2. Kapitel
Rechtsgrundlagen der Cybersicherheit im Gesundheitswesen

Übersicht

	Rn
A. Einführung	1
B. Verfassungsrecht und Grundrechte (Überblick)	4
C. Europarecht	9
I. EU-Grundrechte-Charta	10
II. NIS-Richtlinie	12
III. NIS-2-Richtlinie	14
IV. Resilienz-Richtlinie	20
V. DSGVO	22
1. Grundsätze und Anforderungen	23
2. Technische und organisatorische Maßnahmen	26
3. Meldungen von Datenschutzverletzungen	31
VI. Europäischer Gesundheitsdatenraum und weitere Vorhaben	32
D. Nationales Recht	34
I. BSIG mit BSI-KritisV	37
II. BSIG-E aufgrund NIS2UmsuCG	40
III. KRITIS-DachG-E	50
IV. SGB V	54
1. Cybersicherheit nach den Richtlinien gemäß § 390 SGB V	56
2. Cybersicherheit nach § 391 SGB V	57
3. Cybersicherheit in der Telematikinfrastruktur	58
V. Cybersicherheit und Berufsgeheimnisschutz	59
E. Fazit und Ausblick	62

Literatur: *Dittrich* Sanktionskompetenz des BSI im Kampf für mehr Cybersicherheit – Eine kritische Untersuchung der „Bußgeldpraxis" nach dem BSIG, MMR 2022, 267; *Dittrich/Dochow* Cybersicherheitsrecht in der Telematikinfrastruktur mit Blick auf Arztpraxen, GesR 2022, 414; *Dittrich/Dochow/Ippach* Auswirkungen der neuen EU-Cybersicherheitsstrategie auf das Gesundheitswesen – der Entwurf der NIS-2-Richtlinie und der „Resilienz"-Richtlinie, GesR 2021, 613; *Dittrich/Heinelt* Der Europäische DORA – neue Sicherheitsvorgaben für den Finanzsektor, RDi 2023, 164; *Dittrich/Ippach* IT-Sicherheit betrifft nicht nur Großkrankenhäuser – die Regulierung der IT-Sicherheit im ambulanten und stationären Bereich, GesR 2021, 285; *Dochow* Cybersicherheitsrecht im Gesundheitswesen, MedR 2022, 100; *Duttge/Er/Fischer* Vertrauen durch Recht?, Steinfath/Wiesemann (Hrsg.), Autonomie und Vertrauen, 2016; *Eisenmenger* Ein neuer Rechtsrahmen für Kritische Infrastrukturen (KRITIS) – unter Berücksichtigung der EU-Resilienz-Richtlinie, NVwZ 2023, 1203; *Engelbrecht* Meldepflicht gegenüber der Rechts- oder Fachaufsichtsbehörde bei einer Verletzung des Schutzes von Sozialdaten, NZS 2019, 693; *Federmann/Müller/Friedrichsen/Schaich* Rechtliche Vorgaben zur Etablierung eines Business-Continuity-Managements, CB 2021, 55; *Fuhlrott* Data Incident Management: Rechtlicher Umgang mit „Datenpannen", NZA 2019, 649; *Grzesiek* Neue Anforderungen an die IT-Sicherheit in der Arztpraxis, GuP 2021, 171; *Hennemann/Steinrötter* Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, NJW 2022, 1481; *Hornung* Das IT-Sicherheitsgesetz 2.0: Kompetenzaufwuchs des BSI und neue Pflichten für Unternehmen, NJW 2021, 1985; *Kipker/Birreck/Niewöhner/Schnorr* NIS-Richtlinie und der Entwurf der NIS-2-Richtlinie – Überblick, Gemeinsamkeiten und Unterschiede, MMR 2021, 214; *Kipker/Dittrich* Rolle der Kritischen Infrastrukturen nach dem neuen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz MMR 2023, 481; *Kipker/Dittrich* Die Geschäftsleitung im Fokus des IT-Sicherheitsrechts: Teil 1, CB 2023, 483; *Kipker/Dittrich* Die Geschäftsleitung im Fokus des IT-Sicherheitsrechts – Teil 2, CB 1-2/2024, 18; *Kipker/Scholz* Das IT-Sicherheitsgesetz 2.0 – Eine kritische Analyse, MMR 2019, 431; *Kutscha* Mehr Schutz von Computerdaten durch ein neues

