen von allgemeinem Interesse unter Einschluss von Sozialdienstleistungen: Europas neues Engagement, 20.11.2007.

EU-Kommission, Leistungen der Daseinsvorsorge in Europa, ABl. 1996 Nr. C 281/3.

EU-Kommission, Pressemitteilung vom 25.04.2023, Gesetz über digitale Dienste: Kommission benennt erstmals sehr große Online-Plattformen und Suchmaschinen, https://ec.europa.eu/commission/presscorner/detail/de/ip_23_2413 (zugegriffen am 16.4.2024).

Fang, Minghong/Yang, Guolei/Gong, Neil Zhenqiang/Liu, Jia, Poisoning Attacks to Graph-Based Recommender Systems, in: Proceedings of the 34th Annual Computer Security Applications Conference, 03.-07.12.2008, San Juan, USA, S. 381–392.

Fang, Yiping/Zio, Enrico, Game-Theoretic Decision Making for Game-Theoretic Decision Making for the Resilience of Interdependent Infrastructures Exposed to Disruptions, in: Gritzalis, Theocharidou, Stergiopoulos (Hrsg.), Critical Infrastructure Security and Resilience, Cham 2019, S. 97–114.

Fathi, Karim, Resilienz im Spannungsfeld zwischen Entwicklung und Nachhaltigkeit, Wiesbaden 2019.

Fekete, Alexander/Grinda, Christiane/Norf, Celia, Resilienz in der Risiko- und Katastrophenforschung, Perspektiven für disziplinübergreifende Arbeitsfelder, in: Wink (Hrsg.), Multidisziplinäre Perspektiven der Resilienzforschung, Wiesbaden 2016, S. 215–231.

Fischer, Lars/Lehnhoff, Sebastian, IT security for functional resilience in energy systems: effect-centric IT security, in: Ruth, Goessling-Reisemann (Hrsg.), Handbook on resilience of socio-technical systems, Cheltenham/Northampton, Großbritannien 2019, S. 316–340.

Fischer, Matthias, IT-Sicherheitsanforderungen an Kritische Infrastrukturen und digitale Dienste, in: Hornung, Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2021, S. 299–323.

Folkers, Andreas, Was ist kritisch an Kritischer Infrastruktur?, Kriegswichtigkeit, Lebenswichtigkeit, Systemwichtigkeit und die Infrastrukturen der Kritik, in: Engels, Nordmann (Hrsg.), Was heißt Kritikalität?, 2018, S. 123–154.

Fooken, Insa, Psychologische Perspektiven der Resilienzforschung, in: Wink (Hrsg.), Multidisziplinäre Perspektiven der Resilienzforschung, Wiesbaden 2016, S. 13–45.

Forgó, Nikolaus, Datenschutzrechtliche Fragestellungen des autonomen Fahrens, in: Oppermann, Stender-Vorwachs (Hrsg.), Autonomes Fahren, Rechtsprobleme, Rechtsfolgen, technische Grundlagen, 2. Auflage, 2020, S. 353.

Forschungszentrum Informatik (FZI), Wirksame Sicherheitsmaßnahmen für IoT-Produkte, Ein Ergebnis des Forschungsprojekts DEAL – Demonstration, Erklärung, Anleitung und Lehre zu Prinzipien der IT-Sicherheit., 25.01.2021, https://www.fzi.de/aktuelles/news/detail/artikel/whitepaper-wirksame-sicherheitsmassnahmen-fuer-iot-produkte/.

Forsthoff, Ernst, Rechtsfragen der leistenden Verwaltung, Stuttgart 1959.

Fox, Dirk, Zu einem prinzipiellen Problem digitaler Signaturen, Datenschutz und Datensicherheit (DuD) 1997, S. 386–388.

Franck, Lorenz, Gesetzgebungskompetenz(en) des Bundes für das IT-Sicherheitsrecht Kritischer Infrastrukturen – Teil I, Recht der Datenverarbeitung (RDV) 2022, S. 3–6.

Frankl, Viktor E./Batthyány, Alexander, Wer ein Warum zu leben hat, Lebenssinn und Resilienz, Weinheim, Basel 2017.

Freimuth, Christoph, Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, Dissertation, Berlin, Duncker & Humblot, 2018.

Friauf, Karl Heinrich, Zur Rolle der Grundrechte im Interventions- und Leistungsstaat, Deutsches Verwaltungsblatt (DVBl) 1971, S. 674–682.

Fritz, Florian, Resilienz als sicherheitspolitisches Gestaltungsbild, Faktoren und Metaphern in Fallbeispielen, Vol. 6, Wien 2014.

Fröhlich-Gildhoff, Klaus/Rönnau-Böse, Maike, Resilienz, 2. Aufl., München 2011.

Funtowicz, Silvio/Ravetz, Jerome R., Emergent complex systems, Futures 1994, S. 568–582.

Gabriel, Lorenz, Die Macht digitaler Plattformen, Wiesbaden 2023.

Gadatsch, Andreas/Mangiapane, Markus, IT-Sicherheit, Digitalisierung der Geschäftsprozesse und Informationssicherheit, Wiesbaden 2017.

Gazos, Alexandros, Die soziomaterielle Konstitution von Cybersicherheit in der Dynamik kritischer Informationsinfrastrukturen, in: Villa (Hrsg.), Polarisierte Welten: Verhandlungen des 41. Kongresses der Deutschen Gesellschaft für Soziologie.

Gehrmann, Mareike/Klett, Detlef, IT-Sicherheit in Unternehmen, Weiterhin viel Unsicherheit bei der Umsetzung des IT-Sicherheitsgesetzes, Kommunikation und Recht (K&R) 2017, S. 372–378.

Geppert, Martin/Schütz, Raimund (Hrsg.), Beck'scher Kommentar zum TKG, 5. Aufl., 2023.

Ghafoor, Imran/Jattala, Imran/Durrani, Shakeel/Muhammad Tahir, Ch, Analysis of OpenSSL Heartbleed vulnerability for embedded systems, in: 17th IEEE International Multi Topic Conference 2014, 08.-10.12.2014, Karachi, Pakistan, S. 314–319.

Gierschmann, Sibylle et al. (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln 2018.

Gigerenzer, Gerd, Rationales Entscheiden unter Ungewissheit ≠ Rationales Entscheiden unter Risiko, in: Fleischer (Hrsg.), Rationale Entscheidungen unter Unsicherheit, Abhandlungen der Akademie der Wissenschaften in Hamburg Ser v.8, Berlin/Boston 2019, S. 1–14.

Glinz, Martin, On Non-Functional Requirements, in: 15th IEEE International Requirements Engineering Conference (RE '07), 15.-19.10.2007, Delhi, Indien, S. 21–26.

Goessling-Reisemann, Stefan/Thier, Pablo, On the difference between risk management and resilience management for critical infrastructures, in: Ruth, Goessling-Reisemann (Hrsg.), Handbook on resilience of socio-technical systems, Cheltenham/Northampton, Großbritannien 2019, S. 117–135.

Gola, Peter/Heckmann, Dirk (Hrsg.), DS-GVO, VO (EU) 2016/679 : Kommentar, 3. Aufl., München 2022.

Gola, Peter/Schomerus, Rudolf (Hrsg.), Bundesdatenschutzgesetz [a.F.], 12. Aufl., München 2015.

Gonscherowski, Susan/Hansen, Marit/Rost, Martin, Resilienz – eine neue Anforderung aus der Datenschutz-Grundverordnung, Datenschutz und Datensicherheit (DuD) 2018, S. 442–446.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.), Das Recht der europäischen Union, 80. Aufl., München 2023.

Gramlich, Ludwig, Art. 10 GG nach der zweiten Postreform 1994, Computer und Recht (CR) 1996, S. 102–115.

Grimm, Rüdiger/Waidner, Michael, § 2 - IT-Sicherheit aus technischer Sicht, in: Hornung, Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2021, S. 33–62.

Grossman, Jeremiah, Cross-Site Scripting Worms & Viruses, The Impending Threat & the Best Defense, WhiteHat Security, Juni 2007 (zugegriffen am 15.4.2024).

Gunes, Ihsan/Kaleli, Cihan/Bilge, Alper/Polat, Huseyin, Shilling attacks against recommender systems: a comprehensive survey, Artificial Intelligence Review (AIR) 2014, S. 767–799.

Haack, Stefan, Kommunales W-LAN als Daseinsvorsorge, Verwaltungsarchiv (VerwArch) 2009, S. 197–218.

Häfele, Wolf/Renn, O./Erdmann, G., Risiko, Unsicherheit und Undeutlichkeit, in: Häfele (Hrsg.), Energiesysteme im Übergang, Unter den Bedingungen der Zukunft, Ergebnisse einer Studie des Forschungszentrums Jülich GmbH, Landsberg/Lech 1990, S. 375–423.

