Prozedurales IT-Sicherheitsrecht

Von der Notwendigkeit eines gesetzlichen IT-Sicherheitsrisikomanagements

Kern des IT-Sicherheitsrechts ist die Verpflichtung des Normadressaten, Maßnahmen vornehmen, um die durch seine Informationstechnik (IT) wirkenden Risiken für rechtlich relevante Schutzgüter einzudämmen. Wie weit diese Eindämmungspflicht und damit Qualität und Quantität der zu treffenden Maßnahmen reicht, wird regelmäßig mit dem unbestimmten Rechtsbegriff der *Angemessenheit* beschrieben (vgl. etwa § 8a BSIG, § 11 Abs. 1a EnWG oder § 165 TKG).

Gegenstand dieses Aufsatzes ist die Frage, ob eine solche Grobkonturierung des Handlungsauftrags hinreichend ist oder ob es nicht vielmehr einer Prozeduralisierung des IT-Sicherheitsrechts bedarf. Zur Beantwortung der Frage werden folgende Schritte vorgenommen: Zunächst wird der Begriff Prozeduralisierung allgemein beschrieben, indem er rechtstheoretisch hergeleitet wird (A.). Anschließend wird das bestehende IT-Sicherheitsrecht anhand dieses rechtstheoretischen Modells eingeordnet (B.). Unter C. wird sodann erläutert, ob eine Prozeduralisierung im Sinne der Vorgabe eines gesetzlichen Risikomanagements erforderlich ist. Schließlich erfolgt die Erörterung, ob die gerichtliche Kontrolle in der Konsequenz angepasst werden muss (D.), gefolgt von einem Gesamtergebnis mit Ausblick unter E.

Inhalt

A. Herleitung des Begriffs: Rechtstheoretische Einordung

Im nachfolgenden Abschnitt soll sich dem Begriff der Prozeduralisierung genähert werden. Hierfür wird das prozedurale Recht rechtstheoretisch in Abgrenzung zum formalen und zum materialen Recht beschrieben (I. – III.). Aus rechtstheoretischer Sicht ist der Begriff der Prozeduralisierung eng mit dem der Formalisierung sowie der Materialisierung des Rechts verknüpft. Beide Begriffe sollen daher zunächst dargestellt und in Abgrenzung dazu die Prozeduralisierung erläutert werden.

I. Formales Recht

Als formales Recht werden Normen bezeichnet, die eindeutige Regeln enthalten und bei denen der Eintritt der Rechtsfolge ausschließlich durch das Vorliegen aller Tatbestandsmerkmale bedingt ist. Sie werden von *Luhmann* auch als Konditionalprogramme bezeichnet.[1] Dabei verzichtet das formale Recht auf die Einbeziehung außerrechtlicher Aspekte wie allgemeine Ethik- und Moralvorstellungen und leitet das Ergebnis ausschließlich als „juristisch präzise Einzelfallentscheidung“ intrinsisch aus dem Recht selbst ab.[2]

II. Materiales Recht

Von materialem Recht wird hingegen gesprochen, wenn sich die Rechtsfolge nicht unmittelbar als Ergebnis der Subsumtion des Konditionalprogramms der Norm ergibt, sondern durch den Normanwender weitergehende, kontextspezifische Er- und Abwägungen angestellt werden

[1] *G.-P. Calliess*, Prozedurales Recht, S. 19; *Luhmann*, Das Recht der Gesellschaft, S. 195 ff.
[2] *Kehrberger*, Die Materialisierung des Zivilprozessrechts, S. 8; *Trubek*, The Sociology of Law 1972, 720 (730); grundlegend: *M. Weber*, Wirtschaft und Gesellschaft, S. 503 ff.

müssen.[3] Von *Luhmann* werden diese Vorgaben in Abgrenzung von Konditionalprogrammen auch als „Zweckprogramme“ bezeichnet,[4] d.h. das vom Normadressaten verlangte Verhalten oder das von ihm herzustellende Ergebnis orientiert sich an normativen Zwecken wie z.B. der „wirksamen Umweltvorsorge“.[5]

Um sich solchen indes nicht absolut geltenden Zwecken zu nähern, enthalten diese Normen unbestimmte Rechtsbegriffe und Generalklauseln[6] wie „Angemessenheit“[7] oder „Treu und Glauben“, die nach einer einzelfallbezogenen Abwägungsentscheidung bzgl. der von der Norm betroffenen, konfligierenden Interessen verlangen.[8] Dabei müssen anders als im formalen Recht auch außerrechtliche Ethik- und Moralvorstellungen herangezogen werden.[9] In diesem Sinne beschrieb etwa auch *Wieacker* mit dem Begriff Materialisierung die damalige Einführung von Normen des Privatrechts, die abweichend von der früheren formalen Gleichheit den Individualschutz für (vermeintlich) unterlegene Gruppen sowie Aspekte der Verteilungsgerechtigkeit im Gesetz etablierten.[10] Heute wird diese Entwicklung im Privatrecht vor allem durch den europäischen Verbraucherschutz weiter vorangetrieben.[11]

III. Prozedurales Recht

Als prozedurales Recht lassen sich schließlich Normen bezeichnen, die durch ein Verfahren mit zumindest reduzierten materialen Vorgaben eine Entscheidung durch den Normadressaten konstituieren und inhaltlich determinieren.[12] Gänzlich ohne materiale Vorgaben kommt prozedurales Recht indes nicht aus, sondern es wird ein gelockerter, flexibler Rahmen geschaffen,[13] innerhalb dessen der Adressat unter Berücksichtigung des situativen Kontextes[14] eine rechtlich gewünschte oder zumindest gebilligte Entscheidung treffen soll. Der Adressat wird mithin durch das Verfahren in die entsprechende Richtung gelenkt, ohne dass er dadurch notwendigerweise auch von den Rechtsfolgen einer trotz Einhaltung des Verfahrens getroffenen unrichtigen Entscheidung befreit wird.[15]

---

[3] *G.-P. Calliess*, Prozedurales Recht, S. 19.
[4] *Luhmann*, Das Recht der Gesellschaft, S. 198 ff.
[5] § 1 UVPG, dazu später noch ausführlich; *Vesting*, Rechtstheorie, S. 19.
[6] Zur Unterscheidung beider Begriffe: *Nastelski*, GRUR 1968, 545 (545 f.).
[7] Siehe statt vieler: *Rüscher*, in: MüKoBGB, 8. Auflage 2021, § 20 WEG, Rn. 114.
[8] *G.-P. Calliess*, Prozedurales Recht, S. 19.
[9] *Kehrberger*, Die Materialisierung des Zivilprozessrechts, S. 10; *M. Weber*, Wirtschaft und Gesellschaft, S. 507.
[10] *Renner*, in: Grundmann/Micklitz/Renner, Formalisierung, Materialisierung und Prozeduralisierung, 821 (825).
[11] *Renner*, wie zuvor.
[12] *Hagenah*, in: Grimm, Neue Instrumente für eine neue Staatsaufgabe, 487 (492); *Voßkuhle*, Das Kompensationsprinzip, S. 64.
[13] *Voßkuhle*, Das Kompensationsprinzip, S. 65 f.
[14] *Campos*, KJ 2019, 400 (401).
[15] Siehe dazu Kap. E, S. 12.