Grundrecht?, NJW 2008, 1042; *Nadeborn/Dittrich* Cybersicherheit in Krankenhäusern – Teil 2: vom Normalfall zum Notfall, ICLR 2/2022, 273; *Nardone* Referentenentwurf des BMI zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, ITRB 2023, 182; *Risini* IT-Sicherheit: ein verfassungsrechtlicher Zugang, Bittner/Guntermann/Müller/Rostam (Hrsg.), Cybersecurity als Unternehmensleitungsaufgabe, 2021, 107; *Schmidt* Neue europäische Anforderungen im Cybersicherheitsrecht – die NIS2-Richtlinie im Überblick, K&R 2023, 705; *Voigt/Schmalenberger* Die Gesetzesentwürfe zur Umsetzung von NIS2 und CER im Überblick, CR 2023, 717; *Wybitul* Vermeidung von DS-GVO-Risiken nach Datenpannen und Cyberangriffen, NJW 2020, 2577; *Ziegler* Anforderungen an die Cybersicherheit bei der Erbringung von IT-Dienstleistungen für Arztpraxen sowie Krankenhäuser und Möglichkeiten der Vertragsgestaltung, ICLR 1/2023, 61.

A. Einführung

1 **Cybersicherheitsrecht**[1] im Gesundheitswesen ist nicht einheitlich kodifiziert, sondern eine Zusammenschau von – zum Teil sehr entlegen und nur untergesetzlich gefassten[2] – Regelungen aus verschiedenen Rechtsbereichen. Es ist damit – wie das Datenschutzrecht – eine Querschnittsmaterie, die stark fragmentiert und kleinteilig reguliert ist.[3] Der Grund hierfür ist eine Lokalisierung der Rechtsgrundlagen in dem Mehrebenensystem von nationalem und europäischem Recht, die föderale Struktur in der Bundesrepublik Deutschland und ein sektoral zergliedertes und zum Teil von einer Selbstverwaltung geprägtes Recht im Gesundheitswesen. Gefahren für die IT- und Cybersicherheit enden aber nicht an Sektoren- oder Zuständigkeitsgrenzen und adressieren damit nicht allein den Verantwortlichen. Daher ist eine Regulierung zur Sicherstellung von Cybersicherheit im Gemeinwohlinteresse ebenso wie eine Systematisierung erforderlich.

2 Aufgrund der geringen Konkretisierungsdichte im Verfassungsrecht[4] geben die Grundrechtsordnungen wenig greifbare Orientierung für das Cybersicherheitsrecht. Kennzeichnend für das Cybersicherheitsrecht im Gesundheitswesen ist daher der Versuch neben einer Regulierung in Spezialgesetzen (z.B. BSIG oder §§ 75b, 75c SGB V a.F. = §§ 390, 391 SGB V n.F.)[5] und untergesetzlichen Vorschriften (z.B. in Anlagen zum BMV-Ä)[6] sich durch einen Verweis auf technische Normen (ISO 27000-Reihe) und Empfehlungen (IT-Grundschutz des BSI) zu behelfen. Dieser Verweis erfolgt über **unbestimmte Rechtsbegriffe**[7] wie den „***Stand der Technik***“[8] als zentralem normativen Anker zur Technik. Zugleich kann damit auf die **Dynamik** der techni-

