IT-Sicherheit: ein verfassungsrechtlicher Zugang

Isabella Risini

A. Die verfassungsrechtliche Relevanz von IT-Sicherheit

Der Beitrag beleuchtet Fragen der IT-Sicherheit aus einer verfassungsrechtlichen Perspektive. Besonderes Augenmerk liegt auf der möglichen Verantwortung des Staates im Bereich der IT-Sicherheit. Begrifflich verknüpft er die traditionell staatliche Aufgabe der Gewährleistung von Sicherheit, einschließlich der IT-Sicherheit, mit der faktischen und rechtlichen Verantwortung von Unternehmen für IT-Sicherheit. Dieser Ansatz soll den Blick darauf ermöglichen, dass die Rückbindung von IT-Sicherheit in das Verfassungsrecht bisher unzureichend dogmatisch durchdrungen ist.

Das Sicherheitsrecht ist traditionell eines der am stärksten verfassungsrechtlich determinierten Rechtsgebiete.[1] Das Verständnis von Sicherheit und Sicherheitsrecht gibt Auskunft zum Verhältnis zwischen Staat und seinen Bürgern; die Risikotoleranz indiziert die Freiheitsgrade, die sich eine Gesellschaft bewusst bewahren möchte.

Mit Blick auf die zunehmende Abhängigkeit von Datenverarbeitung quer durch alle Lebensbereiche, oft verschlagwortet mit dem Begriff der „Digitalisierung", ist eine sichere IT-Umgebung eine wichtige Vorbedingung für die Ausübung der meisten Grundrechte geworden. Die Sicherheit von Datensystemen ist auch die Grundbedingung für einen Großteil der wirtschaftlichen Wertschöpfung. Die Zukunft in einer Welt mit autonomen Fahrzeugen zu Lande[2] und in der Luft sowie allerlei künstlich intelligenten Maschinen und Robotern[3], die unseren Alltag begleiten und erleichtern sollen, ist ohne IT-Sicherheit undenkbar.[4] Bislang bleibt das

---

1 *Gärditz*, Sicherheitsrecht als Perspektive, GSZ 2017, S. 1.

2 *Roßnagel/ Hornung*, (Hrsg.) Grundrechtsschutz im Smart Car, Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug, 2019.

3 *Eberstaller/Forgó*, KI-spezifische Rechtsfragen der Cybersicherheit, in: Ebers/Heinze/Krügel/Steinrötter (Hrsg.), Künstliche Intelligenz und Robotik, Rechtshandbuch, 2020, S. 441; Ebers/Steinrötter (Hrsg.), Künstliche Intelligenz und smarte Robotik im IT-Sicherheitsrecht, 2021 (im Erscheinen).

4 *Müller-Quade* u.a., AG IT-Sicherheit, Privacy und Ethik, Whitepaper Künstliche Intelligenz und IT-Sicherheit, Bestandsaufnahme und Lösungsansätze, 4.4.2019,

Verfassungsrecht noch schuldig, wie der überragende, aus rechtswissenschaftlicher Sicht verhältnismäßig neue Zielwert der IT-Sicherheit optimal zu verwirklichen ist.

Dieser Beitrag gibt zunächst eine begriffliche Orientierung zum Topos „IT-Sicherheit" (B.). Im darauffolgenden Abschnitt (C.) erfolgt eine Rekonstruktion dessen, was das Grundgesetz in Bezug auf IT-Sicherheit ausdrücklich und qua richterlicher Rechtsfortbildung regelt. Insbesondere wird die Aufteilung von Verantwortungen für Universaldienste zwischen Staat und Unternehmen im Rahmen des Privatisierungsfolgenrechts beleuchtet. Sodann werden der grundrechtliche Schutz von IT-Sicherheit und seine Grenzen in den Blick genommen.

In Abschnitt D. wird der Blick auf den inter- und intradisziplinären Mehrwert gelegt, der in besonderem Maße für Fragen der IT-Sicherheit vorhanden ist. Insbesondere wird anhand von Beispielen aus verschiedenen Fachsäulen der Rechtswissenschaft herausgearbeitet, wo ein klarerer verfassungsrechtlicher Maßstab zum Oberthema IT-Sicherheit wünschenswert wäre. Im Fazit wird hervorgehoben, dass es über den Selbstzweck der Dogmatik hinaus einen Gewinn an Rechtssicherheit bedeuten würde, wenn das deutsche Verfassungsrecht einen Kompass für Fragen der IT-Sicherheit bereithielte.

B. Der Begriff der IT-Sicherheit – ein Zugang über Schutzziele

IT-Sicherheit, auch Cybersicherheit, Cybersecurity oder Information Security, ist ein technischer Idealzustand, in dem ein IT-System vor Angreifern von innen und von außen geschützt ist. Cyber-Sicherheit ist indes kein statisches Ziel. Eine besondere Eigenschaft aller Fragen der IT-Sicherheit ist die Notwendigkeit, der ständigen Anpassung und Weiterentwicklung der Schutzmechanismen und Abwehrstrategien. Diese zeitliche Dimension der IT-Sicherheit, mit schnell fortschreitenden technischen Anforderungen, macht die rechtliche Einhegung über schwerfällige Gesetzgebungsmechanismen jedenfalls herausfordernd.

Wegen der Vielgestaltigkeit von Fragen der Sicherheit von Daten ist eine übergreifende rechtliche Definition von IT-Sicherheit Desiderat.[5] Er-

---

https://www.plattform-lernende-systeme.de/publikationen-details/id-1-broschuere.html (abgerufen am 10.1.2020).

5 *Kipker*, Grundlagen und Strukturen, in: Kipker (Hrsg.), Cybersecurity, 2020, Rn. 4 ff.; *Hornung/Schallbruch*, Einführung, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, S. 25.

schwerend für den Prozess einer einheitlichen Begriffsbildung kommt hinzu, dass die Begrifflichkeiten rund um die IT-Sicherheit inter- und intradisziplinär mit vielen verschiedenen Konnotationen belegt sind.