Durch die Fokussierung auf einen spezifischen, materialen Zweck (wie der o.g. Umweltvorsorge) unterscheidet sich das prozedurale Recht vom allgemeinen Verfahrensrecht (z.B. VwVfG) und dem Prozessrecht (ZPO, VwGO, StPO).[16] Diese Rechtskategorien bieten ein universelles Verfahren an, das gerade nicht auf die Herstellung oder Erreichung einer durch dieses Recht vorgezeichneten Wertentscheidung gerichtet ist.[17] Auf der Anwendungsebene erfüllt zumindest das Prozessrecht mit Blick auf die Entscheidungsfindung auch einen anderen Zweck: Es lenkt den Normadressaten nicht prospektiv zu einer rechtlich gewünschten Entscheidung, sondern ermöglicht v.a. die retrospektive Überprüfung derselben.

B. Einordnung der Pflichtennormen des IT-Sicherheitsrechts

Das IT-Sicherheitsrecht stellt kein einheitliches, zusammenhängend kodifiziertes Recht dar, sondern erfasst als Sammelbezeichnung alle Normen, die technische und rechtliche Maßgaben im Hinblick auf die IT-Systeme eines Unternehmens oder eines öffentlich-rechtlichen Betreibers regeln und diese in die Lage versetzen sollen, auf Gefährdungslagen in verschiedene Richtungen reagieren zu können.[18]

Das IT-Sicherheitsrecht umfasst auf europäischer Ebene insbesondere die NIS2-RL[19] sowie auf nationaler Ebene die Normen des BSIG. Daneben wird die Datensicherheit in Art. 32 DS-GVO geregelt, welche für diesen Aufsatz der sprachlichen Vereinfachung wegen ebenfalls unter das IT-Sicherheitsrecht gefasst wird.[20] Weiterhin können Regelungen im Energie-, Sozial-, Steuer- und Gesundheitsbereich als bereichsspezifisches IT-Sicherheitsrecht bezeichnet werden.[21]

Gemein ist den Pflichtennormen des IT-Sicherheitsrechts, dass sie von den Normadressaten die Vornahme technischer und organisatorischer Maßnahmen verlangen. Die Maßnahmen müssen durch den Adressaten selbst insbesondere mit Blick auf die Schutzziele Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme bzw. der Daten ausgewählt werden, indem eine Risikoabwägung durchgeführt wird. Dabei wird das Kriterium der Angemessenheit abwägungsleitend herangezogen. Der Umsetzungsaufwand

[16] Teilweise werden Materialisierungstendenzen aber auch im Prozessrecht gesehen; eine Übersicht bei *Kehrberger*, Die Materialisierung des Zivilprozessrechts, S. 19 ff. *Sheplyakova*, in: Sheplyakova, Prozeduralisierung des Rechts. Tema con Variazioni, 1, (5) versteht prozedurales Recht als weder zum formellen noch zum materiellen Recht gehörige Rechtskategorie „sui generis".
[17] Vgl.: *Hagenah*, in: Grimm, Neue Instrumente für eine neue Staatsaufgabe, 487 (492).
[18] Auer-Reinsdorff/*Conrad*, Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33, Rn. 8.
[19] RL (EU) 2022/2555, verabschiedet am 27.12.22, ersetzt die NIS-RL (EU) 2016/1148.
[20] Zur Unterscheidung zwischen Daten- und IT-Sicherheit sowie den zugehörigen Rechtsmaterien: *Jandt* in Hornung/Schallbruch, IT-SR-Hdb., 1. Aufl. 2021, § 17, Rn. 3 ff., 8.
[21] Raabe/Schallbruch/Steinbrück, Systematisierung des IT-Sicherheitsrechts, CR 2018, 706-715, 707 Rn. 4.

einer Maßnahme muss den Risiken, d.h. der Eintrittswahrscheinlichkeit und den Folgen[22] etwaiger IT-Ereignisse entsprechen, wobei der Adressat nicht verpflichtet ist, die bestmögliche Maßnahme zu ergreifen, sondern diese (nur) verhältnismäßig zu den einhergehenden Risiken auswählen muss. [23]

Ordnet man die genannten Pflichtennormen in die im voranstehenden Kapitel beschriebenen Rechtskategorien ein, ergibt sich folgendes Bild: In formaler Hinsicht wird dem Adressaten vorgegeben, technische und organisatorische Maßnahmen zur Sicherung der genannten Schutzziele vorzunehmen. Allerdings wird die Maßnahmenwahl durch den unbestimmten Rechtsbegriff der Angemessenheit ausgestaltet. Dadurch weist dieser entscheidende Teil der Normen bislang (nur) einen materialen Charakter auf.

C. Prozeduralisierung des Angemessenheitsbegriffs

Fraglich ist somit nun, ob mit dem materialen Begriff der Angemessenheit, der gleichsam das Herzstück dieser IT-Sicherheitsnormen darstellt, die optimale rechtliche Lösung gefunden ist. Denkbar wäre, diesen Begriff und damit die Maßnahmenwahl unter dem Primat der Herstellung eines angemessenen Ausgleichs durch die Vorgabe eines Verfahrens zu prozeduralisieren.

Hierfür soll zunächst der Begriff der Angemessenheit näher beschrieben werden (I.). Im Anschluss daran werden die Argumente dargelegt, die für eine Prozeduralisierung des Begriffs sprechen (II.), bevor die Vorgabe eines gesetzlichen Risikomanagements als Lösungsvorschlag diskutiert wird (III.).