1 Zum Begriff s. 3. Kap. Rz. 4; s.a. Kipker/*Kipker* Cybersecurity, 1. Kap. Rz. 4.

2 Vgl. z.B. Anlagen 31, 31a, 31b BMV-Ä.

3 Vgl. allg. zum Cybersicherheitsrecht etwa auch Hornung/Schallbruch/*Hornung/Schallbruch* IT-Sicherheitsrecht, Einf. Rz. 9, 33 und mit Krit. an mangelnder Systematisierung Rz. 40; Kipker/*Schrooten* Cybersecurity, 2. Kap. Rz. 6; *Risini* IT-Sicherheit, 109; anschaulich zur kleinteiligen Regulierung auf untergesetzlicher Ebene durch die Selbstverwaltung für den Bereich der Telemedizin s. 13. Kap.

4 Vgl. allein § 93c GG, dem jedoch für das Cybersicherheitsrecht eher geringe Bedeutung zugemessen wird, Kipker/*Schrooten* Cybersecurity, 2. Kap. Rz. 19.

5 S. 9. Kap.

6 S. 13. Kap.

7 Kipker/*Schrooten* Cybersecurity, 2. Kap. Rz. 23 weist in diesem Zusammenhang auf die Rechtsprechung des BVerfG zum Bestimmtheitsgebot hin.

8 3. Kap. Rz. 23; s. Kipker/*Ekrot/Fischer* Cybersecurity, 4. Kap. Rz. 1 ff. auch zu den Begriffen „*Allgemein anerkannte Regeln der Technik*“ und „*Stand von Wissenschaft und Forschung*“.

schen Entwicklungen im Zuge der Digitalisierung und die Defizite der Gesetzgebung im Hinblick auf die Flexibilität geantwortet werden, denn nur mit zeitlichen Verzögerungen gesetztes Recht steht im Spannungsverhältnis zur hohen Dynamik der Entwicklungen und Bedrohungslagen. Letztlich findet die Umsetzung der im Allgemeinen vorfindlichen rechtlichen Anforderungen in Orientierung an technische Normen und Empfehlungen statt. Das Cybersicherheitsrecht ist damit auch eine stark **soft law**-geprägte Materie. Die Konkretisierungshilfen können zur Rechtssicherheit für Unternehmen beitragen, die überwiegend für die Gestaltung des digitalen Raums im Gesundheitswesen verantwortlich sind. Die Gewährleistung von struktureller Daten- und IT-Sicherheit ist für alle Beteiligten existenziell, weil ohne diese Sicherheit ein Vertrauen in die Nutzung von Daten und in digitalisierte Prozesse nicht entstehen kann.[9] Weil Vertrauen in das Gesundheitssystem und bei der Gesundheitsversorgung traditionell ein besonderes Gewicht zukommt, hat Cybersicherheit in einem digital-vernetzten Gesundheitswesen zunehmende Bedeutung.[10]

Zentral sind hierbei auch die sog. **Schutzziele** (näher s. 3. Kap. Rz. 7 ff.)[11] zur Gewährleistung von IT- und Cybersicherheit, die in verschiedenen Normtexten regelmäßig Erwähnung finden (z.B. Vertraulichkeit, Integrität, Verfügbarkeit).[12] Ein besonderes Schutzziel der Cybersicherheit im Gesundheitswesen ist die Bewahrung von **Vertraulichkeit** vor einer unbefugten Offenlegung oder einem unbefugten Zugang zu Patientengeheimnissen.[13] Hintergrund dafür ist das Verhältnis zwischen Patient und Arzt, in welchem Vertrauen zu den „*Grundvoraussetzungen ärztlichen Wirkens [zählt], weil es die Chancen der Heilung vergrößert und damit – im Ganzen gesehen – der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge dient*".[14] Ebenfalls von besonderer Bedeutung ist das Schutzziel der **Verfügbarkeit**, denn es weist auf die individuelle, wirtschaftliche und gesellschaftliche Abhängigkeit von funktionsfähigen IT-Systemen hin. **3**