Hain, Karl-Eberhard, Medienmarkt im Wandel, Technische Konvergenz und Anbieterkonkurrenz als Herausforderung an Verfassungsrecht und REgulierung, Zeitschrift für Medien- und Kommunikationsrecht; ehemals: Archiv für Presserecht (AfP) 2012, S. 313–328.

Hannak, Aniko/Soeller, Gary/Lazer, David/Mislove, Alan/Wilson, Christo, Measuring Price Discrimination and Steering on E-commerce Web Sites, in: Williamson, Akella, Taft (Hrsg.), Proceedings of the 2014 Conference on Internet Measurement Conference, 05.-07.11.2014, Vancouver, Canada, S. 305–318.

Heckmann, Dirk, Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen, Maßstäbe für ein IT-Sicherheitsrecht, Multimedia und Recht (MMR) 2006, S. 280–285.

Heeks, Richard/Ospina, Angelica V., Conceptualising the link between information systems and resilience: A developing country field study, ISJ (Information Systems Journal) 2019, S. 70–96.

Heinemann, Carmen, Kap. 13, Technischer Datenschutz, in: Moos, Arning, Schefzig (Hrsg.), Die neue Datenschutz-Grundverordnung, Mit Bundesdatenschutzgesetz 2018, De Gruyter Praxishandbuch, Berlin, Boston 2018, S. 463–522.

Heinemeyer, Max/Herpig, Sven, § 3 - Maschinelles Lernen als Angriffsobjekt, in: Ebers, Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, Baden-Baden 2021, S. 65–90.

Heitmann, Marcus, IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie, Wiesbaden 2007.

Helmreich, Isabella/Kunzler, Angela/Lieb, Klaus, Schutzschild gegen Stress, Im OP 2016, Heft 6, S. 270–274.

Henneke, Hans-Günter, Die Daseinsvorsorge in Deutschland, Begriff, historische Entwicklung, rechtliche Grundlagen und Organisation, in: Krautscheid, Waiz, Münch (Hrsg.), Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl, Eine sektorspezifische Betrachtung, Wiesbaden 2009, S. 17–37.

Hennrich, Thorsten, Cloud Computing, Herausforderungen an den Rechtsrahmen für Datenschutz, Berlin 2016.

Herdegen, Matthias, Europarecht, 23. Aufl., 2021.

Hermes, Georg, Gewährleistungsverantwortung als Infrastrukturverantwortung, in: Schuppert (Hrsg.), Der Gewährleistungsstaat, Ein Leitbild auf dem Prüfstand, Baden-Baden 2005, S. 111–132.

Herzog, Roman, § 72 - Ziele, Vorbehalte und Grenzen der Staatstätigkeit, in: Isensee, Kirchhof (Hrsg.), Handbuch des Staatsrechts, Band IV, Historische Grundlagen : Verfassungsstaat : Demokratie - Bundesorgane : Aufgaben des Staates : Rechtsquellen, Organisation, Finanzen : Bundesstaat : Freiheitsrechte : Grundrechte: Wirtschaft, Verfahren, Gleichheit : Allgemeine Grundrechtslehren, 3. Auflage IV, Heidelberg 2006, S. 81–116.

Hiermaier, Stefan/Scharte, Benjamin/Fischer, Kai, Resilience Engineering: chances and challenges for a comprehensive concept, in: Ruth, Goessling-Reisemann (Hrsg.), Handbook on resilience of socio-technical systems, Cheltenham/Northampton, Großbritannien 2019, S. 155–166.

Himeur, Yassine/Sohail, Shahab Saquib/Bensaali, Faycal/Amira, Abbes/Alazab, Mamoun, Latest trends of security and privacy in recommender systems: A comprehensive review and future perspectives, Computers & Security, Vol. 118 (2022), AS-Nr. 102746.

Hof, Hans-Joachim, Datenschutz mittels IT-Sicherheit, in: Tinnefeld, Buchner, Petri et al. (Hrsg.), Einführung in das Datenschutzrecht, Datenschutz und Informationsfreiheit in europäischer Sicht, 7., überarbeitete und aktualisierte Auflage, Berlin, Boston 2020, S. 477–536.

Hoffmann, Gregor Paul, Organisationale Resilienz, Kernressource moderner Organisationen, Berlin, Heidelberg 2017.

Hoffmann-Riem, Wolfgang, Informationelle Selbstbestimmung in der Informationsgesellschaft, Auf dem Wege zu einem neuen Konzept des Datenschutzes, Archiv des öffentlichen Rechts (AöR) 1998, S. 513–540.

Holland, John, Complexity, A Very Short Introduction, 2014.

Holling, Crawford Stanley, Resilience and stability of ecological systems, Annual Review of Ecology and Systematics 1973, S. 1.

Hollnagel, Erik/Woods, David D., Epilogue: Resilience Engineering Precepts, in: Hollnagel, Woods, Leveson (Hrsg.), Resilience engineering, Concepts and precepts, Aldershot, England, Burlington, VT 2006, S. 347–358.

Holznagel, Bernd, Verfassungsrechtliche Fragen der Umsetzung von Art. 17 DSM-RL, Zeitschrift für Urheber- und Medienrecht (ZUM) 2020, S. 1–7.

Honsell, Heinrich, Die rhetorischen Wurzeln der juristischen Auslegung, Zeitschrift für die gesamte Privatrechtswissenschaft (ZfPW) 2016, S. 106.

Hornung, Gerrit/Schallbruch, Martin, § 1 - Einführung, in: Hornung, Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2021, S. 23–32.

Huang, Hai/Mu, Jiaming/Gong, Neil Zhenqiang/Li, Qi/Liu, Bin/Xu, Mingwei, Data Poisoning Attacks to Deep Learning Based Recommender Systems, in: Sadeghi, Koushanfar (Hrsg.), Proceedings 2021 Network and Distributed System Security Symposium, 21.-25.02.2021.

Huber, Peter/Voßkuhle, Andreas (Hrsg.), Grundgesetz, 8. Aufl., 2024.

Isensee, Josef, § 71 - Gemeinwohl im Verfassungsstaat, in: Isensee, Kirchhof (Hrsg.), Handbuch des Staatsrechts, Band IV, Historische Grundlagen : Verfassungsstaat : Demokratie - Bundesorgane : Aufgaben des Staates : Rechtsquellen, Organisation, Finanzen : Bundesstaat : Freiheitsrechte : Grundrechte: Wirtschaft, Verfahren, Gleichheit : Allgemeine Grundrechtslehren, 3. Auflage IV, Heidelberg 2006, S. 3–79.

Isensee, Josef, § 73 - Staatsaufgaben, in: Isensee, Kirchhof (Hrsg.), Handbuch des Staatsrechts, Band IV, Historische Grundlagen : Verfassungsstaat : Demokratie - Bundesorgane : Aufgaben des Staates : Rechtsquellen, Organisation, Finanzen : Bundesstaat : Freiheitsrechte : Grundrechte: Wirtschaft, Verfahren, Gleichheit : Allgemeine Grundrechtslehren, 3. Auflage IV, Heidelberg 2006, S. 117–160.

Isensee, Josef, Das Grundrecht als Abwehrrecht und als staatliche Schutzpflicht, in: Isensee, Kirchhof (Hrsg.), Handbuch des Staatsrechts, Band IX, Historische Grundlagen : Verfassungsstaat : Demokratie - Bundesorgane : Aufgaben des Staates : Rechtsquellen, Organisation, Finanzen : Bundesstaat : Freiheitsrechte : Grundrechte: Wirtschaft, Verfahren, Gleichheit : Allgemeine Grundrechtslehren, 3. Auflage, Heidelberg 2011, S. 413–568.

IT Finanzmagazin, Schwerwiegender Cyberangriff auf Deutsche Leasing, 05.06.2023, https://www.it-finanzmagazin.de/schwerwiegender-cyberangriff-auf-deutsche-leasing-154121/ (zugegriffen am 16.11.2023).

Jagielski, Matthew/Oprea, Alina/Biggio, Battista/Liu, Chang/Nita-Rotaru, Cristina/Li, Bo, Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning, in: 2018 IEEE Symposium on Security and Privacy (SP), 21.-23.05.2018, San Francisco, USA, S. 19–35.

Jandt, Silke, § 17 - IT-Sicherheit als Mittel und als Bedrohung des Datenschutzes, in: Hornung, Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2021, S. 391–414.

Jarass, Hans D., Charta der Grundrechte der Europäischen Union, Unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK : Kommentar, 4. Aufl., München 2021.

Jendrian, Kai/Weinmann, Christoph, Daten und Informationen, Datenschutz und Datensicherheit (DuD) 2010, S. 108.

Jescheck, Hans-Heinrich/Weigend, Thomas, Lehrbuch des Strafrechts, Allgemeiner Teil, 5. Aufl., Berlin 1996.

