Der Einsatz von Angriffserkennungssystemen im Gesundheitswesen

Eine Betrachtung am Beispiel des Krankenhauses in privater Trägerschaft

Von der Philosophischen Fakultät der Gottfried Wilhelm Leibniz Universität Hannover zur Erlangung des Grades einer Doktorin der Philosophie (Dr. phil.) genehmigte Dissertation von

Sina Marie Köhler

2024

Referent: Prof. Dr. Nils Hoppe

Korreferent: Prof. Dr. Fabian Schmieder

Tag der Promotion: 16.09.2022

Inhaltsverzeichnis

Abbildungsverzeichnis

I. Einleitung

„*Die Welt wartet nicht auf uns*“ äußerte der ehemalige Bundesgesundheitsminister Jens Spahn im Jahr 2019 in Bezug auf den Stand der Digitalisierung im deutschen Gesundheitswesen. Es sei notwendig, endlich eine Vorreiterposition in der Digitalisierung einzunehmen, um den Patienten und Patientinnen weiterhin eines der besten Gesundheitssysteme der Welt zur Verfügung stellen zu können.[1] Denn die umfassende Digitalisierung im Gesundheitsbereich verheißt Großes: Softwarebasierte Analyseinstrumente sowie umfassende Auswertungen von hochwertigen Datensätzen sollen die Grundlage für innovative Behandlungs- und Therapiemethoden bilden. Algorithmen können bereits jetzt im Bereich der Hautkrebs und Brustkrebsfrüherkennung Tumore anhand von CT-Bildern schnell und treffsicher erkennen. Auch seltene Krankheiten können durch den Einsatz von Methoden des maschinellen Lernens zuverlässiger und schneller diagnostiziert werden, als bisher.[2] Durch die Verschmelzung von Bio- und Gentechnik mit Informationstechnik entwickelt sich der Gesundheitsbereich momentan mit enormer Geschwindigkeit.[3]

Bereits jetzt werden in Krankenhäusern wesentliche Geschäftsprozesse, insbesondere im Bereich der Patienten- und Patientinnenversorgung, größtenteils durch Informationstechnik unterstützt. So werden Krankenakten elektronisch geführt und mit entsprechenden Anwendungssystemen vernetzt.[4] Der Markt ist voller Gesundheits-Apps und telemedizinischer Anwendungen, eine digitale Echtzeitkommunikation mit Ärzten und Ärztinnen ist möglich.[5] Als Teil des Digitalisierungsprozesses im Gesundheitswesen ist zudem mit dem Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) die Einführung der sogenannte Telematikinfrastruktur beschlossen wurden. Diese wird im Referentenentwurf des Patientendaten-Schutz-Gesetz (PDSG) als „Datenautobahn des Gesundheitswesens“ betitelt und stellt eine umfassende digitale Vernetzung aller Akteure und Akteurinnen im Gesundheitswesen dar. So soll eine sicherere, schnellere und übergreifende Kommunikation zwischen den diversen Akteuren und Akteurinnen des Gesundheitswesens geschaffen werden.[6]

Die IT-Systeme in Krankenhäusern dienen unmittelbar der Versorgung und Behandlung der Patienten und Patientinnen und beinhalten entsprechende detaillierte Informationen über diese.[7] Mittlerweile ist ein ordnungsgemäßer Krankenhausbetrieb ohne ein funktionierendes IT-System nicht mehr realisierbar. Die Abhängigkeit zieht sich von medizinischen IT-Systemen über

---

[1] Bundesministerium für Gesundheit, *Spahn: „Die Welt wartet nicht auf uns“.*
[2] Martini/Hohmann, *NJW 2020, 3573 Rn 1, 2.*
[3] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 94.*
[4] Bundesamt für Sicherheit in der Informationstechnik, *Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Leitfaden, S. 5.*
[5] Kugelmann, *DuD 2019, 398 (398).*
[6] Bundesministerium für Gesundheit, *Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, S. 83.*
[7] Jorzig/Sarangi, *Digitalisierung im Gesundheitswesen, S. 82.*

die Gebäudeleittechnik bis zur Speiseversorgung der Patienten und Patientinnen durch den gesamten Krankenhausalltag.[8]

Die immer komplexeren IT-Infrastrukturen und der zunehmende Grad der Vernetzung ermöglichen zwar eine effektivere und effizientere Abwicklung von Diensten und globale Zugangsmöglichkeiten für jedermann zu jederzeit von jedem Ort. Mit der Verlagerung der gesellschaftlichen Prozesse auf IT-Systeme kommt allerdings auch eine Abhängigkeit von diesen Systemen daher, gepaart mit einem zunehmenden Interesse an gezielten Missbräuchen. Zudem steigen mit wachsender Komplexität der IT-Systeme auch die Einfallstormöglichkeiten und die Anzahl an Schwachstellen in den Systemen. Entsprechend wichtig ist der Schutz dieser IT-Systeme.[9] Da das Vorhandensein von Schwachstellen in einem System nie vollständig ausgeschlossen werden kann, ist es umso wichtiger, Angriffe auf diese Schwachstellen möglichst frühzeitig zu erkennen, um den Schaden möglichst gering zu halten.[10] Je länger ein Angriff unentdeckt bleibt, desto länger dauert die Wiederherstellung des Betriebszustandes. Verlorene Daten müssen rekonstruiert werden und in der Zwischenzeit angefallene Arbeit muss nachgeholt werden. Die Zeitspanne, die vergeht, bis nach einem erfolgreichen Angriff der Normalzustand wiederhergestellt ist, ist zehnmal so lang, wie die Rückkehr zum Normalzustand nach einer geplanten Betriebsunterbrechung.[11]

Besonders für Unternehmen und Behörden kann eine effiziente IT-Sicherheit existentiell sein.[12] So gaben in einer Studie der DISA (Defense Information Systems Agency) US-Behörden an, dass 72 Prozent der Angriffe auf Computer der Behörden erfolgreich waren. 82 Prozent dieser Angriffe blieben vollkommen unbemerkt.[13] Speziell im Gesundheitssektor steigt die Bedeutung der IT-Sicherheit durch die stetig zunehmende Vernetzung.[14] Die Folgen von erfolgreichen Angriffen auf diese IT-Systeme können weitreichen sein, da Angriffe auf die kritischen Infrastrukturen eines Landes ein besonders hohes gesellschaftliches Schadenspotential aufweisen und für die Täter und Täterinnen somit besonders lukrativ sind, da diese von der Notwendigkeit der Funktionsfähigkeit der Infrastrukturen wissen.[15] Werden IT-Systeme zur Behandlung von Patienten und Patientinnen verwendet, kann eine unberechtigte Infiltration dieser Systeme unmittelbar zur Gefährdung für Leib und Leben der Patienten und Patientinnen werden. Zudem kann der unberechtigte Zugriff auf die Gesundheitsdaten der Patienten und Patientinnen einen schweren Eingriff in deren Grundrechte sowie eine Verletzung der ärztlichen Schweigepflicht

[8] Deutsche Krankenhaus Gesellschaft, *Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, S. 6.*
[9] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 1;* Dehn, *Netzwerke Sicherheit, S. 15.*
[10] Kappes, *Netzwerk- und Datensicherheit, S. 229.*
[11] Dehn, *Netzwerke Sicherheit, S. 16.*
[12] Mehler-Bicher u. a., *Wirtschaftsinformatik Klipp und Klar, S. 101.*
[13] Dehn, *Netzwerke Sicherheit, S. 175.*
[14] Darms u. a., *IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker, und Geschäftsführer in Klink und Praxis, S. 175.*
[15] Bundesamt für Sicherheit in der Informationstechnik, *Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS, S. 5;* Dürig/Fischer, *DuD 2018, 209 (209);* BKA, *Cybercrime Bundeslagebild 2020, S. 29.*

bedeuten.[16] Erfolgreiche Angriffe auf die IT-Infrastrukturen der Krankenhäuser untergraben zudem das Vertrauen der Patienten und Patientinnen in die digitale medizinische Versorgung.[17] Ferner stellt der Gesundheitssektor in Deutschland einen der wichtigsten Wirtschaftsbereiche mit rund 4,5 Millionen Arbeitsplätzen und 8 Prozent des Bruttoinlandsproduktes dar, ein flächendeckender Angriff kann somit auch hohe wirtschaftliche Folgeschäden mit sich führen.[18]

Mit der fortschreitenden Digitalisierung im Gesundheitssektor steigt auch die Bedeutung und der Stellenwert des Datenschutzes in der Medizin. Seit jeher ist dieser durch das Patientengeheimnis und die Schweigepflicht der Ärzte und Ärztinnen bereits durch Hippokrates fest in den Grundsätzen der Medizinethik verankert. Mit einer zunehmenden Digitalisierung muss auch das Selbstbestimmungsrecht des Patienten und der Patientin sowie deren Recht auf informationelle Selbstbestimmung entsprechend geschützt werden, da die Verarbeitung personenbezogener Patientendaten im digitalen Versorgungsalltag allgegenwärtig ist.[19] Oftmals ist den Akteuren beim Einsatz digitaler Technologie nicht bewusst, welche konkreten Gefährdungen für Patientendaten bestehen und wie man diese besser schützen kann.[20] Häufig werden datenschutzrechtliche Vorgaben auch als Hindernis für den technischen Fortschritt im Gesundheitswesen gesehen.[21] Dabei ist die Sicherheit der Informationen, die über die IT-Systeme verarbeitet werden, von hoher Bedeutung. Diese müssen ebenfalls durch technische und organisatorische Vorkehrung gesichert werden. Die Datensicherheit bildet gemeinsam mit dem Datenschutz die Informationssicherheit, deren Umsetzung notwendig ist, um die Aufrechterhaltung des gesellschaftlich etablierten Versorgungsniveaus zu gewährleisten.[22]

Um Angriffe auf IT-Systeme frühzeitig erkennen zu können, entwickelte sich in der Mitte der 80er Jahre das Forschungsgebiet der Angriffserkennung (Intrusion Detection). Mittlerweile sind kommerzielle Intrusion-Detection-Systeme (IDS) für den Einsatz zum Schutz in IT-Systemen verfügbar und gehören zum Stand der Technik.[23]

A. Cyber-Angriffe auf Krankenhäuser

Dass die Gefahr vor Angriffen auf die Infrastrukturen von Krankenhäusern nicht nur theoretischer Natur ist, sondern in der Realität bereits zu weitreichenden Schäden geführt hat, zeigen die jüngsten Angriffe auf die Systeme und Netzwerke von Krankenhäusern:

So wurden im Juli 2019 die zentralen Systeme der DRK-Trägergesellschaft Süd-West durch eine Schadprogramm verschlüsselt. Die an die Systeme angeschlossenen Krankenhäuser in

[16] Tschammler, *PharmR 2019, 509 (509).*
[17] BSI, *Die Lage der IT-Sicherheit in Deutschland 2021, S. 89.*
[18] Jorzig/Sarangi, *Digitalisierung im Gesundheitswesen, S. 81.*
[19] Bauer u. a., *E-Health: Datenschutz und Datensicherheit, S. 35.*
[20] Kugelmann, *DuD 2019, 398 (398).*
[21] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 94.*
[22] DKG, *Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, S. 6.*
[23] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. VII, 1.*

Rheinland-Pfalz und im Saarland wurden hierdurch erheblich in ihrer Versorgungsleistung beeinträchtigt. Um den Umfang des Angriffes feststellen zu können, das Einfallstor zu ermitteln, den Angreifer oder die Angreiferin vom System auszusperren und das Netzwerk wieder in einen arbeitsfähigen Zustand zu versetzen, wurden 13 Tage benötigt.[24]

Ebenfalls ein Opfer von Ransomware wurde im September 2020 das Düsseldorfer Universitätsklinikum in Nordrhein-Westfalen. Es wurden hierbei 30 Server verschlüsselt, was zur Folge hatte, dass akute Fälle 13 Tage lang nicht mehr aufgenommen werden konnten, da die Klinik-IT nicht funktionsfähig war.[25] Bereits stationär behandelte Patienten und Patientinnen konnten weiterhin medizinisch versorgt werden, planbare und ambulante Behandlungen mussten jedoch abgesagt oder verschoben werden. Die telekommunikative Erreichbarkeit des Krankenhauses war zudem stark eingeschränkt.[26] Rettungswagen mussten zu anderen Kliniken umgeleitet werden, was Verzögerungen in der Erstversorgen zur Folge hatte. Eine Frau starb unmittelbar nach der Einlieferung in ein entfernteres Krankenhaus.[27]

Im Dezember 2019 wurden die IT-Systeme des Klinikums in Fürth durch einen Virus via E-Mail angegriffen, was den Krankenhausbetrieb stark einschränkte. Neue Patienten und Patientinnen konnten nicht aufgenommen werden, planbare Operationen wurden abgesagt.[28]

Im Rahmen eines Gutachtens der Personalberatung Rochus Mummert Healthcare Consulting gaben zudem 43 Prozent der Führungskräfte deutscher Krankenhäuser und Pflegeeinrichtungen an, schon Ziel eines Hackerangriffs geworden zu sein.[29]

Es ist somit von dringender Notwendigkeit, die IT-Systeme in Krankenhäusern vor Angriffen zu schützen, um die Funktionalität des Krankenhausbetriebes zu gewährleisten und die sensiblen Daten der Patienten und Patientinnen zu schützen. Eine der wohl effizientesten Möglichkeiten, die Sicherheit von Netzwerken zu gewährleisten, ist die Installation von sogenannten Angriffserkennungssystemen.[30]

B. Ziele und Grenzen der Untersuchung

Anhand dieser Untersuchung wird die rechtliche Ist-Situation auf nationaler sowie unionsrechtlicher Ebene für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater

[24] BSI, *Die Lage der IT-Sicherheit in Deutschland 2020, S. 14.*
[25] BKA, *Cybercrime Bundeslagebild 2020, S. 6.*
[26] BSI, *Die Lage der IT-Sicherheit in Deutschland 2021, S. 15.*
[27] zdf.de, *IT-Ausfall war erpresserischer Hacker-Angriff.*
[28] aerzteblatt.de, *Betrieb im Klinikum Fürth wegen Hacker-Attacke eingeschränkt.*
[29] Ärzteblatt, *IT-Sicherheit und Datenschutz für Kliniken immer wichtiger.*
[30] Smart Grid Task Force EG2, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection.*

Trägerschaft durchleuchtet. Sich bei der Frage der Rechtmäßigkeit des Einsatzes solcher Systeme ergebende Schwachstellen, werden durch Gesetzesimplikationen gelöst.

Im Rahmen dieser Untersuchung wird die Rechtmäßigkeit des Einsatzes von Angriffserkennungssysteme in den IT-Netzen von Krankenhäusern in privater Trägerschaft nach der aktuellen Gesetzeslage geprüft. Ziel der Untersuchung ist es, einen rechtlichen Rahmen für eine umfassende Rechtfertigung des Einsatzes dieser Systeme in privatrechtlich organisierten Krankenhäusern zu finden und entsprechende Implikationen für eine konkrete rechtliche Umsetzung zu formulieren. Die Untersuchung bezieht sich hierbei ausschließlich auf den Einsatz von Angriffserkennungssystemen in Krankenhäusern und nicht auf den Gesundheitssektor im Allgemeinen. Zudem konzentriert sich die Untersuchung auf das Verhältnis zwischen Privatrechtssubjekten, was sich vordergründig in den verfassungsrechtlichen Abhandlungen zeigen wird. Öffentlich-rechtlich organisierte Krankenhäuser sind nicht Gegenstand dieser Untersuchung.

C. Gang der Untersuchung

Es erfolgt zunächst eine Einführung in die relevanten informationstechnischen Grundlagen, bevor das Krankenhaus in privater Trägerschaft als Betrachtungsgegenstand dieser Untersuchung vorgestellt wird. Im Anschluss befasst sich die Untersuchung in der verfassungsrechtlichen Beurteilung mit der Frage, ob es für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft einer ermächtigenden Norm bedarf. Hierbei wird insbesondere auf das Verhältnis der unionsrechtlichen und nationalen Grundrechte sowie auf die Wirkung von Grundrechten auf das Verhältnis zwischen Privatrechtssubjekten eingegangen. Im weiteren Verlauf der Untersuchung werden einschlägige nationale sowie unionsrechtliche Regelungen auf ihre Anwendbarkeit im konkreten Fall geprüft. Ausgehend von den Ergebnissen dieser Untersuchung wird die bestehende Rechtslage durch Implikationen an die Legislative dergestalt novelliert, dass der Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft sowohl auf nationaler als auch auf unionsrechtlicher Ebene hierdurch umfassend gerechtfertigt sein könnte.

II. Betrachtungsgegenstand

Im Rahmen dieser Arbeit wird erörtert, ob der Einsatz von Angriffserkennungssystemen im Gesundheitswesen nach der derzeitigen Gesetzeslage auf nationaler sowie unionsrechtlicher Ebene gerechtfertigt ist. Hierbei wird der Schwerpunkt der Arbeit auf den Einsatz der Systeme in Krankenhäusern in privater Trägerschaft gelegt.

Für das bessere Verständnis werden in diesem Kapitel die relevanten informationstechnischen Grundlagen zusammengefasst. Im Anschluss wird der Einsatzort der Angriffserkennungssysteme, namentlich die IT-Netzwerke und IT-Systeme von Krankenhäusern in privater Trägerschaft, erörtert.

A. Netzwerke

In seinen gänzlichen Grundsätzen kann ein Netzwerk als „Gruppe miteinander verbundener Systeme“ definiert werden, „die in der Lage sind, untereinander zu kommunizieren“. Die kleinste Variante stellt hierbei der Datenaustausch zweier Computer via Kabel oder Funk dar, das Pendant hierzu ist das Internet.[31] Netzwerke unterscheiden sich in ihren Reichweiten, ihrer Topologie sowie Architektur.[32]

In diesem Unterkapitel werden die wichtigsten Begriffe eines Netzwerkes sowie dessen grober Aufbau kurz vorgestellt, um ein besseres Verständnis für die späteren Ausführungen zu erlangen.

1. Architekturmodelle

Die Organisation sowie Rollenvergabe der Anwendungskomponenten eines Netzwerkes werden durch Architekturmodelle beschrieben. Für verteilte Anwendungen wird hierbei zwischen zwei Modellen unterschieden, dem Peer-to-peer-Modell sowie dem Client-Server-Modell.[33]

a) Peer-to-peer

Das englische Wort Peer (gleichgestellt, ebenbürtig) zeigt die Grundstruktur des Architekturmodells auf: das Peer-to-peer-Modell stellt eine Organisationsform dar, bei der im Prinzip alle Computersysteme gleichberechtig sind. Jede Anwendungskomponente kann hierbei sowohl als Server, als auch als Client agieren.[34] Vorteile dieses Architekturmodells sind die Kosteneinsparungen durch die Unabhängigkeit von Servern oder speziellen Betriebssystemen. Allerdings kann es aufgrund der fehlenden zentralen Verwaltung zu Sicherheitsrisiken kommen.[35]

b) Client-Server

Sobald ein Netzwerk eine bestimme Größe erreicht, wird das Peer-to-peer-Modell zunehmend unübersichtlicher.[36] Um eine administrative Verwaltung gewährleisten zu können, wird bei dem Client-Server-Modell das Konzept von Dienstnutzern (Clients) und Diensterbringer (Server) genutzt. Der Server ist als zentrale Anwendungskomponente auf separaten, leistungsfähigen Rechnern angesiedelt und wartet passiv auf Anfragen. Die Clients können unabhängig voneinander vom Server Dienste aktiv anfordern.[37] Hierbei kommunizieren die Clients mit dem

---

[31] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 8.*
[32] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 8.*
[33] Eigner u. a., *Informationstechnologie für Ingenieure, S. 122.*
[34] Eigner u. a., *Informationstechnologie für Ingenieure, S. 123.*
[35] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 10.*
[36] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 10.*
[37] Eigner u. a., *Informationstechnologie für Ingenieure, S. 123.*

Server über eine „Sprache“, dem Protokoll.[38] Je größer ein Netzwerk ist, desto ratsamer ist es, anfallende Aufgaben auf mehrere Server zu verteilen, um die Ressourcen effektiver nutzen zu können. Zudem bietet sich so weniger Angriffsfläche, was die Sicherheit des Netzwerkes erhöht.[39]

2. Protokolle

Protokolle bezeichnen in der IT „Kommunikationsregeln zwischen Systemen und die darauf zugreifenden Prozesse“.[40] Sie definieren das Format und die Reihenfolge des Nachrichtenaustausches sowie Handlungsmaßnahmen für mögliche auftretende Ereignisse.[41] Protokolle können hierbei in Protokoll-Familien (Protokoll-Stacks) zusammengefasst werden. Um die Komplexität der vielen Protokolldetails beherrschen zu können, wurden sogenannte Referenzmodelle entwickelt, in denen die Komplexität von Protokollen in der nachrichtenbasierten Kommunikation durch eine Schichtung überschaubarer dargestellt wurde.[42]

a) Das OSI-Referenzmodell

Das 1983 durch die Internationale Organisation für Normung (ISO) standardisierte Referenzmodell „Open Systems Interconnection Reference Model“ (OSI-Referenzmodell oder ISO/OSI-Referenzmodell) ist ein Schichtmodell, welches sieben aufeinander aufbauende Schichten (Layer) definiert. Es gilt als abstrakte Grundlage für die Beschreibung von Netzwerken, ihren Protokollen und die Entwicklung weiterer Standards.[43]

Die Schichten im OSI-Referenzmodell arbeiten unabhängig voneinander und stellen der nächst höheren Schicht bestimmte Dienste bereit.[44] Hierbei können nur direkt beieinanderliegende Schichten miteinander kommunizieren, einzelne Schichten können nicht übersprungen werden.[45] Für jede Schicht werden Protokolle definiert, die die Handhabung der Daten in der jeweiligen Schicht regeln. Sämtliche Protokolle einer Schicht werden in Protokoll-Stacks zusammengefasst.[46] Jedes Datenpaket passiert alle Schichten bis zu der Schicht, auf der es arbeitet.[47] Findet also eine Kommunikation zwischen zwei Geräten statt, durchläuft auf dem Sendegerät die Nachricht die verschiedenen Schichten, die diese Nachricht Stück für Stück für die Übertragung präparieren. Nach der Übertragung durchläuft die Nachricht auf dem Empfangsgerät wiederum sämtliche Schichten in umgekehrter Reihenfolge, um sie Stück für Stück wieder

[38] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 10.*
[39] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 11.*
[40] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 105.*
[41] Eigner u. a., *Informationstechnologie für Ingenieure, S. 125.*
[42] Mandl, *Internet Internals - Vermittlungsschicht, Aufbau und Protokolle, S. 1.*
[43] Eigner u. a., *Informationstechnologie für Ingenieure, S. 127.*
[44] Obermann/Horneffer, *Datennetztechnologien für Next Generation Networks, S. 17.*
[45] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 98.*
[46] Keller, *Breitbandkabel und Zugangsnetze, S. 289.*
[47] Ballmann, *Network Hacks, S. 8.*

zurück zu transformieren.[48] Grob unterteilt sind die ersten vier Schichten für den Transport der Nachricht zuständig, die oberen Schichten arbeiten anwendungsorientiert, wobei die Komplexität der Arbeitsaufgaben mit der steigender Schicht zunimmt.[49]

Nr.	Layer	Schicht	Aufgaben
7	Application	Anwendung	Schnittstelle der Anwendung auf das Netzwerk
6	Presentation	Darstellung Präsentation	Protokolle für die Syntax der Daten
5	Session	Sitzung	Funktionen für den Auf- und Abbau einer Sitzung, Festlegung von Synchronisationspunkten
4	Transport	Transport	Ende-zu-Ende-Kommunikation
3	Network	Vermittlung Netzwerk	Routing der Pakete
2	Data-Link	Sicherung Datenverbindung	Festlegung des Zugriffsverfahrens, Fehlererkennung der Frames oder Zellen
1	Physical	Bitübertragung	Definition von Aspekten für die Bitübertragung auf dem Medium

Abbildung 1: Aufbau des OSI-Referenzmodells aus Bratvogel/Schmidt, Netzwerke Grundlagen, S. 96

Im Folgenden werden die Eigenschaften und Aufgaben der einzelnen Schichten kurz vorgestellt.