I. Fragmentiertheit rechtlicher Anforderungen an die IT-Sicherheit

Bisher zeichnen sich die rechtlichen Anforderungen an IT-Sicherheit als Querschnittsmaterie vor allem durch ihre Fragmentiertheit aus. Eine Bestandsaufnahme des Rechts der der IT-Sicherheit darf nicht nur entlang der vorgefundenen Rechtsgebietsgrenzen und Fachsäulen verlaufen. Ohne Anspruch auf eine vollständige Auflistung von Rechtssätzen und Materien, die sich mit IT-Sicherheit befassen, reicht diese vom Recht der Produkthaftung[6] über das klassische zivile Haftungsrecht[7] bis hin zum Urheber- und Lauterkeitsrecht.[8] Am Beispiel des Rechtes des Datenschutzes kann außerdem abgelesen werden, wie sehr das Zusammenspiel von verschiedenen Ebenen entscheidend war und wohl auch in Zukunft sein wird.[9]

Beispielhaft für das öffentliche Recht sei hier aufgeführt, dass die Betreiber von sogenannten kritischen Infrastrukturen (Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen) sektoral besondere Anforderungen erfüllen müssen.[10] Diese Diskriminierung zwischen Unternehmen, die in gewissen Sektoren agieren und „normalen" Unternehmen wird bislang allgemein hingenommen.

Die Fragmentiertheit des Rechts der IT-Sicherheit lässt sich nicht zuletzt auf die Gesetzgebungs- und Verwaltungszuständigkeiten im föderalen Ver-

---

6 *Spindler*, Verantwortung der IT-Hersteller (produktbezogene Pflichten), in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, S. 248.

7 *Voigt*, IT-Sicherheitsrecht, Pflichten und Haftung im Unternehmen, Otto Schmidt Verlag, 2018.

8 *Barudi*, Urheber- und Lauterkeitsrecht, Know-How-Schutz, in Kipker (Hrsg.), Cybersecurity, 2020, S. 273.

9 *T. Streinz*, The Evolution of European Data Law, in: Caig/de Búrca, The Evolution of EU Law, 2021 im Erscheinen; *Voskamp*, Datenschutz, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 151; siehe auch *Conrad/Eckhardt/Fleischhauer/Huppertz/Streitz*, Compliance, IT-Sicherheit, Ordnungsmäßigkeit der Datenverarbeitung, in: Auer-Reinsdorff / Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 2019, S. 1637.

10 § 2 Abs. 9 und 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), in Verbindung mit der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV).

fassungsstaat zurückführen.[11] Art. 91 c Abs. 2 GG, der in einem gewissen Teilbereich eine Kooperation von Bund und Ländern ermöglicht, lässt erahnen, wie schwierig ein übergreifender Ansatz für das Recht der IT-Sicherheit umzusetzen wäre.[12] Ein solcher übergreifender Ansatz geht weit über die Ambition des vorliegenden Beitrages hinaus.

Die Auffächerung des Rechts der IT-Sicherheit geht einher mit einer höher werdenden Regelungsdichte, bisweilen ist auch die Rede von einem „Normenzoo".[13] Außerdem fließen in die Standardisierung bzw. Normgebung vielfältige Interessen ein. Flankiert wird diese Entwicklung von steigender Komplexität von informationstechnischen Systemen im Zeitalter des Internets der Dinge (Internet of Things) und entsprechend höheren Anforderungen an die Absicherung vor Angriffen.

II. Ein Zugang über Schutzziele

IT-Sicherheit verfolgt verschiedene Schutzziele.[14] Diese verschiedenen Ziele müssen jeweils bedarfsorientiert durch Priorisierung miteinander in Einklang gebracht werden. Die Schutzziele werden durch verschiedene technische Methoden verfolgt. Die Ziele überschneiden sich vielfach; eine abschließende Aufzählung ist schwer möglich. In der Verfolgung dieser Ziele kommt zum Ausdruck, dass es sich um einen sehr dynamischen Prozess handelt, der stets einen Idealzustand anstrebt. Regelungstechnisch wird diese Dynamik mit unbestimmten Rechtsbegriffen abgefedert, insbesondere dem „Stand der Technik".[15]

1. Vertraulichkeit

Zu den Zielen der IT-Sicherheit gehört die Vertraulichkeit, die trotz der Benutzung von IT-Systemen gewahrt werden soll. Vertraulichkeit wird

11 Z.B. Art. 74 Nr. 11 GG „Recht der Wirtschaft".
12 *Spiegel*, IT im Grundgesetz, NvWZ 2009, S. 1128.
13 Siehe dazu etwa den „Cybersecurity-Navigator", https://cybersecurity-navigator.de.
14 *Sohr/Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 23, 26ff.
15 Siehe *Ekrot/Fischer/Müller*, Stand der Technik, in: Kipker, (Hrsg.), Cybersecurity, 2020, S. 83, 85ff, und zur Differenzierung zwischen Begriffen wie „Allgemein anerkannte Regeln der Technik", „Stand der Technik" und „Stand von Wissenschaft und Forschung".

hier verstanden als das Bedürfnis, Daten geheim zu halten und einen Zugriff nur an einen bestimmten Personenkreis zu ermöglichen.[16] Ein Beispiel sind Firmengeheimnisse oder Forschungsergebnisse wie etwa die Formel für ein Vakzin gegen das Corona-Virus.[17] Das Recht des Datenschutzes hebt den Schutz von personenbezogenen Daten heraus.[18]

2. *Verfügbarkeit*

Die Verfügbarkeit (availability) eines IT-Systems ist ebenfalls ein Schutzziel. IT-Systeme müssen jederzeit einen Zugriff erlauben, um die Nutzung eines Dienstes zu ermöglichen.[19] So wurde etwa die Ruhr-Universität Bochum im Mai 2020 Ziel einer Attacke, die es für Studierende und Mitarbeitende für Wochen unmöglich machte, auf E-Mails, Online-Lernplattformen und auch Notendatenbaken zuzugreifen.[20] Der Hackerangriff auf ein Universitätsklinikum in Düsseldorf im September 2020 stand zunächst in Verdacht, Ursache für den Tod einer Patientin gewesen zu sein. Medienberichten zufolge konnte die Staatsanwaltschaft diesen Verdacht zwar nicht erhärten.[21] Ein Angriff auf ein Krankenhaus, der tatsächlich Menschenleben gefährdet ist durchaus denkbar. Ein Angriff auf die Funke Mediengruppe im Dezember 2020 erschwerte das Erscheinen vieler Blätter

16 *Sohr/Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 23, 26.