Jonsson, Erland/Olovsson, Tomas, On the Integration of Security and Dependability in Computer Systems*, in: Pham, Hamza (Hrsg.), Proceedings of the IASTED International Conference on Reliability, Quality Control and Risk Assessment, Washington DC, USA 04-06.11.1992, S. 93–97.

Jung, Maribel, Die Europäisierung des Gemeinwohls am Beispiel des Art. 106 Abs. 2 AEUV, 2018.

Jürgens, Pascal/Stark, Birgit/Magin, Melanie, Gefangen in der Filter Bubble?, Search Engine Bias und Personalisierungsprozesse bei Suchmaschinen, in: Stark, Dörr, Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, Suchmaschinen zwischen Nutzung und Regulierung, De Gruyter eBook-Paket Bibliothekswesen, Dokumentation und Information Bd. 10, Berlin 2014, S. 98–135.

Kalisch, Raffael/Müller, Marianne B./Tüscher, Oliver, Advancing empirical resilience research, Behavioral and Brain Sciences 2015, AS-Nr. e128.

Kamishima, Toshihiro/Akaho, Shotaro, Personalized pricing recommender system, in: Cantador, Brusilovsky, Kuflik (Hrsg.), Proceedings of the 2nd International Workshop on Information Heterogeneity and Fusion in Recommender Systems, , S. 57–64.

Karg, Stefan, Datenschutz und Informationssicherheit: ungleiche Zwillinge, in: Lang, Löhr (Hrsg.), IT-Sicherheit, Technologien und Best Practices für die Umsetzung im Unternehmen, München 2022, S. 99–114.

Kaufmann, Marcel, Integrierte Staatlichkeit als Staatsstrukturprinzip, JuristenZeitung (JZ) 1999, S. 814–822.

Kaufmann, Stefan/Blum, Sabine, Governing (In)Security: The Rise of Resilience, in: Gander, Perron, Poscher et al. (Hrsg.), Resilienz in der offenen Gesellschaft, Symposium des Centre for Security and Society, Sicherheit und Gesellschaft Bd. 1, Baden-Baden 2012, S. 235–257.

Kaur, Parneet/Goel, Shivani, Shilling attack models in recommender system, in: 2016 International Conference on Inventive Computation Technologies (ICICT), 26.-27.08.2016, Coimbatore, Indien, S. 1–5.

Kausar, Mohammad Abu/Dhaka, Vijay/Singh, Sanjeev Kumar, Web Crawler: A Review, International Journal of Computer Applications (IJCA), Vol. 63 (2013), Heft 2, S. 31–36.

Keppler, Martin, Personenbezug und Transparenz im Smart Meter-Datenschutz zwischen europäischem und nationalem Recht, Keine klare Entwicklungslinie durch BDSG, EnWG, MsbG und DS-GVO, Zeitschrift für das gesamte Recht der Energiewirtschaft (EnWZ) 2016, S. 99–106.

Kipker, Dennis-Kenji, Kap. 1, Grundlagen und Strukturen, in: Kipker (Hrsg.), Cybersecurity, 2. Auflage, 2023, S. 1–27.

Kipker, Dennis-Kenji/Dittrich, Tilmann, Rolle der Kritischen Infrastrukturen nach dem neuen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, Nationale Besonderheiten und europäische Überformung, Multimedia und Recht (MMR) 2023, S. 481–487.

Kipker, Dennis-Kenji/Reusch, Philipp/Ritter, Steve (Hrsg.), Recht der Informationssicherheit, München 2023.

Kirchhof, Gregor, Rechtsfolgen der Privatisierung, Jede Privatisierung lockert, löst öffentlich-rechtliche Bindungen, Archiv des öffentlichen Rechts (AöR) 2007, S. 215–256.

Klaus, Marko/Weißhaar, Dominik/Lang, Andreas/Weide, Enrico, Identifizierung relevanter Schutzziele, Datenschutz und Datensicherheit (DuD) 2021, S. 738–741.

Kleim, B./Kalisch, R., Wer bleibt gesund? Zum Problem der Vorhersage von Resilienz, Der Nervenarzt 2018, S. 754–758.

Klein, Hans, Die grundrechtliche Schutzpflicht, Deutsches Verwaltungsblatt (DVBl) 1994, S. 489–497.

Klimke, Dominik, Telematik-Tarife in der Kfz-Versicherung, Recht und Schaden (r+s) 2015, S. 217–225.

Kloepfer, Michael, Informationsrecht, München 2002.

Knauff, Matthias, Der Gewährleistungsstaat: Reform der Daseinsvorsorge, Eine rechtswissenschaftliche Untersuchung unter besonderer Berücksichtigung des ÖPNV, Berlin 2011.

Knieps, Günter, Wettbewerbsökonomie, Regulierungstheorie, Industrieökonomie, Wettbewerbspolitik, 3. Aufl., Berlin, Heidelberg 2008.

Knight, Frank H., Risk, Uncertainty and Profit, 1921.

Koene, Ansgar/Perez, Elvira/Carter, Christopher James/Statache, Ramona/Adolphs, Svenja/O'Malley, Claire/Rodden, Tom/McAuley, Derek, Ethics of Personalized Information Filtering, in: Tiropanis, Vakali, Sartori et al. (Hrsg.), Internet Science, 2nd International Conference (INSCI 2015), 27.-29.05.2015, Brüssel, Belgien, S. 123–132.

Kohpeiß, Marcel/Schaller, Till, Systeme zur Angriffserkennung nach dem neuen EU-Cybersicherheitsrahmen – Hochrisiko-Systeme der KI-Verordnung? — Systeme zur Angriffserkennung unter Berücksichtigung der NIS-2-RL, CER-RL und dem NIS2UmsetzG, sowie eine Einordnung in die Vorschriften der KI-VO, Computer und Recht (CR) 2024, Heft 1, S. 22–29.

Kolcz, Aleksander/Teo, Choon-Hui, Feature weighting for improved classifier robustness, 2009.

Kolliarakis, Georgios, Der Umgang mit Ungewissheit in der Politik ziviler Sicherheit, in: Jeschke, Jakobs, Dröge (Hrsg.), Exploring Uncertainty, Ungewissheit und Unsicherheit im interdisziplinären Diskurs, Textlinguistik & Technikkommunikation, Wiesbaden 2013, S. 313–332.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, 26.04.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf (zugegriffen am 20.3.2024).

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, 17.10.2018, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeDSK.pdf?__blob=publicationFile&v=7 (zugegriffen am 18.1.2024).

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, 3. Aufl.

Königshofen, Mario, Daseinsvorsorge in Zeiten des demographischen Umbruchs, Berlin.

Koreng, Ansgar, Netzneutralität und Meinungsmonopole, in: Stark, Dörr, Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, Suchmaschinen zwischen Nutzung und Regulierung, De Gruyter eBook-Paket Bibliothekswesen, Dokumentation und Information Bd. 10, Berlin 2014, S. 245–261.

Korff, Rüdiger, Resilienz: Eine Frage von Biegen oder Brechen im Ausnahmefall, in: Lewinski (Hrsg.), Resilienz des Rechts, Schriften zum Katastrophenrecht Band 10, Baden-Baden 2016, S. 23–32.

Krafft, Tobias/Gamer, Michael/Laessing, Marcel/Zweig, Katharina, Filterblase geplatzt? Kaum Raum für Personalisierung bei Google-Suchen zur Bundestagswahl 2017, 1. Zwischenbericht Datenspende, Algorithmenwatch (zugegriffen am 20.3.2024).

Krajewski, Markus, Leistungen der Daseinsvorsorge im Gemeinschaftsrecht, Freier Wettbewerb oder öffentliche Aufgabe?, in: Wagner, Wedl (Hrsg.), Bilanz und Perspektiven zum europäischen Recht, Eine Nachdenkschrift anlässlich 50 Jahre Römische Verträge, , S. 433–453.

Krajewski, Markus, Rechtsbegriff Daseinsvorsorge?, Verwaltungsarchiv (VerwArch) 2008, S. 174–196.

Krüger, Marco/Max, Matthias, Resilienz im Katastrophenfall, Konzepte zur Stärkung von Pflege- und Hilfsbedürftigen im Bevölkerungsschutz, 2019.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG, Kommentar, 4. Aufl., München 2024.

Kunzler, A. M./Gilan, D. A./Kalisch, R./Tüscher, O./Lieb, K., Aktuelle Konzepte der Resilienzforschung, Der Nervenarzt 2018, S. 747–753.

Lamker, Christian, Unsicherheit und Komplexität in Planungsprozessen, Planungstheoretische Perspektiven auf Regionalplanung und Klimaanpassung, 2016.

Landmann, Robert von/Rohmer, Gustav (Hrsg.), Umweltrecht, Kommentar, 102. Aufl., München 2023.