(1) Physical Layer

Die unterste Schicht des OSI-Referenzmodells stellt eine physikalische Verbindung bereit und ist für die Zustellung einzelner Bits zuständig.[50] Der Physical Layer ist hierbei die einzige Schicht, die analoge Signale verarbeiten muss[51], es wird u.a. festgelegt, welche Form die

[48] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 96.*
[49] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 98.*
[50] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 12.*
[51] Obermann/Horneffer, *Datennetztechnologien für Next Generation Networks, S. 17.*

Netzwerkstecker haben müssen und wie die Belegung der einzelnen Pins aussieht.[52] Durch mechanische und elektrische Teilaufgaben wird eine maximale Datenübertragungsrate angestrebt.[53]

(2) Data Link Layer

Wie der Physical Layer konzentriert sich der Data Link Layer ebenfalls ausschließlich auf die Kommunikationsverbindung zweier verbundener Systeme.[54] Der Data Link Layer transformiert die Daten, die er vom Physical Layer bekommt, in Frames (Datenrahmen) bzw. zerlegt Frames, die er von dem darüber liegenden Network Layer bekommt in einzelne Bits für den Physical Layer. Er verbindet folglich die beiden an ihn angrenzenden Schichten.[55] Hierfür werden den Frames im Header und Trailer Informationen hinzugefügt, die es zur Weiterleitung benötigt.[56] Zudem untersucht der Data Link Layer den Bitstrom auf Fehler, korrigiert diese[57] und sorgt im Rahmen einer grundlegenden Flusskontrolle dafür, dass Nachrichten nur übertragen werden, wenn das Empfangsgerät auch empfangsbereit ist.[58]

(3) Network Layer

Der Network Layer teilt Nachrichten in Pakete auf, adressiert sie und legt dabei fest, „in welche Form und auf welchem Weg diese zum gewünschten Ziel übertragen werden“. Die Wegfindung über verschiedene Netzwerkknoten wird Routing genannt und ist die wichtigste Funktion des Network Layer.[59] Der Network Layer ist folglich die erste Schicht im Referenzmodell, die sich mit der Ende-zu-Ende Übertragung in einem Netzwerk befasst.[60]

Das Protokoll, das dieser Schicht in der Regel zugrunde liegt, ist das Internet-Protocol (IP).[61]

(4) Transport Layer

Der Transport Layer ist als vierte Schicht das Bindeglied zwischen den anwendungs- und den transportorientierten Schichten.[62] Der Transport Layer sorgt für eine stabile Ende-zu-Ende Übertragung zwischen zwei Kommunikationsprozessen.[63] Hierzu gehört, neben allgemeinen

---

[52] Eigner u. a., *Informationstechnologie für Ingenieure, S. 129.*
[53] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 100.*
[54] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 12.*
[55] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 100.*
[56] Keller, *Breitbandkabel und Zugangsnetze, S. 289.*
[57] Mandl u. a., *Grundkurs Datenkommunikation, S. 3.*
[58] Obermann/Horneffer, *Datennetztechnologien für Next Generation Networks, S. 18.*
[59] Obermann/Horneffer, *Datennetztechnologien für Next Generation Networks, S. 19.*
[60] Mandl u. a., *Grundkurs Datenkommunikation, S. 85.*
[61] Obermann/Horneffer, *Datennetztechnologien für Next Generation Networks, S. 124.*
[62] Eigner u. a., *Informationstechnologie für Ingenieure, S. 129.*
[63] Mandl u. a., *Grundkurs Datenkommunikation, S. 3.*

Fehlerkorrekturen und Stauvermeidung, die Aufteilung von Daten in Pakete, das erneute Senden verlorengegangener Segmente und das Sortieren empfangener Daten.[64] Im Gegensatz zu den darunter liegenden Schichten stellt der Transport Layer nicht nur eine Verbindung zu den angrenzenden Schichten des Referenzmodells dar, sondern schafft eine Kopplung zwischen zwei Endsystemen.[65]

Für die gesicherte Datenübertragung wird hierbei oft das Transmission Control Protocol (TCP) verwendet.[66]

(5) Session Layer

Der Session Layer ist für den Auf- und Abbau sowie die Aufrechterhaltung von Sitzungen (Sessions) zwischen zwei Systemen zuständig.[67] Hierzu gehört zuvorderst die Synchronisation und die Dialogsteuerung.[68]

(6) Presentation Layer

Der Presentation Layer ist die Darstellungsschicht im OSI-Referenzmodell. Er hat die Aufgabe eines „Dolmetschers" zwischen den Endsystemen und dem Netz[69], da nicht alle Rechnersysteme ihre Daten in gleicher Art und Weise darstellen.[70] Hierfür werden alle Daten in ein allgemein verständliches Standardformat (Transfersyntax) konvertiert.[71] Wichtige Aufgaben des Presentation Layer sind zudem die Datenkodierung, die Datenkompression zur Reduzierung der übertragenden Datenmenge sowie die Datenverschlüsselung.[72]

(7) Application Layer

Die oberste Schicht des OSI-Referenzmodells ist der Application Layer. Hier werden Anwendungsprogramme zur Verfügung gestellt.[73] Er bildet somit die Schnittstelle zwischen Anwendungen und dem Netzwerk zum gegenseitigen Nachrichtenaustausch, wobei die eigentliche Anwendung nicht zu dieser Schicht gehört.[74] Die bekanntesten Protokolle hierfür sind das Hypertext Transfer Protocol (HTTP) und das Simple Mail Transfer Protocol (SMTP).[75]

---

[64] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 13.*
[65] Obermann/Horneffer, *Datennetztechnologien für Next Generation Networks, S. 19.*
[66] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 118.*
[67] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 13.*
[68] Obermann/Horneffer, *Datennetztechnologien für Next Generation Networks, S. 19.*
[69] Obermann/Horneffer, *Datennetztechnologien für Next Generation Networks, S. 19.*
[70] Mandl u. a., *Grundkurs Datenkommunikation, S. 3.*
[71] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 101.*
[72] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 101.*
[73] Obermann/Horneffer, *Datennetztechnologien für Next Generation Networks, S. 19.*
[74] Mandl u. a., *Grundkurs Datenkommunikation, S. 4.*
[75] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 101.*

b) Das TCP/IP-Referenzmodell

Ebenso wie das OSI-Referenzmodell bildet das TCP/IP-Referenzmodell eine logische Sicht auf real arbeitende Protokolle ab. Der Unterschied zwischen den beiden Modellen liegt primär in der Betrachtungsweise.[76] Im TCP/IP-Referenzmodell wird ebenfalls eine Kommunikationsarchitektur über mehrere Schichten beschrieben[77], wobei es im Gegensatz zu dem OSI-Referenzmodell nur vier Schichten aufweist, von denen Schicht 3 und Schicht 4 die tragenden Schichten sind.[78]

Die Schichten des TCP/IP-Referenzmodells lassen sich folgendermaßen mit dem Aufbau des OSI-Referenzmodells vergleichen:

TCP/IP-Schicht	**TCP/IP**	**OSI**	**OSI-Schicht**
4	Anwendungs-Schicht	Application Layer	7
		Presentation Layer	6
		Session Layer	5
3	Transport-Schicht (TCP)	Transport Layer	4
2	Internet-Schicht (IP)	Network Layer	3
1	Netzwerk- und Link-Schicht	Data Link Layer	2
		Physcial Layer	1

Abbildung 2: Vergleich des Aufbaus von OSI-Referenzmodells zu TCP/IP-Referenzmodell aus Bratvogel/Schmidt, Netzwerke Grundlagen, S. 107

Das TCP/IP-Referenzmodell gilt als Standard des Internets, es wird von jeder Rechnerplattform unterstützt.[79]

Im Folgenden werden die vier Schichten des TCP/IP-Referenzmodells kurz vorgestellt und ihre Arbeitsweise sowie ihre Aufgaben im Gesamtsystem erläutert.

[76] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 12.*
[77] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 10.*
[78] Mandl u. a., *Grundkurs Datenkommunikation, S. 9.*
[79] Eigner u. a., *Informationstechnologie für Ingenieure, S. 132.*

(1) Link Layer

Die erste Schicht des TCP/IP-Referenzmodells, der Link Layer, ist eine Zusammenfassung des Physical Layers und des Data Link Layers aus dem OSI-Referenzmodell.[80] Der Layer umfasst die eigentliche Datenübertragung, also die Übertragung einzelner Bits über ein physikalisches Medium zu einem Netzwerkrechner.[81] Hierbei werden Datenframes zwischen Hardwareadressen (Mac-Adressen) übertragen.[82] Typische Netzwerktechnologien, zu denen der Link Layer einen Zugang ermöglicht, sind das Ethernet oder das Wireless LAN (WLAN).[83]

(2) Internet Layer

Der Internet Layer „dient der verbindungslosen, paketorientierten Kommunikation über Netzwerke hinweg".[84] Er hat die Aufgabe, die empfangenen Frames aus dem Link Layer zu abstrahieren und die enthaltenen Dateneinheiten als Pakete zu bezeichnen. Diese Datenpakete werden mit Hilfe des Internet-Protokolls (IP) versendet bzw. empfangen. Hierbei werden die Hosts mittels IP-Adressierung kenntlich gemacht.[85] Die Wegfindung ist die Aufgabe von Routern[86], was eine weltweite Übertragung ermöglicht.[87]

(3) Transport Layer

Aufgabe des Transport Layers ist die zielgerichtete Beförderung von Daten an die richtigen Anwendungen. Der Transport Layer ist folglich ein Vermittler zwischen IP und möglichen Anwendungen.[88] Das gängige Protokoll für den verbindungsorientierten Tramsportdient ist TCP.[89] Anwendungen sind hierbei sog. Ports zugeordnet. Es gibt pro Verbindung zwei Ports, den Quellport (Senderseite) und denn Zielport (Empfängerseite). Die Paarung von Quell- und Zielport erlaubt die eindeutige Zuordnung von Rechnerverbindungen, die fest bestehen.[90] Ist eine solche Verbindung hergestellt, können Datenströme entgegengenommen werden und in IP-gerechte Pakete zerlegt werden. Diese werden mit zusätzlichen Informationen versehen in das Netz geschickt. Die Verbindung wird geschlossen, wenn von beiden Seiten keine Daten mehr übertragen werden sollen.[91]

---

[80] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 13.*
[81] Wendzel, *Tunnel und verdeckte Kanäle im Netz - Grundlagen, Protokolle, Sicherheit und Methoden, S. 7.*
[82] Plenk, *Angewandte Netzwerktechnik kompakt, S. 7.*
[83] Mandl, *Internet Internals - Vermittlungsschicht, Aufbau und Protokolle, S. 2.*
[84] Mandl, *Internet Internals - Vermittlungsschicht, Aufbau und Protokolle, S. 2.*
[85] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 23.*
[86] Wendzel, *Tunnel und verdeckte Kanäle im Netz - Grundlagen, Protokolle, Sicherheit und Methoden, S. 12.*
[87] Plenk, *Angewandte Netzwerktechnik kompakt, S. 7.*
[88] Wendzel, *Tunnel und verdeckte Kanäle im Netz - Grundlagen, Protokolle, Sicherheit und Methoden, S. 8.*
[89] Mandl, *Internet Internals - Vermittlungsschicht, Aufbau und Protokolle, S. 2.*
[90] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 24.*
[91] Keller, *Breitbandkabel und Zugangsnetze, S. 310.*

(4) Application Layer

Auf dem Application Layer finden Netzwerkprogramme und -dienste ihren Platz im Schichtenmodell.[92] Hier wird die bloße Datenübertragung um Datenstrukturen erweitert.[93] Anwendungen stellen hierbei über einen Port einen Dient zur Verfügung, über den sie senden und empfangen können.[94] Typische Anwendungsprotokolle hierfür sind HTTP (Web-Kommunikation) und SMPT (Mail-Kommunikation).[95]

c) IP-Adressierung

Wird TCP/IP verwendet, muss jeder Schnittstelle im Netzwerk innerhalb eines Netzwerkverbundes eine IP-Adresse zugewiesen werden. Hierdurch wird der physikalischen Hardware-Adresse (MAC-Adresse) eine logische IP-Adresse zugeordnet.[96] Die Adressierung kann zur Pfadfindung genutzt werden, da jeder Router Adress-Informationen in seiner Routing-Tabelle führt.[97] IP-Adressen sind somit elektronische Adressen von Rechnern (Servern), die hierrüber eindeutig im Netz identifizierbar sind.[98]

In der aktuell genutzten Version IPv4 sind IP-Adressen 32 Bit lange Binärzahlen, die im Dotted-Decimal-Format angegeben werden[99]. Hieraus ergeben sich vier Zahlenblöcke mit einer maximal dreistelligen Zahl aus dem Bereich 0 bis 255, die durch einen Punkt voneinander getrennt sind (z. B. 193.96.1.200.).[100] Sie sind hierarchisch gegliedert und werden zentral durch IANA 7 (global) und RIPE 8 (Europa) vergeben.[101]

Da der Adressvorrat von IPv4 endlich ist und bereits erschöpft ist, wird eine Umstellung auf IPv6-Adressen vollzogen. Hierbei wird die Adressierungskapazität von 32 Bit auf 128 Bit erweitert. IPv6-Adressen bestehen aus acht durch Doppelpunkte getrennte Zahlengruppen. Es werden Ziffern des Hexadezimalsystems verwendet.[102]

---

[92] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 26.*
[93] Plenk, *Angewandte Netzwerktechnik kompakt, S. 8.*
[94] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 26.*
[95] Mandl, *Internet Internals - Vermittlungsschicht, Aufbau und Protokolle, S. 2.*
[96] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 109.*
[97] Keller, *Breitbandkabel und Zugangsnetze, S. 298.*
[98] Fezer u. a., *Lauterkeitsrecht - Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG) Domainrecht Rn 1.*
[99] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 108.*
[100] Bratvogel/Schmidt, *Netzwerke Grundlagen, S. 113.*
[101] Keller, *Breitbandkabel und Zugangsnetze, S. 298.*
[102] Fezer u. a., *Lauterkeitsrecht - Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG) Domainrecht Rn 1.*

3. Das Internet

Das Internet ist ein „dezentral organisiertes, globales Rechnernetzwerk, das aus beliebig vielen miteinander verbundenen und eindeutig adressierten lokalen und nationalen Netzen besteht und auf einem einheitlichen und offenen Netzwerkprotokoll basiert“.[103]

Im Hinblick auf den Datenschutz kann das Internet in drei wichtige Teilbereiche unterteilt werden: Das physikalische Netz bestehend aus Festnetz, Funk, Satellit, GPRS und UMTS, das auf Basis einheitlicher Netzwerkprotokolle Rechner miteinander verbindet. Dann die digitale, transportierende IP-Schicht, durch die unterschiedliche Internetdienste (WWW, E-Mail) als zweiter Bereich überhaupt ermöglicht werden. Und schließlich der dritte Bereich, das World Wide Web als Ausschnitt des Internets mit seiner gesellschaftlichen Bedeutung in Bezug auf Suchmaschinen, Social Media, Online Shops etc..[104]

An das Internet angeschlossene Rechner können durch ihre IP-Adressierung eindeutig identifiziert werden.[105] In engem Zusammenhang hierzu steht das **Domain Name System (DNS)**.[106] Hier wird jeder statischen IP-Adresse eine symbolische Anschrift (Domain) zugeordnet, die nutzerfreundlicher gestaltet ist, als die numerische IP-Adresse.[107] Sie wird zudem nicht automatisiert zugewiesen, sondern kann unter Berücksichtigung der Regeln frei gewählt werden.[108] Nach Eingabe des Domainnamens wird dieser auf einem Domain Name System Server durch ein Programm in die IP-Adresse umgewandelt. Ein am Internet angeschlossener Rechner kann sowohl über seine IP-Adresse als auch über seinen Domainnamen kontaktiert werden.[109]

B. IT-Sicherheit in Netzwerken

Das Ziel der IT-Sicherheit ist „die Erreichung von Schutzzielen trotz der Präsenz intelligenter Angreifer und Angreiferinnen.“[110]

Im Folgenden werden die Grundlagen der IT-Sicherheit erörtert. Neben den Schutzzielen werden grundlegende Definitionen des Angreifenden, des Angriffs sowie der Ausgestaltung von ebendiesem aufgeführt. Zudem werden Firewalls und Angriffserkennungssysteme als Werkzeuge der IT-Sicherheit vorgestellt.

---

[103] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 3.*
[104] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 2.*
[105] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 6.*
[106] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 8.*
[107] Fezer u. a., *Lauterkeitsrecht - Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG) Domainrecht Rn 3.*
[108] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 8.*
[109] Fezer u. a., *Lauterkeitsrecht - Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG) Domainrecht Rn 3.*
[110] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 6.*

1. Schutzziele

Die mit den Anforderungen an IT-Sicherheit einhergehenden Aufgabenbereiche können als Schutzziele zusammengefasst werden. Die drei wesentlichen Schutzziele werden als CIA-Tirade bezeichnet: Vertraulichkeit (confidentiality), Integrität (integrity) und Verfügbarkeit (availability).[111] Vertraulichkeit meint hierbei den Schutz der Daten vor unautorisierter Kenntnisnahme.[112] Die Integrität eines IT-Systems ist gegeben, wenn zu übertragende Informationen nicht unautorisiert geändert werden können bzw. solche Änderungen zuverlässig erkannt und kompensiert werden können.[113] Mit der Verfügbarkeit ist die Anforderung an das System gemeint, zur gewünschten Zeit die gewünschten Informationen erhalten zu können.[114]

Neben den Schutzzielen der CIA-Tirade gibt es zudem noch das Schutzziel der Authentizität. Hiermit ist die Überprüfbarkeit der Echtheit einer Nachricht oder der Identität des Absenders oder der Absenderin gemeint.[115]

Es soll demnach ein Zustand gewahrt werden, in dem ein Rechnernetz und dessen Werte wie Kunden- und Kundinnendaten, Personaldaten oder abgespeichertes Wissen ebenso geschützt sind wie die Integrität der Wirtschaftlichkeit.[116] Nur mit einer funktionierenden IT-Sicherheit kann ein effektiver Datenschutz gewährleistet werden.[117]

Die Schutzziele können erreicht werden durch konsequente Angriffsprävention sowie -detektion und, im Falle eines dennoch erfolgreichen Angriffs, eines Systemwiederherstellungsmanagements, welches neben dem Stoppen des Angriffes die Reparatur des Systems sowie die Gewährleistung der Funktionsfähigkeit des Systems während des Angriffes gewährleistet.[118]

2. Angreifer/Angreiferin

Angreifer und Angreiferinnen von IT-Systemen werden als Hacker bezeichnet. Sie entwickeln Verfahren, um in Applikationen oder Netzwerke ohne Befugnis einzudringen.[119] Hierfür entwickeln sie teils bedeutsame Software, welche in der Community mitsamt Wissen, Erkenntnissen und Werkzeugen geteilt wird.[120] Jedoch agiert nicht jeder Hacker böswillig. Ethikhacker, sogenannte, „white hat hacker“, helfen in der IT-Sicherheit, Schwachstellen in Netzwerken

---

[111] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 83.*
[112] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 5.*
[113] Schill/Springer, *Verteilte Systeme, S. 134.*
[114] Mehler-Bicher u. a., *Wirtschaftsinformatik Klipp und Klar, S. 102.*
[115] Schill/Springer, *Verteilte Systeme, S. 134.*
[116] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 80;* Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kap. 1 Rn 4.*
[117] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kap.1 Rn 5.*
[118] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 82.*
[119] Dehn, *Netzwerke Sicherheit, S. 18.*
[120] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 83.*

aufzudecken und zu dokumentieren. „Black hat hacker“ oder „crackers“ hingegen versuchen illegal in Netzwerke zu gelangen, um negativen Einfluss zu gewinnen.[121]

3. Angriffe

Angriffe („attack“ oder „intrusion“) sind vorsätzliche Versuche, die Sicherheitseigenschaften eines Netzwerkes zu verletzen. Hierbei kann zwischen Fernangriffen über eine Netzwerkverbindung wie beispielsweise das Internet und Nahangriffen durch die lokalen Benutzer oder Benutzerinnen des Zielsystems[122] sowie zwischen passiven (Informationsgewinnung) und aktiven (Zielsystembeeinflussung) Angriffen unterschieden werden.[123] Angriffe können sich in einem Verhindern, Erlangen, Modifizieren oder Fälschen manifestieren. Davon betroffen sind die Daten, Dienste und Nachrichten der Systeme.[124]

Für einen erfolgreichen Angriff bedarf es einer Sicherheitslücke, die ausgenutzt werden kann. Solche Sicherheitslücken können in jeder Phase des Systementwicklungsprozesses entstehen und in Hardware- sowie Softwarekomponenten vorkommen.[125]

Immer häufiger wird bei Angriffen als Werkzeug auf automatisierte Programme, sogenannte „**exploits**“, zurückgegriffen.[126] Durch ein gezieltes Einsetzen können Hacker administrative Rechte und somit uneingeschränkten Netzwerkzugriff erreichen.[127] Exploits nutzen hierbei die Verwundbarkeit von Software aus.[128] Hat ein Hacker über einen Exploit erfolgreich die Kontrolle über ein System erlangt, verschleiert er oder sie die Spuren seiner Tätigkeiten durch sogenannte „**rootkits**“, das wichtige Module des Zielbetriebssystems in modifizierter Form beinhaltet und die Originalkomponenten ersetzt. Hierdurch bleiben zukünftige Aktionen des Hackers verborgen.[129]

Automatisierte, fernsteuerbare Angriffe in Form von Schadsoftware werden „**Bots**“ genannt. Diese können zu ganzen Netzwerken zusammengeschlossen werden (Botnet), die durch Botmaster per Internet gesteuert werden.[130] Bots können auf Befehl des Botmasters weitere Systeme für potentielle Angriffe suchen und diese auf Basis von Exploits infiltrieren. Zudem können Bots sog. **Denial-of-Service-Angriffe (DoS)** durchführen.[131] Diese Angriffe dienen dazu, den TCP/IP-Stack eines Dienstes im Netzwerk zu überlasten und so die Kommunikation mit dem Zielrechner einzuschränken oder ganz zu unterbrechen.[132] Dies geschieht durch das

[121] Franzetti, *Essenz der Infortmatik, S. 179.*
[122] Milenkoski, *Evaluation of Intrusion Detection Systems in Virtualized Environments, S. 13.*
[123] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 191.*
[124] Schill/Springer, *Verteilte Systeme, S. 134.*
[125] Kappes, *Netzwerk- und Datensicherheit, S. 6.*
[126] Groß, *Kooperative Angriffserkennung in drahtlosen Ad-hoc- und Infrastrukturnetzen, S. 40.*
[127] Dehn, *Netzwerke Sicherheit, S. 31.*
[128] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 196.*
[129] Dehn, *Netzwerke Sicherheit, S. 38.*
[130] Franzetti, *Essenz der Infortmatik, S. 180.*
[131] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 97.*
[132] Dehn, *Netzwerke Sicherheit, S. 39.*

gezielte Ausnutzen von Implementierungs- bzw. Protokollfehlern oder durch das Überfluten der Ressourcen (Speicherplatz, Rechenzeit oder Bandbreite) des Angriffsziels.[133] DoS-Angriffe können auch verteilt agieren, als **Distributed Denial of Service-Angriff (DDoS)**. Sie werden über unterschiedliche IP-Adressen initiiert, was die Abwehr der Angriffe deutlich erschwert.[134]

Eine andere Möglichkeit, um unerlaubten Zugang zu einem Netzwerk zu erlangen, ist die Nutzung von **Sniffern**. Diese protokollieren unbemerkt alle Tastatureingaben im Anmeldedialog und legen hierdurch die Anmeldeinformationen von Administratoren und Usern für den Hacker frei.[135] Netzwerk-Siffer können zudem den ganzen Datenverkehr eines Computers überwachen.[136]

4. Schadprogramme

Schadprogramme, auch Malware genannt, können auf sämtlichen Softwareebenen operieren und angreifen.[137] Gelangen sie unerlaubt in das fremde Computersystem, haben sie zum Ziel, dort Schaden anzurichten.[138] Im Folgenden werden die am häufigsten vorkommenden Schadprogramme vorgestellt.