17 Siehe dazu die Informationen der European Medicines Agency, die im Dezember angeriffen wurde: Cyberattack on EMA – update 5, https://www.ema.europa.eu/en/news/cyberattack-ema-update-5, mit weiteren Nachweisen auf die Historie des Angriffs. (abgerufen am 10.1.2020), die Debatte, ob die Formeln für die Vakzine der Öffentlichkeit gleichsam als öffentliches Gut zur Verfügung stehen sollten wird hier außen vorgelassen.

18 *Jandt*, IT-Sicherheit als Mittel und als Bedrohung des Datenschutzes, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, S. 391.

19 *Sohr/Kemmerich*, Technische Grundlagen der Informationssicherheit, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 23.

20 Ruhr-Uni fährt IT nach Cyberangriff wieder hoch, https://www.forschung-und-lehre.de/politik/ruhr-uni-faehrt-it-nach-cyberangriff-wieder-hoch-2797/. (abgerufen am 10.1.2020).

21 Hackerangriff auf Düsseldorfer Uniklinik: Ermittlungen wegen fahrlässiger Tötung eingestellt, https://www1.wdr.de/nachrichten/rheinland/duesseldorf-uniklinik-hackerangriff-ermittlungen-fahrlaessige-toetung-100.html. (abgerufen am 10.1.2020).

in Deutschland.[22] Die wirtschaftlichen Folgen des Angriffs dürften erheblich sein.[23]

3. *Integrität und Authentizität*

Schließlich sind die Integrität und die Authentizität von Daten zu nennen. Der Autor oder Urheber einer Nachricht oder eines Datensatzes müssen eindeutig sein. Für den Bereich der *Smart Contracts* wird hier auch oft von der Nicht-Abstreitbarkeit eines Datensatzes (etwa einer Willenserklärung) gesprochen.

4. *IT-Sicherheit und der Gedanke der Vorsorge*

Der IT-Sicherheit wohnt die Idee und die Notwendigkeit der Vorsorge inne.[24] Der Gedanke der Vorsorge scheint dahingehend immer dringender geboten, dass das heraufziehende Zeitalter der Quantencomputer viele auf klassischer Kryptografie basierenden IT-Sicherheitsmaßnahmen schon heute in Frage stellt (*record now, decrypt later*).[25] Die Notwendigkeit zur Vorsorge dürfte gleichzeitig Hemmschuh für eine systematische politisch-rechtliche Durchdringung des Themenfelds IT-Sicherheit sein: das in Zeiten von Corona viel zitierte Präventionsparadox – *there is no glory in prevention*.

Der Ansatz, Unternehmen verstärkt Vorsorgepflichten in Bezug auf IT-Sicherheit aufzuerlegen, findet sich bereits vielfach einfachgesetzlich[26], und wird im „Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“, auch bekannt als „IT-Sicherheits-

22 *Muth*, Der Ransomware-Schrecken des deutschen Mittelstands, Süddeutsche Zeitung, 31.12.2020 zur Attacke auf die Funke Mediengruppe, https://www.sueddeutsche.de/digital/ransomware-clop-fin11-fire-eye-cybercrime-1.5161726. (abgerufen am 10.1.2020).

23 Konkrete Zahlen zum Vorfall sind nicht verfügbar; siehe generell *Bertschek/Janßen/Ohnemus*, IT-Sicherheit aus ökonomischer Perspektive, in: Kipker (Hrsg.), Cybersecurity, 2020, S. 63f.

24 *Wolff*, You'll See This Message When It Is Too Late, The Legal and Economic Aftermath of Cybersecurity Breaches, 2018, S. 205ff.

25 Zum Entwicklungsstand von Quantencomputern mit Daten aus einer Studie mit dem Stand Juni 2020 siehe etwa https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer_node.html. (abgerufen am 10.1.2020).

26 Z.B. § 8a BSIG.

gesetzes 2.0“, der im Dezember 2020 auf Ebene des Bundeskabinetts beschlossen wurde[27], weiter ausgedehnt. Sicherheit ist indes teuer. Der „Erfüllungsaufwand“ für die Wirtschaft allein in der Folge der Änderungen im „IT-Sicherheitsgesetz 2.0“ wird auf 21,6 Millionen Euro geschätzt. Für die Verwaltung werden die Kosten auf 202,2 Millionen Euro jährlich geschätzt.[28]

C. IT-Sicherheit und Verfassungsrecht

In diesem Abschnitt erfolgen Bestandsaufnahme und Rekonstruktion dessen, was die Verfassung in Bezug auf die „IT-Sicherheit“ aufweist. Der Abschnitt dient dazu, verschiedene verfassungsrechtliche Bausteine sichtbar zu machen. Das uneinheitliche Gesamtbild, zu dem sich die Bausteine fügen, offenbart den Bedarf, Fragen der IT-Sicherheit grundsätzlich zu beleuchten.

I. IT-Sicherheit in privater Hand und die Rolle des Gewährleistungsstaates

Lagen in analogeren Zeiten zentrale „digitale“ Leistungen in den Händen des Staates, etwa die Telekommunikation, ist heute der private Wettbewerb die Regel: Die meisten Dienste, die jeder Zeitgenosse und jede Zeitgenossin in der Informationsgesellschaft über Kommunikationsinfrastrukturen benutzt, werden privatwirtschaftlich ermöglicht. Dabei sind die beteiligten Unternehmen oft mächtig; jedenfalls dem *durchschnittlichen* Nutzer überlegen.[29] In weiten Teilen handelt es sich also bei der Bereitstellung des digitalen Raumes als Grundlage für die Ausübung von Grundrechten einschließlich wirtschaftlicher Wertschöpfung nicht um staatliche Daseinsvorsorge, sondern um privatwirtschaftliche Wertschöpfung. Diese Ausgangslage ist für die heutige Rolle des „Gewährleistungsstaates“ prägend.

---

27 Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme; https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf;jsessionid=39F809A1188D562C61D08270E7764FA0.2_cid295?__blob=publicationFile&v=2 (abgerufen am 10.1.2020).

28 Siehe E 2 und E 3 in Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, Fn. 27).

29 *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009, 1010.

Diejenigen Rechtsbereiche, die die Folgen der Privatisierung betreffen – auch „Privatisierungsfolgenrecht“[30] – regeln für gewisse netzgebundene Sektoren (z.B. Post, Telekommunikation) besondere Gewährleistungspflichten direkt in der Verfassung. So geht Art. 87f Abs. 1 GG in seinem Wortlaut davon aus, dass der Bund im Bereich des Postwesens und der Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen *gewährleistet*. Für den Bereich der Energie finden sich keine expliziten verfassungsrechtlichen Vorgaben. Indes wird hier ein verfassungsrechtliches Mindestmaß über das verfassungsrechtliche Gebot der Gewährleistung gleichwertiger Lebensverhältnisse über die Ländergrenzen hinweg (Art. 72 Abs. 2 GG, Art. 104b Abs. 1 Nr. 2 GG) konstruiert, unter Zuhilfenahme des Sozialstaatsprinzips.