Lange, Klaus, Öffentlicher Zweck, öffentliches Interesse und Daseinsvorsorge als Schlüsselbegriffe des kommunalen Wirtschaftsrechts, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2014, S. 616–621.

Laprie, Jean-Claude, From Dependability to Resilience, in: Koopman (Hrsg.), 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), G8-G9.

Laprie, Jean-Claude, Resilience for the Scalability of Dependability, in: Fourth IEEE International Symposium on Network Computing and Applications, 27.-29.07.2005, Cambridge, USA, S. 5–6.

Leisner, Walter Georg, Die subjektiv-historische Auslegung des Gemeinschaftsrechts, Der "Wille des Gesetzgebers" in der Judikatur des EuGH, Europarecht (EuR) 2007, 689-706.

Lewandowski, Dirk/Kerkmann, Friederike/Sünkler, Sebastian, Wie Nutzer im Suchprozess gelenkt werden, Zwischen technischer Unterstützung und interessengeleiteter Darstellung, in: Stark, Dörr, Aufenanger (Hrsg.), Die Googleisierung der Informationssuche, Suchmaschinen zwischen Nutzung und Regulierung, De Gruyter eBook-Paket Bibliothekswesen, Dokumentation und Information Bd. 10, Berlin 2014, S. 75–97.

LfDI BW, Pressemitteilung vom 18.06.2019, LfDI Baden-Württemberg verhängt erstes Bußgeld gegen Polizeibeamten - Mitarbeiter öffentlicher Stellen genießen keine „Immunität“ bei illegaler Datenverarbeitung zu privaten Zwecken –, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/06/Erstes-Bu%C3%9Fgeld-gegen-Polizeibeamten.pdf (zugegriffen am 12.3.2024).

Liedtke, Thomas, Informationssicherheit, Berlin, Heidelberg 2022.

Linden, G./Smith, B./York, J., Amazon.com recommendations: item-to-item collaborative filtering, IEEE Internet Computing 2003, Heft 1, S. 76–80.

Linkov, Igor/Kott, Alexander, Fundamental Concepts of Cyber Resilience: Introduction and Overview, in: Kott, Linkov (Hrsg.), Cyber Resilience of Systems and Networks, Cham 2019, S. 1–25.

Lipp, Moritz/Schwarz, Michael/Gruss, Daniel/Prescher, Thomas/Haas, Werner/Horn, Jann/Mangard, Stefan/Kocher, Paul/Genkin, Daniel/Yarom, Yuval/Hamburg, Mike/Strackx, Raoul, Meltdown: Reading kernel memory from user space, Communications of the ACM (CACM), Vol. 63 (2020), Heft 6, S. 46–56, https://dl.acm.org/doi/fullhtml/10.1145/3357033.

Liszt, Franz von, Rechtgut und Handlungsbegriff im Bindingschen Handbuche, Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 1886, S. 663–698.

Liu, Pan/Xu, Zhenning/Ai, Jun/Wang, Fei, Identifying Indicators of Fake Reviews Based on Spammer's Behavior Features, in: IEEE International Conference on Software Quality, Reliability and Security, 25.-29.07.2017, Prag, Tschechien, S. 396–403.

Longstaff, Patricia H., Complexity and Resilience: Concepts for Community Security, in: Gander, Perron, Poscher et al. (Hrsg.), Resilienz in der offenen Gesellschaft, Symposium des Centre for Security and Society, Sicherheit und Gesellschaft Bd. 1, Baden-Baden 2012, S. 259–279.

Lösel, Friedrich/Farrington, David P., Direct protective and buffering protective factors in the development of youth violence, American Journal of Preventive Medicine (AJPM), Vol. 43 (2012), 8-23.

Louis, Hans Walter, Die Besteuerung der öffentlichen Unternehmen und Einrichtungen der Daseinsvorsorge, Göttingen 1981.

Lu, Jie/Wu, Dianshuang/Mao, Mingsong/Wang, Wei/Zhang, Guangquan, Recommender system application developments: A survey, Decision Support Systems, Vol. 74 (2015), S. 12–32.

Luch, Anika D./Schulz, Sönke E., eDaseinsvorsorge, Neuorientierung des überkommenen (Rechts-)Begriffs „Daseinsvorsorge" im Zuge technischer Entwicklungen?, Multimedia und Recht (MMR) 2009, S. 19–24.

Luhmann, Niklas, Soziologische Aufklärung 5, Konstruktivistische Perspektiven, 3. Aufl., Wiesbaden 2005.

Luo, Weimin/Liu, Jingbo/Liu, Jing/Fan, Chengyu, An Analysis of Security in Social Networks, in: Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), 12.-14.12.2009, Chengdu, China, S. 648–651.

Ma, Zhongming/Pant, Gautam/Sheng, Olivia R. Liu, Interest-based personalized search, ACM Transactions on Information Systems (ACM TOIS), Vol. 25 (2007), Heft 1, AS-Nr. 5, S. 1–38.

Machida, Fumio, On the Diversity of Machine Learning Models for System Reliability, in: IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), 01.-03.12.2019, Kyoto, Japan, S. 276–285.

Mahmood, Tropa/Adnan, Muhammad Abdullah, Detecting Fake Co-visitation Injection Attack in Graph-based Recommendation Systems, in: 9th International Conference on Networking, Systems and Security (NSysS), 20.-22.12.2022, Cox's Bazar, Bangladesch, S. 30–40.

Mahmoud, Dima S./John, Robert I., Enhanced content-based filtering algorithm using Artificial Bee Colony optimisation, in: SAI Intelligent Systems Conference (IntelliSys), 10.-11.11.2015, London, Großbritannien, S. 155–163.

Mangoldt, Hermann von/Klein, Friedrich/Starck, Christian (Hrsg.), Grundgesetz, 7. Aufl., München 2018.

Masing, Johannes, Herausforderungen des Datenschutzes, Neue Juristische Wochenschrift (NJW) 2012, S. 2305–2311.

Maurer, Hartmut/Schwarz, Kyrill-Alexander, Staatsrecht I, 7. Aufl., München 2023.

Maurer, Hartmut/Waldhoff, Christian, Allgemeines Verwaltungsrecht, 20. Aufl., München 2020.

Mayras, Henri, Schlussanträge EuGH Urt. v. 23.10.1974 – Rs. 32/74.

McGregor, Shannon C./Molyneux, Logan, Twitter's influence on news judgment: An experiment among journalists, Journalism 2020, S. 597–613.

Menges, Eva, § 23 - Basiskonto, in: Ellenberger, Bunte (Hrsg.), Bankrechts-Handbuch, 6. Aufl., München 2022.

Menges, Günter, Kriterien optimaler Entscheidungen unter Ungewißheit, Statistische Hefte (Statistische Hefte) 1963, S. 151–171.

Meridan Institute, Definitions of Community Resilience: An Analysis, A CARRI Report, https://s31207.pcdn.co/wp-content/uploads/2019/08/Definitions-of-community-resilience.pdf.

Merkow, Mark S./Raghavan, Lakshmikanth, Secure and resilient software, Requirements, test cases, and testing methods. - "An Auerback book.", Boca Raton, Fla. 2012.

Merz, Fabien, Cybersicherheit: Was lässt sich von Israel lernen?, in: Nünlist, Thränert (Hrsg.), Bulletin 2018 zur schweizerischen Sicherheitspolitik, , S. 73–91.

Metzger, Jan, Das Konzept "Schutz kritischer Infrastrukturen" hinterfragt, in: Wenger (Hrsg.), Bulletin 2004 zur schweizerischen Sicherheitspolitik, 2004, S. 73–85.

Meyer, Jürgen/Hölscheidt, Sven (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019.

Milker, Jens, "Social-Bots" im Meinungskampf, Zeitschrift für Urheber- und Medienrecht (ZUM) 2017, S. 216–222.

Mitsch, Lukas, Soziale Netzwerke und der Pradigmenwechsel des öffentlichen Meinungsbildungsprozesses, Deutsches Verwaltungsblatt (DVBl) 2019, S. 811–818.

Monschke, Julian/Copeland, Victoria, Ein Überblick über Pflichten von Unternehmen im besonderen öffentlichen Interesse gemäß § 2 Abs. 14 BSIG, Corporate Compliance Zeitschrift (CCZ) 2022, S. 152–154.

Montgomery, Alan L./Smith, Michael D., Prospects for Personalization on the Internet, Journal of Interactive Marketing 2009, S. 130–137.

Mühlenkamp, Holger, "Marktversagen" als ökonomische Begründung für Interventionen der öffentlichen Hand, in: Hrbek, Nettesheim (Hrsg.), Europäische Union und mitgliedstaatliche Daseinsvorsorge, Baden-Baden 2002, S. 65–78.