I. Bedeutung der Angemessenheit

Der Begriff der Angemessenheit geht auf rechtliche Mechanismen zur Einschränkung von Grundrechten zurück.[24]

Im Geltungsbereich des Grundgesetzes gilt bei der Abwägung schrankenloser Grundrechte das Prinzip der praktischen Konkordanz: Die Verfassungsgüter sind einander so zuzuordnen, dass sie zu optimaler Wirksamkeit gelangen.[25] Im Rahmen jeder Abwägung zur

[22] IT-Risiken werden i.d.R. als Kombination aus der Eintrittswahrscheinlichkeit eines Ereignisses mit informationstechnischen Auswirkungen und der Höhe seiner Schadfolgen beschrieben; vgl.: *Skiera* in Hornung/Schallbruch, IT-SR-Hdb., 1. Aufl. 2021, § 8, S. 162, Rn. 33; CNSSI No. 4009, 06.04.2015, S. 104.
[23] BT-Drs. 18/4096, S. 25 ff.
[24] So auch Paal/Pauly/*Martini*, DS-GVO BDSG, Art. 32, Rn. 48; Spindler/Schuster/*Laue*, DSGVO, Art. 32, Rn. 3, die den Begriff der Angemessenheit als Ausfluss des Verhältnismäßigkeitsprinzips einordnen.
[25] *Hesse*, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Auflage 1999, Rn. 317.

Verfassungsmäßigkeit von Grundrechtseingriffen wird dieses Prinzip zur geringstmöglichen Einschränkung der jeweiligen Positionen herangezogen.
Garantiert sowohl in der deutschen Verfassung als auch durch die Grundrechtecharta findet das Verhältnismäßigkeitsprinzip darüber hinaus Anwendung: Unabhängig davon, ob die einschränkende Maßnahme aus einer grundrechtlich geschützten Position herrührt, muss diese ein legitimes Ziel verfolgen, sowie erforderlich und geeignet sein, um dieses Ziel zu erreichen. Den Kern des Verhältnismäßigkeitsprinzips macht schließlich die Angemessenheit im engeren Sinne aus, die eine Gegenüberstellung der Positionen mit der Maßgabe, beiden zu ihrer jeweils größtmöglichen Wirkung zu verhelfen, verlangt.[26]

Als einfachrechtlicher, materialer Rechtsbegriff ist die „Angemessenheit" hingegen reduzierter. Vom Normadressaten kann keine verfassungsrechtliche Angemessenheitsprüfung im eigentlichen Sinn verlangt werden. Vielmehr ist insofern unter Rückgriff auf außerrechtliche Kriterien eine sachgerechte Prüfung vorzunehmen, um rechtliche Fragen eines angemessenen Ausgleichs zu beantworten.[27]
Dieser Ausgleich soll den Werten und Zielen entsprechen, die aus der Verfassung deutlich werden. Zur Erfüllung der Aufgaben aus dem Sozialstaatsprinzip[28] wird beispielsweise die Unterstützung benachteiligter Gruppen forciert.[29] Deutlich wird eine solche Funktion etwa im BGB in den Vorschriften zu Allgemeinen Geschäftsbedingungen (AGB). In der Generalklausel des § 307 BGB verlangt der Gesetzgeber eine Abwägung zwischen dem Schutzbedürfnis des Verbrauchers und der Vertragsfreiheit des Verwenders. Eine Bestimmung ist demnach unwirksam, wenn sie den Vertragspartner – auch unter Rekurs auf Treu und Glauben, § 242 BGB – unangemessen benachteiligt.
Um der Norm zu entsprechen, hat der Verwender folgendes Procedere durchzuführen: Er muss das Gesetzesrecht als Bewertungsmaßstab zugrunde zu legen, von dem abgewichen werden soll,[30] und im Rahmen einer generell-typisierenden Betrachtung, ohne auf die konkreten Vertragsparteien einzugehen, die Interessen zunächst ermitteln[31] und dann gegeneinander

[26] BVerfGE 80, 137 (159 ff.).
[27] Beispielhaft: Außerrechtliche Kriterien sollen im AGB-Recht bei § 307 BGB herangezogen werden, indem zur Ermittlung der Angemessenheit die Analyse sämtlicher in Betracht kommender Interessen erfolgt, BeckOKBGB/*H. Schmidt*, § 307, Rn. 29. Im IT-Sicherheitsrecht stellen z.B. sowohl Spindler/Schuster/*Laue*, DSGVO, Art. 32, Rn. 3 ff. als auch Borges/Hilber/*Borges*, BeckOK IT-Recht, DSGVO, Art. 32, Rn. 20 ff. die nach Art. 32 DSGVO in der Verhältnismäßigkeitsprüfung zu berücksichtigenden außerrechtlichen Faktoren dar.
[28] *Teubner*, in: Verrechtlichung – Begriffe, Merkmale, Grenzen, Auswege, 289, 311 f.
[29] BVerfGE 100, 271 (284), hier im Zusammenhang mit Tarifvertragsrecht.
[30] Hau/Poseck/*Schmidt*, BeckOKBGB, § 307, Rn. 30.
[31] Ebd., Rn. 31.

abwägen[32]. Nach dem BGH liegt eine unangemessene Benachteiligung vor, wenn „der Verwender durch einseitige Vertragsgestaltung missbräuchlich eigene Interessen auf Kosten seines Vertragspartners durchzusetzen versucht, ohne von vornherein auch dessen Belange hinreichend zu berücksichtigen und ihm einen angemessenen Ausgleich zuzugestehen“[33].
Der AGB-Verwender als Normadressat muss mithin eine Interessenabwägung anstellen und bei der Formulierung seiner AGB darauf achten, die Rechte der Vertragspartner in Ausgleich zu bringen. Dazu ist es unter Bezugnahme auf Treu und Glauben notwendig, auf soziale Gebote und Schranken sowie ethische Prinzipien Rücksicht zu nehmen, die der gesamten Rechtsordnung immanent sind.[34]