a) Computerviren

Eine populäre und weit verbreitete Art der Schadprogramme sind Computerviren. Diese sind Programme, die sich durch die Indizierung eines eigenen Codes in andere Programme bei Ausführung replizieren. Werden die infiltrierten Programme ausgeführt, wird folglich auch der Virencode ausgeführt.[139] Ein Computervirus beinhaltet die Komponenten Infektion, Payload und Tarnung.[140] Zudem haben sie die Eigenschaft, sich durch stetiges Modifizieren und Integrieren in neue Dateien zu reproduzieren. Die Übertragung und Infektion werden in der Regel durch Benutzer oder Benutzerinnen umgesetzt, beispielsweise durch das Versenden bereits infizierter Programme per Mail. Dies geschieht im Regelfall unbemerkt.[141]

Die älteste Art von Computerviren sind **Bootsektorviren**, die über bootfähige CDs, DVDs und USB-Sticks agieren. Bootsektorviren nutzen den Neustart eines Computers, um den Virus vom Datenträger auf den Computer zu übertragen und zu speichern. Verbreitet werden Bootsektorviren durch die Weitergabe und -nutzung von befallenen CDs, DVDs und USB-Sticks.[142]

---

[133] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 12.*
[134] Dehn, *Netzwerke Sicherheit, S. 39.*
[135] Dehn, *Netzwerke Sicherheit, S. 40.*
[136] Dehn, *Netzwerke Sicherheit, S. 40.*
[137] Kappes, *Netzwerk- und Datensicherheit, S. 96.*
[138] Franzetti, *Essenz der Infortmatik, S. 180.*
[139] Kappes, *Netzwerk- und Datensicherheit, S. 95.*
[140] Kappes, *Netzwerk- und Datensicherheit, S. 96.*
[141] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 95.*
[142] Dehn, *Netzwerke Sicherheit, S. 54.*

Relativ populär sind sogenannte **Dateiviren**. Hier versucht der Virus, sich an das Ende der Wirtsdatei anzuhängen und wird beim Aufruf der Datei mit ausgeführt.[143]

Unabhängig von Bootsektoren und Programmdateien und somit unabhängig von ausführbaren Codes sind **Makroviren**. Makros sind nicht eigenständig, sondern werden innerhalb eines anderen Programmes zur Automatisierung komplexer Abläufe innerhalb des Programmes ausgeführt. Oft sind sie Bestandteil der in Dateien abgespeicherten Anwendungsdaten. Makroviren werden in derselben Sprache geschrieben, wie die Markos selbst. Sie können sich folglich auch nur in Umgebungen verbreiten, in denen in Makrosprache ausgeführt wird.[144]

b) Würmer

Im Gegensatz zu Computerviren sind Würmer bei ihrer Verbreitung nicht auf Interaktionen des Benutzers oder der Benutzerin angewiesen. Sie können sich selbstständig in Rechnernetzen vervielfältigen.[145] Hierfür nutzen Würmer gezielt die Schwachstellen der über das Netzwerk angebotenen Dienste.[146] Ist ein fremder Rechner von einem Wurm befallen, kann sich dieser mittels E-Mail und dem gefundenen Adressbuch fortbewegen. Er versucht dabei über das infiltrierte Netzwerk andere Rechner zu finden, die ebenfalls die erfolgreich genutzte Schwachstelle besitzen.[147] Somit ist die Infektionsrate von Würmern deutlich höher als die der Computerviren.[148] Als Grundidee für dieses Konzept gilt das Computerspiel Core Wars aus den 70er Jahren. Hier mussten geschriebene Programme gegeneinander antreten mit dem Ziel, dem gegnerischen Programm Rechenzeit zu entziehen oder es zu zerstören.[149]

c) Trojaner

Trojanische Pferde (kurz Trojaner) sind Schadsoftware, die als legitime Software getarnt werden. Der im Programm versteckte schädliche Code arbeitet nach der Installation des Programmes wie ein Virus[150] und ermöglicht dem Angreifer beispielsweise Zugang zum Netzwerk durch sogenannte Backdoors oder das Protokollieren von Passworteingaben.[151] Zudem können Trojaner in Form von Ransomware den Zugriff auf Daten und Systeme durch Verschlüsselung vor dem eigentlichen Netzwerkbesitzer verhindern, um so gegen Freigabe Lösegeld zu erpressen.[152]

---

[143] Dehn, *Netzwerke Sicherheit, S. 56.*
[144] Kappes, *Netzwerk- und Datensicherheit, S. 99.*
[145] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 96.*
[146] Kappes, *Netzwerk- und Datensicherheit, S. 95.*
[147] Kappes, *Netzwerk- und Datensicherheit, S. 99.*
[148] Franzetti, *Essenz der Infortmatik, S. 181.*
[149] Dehn, *Netzwerke Sicherheit, S. 66.*
[150] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 96.*
[151] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 11.*
[152] Dehn, *Netzwerke Sicherheit, S. 67.*

5. Schaden

Der durch Malware entstandene Schaden ist vielfältig. Möglich ist die Zerstörung von Hard- und Software auf den infiltrierten Rechnern oder die Beeinträchtigung der Benutzbarkeit des Rechners oder des Netzwerkes. Malware kann für Datendiebstahl und Datenmissbrauch genutzt werden. Zudem kann der Rechner an sich missbraucht werden, beispielsweise zum Versenden von infizierten Massenmails. Ist ein Rechner infiziert, fallen oftmals hohe Kosten für die Entfernung der Malware an.[153]

6. Firewalls

Firewalls werden im Baugewerbe verbaut, um bei einem ausgebrochenen Feuer das Übergreifen auf andere Gebäudeteile zu verhindern. Übertragen auf Computernetzwerke fällt unter den Begriff Firewall die Aufgabe, Segmente eines Computernetzwerkes gegeneinander abzuschotten.[154] Klassischerweise werden Firewalls an der Schnittstelle zwischen eigenem Netzwerk und Internet positioniert.[155] Angepasst an Schutzbedarf und Topologie des Netzwerkes können auch mehrere Firewalls platziert werden.[156] Firewalls kontrollieren den Verkehr zwischen den kommunizierenden Netzen nach festgelegten Regeln (Policies), die den Verkehr in erlaubten und nicht erlaubten Verkehr unterteilen.[157] Stuft die Firewalls ein eintreffendes Paket als nicht erlaubt ein, wird dieses verworfen und nicht weitergeleitet.[158]

Man kann zwischen zwei Arten von Firewalls unterscheiden: den Network Firewalls, die auf Kopplungselementen wie beispielsweise Routern installiert werden sowie den Personal Firewalls auf den Endgeräten von Endnutzern und -nutzerinnen.[159]

a) Network Firewalls

Network Firewalls können entsprechend der Schichten des OSI-Referenzmodells als Paketfilter, Applikationsfilter sowie Proxyfilter unterschieden werden.[160] Paketfilter filtrieren hierbei den Verkehr auf Netzwerk- und Transportprotokollebene, Proxyfilter und Applikationsfilter die Kommunikation auf der Applikationsebene.[161]

Die **Paketfilter Firewall** ist der einfachste Firewalltyp und kann auf jedem Router platziert werden. Sie arbeitet auf der dritten und vierten Schicht des OSI-Referenzmodells. Das

---

[153] Kappes, *Netzwerk- und Datensicherheit, S. 96.*
[154] Dinger/Hartenstein, *Netzwerk- und IT-Sicherheitsmanagement - Eine Einführung, S. 257.*
[155] Dehn, *Netzwerke Sicherheit, S. 163.*
[156] Dehn, *Netzwerke Sicherheit, S. 164.*
[157] Kappes, *Netzwerk- und Datensicherheit, S. 162.*
[158] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 199.*
[159] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 199.*
[160] Schill/Springer, *Verteilte Systeme, S. 150.*
[161] Kappes, *Netzwerk- und Datensicherheit, S. 195.*

Regelwerk der Paketfilter Firewall wird Access Control List (ACL) genannt.[162] Sie filtern Pakete aufgrund ihrer Informationen über Quell- und Zieladressen, Protokolltypen und über verwendete Dienste bzw. Portnummern.[163]

Applikationsfilter arbeiten hingegen ausschließlich auf der Anwendungsschicht des OSI-Referenzmodells. Hierfür ist es nötig, dass die Filter die Spezifikationen der zu untersuchenden Anwendungsprotokolle, wie beispielsweise http, kennen.[164] Dies macht die Implementierung von Applikationsfiltern jedoch sehr aufwändig, denn es bedarf für jeden Dienst einen entsprechenden Applikationsfilter.[165]

Proxyfilter arbeiten ähnlich wie Applikationsfilter, sie können als besondere Variante ebendieser gesehen werden.[166] Proxy-Server agieren als eine Art Stellvertreter. Sie handeln gegenüber dem Client wie der anzusprechende Server und andersrum gegenüber dem Server wie ein Client. Durch diese Zwischenschaltung wir die Anonymität der Netzwerkadresse des Clients gewährleistet und der Proxy-Server entscheidet über die Weiterleitung von Anfragen oder Antworten.[167] Auch hier bedarf es einen höheren Ressourcenaufwand als bei der Anwendung von Paketfilter Firewalls, da die Firewall die Protokolle zunächst nachbilden muss, um entsprechende Filterregeln anzuwenden. Auch hier ist zudem für jeden Anwendung und jedes Protokoll eine eigene, kompatible Firewall notwendig.[168]

b) Personal Firewalls

Personal Firewalls werden direkt auf dem Rechner des Endnutzers oder der Endnutzerin zur Paketfilterung installiert.[169] Sie sitzt zwischen dem Rechner und dem Netzwerk und fungiert ähnlich wie die Paketfilter Firewall, wobei eine detailliertere Filterung aufgrund des Zugriffs auf lokale Zusatzinformationen möglich ist. Personal Firewalls unterliegen oftmals der Administration der Endnutzer und Endnutzerinnen, was bei ungenügenden Fachkenntnissen zu Sicherheitslücken führen kann. Zudem kann eine Personal Firewall durch Malware abgeschaltet werden, da diese auf dem Rechner selbst verankert ist.[170]

c) Netzwerkadressübersetzung (NAT)

Die Grundidee der Netzwerkadressübersetzung (Network Address Translation, kurz NAT) ist die Mehrfachnutzung einzelner IP-Adressen für verschiedene Systeme. Diese Idee resultierte

[162] Dehn, *Netzwerke Sicherheit, S. 165.*
[163] Schill/Springer, *Verteilte Systeme, S. 150.*
[164] Dinger/Hartenstein, *Netzwerk- und IT-Sicherheitsmanagement - Eine Einführung, S. 261.*
[165] Schill/Springer, *Verteilte Systeme, S. 151.*
[166] Schill/Springer, *Verteilte Systeme, S. 151.*
[167] Mehler-Bicher u. a., *Wirtschaftsinformatik Klipp und Klar, S. 113.*
[168] Dehn, *Netzwerke Sicherheit, S. 168.*
[169] Bless u. a., *Sichere Netzwerkkommunikation, S. 263.*
[170] Kappes, *Netzwerk- und Datensicherheit, S. 194.*

ursprünglich aus dem absehbaren Mangel an verfügbaren öffentlichen IP-Adressen.[171] Private IP-Adressen, die ausschließlich zur Nutzung in privaten Netzen gedacht sind und somit keinen direkten Zugriff auf das Internet haben, können durch NAT Zugang zu öffentlichen Netzen erlangen.[172] Würden Netzwerkrechner mit ihren öffentlichen IP-Adressen an das Internet angeschlossen werden, könnten diese durch die sichtbare IP-Adressierung von außen erreicht werden, was die Nutzung von Paketfiltern unumgänglich macht. Durch die Nutzung der NAT besitzt nur die Firewall oder der Router eine öffentliche IP-Adresse und sämtliche dahinterstehende Rechner erhalten private IP-Adressen. Außenstehende sehen hierdurch nur die Firewall bzw. den Router als Kommunikationspartner.[173] NAT dient somit auch der Anonymisierung des Datenverkehrs. Eine genaue Identifizierung des kommunizierenden Rechners eines privaten Adressbereiches ist folglich nicht möglich.[174] Streng genommen ist NAT kein Sicherheitsmechanismus, kann aber in Kombination mit Firewalls zur Sicherheit in einem Netzwerk beitragen.[175]

7. Angriffserkennungssysteme

Aufgrund der zuvor beschriebenen Bedrohungen in Netzwerken ist die Nutzung von Firewalls und sogenannten Angriffserkennungssystemen essentiell. Zur Erkennung von Angriffen wird zwischen präventiven und reaktiven Maßnahmen unterschieden. Präventive Mechanismen sind beispielsweise die Lokalisierung und Schließung von Schwachstellen und Sicherheitslücken. Reaktive Maßnahmen hingegen sind Methoden, die Angriffe erkennen können, um im Anschluss gegebenenfalls Gegenmaßnahmen durchzuführen.[176] Angriffserkennungssysteme sind nach der Legaldefinition des § 2 Nr. 9b BSIG „*durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.*“

Zu den Angriffserkennungssystemen gehören Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS). IDS agieren passiv. Sie können Angriffe erkennen, protokollieren und melden, diese aber nicht abwehren. IPS hingegen können nach einem erkannten Angriff Gegenmaßnahmen einleiten, beispielsweise in Form von Firewallregel-Modifizierungen. IPS sind grundsätzlich keine Erweiterung eines IDS, sondern können auch angriffsunabhängig auf Basis präventiver Regelsätze agieren.[177]

---

[171] Bless u. a., *Sichere Netzwerkkommunikation, S. 246.*
[172] Kappes, *Netzwerk- und Datensicherheit, S. 171.*
[173] Dehn, *Netzwerke Sicherheit, S. 169.*
[174] Kappes, *Netzwerk- und Datensicherheit, S. 174.*
[175] Bless u. a., *Sichere Netzwerkkommunikation, S. 246.*
[176] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 17.*
[177] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 199.*

Zudem zählen Security Information and Event Management-Systeme (SIEM-Systeme) zu den Angriffserkennungssystemen, die in Echtzeit die sicherheitsrelevanten Ereignisse analysieren, die in den automatisiert erhoben Logfiles protokolliert sind.[178] Um nach dem Stand der Technik zu agieren ist es erforderlich, IDS und SIEM-Systeme einzusetzen.[179]

Im Folgenden werden IDS, IPS und SIEM-Systeme vorgestellt.

a) Intrusion Detection Systeme (IDS)

Bei IDS handelt es sich um IT-Systeme, die den Einbruch in ein Computersystem oder Rechnernetz automatisiert erkennen sollen.[180] Ein solcher Einbruch liegt vor, wenn sich eine Person unberechtigt Zugriff zu einem IT-System verschafft. IDS sollen bestehende Sicherheitsmaßnahmen zur Verhinderung von Einbrüchen flankieren. Gesucht wird nach verdächtigem Netzverkehr, Viren in Dateien und unerlaubten Änderungen an Dateien.[181] Jeglichen Arten von IDS ist gemeinsam, dass sie zur Erkennung auf Daten der bestehenden IT-Systeme Zugriff haben müssen. Zudem sammeln IDS Informationen über neue Angriffstechniken, um ihren Schutzstandard fortlaufend zu verbessern.[182] Die Erkennung von Angriffen kann sowohl online als auch offline erfolgen. Der Unterschied liegt darin, dass die Online-Erkennung in Echtzeit durchgeführt wird und Angriffe zeitnah erkannt werden können, wohingegen die Offline-Erkennung den aufgezeichneten Verkehr erst im Nachhinein auf Angriffe untersucht, was der Analyse jedoch einen breiteren Spielraum bietet.[183]

IDS bestehen typischerweise aus Netzwerksensoren und/oder Hostsensoren, Datenbankkomponenten, Managementstationen und Auswertungsstationen.[184]

(1) Netzwerkbasierte und hostbasierte IDS

Es wird zwischen zwei verschiedenen Arten von IDS unterschieden: den hostbasierten IDS (HIDS) und den netzwerkbasierten IDS (NIDS)[185], wobei auch hybride IDS möglich sind, die beide Komponenten vereinen.[186] NIDS überwachen den Netzwerkverkehr, wohingegen HIDS die einzelnen Rechner überwachen.[187]

---

[178] Miller, *NdsVBl 2021, 1 (2).*
[179] Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 38.*
[180] Dehn, *Netzwerke Sicherheit, S. 174.*
[181] Forgó u. a., *Rechtsgutachten zum Betrieb von IDS & Event Management-Systemen in Netzen der öffentlichen Verwaltung, S. 9.*
[182] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 9.*
[183] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 17.*
[184] *Einführung von Intrusion-Detection-Systemen - Grundlagen, S. 6.*
[185] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 199.*
[186] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 200.*
[187] Dinger/Hartenstein, *Netzwerk- und IT-Sicherheitsmanagement - Eine Einführung, S. 264.*

IDS können folglich vor der Firewall und somit vor dem zu schützenden Netz stehen oder hinter der Firewall in dem zu schützenden Netz. Arbeitet die Firewall mit NAT, kann die original IP-Adresse des Angreifers bei Detektion des Angriffes hinter der Firewall nicht erkannt werden.[188]

Netzwerkbasierte IDS (NIDS) überwachen und analysieren den Datenverkehr in einem Netzwerk auf verdächtige Ereignisse und vergleichen diese mit bekannten Angriffsmustern.[189] Der Netzwerksensor kann sich hierbei direkt im Datenstrom befinden oder den Datenstromverkehr indirekt durch Beobachtung analysieren.[190] Sie werden an sogenannten Choke Points (Verbindungspunkte) im Netzwerk installiert, die für den Netzbetrieb von hoher Bedeutung sind.[191] Die Netzwerksensoren können durch hohe Netz- und Angriffslast sowie durch gezielte Angriffe oder Programmfehler eingeschränkt sein.[192]

Auf den ersten Blick mag die Funktionsweise des NIDS der Funktionsweise der Paketfilter-Firewall ähneln. Jedoch muss ein Paketfilter bei jedem einzelnen ankommenden Paket entscheiden, ob dieses durchgelassen wird oder nicht. NIDS hingegen kann mehrere Ereignisse miteinander vergleichen und so zu wesentlich detaillierten Analysen gelangen. Somit können auch Angriffe erkannt werden, die sich aus zeitversetzten und scheinbar harmlosen Paketen zusammensetzen.[193] Ein NIDS verhält sich zudem passiv und kann von Angreifenden nicht bemerkt werden, wohingegen Paketfilter bereits durch einfache Analysen des Netzwerkverkehres zu entdecken sind.[194] NIDS und Paketfilter-Firewalls sind folglich „komplementäre Mechanismen, die sich gegenseitig ergänzen und nicht ersetzen".[195]

Hostbasierte IDS (HIDS) hingegen untersuchen den Datenverkehr eines Rechners, sie werden direkt auf dem zu überwachenden System betrieben.[196] Sie sollen vor allen Dingen Angriffe erkennen, die auf der Anwendungs- und Betriebssystemebene durchgeführt werden wie beispielsweise Login-Fehlversuche oder Trojaner.[197] Hostsensoren können durch direkte Angriffe beeinträchtigt werden sowie indirekt durch Angriffe auf das zu überwachende System.[198]

(2) Signaturbasierte und anomaliebasierte Angriffserkennung

Bei der Art und Weise, wie IDS Sicherheitsverletzungen erkennen, werden zwei unterschiedliche Ansätze verfolgt: die signaturbasierte (Misuse oder Signature Detection) und die

---

[188] Dehn, *Netzwerke Sicherheit, S. 177.*
[189] Mehler-Bicher u. a., *Wirtschaftsinformatik Klipp und Klar, S. 114; Einführung von Intrusion-Detection-Systemen - Grundlagen, S. 6.*
[190] Kappes, *Netzwerk- und Datensicherheit, S. 233.*
[191] Kappes, *Netzwerk- und Datensicherheit, S. 232.*
[192] *Einführung von Intrusion-Detection-Systemen - Grundlagen, S. 15.*
[193] Kappes, *Netzwerk- und Datensicherheit, S. 235.*
[194] Kappes, *Netzwerk- und Datensicherheit, S. 234.*
[195] Kappes, *Netzwerk- und Datensicherheit, S. 235.*
[196] Mehler-Bicher u. a., *Wirtschaftsinformatik Klipp und Klar, S. 114.*
[197] *Einführung von Intrusion-Detection-Systemen - Grundlagen, S. 7.*
[198] *Einführung von Intrusion-Detection-Systemen - Grundlagen, S. 16.*

anomaliebasierte Angriffserkennung (Anomaly Detection).[199] Zudem gibt es hybride Systeme, die die beiden Ansätze parallel nutzen.[200]

(a) Anomaliebasierte Angriffserkennung

Das Prinzip der anomaliebasierten Angriffserkennung basiert auf der genauen Definition des normalen Verhaltens sowie der charakteristischen Eigenschaften eines Systems und dem Detektieren von Abweichungen dieser Norm.[201] Grundlage hierfür bilden Schwellenwerte, die die Grenzen des Normverhaltens setzen.[202] Die Anomalieerkennung kann selbstlernend oder spezifikationsbasiert erfolgen. Bei spezifikationsbasierten Verfahren wird das Normverhalten des Systems durch einen Administrator oder eine Administratorin anhand von genauen Regeln in die Angriffserkennung einprogrammiert, wohingegen die selbstlernende Anomalieerkennung in einer Lernphase das System beobachtet und hieraus das normale Verhalten ableitet.[203]

Die anomaliebasierte Angriffserkennung hat gegenüber der signaturbasierten Angriffserkennung den Vorteil, auch bisher unbekannte Angriffe detektieren zu können. Zudem ist kein spezifisches Wissen über die Natur der Angriffe für die Detektion erforderlich. Dies erübrigt auch die fortlaufende Einspeisung neuer Wissensstände (Signaturen).[204]

Ein Nachteil der anomaliebasierten Angriffserkennung ist die kontinuierliche Anpassung der Normverhaltensdefinition.[205] Zudem stellt nicht jede Abweichung von der Norm automatisch eine Sicherheitsverletzung dar, was zu ungenauen Ergebnissen führen kann.[206]

(b) Signaturbasierte Angriffserkennung

Ähnlich wie ein Virenscanner arbeitet die signaturbasierte Angriffserkennung mit Datensätzen aus typischen Angriffsszenarien. Jeder registrierte Angriff hat ein für ihn typisches Paketmuster, die Signatur.[207] Diese definiert eine bestimmte Bitfolge, wie sie nur einer Dateneinheit gehören kann, die einen Angriff verkörpert.[208] Das IDS überwacht den laufenden Datenverkehr und meldet eine Sicherheitsverletzung, wenn eine Signaturübereinstimmung erkannt wird. Die Signaturen sind lokal in einer Datenbank gespeichert.[209]

---

[199] Dinger/Hartenstein, *Netzwerk- und IT-Sicherheitsmanagement - Eine Einführung, S. 264;* Winter u. a., *DuD 2011, 235 (235).*
[200] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 17.*
[201] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 1;* Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 200.*
[202] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 19.*
[203] Groß, *Kooperative Angriffserkennung in drahtlosen Ad-hoc- und Infrastrukturnetzen, S. 43.*
[204] Winter u. a., *DuD 2011, 235 (235).*
[205] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 19.*
[206] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 1.*
[207] Dehn, *Netzwerke Sicherheit, S. 176.*
[208] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 17.*
[209] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 18.*

Bei der signaturbasierten Angriffserkennung können jedoch keine Angriffe detektiert werden, die nicht schon als Signatur in der Datenbank gespeichert sind. Zudem nimmt das Erstellen einer neuen Signatur Zeit in Anspruch und gibt neuen Angriffsmustern einen gewissen Zeitraum zum Agieren ohne Erkennungsmöglichkeit. Aufgrund der hohen Datenraten ist der Abgleich der Dateneinheiten mit der Datenbank zudem mit einem hohen Aufwand verbunden.[210] Ist die Signatur eines Angriffes allerdings in der Datenbank eingespeist, ist die Erkennungsgenauigkeit bei einem Angriff sehr hoch und das Angriffserkennungssystem liefert fehlerfreie Ergebnisse.[211] Zudem sind die Chancen auf einen Fehlalarm im Gegensatz zur anomaliebasierten Angriffserkennung deutlich geringer, da nicht jede Abweichung vom alltäglichen Verhalten gleich als Angriff gewertet wird.[212]

