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).

I. Datensicherheitsrecht und IT-Sicherheitsrecht

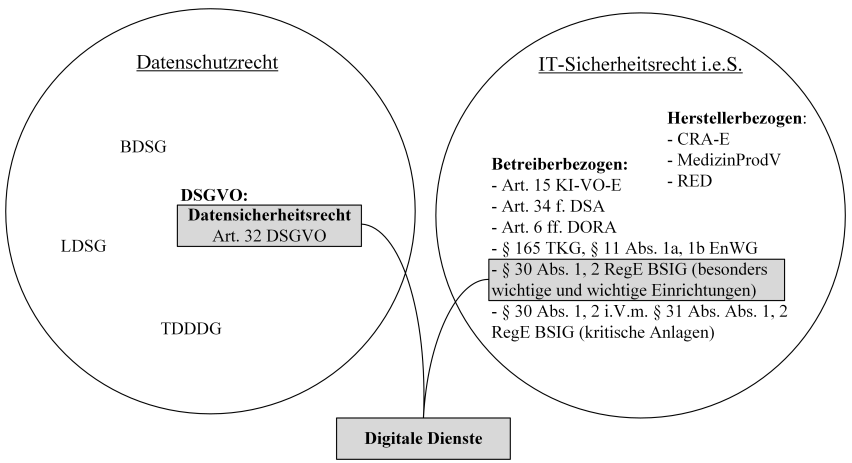

Abbildung 1: Datenschutzrecht und IT-Sicherheitsrecht

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.

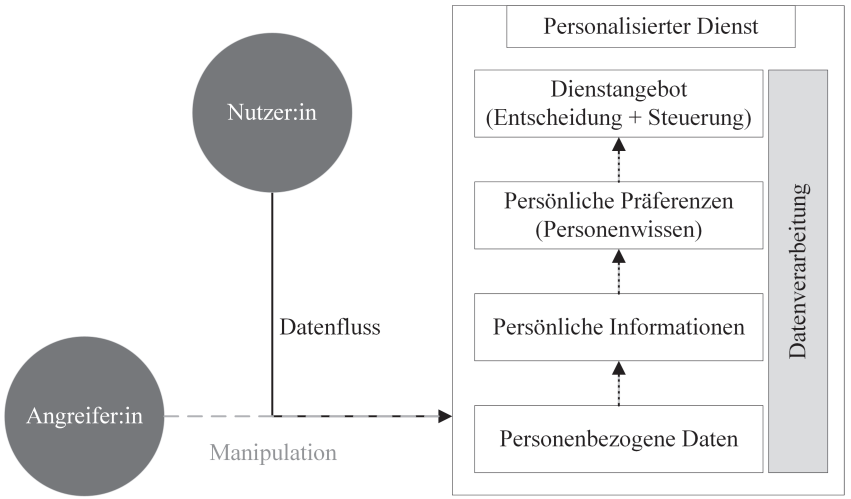

Abbildung 2: Manipulation von personalisierten Diensten

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.