Im Rahmen des IT-Sicherheitsrechts sind nun, wie bereits angedeutet, ebenfalls zwei rechtliche Interessen durch den Normadressaten gegeneinander abzuwägen.
Auf der einen Seite stehen die jeweils betroffenen individual- und gemeinschaftsrechtlichen Schutzgüter. Während individualrechtliche Schutzgüter als Grundrechtspositionen definiert werden können, betreffen die gemeinschaftsrechtlichen Schutzgüter öffentliche Interessen[35]. Zum Teil werden beide Kategorien auch in einem vermittelnden Element wie der „Versorgungssicherheit“ mit kritischen Dienstleistungen vereinigt, wodurch sowohl individuelle Grundrechtsbeeinträchtigen[36] als auch öffentliche Interessen wie den Erhalt der Wirtschaftsleistung[37] umfasst werden. § 2 Abs. 10 Nr. 2 BSIG normiert weiterhin den Begriff der öffentlichen Sicherheit, der als Sammelbegriff ebenfalls sowohl gemeinschaftliche als auch individuelle Schutzgüter umfasst.
Diese Schutzgüter sind durch die Verwendung von IT besonderen Risiken ausgesetzt. Durch die Vornahme bestimmter Maßnahmen können die Risiken entsprechend gemindert werden. Das diesseitige Interesse ist somit darauf gerichtet, die gefährdeten Schutzgüter einem möglichst geringen Risiko auszusetzen bzw. das Risiko möglichst weitgehend zu vermindern.
Demgegenüber steht die Belastung, die die Maßnahmen für den Normadressaten darstellen: Sie erfordern einen zeitlichen, administrativen und finanziellen Aufwand. Damit wird die

[32] Ebd., Rn. 32.
[33] St. Rspr., BGH NJW 2001, 2331, 2331.
[34] Erman/*Böttcher*, BGB, § 242, Rn. 3; MüKoBGB/*Schubert*, § 242, Rn. 10 mwN.
[35] Hierunter fällt exemplarisch die Umwelt, wie sie beispielsweise in Art. 5 RL 2012/18/EU, § 2 Nr. 8 lit. c Störfall-VO geschützt wird. Diese ist durch die technische Steuerung von Betriebsabläufen zum Beispiel im produzierenden Gewerbe in Bezug auf IT-Sicherheitsvorfälle besonders gefährdet.
[36] So etwa „Leib, Leben, Gesundheit und Eigentum“, BT-Drs. 18/4096, S. 30 f.
[37] Unter anderem „Sicherung des Zahlungsverkehrs […], Bargeldversorgung […], Kreditvergabe“ etc., BT-Drs. 18/4096, S. 31. Die Aufrechterhaltung der Versorgungssicherheit soll die nötigen Funktionen des Zusammenlebens sichern. Sie dient der Gewährleistung des Existenzminimums nach Art. 1 GG und erfüllt damit eine Schutzpflicht des Staates.

Berufsausübung des Normadressaten beeinträchtigt. Auf dieser Seite ist das Interesse darauf gerichtet, diesen Aufwand so gering wie möglich zu halten.

Beide Positionen sind vom Normadressaten in einen angemessenen Ausgleich zu bringen, wie auch in der negativen Legaldefinition der Angemessenheit nach § 8a Abs. 1 S. 3 BSIG zum Ausdruck kommt: „Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht".[38] Dabei lässt sich der damit verbundene Ausgleichsprozess auch als eine Kosten-Nutzen-Analyse umschreiben, bei dem die Kosten bzw. der Aufwand für die zu treffenden Maßnahmen einerseits mit der damit zu erreichenden Minderung der Risiken für die Schutzgüter der Betroffenen in ein angemessenes Verhältnis zu bringen sind. Hierbei „soll" auch der Stand der Technik eingehalten bzw. berücksichtigt werden (§ 8a Abs. 1 BSIG, Art. 32 DSGVO). Wie genau dieser in die Maßnahmenwahl einfließt, ist durch diese unterschiedlich strengen, aber gleichwohl offenen Bindungen, Teil der materialen Abwägung; hingegen ist der Stand der Technik selbst objektiv bestimmt und verweist formal in ein anderes Wissenschaftsgebiet.

II. Argumente für eine Prozeduralisierung

Für den Einsatz von prozeduralem Recht (Prozeduralisierung des Rechts)[39] sprechen eine Reihe von steuerungsrechtlichen Schwierigkeiten, die sich durch prozedurales Recht lösen lassen könnten. Hierzu gehören die Anforderungen an die Regulierung autopoietischer Systeme nach der Systemtheorie (1.), die schwindende materielle Legitimität parlamentarischer Gesetze (2.) sowie die Bewältigung von Ungewissheit durch den Normadressaten (3.). Im folgenden Abschnitt sollen diese Herausforderungen allgemein beschrieben und auf ihre Einschlägigkeit im IT-Sicherheitsrecht mit Blick auf den Angemessenheitsbegriff hin untersucht werden.

1. Systemtheorie

Aus steuerungswissenschaftlicher Sicht[40] liefert zunächst *Luhmanns* Systemtheorie Argumente für die vermehrte Prozeduralisierung des Rechts. Nach dieser Theorie steht das Recht in der Gesellschaft als ein eigenständiges System diversen anderen sozialen Systemen gegenüber, wobei für ein System jedes andere System stets die „Umwelt" darstellt.[41]

---

[38] Vgl. auch § 165 Abs. 6 TKG und § 11 Abs. 1e, S. 3 EnWG.
[39] *Eder*, in: Grimm, Prozedurales Recht und Prozeduralisierung des Rechts, 156 (155).
[40] Zum Konzept der „Steuerung" durch Recht, bei der der Staat als Steuerungssubjekt auftritt und versucht gesellschaftliche Gruppen im Sinne sozialer Teilsysteme (Steuerungsobjekt) zu einem spezifischen Verhalten zu bewegen: *Linzbach*, EurUP 2020, 93 (93).
[41] *Francuski*, Prozeduralisierung im Wirtschaftsstrafrecht, S. 92 ff; *Luhmann*, Die Gesellschaft der Gesellschaft, S. 609 ff.; *Teubner*, ARSP 1982, 13 (48, 57).