(3) Aufbau

Ein IDS ist in drei grundlegende logische Komponenten gegliedert: Der Agent, der Director und der Notifier. Der Agent ist für die Überwachung des Systems zuständig. Die relevanten Daten, die er hierbei sammelt, werden an den Director versendet. Dieser analysiert die Daten auf anomaliebasierter oder signaturbasierter Grundlage. Wird hierbei ein Angriff entdeckt, wird der Notifier benachrichtigt. Dieser wiederum entscheidet, welche aktiven oder passiven Maßnahmen zur Erwiderung des Angriffes eingeleitet werden, wobei unter passiven Maßnahmen die bloße Protokollierung und Benachrichtigung des Nutzers oder der Nutzerin verstanden wird.[213]

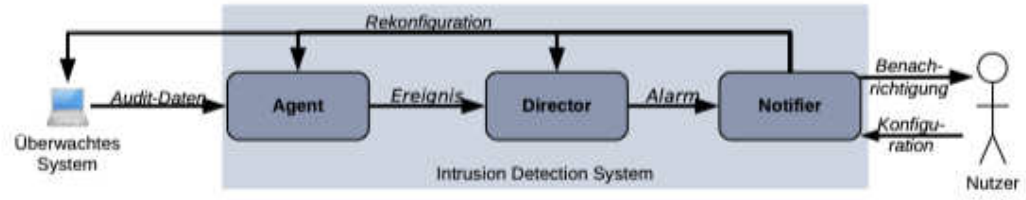

Abbildung 2.7: Allgemeine Architektur eines Intrusion Detection Systems

Abbildung 3: Allgemeine Architektur eines IDS aus Groß, Kooperative Angriffserkennung in drahtlosen Ad-hoc- und Infrastrukturnetzen, S. 44

b) Intrusion-Prevention-Systeme (IPS)

IPS sind eine Weiterentwicklung bzw. Erweiterung der IDS. Hierbei soll durch eine sofortige Gegenreaktion im Falle eines Angriffs die schädlichen Auswirkungen verhindert oder gemindert werden. Die Gegenmaßnahmen changieren je nachdem, ob das IPS hostbasiert oder

[210] Gamer, *Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, S. 18.*
[211] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 2.*
[212] Dehn, *Netzwerke Sicherheit, S. 176.*
[213] Groß, *Kooperative Angriffserkennung in drahtlosen Ad-hoc- und Infrastrukturnetzen, S. 44.*

netzbasiert platziert wurde.[214] In vielen Firewalls und Sicherheitsroutern sind IPS eingebaut, um den Datenstrom, der die Firewall passieren kann, nochmals gezielt auf Angriffe zu untersuchen.[215]

c) Security Incident and Event Management Systeme (SIEM)

SIEM-Systeme werden zu Zwecken der Datensicherheit und der Datenschutzkontrolle eingesetzt.[216] Sie analysieren in Echtzeit die Protokolldateien, die beim Betrieb von IT-Systemen und darauf betriebenen Computerprogrammen sowie dem Betriebssystem anfallen.[217] Diese stammen aus unterschiedlichen Quellen wie beispielsweise Firewalls, Servern, Proxys, Authentifizierungsprotokollen oder Clients verschiedener Hardware, Netzwerkkomponenten sowie Anwendungen.[218] Diese sogenannten log files werden durch SIEM-Systeme an einer zentralen Stelle gesammelt und in Echtzeit ausgewertet.[219] So nimmt beispielsweise bei Webservern eine spezielle Software wie der Apache HTTP Server Anfragen der Nutzer und Nutzerinnen entgegen und verarbeitet und beantwortet diese. Über diese Tätigkeiten wird standardgemäß von der Software ein Ereignisprotokoll geführt, das log file.[220] Zudem können auch IDS und IPS die Events in ein SIEM-System liefern.[221] Durch die Analyse sollen Anomalien, wie beispielsweise falsche Anmeldeversuche, und somit Angriffe erkannt werden.[222]

d) Notwendige Daten

Damit IDS arbeiten können, müssen Informationen über Abläufe oder Zustände des Netzwerkes aufgezeichnet werden, die für die Sicherheit ebendiesem relevant sind. Verfahren zur Protokollierung und zur Analyse werden Audit genannt. Der Informationsgehalt dieser Auditdateien stellt die Basis der Qualität der IDS-Ergebnisse dar, da sie die Grundlage der Analyse des IDS bilden.[223] Audits können in zustandsbasierte sowie transitions- bzw. aktionsbasierte Audits unterteilt werden. Während zustandsbasierte Audits Informationen über den Zustand des IT-

---

[214] Dinger/Hartenstein, *Netzwerk- und IT-Sicherheitsmanagement - Eine Einführung, S. 264.*
[215] Dehn, *Netzwerke Sicherheit, S. 178.*
[216] Kort, *NZA 2011, 1319 (1319).*
[217] Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 38.*
[218] heise online, *Höhere Sicherheit mit wenig Aufwand: Wie innovative SIEM-Lösungen helfen, Cyber-Angriffe abzuwehren.*
[219] Kort, *NZA 2011, 1319 (1319);* heise online, *Höhere Sicherheit mit wenig Aufwand: Wie innovative SIEM-Lösungen helfen, Cyber-Angriffe abzuwehren.*
[220] Auer-Reinsdorff/Conrad, *Handbuch IT- und Datenschutzrecht§ 36 Rn 125.*
[221] Casper/Strobel, *iX 2018, (44);* Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 38.*
[222] Benner, *ZD-Aktuell 2017, 05556;* heise online, *Höhere Sicherheit mit wenig Aufwand: Wie innovative SIEM-Lösungen helfen, Cyber-Angriffe abzuwehren.*
[223] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 10.*

Systems liefern, zeichnen transitions- bzw. aktionsbasierte Audits Informationen über sicherheitsrelevante Aktivitäten (Wer? Wann? Wie?) im IT-System auf.[224]

IDS sind grundsätzlich so ausgelegt, dass sämtliche Daten, die im Rahmen von Kommunikationsvorgängen anfallen können, automatisiert erhoben und verarbeitet werden mit dem Ziel, auffällige Datenpakete identifizieren zu können.[225] Hierbei wird nicht stichprobenartig vorgegangen, sondern der gesamte Datenstrom wird in Echtzeit analysiert.[226] Jeglichen Arten von IDS ist hierbei gemeinsam, dass sie zur Erkennung auf die Audit-Daten der bestehenden IT-Systeme Zugriff haben müssen.[227]

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verweist in seinem Leitfaden zur Einführung von IDS darauf, dass IDS eine Vielzahl von Daten aufzeichnen, die in Teilen einen Personenbezug herstellen bzw. herstellen lassen. Insbesondere beim Einsatz eines IDS zur Überwachung von internen Netzen kann von einer hohen Dichte an personenbezogenen Daten ausgegangen werden.[228]

Fraglich ist, ob unter die für Nutzung eines IDS notwendigen Daten auch die IP-Adressen der Netzwerknutzer fallen oder ob eine Speicherung der IP-Adressen im Rahmen der Angriffserkennung nicht vonnöten ist. Unumstritten ist, dass die alleinige Speicherung von IP-Adressen für eine verlässliche Identifizierung von Angreifenden nicht ausreichend ist.[229] Quell-IP-Adressen sind leicht fälschbar durch frei verfügbare Anonymisierungsdienste und verbergen den ursprünglichen Absender.[230] IDS, die als Maßnahme zum Schutz des Internet-Übergangs eingesetzt werden, liegen bei einem Angriff grundsätzlich nur die IP-Adressen vor. Die Zuordnung der IP-Adresse zu einer bestimmten Person ist jedoch aufgrund temporär eingerichteter oder gefälschter IP-Adressen oftmals nicht möglich.[231] Abgesehen hiervon kann das Speichern von IP-Adressen notwendig sein, um nationale und internationale Empfehlungen und Standards zu erfüllen. Hier wird eine Speicherung von IP-Adressen zur Gewährleistung der Auditierbarkeit des Systems verlangt.[232]

SIEM-Systeme analysieren sämtliche log-files eines IT-Systems, inklusive der darauf betriebenen Anwendungen sowie des Betriebssystems.

---

[224] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 11.*
[225] Krügel, *MMR 2017, 795 (796).*
[226] Miller, *NdsVBl 2021, 1 (2).*
[227] Meier, *IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, S. 9.*
[228] BSI, *BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen (IDS) - Rechtliche Aspekte beim Einsatz von IDS.*
[229] *Sachverständigengutachten zu 57 S 87/08 https://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2011-07-29_Sachverst_an_LG.pdf, S. 3.*
[230] *Sachverständigengutachten zu 57 S 87/08 https://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2011-07-29_Sachverst_an_LG.pdf, S. 5.*
[231] BSI, *BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen (IDS) - Rechtliche Aspekte beim Einsatz von IDS.*
[232] *Sachverständigengutachten zu 57 S 87/08 https://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2011-07-29_Sachverst_an_LG.pdf, S. 11.*

Grundsätzlich ist allen drei Arten von Angriffserkennungssystemen gemein, dass sie die gesamten Datenströme in Echtzeit auswerten und entsprechend große Mengen an geschützten Daten verarbeiten.[233]

C. Das Krankenhaus in privater Trägerschaft als Betrachtungsgegenstand

In dieser Arbeit wird untersucht, ob eine Rechtfertigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft vorliegt.

Für das bessere Verständnis wird im Folgenden ein Überblick über die Situation im krankenhäuslichen Versorgungssektor in Deutschland gegeben sowie rechtliche Organisationsmöglichkeiten für Krankenhäuser erläutert.

In Deutschland können sich Krankenhausbetreibende öffentlich-rechtlich, freigemeinnützig oder privatrechtlich organisieren und somit in diversen Rechtsformen geführt werden, wobei die Rechtsform der GmbH am häufigsten gewählt wird.[234] Die Anzahl der Krankenhäuser ist in Deutschland in den vergangenen Jahren stetig zurückgegangen. So stehen im Jahr 2010 2.062 Krankenhäuser mit insgesamt 502.749 Betten in 2019 1.914 Krankenhäusern und 494.326 Betten entgegen, was rund 8 Prozent weniger Krankenhäuser und 2 Prozent weniger Betten ausmacht. Während sich in 2010 noch 29,4 Prozent aller Krankenhäuser in Deutschland in privater Trägerschaft befanden, waren es im Jahr 2019 bereits 37, 2 Prozent aller Krankenhäuser. 33,8 Prozent der Krankenhäuser sind 2019 freigemeinnützig, während sich 29,1 Prozent der Krankenhäuser in öffentlicher Trägerschaft befinden. Von den aufgestellten Betten in 2019 fallen jedoch nur 18,4 Prozent auf Krankenhäuser in privater Trägerschaft.[235]

Die Trägerschaft kann von einer natürlichen oder juristischen Person wahrgenommen werden. Sie kann öffentlich, freigemeinnützig oder privat organisiert sein. **Öffentliche Krankenhausträger** können Bund, Länder oder kommunale Gebietskörperschaften sein, der oder die Betreibende des Krankenhauses ist eine Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts. Hierzu gehören auch die von öffentlich-rechtlichen Institutionen beherrschten Krankenhäuser in privatrechtlicher Gesellschaftsform. **Freigemeinnützige Träger** sind einer religiösen, humanitären oder sozialen Vereinigung zuzuordnen, die das Krankenhaus auf der Grundlage der Freiwilligkeit und gemeinnützig, also ohne Absicht der Gewinnerzielung betrieben. Hierzu gehören karitative Organisationen, kirchliche Orden und Kongregationen sowie gemeinnützige Vereine und Stiftungen wie beispielsweise die Caritas und das Deutsche Rote Kreuz.[236]

---

[233] Miller, *NdsVBl 2021, 1 (2).*
[234] Eisenreich, *Digitalisierung im Krankenhaus: Entwicklung und Validierung eines konzeptionellen Akzeptanzmodells im Rahmen der Implementierung eines Krankenhausinformationssystems in einer Universitätsklinik, S. 13.*
[235] Deutsche Krankenhaus Gesellschaft, *Krankenhausstatistik - Eckdaten der Krankenhausversorgung.*
[236] Deutscher Bundestag, *Ausarbeitung: Krankenhäuser in privater Trägerschaft – Rechtsgrundlagen, verfassungsrechtliche Vorgaben und Finanzierung, S. 27.*

Krankenhäuser in **privater Trägerschaft** hingegen werden von natürlichen Personen, von einer juristischen Person des Privatrechts oder von einer rechtsfähigen Gesamthandsgemeinschaft des privaten Rechts mit Gewinnerzielungsabsicht betrieben. Private Krankenhausträger können ein rechtsfähiger Verein, eine Stiftung des Privatrechts, eine Gesellschaft mit beschränkter Haftung (GmbH), eine Aktiengesellschaft (AG), eine Gesellschaft bürgerlichen Rechts (GbR) eine Offene Handelsgesellschaft (OHG) oder eine Kommanditgesellschaft (KG) sein.[237] Krankenhäuser in privater Trägerschaft sind nicht gleichzusetzen mit „Privatkliniken". Diese haben im Unterschied zu Krankenhäusern in privater Trägerschaft keine Kassenzulassung i.S.d. SGB V und sind nicht zur Teilnahme an der gesetzlichen Krankenversorgung berechtigt.[238]

Laut der Deutschen Krankenhausgesellschaft bestehen bei der medizinischen Versorgung eine Reihe von branchenspezifischen Gefährdungsszenarien, die vor allem auf die unterstützenden IT-Systeme zurückzuführen sind. Es sind folglich besondere Anforderungen an die Patienten- und Patientinnensicherheit und die Behandlungseffektivität zu stellen.[239]

Um die Digitalisierung in Krankenhäusern voran zu treiben, wurde im Rahmen des Krankenhauszukunftsgesetzes (KHZG) ein Investitionsprogramm geschaffen, durch das ab Januar 2021 hohe Geldsummen zur Modernisierung, Digitalisierung sowie den Ausbau der IT-Sicherheit in Krankenhäusern bereitgestellt wurden.[240]

Folgend werden – kontextbezogen auf den Gesundheitssektor – spezialrechtliche Anforderungen an Kritische Infrastrukturen (KRITIS) vorgestellt. Unter den Begriff fallen bei Vorliegen bestimmten Voraussetzungen auch Krankenhäuser. Zudem werden die gängigen nationalen und internationalen Standards für die IT-Sicherheit, bezogen auf die speziellen Umstände im Krankenhauskontext, vorgestellt.

1. Rechtsgrundlagen für die IT-Sicherheitsanforderungen an KRITIS

Die Rechtsgrundlage für KRITIS bildet auf nationaler Ebene das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), welches durch die BSI-Kritisverordnung (BSI-KritisV) konkretisiert wird. Das Artikelgesetz „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" erweitert unter anderem das BSIG.

---

[237] Deutscher Bundestag, *Ausarbeitung: Krankenhäuser in privater Trägerschaft – Rechtsgrundlagen, verfassungsrechtliche Vorgaben und Finanzierung, S. 28.*
[238] Deutscher Bundestag, *Ausarbeitung: Krankenhäuser in privater Trägerschaft – Rechtsgrundlagen, verfassungsrechtliche Vorgaben und Finanzierung, S. 30.*
[239] DKG, *Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, S. 46.*
[240] Bundesministerium für Gesundheit, *Krankenhauszukunftsgesetz für die Digitalisierung von Krankenhäusern.*

Auf europäischer Ebene wurde im Juli 2016 die EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-Richtlinie) im Amtsblatt der europäischen Union veröffentlicht. Da bereits viele der Anforderungen durch das im Jahr 2015 in Kraft getretene IT-Sicherheitsgesetz umgesetzt wurden, wurde im Juni 2017 das NIS-Richtlinien-Umsetzungsgesetz veröffentlicht.[241]

Im Folgenden werden die wesentlichen Bestandteile der Rechtsgrundlagen sowie deren Beziehung zueinander aufgezeigt.

a) BSIG und BSI-KritisV

Anhand des BSIG wird das Ziel verfolgt, die IT-Sicherheit von KRITIS und somit den Schutz des Allgemeinwohls zu gewährleisten.[242] Es verpflichtet den oder die Betreibenden Kritischer Infrastrukturen zur Einhaltung eines Mindestniveaus an IT-Sicherheit und sieht eine Meldepflicht von IT-Sicherheitsvorfällen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gegenüber vor.[243] Zum Adressaten- und Adressatinnenkreis zählen auch medizinische Leistungsträger wie beispielsweise Krankenhäuser, Hersteller von Medizinprodukten und Arzneimitteln sowie Apotheken, soweit diese im Rahmen ihrer Tätigkeit bestimmte Schwellwerte überschreiten.[244]

Gemäß § 8a I BSIG sind Betreibende Kritischer Infrastrukturen dazu verpflichtet, „*angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. 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.*“ Laut Absatz 1a gehören zu den geforderten Verpflichtungen ab dem 1. Mai 2023 auch der Einsatz von Angriffserkennungssystemen. Diese „*müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen*“. Zudem können internationale sowie nationale Standards bei der Ausgestaltung am Stand der Technik unterstützen. Auch können nach § 8a II BSIG eigene branchenspezifische Sicherheitsstandards von den Betreibenden Kritischer Infrastrukturen vorgeschlagen werden[245] (sog. B3S).[246]

---

[241] Bundesamt für Sicherheit in der Informationstechnik.
[242] Jorzig/Sarangi, *Digitalisierung im Gesundheitswesen, S. 82.*
[243] Dürig/Fischer, *DuD 2018, 209 (211).*
[244] Jorzig/Sarangi, *Digitalisierung im Gesundheitswesen, S. 83.*
[245] Dürig/Fischer, *DuD 2018, 209 (212).*
[246] *Für weiterführende Informationen wird auf das Kapitel „Nationale und internationale Standards“ verwiesen.*

Die Deutsche Krankenhausgesellschaft (DKG) hat von dieser Möglichkeit Gebrauch gemacht und 2019 den **branchenspezifischen Sicherheitsstandard (B3S) für die medizinische Versorgung veröffentlicht**, der gemäß Feststellungsbescheid vom 22. Oktober 2019 zur Gewährleistung der Anforderungen nach § 8a I BSIG geeignet ist. Der B3S für medizinische Versorgung orientiert sich an der Norm ISO 27001, dem Stand der Technik sowie den branchenspezifischen Anforderungen der Norm ISO 27799.[247] Im Rahmen der Technischen Informationssicherheit wird hierbei im B3S ausdrücklich auf die Nutzung von IDS sowie IPS eingegangen. So soll laut Abschnitt ANF-MN 106 *„ein System zur Vorbeugung und Erkennung von nicht authorisierten Zugriffsversuchen auf das Netzwerk und die Systeme des Krankenhauses implementiert werden, das neben dem Verhindern unberechtigter Zugriffsversuche (z. B. durch Firewall) auch den prinzipiell erlaubten Netzwerkverkehr auf gefährliche Inhalte kontrolliert".* Zudem müssen laut ANF-MN 107 *„regelmäßige Überprüfungen auf Schwachstellen des eigenen Netzes erfolgen, um sowohl externe Angriffsmöglichkeiten zu identifizieren, als auch interne Schwachstellen zu erkennen, die aufgrund eines Firewallschutzes (derzeit) nicht zu einer direkten Gefährdung führen."*[248] Was in Bezug auf den B3S für medizinische Versorgung auffällt, ist die Wortwahl bei der Angriffserkennung. So „sollen" Systeme zur Vorbeugung und Erkennung von nicht authorisierten Zugriffsversuchen implementiert werden. Der B3S für medizinische Versorgung stuft in seinem Maßnahmenkatalog die Dringlichkeit der Umsetzung nach „Muss"-Maßnahmen, „Soll"-Maßnahmen und „Kann"-Maßnahmen ein. Im Rahmen der „Deklaration von Anforderungen innerhalb des B3S" wird im B3S für medizinische Versorgung definiert, dass „Muss"-Anforderungen zwingend umzusetzen sind, die Einhaltung von „Soll"-Anforderungen ist hingegen nur grundsätzlich erforderlich. Auf die Umsetzung kann verzichtet werden, wenn hierdurch die Informationssicherheit nicht gefährdet wird und dies nachvollziehbar begründet wird. Die Einhaltung von „Kann"-Anforderungen wird empfohlen, ist jedoch nicht zwingend für die Umsetzung des Standards. Die Legaldefinitionen des B3S für medizinische Versorgung decken sich mit dem allgemeinen juristischen Verständnis dieser Begriffe, wonach „Muss"-Vorschriften eine gebundene Entscheidung ohne Ermessensspielraum darstellen, wohingegen „Kann"-Vorschriften auf einen Ermessensspielraum hinweisen. „Soll"-Vorschriften hingegen verpflichten in der Regel, können aber in Ausnahmesituationen einen gewissen Ermessensspielraum einräumen. Zudem ist die Rechtsfolge eines Verstoßes gegen „Soll"-Vorschriften oftmals nicht so schwerwiegend wie der Verstoß gegen „Muss"-Vorschriften.[249] Hieraus lässt sich herleiten, dass im Gesamtkontext des B3S für medizinische Versorgung die Implementierung von Angriffserkennungssystemen zwar als durchaus wichtig eingestuft wird, allerdings nicht zu den notwendigsten Maßnahmen für die Sicherstellung der IT-Sicherheit in Krankenhäusern gehört.

---

[247] Deutsche Krankenhaus Gesellschaft, *Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, S. 10.*
[248] Deutsche Krankenhaus Gesellschaft, *Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, S. 74.*
[249] Bundesministerium der Justiz, *Handbuch der Rechtsförmlichkeit Rn 82-84.*

§ 8b I BSIG weist das BSI als *„die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik“* aus. Vorgesehen ist ein bilateraler Informationsaustausch zwischen dem BSI und den Betreibenden Kritischer Infrastrukturen.[250] Hierfür sind im § 8b II BSIG dem Bundesamt umfangreiche Aufgaben übertragen wurden. Zudem haben Betreibende Kritischer Infrastrukturen nach Absatz III eine Kontaktstelle zu benennen und unterliegen nach Absatz IV einer Meldepflicht bei erheblichen Störungen der IT-Sicherheit.

Auf Grundlage des § 10 I BSIG wurde im Mai 2016 die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSIG (BSI-KritisV) erlassen und im Juni 2017 erweitert. Die BSI-KritisV enthält ein Rahmenwerk zur Identifikation Kritischer Infrastrukturen anhand von Schwellwerten. Sie verpflichtet die Betreibenden Kritischer Infrastrukturen auf Grundlage transparenter Kriterien zur Feststellung, ob der jeweilige Betrieb den Schwellenwert einer KRITIS überschreitet.[251]

b) IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz ist ein Artikelgesetz, das neben dem BSIG auch insbesondere das Energiewirtschaftsgesetz, das Telemediengesetz und das Telekommunikationsgesetz ändert und ergänzt.[252] Mit Inkrafttreten des IT-Sicherheitsgesetzes im Juli 2015 wurde das BSI als zentrale Stelle für die IT-Sicherheit bestimmt.[253]

Im Mai 2021 wurde dieses durch ein Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz 2.0**) ersetzt. Unter anderem wurde im Rahmen der Novellierung die Rolle des BSI durch die Schaffung des § 4b BSIG deutlich gestärkt.[254] Zudem werden Angriffserkennungssysteme erstmals in § 8a Ia BSIG als angemessene organisatorische und technische Vorkehrungen zur IT-Sicherheit benannt. Diese müssen nach Satz 2 *„geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten“.* Zudem sollten sie *„dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen“.* Angriffserkennungssysteme sind nach der Legaldefinition des § 2 9b BSIG *„durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten“*.