Müller-Quade, Jörn/Meister, Gisela/Holz, Thorsten/Houdeau, Detlef/Rieck, Konrad/Rost, Peter/Schauf, Thomas/Schindler, Werner, Whitepaper: Künstliche Intelligenz und IT-Sicherheit, https://www.acatech.de/wp-content/uploads/2019/04/Whitepaper_AG3_final.pdf, April 2019 (zugegriffen am 21.4.2024).

Müller-Terpitz, Ralf, Filter als Gefahr für die Meinungspluralität?, Verfassungsrechtliche Erwägungen zum Einsatz von Filtertechnologien, Zeitschrift für Urheber- und Medienrecht (ZUM) 2020, S. 365–374.

Muth, Max, Cyber-Erpresser in Finnland, Süddeutsche Zeitung vom 29.10.2020, https://www.sueddeutsche.de/digital/vastaamo-erpresser-cyberkriminalitaet-1.5097181 (zugegriffen am 18.3.2024).

Nadeborn, Diana/Dittrich, Tilmann, Cybersicherheit in Krankenhäusern – Teil 1: IT-Compliance als Leitungsaufgabe, International Cybersecurity Law Review (Int. Cybersecur. Law Rev.) 2022, S. 147–161.

NASA, Program Management and Procurement Procedures and Practices, Hearings Before the Subcommittee on Space Science and Applications of the Committee on Science and Technology, U.S. House of Representatives, Ninety-seventh Congress, First Session, 24.06.1981, https://books.google.de/books?id=dRMrAAAAMAAJ (zugegriffen am 17.4.2024).

Nassif, Ali Bou/Talib, Manar Abu/Nasir, Qassim/Dakalbab, Fatima Mohamad, Machine Learning for Anomaly Detection: A Systematic Review, IEEE Access, Vol. 9 (2021), S. 78658–78700.

National Infrastructure Advisory Council (NIAC), Critical Infrastructure Resilience, Final report and recommendations, 08.09.2009, https://www.cisa.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf (zugegriffen am 17.4.2024).

Nell, Ernst Ludwig, Wahrscheinlichkeitsurteile in juristischen Entscheidungen, Zugl.: Bayreuth, Univ., Diss., 1982-1983, Vol. 446, Berlin 1983.

Nerdinger, Friedemann W./Blickle, Gerhard/Schaper, Niclas, Arbeits- und Organisationspsychologie, Berlin, Heidelberg 2014.

OECD, Concepts and dilemmas of State building in fragile situations, From fragility to resilience, 2009, https://www.oecd.org/dac/conflict-fragility-resilience/docs/41100930.pdf (zugegriffen am 17.4.2024).

Paal, Boris P./Hennemann, Moritz, Meinungsbildung im digitalen Zeitalter, Regulierungsinstrumente für einen gefährdungsadäquaten Rechtsrahmen, JuristenZeitung (JZ) 2017, S. 641–652.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), DSGVO, BDSG, 3. Aufl., München 2021.

Pagenkopf, Martin, Glücksspielrechtliche Variationen, Urt.e des BVerwG vom 24. 11. 2010, Neue Juristische Wochenschrift (NJW) 2011, S. 513–522.

Pariser, Eli, Filter Bubble, Wie wir im Internet entmündigt werden, München 2012.

Park, J./Seager, T. P./Rao, P. S. C./Convertino, M./Linkov, I., Integrating risk and resilience approaches to catastrophe management in engineering systems, Risk analysis 2013, S. 356–367.

Pechstein, Matthias/Nowak, Carsten/Häde, Ulrich (Hrsg.), Frankfurter Kommentar zu EUV, GRC und AEUV, 2. Aufl., Tübingen 2023.

Pfannkuch, Benjamin, Ladeinfrastruktur als Bestandteil der Daseinsvorsorge, Kommunaljurist (KommJur) 2023, S. 245–249.

Pfitzmann, Andreas, Buchbesprechung: Jean-Cloaude Laprie, Dependability: Basic Concepts and Terminology […] Wien 1992, Datenschutz und Datensicherheit (DuD) 1993, S. 539–540.

Picot, Arnold/Neuburger, Rahild, Controlling von Wissen, Zeitschrift für Controlling & Management (ZfCM) 2005, S. 76–85.

Pieper, Stefan Ulrich, B. I. Rechtsquellen, in: Dauses, Ludwigs (Hrsg.), Handbuch des EU-Wirtschaftsrechts, Stand: Januar 2022 Bd. 1,

Pille, Jens-Ullrich, Meinungsmacht sozialer Netzwerke, Baden-Baden 2016.

Plath, Kai-Uwe (Hrsg.), BDSG Kommentar, Saarbrücken, Köln 2013.

Plath, Kai-Uwe (Hrsg.), DSGVO, BDSG, TTDSG Kommentar, 4. Aufl., Köln 2023.

Pohlmann, Norbert, IT-Sicherheit konsequent und effizient umsetzen, in: Lang, Löhr (Hrsg.), IT-Sicherheit, Technologien und Best Practices für die Umsetzung im Unternehmen, München 2022, S. 1–22.

Portugal, Ivens/Alencar, Paulo/Cowan, Donald, The use of machine learning algorithms in recommender systems: A systematic review, Expert Systems with Applications, Vol. 97 (2018), S. 205–227.

Poscher, Ralf/Lassahn, Philipp, § 7 - Verfassungsrechtliche Dimensionen der IT-Sicherheit, in: Hornung, Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2021, S. 133–153.

Prell, Lorenz, E-Government: Paradigmenwechsel in Verwaltung und Verwaltungsrecht?, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2018, S. 1255–1259.

Püttner, Günter, Das grundlegende Konzept der Daseinsvorsorge, Kommunale Daseinsvorsorge - Begriff, Geschichte, Inhalte, in: Hrbek, Nettesheim (Hrsg.), Europäische Union und mitgliedstaatliche Daseinsvorsorge, Baden-Baden 2002, S. 32–38.

Quaritsch, Helmut, Staat und Souveränität, Frankfurt am Main 1970.

Raabe, Oliver/Schallbruch, Martin/Steinbrück, Anne, Systematisierung des IT-Sicherheitsrechts, Computer und Recht (CR) 2018, S. 706–715.

Rajamaki, Jyri/Nevmerzhitskaya, Julia/Virag, Csaba, Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF), in: Proceedings of 2018 IEEE Global Engineering Education Conference (EDUCON), 17.-20.04.2018, Santa Cruz de Tenerife, Spanien, S. 2042–2046.

Randell, B./Lee, P./Treleaven, P. C., Reliability Issues in Computing System Design, ACM Computing Surveys (ACM CSUR) 1978, S. 123–165.

Ratasich, Denise/Khalid, Faiq/Geissler, Florian/Grosu, Radu/Shafique, Muhammad/Bartocci, Ezio, A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems, IEEE Access 2019, S. 13260–13283.

Rath, Michael/Feuerherdt, Gerrit, Datenschutz-Folgenabschätzung als Standard im Konzern, Hinweise zur Anwendung des Kriteriums „hohes Risiko" einer Datenverarbeitung und Vorschläge zur Verknüpfung mit dem Standard- Datenschutzmodell sowie den ISO-Standards 29100 und 29134, Computer und Recht (CR) 2017, S. 500–504.

Raue, Benjamin, Meinungsfreiheit in sozialen Netzwerken, Ansprüche von Nutzern sozialer Netzwerke gegen die Löschung ihrer Beiträge, JuristenZeitung (JZ) 2018, S. 961–970.

Reviglio, Urbano/Agosti, Claudio, Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media, 28.04.2020, DOI: 10.1177/2056305120915613, Social Media + Society (SM+S) 2020, Heft 2.

Ricci, Francesco/Rokach, Lior/Shapira, Bracha/Kantor, Paul B., Recommender systems handbook, New York 2011.

Riesenhuber, Karl, § 10 Auslegung, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, Handbuch für Ausbildung und Praxis, 4. Auflage, Berlin 2021, S. 285–321.

Ritter, Franzisika/Reibach, Boris/Lee, Morris, Lösungsvorschlag für eine praxisgerechte Risikobeurteilung von Verarbeitungen, Ansatz zur Bestimmung von Eintrittswahrscheinlichkeit und Schadensausmaß bei der Bewertung datenschutzrechtlicher Risiken, Zeitschrift für Datenschutz (ZD) 2019, S. 531–535.