Jedes System agiert dabei nur nach seiner eigenen inneren Konditionierung und Struktur,[42] was von *Luhmann* als „Autopoiesis" bezeichnet wurde.[43] Die für die vorliegende Untersuchung entscheidende Erkenntnis hieraus ist, dass das Rechtssystem keine Möglichkeit zur direkten Steuerung anderer Systeme besitzt.[44] Vielmehr stellt jeder Rechtsakt lediglich eine Kommunikation an ein anderes System dar. Wie dieser kommunikative Rechtsakt aber im adressierten System aufgenommen wird, entzieht sich dem Einfluss des Rechtssystems. Denn für das adressierte System ist das Rechtssystem Umwelt, aus der es Kommunikationsimpulse nur im Kontext seiner eigenen Autopoiesis aufnimmt.[45]

Um somit eine höhere Effektivität des Rechts zu erreichen, sollte das Gesetz an diesen internen Operationen des zu regulierenden Systems ansetzen. Dies kann statt durch formale und materiale insbesondere durch prozedurale Normen erreicht werden, die durch ein Verfahren auf die Besonderheiten des zu regulierenden Systems eingehen.[46]

Im IT-Sicherheitsrecht sind die Normadressaten, insbesondere die Betreiber kritischer Infrastrukturen, häufig Wirtschaftsunternehmen. Diese sind auf den Umgang mit unternehmerischen Risiken, der Abwägung von Chancen zwischen Gewinn und Verlust einer geschäftlichen Entscheidung, konditioniert. So gilt dies auch für Investitionen in die IT-Sicherheit im Unternehmensinteresse, die sich als Verlust gegenüber dem damit zu erreichenden Gewinn (Schutz von Geschäftsgeheimnissen, keine Produktionsunterbrechung durch IT-Angriffe) messen lassen müssen.[47] Es bietet sich daher an, die Angemessenheit im IT-Sicherheitsrecht durch ein Verfahren zu konturieren, dass auf diese bestehenden

---

[42] *Vesting*, Rechtstheorie, S. 59 f.
[43] *Luhmann*, Das Recht der Gesellschaft, S. 45 f.
[44] *Francuski*, Prozeduralisierung im Wirtschaftsstrafrecht, S. 156; *Teubner*, ARSP 1982, 13 (48).
[45] *Luhmann*, Zeitschrift für Rechtssoziologie 1985, 1 (18).
[46] Exemplarisch etwa das System der Wirtschaft, dass nach dem Prinzip des größtmöglichen Profits operiert. Normen zur Verhaltenssteuerung können hier v.a. dann erfolgreich sein, wenn sie auf markttechnische Verfahren beruhen, also wenn etwa für den Klimaschutz statt Grenzwerten für den CO2-Ausstoß der auf Marktprinzipien beruhenden CO2-Zertifikate-Handel etabliert wird, vgl.: *G.-P. Calliess*, Prozedurales Recht, S. 130.
[47] Dazu *Pohlmann*, IT-Sicherheit konsequent und effizient umsetzen, in: *Lang/Löhr (Hrsg.)*, IT-Sicherheit. Technologien und Best Practices für die Umsetzung im Unternehmen, S. 1-22,
der IT-Sicherheitsstrategien darstellt und diese in Relation zu der Wirtschaftlichkeit eines Unternehmens setzt.
Nauroth, Organisation des IT-Sicherheitsmanagements im Unternehmen, ebd., S. 43-59, erörtert, wie eine Organisationsstruktur so optimiert werden kann, dass Sicherheit und Compliance nahtlos ineinander übergehen und so der Sicherheit von Unternehmensgütern eine möglichst geringe finanzielle Einbuße gegenübersteht, angepasst an die Größe der Unternehmen.
Lohre, Standards und Zertifizierungen, ebd., S. 77-98, beschäftigt sich mit dem Unternehmensinteresse, nach außen als sicherer Geschäftspartner aufzutreten, indem er die Vorteile und Verfahren von Zertifizierungen darstellt.
Leeser, Digitalisierung in KMU kompakt. Compliance und IT-Security, S. 73 ff., analysiert die für KMU bestehenden Probleme und schlägt Lösungsmöglichkeiten vor.
In *Bartsch/Frey (Hrsg.)*, Cybersecurity. Best Practices. Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden, werden durch Essays verschiedener Autoren einzelne Sicherheitsvorfälle herausgenommen und notwendige Maßnahmen analysiert.

Konditionierungen und Verfahrensabläufe im Unternehmen aufbaut und nur im notwendigen Umfang an die normativen Anforderungen angepasst ist.

2. Legitimation gesetzlicher Regelungen

Ein weiterer Grund kann in der Legitimation gesetzlicher Regelungen gesehen werden. Hierbei kann die formale und die materielle Legitimation unterschieden werden:

Zunächst ist der parlamentarische Gesetzgeber dazu berufen, die wesentlichen Entscheidungen im normativen Bereich selbst zu treffen (Parlamentsvorbehalt); als unmittelbar vom Volk gewählten Legislativorgan zeichnen sich die von ihm verabschiedeten Gesetze durch eine hohe formale Legitimation aus.[48]

Allerdings können nicht alle Sachbereiche durch Parlamentsgesetze inhaltlich rational geregelt werden. Dies gilt besonders für Bereiche, die von hoher Komplexität, Dynamik und Gefahrgeneigtheit geprägt sind.[49] Formale und materiale Parlamentsgesetze können die Komplexität in diesen Bereichen nicht in ausreichendem Maße erfassen, ohne untaugliche Quantitäten anzunehmen,[50] wären in kurzer Zeit veraltet oder würden an der treffsicheren Erfassung aller drohenden Gefahrszenarien scheitern.

Solchen Parlamentsgesetzen würde die materielle Legitimation im Sinne einer sachlich-inhaltlichen Entscheidungskompetenz fehlen.[51] Dieses Defizit kann neben der Verwendung materialer Rechtsbegriffe wie der Angemessenheit besser noch durch inhaltlich reduzierte, prozedurale Vorschriften, die an den entscheidenden, sachnäheren Adressaten gerichtet sind, kompensiert werden. Um gleichwohl ein hinreichendes Maß an formaler Legitimation zu erreichen, können Beteiligungsrechte vorgesehen werden,[52] was auch als „partizipative Demokratie“ bezeichnet wird.[53] Daneben sichern Dokumentations- und Transparenzpflichten eine hinreichende rechtsstaatliche und gesellschaftliche Kontrolle.