B. Verfassungsrecht und Grundrechte (Überblick)

Eine verfassungsrechtliche Annäherung an die Cybersicherheit verdeutlicht, dass die Cybersicherheit aus vielen Perspektiven betrachtet werden kann und muss: Neben der Kompetenzordnung[15] und den allgemeinen Verfassungsprinzipien[16] des Grundgesetzes bilden vor allem die Grundrechte mit ihrer Abwehr- und Schutzfunktion[17] sowie der mittelbaren Drittwirkung[18] einen wichtigen Rahmen für das Cybersicherheitsrecht. Eine in der Praxis bedeutsame Ver- **4**

9 Datenstrategie der Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, 27.1.2021, 25, abrufbar unter: https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632.

10 *Dochow* MedR 2022, 100, 102.

11 Kipker/*Sohr/Kemmerich* Cybersecurity, 3. Kap. Rz. 6 ff.; Hornung/Schallbruch/*Jandt* IT-Sicherheitsrecht, 17. Kap. Rz. 36 ff.

12 Z.B. Art. 32 Abs. 1 lit. b DSGVO; § 2 Abs. 2 S. 4 BSIG; § 22 Abs. 2 S. 2 Nr. 8 BDSG, § 390 Abs. 2 SGB V und § 391 Abs. 1 SGB V.

13 S. Rz. 25, 59.

14 BVerfGE 32, 373, 380; zum Vertrauen durch Recht s. näher *Duttge/Er/Fischer* Vertrauen durch Recht?, 239 ff.

15 Dazu Kipker/*Schrooten* Cybersecurity, 2. Kap. Rz. 5 ff.; Hornung/Schallbruch/*Poscher/Lassahn* IT-Sicherheitsrecht, 7. Kap. Rz. 50 ff.

16 Kipker/*Schrooten* Cybersecurity, 2. Kap. Rz. 21 ff.

17 Zu Schutzpflichten s. allg. Leibholz/Rinck/*Burghart* Vorbem. Art. 1–19 Rz. 50; im Kontext der IT-Sicherheit s. Hornung/Schallbruch/*Poscher/Lassahn* IT-Sicherheitsrecht, 7. Kap. Rz. 41 ff.

18 St. Rspr. s. BVerfGE 7, 198, 205 f.; BVerfGE 148, 267, 280 ff.; bestätigt für das Recht auf informationelle Selbstbestimmung in *BVerfG* MedR 351, 352; s.a. *Dochow* Grundlagen, 495 ff.

knüpfung besteht vor allem zum Datenschutzrecht, das Ausprägung des Rechts auf informationelle Selbstbestimmung bzw. von Art. 8 GRCh ist (s. Rz. 5 f., 10). Aus dem Blickwinkel des Gesundheitswesens kommt aber ein elementarer Gesichtspunkt hinzu: Es müssen neben den Persönlichkeitsinteressen zusätzlich die Funktionsfähigkeit der Gesundheitsversorgung und vitale Interessen, wie das Leben und die körperliche Unversehrtheit (s. Rz. 7), geschützt werden. Die fortschreitende Digitalisierung und zunehmende Abhängigkeit von funktionsfähigen und vernetzten Systemen für die Informationsverarbeitung und Kommunikation bedingen, dass die Aufrechterhaltung der Infrastrukturen für die Gesundheitsversorgungssicherheit ein fundamentales Ziel auch der Cybersicherheit geworden ist, das über Persönlichkeitsrechte der Patienten hinaus zudem die (geschäftlichen) Interessen der Institutionen des Gesundheitswesens tangiert und damit weitere Grundrechte berührt (s. Rz. 8). Cybersicherheit ist damit eine wichtige Vorbedingung für die Ausübung von Grundrechten und Grundbedingung für einen Großteil der wirtschaftlichen Wertschöpfung, wobei die Gewährleistung von Sicherheit zugleich traditionell eine staatliche Aufgabe ist.[19] Für die Schaffung der Rahmenbedingungen zur Sicherung von Individual- und Gemeinwohl kann der Staat im Rahmen der grundgesetzlichen Kompetenzordnung auf das Steuerungsinstrument des Rechts zurückgreifen.[20] Das Grundgesetz bietet hierfür einen abstrakten, aber zukunfts- und grundsätzlich technologieoffenen Rahmen,[21] sodass vor allem die Auslegung der Grundrechte im Lichte der Rechtsprechung des Bundesverfassungsgerichts – ggf. unter Berücksichtigung der Schutzpflichtdimension – einen wichtigen verfassungsrechtlichen Absprungpunkt für die Gewährleistung von Cybersicherheit für den digitalen Raum der Gesundheitsversorgung bieten kann.