Rockström, Johan/Steffen, Will/Noone, Kevin/Persson, Åsa/Chapin, F. Stuart, III/Lambin, Eric/Lenton, Timothy M./Scheffer, Marten/Folke, Carl/Schellnhuber, Hans Joachim/Nykvist, Björn/Wit, Cynthia A. de/Hughes, Terry/van der Leeuw, Sander/Rodhe, Henning/Sörlin, Sverker/Snyder, Peter K./Costanza, Robert/Svedin, Uno/Falkenmark, Malin/Karlberg, Louise/Corell, Robert W./Fabry, Victoria J./Hansen, James/Walker, Brian/Liverman, Diana/Richardson, Katherine/Crutzen, Paul/Foley, Jonathan, Planetary Boundaries: Exploring the Safe Operating Space for Humanity, Ecology and Society (E&S), Vol. 14 (2009), Heft 2, AS-Nr. 32.

Ronellenfitsch, Michael, Daseinsvorsorge und service d'intégrêt général im Interventionsstaat, in: Magiera, Sommermann (Hrsg.), Daseinsvorsorge und Infrastrukturgewährleistung, Symposium zu Ehren von Willi Blümel zum 80. Geburtstag, Schriftenreihe der Hochschule Speyer Bd. 200, Berlin 2009, S. 27–63.

Ronellenfitsch, Michael, Der Verkehrssektor als Bereich der öffentlichen Daseinsvorsorge in Deutschland, in: Hrbek, Nettesheim (Hrsg.), Europäische Union und mitgliedstaatliche Daseinsvorsorge, Baden-Baden 2002, S. 89–95.

Ross, Ron/Pillitteri, Victoria/Graubart, Richard/Bodeau, Deborah/McQuaid, Rosalie, Developing cyber resilient systems, Gaithersburg, USA 2019.

Rost, Martin, Die Ordnung der Schutzziele, Datenschutz und Datensicherheit (DuD) 2018, S. 13–17.

Roth, Wulf-Henning/Jopen, Christian, § 13 - Die richtlinienkonforme Auslegung, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, Handbuch für Ausbildung und Praxis, 4. Auflage, Berlin 2021, S. 377–452.

Rüthers, Bernd/Fischer, Christian/Birk, Axel, Rechtstheorie, München 2019.

Rutter, Michael, Resilience as a dynamic concept, Development and psychopathology 2012, S. 335–344.

Säcker, Franz Jürgen/Körber, Torsten (Hrsg.), Kommentar TKG - TTDSG, 4. Aufl., Frankfurt am Main 2023.

Sahoo, Somya Ranjan/Gupta, Brij Bhooshan, Classification of various attacks and their defence mechanism in online social networks: a survey, Enterprise Information Systems 2019, S. 832–864.

Saltzer, J. H./Schroeder, M. D., The protection of information in computer systems, Proceedings of the IEEE (Proc. IEEE) 1975, S. 1278–1308.

Samonas, Spyridon/Coss, David, The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security, Journal of Information Systems Security (JISSec), Vol. 10 (2014), Heft 3, S. 21–45.

Sattler, Andreas, § 8 - Vorgaben der DSGVO für die IT-Sicherheit, in: Ebers, Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, Baden-Baden 2021, S. 197–240.

Savigny, Friedrich Carl von, System des heutigen Römischen Rechts, Band I, Berlin 1840.

Schallbruch, Martin, Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste, Computer und Recht (CR) 2016, S. 663.

Schallbruch, Martin, IT-Sicherheitsrecht – Schutz digitaler Dienste, Datenschutz und Datensicherheit, Zur Entwicklung des IT-Sicherheitsrechts in der 18. Wahlperiode (Folge 2), Computer und Recht (CR) 2017, S. 798–804.

Scharte, Benjamin, Resilience Engineering, Baden-Baden 2020.

Scharte, Benjamin/Thoma, Klaus, Resilienz – Ingenieurwissenschaftliche Perspektive, in: Wink (Hrsg.), Multidisziplinäre Perspektiven der Resilienzforschung, Wiesbaden 2016, 82-98.

Schenke, Wolf-Rüdiger/Graulich, Kurt/Ruthig, Josef (Hrsg.), Sicherheitsrecht des Bundes, 2. Aufl., München 2019.

Scherzberg, Arno, Wissen, Nichtwissen und Ungewissheit im Recht, in: Engel, Halfmann, Schulte (Hrsg.), Wissen, Nichtwissen, unsicheres Wissen, Common goods Legal series Bd. 8, Baden-Baden 2002, S. 113–144.

Scherzberg, Arno, Zum Umgang mit implizitem Wissen - eine disziplinübergreifende Perspektive, in: Schuppert, Voßkuhle (Hrsg.), Governance von und durch Wissen, Schriften zur Governance-Forschung, Baden-Baden 2008, S. 240–256.

Scheuer, Stephan, Waymo - Was ein Robotaxi-Selbstversuch über autonomes Fahren sagt, Die Google-Tochter Waymo darf Fahrgäste in San Francisco nun autonom befördern – ein weltweites Novum. Doch das Angebot hat noch einige Tücken., Handelsblatt vom 11.08.2023, https://www.handelsblatt.com/technik/it-internet/waymo-was-ein-robotaxi-selbstversuch-ueber-autonomes-fahren-sagt/29263550.html (zugegriffen am 20.3.2024).

Schiller, Marcus, Staatliche Gewährleistungsverantwortung und die Sicherstellung von Anschluss und Versorgung im Bereich der Energiewirtschaft, Baden-Baden 2012.

Schillmöller, Jan, Die Informationsfreiheit in der Filterblase, Zeitschrift für Innovations- und Technikrecht (InTer) 2020, S. 150–153.

Schladebach, Marcus, Praktische Konkordanz als verfassungsrechtliches Kollisionsprinzip, Der Staat 2014, S. 263–283.

Schmid, Michael, Ungewissheit und das Problem des sozialen Handelns, Einige methodologische Bemerkungen zum Forschungsprogramm der „Theorie reflexiver Modernisierung", in: Pelizäus, Nieder (Hrsg.), Das Risiko – Gedanken übers und ins Ungewisse, Interdisziplinäre Aushandlungen des Risikophänomens im Lichte der Reflexiven Moderne. Eine Festschrift für Wolfgang Bonß., Wiesbaden 2019, S. 31–79.

Schmidt, Michael, Cyberkrieg gegen Estland macht Westen ratlos, Angriffe auf Computer gehen offenbar weiter, Tagesspiegel vom 30.05.2007, https://www.tagesspiegel.de/politik/cyberkrieg-gegen-estland-macht-westen-ratlos-1499380.html (zugegriffen am 20.3.2024).

Schmidt-Bleibtreu, Bruno/Klein, Franz/Bethge, Herbert (Hrsg.), Bundesverfassungsgerichtsgesetz, Kommentar, 63. Aufl., München 2023.

Schmitz, Barbara/Dall'Armi, Jonas von, Teil XII. Kap. 1, Anforderungen an die IT-Sicherheit und deren rechtliche Grundlage, in: Forgó, Helfrich, Schneider (Hrsg.), Betrieblicher Datenschutz, Rechtshandbuch, 3. Auflage, München, Wien 2019.

Schneeweiß, Hans, Entscheidungskriterien bei Risiko, Berlin, Heidelberg 1967.

Schneier, Bruce, Attack trees, Dr. Dobb's journal, Vol. 24 (1999), Heft 12, S. 21–29, https://www.schneier.com/academic/archives/1999/12/attack_trees.html (zugegriffen am 18.4.2024).

Schulze, Andreas, Liberalisierung und Re-Regulierung von Netzindustrien, Ordnungspolitisches Paradoxon oder wettbewerbsökonomische Notwendigkeit?, Potsdam 2003.

Schulze-Fielitz, Helmuth, Staatsaufgabenentwicklung und Verfassung, Zur normativen Kraft der Verfassung für das Wachstum und die Begrenzung der Staatsaufgaben, in: Grimm (Hrsg.), Wachsende Staatsaufgaben - sinkende Steuerungsfähigkeit des Rechts, Baden-Baden 1990, S. 11–47.

Schuppert, Gunnar Folke, Der Gewährleistungsstaat - modisches Label oder Leitbild sich wandelnder Staatlichkeit, in: Schuppert (Hrsg.), Der Gewährleistungsstaat, Ein Leitbild auf dem Prüfstand, Baden-Baden 2005, S. 11–52.

Schuppert, Gunnar Folke, Gemeinwohldefinition im pluralistischen Verfassungsstaat, Gewerbearchiv (GewArch) 2004, S. 441–447.

Schuster, Fabian/Grützmacher, Malte (Hrsg.), IT-Recht, Kommentar: EU-Recht, nationales Recht, besondere Vertragsbedingungen, Köln 2020.

Schütze, Bernd/Spyra, GErald, DS-GVO – Was ändert sich im Gesundheitswesen?, Recht der Datenverarbeitung (RDV) 2016, S. 285–294.

Schwartmann, Rolf et al. (Hrsg.), DSGVO/BDSG, Datenschutzgrundverordnung, Bundesdatenschutzgesetz, 2. Aufl., Heidelberg 2020.