Zur angemessenen Gewährleistung von IT-Sicherheit durch die Wahl entsprechender Maßnahmen kann ein Parlamentsgesetz keine abschließende Lösung vorgeben. Zu unterschiedlich sind die Anforderungen an die IT-Sicherheit je nach Sachbereich und zu dynamisch ist die technische Entwicklung. Allenfalls sind solche starren Gesetze in der IT-

---

[48] *Arnim*, DVBl 1987, 1241 (1241 f.).
[49] *Quabeck*, Dienende Funktion des Verwaltungsverfahrens und Prozeduralisierung, S. 185.
[50] Vgl.: *Linzbach*, EurUP 2020, 93 (103).
[51] *Quabeck*, wie zuvor, spricht im Ergebnis zustimmend davon, dass der Versuch der Einflussnahme durch solche parlamentarischen Gesetze „ins Leere läuft“; Vgl.: *Rossen-Stadtfeld*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, § 29, S. 669 f., Rn. 9 f.
[52] *Quabeck*, Dienende Funktion des Verwaltungsverfahrens und Prozeduralisierung, S. 186; *Fisahn*, Demokratie und Öffentlichkeitsbeteiligung, S. 334 ff.
[53] Mit Verweis auf Art. 11 EUV: *Linzbach*, EurUP 2020, 93 (97); siehe hierzu auch: *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 6. Auflage 2022, Art. 11 EUV, Rn. 3.

Sicherheit für sehr kleine Teilbereiche möglich, wie etwa das SmartMeter-Gateway nach den §§ 19 ff. MsbG.[54]

Im Regelfall ist aber vielmehr eine situative Entscheidung der sachnäheren Person oder Institution vorzugswürdig. Eine angemessene Maßnahmenwahl kann durch den Normadressaten selbst sachgerechter vorgenommen werden, da nur dieser Kenntnis über die von ihm verwendeten informationstechnischen Systeme, die damit erbrachten Dienste und damit auch über die heraus resultierenden Risiken sowie die notwendigen Maßnahmenanforderungen hat. Wenn eine Norm auch im IT-Sicherheitsrecht so gestaltet ist, dass dem Adressaten ein Verfahren an die Hand gegeben wird, wie er sich gesetzeskonform verhalten kann, erhöht dies außerdem die Klarheit und das Verständnis bei der Prüfung und auch die Akzeptanz sowie die gesellschaftliche Wirksamkeit von Gesetzen kann gefördert werden.[55] Gleichzeitig wird es so vor dem Hintergrund der stetigen Entwicklung der IT-Sicherheitslage möglich, die Entscheidungen fortlaufend anzupassen, weil keine Einschränkung durch gesetzlich festgelegte Geltungsmaßstäbe vorliegt. Der Entscheidungsprozess kann dann insbesondere durch Dokumentationspflichten rechtsstaatlich kontrolliert werden.

3. Bewältigung von Ungewissheit

Dies führt direkt zum nächsten Argument, namentlich der Ungewissheit aufseiten des Adressaten.

Selbst wenn der Gesetzgeber durch ggf. weniger granulare Gesetze unter Zuhilfenahme unbestimmter Rechtsbegriffe versucht den Sachbereich zu regeln, besteht die sachliche Ungewissheit aufseiten des Adressaten fort.[56] Für die Befolgung formaler und insbesondere auch materialer Normen ist stets spezifisches Wissen erforderlich, um das (Nicht-)Vorliegen der rechtsfolgenbegründenden Tatbestandsmerkmale prüfen bzw. die unbestimmten

---

[54] Hier wird dem Problem sich ständig verändernder technischer Anforderungen über den Verweis auf Schutzprofile begegnet, die durch das BSI ständig zu aktualisieren sind, §§ 19 Abs. 2 und 3, 22 Abs. 1 und 2 MsbG iVm der Anlage zu § 22 Absatz 2 Satz 1 MsbG (BT-Drs. 18/7555, S. 85). Teilweise wird an dieser Stelle jedoch eine zu weitreichende Auslagerung der Regelungsbefugnisse an die Behörde kritisiert, zumal es sich um eine dynamische Verweisung handelt und diese im Einzelfall erheblich in Grundrechte des Betreibers eingreifen kann, Säcker/Zwanziger/*Schmidt*, Berliner Kommentar zum Energierecht, § 22, Rn. 63 ff.

[55] *Beutin*, Die Rationalität der Risikoentscheidung, S. 37 f., m.w.N. *Beutin* ordnet die Rationalität von Gesetzen als Verfassungsgebot ein und legt dar, dass Gesetze durch ihre Funktion und wirkungsvolle Umsetzung der Steuerung der Gesellschaft dienen sollen, um den freiheitlichen Funktionsbestand zu sichern. Die wirkungsvolle Umsetzung sei vor allem durch gesellschaftliches Verständnis und Akzeptanz zu erreichen. Das „möglichst richtige Ergebnis", ermittelt durch Abwägungen, stelle dabei den Kern der Rationalität dar. Dabei bewertet er die Prozeduralisierung von Gesetzen als hilfreiches Mittel zur Regelung nicht vollständig von Erfahrungswissen geprägter Materien.

[56] Ähnlich auch: *Vesting*, Rechtstheorie, S. 32, Rn. 63; *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, § 10, S. 756 f., Rn. 113 f.

Rechtsbegriffe auszufüllen.[57] Diese gilt im Besonderen, wenn sich dem Recht immer komplexer werdende und daher schwerer zu erfassende Sach- und Interessenlagen gegenüberstellen. Solche komplexen Situationen bestehen etwa im Umwelt- und Technikrecht: Oft existiert schon kein verlässliches Wissen, da die entsprechenden Sachphänomene (z.B. Umweltauswirkungen) gar nicht ohne weiteres antizipierbar sind. Selbst wenn Wissen objektiv vorhanden ist, muss dieses für den Entscheidungsprozess erst gefunden und aufbereitet werden.[58] Aber auch bei Entscheidungen in komplexen Gemengelagen von widerstreitenden Interessen besteht oft kein abstraktes Wissen zur Herstellung des tatbestandlich geforderten angemessenen Ausgleichs.[59] Vielmehr müssen die Interessen im jeweiligen, konkreten Einzelfall durch ein Verfahren ermittelt, bewertet und gegenübergestellt werden. Insgesamt kann mithilfe von prozeduralem Recht sowohl sachliche als auch rechtliche Ungewissheit durch die Etablierung eines Verfahrens anstelle materialer Vorgaben gemindert werden.