---

[250] Dürig/Fischer, *DuD 2018, 209 (212).*
[251] Dürig/Fischer, *DuD 2018, 209 (212).*
[252] Deutsche Krankenhaus Gesellschaft, *Krankenhäuser als kritische Infrastrukturen - Umsetzungshinweise der Deutschen Krankenhausgesellschaft, S. 6.*
[253] Tschammler, *PharmR 2019, 509 (509).*
[254] Kipker/Scholz, *MMR 2019, 431 (431).*

c) NIS-Richtlinie und NIS-Richtlinien-Umsetzungsgesetz

Die NIS-Richtlinie bildet das europäische Rahmenwerk für ein mitgliedstaatenübergreifendes gemeinsames IT-Sicherheitsniveau.[255] Für Betreibende wesentlicher Dienste sieht die NIS-Richtlinie diverse Sicherheitsanforderungen sowie Meldepflichten vor, wobei die Mitgliedstaaten bei der nationalen Umsetzung strengere Anforderungen stellen können. Laut Legaldefinition des Art. 4 Ziff. 4 RL i.V.m. Anhang II RL sind Betreibende wesentlicher Dienste unter anderem *„öffentliche oder private Einrichtungen der Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung und -versorgung“.* Durch Art. 14 I, II RL werden die Mitgliedstaaten dazu verpflichtet sicherzustellen, dass die Betreibende wesentlicher Dienste entsprechende „geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die IT-Sicherheit ihrer Systeme zu schützen“. Sicherheitsvorfälle sind nach Art. 14 III RL unverzüglich zu melden.[256]

Auf nationaler Ebene hat die Legislative die Vorgaben der NIS-Richtlinie, die im IT-Sicherheitsgesetz bisher noch nicht oder nur ungenügend geregelt wurden, im Rahmen des NIS-Richtlinien-Umsetzungsgesetzes umgesetzt. So wurden Änderungen an § 8a sowie § 8b des BSIG vorgenommen.[257] In Gänze ist die NIS-Richtlinie durch das IT-Sicherheitsgesetz, das NIS-Richtlinien-Umsetzungsgesetz sowie die BSI-KritisV im deutschen Recht umgesetzt.[258]

Am 16. Dezember 2020 hat die EU-Kommission zusammen mit der neuen EU-Cybersicherheitsstrategie „The EU’s Cybersecurity Strategy for the Digital Decade“ den Entwurf einer neuen NIS-2-Richtlinie vorgestellt. Diese basiert auf den Grundlagen und Erfahrungen der ersten NIS-Richtlinie, beinhaltet jedoch auch Anforderungs- und Maßnahmenverschärfungen sowie Kontroll- und Sanktionsmöglichkeiten. Zudem soll der Anwendungsbereich ausgeweitet werden.[259]

Im Entwurf werden die Vorgaben zur IT-Sicherheit in Art. 18 aufgegriffen, der in seinen Absätzen 1 bis 4 teilweise Art. 14 NIS-RL entspricht. Art. 18 II bis IV NIS-2-RL-E konkretisiert die Maßnahmen, die für die Anforderung zu treffen sind.[260]

2. Kritische Infrastruktur Krankenhaus

Kritische Infrastrukturen (KRITIS) zeichnen sich durch ihre besondere Relevanz für die Versorgung der deutschen Märkte aus.[261] Laut § 2 X BSIG können KRITIS jedoch nur

[255] Dürig/Fischer, *DuD 2018, 209 (209).*
[256] Dürig/Fischer, *DuD 2018, 209 (210).*
[257] Dürig/Fischer, *DuD 2018, 209 (213).*
[258] Dürig/Fischer, *DuD 2018, 209 (212).*
[259] Kipker u. a., *MMR 2021, 214 (214).*
[260] Kipker u. a., *MMR 2021, 214 (216).*
[261] Tschammler, *PharmR 2019, 509 (510).*

Einrichtungen, Anlagen oder Teile sein, die den Sektoren *„Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen“* angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Ein weiterer Zuschnitt des KRITIS-Begriffs erfolgt dann durch die BSI-KritisV.

Gem. § 6 i.V.m. Anhang 5 Teil 3 BSI-Kritisverordnung zählen Krankenhäuser ab 30.000 Behandlungsfällen pro Jahr zu den kritischen Infrastrukturen. Zur Ermittlung der Behandlungsfälle ist eine anlagenbezogene Betrachtung und keine geschäftsbezogene Betrachtung vorzunehmen. Es muss somit jede Anlage individuell auf ihren KRITIS-Status geprüft werden. Zudem bezieht sich die KRITIS-Prüfung auf das Kalenderjahr. Wird der Schwellenwert erreicht, gilt der KRITIS-Status ab April des folgenden Jahres.[262]

In Deutschland fallen ca. 110 Krankenhäuser unter den KRITIS-Begriff, was laut der Deutschen Krankenhausgesellschaft (DKG) für das Jahr 2017 ca. 5 bis 10 % der Krankenhäuser in Deutschland ausmacht.[263] Zudem fallen 151 Apotheken und Betriebsstätten zur Entnahme, Weiterverarbeitung und Lagerung von Blutspenden, 105 Einrichtungen aus der Laboratoriumsdiagnostik und zwei Hersteller beziehungsweise Herstellerinnen von unmittelbar lebenswichtigen Medizinprodukten unter den Begriff der Kritischen Infrastruktur.[264] Das Lukaskrankenhaus in Neuss, das im Februar 2016 Opfer eines Cyber-Angriffs durch ein Schadprogramm wurde[265], fällt mit einer Quote von 28.500 behandelten Patienten und Patientinnen pro Jahr beispielsweise nicht unter die besonderen Sicherheits- und Schutzanforderung der kritischen Infrastrukturen.[266]

3. Nationale und internationale Standards

Wie bereits erwähnt, können internationale sowie nationale Standards bei der Ausgestaltung der IT-Sicherheit am Stand der Technik nach § 8a I BSIG herangezogen werden. Zudem können Betreibende Kritischer Infrastrukturen eigene branchenspezifische Standards erarbeiten (sog. B3S) und nach § 8a II BSIG auf ihre Eignung durch das BSI prüfen lassen.

Im Folgenden werden die wichtigsten nationalen und internationalen Standards im Bereich der IT-Sicherheit im Gesundheitswesen kurz vorgestellt, gefolgt vom B3S-Standard der Deutschen Krankenhausgesellschaft (DKG).

Der Standard **ISO/IEC 27001** umfasst die Absicherung der IT-Infrastruktur mithilfe eines Informationssicherheits-Managementsystem (ISMS). Dieses wird nicht nur beschrieben, Betreibende Kritischer Infrastrukturen können bei entsprechendem Nachweis eines ISMS ein

[262] Tschammler, *PharmR 2019, 509 (511).*
[263] Jorzig/Sarangi, *Digitalisierung im Gesundheitswesen, S. 85.*
[264] Ärzteblatt, *Kritische Infrastruktur.*
[265] Bundesamt für Sicherheit in der Informationstechnik, *Die Lage der IT-Sicherheit in Deutschland 2016, S. 39.*
[266] Ärzteblatt, *Kritische Infrastruktur.*

Zertifikat bei einem zertifizierten Auditor oder auf der Basis des IT-Grundschutzes beim BSI erlangen.[267]

Der Standard **ISO/IEC 27002** beinhaltet eine Liste von allgemein anerkannten Kontrollzielen und Best Practices in Bezug auf die IT-Sicherheit im medizinischen Kontext. In Gänze werden 114 Maßnahmen benannt. Da die ISO/IEC 27002 keine Anforderungen beinhaltet, ist eine Zertifizierung nach ISO/IEC 27002 nicht möglich.[268]

Ein systematisches Verfahren zur Durchführung einer Risikoanalyse zur Behandlung von IT-Risiken gibt der Standard **ISO/IEC 27005**. Hierdurch können, insbesondere im Zusammenhang mit der Implementierung eines ISMS nach ISO/IEC 27001, Risiken bewertet und Zusammenhänge transparent gemacht werden.[269]

Der Standard **ISO/IEC 27789** enthält die Vorgehensweise bei der Erzeugung, Aktualisierung und Archivierung von sicheren Audit-Einträgen, die für Informationssysteme, die persönliche Gesundheitsinformationen enthalten, verpflichtend ist.[270]

Insbesondere für Krankenhäuser und Kliniken ist der Standard **ISO/IEC 27799** von Bedeutung. Da die Normenreihe ISO 27000 allgemein gehalten ist, geht die ISO/IEC 27799 detailliert auf die Besonderheiten der medizinischen Informatik sowie deren Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 ein.[271]

Der Standard **IEC EN 80001** unterstützt bei der Anwendung eines Risikomanagements beim Betrieb von medizinischen Netzwerken. Neben der Erläuterung von Rollen und Verantwortlichkeiten werden Aufgaben und Aktivitäten im Rahmen des Risikomanagements festgelegt. Die Norm bildet den Stand der Technik ab und wird ausdrücklich für die Betreibende medizinischer IT-Netzwerke, das heißt für Krankenhäuser oder Kliniken, empfohlen.[272]

Auf nationaler Ebene stellt das BSI anhand des **IT-Grundschutzes** eine Vorgehensweise zur Identifizierung und Umsetzung von Sicherheitsmaßnahmen in IT-Netzwerken. Hierbei bilden die BSI-Standards durch die enthaltenen Methoden und Vorgehensweisen zu den unterschiedlichsten Themen aus dem Bereich der Informationssicherheit das Fundament. Das IT-Grundschutz-Kompendium hingegen enthält darauf aufbauend prozess- und systembezogene Bausteine zur Umsetzung der IT-Grundschutz-Methodik.[273] Im Vergleich zu den Standards der ISO

---

[267] Darms u. a., *IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker, und Geschäftsführer in Klink und Praxis, S. 166.*
[268] Darms u. a., *IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker, und Geschäftsführer in Klink und Praxis, S. 167.*
[269] Darms u. a., *IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker, und Geschäftsführer in Klink und Praxis, S. 167.*
[270] Darms u. a., *IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker, und Geschäftsführer in Klink und Praxis, S. 167.*
[271] Darms u. a., *IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker, und Geschäftsführer in Klink und Praxis, S. 168.*
[272] Darms u. a., *IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker, und Geschäftsführer in Klink und Praxis, S. 169.*
[273] BSI, *Über den IT-Grund-schutz.*

ist der IT-Grundschutz deutlich konkreter und detaillierter, da nicht nur die Anforderungen, sondern auch Umsetzungsmöglichkeiten beschrieben werden.[274]

Zudem können Betreibende Kritischer Infrastrukturen nach § 8a II BSIG branchenspezifische Sicherheitsstandards (**B3S**) vorschlagen, die im Anschluss durch das BSI im Rahmen einer Eignungsprüfung bewertet werden. Sobald eine Eignung des Entwurfs durch das BSI festgestellt wurde, handelt es sich um einen für die jeweilige Branche anerkannten Sicherheitsstandard. So entstandene B3S sollen als nicht bindende Orientierungshilfe für Betreibende Kritischer Infrastrukturen dienen und den Umgang mit den Sicherheits- und Nachweispflichten des BSI erleichtern.[275]

III. Verfassungsrechtliche Bewertung

Ob es für die rechtmäßige Nutzung von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft einer gesetzliche Ermächtigungsgrundlage bedarf, muss zunächst verfassungsrechtlich geprüft werden. Würde die Nutzung entsprechender Systeme in die Grundrechte der Patienten, Patientinnen und Mitarbeitenden eingreifen, müsste dieser Eingriff aufgrund des Vorbehalts des Gesetzes per Gesetz gerechtfertigt sein. Die europäische DS-GVO könnte eine solche Ermächtigungsgrundlage darstellen beziehungsweise den Raum für eine speziellere nationale Regelung öffnen. In diesem Kapitel wird deshalb untersucht, in welchem Verhältnis die europäischen Grundrechte zu den Grundrechten der Mitgliedstaaten stehen und welche Grundrechtsebene im Anwendungsbereich der DS-GVO im Allgemeinen und ihren Öffnungsklauseln im Speziellen greift. Anschließend wird diskutiert, ob Betreibende privatrechtlich strukturierter Krankenhäuser als Privatrechtssubjekte in ihrer Tätigkeit überhaupt grundrechtgebunden sind. Abschließend wird geprüft, ob die Nutzung von Angriffserkennungssystemen in den Schutzbereich der Grundrechte der entsprechend anwendbaren Verfassung eingreift und somit eine rechtfertigende Ermächtigungsgrundlage für die Nutzung von Angriffserkennungssystemen in den Netzwerken notwendig ist.

A. Das Verhältnis der europäischen Grundrechte-Charta zu den deutschen Grundrechten

Die grundlegende Auffassung zur Vorrangstellung von Unionsrecht vor nationalem Recht ist geprägt von den Entscheidungen „Van Gend & Loos“ und „Costa/ENEL“. Seitdem tritt das nationale Recht der Mitgliedstaaten im konkreten Kollisionsfall hinter dem Unionsrecht zurück und ruht, ohne dadurch beseitigt zu werden. Entscheidendes Argument und dogmatische Basis

[274] Darms u. a., *IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker, und Geschäftsführer in Klink und Praxis, S. 84.*
[275] Tschammler, *PharmR 2019, 509 (511).*

für diesen Anwendungsvorrang ist die Integrationsfunktion des Unionsrecht, deren Ziel ein vereintes Europa darstellt. [276]

Strittig ist indes, ob der generelle Anwendungsvorrang von Unionsrecht auch die Ebene der Grundrechte beherrscht. Denn ebenso wie auf nationaler Ebene, existiert auch auf der Ebene der Europäischen Union ein Katalog verbindlicher Grundrechte in Form der „Charta der Grundrechte der Europäischen Union". Die Europäische Grundrechte-Charta soll einen unionalen Grundrechtsschutz gewährleisten und ist somit unstrittig nicht anwendbar, wenn die Mitgliedstaaten allein in ihrer nationalen Zuständigkeit handeln. Hier gelten nach wie vor die entsprechenden nationalen Grundrechte. [277] Führen die Mitgliedstaaten indes Unionsrecht aus, ist für die Beurteilung des Anwendungsvorrangs zwischen zwingendem Unionsrecht und Unionsrecht mit Gestaltungsspielraum zu unterscheiden.

1. Zwingendes Unionsrecht

Während die Grundrechte der deutschen Verfassung unmittelbar die deutsche öffentliche Gewalt nach Art. 1 III GG binden, binden die europäischen Grundrechte nach Art. 51 I GRCh die Organe der Union und die Mitgliedstaaten bei der Durchführung des Rechts der Union.[278] Da die Grundrechte-Charta keinen gemeinsamen Grundrechtskatalog der Union und ihrer Mitgliedstaaten darstellt, sind die Mitgliedstaaten – anders als bei der EMRK – nicht bei jeder hoheitlichen Tätigkeit an diese gebunden, sondern ausschließlich bei der Durchführung von europäischem Recht.[279] Eine Durchführung i.S.v. Art. 51 Abs. 1 Satz 1 GRCh liegt vor, wenn es um die Umsetzung oder den Vollzug zwingenden Unionsrechts durch die mitgliedstaatliche Legislative, Exekutive oder Judikative geht.[280] Dass in diesem Fall die nationalen Grundrechte der Mitgliedstaaten keine Anwendung finden, hat das BVerfG in der sogenannten **Solange II-Entscheidung** festgestellt.[281] Das nationale Recht tritt in einem Kollisionsfall hinter den europäischen Grundrechten zurück und ruht, ohne dabei beseitigt zu werden.[282] Solange die Europäische Gemeinschaft einen „wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften generell gewährleistet", wird dieses Recht vom BVerfG „mithin nicht mehr am Maßstab der Grundrechte des Grundgesetzes überprüft". [283] Sobald der europäische Grundrechtsschutz allerdings unter ein unabdingbares Mindestniveau sinkt, kann das nationale Grundgesetz wieder angewendet werden.[284] Das europäische Recht hat demnach keinen „Geltungsvorrang" gegenüber dem deutschen Recht, sondern lediglich einen

[276] Kirchhof, *NVwZ 2014, 1537 (1537).*
[277] Meyer, *Charta der Grundrechte der Europäischen Union Kommentar GRCh Art. 51 Rn 36.*
[278] Papier, *NJW 2017, 3025 (3026).*
[279] Schmitz, *EuR 2004, 691 (695);* Meyer, *Charta der Grundrechte der Europäischen Union Kommentar GRCh Art. 51 Rn 37.*
[280] Katsivelas, *MMR 2017, 286 (287).*
[281] Härtel, *LKV 2019, 49 (54);* Safferling, *NStZ 2014, 545 (547).*
[282] Kirchhof, *NVwZ 2014, 1537 (1537).*
[283] Vgl. Solange II, BVerfGE 73, 339.
[284] Bäcker, *EuR 2015, 389 (391).*

„Anwendungsvorrang“, der auch hier dem Integrationsgedanken der Europäischen Union folgt.[285] Dieser Anwendungsvorrang wird auch vom EuGH in dessen Rechtsprechung bestätigt[286] und als „agency situation“ bezeichnet, in der die Mitgliedstaaten als verlängerter Arm der EU tätig werden.[287] Kritischen Stimmen, die im Wortlaut des Art. 51 I GRCh keine Kollisionsregel sehen, sondern lediglich eine Bestimmung, welche Organe der Mitgliedstaaten die Grundrechte-Charta zu beachten haben und einen Anwendungsvorrang im Kollisionsfall in einem weiteren Schritt nach anderen Gesichtspunkten beurteilen wollen[288], ist aufgrund der Auslegung von EuGH und BVerfG zu widersprechen.

2. Unionsrecht mit Gestaltungsspielraum

Eröffnet das Unionsrecht den Mitgliedstaaten Gestaltungsspielräume, ist die Anwendbarkeit der europäischen Grundrechte allerdings strittig.

Laut der vom BVerfG vertretenen **Alternativitätsthese** (auch Trennungsthese genannt) besteht in diesen Gestaltungsspielräumen kein Anwendungsvorrang des Unionrechts und der Sachverhalt wird nach nationalen Grundrechtsmaßstäben beurteilt.[289] Unionsgrundrechte und nationale Grundrechte bestehen demnach als getrennte Sphären.[290] Entscheidend ist für das BVerfG, inwieweit die nationale Durchführung von unionsrechtlichen Vorgaben bestimmt ist. Kritische Stimmen bemängeln hierbei allerdings mangelnde Trennschärfe, da Sachverhalte teilweise im unionsrechtlichen Bereich ihre Rechtsvorgaben finden, die teilweise den Mitgliedstaaten zur Regelung überantwortet wurden. [291] Als Argument für diese These wird angeführt, dass die Bedeutung der Grundrechte-Charta nicht wie bei der EMRK in der Herstellung eines Mindeststandards an Grundrechten liegt, sondern der gleichmäßigen Anwendung des Unionsrechts in den Mitgliedstaaten dient.[292]

Vertreter und Vertreterinnen der **Kumulationsthese** (auch Verbindungsthese genannt) hingegen sehen Unionsgrundrechte und nationale Grundrechte auch bei Überschneidungsbereichen als nebeneinander stehend und sprechen den Unionsgrundrechten einen weiten Anwendungsbereich zu.[293] Der EuGH als Befürworter dieser These zieht den Anwendungsbereich der europäischen Grundrechte entsprechend weit und konkretisiert im Åkerberg Fransson-Urteil eine vorrangige Überprüfung anhand der Unionsgrundrechte sogar im Bereich nicht zwingenden Richtlinienrechts nach dem Grundsatz „Wo Unionsrecht hinreicht, gelten die

[285] Hwang, *EuR 2016, 355 (355);* Kirchhof, *NVwZ 2014, 1537 (1537).*
[286] Stelkens u. a., *Verwaltungsverfahrensgesetz – Kommentar, Z. 48.*
[287] Katsivelas, *MMR 2017, 286 (287).*
[288] Kirchhof, *NVwZ 2014, 1537 (1538).*
[289] Katsivelas, *MMR 2017, 286 (287).*
[290] Härtel, *LKV 2019, 49 (53).*
[291] Meyer, *Charta der Grundrechte der Europäischen Union Kommentar GRCh Art. 51 Rn 43.*
[292] Katsivelas, *MMR 2017, 286 (287).*
[293] Härtel, *LKV 2019, 49 (53).*

Unionsgrundrechte“ [294], wobei das Handeln des Mitgliedstaates „nicht vollständig durch das Unionsrecht bestimmt“ [295] sein müsse.[296] Es reicht demnach ein hinreichender Zusammenhang zwischen unionsrechtlichen Maßgaben und der konkreten nationalen Maßnahme, wobei die Unionsgrundrechte nicht greifen, wenn das Unionsrecht in dem vorliegenden Sachbereich keine bestimmten Verpflichtungen der Mitgliedstaaten im Hinblick auf den konkreten Sachverhalt geschaffen hat. Dies ist beispielweise bei unionsrechtliche Mindestregelungen der Fall, wenn sich die nationalen Regelungen hierzu außerhalb des erfassten Bereiches bewegen. [297] Zudem sieht der EuGH den Anwendungsbereich der unionsrechtlichen Grundrechte eröffnet, wenn Mitgliedstaaten eine unionsrechtlich vorgesehene Ausnahme wahrnehmen, um die Einschränkung von Grundfreiheiten zu rechtfertigen. Hierbei fungieren die europäischen Grundrechte als eine Art Schranke-Schranke für die Grundfreiheiten.[298] Nach dem Verständnis des EuGH lässt sich die Grundrechte-Charta folglich als „Schatten des Unionsrechts“ verstehen.[299] Gestützt wird diese These zudem auf dem Wortlaut des Art. 53 GRCh, der das Schutzniveau der unionalen Grundrechte behandelt. Art. 53 GRCh erlaubt die Koexistenz und die gleichzeitige Anwendbarkeit unionsrechtlicher sowie nationaler Grundrechte. Im konkreten Fall ist das einschlägige Grundrecht mit dem höheren Schutzniveau anzuwenden, solange keine Vorgaben des Unionsrechts hierfür missachtet werden müssten.[300] In der Literatur wird die Kumulationsthese zudem durch eine teleologische Auslegung des Durchführungs-Begriffs aus Art. 51 GRCh befürwortet. Unionsgrundrechten käme überhaupt erst bei mitgliedsstaatlichen Gestaltungsspielräumen eine Bedeutung zu, da bei zwingendem Unionsrecht die zu vollziehende Vorgabe grundrechtswidrig oder grundrechtskonform sei und mit ihr entsprechend auch der Vollzug.[301]

Kritik an der Kumulationsthese und der dazugehörigen Rechtsprechung des EuGH übt auf nationaler Mitgliederebene vor allem das BVerfG. So heißt es, bezogen auf das Åkerberg Fransson-Urteil, im Urteil zum Antiterrordateiengesetz, dass der Senat davon ausgeht, „dass die in der EuGH-Entscheidung enthaltenen Aussagen auf Besonderheiten des Umsatzsteuerrechts beruhen, aber keine grundsätzliche Auffassung äußern“[302]. Das BVerfG lehnte im Antiterrordateiengesetz-Urteil ein Vorabentscheidungsersuchen an den EuGH ab, da die entsprechenden Vorschriften nicht durch Unionsrecht determiniert seien und die Grundrechte-Charta folglich nicht anwendbar sei. Dies würden auch teilweise Berührungen von unionsrechtlichen Regelungsbereichen nicht ändern. [303]

---

[294] Bergmann/Dienelt, *Ausländerrecht: AuslR EU-Grundrechte-Charta Art. 51 Rn 5.*
[295] Meyer, *Charta der Grundrechte der Europäischen Union Kommentar GRCh Art. 51 Rn 44.*
[296] Oppel/Sendke, *IStR 2018, 110 (113).*
[297] Meyer, *Charta der Grundrechte der Europäischen Union Kommentar GRCh Art. 51 Rn 46.*
[298] Meyer, *Charta der Grundrechte der Europäischen Union Kommentar GRCh Art. 51 Rn 48.*
[299] Meyer, *Charta der Grundrechte der Europäischen Union Kommentar GRCh Art. 51 Rn 40.*
[300] Streinz, *EUV/AEUV Kommentar EU-Grundrechte-Charta 2000 Art. 51 Rn 26.*
[301] Matz-Lück/Hong, *Grundrechte und Grundfreiheiten im Mehrebenensystem - Konkurrenzen und Interferenzen, S. 24.*
[302] *24.4.2013 – 1 BvR 1215/07.*
[303] Meyer, *Charta der Grundrechte der Europäischen Union Kommentar GRCh Art. 51 Rn 45.*

3. Die DS-GVO im verfassungsrechtlichen Kontext

Im Hinblick auf die zuvor dargestellten gegensätzlichen Auffassungen zur Reichweite des Anwendungsvorrang unionsrechtlicher Grundrechte wird im Folgenden die DS-GVO als wesentlicher Bestandteil dieser Arbeit in ihrer Form als europäische Verordnung mit partiellen nationalen Gestaltungsspielräumen auf ihre grundrechtliche Zuordnung beleuchtet.