5 Das **Recht auf informationelle Selbstbestimmung** stellt eine besondere Ausformung des Allgemeinen Persönlichkeitsrechts dar, das auf Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 gestützt wird.[22] Mit dem Aspekt der Informations- und Datensicherheit spielt das Recht auf informationelle Selbstbestimmung für die Cybersicherheit eine große Rolle.[23] In seinem Volkszählungs-Urteil aus dem Jahr 1983 entschied das BVerfG, dass die „*freie Entfaltung der Persönlichkeit (…) unter den modernen Bedingungen der Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus[setzt].*“[24] Das Recht auf informationelle Selbstbestimmtheit gewährleiste „*insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*“.[25] Im Kontext der Cybersicherheit ist bedeutsam, dass das Grundrecht den Einzelnen vor Kontrollverlusten über die eigenen Daten schützt, denn „*wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, […], kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.*“ Insoweit soll insbesondere die betroffene Person wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.[26] Insbesondere aufgrund der sensiblen Verarbeitungskontexte, in den personenbezogene Daten im Gesundheitswesen regelmäßig verarbeitet werden, ist ein besonderes Schutzniveau geboten.

19 Vgl. für den Schutz der IT-Sicherheit *Risini* IT-Sicherheit, 107, 115 ff.; vgl. Hornung/Schallbruch/*Poscher/Lassahn* IT-Sicherheitsrecht, 7. Kap. Rz. 48 f.; Hornung/Schallbruch/*Hornung/Schallbruch* IT-Sicherheitsrecht, Einf. Rz. 7 unter Hinw. auf BVerfGE 49, 24, 56 f.

20 Vgl. *Hoffmann-Riem* Big Data – Regulative Herausforderungen, 5.

21 Vgl. *Risini* IT-Sicherheit, 124.

22 Leibholz/Rinck/*Burghart* Art. 2 Rz. 104 m.w.N.

23 Ausführlich *Freimuth* 129 ff.

24 BVerfGE 65, 1, 43.

25 BVerfGE 65, 1, 43; näher *Dochow* Grundlagen, 456 ff.

26 BVerfGE 65, 1, 43.

Als besonderen Aspekt des allgemeinen Persönlichkeitsrechts hat das BVerfG im Jahr 2008 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme anerkannt.[27] Dieses wird auch als **Computergrundrecht**[28] oder **IT-Grundrecht**[29] bezeichnet und schützt den Nutzer eines IT-Systems im Hinblick darauf, dass seine Daten vertraulich bleiben und auf das von ihm genutzte IT-System nicht unzulässig, durch „*Ausspähung, Überwachung oder Manipulation des Systems*", zugegriffen wird.[30] Es soll dort seinen Anwendungsbereich haben, wo der Schutz nicht durch andere Grundrechte, insbesondere Art. 10, 13 GG oder das Recht auf informationelle Selbstbestimmung, gewährleistet ist.[31] Dadurch soll eine Schutzlücke geschlossen werden, „*um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann*".[32] Die **Schutzpflichtdimension** der Grundrechtsausprägung wird in der Literatur zum Teil anerkannt.[33] **6**