Auch in der IT-Sicherheit hat der Normadressat zunächst kein abschließendes Wissen über die bestehenden Risiken und entsprechende Gegenmaßnahmen, welches jedoch für die angemessene Maßnahmenwahl erforderlich ist. Die Risiken müssen somit erst in einem Verfahren sorgfältig identifiziert und analysiert werden. In einem weiteren Schritt müssen dann Maßnahmen betrachtet werden, die das Risiko mindern können. Anschließend ist eine Interessenabwägung zwischen der zu erreichenden Risikominderung durch die Maßnahmen und dem hierfür erforderlichen Aufwand vorzunehmen, wobei auch der ebenfalls nicht immer eindeutig zu bestimmende Stand der Technik zu berücksichtigen ist. Insofern besteht hinsichtlich der angemessenen Maßnahmenwahl als Handlungsauftrag eine hohe Ungewissheit, die erst durch das Verfahren zumindest teilweise reduziert werden kann.

III. Lösung durch die Vorgabe eines gesetzlichen Risikomanagements

Wie gezeigt werden konnte, sprechen mehrere starke Argumente für eine Prozeduralisierung des Angemessenheitsbegriffs. Als Lösung könnte ein gesetzliches Risikomanagement vorgegeben werden, die das Verfahren zur Auswahl angemessener Maßnahmen festlegt. Bisher wird statt eines solchen auf privaten Standards wie etwa der ISO 27.000 verwiesen. Daneben existieren auch behördliche Standards wie der BSI-Grundschutz.

Die private Normung erweist sich aber aus mehreren Gründen nicht als uneingeschränkt geeignet, weil sie letztlich mit ihrem Zuschnitt auf private Unternehmen „andersartige

[57] Vgl.: *Campos*, KJ 2019, 400 (401).
[58] *Hagenah*, in: Grimm, Neue Instrumente für eine neue Staatsaufgabe, 487 (488).
[59] Allenfalls kann solches Wissen näherungsweise durch die systematische Sammlung entsprechender Entscheidungen erzeugt werden.

Spannungslagen“[60] bewältigt; sie hat insofern insbesondere keinen primären Fokus auf rechtliche Schutzgüter und erlaubt eine individuell-wirtschaftliche Risikoakzeptanz.[61]

Behördliche Standards wie etwa der BSI-Grundschutz, der IT-Sicherheitskatalog zu § 11a EnWG oder die MaRisk sind zunächst anders als private Standards an die normativen Anforderungen angepasst. Weiterhin können die Behörden bei deren Ausgestaltung auf großes Sachwissen zurückgreifen, das die Behörde durch die Nähe zur realen Entwicklung im technischen Bereich und das einhergehende Verständnis von Neuerungen aufweisen kann.[62]

Den behördlichen Standards fehlt es hingegen an einer direkten legislativen Legitimation. Die Behörde ist im Rahmen der Gewaltenteilung nach Art. 20 Abs. 3 GG Teil der Exekutive. Als durch das Volk gewähltes Organ entspricht es dem Demokratieprinzip, wenn Regelungen durch das Parlament als formelle Gesetze getroffen werden. Als übergeordnetes Gesetz würde es auch für mehr Einheitlichkeit sorgen als die modifizierenden Verweise der jeweiligen Behörden (BSI, BNetzA, BaFin). Insgesamt spricht somit viel für die gesetzliche Implementierung eines Risikomanagements.

D. Notwendigkeit einer Anpassung der gerichtlichen Kontrolle

Korrespondierend zu einer Prozeduralisierung des Angemessenheitsbegriffs ist auch die gerichtliche Kontrolle des Abwägungsergebnisses zu diskutieren. Dabei ist insbesondere relevant, nach welchen Maßstäben ein Gericht im Falle einer streitigen Auseinandersetzung in die getroffene Entscheidung des Adressaten eingreifen sollte.

I. Bisherige Kontrolldichte

Bisher ist die Einhaltung der Normen des IT-Sicherheitsrecht vollständig gerichtlich überprüfbar, d.h. der unbestimmte Rechtsbegriff der Angemessenheit wird auf seine Einhaltung hin überprüft. Es verbleibt dem Normadressaten auf Rechtsfolgenseite im Ergebnis kein Spielraum, der eine eingeschränkte gerichtliche Kontrolle, vergleichbar der Ermessensfehlerlehre im Verwaltungsrecht, nach sich ziehen könnte.

Zwar wird insofern keine Punktlandung erwartet, d.h. der Normadressat muss nicht genau jene Maßnahmen treffen, die gerade so ausreichend wären. Über das Erfordernis der Angemessenheit hinausgehende Maßnahmen sind freilich zulässig und auch alternative,

[60] BVerfG NJW 2020, 2235, 2256, Rn. 215.
[61] Vgl. hierzu ausführlich: *Sterz/Werner/Raabe*, Intelligente Verkehrssysteme - IT-Sicherheit in offenen Infrastrukturen, RDV 6/2022.
[62] *Lorenz*, Optimierung von Verfahren zur Lösung rechtsrelevanter Wissensprobleme in kritischen Infrastrukturen, S. 98.

gleichwertige Maßnahmen sind möglich. Allerdings stellt das Gericht zweifelsfrei fest, wenn Maßnahmen nicht mehr angemessen sind.[63]

Diese Vorgehensweise könnte das oben aufgezeigte Problem einer mangelnden sachlich-inhaltlichen Kompetenz des Gesetzgebers in dem IT-sicherheitsrechtlichen Regelungsbereich auf die Justiz verlagern. Im Vergleich zu der zuständigen Fachverwaltung (etwa dem BSI) fehlen der rechtsprechenden Gewalt in Gebieten des nicht vorgeprägten, einschätzenden und gestalterischen Handelns die Informationen über wissensintensive Bereiche.[64] In Gebieten wie beispielsweise dem Arzthaftungsrecht, die ähnlich wissenschaftlich geprägt sind, wird diesem Defizit durch die Einholung von Sachverständigengutachten Rechnung getragen. Dies ist jedoch kostenintensiv und verkompliziert sowie verlängert das Verfahren. Dem könnte dadurch begegnet werden, die gerichtliche Kontrolle in den Bereichen einzusetzen, in denen das Recht gerichtlich einfacher überprüfbare Maßstäbe bereithält.