Einfachgesetzlich findet sich die Idee der Gewährleistung bzw. des Gewährleistungsstaates in dem Begriff des „Universaldienstes“ wieder.[31] So sieht z.B. das Regelungsmodell des Telekommunikationsgesetz (TKG) vor, dass ein konkret verpflichtetes Unternehmen einen finanziellen Ausgleich erhalten soll, zu dem alle abstrakt verpflichteten Unternehmen eine Abgabe leisten (§§ 82, 83 TKG). Die Verfassungsmäßigkeit dieser Sonderabgabe ist wiederum zweifelhaft.[32] Die Finanzverfassung geht von der Leitidee aus, dass die Finanzierung der staatlichen Aufgaben in erster Linie aus dem Ertrag der in Art. 105 ff. GG geregelten Einnahmequellen erfolgt. Alle Gemeinlasten sind danach aus Steuern zu finanzieren.

Bisher haben Unternehmen durch die freiwillige Übernahme von Pflichten das Universaldienstmodell praktisch kaum relevant werden lassen.[33] Ob sich das hier skizzierte Modell auf den Aspekt der IT-Sicherheit bei der Erbringung von Universaldiensten übertragen lässt, sei hier dahingestellt. Vor dem Hintergrund der verfassungsrechtlichen Fragwürdigkeiten wäre das Modell wohl auch über die sektoralen Grenzen des Privatisierungsfolgenrecht hinaus nicht tauglich, um Verantwortung zwischen Staat und Privaten aufzuteilen.

---

30 *Gärditz*, Die Organisation der Wirtschaftsverwaltung, § 4, Rn. 40; auch *Ludwigs*, Netzregulierungsrecht, § 12 Rn. 2, jeweils in Schmidt/Wollenschläger (Hrsg.), Kompendium Öffentliches Wirtschaftsrecht, 2016, 4. Auflage.

31 *Ludwigs*, § 12, Rn. 3, 33, 82.

32 Statt vieler etwa *Von Danwitz*, Die Universaldienstfinanzierungsabgaben im Telekommunikationsgesetz und im Postgesetz als verfassungswidrige Sonderabgaben, NvwZ 2000, S. 615.

33 *Möstl*, Art. 87f GG, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, Rn. 81, 82 (Stand: 92. EL 2020).

II. IT-Sicherheit als Staatsaufgabe und der Gedanke der Vorsorge

Sicherheit ist Grund und Rechtfertigung jedes Staatswesens. In der aktuellen „Datenstrategie der Bundesregierung" heißt es dazu: „Neben entsprechenden Rechten der Einzelnen und Transparenz im Umgang mit Daten ist die Gewährleistung von struktureller Daten- und IT-Sicherheit für alle Beteiligten *existenziell*.[34] Die Fassbarkeit von IT-Sicherheit in der Kategorie „Staatsaufgabe" wird im Kern zu bejahen sein.[35] IT-Sicherheit als Staatsaufgabe bedeutet nicht, dass der Staat selbst tätig werden muss, vgl. auch Art. 33 Abs. 4 GG. *Hornung/Schallbruch* leiten einen „Auftrag" des angemessenen Schutzes von IT-Sicherheit aus der „Kernaufgabe des modernen Staates zur Gewährleistung von Sicherheit" ab, und führen zur verfassungsrechtlichen Herleitung den Beschluss des Bundesverfassungsgericht zum Kontaktsperregesetz von 1978 an.[36] Das Bundesverfassungsgericht ließ dort wissen, dass

> „[d]ie Sicherheit des Staates als verfaßter Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit seiner Bevölkerung […] *Verfassungswerte* [sind], die mit anderen im gleichen Rang stehen und unverzichtbar sind, weil die Institution Staat von ihnen die eigentliche und letzte Rechtfertigung herleitet."[37]

Betrachtet man die Entwicklungen, die das heute 30-jährige Bundesamt für Sicherheit in der Informationstechnik (BSI) durchlaufen hat, so zeichnet sich hier eine Ausweitung der Aufgaben ab: zunächst stand der Schutz staatlicher Einrichtungen vor IT-Risiken im Vordergrund. Inzwischen werden auch Akteure in der Wirtschaft einbezogen.[38]

---

34 Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt
und nachhaltiges Wachstum, 27.1.2021. https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632. Hervorhebung der Autorin (abgerufen am 30.1.2020).

35 *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, Rn. 48.

36 *Hornung/Schallbruch*, Einführung, Rn. 7, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, unter Rekurs auf BVerfG 49, 24, 56.

37 BVerfG 49, 24, 56, Hervorhebung von der Autorin.

38 *Hornung*, Neue Pflichten für Betreiber kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes, NJW 2015, 334; Selbstdarstellung des BSI: „Entscheidend erweitert wurden die Aufgaben und Befugnisse des BSI durch das im Juli 2015 in Kraft getretene „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz). Mit verbindlichen Mindestanforderungen an die

Staatsaufgabe ist dabei, was der Staat sich selbst zur Aufgabe macht, die Begründung einer Staatsaufgabe unterliegt keinem Verfassungsvorbehalt.[39] Die Einrichtung von Behörden wie etwa dem BSI und der immer weiter aufgefächerten Gesetzgebung im Bereich der IT-Sicherheit können dabei Indiz für eine Staatsaufgabe sein. Ein Schluss auf die Modalitäten und wohl auch Lastentragung der Aufgabenwahrnehmung durch den Staat selbst oder durch Dritte ist jedoch nicht möglich.