Bislang standen im Gesundheitswesen in Deutschland noch keine Patientenschäden in direktem Zusammenhang mit Cybervorfällen.[34] Dennoch nehmen bereits einige Rechtsvorschriften die Patientensicherheit in den Blick und stellen Anforderungen an Schutzmaßnahmen der Cybersicherheit.[35] Dadurch versucht der Gesetzgeber, seinen staatlichen **Schutzpflichten** zugunsten des **Lebens** und der **körperlichen Unversehrtheit** nach Art. 2 Abs. 2 S. 1 GG, insbesondere auch vor den rechtswidrigen Eingriffen Dritter (hier: durch Cyberangriffe), nachzukommen.[36] Der **Schutzpflichtdimension der Grundrechte** kommt im Cybersicherheitsrecht im Gesundheitswesen also gewissermaßen in mehrfacher Hinsicht Relevanz zu. **7**

Daneben sind weitere Grundrechte einschlägig wie insbesondere das Fernmelde- bzw. „*Telekommunikationsgeheimnis*" (Art. 10 GG), das vor allem die Übertragung von Informationen schützt, oder das Eigentumsrecht (Art. 14 GG) und die Berufsfreiheit (Art. 12 Abs. 1 GG).[37] Der verfassungsrechtliche Schutz ist dabei nicht allein mit Blick auf die Versicherten- oder Patienteninteressen von Bedeutung. Schutzbedürftig sind ferner IT-Systeme und Daten **juristischer Personen**. Bei den von den Leistungserbringern sowie anderen Akteuren und Institutionen des Gesundheitswesens[38] verarbeiteten Daten handelt es sich regelmäßig um **Geschäftsgeheimnisse**, die von Art. 12 GG geschützt werden.[39] Der **Eigentumsschutz** aus Art. 14 GG bietet für den Bereich der Cybersicherheit bislang noch zu wenig Schutz und Klarheit. Die intensiven juristischen Debatten über ein grundrechtlich geschütztes Dateneigentum bzw. einen Datenbesitz dauern weiter an.[40] Die über Art. 12 GG und 14 GG grundrechtlich abgesicherte unter- **8**

27 BVerfGE 120, 274, 303; s. m.N.w. *Dochow* Grundlagen, 537 ff.
28 *Kutscha* NJW 2008, 1042, 1044.
29 Krit. BeckOK Informations- und Medienrecht/*Gersdorf* Art. 2 GG Rz. 22.
30 BVerfGE 120, 274, 314.
31 BVerfGE 120, 274, 303; krit. BeckOK Informations- und Medienrecht/*Gersdorf* Art. 2 GG Rz. 23 m.w.N.
32 BVerfGE 120, 274, 303.
33 *Hoffmann-Riem* JZ 2008, 1009, 1019 f.; *Gusy* DuD 2009, 33, 37 f.; *Roßnagel/Schnabel* NJW 2008, 3534, 3535; **a.A.** BeckOK Informations- und Medienrecht/*Gersdorf* Art. 2 GG Rz. 29.
34 S. 1. Kap. Rz. 13.
35 S. 2. Kap. Rz. 37.
36 Zur Schutzpflicht vor lebensbedrohlichen terroristischen Erpressungen: *BVerfG* NJW 1977, 2255; die Schutzpflicht beim Schwangerschaftsabbruch: *BVerfG* NJW 1975, 573, 575; jüngst zur Schutzpflicht vor den Gefahren des Klimawandels: *BVerfG* NJW 2021, 1723.
37 Näher Kipker/*Schrooten* Cybersecurity, 2. Kap. Rz. 40 ff.
38 Z.B. Krankenversicherungen, Forschungseinrichtungen, Selbstverwaltung.
39 *BVerfG* NJW 2007, 2464, 2471; Jarass/Pieroth/*Jarass* Art. 2 Rz. 43.
40 *Michl* NJW 2019, 2729 ff.; MüKo-BGB/*Wagner* § 823 Rz. 332 ff.

nehmerische Freiheit begrenzt auf der anderen Seite eine Regulierung zugunsten der Cybersicherheit, die Ausdruck der Risikovorsorge oder der Sicherheitsverantwortung als Staatsaufgabe oder der Schutzpflichtdimension der Grundrechte sein kann.