II. Ansätze zur Überprüfung nach der Prozeduralisierung

Denkbar wäre, dass das Gericht nach einer Prozeduralisierung des IT-Sicherheitsrechts nur die Einhaltung des Verfahrens, also des Risikomanagements, prüfen würde. Ob die Maßnahmen am Ende angemessen sind, würde hingegen offenbleiben. Die gerichtliche Kontrolle würde sich damit darauf konzentrieren, außerhalb des Sachwissens überprüfbare, verfahrensrechtliche Maßstäbe zu überprüfen.

Gesetzlich ausgestaltet ist ein solches Vorgehen beispielsweise in § 1 Abs. 2 UrhDaG, der eine Verantwortlichkeit des Diensteanbieters nur bei Verstoß gegen die Verfahrenspflichten, gegen branchenübliche Standards und den Verhältnismäßigkeitsgrundsatz vorsieht. Selbst wenn nach materiellem Recht eine Maßnahme (dort das Löschen bzw. nicht-Löschen eines (vermeintlich) urheberrechtswidrigen Inhalts) rechtswidrig ist, resultiert daraus somit keine Haftung.[65]

Ein anderes Beispiel für eine solche eingeschränkte Prüfung liegt in der Kontrolle verwaltungsrechtlichen Ermessens. Der hohen Sachnähe und Kompetenz der Verwaltung wird durch eine eingeschränkte Kontrolle Rechnung getragen. Im Rahmen der Ermessensfehlerlehre werden Entscheidungen nicht hinsichtlich ihrer Zweckmäßigkeit, sondern nur in Bezug auf

[63] So entschied das LG Bonn mit Urteil vom 11.11.2020 – 29 OWi 1/20, dass ein Callcenter für die Herausgabe von Daten zur Identifizierung des Anrufers zwei Authenitifizierungsmethoden heranziehen muss.

[64] Quabeck, Dienende Funktion des Verwaltungsverfahrens und Prozeduralisierung, S. 207 f.

[65] Das Verfahren ist in den §§ 4, 7-11 UrhDaG geregelt. Eine Entscheidung muss beispielsweise nach § 14 Abs. 3 Nr. 3 i.V.m. § 12 Abs. 2 S. 1 UrhDaG innerhalb der Frist von einer Woche getroffen werden. Auch wenn eine Nutzung zu Unrecht erlaubt wurde, führt dies nach § 12 Abs. 2 UrhDaG nicht zu einer Haftung. Siehe auch: *Spindler*, WRP 2021, 1245 (1248).

Fehler im Abwägungsvorgang geprüft. Nur, wenn die Behörde die Ermessensgrenzen überschreitet, ist ihr Handeln als rechtswidrig zu bewerten, § 114 VwGO.[66]

Im Ergebnis ist im IT-Sicherheitsrecht jedoch für eine solche Einschränkung der gerichtlichen Kontrolle kein Raum. Gegen eine Beschränkung auf die reine Verfahrenseinhaltung wie im UrhDaG spricht die deutlich höhere Bedeutung der Schutzgüter. Insbesondere im KRITIS-Recht werden höchstrangige Rechtsgüter wie etwa die Versorgungssicherheit mit Elektrizität oder Trinkwasser verbunden mit den Individualgrundrechten der Nutzer:innen (z.B. Leben und körperliche Unversehrtheit) geschützt.

Mit Blick auf die Ermessensfehlerlehre kommt hinzu, dass die Adressaten des IT-Sicherheitsrechts teilweise private Unternehmen sind, die keine direkte Grundrechtsbindung trifft.[67] Sie sind somit auch nicht als Teil des Staates dem öffentlichen Wohl, sondern vorrangig eigenen Unternehmensinteressen verpflichtet und finanziell eigenverantwortlich, was eine unangemessen niedrige Maßnahmenwahl wahrscheinlicher erscheinen lässt.[68]

III. Fazit

Insgesamt ist somit eine strenge, gerichtliche Prüfdichte gefordert, die nicht bei der Einhaltung des Verfahrens Halt machen kann, sondern die konkreten Maßnahmen auf ihre Wirksamkeit und Angemessenheit hin überprüfen muss. Das gesetzliche Risikomanagement stellt insofern nur ein Hilfsmittel für den Normadressaten zur Erfüllung seiner gesetzlichen Pflichten dar, ohne aber die Haftung und die damit verbundene gerichtliche Kontrolle zu modifizieren.

E. Gesamtergebnis und Ausblick

Ausgangspunkt des Aufsatzes war die Frage, ob es im IT-Sicherheitsrecht sachgerecht und hinreichend ist, wenn der Handlungsauftrag zur Gewährleistung derselben nur mit dem materialen Begriff der „Angemessenheit“ konturiert wird. Im Ergebnis ist diese Frage negativ zu beantworten, da die besseren Argumente für eine Prozeduralisierung des Angemessenheitsbegriff durch die Vorgabe eines gesetzlichen Risikomanagements sprechen. Diese würde ein einheitliches Verfahren bereitstellen, mithilfe dessen der Normadressat die

[66] Dabei kann die Ermessensfehlerlehre nicht als prozedurales Recht eingeordnet werden. Statt eines Verfahrens, das die Behörde auf dem Weg zu einer Entscheidung leiten könnte, sind die Begrenzungen im Entscheidungsspielraum negativ vorgegeben, es wird statt einer Leitlinie eher klargestellt, aus welchem Rahmen die Entscheidung nicht hinaustreten darf; Bader/Ronellenfitsch/*Aschke*, BeckOKVwVfG, § 40 Rn. 5.

[67] Anders bei Betrieben, die ganz oder überwiegend in öffentlicher Hand stehen: Diese sind an Grundrechte gebunden, um der Verwaltung keine „Flucht ins Privatrecht“ zu ermöglichen, *BVerfG* NJW 2011, 1201, 1202, Rn. 48 ff.; beachte aber zu Plattformen wie Facebook, welches als soziales Netzwerk unter der NIS2-RL auch kritische Infrastuktur wird die gesteigerte Grundrechtsbindung nach *BGH* GRUR 2020, 1318 Rn. 105.

[68] Dabei wird nicht verkannt, dass durch ein entsprechendes Sanktions- und Haftungsregime auch für private Unternehmen ein entsprechendes Anreizsystem etablieren kann.

angemessenen Maßnahmen auswählen und somit dem Normauftrag bestmöglich entsprechen kann. Eine Beschränkung der gerichtlichen Kontrolle auf das Verfahren sollte insbesondere aufgrund der Bedeutung der zu schützenden Rechtsgüter damit hingegen nicht einhergehen.