Die Rolle des Staates in der sich wandelnden Gesellschaft gepaart mit Herausforderungen neuer Technologien ist indes keine neue Fragestellung.[40] Der Begriff der Risikogesellschaft[41] drängt sich dabei im Zusammenhang mit der Frage nach Staatsaufgaben auf und stammt aus dem Kontext eines vorwiegend anlagenbezogenen staatlichen Risikomanagements. In der Staatsrechtslehre, insbesondere von *Grimm*, wird dazu beobachtet, dass im Zusammenhang mit immer weiter gehenden Staatsaufgaben das (Verfassungs-)recht an Steuerungskraft verliert. Damit einher gehen größere Handlungsspielräume der Administration.[42] *Köck* kommt (nicht im konkreten Kontext der IT-Sicherheit) zu dem Ergebnis, dass die Rolle des Staates sich dahingehend gewandelt hat, „die Organisation von Kommunikations- und Koordinationsprozessen durch Institutionalisierung von Wissen und Interessen, die Organisation von Wissensaggregierung (Monitoring) und die Ermöglichung von Risikotransparenz“[43] zu übernehmen.

IT-Sicherheit verbessert es vor allem den Schutz der Kritischen Infrastrukturen (KRITIS) und erhöht die Netzsicherheit in den Bereichen, deren Ausfall oder Beeinträchtigung *dramatische Folgen für Wirtschaft*, Staat und Gesellschaft in Deutschland hätte. Außerdem besteht eine Verpflichtung von KRITIS-Betreibern zur Meldung von erheblichen IT-Sicherheitsvorfällen an das BSI.“, https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html (abgerufen am 10.1.2020).

39 Statt vieler: *Korioth* in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, Art. 30 GG, Rn. 9 (Stand: 92. EL 2020).

40 Überblick etwa bei *Stoll*, Sicherheit als Aufgabe von Staat und Gesellschaft, Verfassungsordnung, Umwelt- und Technikrecht im Umgang mit Unsicherheit und Risiko, 2003, S. 8ff; *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, Verfassungsrechtliche Grundlagen und immissionsschutzrechtliche Ausformung, 1985.

41 Zum Begriff *Beck*, Risikogesellschaft. Auf dem Weg in eine andere Moderne, 1986.

42 *Grimm*, Der Wandel der Staatsaufgaben und die Krise des Rechtsstaates, in Grimm (Hrsg.), Wachsende Staatsaufgaben – sinkende Steuerungsfähigkeit des Rechts, 1990, S. 291, 300.

43 *Köck*, Risikovorsorge als Staatsaufgabe, Archiv des öffentlichen Rechts, 1996, S. 1, 22.

Als Zwischenergebnis ist festzuhalten, dass IT-Sicherheit zu einer Staatsaufgabe geworden ist. Jedoch lassen sich daraus keine konkreten verfassungsrechtlichen Maßstäbe für die angemessene Verteilung von Verantwortung zwischen Staat und Privaten entwickeln, vor allem nicht zu Detailfragen und zur Finanzierung.

Auch der Rechtsgedanke der Vorsorge kann, mangels einer ausdrücklichen Staatszielbestimmung zur IT-Sicherheit, allein keine verfassungsrechtliche Steuerungskraft entfalten.

Positiv-rechtlich ist das Vorsorgeprinzip im Grundgesetz etwa in Form der Staatszielbestimmung des Umweltschutzes in Art. 20a GG verankert. Grundsätzlich kann Art. 20a GG auch dazu dienen, den gesetzgeberischen Spielraum bei der Frage, ob dieser tätig werden muss, einzuschränken, wenn auch Spielräume größer sind als die Beschränkungen.[44] Jedoch sind Staatszielbestimmungen keine aus sich selbst heraus operationalisierbaren Normen. Sie wirken grundsätzlich erst durch und über die konkretisierende wie aktualisierende Gesetzgebung.[45]

Wenn man den Staat in der Rolle des Vorsorge-Staates sieht, kommt der Staat seinen verfassungsrechtlichen Pflichten bereits dann nach, wenn er seine Verantwortung prozesshaft wahrnimmt, ohne jedoch ein konkretes Ergebnis zu schulden.

III. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die Schutzpflichtendogmatik der Grundrechte könnte für ein Tätigwerden des Staates im Bereich der IT-Sicherheit in den Dienst genommen werden.[46] Grundrechte haben mehrere Dimensionen, in denen sie wirken. Sind in erster Linie Abwehrechte gegen staatliches Eingriffshandeln. Sie gelten gemäß Artikel 1 Abs. 3 GG primär im Verhältnis zwischen Bürger und Staat. Grundrechte können auch schützendes Verhalten angesichts von Verletzungen und Gefährdungen grundrechtlich geschützter Güter erfordern. *Isensee* griff bereits 1982 das Spannungsverhältnis zwischen Sicherheit und Freiheit auf und versuchte, es über die Grundrechte zu lösen.[47]

---

44 *Voßkuhle*, Umweltschutz und Grundgesetz, NVwZ 2013, S. 1, 5.

45 *Scholz*, Art. 20 a GG, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar (Stand: 92. EL, 2020) Rn. 47.

46 Generell zurückhaltend: *Di Fabio*, Art. 2 GG in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar (Stand: 92. EL, 2020) Rn. 61f.

47 Grundlegend: *Isensee*, Das Grundrecht auf Sicherheit, 1983.

Angesprochen sein kann dabei die Legislative, die Exekutive oder die Judikative. Zudem können Grundrechte Drittwirkung entfalten, also in das Verhältnis von Privaten untereinander einwirken.[48]

Die meisten Grundrechte der deutschen Verfassungsordnung, ob positiv-rechtlich in der Verfassung verankert oder als Ausfluss der Rechtsfortbildung durch das Bundesverfassungsgericht, haben Anwendungsbereiche im digitalen Raum. Bei der Ausübung von einem Großteil der Grundrechte ist ein sicherer digitaler Raum Voraussetzung. Selbstverständlich können Grundrechte auch nach wie vor analog genossen werden, jedoch steigt die verfassungsrechtliche Relevanz der Vorbedingung der IT-Sicherheit für die Ausübung von einer großen Zahl von Grundrechten.

1. Positiv-rechtliche Aussagen des Grundgesetzes zur IT-Sicherheit

Der textliche Befund des Grundgesetzes zeigt, dass einige Grundrechte, etwa Art. 5 GG (Meinungs- und Pressefreiheit), Art. 10 GG (Fernmeldegeheimnis)[49] und Art. 13 GG (Unverletzlichkeit der Wohnung), gewisse Aspekte der Grundrechtsausübung im digitalen Raum schützen.[50] Eine eindeutige Zuweisung im Hinblick auf die Wahrnehmung und Ausgestaltung von IT-Sicherheit durch den Staat oder private Unternehmen lässt sich indes daraus nicht entnehmen. Vielmehr steht diesen Grundrechten die ebenfalls grundrechtlich abgesicherte unternehmerische Freiheit gegenüber, Art. 12 und 14 GG.