Schwartmann, Rolf/Jaspers, Andreas/Eckhardt, Jens (Hrsg.), TTDSG, Telekommunikation-Telemedien-Datenschutz-Gesetz, Heidelberg 2022.

Schwarz, Kyrill-Alexander, § 20 Grundfragen, in: Stern, Sodan, Möstl (Hrsg.), Das Staatsrecht der BRD im europäischen Staatenverbund, 2. Auflage, München 2022.

Schwarze, Jürgen et al. (Hrsg.), EU-Kommentar, 4. Aufl., Baden-Baden 2019.

Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen, Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen, 16.06.2023, https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/07/3159c04b-ffc8-4f4e-b72f-ccba6b6a800e.pdf (zugegriffen am 18.4.2024).

Schweizerischer Bundesrat, Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022, 08.12.2017, https://backend.babs.admin.ch/fileservice/sdweb-docs-prod-babsch-files/files/2024/03/22/e58f36ee-10cb-4909-94f3-25a8827135da.pdf (zugegriffen am 24.3.2024).

Schwenke, Matthias Christoph, Individualisierung und Datenschutz, Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung, Wiesbaden 2006.

Selye, Hans, Stress beherrscht unser Leben, Düsseldorf 1957.

Seufert, Julia, Datensicherheit in autonomen Fahrzeugen, Technische und organisatorische Maßnahmen für Fahrzeughersteller, Zeitschrift für Datenschutz (ZD) 2023, S. 256–261.

Sharkov, George, From Cybersecurity to Collaborative Resiliency, in: Multari, Singhal, Manz (Hrsg.), Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense - SafeConfig'16, 24.10.2016, Wien, Österreich, , S. 3–9.

Shashanka, Madhu/Shen, Min-Yi/Wang, Jisheng, User and entity behavior analytics for enterprise security, in: 2016 IEEE International Conference on Big Data (Big Data), 05.-08.12.2016, Washington DC, USA, S. 1867–1874.

Sheridan, Thomas B., Risk, human error, and system resilience: fundamental ideas, Human factors 2008, S. 418–426.

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019.

Singer, P. W./Friedman, Allan, Cybersecurity and cyberwar, What everyone needs to know, Oxford 2014.

Sohr, Karsten/Kemmerrich, Thomas, Kap. 3, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), Cybersecurity, 2. Auflage, 2023, S. 49–115.

Solms, Rossouw von/van Niekerk, Johan, From information security to cyber security, Computers & Security, Vol. 38 (2013), S. 97–102.

Spannowsky, Willy/Runkel, Peter/Goppel, Konrad (Hrsg.), Raumordnungsgesetz (ROG), Kommentar, 2. Aufl., München 2018.

Spiecker gen. Döhmann, Indra, Wissensverarbeitung im Öffentlichen Recht, Rechtswissenschaft (RW) 2010, S. 247–282.

Spindler, Gerald/Schuster, Fabian (Hrsg.), Recht der elektronischen Medien, 4. Aufl., München 2019.

Sreevallabh Chivukula, Aneesh/Yang, Xinghao/Liu, Bo/Liu, Wei/Zhou, Wanlei, Adversarial Deep Learning in Cybersecurity, Attack Taxonomies, Defence Mechanisms, and Learning Theories, Cham 2023.

Stadler, Thomas, Zulässigkeit der heimlichen Installation von Überwachungssoftware, Trennung von Online-Durchsuchung und Quellen-Telekommunikationsüberwachung möglich?, Multimedia und Recht (MMR) 2012, S. 18–20.

Staehelin, Alesch, Begriff und Wesen der Künstlichen Intelligenz, Möglichkeiten, Realitäten, Grenzen, Gewerberlicher Rechtsschutz und Urheberrecht (GRUR) 2022, S. 1569–1571.

Stamminger, Andreas/Krügel, Christopher/Vigna, Giovanni/Kirda, Engin, Automated Spyware Collection and Analysis, in: Samarati (Hrsg.), Information Security, 12th International Conference, ISC 07-09.09.2009, Proceedings, SpringerLink Bücher Bd. 5735, Pisa, Italien 2009, S. 202–217.

Steege, Hans, Algorithmenbasierte Diskriminierung durch Einsatz von Künstlicher Intelligenz, Multimedia und Recht (MMR) 2019, S. 715–721.

Steinmüller, Wilhelm, Automationsunterstützte Informationssysteme in privaten und öffentlichen Verwaltungen: Bruchstücke einer alternativen Theorie des Datenzeitalters, Leviathan 1975, S. 508–543.

Steinmüller, Wilhelm, Informationstechnologie und Gesellschaft, Einführung in die Angewandte Informatik, Darmstadt 1993.

Steinmüller, Wilhelm/Eberle, Carl-Eugen/Garstka, Hansjürgen/Schimmel, Wolfgang/Wegschneider, Herbert/Wolter, Henner, JA-Sonderheft 6: ADV und Recht, Einführung in die Rechtsinformatik und das Recht der Informationsverarbeitung, 2. Aufl., Berlin 1976.

Sterbenz, James P.G./Hutchison, David/Çetinkaya, Egemen K./Jabbar, Abdul/Rohrer, Justin P./Schöller, Marcus/Smith, Paul, Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines, Computer Networks 2010, S. 1245–1265.

Stern, Klaus/Sachs, Michael (Hrsg.), Europäische Grundrechte-Charta, München 2016.

Sterz, Leonie/Werner, Christoph/Raabe, Oliver, Intelligente Verkehrssysteme – IT-Sicherheit in offenen Infrastrukturen Teil 1, Recht der Datenverarbeitung (RDV) 2022, S. 291–299.

Sterz, Leonie/Werner, Christoph/Raabe, Oliver, Intelligente Verkehrssysteme – IT-Sicherheit in offenen Infrastrukturen Teil 2, Recht der Datenverarbeitung (RDV) 2023, S. 97–105.

Stevens, Jeremy, Regelungsvielfalt im IT-Sicherheitsrecht, Computer und Recht (CR) 2021, S. 841–848.

Stinner, Julia, Staatliche Schutzpflichten im Rahmen informationstechnischer Systeme, Baden-Baden 2017.

Stober, Rolf/Korte, Stefan, Öffentliches Wirtschaftsrecht - Allgemeiner Teil, Grundlagen des deutschen, europäischen und internationalen Öffentlichen Wirtschaftsrechts, 20. Aufl., Stuttgart 2023.

Sundar, Agnideven Palanisamy/Li, Feng/Zou, Xukai/Gao, Tianchong/Russomanno, Evan D., Understanding Shilling Attacks and Their Detection Traits: A Comprehensive Survey, IEEE Access, Vol. 8 (2020), S. 171703–171715.

Syckor, Jens/Strufe, Thorsten/Lauber-Rönsberg, Anne, Die Datenschutz-Folgenabschätzung: Ausnahme oder Regelfall?, Wann muss eine Datenschutz-Folgenabschätzung durchgeführt werden?, Zeitschrift für Datenschutz (ZD) 2019, S. 390–394.

Sydow, Gernot/Marsch, Nikolaus (Hrsg.), DS-GVO, BDSG, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz : Handkommentar, 3. Aufl., Baden-Baden u.a. 2022.

Taeger, Jürgen/Gabel, Detlev (Hrsg.), DSGVO - BDSG, Kommentar, 4. Aufl., Frankfurt am Main 2022.

Taeger, Jürgen/Gabel, Detlev (Hrsg.), Kommentar zum BDSG [a.F.], und zu den Datenschutzvorschriften des TKG und TMG, 2. Aufl., Frankfurt a.M. 2013.

Taleb, Nassim Nicholas, Der Schwarze Schwan, Die Macht höchst unwahrscheinlicher Ereignisse, 6. Aufl., München 2013.

Teen claims responsibility for disrupting Twitter, CNN vom 13.04.2009, http://edition.cnn.com/2009/TECH/04/13/twitter.worm/index.html (zugegriffen am 17.4.2024).

Thoma, Florian, Risiko im Datenschutz, Stellenwert eines systematischen Risikomanagements in BDSG und DS-GVO-E, Zeitschrift für Datenschutz (ZD) 2013, S. 578–581.

Tinnefeld, Marie-Theres, Meinungsfreiheit durch Datenschutz - Voraussetzung einer zivilen Rechtskultur, Zeitschrift für Datenschutz (ZD) 2015, S. 22–26.

Trautwein, Frank/Kurpierz, Dennis, Datenschutz-Folgenabschätzung und die neu veröffentlichte ISO/IEC 29134:2017, Privacy in Germany (PinG) 2018, S. 26–30.

Tremmel, Moritz, Neue Schadsoftware möchte IoT-Geräte zerstören – Brickerbot 2.0, golem.de vom 26.06.2019, https://www.golem.de/news/brickerbot-2-0-neue-schadsoftware-moechte-iot-geraete-zerstoeren-1906-142153.html (zugegriffen am 30.06.2024).