Die DS-GVO verkörpert einen Rechtsakt der EU und ist dementsprechend gem. Art. 288 II AEUV verbindlich und gilt in den Mitgliedstaaten als unmittelbar geltendes Recht.[304] Sie ist in ihrem Kern die einfachrechtliche Konkretisierung des Grundrechts auf Schutz der personenbezogenen Daten nach Art. 8 GRCh und bezieht sich zudem in ihren Erwägungsgründen auf Art. 16 AEUV. Der EuGH leitet in seiner Rechtsprechung den unionsrechtlichen Datenschutz zudem auch aus Art. 7 GRCh her.[305]

Nach dem Solange II-Urteil des BVerfG sowie der Rechtsprechung des EuGHs ist unstrittig ein Anwendungsvorrang der europäischen Grundrechte-Charta vor den deutschen Grundrechten in Bezug auf die Teile der DS-GVO zu bejahen, die die Mitgliedstaaten zwingend umzusetzen haben.

Fraglich ist, welche Grundrechte bei den sogenannten **Öffnungsklauseln** der DS-GVO Anwendung finden.

Nach der Alternativitätsthese des BVerfG sind für den Rechtsbereich der Öffnungsklauseln die Grundrechte der deutschen Verfassung anwendbar[306], da die unionsrechtliche Legislative den Mitgliedstaaten einen eigenständigen Gestaltungsspielraum überlassen hat. Den Mitgliedstaaten steht es frei, von der Öffnungsklausel Gebrauch zu machen. Geschieht dies, genießen die nationalen Grundrechte und die dazugehörige verfassungsrechtliche Rechtsprechung für diesen Abschnitt des Datenschutzrechtes Anwendungsvorrang. Dies gilt nach der Alternativitätsthese auch für nationale Datenschutzvorschriften aus Bereichen, in denen die DS-GVO sachlich nicht anwendbar ist.[307] Die verfassungsrechtliche Beurteilung konkreter Sachverhalte würde sich bei Öffnungsklauseln folglich an dem datenschutzrelevanten Grundrecht der informationellen Selbstbestimmung als Konkretisierung des allgemeinen Persönlichkeitsrechts nach Art. 2 I i.V.m. Art. 1 I GG orientieren.[308]

Nach der Kumulationsthese des EuGH hingegen wird weiterhin der Anwendungsvorrang der europäischen Grundrechte-Charta bejaht werden müssen, da ein Sachzusammenhang zu einem Unionsrechtsakt besteht. Dies kann u.a. abgeleitet werden aus dem Urteil zur Familienzusammenführungsrichtlinie des EuGH, in dessen Rahmen der EuGH den Anwendungsbereich der

[304] Auer-Reinsdorff/Conrad, *Handbuch IT- und Datenschutzrecht§ 34 Rn 19.*
[305] Härtel, *LKV 2019, 49 (54) f;* Auer-Reinsdorff/Conrad, *Handbuch IT- und Datenschutzrecht§ 34 Rn 20.*
[306] Härtel, *LKV 2019, 49 (54) f.*
[307] Auer-Reinsdorff/Conrad, *Handbuch IT- und Datenschutzrecht§ 34 Rn 18.*
[308] Bäcker, *EuR 2015, 389 (392).*

Unionsgrundrechte für eine Öffnungsklausel einer Richtlinie erstmals konkret bejahte.[309] Zwar handelt es sich bei der DS-GVO um eine Verordnung und keine Richtlinie, es kann aber davon ausgegangen werden, dass die Ansicht des EuGH für sämtliche Rechtsakte mit den jeweiligen Öffnungsklauseln gilt. Bei der Wahrnehmung von Öffnungsklauseln müssen in einem angemessenen Gleichgewicht zugunsten der GRCh neben den unionsrechtlichen Grundrechten jedoch auch die nationalen Grundrechte respektiert werden.[310]

Überdies problematisch ist die verfassungsrechtliche Einordnung des **Art. 6 II, III DS-GVO**. Absatz 2 und 3 des Art. 6 DS-GVO können als beschränkte Öffnungsklauseln verstanden werden. In der Literatur wird die Meinung vertreten, dass in diesem Fall der Anwendungsbereich des Unionsrechts eröffnet sei, da die DS-GVO zwar keine konkreten Handlungen fordere, auf der Grundlage des Art. 6 II, III DS-GVO ausgeführte Handlungen aber an den Unionsgrundrechten zu messen seien.[311] Durch die Eingeschränktheit dieser Öffnungsklausel würden die deutschen Grundrechte im Mehrebenen-System durch die Grundrechte-Charta überlagert werden und könnten allenfalls als Orientierungspunkt dienen.[312]

4. Zusammenfassung

Wird von Mitgliedstaaten der EU zwingendes Unionsrecht umgesetzt oder vollzogen, so ist das mitgliedstaatliche Handeln an der europäischen Grundrechte-Charta zu bemessen. Lässt das Unionsrecht derweil den Mitgliedstaaten einen Gestaltungsspielraum bei der Durchführung von ebendiesem, ist der unionsrechtliche Anwendungsvorrang umstritten. Das BVerfG vertritt die Meinung, dass staatliches Handeln im Rahmen der gesetzlichen Spielräume nach nationalen Grundrechten beurteilt werden sollte. Der EuGH hingegen bejaht unionsrechtliche Anwendungsvorrang auch dann noch, wenn ein hinreichender Zusammenhang zu den unionsrechtlichen Maßgaben besteht. Erst wenn keine unionsrechtlichen Verpflichtungen mehr greifen, rücken die nationalen Grundrechte in den Vordergrund.

In Bezug auf die DS-GVO liegt für weite Teile ein unumstrittener Anwendungsvorrang der Unions-Grundrechte vor. Die Öffnungsklauseln der Verordnung jedoch sind Gestaltungsspielräume, deren grundrechtliche Beurteilungsebene nach oben genannten Auffassungen strittig ist.

Da die DS-GVO im weiteren Verlauf auf eine schon bestehende Erlaubnisnorm zur Nutzung von Angriffserkennungssystem im privatrechtlichen Kontext in ihren zwingenden unionsrechtlichen Abschnitten untersucht wird sowie über Lösungsansätze durch die Nutzung der grundrechtlich umstrittenen Öffnungsklauseln diskutiert wird, wird zur Absicherung die unionsrechtliche sowie die nationale Grundrechtsebene im Folgenden betrachtet.

---

[309] Matz-Lück/Hong*, Grundrechte und Grundfreiheiten im Mehrebenensystem - Konkurrenzen und Interferenzen, S. 182.*
[310] Grabitz u. a.*, Das Recht der Europäischen Union: EUV/AEUV AEUV Art. 16 Rn 15.*
[311] Bäcker*, EuR 2015, 389 (394).*
[312] Paal/Pauly*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 6 Rn 53.*

B. Anwendbarkeit von Grundrechten auf die Rechtsbeziehungen zwischen Privatrechtssubjekten

Krankenhausbetreibende i.S.d. Untersuchung – und folglich die Betreibenden der Angriffserkennungssysteme – sind Privatrechtssubjekte. Im klassischen Sinn stellen Grundrechte jedoch Abwehrrechte und Schutzrechte gegen staatliches Handeln dar. Ob Grundrechte auch auf das Verhältnis zwischen Privatpersonen, hier: Krankenhausbetreibende, Patient und Patientin sowie Mitarbeitende, anwendbar sind und ob dieses Verhältnis nicht allein schon durch die aus den Grundrechten resultierenden Schutzpflichten des Staates durch gesetzliche Regelungen gesichert werden muss, wird im folgenden Kapitel auf europäischer sowie nationaler Ebene erläutert.

1. Unionsrechtliche Ebene

a) Die mittelbare Drittwirkung von Grundrechten im europäischen Kontext

Die Grundrechte der GRCh verpflichten gem. Art. 51 I 1 GRCh die Union sowie unter bestimmten Voraussetzungen deren Mitgliedstaaten. Eine unmittelbare Verpflichtung von Privatpersonen ist nicht vorgesehen. Es kann sich jedoch eine Bindung von Privatpersonen durch eine **Drittwirkung** („horizontal effect") der Grundrechte ergeben.[313] Eine eindeutige Regelung hierfür ist in der GRCh nicht enthalten, wird jedoch von Literatur sowie Rechtsprechung angenommen.[314] Dass diese Drittwirkung nicht **unmittelbar** („direct horizontal effect") stattfinden kann, wird einerseits durch den Wortlaut des Art. 51 GRCh begründet, der Privatpersonen nicht als Adressaten und Adressatinnen der Grundrechtsverpflichtung nennt. Zum anderen wird argumentiert, dass Privatpersonen als Grundrechtsträger und -trägerinnen nicht auch noch unmittelbar grundrechtsverpflichtet sein können.[315] Ein entstandenes Schutzdefizit müsse und solle durch die Schutzpflicht der Mitgliedstaaten ausgeglichen werden, weswegen eine unmittelbare Drittwirkung bereits bei der Erarbeitung der GRCh von der Literatur abgelehnt wurde.[316] Die Rechtsprechung des EuGH, in der zwar für die Grundfreiheiten eine unmittelbare Drittwirkung anerkannt wird, kann jedoch aufgrund der Binnenmarktorientierung der Grundfreiheiten nicht auf die Grundrechte übertragen werden.[317]

---

[313] Jarass, *Charta der Grundrechte der Europäischen Union Kommentar EU-Grundrechte-Charta Art.51 Anwendungsbereich Rn 31.*
[314] Franzen u. a., *Kommentar zum europäischen Arbeitsrecht GRCh Art. 51 Rn 34.*
[315] Meyer, *Charta der Grundrechte der Europäischen Union Kommentar GRCh Art. 51 Rn 57.*
[316] Franzen u. a., *Kommentar zum europäischen Arbeitsrecht GRCh Art. 51 Rn 34.*
[317] Franzen u. a., *Kommentar zum europäischen Arbeitsrecht GRCh Art. 51 Rn 35.*

Eine **mittelbare** Drittwirkung („indirect horizontal effect“) wird jedoch von Literatur und Rechtsprechung überwiegend anerkannt.[318] Hiernach können Grundrechte in bestimmten Sonderkonstellationen auch im Verhältnis zwischen Privatpersonen Wirkung entfalten. Legislative und rechtsprechende Gewalt vermitteln „indirekt“ die grundrechtliche Wirkung durch ihr grundrechtsgebundenes hoheitliches Handeln auf Privatrechtsverhältnisse. Privatrechtliche Normen müssen grundrechtskonform sein, Gerichte müssen in ihren Entscheidungen die grundrechtlichen Wertungen einbeziehen und entsprechend gewichten. Eine Grundrechtsgebundenheit von Privatpersonen wird bei der mittelbaren Drittwirkung jedoch verneint.[319] Zwar hat der EuGH den Begriff in seiner Rechtsprechung nie verwendet, jedoch legt er in privatrechtlichen Fällen die entsprechenden Vorschriften „im Licht“ der Grundrechte aus, was dem Prinzip der mittelbaren Drittwirkung entspricht.[320]

Insbesondere für das Grundrecht auf Datenschutz ist eine mittelbare Drittwirkung in Privatrechtsverhältnisse anerkannt. Aufgrund des technischen Fortschritts, des steigenden Wertes von Daten und der fortlaufenden Digitalisierung geht heutzutage die Gefährdungslage gleichermaßen von privaten und öffentlichen Stellen aus.[321]

b) Die Schutzpflicht der Mitgliedstaaten

Soweit nicht-öffentliche Verantwortliche in den Schutzbereich der Grundrechte eingreifen, ist die Legislative durch die Artikel der Grundrechte-Charta im Rahmen ihrer Schutzpflichten verpflichtet, die betroffenen Grundrechte gegen Eingriffe durch private Personen zu schützen. Ziel und Zweck der Schutzpflichten ist demnach die tatsächliche Freiheitsverwirklichung des Grundrechtsträgers und der -trägerin. Diese sollen durch die Schutzpflichten in die Lage versetzt werden, ihr Grundrecht wahrzunehmen oder ggfs. durchzusetzen.[322] Schutzpflichten greifen demnach erst, wenn eine Grundrechtsbeeinträchtigung vorliegt oder vorzuliegen droht. Neben einer Beeinträchtigung durch Privatpersonen sind Beeinträchtigungen durch Naturereignisse ebenso anerkannt.[323] Die Schutzpflicht ergibt sich aus der allgemeinen Dogmatik der Grundrechte. Die Verpflichtung der Legislative zum Handeln ist umso stärker, je hilfloser der betroffene Bürger oder die betroffene Bürgerin ist.[324] Diese Schutzpflichten können auch unter den Begriff der mittelbaren Drittwirkung eingeordnet werden[325], wobei in diesem Fall keine

[318] Roßnagel, *NJW 2019, 1 (4).*
[319] Jobst, *NJW 2020, 11 (11).*
[320] Jarass, *Charta der Grundrechte der Europäischen Union Kommentar EU-Grundrechte-Charta Art.51 Anwendungsbereich Rn 32.*
[321] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 64.*
[322] Franzen u. a., *Kommentar zum europäischen Arbeitsrecht GRCh Art. 51 Rn 60.*
[323] Franzen u. a., *Kommentar zum europäischen Arbeitsrecht GRCh Art. 51 Rn 64.*
[324] Roßnagel, *NJW 2019, 1 (3) f.*
[325] Franzen u. a., *Kommentar zum europäischen Arbeitsrecht GRCh Art. 51 Rn 46.*

mittelbare Grundrechtsbindung von Privatpersonen gemeint ist, sondern eine Erlasspflicht von privatrechtlichen Regelungen durch den Hoheitsträger im Rahmen seiner Schutzfunktion.[326]

2. Nationale Ebene

a) Die mittelbare Drittwirkung von Grundrechten im nationalen Kontext

Die in Art. 1 III GG normierte Vorschrift über die Grundrechtsorientierung aller staatlichen Gewalt bildet die Grundlage für unseren grundrechtsgebundenen Verfassungsstaat.[327] Sie besagt, dass jede Äußerung staatlicher Gewalt – ob durch Rechtsakt oder faktisches Handeln, ob final und unmittelbar oder nicht[328] – einen Eingriff in den Schutzbereich der betroffenen Grundrechte darstellt. Das BVerfG vertritt in ständiger Rechtsprechung und in Übereinstimmung mit der herrschenden Staatslehre die Auffassung, dass Grundrechte keine **unmittelbare** Drittwirkung entfalten können[329], um die grundsätzlich privatautonome Gestaltung individueller Rechtsbeziehungen zu schützen.[330] Dies gelte auch, wenn gegenüber anderen Privaten über eine weit überlegene wirtschaftliche oder soziale Machtposition verfügt wird.[331] Die Grundrechte entfalten als Ausdruck einer Wertordnung und durch verfassungsrechtliche Grundentscheidungen[332] jedoch eine abgeschwächte, **mittelbare** Drittwirkung auf die Rechtsbeziehung zwischen Privaten[333], insbesondere über die privatrechtlichen Generalklauseln.[334] Die Rechtfertigung für diese mittelbare Wirkung liegt darin, dass gerade in der von der Eigenverantwortung des Individuums bestimmten Rechtsordnung des Grundgesetzes privatautonome Gestaltungsmöglichkeiten unter Ausnutzung sozialer, wirtschaftlicher und anderer Asymmetrien Grundrechtssubstanzen gefährden können.[335]

In den letzten Jahren ist mit einer Reihe an Entscheidungen wieder Bewegung in der Diskussion um den Begriff der mittelbaren Drittwirkung entstanden: Zentraler Punkt ist die Umdeutung oder vielmehr Anerkennung der mittelbaren Drittwirkung der Grundrechte als verfassungskonforme Auslegung. Zum einen beginnt das BVerfG, den Begriff der mittelbaren Drittwirkung zu vermeiden, zum anderen betont es indes erstmals explizit, dass nicht nur die zivilrechtlichen Generalklauseln, sondern alle Zivilrechtsnormen im Lichte der Grundrechte auszulegen

[326] Berlth*, Artikel 1 GRCh – Die Menschenwürde im Unionsrecht, S. 42.*
[327] Maunz u. a.*, GG – Kommentar, Z. 2 f.*
[328] Nach der „weiten" Definition des Grundrechtseingriffs, siehe Maunz u. a.*, GG – Kommentar, V. Art. 1 Abs. 3 Rn 39.*
[329] Wente*, NJW 1984, 1446 (1446).*
[330] Maunz u. a.*, GG – Kommentar Art. 1 Abs. 3 Rn 59.*
[331] Hillgruber/Epping*, BeckOK Grundgesetz Art. 1 Rn 72;* Maunz u. a.*, GG – Kommentar Art. 1 Abs. 3 Rn 100.*
[332] Fischinger*, Münchener Handbuch zum Arbeitsrecht§ 7 Grundrechte im Arbeitsverhältnis Rn 9.*
[333] Maunz u. a.*, GG – Kommentar Art. 1 Abs. 3 Rn 59.*
[334] Kulick*, NJW 2016, 2236 (2236).*
[335] Maunz u. a.*, GG – Kommentar Art. 1 Abs. 3 Rn 65.*

seien.[336] Habe der Gesetzgeber es versäumt, seine grundrechtlichen Schutzaufträge zu erfüllen, ließen sich sogar ausnahmsweise konkrete Regelungspflichten des Privatrechtsgesetzgebers aus den Grundrechten ableiten.[337] So führte das BVerfG in der Bierdosen-Flashmob-Entscheidung von 2015 aus, dass „Private im Wege der mittelbaren Drittwirkung von Grundrechten (…) auch ähnlich oder auch genauso weit wie der Staat durch die Grundrechte in Pflicht genommen werden [können], insbesondere, wenn sie in tatsächlicher Hinsicht in eine vergleichbare Pflichten oder Garantenstellung hineinwachsen wie traditionell der Staat".[338] Ähnliches gilt in Bezug auf den Kommunikationsschutz der Bürger und Bürgerinnen. Das BVerfG hat anerkannt, dass eine Annäherung der mittelbaren Grundrechtsbindung Privater an die Grundrechtsbindung des Staates insbesondere dann in Betracht kommt, „wenn private Unternehmen die Bereitstellung schon der Rahmenbedingungen öffentlicher Kommunikation selbst übernehmen und damit in Funktionen eintreten, die – wie die Sicherstellung der Post- und Telekommunikationsdienstleistungen – früher dem Staat als Aufgabe der Daseinsvorsorge zugewiesen waren".[339] In der Entscheidung zum Stadionverbot von 2018 ging das BVerfG sogar noch weiter und prüfte den Gleichheitsgrundsatz des Art. 3 I GG in einer Konstellation, die ausschließlich Privatpersonen betrifft (Fußballverein gegen Fußballfan).[340] Jedoch muss beachtet werden, dass es sich hier um eine „situative Grundrechtsbindung" handelt, da laut BVerfG die „spezifische Konstellation des Einzelfalls" entscheidend gewesen sei. Entscheidendes Kriterium war hier die Öffnung der Fußballveranstaltung des Stadionbetreibers (Fußballverein) für ein großes Publikum und die daraus resultierende strukturelle Überlegenheit.[341] Auch im Bereich des Grundrechts der informationellen Selbstbestimmung aus Art. 2 I i.V.m. Art. 1 I 1 GG wird eine Drittwirkung mittlerweile akzeptiert. Dies liegt vor allem daran, dass – ähnlich wie die Annahme auf unionsrechtlicher Ebene – durch technische Innovationen Privatpersonen und -unternehmen mittlerweile eine größere Bedrohung für den Grundrechtsschutz darstellen als der öffentliche Bereich.[342]

b) Die nationalen grundrechtlichen Schutzpflichten

Zudem kann die Legislative aufgrund der zweifachen Schutzdimension der Grundrechte zum Handeln gezwungen sein. Denn die Grundrechte sind zwar in erster Linie dazu bestimmt, die Freiheitssphäre des und der Einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern.[343] Daneben begründen sie aber auch grundrechtliche Schutzpflichten im Rahmen ihrer objektiven Prinzipien und bilden ein „zielorientiertes Handlungsprogramm für den Gesetzgeber"[344]

[336] Kulick, *NJW 2016, 2236 (2238).*
[337] Kulick, *NJW 2016, 2236 (2240).*
[338] Jobst, *NJW 2020, 11 (12).*
[339] Roßnagel, *NJW 2019, 1 (4).*
[340] Jobst, *NJW 2020, 11 (12).*
[341] Jobst, *NJW 2020, 11 (13).*
[342] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch I. Kapitel 1. Rn 35 ff.*
[343] Klein, *NJW 1989, 1633 (1633).*
[344] Papier, *NJW 2017, 3025 (3028).*

gegenüber Dritten, die nicht zum Adressaten- und Adressatinnenkreis der Grundrechte gehören.[345] Dieses muss, schon allein aufgrund des Grundsatzes des Vorbehalts des Gesetzes, in Form von gesetzlichen Ermächtigungsgrundlagen umgesetzt werden[346], wobei der Gesetzgeber hierbei über einen grundsätzlichen Gestaltungs- und Ermessenspielraum verfügt.[347] Die Rechtsfigur der grundrechtlichen Schutzpflichten kann folglich als „Rechtsgebot zum Eingriff in Rechte Dritter zu Gunsten eines anderen Grundrechtsträgers" verstanden werden.[348]

3. Zusammenfassung

Auf unionsrechtlicher sowie nationaler Ebene ist eine mittelbare Drittwirkung der Grundrechte auf Privatrechtssubjekte anerkannt. Zudem können die Mitgliedstaaten aufgrund der auf beiden Grundrechtsebenen bestehenden Schutzpflichten verpflichtet werden, Maßnahmen zu ergreifen, wenn die Grundrechte der Bürger und Bürgerinnen durch Dritte bedroht oder verletzt werden.

Das privatrechtliche Verhältnis zwischen Krankenhausbetreibendem und Patient beziehungsweise Patientin kann somit mittelbar an den Grundrechten der jeweiligen Verfassung gemessen werden und die EU bzw. der Staat kann verpflichtet sein, Schutzmaßnahmen in Form eines Gesetzes zu erlassen, wenn durch den Betrieb von Angriffserkennungssystemen im Privatrechtsverhältnis die Grundrechte der Patienten und Patientinnen gefährdet sein würden.

C. Betroffene Grundrechte

Da die Grundrechte durch ihre mittelbare Drittwirkung auch auf das Verhältnis zwischen Privatrechtssubjekten anwendbar sind, ist eine Rechtsgrundlage zur Nutzung von Angriffserkennungssystemen in Netzwerken privatrechtlich organisierter Krankenhäuser notwendig, wenn ein solcher mittelbarer Grundrechtseingriff vorliegt und die grundrechtlichen Schutzpflichten des Staates somit greifen. Im Folgenden wird, aufgrund der strittigen Lage auf europäischer sowie auf nationaler Grundrechtsebene, geprüft, in welche Grundrechte der Patienten und Patientinnen durch die Nutzung von Angriffserkennungssystem in Krankenhäusern eingegriffen wird.