2. Rechtsfortbildungen durch das Bundesverfassungsgericht hin zur IT-Sicherheit

Das Bundesverfassungsgericht entwickelt seit den 1970er Jahren das allgemeine Persönlichkeitsrecht aus Art. 1 und 2 Abs. 1 GG.[51] Vorausgegangen war dabei schon seit den 1950er Jahren die Rechtsprechung des BGH zum

48 Einführend siehe *Klein*, Grundrechtliche Schutzpflicht des Staates, NJW 1989, S. 1633.

49 BVerfG 100, 313; 106, 28, 110, 33; siehe auch *Hindelang*, Freiheit und Kommunikation. Zur verfassungsrechtlichen Sicherung kommunikativer Selbstbestimmung in einer vernetzten Gesellschaft, 2019.

50 Vgl. *Schliesky*, Digitalisierung – Herausforderung für den demokratischen Verfassungsstaat, Ein Beitrag zur Zukunftsfähigkeit des Grundgesetzes am Vorabend des 70. Geburtstags, NvWZ 2019, S. 693, 698.

51 BVerfG 35, 202.

allgemeinen Persönlichkeitsrecht.[52] In Fortschreibung dieser Rechtsprechung markiert die Errungenschaft des Grundrechts auf informationelle Selbstbestimmung im Volkszählungsurteil von 1983 einen wichtigen Meilenstein.[53]

Seit dem Jahr 2008 spricht das Bundesverfassungsgericht vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[54] Diese grundrechtlichen Entwicklungen betreffen vor allem den *status negativus*, also die Abwehr staatlicher Eingriffe. Das Bundesverfassungsgericht charakterisierte das neu „gefundene" Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als eine „lückenschließende Gewährleistung… um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann."[55] Das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme findet nach der Rechtsprechung des BVerfG im Verhältnis zur Telekommunikationsfreiheit des Art. 10 Abs. 1, zur Unverletzlichkeit der Wohnung des Art. 13 und zum Grundrecht auf informationelle Selbstbestimmung nur subsidiäre Anwendung.[56] In der Literatur wurde diese Neuentwicklung teilweise auch mangels einer Schutzlücke für überflüssig erachtet, die Rezeption war insgesamt eher kritisch.[57] Hier soll keine grundsätzliche Debatte darüber befeuert werden, ob es nicht wünschenswert wäre, die „digitalen" Individualrechte auch zu positiveren. Ihre Sichtbarkeit und Steuerungskraft würden jedoch davon profitieren. Dass eine Kodifikation möglich ist, zeigt etwa die europäische Grundrechtecharta, die entscheidende digitale Grundrechte enthält (z.B. Art. 8 GrC).

---

52 *Kipker*, Informationelle Freiheit und staatliche Sicherheit, 2016, S. 9, mit weiteren Nachweisen.

53 BVerfG 65, 1.

54 BVerfG 120, 274; *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009; *Bäcker*, Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in *Uerpmann-Wittzack* (Hrsg.), Das neue Computergrundrecht, 2009, S. 1; kritisch *Manssen*, Das „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme" – Ein gelungener Beitrag zur Findung unbenannter Freiheitsrechte? In *Uerpmann-Wittzack* (Hrsg.), Das neue Computergrundrecht, 2009, S. 61.

55 BVerfGE 120, 274, Rn. 169.

56 BVerfGE 120, 274, 302.

57 Siehe zum Meinungsstand: *Gersdorf*, Art. 2 GG, in Gersdorf/Paal (Hrsg.), BeckOK Informations- und Medienrecht (30. Ed, 2019), Rn. 23 mit weiteren Nachweisen.

3. Die Rolle des Staates über die Abwehrdimension hinaus?

Weniger klar ist, was die vom Bundesverfassungsgericht ausgegebene Dimension des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme über den *status negativus* des Grundrechts hinaus bedeutet. In der Literatur wurde eine über die abwehrrechtliche Dimension hinaus gehende Wirkmacht im unmittelbaren Nachgang zum Urteil bejaht.[58] In den etwa 12 Jahren, die seither vergangen sind, ist jedoch ein verfassungsrechtlicher Diskurs zur Rolle des Staates in diesem Themenfeld weitgehend ausgeblieben. *Poscher/Lassahan* stellen dies eher versteckt in einer Fußnote fest: „Im Zuge der immer weiteren Vernetzung wird sich in der Zukunft ein effektiver Schutz vor IT-bezogenen Beeinträchtigungen von Grundrechten womöglich nicht mehr allein durch sektorale oder auf den Schutzbereich nur einzelner Grundrechte beschränkter Maßnahmen verwirklichen lassen. Es erscheint denkbar, dass sich angesichts drohender Gefährdungen einer Vielzahl von Grundrechten durch Manipulation umfassend vernetzter, multifunktionaler Systeme im Ergebnis auch aus der Gesamtheit der potentiell betroffenen Grundrechte eine Schutzpflicht des Staates zu einem umfassenden IT-Sicherheits-Basisschutz ergibt."[59]

Freilich ist das Minimum an Schutz, den der Staat schuldet, vor dem Hintergrund des Untermaßverbotes[60] kaum zu konkretisieren. So erscheint es umso gewinnbringender, intra- und interdisziplinäre Argumente zu bündeln, um Handlungsspielräume und -pflichten des Staates genauer einzugrenzen.

---

58 *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009, 1019; *Roßnagel/Schnabel*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, S. 3534, 3535. A.A. in zeitlichem Abstand: *Gersdorf*, Art. 2 GG, in Gersdorf/Paal (Hrsg.), BeckOK Informations- und Medienrecht (30. Ed, 2019), Rn. 29.

59 *Poscher/Lassahn*, Verfassungsrechtliche Dimensionen der IT-Sicherheit in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020, S. 133, 147, dort in der Fußnote 69.