C. Europarecht

9 Deutlich konkreter und umfangreicher für das Cybersicherheitsrecht sind die Regelungen auf europäischer Ebene, die entweder den nationalen Rechtsrahmen bestimmen oder unmittelbar in den Mitgliedstaaten anwendbar sind. Die Grundlagen lassen sich dem Primärrecht mit der EU-Grundrechte-Charta (s. Rz. 10 f.) entnehmen und Spezifizierungen ergeben sich im Sekundärrecht – vor allem aus der NIS-Richtlinie (s. Rz. 12 ff.), die jüngst neugefasst worden ist und mit der NIS-2-Richtlinie (s. Rz. 14 ff.) die Mitgliedstaaten dazu veranlasst ihre Regelungen im Cybersicherheitsrecht zu überarbeiten. Mit der DSGVO (s. Rz. 22 ff.) besteht demgegenüber ein allgemeinerer Rahmen, dem eine gewisse Auffangfunktion zukommt, soweit es um die Verarbeitung von personenbezogenen Daten geht. Perspektivisch relevant können auch Regelungen zum Europäischen Gesundheitsdatenraum (s. Rz. 32) werden.

I. EU-Grundrechte-Charta

10 Der Schutz von Daten vor IT-Sicherheitsrisiken fällt auch in den Schutzbereich von **Art. 7, Art. 8 GRCh**,[41] weshalb die Vertraulichkeit und Unversehrtheit von Kommunikation auch durch technische Maßnahmen gewahrt sein muss.[42] In der europäischen Grundrechteordnung sieht Art. 8 GRCh explizit den „*Schutz personenbezogener Daten*" vor. Entsprechendes regelt Art. 16 Abs. 1 AEUV.[43] Zudem enthält Art. 16 Abs. 2 AEUV die Grundlage für den Erlass von sekundärrechtlichen Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Wie im Datenschutzrecht ist auf der Grundlage der digitalen Grundrechte und der Kompetenztitel eine Überformung des nationalen Rechts auch im Cybersicherheitsrecht vorstellbar. Bislang hat die EU indes mit Richtlinien i.S.v. Art. 288 UAbs. 3 AEUV lediglich einen Regulierungsrahmen vorgegeben (s. Rz. 12 ff.) und bis auf den Digital Operational Resilience Act (DORA)[44] für den Finanzsektor nicht das weitergehende Instrument der Verordnung gemäß Art. 288 UAbs. 2 AEUV gewählt. Mit dem Europäischen Gesundheitsdatenraum (s. Rz. 32) können sich die Maßstäbe nun auch im Gesundheitssektor ändern.

11 Weiterhin folgt aus Art. 3 Abs. 1 GRCh („*Recht auf Unversehrtheit*") eine Pflicht für die EU und ihre Mitgliedstaaten, sich schützend vor die Unversehrtheit ihrer Bürgerinnen und Bürgern bei Eingriffen durch Privatpersonen zu stellen.[45]

41 Charta der Grundrechte der Europäischen Union (GRCh), ABl. EU 2012, C 326, 391.

42 *EuGH* NJW 2014, 2169, 2173; NJW 2021, 531, 543; Taeger/Pohle/*Deusch/Eggendorfer* 50.1 Rz. 262; zum Datenschutz der GRCh bei juristischen Personen: BeckOK DatenSR/*Schneider* Syst. B Rz. 33 ff.

43 Vertrag über die Arbeitsweise der Europäischen Union (AEUV), ABl. EG 2008, C 115, 47.

44 VO (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14.12.2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABl. EU 2022, L 333, 1; vgl. hierzu u.a. *Dittrich/Heinelt* RDi 2023, 164.

45 Bergmann/Dienelt/*Bergmann* Art. 3 GRCh Rz. 1 m.w.N.