Veil, Winfried, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, Der gefährliche Irrweg des alten wie des neuen Datenschutzrechts, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2018, S. 686–696.

Voigt, Paul, Technischer Datenschutz, in: Bussche, Voigt (Hrsg.), Konzerndatenschutz, Rechtshandbuch, 2. Auflage, München 2019.

Voskamp, Friederike/Klein, David, Kap 7. - Datenschutz, in: Kipker (Hrsg.), Cybersecurity, 2. Auflage, 2023.

Voydock, Victor L./Kent, Stephen T., Security Mechanisms in High-Level Network Protocols, ACM Computing Surveys (ACM CSUR) 1983, S. 135–171.

Wagner, Gerhard/Eidenmüller, Horst, In der Falle der Algorithmen? Abschöpfen von Konsumentenrente, Ausnutzen von Verhaltensanomalien und Manipulation von Präferenzen: Die Regulierung der dunklen Seite personalisierter Transaktionen, Zeitschrift für die gesamte Privatrechtswissenschaft (ZfPW) 2019, S. 220–246.

Wagner, Manuela, Datenökonomie und Selbstdatenschutz, Köln, 2020.

Waiz, Eberhard, Daseinsvorsorge in der Europäischen Union, Etappen einer Debatte, in: Krautscheid, Waiz, Münch (Hrsg.), Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl, Eine sektorspezifische Betrachtung, Wiesbaden 2009, S. 41–76.

Walker, Warren/Harremoës, P./Rotmans, Jan/van der Sluijs, J. P./van Asselt, M.B.A./Janssen, Peter/Krayer von Krauss, M. P., Defining Uncertainty: A Conceptual Basis for Uncertainty Management in Model-Based Decision Support, Integrated Assessment 2003, S. 5–17.

Wank, Rolf, Juristische Methodenlehre, Eine Anleitung für Wissenschaft und Praxis, München 2019.

Weber, Rolf H./Yildiz, Okan, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, Zürich, Schweiz 2022.

Weck, Gerhard, Datensicherung - Konzepte und Bewertung, Datenschutz und Datensicherheit (DuD) 1989, S. 386–392.

Weiß, Holger Tobias, Die rechtliche Gewährleistung der Produktsicherheit, Vol. 6, Baden-Baden 2008.

Weiß, Wolfgang, Öffentliche Daseinsvorsorge und soziale Dienstleistungen: Europarechtliche Perspektiven, Europarecht (EuR) 2013, 669–687.

Werner, Christoph, Die Maßnahmenwahl im IT-Sicherheitsrecht, Von den Erfordernissen der "Angemessenheit" und des "Standes der Technik", in: Baumgärtel, Kiparski (Hrsg.), DGRI-Jahrbuch 2021/2022, Köln 2023, S. 161–179.

Werner, Christoph/Brinker, Nils/Raabe, Oliver, Grundlagen für ein gesetzliches IT-Sicherheitsrisikomanagement — Ansätze zur Vereinheitlichung von Rollenmodell, Risikomanagement und Definitionen für das IT-Sicherheitsrecht, Computer und Recht (CR) 2022, S. 817–824.

Whitman, Michael/Mattord, Herbert, Principles of Information Security, 7. Aufl., Boston, USA 2022.

Wiedemann, Herbert, Richterliche Rechtsfortbildung, Neue Juristische Wochenschrift (NJW) 2014, S. 2407–2412.

Wietfeld, Anne Christin, Die richtlinienkonforme Auslegung – Auslegungsmethode oder Zielvorgabe?, JuristenZeitung (JZ) 2020, S. 485–494.

Wildavsky, Aaron, Searching for safety, 4. Aufl., New Brunswick, Kanada 1991.

Wischmeyer, Thomas, Informationssicherheit, 2023.

Wolff, Heinrich Amadeus, Zivile Sicherheit als Infrastrukturgewährleistung und Daseinsvorsorge, in: Gusy, Kugelmann, Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, Berlin, Heidelberg 2017, S. 657–689.

Wollenschläger, Burkard, Wissensgenerierung im Verfahren, Zugl.: Konstanz, Univ., Diss., 2008, Vol. 2, Tübingen 2009.

Wright, Margaret O'Dougherty/Masten, Ann S./Narayan, Angela J., Resilience Processes in Development: Four Waves of Research on Positive Adaptation in the Context of Adversity, in: Goldstein, Brooks (Hrsg.), Handbook of Resilience in Children, 2nd ed. 2013, Boston, MA 2013, S. 15–37.

Würtenberger, Thomas, Resilienz, in: Baumeister (Hrsg.), Staat, Verwaltung und Rechtsschutz, Festschrift für Wolf-Rüdiger Schenke zum 70. Geburtstag, Schriften zum öffentlichen Recht Bd. 1196, Berlin 2011, S. 561–578.

Wustmann, Corina, Die Erkenntnisse der Resilienzforschung – Beziehungserfahrungen und Ressourcenaufbau, Psychotherapie Forum, Vol. 17 (2009), Heft 2, S. 71–78.

Wustmann, Corina, Resilienz, Widerstandsfähigkeit von Kindern in Tageseinrichtungen fördern, 6. Aufl., Weinheim, Basel 2016.

Xie, Linlin/Smith, Paul/Banfield, Paul/Leopold, Helmut/Sterbenz, James P.G./Hutchison, David, Towards Resilient Networks Using Programmable Networking Technologies, in: Hutchison, Denazis, Lefevre et al. (Hrsg.), Active and Programmable Networks, Lecture Notes in Computer Science, Berlin, Heidelberg 2009, S. 83–95.

Xing, Xinyu/Meng, Wei/Doozan, Dan/Snoeren, Alex/Feamster, Nick/Lee, Wenke, Take This Personally: Pollution Attacks on Personalized Services, in: Proceedings of the 22nd USENIX Security Symposium, 14.-16.08.2013, Washington D.C., USA, S. 671–686.

Xu, Han/Ma, Yao/Liu, Hao-Chen/Deb, Debayan/Liu, Hui/Tang, Ji-Liang/Jain, Anil K., Adversarial Attacks and Defenses in Images, Graphs and Text: A Review, IJAC (International Journal of Automation and Computing) 2020, S. 151–178.

Xue, Mingfu/Yuan, Chengxiang/Wu, Heyi/Zhang, Yushu/Liu, Weiqiang, Machine Learning Security: Threats, Countermeasures, and Evaluations, IEEE Access, Vol. 8 (2020), S. 74720–74742.

Yang, Can/Xu, Xinyuan/Nunes, Bernardo Pereira/Siqueira, Sean Wolfgand Matsui, Bubbles bursting: Investigating and measuring the personalisation of social media searches, Telematics and Informatics, Vol. 82 (2023), AS-Nr. 101999.

Yang, Guolei/Gong, Neil Zhenqiang/Cai, Ying, Fake Co-visitation Injection Attacks to Recommender Systems, in: Proceedings 2017 Network and Distributed System Security Symposium, 26.02-01.03.2017, San Diego, USA.

Zampieri, Matteo, Reconciling the ecological and engineering definitions of resilience, Ecosphere, Vol. 12 (2021), Heft 2.

Zeller, William/Felten, Edward W., Cross-Site Request Forgeries: Exploitation and Prevention, https://people.eecs.berkeley.edu/~daw/teaching/cs261-f11/reading/csrf.pdf (zugegriffen am 18.4.2024).

Zhang, Dongyang, Bessere Daseinsvorsorge durch Regulierung im Bereich des ÖPNV, Rechtliche Hinweise für China, Berlin 2019.

Zhang, W. J./Lin, Y., On the principle of design of resilient systems – application to enterprise information systems, Enterprise Information Systems, Vol. 4 (2010), Heft 2, S. 99–110.

Zhang, Yubao/Xiao, Jidong/Hao, Shuai/Wang, Haining/Zhu, Sencun/Jajodia, Sushil, Understanding the Manipulation on Recommender Systems through Web Injection, IEEE Transactions on Information Forensics and Security (IEEE Trans. Inf. Forensics Secur.), Vol. 15 (2020), S. 3807–3818.

Zhao, Songyin/Wang, Xu an, A Survey of Malicious HID Devices, in: Barolli (Hrsg.), Advances on Broad-Band Wireless Computing, Communication and Applications, Proceedings of the 14th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2019), Lecture Notes in Networks and Systems Series v.97, Cham 2020, S. 777–786.

Ziegler, Jürgen/Loepp, Benedikt, Empfehlungssysteme, in: Kollmann (Hrsg.), Handbuch digitale Wirtschaft, Wiesbaden 2020, S. 717–742.

Zobel, Christopher W./Khansa, Lara, Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks, Decision Sciences 2012, S. 687–710.