60 BVerfGE 88, 203, 254 f.

D. Der Mehrwert eines intra- und interdisziplinären Blicks auf verfassungsrechtliche Fragen der IT-Sicherheit

Die Datenethikkommission widmete sich dem Thema IT-Sicherheit nur kursorisch in dem Abschlussgutachten vom 23. Oktober 2019. Dort werden die Begriffe der „risikoadäquaten Informationssicherheit" sowie der „risikoadaptierten Regulierung" verwendet.[61] Diese offenen Begriffe spiegeln die multidisziplinäre Fragestellung wider, die die IT-Sicherheit mit sich bringt. Auf die Notwendigkeit eines gelingenden *inter*disziplinären Austausches mit IT-Sicherheitsingenieuren für die angemessene Bewertung von Risiken der IT-Sicherheit und der entsprechenden Verantwortlichkeiten sei hier nur in der gebotenen Kürze hingewiesen.[62] Technische Fragen determinieren auch, welche Rolle der Staat in Rechtsverhältnissen einnehmen kann, die zwischen Privaten bestehen – etwa zwischen einer privaten Bank und einem Kunden.

I. Interdisziplinäre Möglichkeiten: IT-Sicherheit als Public Good

Ökonomisch geleitete *inter*disziplinäre Betrachtungen sind für die Fragestellung der IT-Sicherheit sehr relevant. IT-Sicherheit wird bisweilen als öffentliches Gut (*public good*) charakterisiert.[63] Bei öffentlichen Gütern kann es dazu kommen, dass die Verteilung von Kosten nicht ausschließlich auf diejenigen erfolgen kann, die ein Gut nutzen. Die vielfältigen ökonomischen Erwägungen, von Investitionskosten über Anreizstrukturen bis hin zu den Risiken staatlicher Sanktionierung, sind eine Dimension, die in diesem Beitrag nicht weiterverfolgt werden kann. Die ökonomischen Hintergründe sind jedoch tauglicher Ansatzpunkt für eine kostenoptimale Verteilung von Verantwortung zwischen Staat und Unternehmen.[64] Für

61 Gutachten der Datenethikkommission, 23.10.2019, www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf?__blob=publicationFile&v=2 (abgerufen am 10.1.2020).

62 Generell dazu bereits *Forsthoff*, Der Jurist in der industriellen Gesellschaft, NJW 1960, S. 1273, 1275.

63 *Bertschek/Janßen/Ohnemus*, IT-Sicherheit aus ökonomischer Perspektive, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020 S. 63, 67; *Schliesky*, Digitalisierung – Herausforderung für den demokratischen Verfassungsstaat, Ein Beitrag zur Zukunftsfähigkeit des Grundgesetzes am Vorabend des 70. Geburtstags, NvWZ 2019, S. 693, 700.

64 Weiterführend *Taddeo*, Is Cybersecurity a Public Good?, Minds and Machines 2019, S. 349.

den vorliegenden Beitrag dient die Hypothese der IT-Sicherheit als öffentliches Gut jedenfalls als Rechtfertigungsmöglichkeit für staatliches Handeln und staatliche Verantwortung für den Bereich der IT-Sicherheit.[65] Für die Risikobewertung im Bereich der IT-Sicherheit ist das Verständnis von (neuen) Geschäftsmodellen von Unternehmen, aber auch von Kriminellen wichtig, um Kosten und Nutzen von IT-Sicherheit besser zu verstehen.[66] So werden nicht nur Kosten für die IT-Sicherheit in den Blick genommen, sondern auch die Kosten sichtbar, die entstehen, wenn ein Angriff auf ein IT-System Erfolg hat.

II. Ein intradisziplinärer Blick auf den verfassungsrechtlicher Konkretisierungsbedarf zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Für die Verantwortung des Staates im Rahmen der Gewährleistung von IT-Sicherheit lassen sich keine konkreten Schlüsse ziehen, welches Ergebnis, wenn überhaupt, der Staat schuldet.

Für den Teilbereich der Ausnutzung von IT-Schwachstellen für straf- und nachrichtendienstliche Maßnahmen haben u.a. *Derin/Golla* angemahnt, dass vor dem Hintergrund des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme die Beeinträchtigungen der IT-Sicherheit grundsätzlich nicht hinnehmbar seien, die entstehen, wenn der Staat Sicherheitslücken weitläufig offenhält und es unterlässt, diese zu melden und zu ihrer Schließung beizutragen.[67]

Auch für das Handeln der gefahrenabwehrenden Verwaltung vermag das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht Recht wahrgenommen zu werden. Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik, das beschrieben wird als „Methode, Anleitung, Empfehlung und Hilfe zur Selbsthilfe für Behörden, Unternehmen und Institutionen aller

65 Grundlegend, wenn auch nicht bezogen auf IT-Sicherheit: *Ostrom*, Governing the Commons: The Evolution of Institutions for Collective Action, 1990.

66 Z.B. *Acquisti/ Taylor/ Wagman*, The Economics of Privacy, Journal of Economic Literature 2016, S. 442; *Lusthaus*, Industry of Anonymity: Inside the Business of Cybercrime, 2018.

67 *Derin/Golla*, Der Staat als Manipulant und Saboteur der IT-Sicherheit? Die Zulässigkeit von Begleitmaßnahmen zu „Online-Durchsuchung" und Quellen-TKÜ, NJW 2019, S. 1111, 1115; siehe auch generell *Snowden*, Permanent Record, 2019.

Größen“[68] ist ein Instrument des soft law. In dem 810-seitigen Werk, das jährlich aktualisiert wird, wird das Grundgesetz nur ein einziges Mal erwähnt, dies geschieht im Zusammenhang mit dem Datenschutz.[69] Ein Rekurs auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfolgt nicht.

Der unbestimmte Rechtsbegriff der Angemessenheit, der etwa in § 8a des BSI-Gesetzes verwendet wird, und in dem gewissen Unternehmen ein Mindestniveau an IT-Sicherheit vorgeschrieben wird, bleibt grobkörnig.[70] Im Kontrast hierzu meint *Bull* für den verwandten Bereich des Datenschutzes Fehlentwicklungen zu beobachten, die mit der zu engmaschigen Durchnormierung aller Formen des Umgangs mit personenbezogenen Daten einher gingen. Er verallgemeinert seine Kritik dahingehend, dass die Wertordnung, die in unserer Verfassung angelegt sei, die Abwehr von unerwünschtem Verhalten grundsätzlich nicht als alleinige Aufgabe des Staates anlege.[71]

Verfassungsrechtliche Wertungen wirken auf vielfache Weise in das Privatrecht und auf das Handeln Privater auch untereinander ein.[72] Der erste Zugriff auf die konkrete Ausgestaltung von IT-Sicherheit liegt in privater Hand. Vor diesem Hintergrund scheint eine *intra*disziplinäre Sichtweise, wie in diesem Tagungsband, auf die Frage der Verantwortungsverteilung besonders lohnend. Für das Zivilrecht, in dem verfassungsrechtliche Wertungen über Generalklauseln wie §§ 133, 134, 157, 242 BGB, das Recht der AGB und anderen generalklauselartigen Auffangnormen (z.B. § 280, § 823 BGB) Wirkung entfalten, bietet der Gehalt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Syste-

68 *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutz- Kompendium, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf?__blob=publicationFile&v=6 (abgerufen am 10.1.2020).

