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.