1. Nationale Ebene

Relevante Grundrechte der deutschen Verfassung sind im konkreten Fall das Fernmeldegeheimnis nach Art. 10 I GG sowie die beiden datenschutzrechtlichen Konkretisierungen des

[345] Klein*, NJW 1989, 1633 (1633).*
[346] Papier*, NJW 2017, 3025 (3028).*
[347] Maunz u. a.*, GG – Kommentar Art. 2 Abs. 1 Rn 61.*
[348] Maunz u. a.*, GG – Kommentar Art. 2 Abs. 1 Rn 61.*

Allgemeinen Persönlichkeitsrechts aus Art. 2 I i.V.m. Art. 1 I 1 GG: das Recht auf informationelle Selbstbestimmung sowie das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

a) Das Fernmeldegeheimnis nach Art. 10 I GG

Dem Schutz der Privatheit dienlich ist das Post- und Fernmeldegeheimnis aus Art. 10 I GG, wobei dieses nicht zwischen Anwesenden greift, sondern für die Kommunikation auf Distanz.[349] Von den verschiedenen Schutzbereichen des Art. 10 I GG ist durch die Digitalisierung das Fernmeldegeheimnis in der Praxis vorrangig relevant.[350]

(1) Schutzbereich

Art. 10 GG schützt über das Fernmeldegeheimnis die unkörperliche Übermittlung von Informationen an individuelle Empfänger und Empfängerinnen mit Hilfe von Fernmeldetechnik, also Telekommunikation.[351] Der Schutz erfasst in erster Linie die Vertraulichkeit der ausgetauschten Informationen und schirmt damit den Kommunikationsinhalt gegen unbefugte Kenntniserlangung durch Dritte ab.[352] Das Fernmeldegeheimnis ist „entwicklungsoffen" und umfasst sämtliche Technologien, die bei Entstehung des Grundgesetzes bekannt waren und seitdem entwickelt wurden.[353] Neben Briefen und Telefonaten sind dementsprechend auch SMS, E-Mails, Chats oder Direktnachrichten in sozialen Netzwerken vom Schutzbereich des Art. 10 I GG umfasst.[354] Zudem kommt es nicht auf die Übertragungsart der Telekommunikation an. Diese kann per Kabel, Funk, analog oder digital gesendet werden. Auch die Ausdrucksformen der Kommunikation sind für den Schutzbereich des Art. 10 I GG irrelevant. Diese kann über die Sprache oder das Senden von Bildern, Tönen oder Zeichen geschehen.[355] Der Schutz der Grundrechte aus Art. 10 I GG besteht unabhängig davon, ob die betreffende Fernkommunikation einen privaten, geschäftlichen, politischen oder sonstigen Inhalt hat[356]; er gewährt Grundrechtsschutz im Hinblick auf alle durch Fernmeldetechnik ausgetauschten nichtöffentlichen Informationen.[357] Geschützt sind zudem die Verkehrsdaten, insbesondere die Metadaten. Diese beinhalten u.a., welche Personen zu welchem Zeitpunkt über welche Dauer kommuniziert haben.[358] Aus den Metadaten einer Kommunikation, die zudem leichter auszuwerten sind

---

[349] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 178.*
[350] Pieper, *JA 2018, (598).*
[351] Gersdorf/Paal, *BeckOK Informations- und Medienrecht GG Art. 10 Rn 11.*
[352] Gersdorf/Paal, *BeckOK Informations- und Medienrecht GG Art. 10 Rn 14.*
[353] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, II. Rechtliche Grundlagen Rn 30.*
[354] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 179.*
[355] Gurlit, *NJW 2010, 1035 (1037).*
[356] Hillgruber/Epping, *BeckOK Grundgesetz GG Art. 10 Rn 13.*
[357] Maunz u. a., *GG – Kommentar Art. 10 Rn 85.*
[358] Pieper, *JA 2018, (600).*

als die inhaltlichen Daten, können Aussagen über die Lebensweisen und Vorlieben sowie Bewegungsmuster der betroffenen Personen erstellt werden.[359] Außerhalb des Schutzbereiches liegt allerdings das bloße Mitführen eines betriebsbereiten Mobiltelefons.[360] Fehlgeschlagene Verbindungsversuche sind indes vom Schutzbereich umfasst.[361]

Nach Abschluss der Nachrichtenübermittlung hingegen sind die bei den Teilnehmenden gespeicherten Kommunikationsinhalte und –umstände nicht mehr denselben spezifischen Risiken ausgesetzt; die mit Rücksicht auf den Normzweck des Art. 10 GG bestimmten Schutzbereiche erfassen solche Daten daher nicht mehr.[362] Ab diesem Moment ist der Empfänger oder die Empfängerin in der Lage, selbst Sicherungsvorkehrung gegen unberechtigte Zugriffe zu ergreifen.[363]

(2) Eingriff in den Schutzbereich

Da Art. 10 I GG die Vertraulichkeit der Kommunikationsinhalte und die Umstände des Kommunikationsvorgangs schützt, stellt jede „Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder sonstige Verwendung durch die öffentliche Gewalt“ einen Grundrechtseingriff dar.[364] Eingriffe in den Schutzbereich können mittels Überwachung der Kommunikationsübertragung oder durch Infiltration des Endgerätes geschehen. Es ist nicht von Bedeutung, ob hierbei personenbezogene Daten erhoben wurden.[365]

Wird bei dem Einsatz von Angriffserkennungssystemen der Telekommunikationsverkehr erfasst, so liegt ein Eingriff in das Fernmeldegeheimnis vor.[366] SIEM-Systeme erfassen im Rahmen ihrer Auswertung von automatisierten Ereignisdokumentationen von Firewalls, Virenscannern, Spam-Filtern, Datenbankanwendungen sowie Betriebs- und Anwendungssoftware von Computern auch Telekommunikations-Verkehrsdaten und bei Netzwerkkomponenten sowie E-Mail-Relais sogar Inhaltsdaten. Die durch IDS durchleuchteten IP-Pakete erfassen Telekommunikations-Inhaltsdaten sowie -Verkehrsdaten.[367] Inhaltsdaten sind Daten, die der Nutzer oder die Nutzerin und der Anbieter oder die Anbieterin online austauschen, wohingegen Verkehrsdaten alle Daten sind, die bei der Erbringung des Telekommunikationsdienstes

---

[359] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 180.*
[360] Gurlit, *NJW 2010, 1035 (1037).*
[361] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, II. Rechtliche Grundlagen Rn 31.*
[362] Maunz u. a., *GG – Kommentar Art. 10 Rn 62.*
[363] Pieper, *JA 2018, (600).*
[364] Gersdorf/Paal, *BeckOK Informations- und Medienrecht GG Art. 10 Rn 27.*
[365] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, II. Rechtliche Grundlagen Rn 33.*
[366] Miller, *NdsVBl 2021, 1 (2).*
[367] Miller, *NdsVBl 2021, 1 (3);* heise online, *Höhere Sicherheit mit wenig Aufwand: Wie innovative SIEM-Lösungen helfen, Cyber-Angriffe abzuwehren.*

erhoben, verarbeitet oder genutzt werden.[368] Während Inhaltsdaten stets dem Fernmeldegeheimnis unterfallen, stehen Verkehrsdaten nur unter dem Schutz des Fernmeldegeheimnisses, soweit sie Aufschluss über die beteiligten Personen und die Umstände der Kommunikation geben.[369]

Da durch IDS und SIEM-Systeme Datenpakete verarbeitet werden, die unter anderem Inhalts- und Verkehrsdaten enthalten können, ist der Schutzbereich des Art. 10 I GG eröffnet. Die Analyse und Auswertung dieser Daten im Rahmen des Einsatzes von Angriffserkennungssystemen stellt einen Eingriff in den Schutzbereich dar. Nach Art. 1 Abs. 3 S. 1 GG sind die Grundrechte allerdings in erster Linie Abwehrrechte gegenüber staatlichen Eingriffen und binden nur die drei Staatsgewalten unmittelbar. Der unmittelbare Eingriff in den Schutzbereich des Art. 10 I GG erfolgt demnach bereits durch die einfachrechtlichen Rechtsgrundlagen, die im Verlauf dieser Abhandlung auf eine Ermächtigungsgrundlage zur Nutzung von Angriffserkennungssystemen durch Privatrechtssubjekte untersucht werden. Dieser staatliche Eingriff in die Grundrechte kann auf zweiter Ebene sogleich die Legitimation des tatsächlichen, mittelbaren Eingriffs in die Rechte der betroffenen Personen durch die Nutzung von Angriffserkennungssysteme durch Privatrechtssubjekte darstellen.

(3) Rechtfertigung eines Eingriffs

Nach Art. 10 II 1 GG dürfen Beschränkungen der Grundrechte aus Art. 10 I GG nur auf Grund eines Gesetzes angeordnet werden[370], wobei das BVerfG hierbei ähnliche Kriterien heranzieht wie für die Rechtfertigung von Eingriffen in das Recht auf informationelle Selbstbestimmung.[371] Als Ermächtigungsgrundlage kommen sowohl Bundes- als auch Ländergesetze in Betracht.[372] Die Schranken des Art. 10 I GG sind hierbei ebenso technisch entwicklungsoffen wie der Schutzbereich.[373]

(4) Verhältnis zu anderen Grundrechten

Soweit personenbezogene Daten durch den Eingriff in den Kommunikationsvorgang erlangt wurden, ist Art. 10 I GG lex specialis zu dem Recht auf informationelle Selbstbestimmung aus Art. 2 I i.V.m. Art. 1 I 1 GG.[374]

---

[368] Spindler u. a., *Telemediengesetz Kommentar TMG § 15 Rn 75;* Brink/Wolff, *BeckOK Datenschutzrecht Syst. I. Rn 91;* Scheurle/Mayen, *Telekommunikationsgesetz - Kommentar TKG § 88 Rn 40.*
[369] Scheurle/Mayen, *Telekommunikationsgesetz - Kommentar TKG § 88 Rn 40;* Miller, *NdsVBl 2021, 1 (8).*
[370] Gersdorf/Paal, *BeckOK Informations- und Medienrecht GG Art. 10 Rn 34.*
[371] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 183.*
[372] Gersdorf/Paal, *BeckOK Informations- und Medienrecht GG Art. 10 Rn 35.*
[373] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, II. Rechtliche Grundlagen Rn 34.*
[374] Gurlit, *NJW 2010, 1035 (1037).*

b) Das Recht auf informationelle Selbstbestimmung aus Art. 2 I i.V.m. Art. 1 I 1 GG

Das Recht auf informationelle Selbstbestimmung ist die Antwort des BVerfG auf die Frage nach der verfassungsrechtlichen Grundlage des Datenschutzes[375]. Es trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich unter den Bedingungen moderner Datenverarbeitung aus informationsbezogenen Maßnahmen ergeben.[376]

Das Recht auf informationelle Selbstbestimmung ist eine Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 I i.V.m. Art. 1 I 1 GG, das ebenfalls Grundrechtscharakter besitzt.[377] Der Anwendungsbereich des Rechts auf informationelle Selbstbestimmung geht über die Schutzwirkung des allgemeinen Persönlichkeitsrechts hinaus. Konkret geht es um das Recht zu bestimmen, welche Informationen Dritte über die eigene Person wissen oder sagen dürfen, selbst, wenn diese Informationen der Wahrheit entsprechen.[378] Dementsprechend beschränkt sich der Schutz des Rechts auf informationelle Selbstbestimmung nicht nur auf seine Funktion als Abwehrrecht, sondern gilt vielmehr als Recht auf staatliche Schutzvorkehrungen.[379]

(1) Schutzbereich

In Parallele zum allgemeinen Persönlichkeitsrecht entfaltet das Grundrecht auf informationelle Selbstbestimmung eine doppelte Schutzfunktion: Es ist sowohl Ausdruck des Rechts auf Selbstbewahrung als auch des Rechts auf Selbstdarstellung.[380] Es gewährleistet die Befugnis des oder der Einzelnen, grundsätzlich selbst darüber zu entscheiden, ob, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte – also personenbezogene Daten – offenbart werden.[381] Der Schutzbereich ist hierbei weit gezogen und umfasst alle Daten, auch wenn diese im ersten Moment nicht personenbezogen scheinen.[382] Laut dem BVerfG gibt es durch die moderne Datenverarbeitungstechnik kein „belangloses Datum“ mehr, da durch die Herstellung von Querverbindungen sowie das Zusammenstellen und Sammeln von beliebig vielen Daten eine Erstellung von Persönlichkeitsprofilen aus zuvor bedenkenlosen Daten ohne großen Zeitaufwand möglich ist.[383] Zur Begriffsbestimmung des Personenbezug wird hierbei vom BVerfG auf § 2 I BDSG aF zurückgegriffen, der nun in ähnlicher Form in der DS-GVO wiederzufinden ist. Da auch Art. 8 I GRCh auf die Legaldefinition der DS-GVO zurückgreift, ist der Begriff des Personenbezuges in beiden Grundrechten identisch.[384] Geschützt wird der oder die Einzelne

---

[375] Simitis, *NJW 1984, 398 (400).*
[376] Gersdorf/Paal, *BeckOK Informations- und Medienrecht GG Art. 2 Rn 16.*
[377] Taeger/Gabel, *Kommentar DSGVO - BDSG, DS-GVO Art. 1 Rn 25.*
[378] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 143.*
[379] Becker, *NVwZ 2015, 1335 (1336).*
[380] Gersdorf/Paal, *BeckOK Informations- und Medienrecht GG Art. 2 Rn 16.*
[381] Gersdorf/Paal, *BeckOK Informations- und Medienrecht BGB § 823 Rn 145.*
[382] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 150.*
[383] Pieper, *JA 2018, (603).*
[384] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 19.*

vor (unbegrenzter) Erhebung, Speicherung, Verwendung und Weitergabe ebendieser persönlichen Daten[385].

Auf das Recht auf informationelle Selbstbestimmung können sich neben natürlichen Personen auch juristische Personen berufen, wodurch Lücken im Grundrechtsschutz für unternehmensbezogene Informationen abgedeckt werden.[386]

(2) Eingriff in den Schutzbereich

Ein Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung liegt in jeder staatlichen Informationsverarbeitung.[387] Ein Eingriff ist demnach nicht nur die Erhebung von personenbezogenen Daten, sondern auch die Verarbeitung dieser.[388] In Anlehnung an die Rechtsprechung des BVerfG zur automatischen Kennzeichenerfassung liegt jedoch kein Eingriff vor, wenn Daten lediglich gesichtet und auf Relevanz geprüft werden, dabei aber nicht aufbewahrt oder anderweitig verwendet werden.[389]

Die Eingriffsvoraussetzungen sind vergleichbar mit den Voraussetzungen, die Art. 8 GRCh an einen Grundrechtseingriff stellt.[390]

Das Fernmeldegeheimnis aus Art. 10 I GG ist lex specialis zu dem Recht auf informationelle Selbstbestimmung.[391] Soweit die Analyse der Daten des Krankenhausbetriebes andere Daten als Telekommunikationsdaten betrifft, ist dennoch der Schutzbereich des Rechts auf informationelle Selbstbestimmung eröffnet.[392] Hierzu gehören die sogenannten Bestandsdaten, die sich nur auf das grundsätzliche Vertragsverhältnis beziehen und nicht auf konkrete Telekommunikationsvorgänge.[393] Da diese Daten als Stammdaten der Nutzer und Nutzerinnen personenbezogene Daten enthalten und ebenfalls zum Datenbestand gehören, der von Angriffserkennungssystemen ausgewertet wird, ist zumindest bezüglich der Bestandsdaten der Schutzbereich des Rechts auf informationelle Selbstbestimmung eröffnet. Ebenfalls können die log files, die von SIEM-Systemen analysiert werden, Rückschlüsse auf natürliche Personen geben, was auch diesbezüglich den Schutzbereich des Art. 2 I i.V.m. Art. 1 I GG eröffnet.

Beim Einsatz von Angriffserkennungssystemen wird der gesamte Datenbestand auf verdächtige Datenpakete reduziert, um diese anschließend zu speichern und auszuwerten. Bei der Speicherung und Auswertung der verdächtigen Datenpakete kann eine Verarbeitung

---

[385] Vgl. BVerfGR 65, 1 (43).
[386] Gurlit, *NJW 2010, 1035 (1037).*
[387] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 153.*
[388] Pieper, *JA 2018, (603).*
[389] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 21.*
[390] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn 45.*
[391] Maunz u. a., *GG – Kommentar Art. 1o Rn 56.*
[392] Miller, *NdsVBl 2021, 1 (4).*
[393] Scheurle/Mayen, *Telekommunikationsgesetz - Kommentar TKG § 88 Rn 39.*

personenbezogener Daten nicht ausgeschlossen werden; dies stellt somit einen Eingriff in Art. 2 I i.V.m. Art. 1 I GG dar. Der restliche Datenbestand, der nach der ersten Prüfung als unverdächtig eingestuft wird, fällt nicht unter die irrelevante Rechtsprechung zur automatischen Kennzeichenerfassung des BVerfG, da die Betreibenden der Angriffserkennungssysteme auf der ersten Auswertungsstufe noch nicht wissen, welche der Daten tatsächlich verdächtig sind und somit alle erfassten Daten gleich wichtig sind.[394]

Auch hier erfolgt der unmittelbare Eingriff in den Schutzbereich bereits durch einfachrechtliche Rechtsgrundlagen, die die Grundlage zur Nutzung von Angriffserkennungssystemen bilden und einen direkten staatlichen Eingriff darstellen. Im Rahmen der mittelbaren Drittwirkung kann zudem ein mittelbarer „Eingriff" in den Schutzbereich des Rechts auf informationelle Selbstbestimmung angenommen werden, soweit die verarbeiteten Daten nicht bereits in den Schutzbereich des Fernmeldegeheimnisses nach Art. 10 I GG fallen.

(3) Rechtfertigung eines Eingriffs

Das informationelle Selbstbestimmungsrecht wirkt mithin als Ausformung des allgemeinen Persönlichkeitsrechts nicht absolut, sondern findet im Rahmen einer Güter- und Interessenabwägung seine Schranken in der Wechselwirkung mit den Rechten anderer und den Bedürfnissen der sozialen Gesellschaft.[395] Zudem kann eine Rechtfertigung aufgrund des Vorbehalts des Gesetzes nur aufgrund einer gesetzlichen Ermächtigungsgrundlage erfolgen.[396] Diese Ermächtigungsgrundlage muss hierbei bestimmt sein, also den Zweck und den Umfang der Datenverarbeitung klar benennen[397], was den Gefahren einer Vorratsdatenspeicherung entgegenwirkt.[398] Jeder Eingriff muss außerdem einer Verhältnismäßigkeitsprüfung standhalten.[399]

(4) Verhältnis zu anderen Grundrechten

Das Fernmeldegeheimnis aus **Art. 10 I GG** ist lex specialis zu dem Recht auf informationelle Selbstbestimmung. In seinem Anwendungsbereich enthält Art. 10 I GG bezogen auf den Telekommunikationsverkehr eine spezielle Garantie, welche die allgemeine Gewährleistung des Rechts auf informationelle Selbstbestimmung verdrängt.[400] Sind personenbezogene Daten vom Eingriff betroffen, sind die Maßgaben des Rechtes auf informationelle Selbstbestimmung als

[394] Miller, *NdsVBl 2021, 1 (2, 4).*
[395] Gersdorf/Paal, *BeckOK Informations- und Medienrecht BGB § 823 Rn 146.*
[396] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 158.*
[397] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 22.*
[398] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 161.*
[399] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn 46.*
[400] Maunz u. a., *GG – Kommentar Art. 1o Rn 56.*

„normative Verstärkung“ auf den Art. 10 I GG zu übertragen.[401] Im Ergebnis führt dieses Verhältnis zu einer weitgehenden Parallelität des jeweils gewährleisteten Grundrechtsschutzes, der eine Abgrenzung immer irrelevanter erscheinen lässt.[402]

Art. 7 und 8 der GRCh haben im Wesentlichen den gleichen Schutzgehalt wie das nationale Recht auf informationelle Selbstbestimmung. Dies ergibt sich unter anderem aus der diesbezüglichen Rechtsprechung des EuGHs und des BVerfG. Somit kann die Rechtsprechung des BVerfG zum Grundrecht auf informationelle Selbstbestimmung bei der Auslegung von unbestimmten Rechtbegriffen aus der GRCh sowie bei der Auslegung der DS-GVO Anwendung finden.[403]

c) Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 I GG i.V.m. Art. 1 I GG

Mit zunehmender Bedeutung der Nutzung von privaten informationstechnischen Systemen wie Computer oder Smartphones, hat das BVerfG 2008 einen neuen Schutzbereich des Allgemeinen Persönlichkeitsrechtes aus Art. 2 I i.V.m. Art. 1 I 1 GG entwickelt.[404] Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – auch IT-Grundrecht oder Computer-Grundrecht genannt – soll vor den „Gefahren des Datenzugriffs durch Infiltration“ schützen, denen moderne Systeme ausgesetzt sind.[405]

In der Literatur werden aus dieser relativ neuen Ausprägung des allgemeinen Persönlichkeitsrechts auch Konsequenzen für private Rechtsverhältnisse und die Verpflichtung des Gesetzgebers zu entsprechender Gesetzgebung abgeleitet.[406] Als Teil der objektiven Wertordnung sei das Grundrecht auch eine Art „Orientierungsmarke für die Gewährleistung von IT-Sicherheit bei der staatlichen, unternehmerischen und privaten IT-Nutzung“.[407]

(1) Schutzbereich

Anknüpfungspunkt für den Grundrechtsschutz ist das gesamte System, nicht das gespeicherte Datum[408], was dieses Grundrecht vom Recht auf informationelle Selbstbestimmung unterscheidet. Dieses schützt einzelne Informationen, nicht aber die Ausforschung einer Persönlichkeit durch das Eindringen in ein informationstechnisches System, auf dessen Nutzung der oder die

---

[401] Gersdorf/Paal*, BeckOK Informations- und Medienrecht GG Art. 10 Rn 19 ;* Maunz u. a.*, GG – Kommentar Art. 10 Rn 56.*
[402] Maunz u. a.*, GG – Kommentar Art. 10 Rn 56.*
[403] Roßnagel*, NJW 2019, 1 (2).*
[404] Pieper*, JA 2018, (602).*
[405] Gurlit*, NJW 2010, 1035 (1038).*
[406] Gola u. a.*, Bundesdatenschutzgesetz Kommentar§ 1 Rn 13.*
[407] Auer-Reinsdorff/Conrad*, Handbuch IT- und Datenschutzrecht, S. Rn 90.*
[408] Skistims/Roßnagel*, ZD 2012, 3 (5).*

Einzelne angewiesen ist und in dem er oder sie unausweichlich zahllose Spuren hinterlassen muss[409] – sowohl von sich, als auch von seinen Kommunikationspartnern und -partnerinnen.[410]

Der Schutzbereich ist eröffnet, wenn Systeme genutzt werden, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des oder der Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.[411] Dazu gehören das Internet, Personalcomputer, Mobiltelefone, ebenso wie elektrische Geräte in Kraftfahrzeugen oder elektronische Terminkalender.[412] Erfasst werden zudem auch vernetze Geräte, so dass auch Daten, die auf Cloud-Servern gespeichert sind, vom Grundrechtsschutz umfasst sind.[413] Geschützt ist also das Interesse des Nutzers oder der Nutzerin, dass die von einem vom Schutzbereich erfassten IT-System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Vom Schutz erfasst ist aber auch die Integrität des IT-Systems. Das Grundrecht verhindert, dass auf das System so zugegriffen wird, dass dessen Leistung, Funktion und Speicherinhalte durch Dritte genutzt werden können.[414] Verlangt wird weiterhin, dass der Nutzer oder die Nutzerin dem System persönliche Daten „anvertraut". Systeme, die Daten eigenständig sammeln, ohne dass der Nutzer oder die Nutzerin diese im Vertrauen auf die Unzugänglichkeit herausgibt, sind nicht Gegenstand des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[415]

(2) Eingriff in den Schutzbereich

Ein Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme liegt dann vor, wenn das informationstechnische System infiltriert ist, beispielsweise durch die Installation einer Späh-Software[416] Es muss derart auf das System zugegriffen werden, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden könnten.[417] Hierbei ist es nicht erforderlich, dass die Daten tatsächlich ausgelesen werden.[418]

Sowohl IDS wie auch SIEM-Systeme analysieren automatisiert die Datenströme eines Netzwerkes auf Auffälligkeiten. Hierbei werden jedoch keine Daten überwacht, ausgespäht oder

---

[409] Hirsch, *NJOZ 2008, 1907 (1915).*
[410] Kutscha, *NJW 2008, 1042 (1043).*
[411] BVerfG Urt. V 27.2.2008 – 1 BvR 370/07 und 1 BvR 595/07, Rn 203.
[412] Gola u. a., *Bundesdatenschutzgesetz Kommentar§ 1 Rn 13.*
[413] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 189.*
[414] Roßnagel/Schnabel, *NJW 2008, 3534 (3535).*
[415] Franck, *Smart Grids und Datenschutz: Verarbeitung von Energiedaten in intelligenten Stromnetzen aus datenschutzrechtlicher Perspektive, S. 155.*
[416] Skistims/Roßnagel, *ZD 2012, 3 (5).*
[417] Luch, *MMR 2011, 75 (76).*
[418] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 42.*

manipuliert. Die Daten verbleiben aufgrund des automatisierten Arbeitsvorganges und dem Unterbleiben einer Inhaltsanalyse vertraulich. Zudem unterwandern die Angriffserkennungssysteme nicht das System, in dem sie eingesetzt werden, sondern sollen vielmehr durch eine Unterwanderung von außen schützen.

Somit fällt der Einsatz von Angriffserkennungssystemen nicht in den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und es liegt dies bezogen kein Grundrechtseingriff vor.