69 *Bundesamt für Sicherheit in der Informationstechnik*, IT-Grundschutz- Kompendium, Abschnitt CON 2 (Fn 68).

70 *Buchberger*, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, Rn. 3.

71 *Bull*, Fehlentwicklungen im Datenschutz am Beispiel der Videoüberwachung, JZ 2017, S. 797, 802.

72 Ausführlich bei *Ruffert*, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, Eine verfassungsrechtliche Untersuchung zur Privatrechtswirkung des Grundgesetzes, 2001.

me noch wenig konkrete Orientierung.[73] Der Ausgleich zwischen verschiedenen nicht nur privaten Interessen und Verantwortungsbereichen scheint somit weitgehend in Richterhand zu liegen. In der Literatur wird versucht, zur Bestimmung von IT-Sicherheitsanforderungen auf spezialgesetzliche Regelungen und technische Normen zurückzugreifen.[74]

E. Fazit: von der Nützlichkeit eines verfassungsrechtlichen Kompasses für Fragen der IT-Sicherheit

Das Grundgesetz ist zukunftsgerichtet. Dies findet unter anderem in der Ewigkeitsklausel Ausdruck. Das Verfassungsrecht hat eine wichtige Orientierungsfunktion inne: technologische Entwicklungen sollen grundrechts- und gemeinwohlverträglich gestaltet werden.

Wolfgang Hoffmann-Riem fasste die Ausgangsposition für den verwandten Bereich der Regulierung von „Big Data" folgendermaßen zusammen:

> *„Ob und wie Chancen der Digitalisierung genutzt und Risiken minimiert werden, ist gestaltbar. Gestaltende Akteure sind wirtschaftliche Unternehmen, die vielen Nutzer, individuelle Innovatoren, interessenwahrnehmende Verbände, aber auch Hacker. Für die Schaffung eines Rahmens zur Sicherung von Individual- und Gemeinwohl aber ist der Staat zuständig. Dabei kann er neben anderem das Steuerungsmedium Recht einsetzen."*[75]

Der Ausgleich von staatlichen und privaten Interessen einerseits, und der Ausgleich zwischen Privaten andererseits, sollte auf die Verfassung rückführbar sein. Dabei muss auch sichergestellt werden, dass die Errungenschaften aus der analogen Zeit angemessen in neue Kontexte übersetzt werden. Verfassungsrechtlich klare Maßstäbe und dogmatische Durchdringung von Fragen der IT-Sicherheit sind dabei kein Selbstzweck. Sie sind auch für Unternehmen ein Gewinn an Rechtssicherheit[76]; sie können auch

---

73 *Wehage*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und seine Auswirkungen auf das Bürgerliche Recht, 2013, S. 155ff.

74 *Pour Rafsendjani/Bomhard*, IT-Sicherheit im Zivilrecht und in der Vertragsgestaltung, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, Praxishandbuch, 2020 S. 181, 190ff.

75 *Hoffmann-Riem*, Big Data – Regulative Herausforderungen, 2018, Vorwort, S. 5.

76 *Roßnagel/Hornung*, Handlungsbedarf für einen Grundrechteausgleich, in: *Roßnagel/ Hornung*, (Hrsg.) Grundrechtsschutz im Smart Car, Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug, 2019, S. 470, 472.

ein Standortvorteil sein. Ein hoher Abstraktionsgrad, den das Verfassungsrecht erlaubt, ist dabei auch nicht in Verdacht, Hemmschuh für Innovationen durch Überregulierung zu sein.

Grundsätzlich fraglich ist, ob die IT-Sicherheit ähnlich kleinteilig zu fassen ist wie bisherige Herausforderungen, wie etwa ausgehend von Atomkraft oder gefährlichen Industrieanlagen. Der Facettenreichtum der Querschnittsmaterie der IT-Sicherheit stellt gegenüber dem klassischen Recht „Recht des Risikomanagements", wie etwa dem des Rechts des Immissionsschutzes, womöglich nicht nur einen graduellen, sondern einen grundsätzlichen Unterschied dar. Dieser Unterschied drückt sich darin aus, dass die Gefahren für die Sicherheit von IT-Systemen bisweilen nicht abgrenzbar und damit für einen allein Pflichtigen beherrschbar sind. Er erfordert aus regulatorischer Sicht einen umfassenden Ansatz. Fragen der IT-Sicherheit betreffen die Hardware, Software und die Personen, die die Technik bedienen und benutzen. Umso mehr scheint eine abstrakte verfassungsrechtliche und zusammenführende Festlegung sinnvoll.

Sollte das deutsche Verfassungsrecht weiter nur zögerlich entwickelt und wissenschaftlich begleitet werden, wird eine noch weitergehende „Hochzonung" auf das (sekundäre) Recht der Europäischen Union erfolgen, wie es beim Recht des Datenschutzes der Fall war. Diese Verlagerung in ein Mehrebenensystem ist durchaus auch vorteilhaft, und im Integrationsprogramm des Grundgesetzes selbst so angelegt. Die Verlagerung in eine Verordnung, wie etwa der Datenschutzgrundverordnung, erschwert jedoch auch die Nachjustierung und die Veränderung von darin enthaltenen Grundentscheidungen. Die Mühe, sich im deutschen Verfassungsrecht vertieft mit der Materie auseinanderzusetzen, lohnt indes. Auch in anderen Teilbereichen haben sich Argumente und Problemlösungen, die im Rahmen einer nationalen Grundrechtsordnung erarbeitet wurden und sich dort als praktikabel erweisen haben, Einfluss auf unionsrechtliche Entwicklungen gezeitigt.[77]

77 *Bäcker* spricht von „grundrechtlichen Exportartikeln" und einem möglichen „Beitrag zum europäischen Rechtsgespräch", Grundrechtlicher Informationsschutz gegen Private, Der Staat 2012, S. 91, 115.