(3) Rechtfertigung eines Eingriffs

Seine Schranken findet das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme im Grundsatz des Gesetzesvorbehalts für Grundrechtseingriffe.[419] Eine heimliche Infiltration ist nur zulässig, wenn Anhaltspunkt für eine konkrete Gefahr für Leib, Leben oder Freiheit der betroffenen Person oder der Allgemeinheit bestehen.[420]

(4) Verhältnis zu anderen Grundrechten

Jedoch ist das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme subsidiär gegenüber den Grundrechten auf Fernmeldegeheimnis (**Art. 10 GG**) sowie dem **Recht auf informationelle Selbstbestimmung** zu behandeln[421] und nur dann anwendbar, wenn diese anderen Grundrechte keinen (hinreichenden) Schutz bieten können.[422]

(5) Kritik

Seit der Schöpfung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, wurde in der Literatur viel Kritik an der Entscheidung des BVerfG geäußert. Kritische Stimmen halten das neue Grundrecht für eine „unnötige Verkomplizierung der grundrechtlichen Dogmatik“, da keine Schutzlücke bestanden hätte. Die Infiltrierung von informationstechnischen Systemen und die Auswertung derer Daten stelle einen Eingriff in das Recht auf informationelle Selbstbestimmung dar und könne ihre Grenzen in der Verhältnismäßigkeitsprüfung finden.[423] Auch gibt es keine weitere Konkretisierung und Auslegung des

[419] Kutscha, *NJW 2008, 1042 (1043).*
[420] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 43.*
[421] Auer-Reinsdorff/Conrad, *Handbuch IT- und Datenschutzrecht, S. Rn 93.*
[422] Franck, *Smart Grids und Datenschutz: Verarbeitung von Energiedaten in intelligenten Stromnetzen aus datenschutzrechtlicher Perspektive, S. 156.*
[423] Pieper, *JA 2018, (602).*

Grundrechtes, da sich das BVerfG bisher in nur wenigen Gerichtsentscheidungen mit der Grundrechtsausprägung auseinandersetzt.[424]

2. Unionsrechtliche Ebene

Auf unionsrechtlicher Ebene bilden Art. 7 und Art. 8 GRCh die datenschutzrechtlich relevanten Grundrechte. Hinzu treten auf europäischer Primärebene Art. 16 AEUV und Art. 39 EUV sowie auf völkerrechtlicher Ebene Art. 8 EMRK.[425]

a) Das Recht auf die Achtung des Privat- und Familienlebens nach Art. 7 GRCh

In Art. 7 GRCh ist das Grundrecht der Privatheit normiert. Dieses ist in vier Teilbereiche, die keine eigenständigen Grundrechte darstellen, unterteilt[426]: Die Gewährleistung auf Privatleben, auf Familienleben, auf die Wohnung und die Kommunikation.[427] Es umfasst somit alle Bereiche des Lebens, die Fremde nicht betreffen sollen und inkludiert somit auch das „Recht auf Alleingelassen werden".[428] Die jeweiligen Schutzbereiche sind teilweise klar voneinander zu trennen, können sich jedoch auch gegenseitig überlagern.[429] Art. 7 GRCh gewährleistet keine allgemeine Handlungsfreiheit.[430]

Die Rechte aus Art. 7 GRCh entsprechen den Vorschriften des Art. 8 EMRK und haben daher gem. Art. 52 III 1 GRCh die gleiche Bedeutung und Tragweite wie die Konventionsrechte, so dass auch die Rechtsprechung des EGMR zu Art. 8 EMRK bei der Anwendung des Art. 7 GRCh hinzugezogen werden kann.[431]

(1) Der Schutzbereich der Gewährleistung auf Privatleben

Unter den Begriff des Privatlebens fällt im Rahmen des Art. 7 GRCh die freie Entscheidung des oder der Einzelnen über seine oder ihre persönliche Lebensführung und ob diese öffentlich gemacht werden soll. Im Vergleich zu den anderen Teilbereichen des Art. 7 GRCh ist das

[424] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Verfassungsrechtliche Grundlagen, Europäisches und nationales Recht Rn 50.*
[425] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch I. Kapitel 1. Rn 11.*
[426] Gersdorf/Paal, *BeckOK Informations- und Medienrecht, Kap. EU-GRCharta Art. 7 Rn 8.*
[427] Roßnagel, *NJW 2019, 1 (2).*
[428] Nebel, *ZD 2015, 517 (521).*
[429] Meyer/Hölscheidt, *Charta der Grundrechte der Europäischen Union, Kap. GRCh Art. 7 Rn 1.*
[430] Meyer/Hölscheidt, *Charta der Grundrechte der Europäischen Union, Kap. GRCh Art. 7 Rn 11.*
[431] Jarass, *Charta der Grundrechte der Europäischen Union Kommentar Art. 7 Rn 1.*

Schutzgut des Privatlebens das weiteste.[432] Ein wichtiges Kriterium des Privatlebens ist laut der Rechtsprechung des EGMR zu Art. 8 EMRK die „Nicht-Öffentlichkeit". Tätigkeiten, die einen ausgeprägten Öffentlichkeitsbezug aufweisen, fallen nicht in den Schutzbereich der Gewährleistung des Privatlebens.[433] Art. 7 GRCh erfasst einhergehend mit der freien Entfaltung der eigenen Persönlichkeit im sozialen Umfeld auch das Recht zu entscheiden, wer darüber Kenntnis erhalten soll.[434]

In der datenschutzrechtlichen Rechtsprechung des EuGH wird überwiegend von Art. 7 GRCh im Zusammenhang mit Art. 8 GRCh gesprochen. Hierbei wird insbesondere der Teilbereich der Gewährleistung des Privatlebens erörtert.[435]

(2) Der Schutzbereich der Kommunikation

Im Gegensatz zu der Freiheit der Meinungsäußerung aus Art. 11 GRCh schützt Art. 7 GRCh nur den Übermittlungsvorgang der Kommunikation durch Dritte, also die Fernkommunikation.[436] Geschützt ist hierbei nur die Individualkommunikation, da Art. 7 GRCh den öffentlichen Bereich nicht miterfasst.[437] Dies liest sich aus dem Kriterium der Privatheit ab, welches nicht auf die Rechtsform der Kommunizierenden abstellt, sondern eben auf die Individualität der Kommunikation.[438]

Der offene Begriff „Kommunikation" lässt hierbei dem technologischen Fortschritt Raum[439], da die Technik keine Rolle im Schutzbereich des Art. 7 GRCh spielt. Erfasst wird eine Übermittlung beispielsweise durch Briefe ebenso wie durch Telefon, E-Mail, Sprachnachrichten oder Messenger-Apps. Es kommt zudem nicht auf den konkreten Inhalt der Kommunikation an. So sind neben dem gesprochenen Wort auch Texte, Fotografien oder Smileys geschützt.[440]

Die Teilbereiche der Gewährleistung des Privatlebens und der Kommunikation entsprechen den Schutzbereichen des deutschen Grundrechtes auf informationelle Selbstbestimmung aus Art. 2 I i.V.m. Art. 1 I GG und dem Telekommunikationsgeheimnis nach Art. 10 GG, wobei Art. 7 GRCh keinen Auffangtatbestand darstellt.[441]

---

[432] Calliess/Ruffert, *EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar, Kap. EU-GRCharta Art. 7 Rn 3.*
[433] Meyer/Hölscheidt, *Charta der Grundrechte der Europäischen Union, Kap. CRCh Art. 7 Rn 15.*
[434] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 31.*
[435] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht § 2 Rn 10.*
[436] Jarass, *Charta der Grundrechte der Europäischen Union Kommentar Art. 7 Rn 6.*
[437] Gersdorf/Paal, *BeckOK Informations- und Medienrecht Art. 7 Rn 35.*
[438] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 26.*
[439] Nebel, *ZD 2015, 517 (521).*
[440] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 26.*
[441] Roßnagel, *NJW 2019, 1 (2).*

Grundrechtsträger und -trägerinnen sind natürliche Personen. Nach Art. 52 GRCh können juristische Personen Träger des Grundrechtes sein, wenn ihre Schutzbedürftigkeit funktionell mit natürlichen Personen vergleichbar ist.[442]

(3) Eingriff in den Schutzbereich

Ein Eingriff in den Schutzbereich des Art. 7 GRCh liegt grundsätzlich beim Eindringen in die Privatsphäre vor, unabhängig davon, ob der dadurch erlangte Zugriff auf Informationen für den Betroffenen oder die Betroffene nachteilig ist oder nicht und um welche Art von Daten es sich handelt.[443]

Ein Eingriff in die Kommunikationsfreiheit ist gegeben, wenn ein Dritter durch Zugriff auf den Kommunikationsvorgang Kenntnis von dessen Inhalt erhält. Ebenfalls wird ein Eingriff in den Schutzbereich bejaht, wenn die Kommunikation verhindert oder verzögert wird.[444]

Zudem wenden der EuGH einen weiten Eingriffsbegriff an und erfasst somit auch mittelbare Beeinträchtigungen als Eingriff in den Schutzbereich des Art. 7 GRCh. Ein mittelbarer Eingriff zeichnet sich dadurch aus, dass die Beeinträchtigung der betroffenen Grundrechte nicht der primäre Zweck ist.[445]

Wie bereits beim im Rahmen der Prüfung des Art. 10 I GG erörtert, werden bei der Auswertung durch Angriffserkennungssystemen sämtliche im zu überwachenden System anfallenden Datenströme, also Verkehrs- und Inhaltsdaten der Telekommunikation, analysiert.

Die europäischen Grundrechte binden nach Art. 51 I GRCh die Organe der Union und die Mitgliedstaaten bei der Durchführung des Rechts der Union und stellen somit, wie in der deutschen Verfassung, in erster Linie Abwehrrechte gegenüber staatlichen Eingriffen dar. Auch hier erflogt der unmittelbare Eingriff in den Schutzbereich des des Art. 7 GRCh primär durch Unionsrecht wie der DS-GVO, die im Verlauf dieser Abhandlung auf eine Ermächtigungsgrundlage zur Nutzung von Angriffserkennungssystemen durch Privatrechtssubjekte untersucht wird. Aus sekundärer, mittelbarer Ebene liegt bei dem Einsatz von Angriffserkennungssystemen ein „Eingriff" i.S.d. grundrechtlichen Drittwirkung in den Schutzbereich der Kommunikationsfreiheit, die das unionrechtliche Pendant zu Art. 10 I GG ergibt, vor.

---

[442] Calliess/Ruffert, *EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar, Kap. EU-GRCharta Art. 7 Rn 11;* Meyer/Hölscheidt, *Charta der Grundrechte der Europäischen Union, Kap. GRCh Art. 7 Rn 22.*

[443] Jarass, *Charta der Grundrechte der Europäischen Union Kommentar Art. 7 Rn 28;* Bieker, *DuD 2018, 27 (28).*

[444] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 27.*

[445] Bieker, *DuD 2018, 27 (28).*

(4) Rechtfertigung eines Eingriffs

Art. 7 GRCh enthält keinen Gesetzesvorbehalt. Es gilt der allgemeine Schrankenvorbehalt des Art. 52 I GRCh.[446] Zudem müssen aufgrund der Entstehungsgeschichte des Art. 7 GRCh und den hierzu getätigten Erläuterung des Präsidiums des Grundrechtskonvents die Vorgaben zu Art. 8 EMRK und der dazugehörigen Rechtsprechung zur Grundrechtseinschränkung ebenfalls befolgt werden.[447] Es bedarf sowohl gem. Art. 52 I GRCh als auch gem. Art. 8 II EMRK einer gesetzlichen Grundlage[448], wobei Art. 52 I GRCh einen einfachen Gesetzesvorbehalt beinhaltet, während Art. 8 II EMRK einen qualifizierten Gesetzesvorbehalt vorgibt und somit lex specialis ist.[449] Laut Art. 8 II EMRK ist ein Eingriff in das Grundrecht des Art. 7 GRCh nur gerechtfertigt, „soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer“.

b) Der Schutz personenbezogener Daten nach Art. 8 GRCh

Anders als in den Verfassungen der Mitgliedstaaten enthält die Grundrechte-Charta durch Art. 8 eine konkrete grundrechtliche Datenschutzgewährleistung.[450] Art. 8 GRCh schützt die Entscheidungsbefugnis des oder der Betroffenen über seine oder ihre personenbezogenen Daten und gibt dem Datenschutz folglich eine unionsrechtliche Stellung.[451] Der Artikel basiert auf Art. 16 AEUV und Art. 39 EUV sowie auf Art. 8 EMRK.[452] Die Norm weist die Besonderheit auf, dass neben dem grundrechtlichen Rahmen auch Sonderpflichten (Abs. II) sowie formellrechtliche Anforderungen (Abs. III) an den Datenschutz gestellt werden.[453]

(1) Schutzbereich

In den Schutzbereich des Art. 8 I GRCh fallen alle personenbezogenen Daten.[454] Für die nähere Definition der Personenbezogenheit wird die Legaldefinition des Art. 4 Nr. 1 DS-GVO genutzt, die als Sekundärrecht zwar nicht unmittelbar aus Art. 8 GRCh ableitbar ist, aber mit dem höherrangigen Recht der Grundrechte-Charta in Einklang steht und somit zur Auslegung der

[446] Jarass, *Charta der Grundrechte der Europäischen Union Kommentar Art. 7 Rn 34.*
[447] Meyer/Hölscheidt, *Charta der Grundrechte der Europäischen Union, Kap. CRCh Art. 7 Rn 14.*
[448] Meyer, *Charta der Grundrechte der Europäischen Union Kommentar Art. 7 Rn 18.*
[449] Gersdorf/Paal, *BeckOK Informations- und Medienrecht, Kap. EU-GRCharta Art. 7 Rn 40.*
[450] Calliess/Ruffert, *EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar, EU-GRCharta Art. 8 Rn 2.*
[451] Grabitz u. a., *Das Recht der Europäischen Union: EUV/AEUV AEUV Art. 16 Rn 5.*
[452] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 12.*
[453] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 24.*
[454] Bergmann/Dienelt, *Ausländerrecht: AuslR EU-Grundrechte-Charta, Art. 8 Rn 1.*

Grundrechte-Charta herangezogen werden kann.[455] Unter den weit gefassten Begriff der Daten fallen sämtliche Informationen, ungeachtet ihres Dateiformates oder des Grades ihrer Sensibilität.[456] Für den Gewährleistungsgehalt des Art. 8 I GRCh ist es zudem unerheblich, ob die personenbezogenen Daten Bedeutung für den europäischen Binnenmarkt haben.[457] Das durch Art. 8 GRCh geschützte Verhalten beinhaltet „die Herrschaft über die eigenen Daten" und dementsprechend das Recht, Dritte von der Verarbeitung dieser Daten auszuschließen.[458] Vom Grundrechtsschutz erfasst sind zudem durch Art. 8 II GRCh die Auskunft- und Berichtigungsrechte der Betroffenen. Diese finden ihre Ausgestaltung in der DS-GVO.[459]

Grundrechtsträger und -trägerinnen sind natürliche Personen. Ob auch juristische Personen grundrechtsberechtigt sein können, ist umstritten. Grundsätzlich können sich juristische Personen jedoch auf das Recht aus Art. 8 I GRCh berufen, sofern die hinter der juristischen Person stehenden natürlichen Personen schutzbedürftig sind.[460]

(2) Eingriff in den Schutzbereich

Ein Eingriff in den Schutzbereich des Art. 8 GRCh liegt vor, wenn personenbezogene Daten verarbeitet werden.[461] Eine Verarbeitung von Daten liegt in jeder Erhebung, Speicherung, Verwendung, Sperrung oder Löschung sowie der Weitergabe von Daten.[462] Hierbei knüpft Art. 8 GRCh an den Begriff des Verarbeitens aus Art. 4 Nr. 2 DS-GVO an.[463] Jede dort aufgeführte Tätigkeit des Verarbeitens stellt laut EuGH stellt einen Eingriff in den Schutzbereich des Art. 8 GRCh dar.[464] Das Verfahren bei der Verarbeitung von personenbezogenen Daten ist nicht entscheidend, sodass sowohl manuelle als auch die automatisierte Datenverarbeitung vom Schutzbereich des Art. 8 GRCh erfasst wird.[465] Irrelevant ist zudem, ob es sich bei den Informationen um sensible Daten handelt, ob die Verarbeitung für den Betroffenen oder die Betroffene nachteilig ist[466] und ob aktiv vom Inhalt der verarbeiteten Daten Kenntnis genommen

---

[455] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 13.*
[456] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 8.*
[457] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 13.*
[458] Calliess/Ruffert, *EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar, EU-GRCharta Art. 8 Rn 9.*
[459] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 11.*
[460] Calliess/Ruffert, *EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar, Kap. EU-GRCharta Art. 8 Rn 11;* Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, Kap. § 2 Rn 15.*
[461] Calliess/Ruffert, *EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar, EU-GRCharta Art. 8 Rn 12.*
[462] Bergmann/Dienelt, *Ausländerrecht: AuslR EU-Grundrechte-Charta, Art. 8 Rn 1.*
[463] Roßnagel, *NJW 2019, 1 (3).*
[464] Gersdorf/Paal, *BeckOK Informations- und Medienrecht EU-GRCharta, Art. 8 Rn 18.*
[465] Gersdorf/Paal, *BeckOK Informations- und Medienrecht EU-GRCharta, Art. 8 Rn 19.*
[466] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 16.*

wurde.[467] Art. 8 GRCh verkörpert neben seiner Daseinsfunktion als klassisches Abwehrrecht gegen staatliches Handeln auch eine Schutzpflicht der Grundrechtsverpflichteten gegenüber privatem Handeln. Ein Eingriff kann demnach auch durch ein Unterlassen trotz Schutzpflicht erfolgen.[468]

Eine Datenverarbeitung stellt jedoch keine Beeinträchtigung dar, wenn der oder die Betroffene wirksam in die Verarbeitung eingewilligt hat. Die **dogmatische Einordnung der Einwilligung** in den Grundrechtsaufbau wird bisweilen in der Literatur diskutiert.[469] Strittig ist, ob die Einwilligung einen Eingriffsausschluss darstellt oder als Rechtfertigungsgrund zu behandeln ist. Als Argument für eine Einordnung der Einwilligung als Rechtfertigungsgrund wird die systematische Verortung von Einwilligung und Schrankenregelungen in Art. 8 II 1 GRCh genannt.[470] Für eine Klassifizierung der Einwilligung als Eingriffsausschluss spricht der Wortlaut der Norm, da durch eine wirksame Einwilligung die Erfordernis einer gesetzlichen Ermächtigungsgrundlage für einen Eingriff entfällt und Art. 52 I GRCh als allgemeiner Schrankenvorbehalt nicht zur Anwendung kommt.[471]

Die Inhalts-, Verkehrs- und Bestandsdaten, die automatisiert von Angriffserkennungssystemen ausgewertet werden, lassen Rückschlüsse auf natürliche Personen zu, wie bereits in der Prüfung zu Art. 2 I i.V.m. Art. 1 I GG erörtert. Der Schutzbereich des Art. 8 I GRCh ist folglich eröffnet. Da bereits jede Verarbeitung dieser Daten einen Eingriff in diesen Schutzbereich darstellt und es nicht auf eine automatische beziehungsweise nichtautomatische Verarbeitung ankommt, liegt ein direkter staatlicher Eingriff bereits durch entsprechende unionsrechtliche Erlaubnistatbestandsnormen vor, wie sie im weiter Verlauf dieser Abhandlung geprüft werden. Ein mittelbarer „Eingriff" i.S.d. Drittwirkung von Grundrechten (der wiederrum durch diese Erlaubnistatbestandsnormen legitimiert werden kann) liegt zudem vor, da die Angriffserkennungssysteme automatisiert die gesamten Datenströme eines Netzwerkes auf Anomalien oder auffällige Muster untersuchen und somit i.S.d. DS-GVO verarbeiten.

(3) Rechtfertigung eines Eingriffs

Art. 8 II und III GRCh konkretisiert den allgemeinen Gesetzesvorbehalt des Art. 52 I GRCh. Ein Eingriff in den Schutzbereich ist nur zulässig, wenn dies ein Gesetz erlaubt und die Verarbeitung dem Grundsatz von Treu und Glauben entspricht. Zudem muss das Gesetz eine Zweckfestlegung und eine Zweckbindung vorsehen, der betroffenen Person ein Recht auf Auskunft zubilligen und die Datenverarbeitung der Kontrolle einer unabhängigen Stelle unterwerfen.[472]

---

[467] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 10.*
[468] Gersdorf/Paal, *BeckOK Informations- und Medienrecht EU-GRCharta, Art. 8 Rn 12.*
[469] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 18.*
[470] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 52.*
[471] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 59.*
[472] Roßnagel, *NJW 2019, 1 (5).*

Art. 8 II GRCh ist nicht lex specialis gegenüber den allgemeinen Schrankenregelungen des Art. 52 I GRCh, sondern lediglich eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes. Es gilt bei einer möglichen Rechtfertigung von Eingriffen in das Datenschutzgrundrecht Art. 8 II GRCh i.V.m. Art. 52 I GRCh zu prüfen.[473]

Hervorzuheben ist hier insbesondere die Zweckbindung als Konkretisierung des allgemeinen Verhältnismäßigkeitsgrundsatzes. Das Erfordernis der Zweckbindung verhindert eine grenzenlose Verwendungsfreiheit für Daten, die zuvor rechtmäßig erhoben wurden.[474] Eine spezielle Ausprägung des Zweckbindungs- und Erforderlichkeitsgrundsatzes ist zudem das vom EuGH entwickelte Recht auf Vergessenwerden, das kein Grundrecht darstellt, sondern eine Ausformung der Schranke des Art. 8 GRCh.[475]

c) Das Verhältnis zwischen Art. 7 und Art. 8 GRCh

Das Verhältnis zwischen Art. 7 und Art. 8 GRCh ist nicht abschließend geklärt.

In seiner Rechtsprechung hat der EuGH in wichtigen Entscheidungen wie Google Spain, Digital Rights Ireland und Tele2Sverige stets beide Artikel gemeinsam geprüft[476], hierbei aber auch gleichzeitig die Selbständigkeit der Vorschriften betont.[477] Aufgrund der gemeinsame Prüfung, kann von einer „ideellen Aufgabenteilung“ zwischen den beiden Grundrechten gesprochen werden. Art. 7 GRCh vertritt hierbei die menschenrechtliche Tradition, auf der der Datenschutz fußt wohingegen Art. 8 GRCh die moderne, digitale Seite des Datenschutzes mit detaillierten Regelungen abdeckt.[478] Beide Grundrechte verstärken sich hierbei gegenseitig. Die Regelungsweise des EuGH wird als Verbindungslösung betitelt.[479] Für eine Idealkonkurrenz zwischen Art. 7 und Art. 8 GRCh spricht zudem der gemeinsame Ursprung. Beide Artikel gehen auf Art. 8 EMRK zurück, der aufgrund Art. 52 III GRCh weiterhin zu beachten ist.[480]

In der Literatur wird weitestgehend Art. 8 GRCh als lex specialis zu Art. 7 GRCh angesehen, sobald personenbezogene Daten verarbeitet werden, da dieser eine Konkretisierung der Gewährleistung des Privatlebens darstelle.[481] So können zudem Abgrenzungsschwierigkeiten vermieden werden, da es – anders als in der deutschen Verfassung – ein zentrales Datenschutzgrundrecht gäbe.[482] Andere Meinungen sprechen zwar von Idealkonkurrenz zwischen den

---

[473] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 61.*
[474] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 13.*
[475] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, A. II. Rechtliche Grundlagen Rn 15.*
[476] Michl, *DuD 2017, 349 (351).*
[477] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 53.*
[478] Michl, *DuD 2017, 349 (353).*
[479] Roßnagel, *NJW 2019, 1 (2).*
[480] Calliess/Ruffert, *EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar, EU-GRCharta Art. 8 Rn 1.*
[481] Gersdorf/Paal, *BeckOK Informations- und Medienrecht, Kap. EU-GRCharta Art. 7 Rn 17.*
[482] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 53.*

beiden Artikeln, räumen Art. 8 GRCh dennoch eine gewisse Art von Spezialisierung gegenüber Art. 7 GRCh ein.[483] Art. 7 GRCh bliebe aber für die Abwägung der Eingriffsintensivität relevant.[484]

In der Praxis kann davon ausgegangen werden, dass sich die Verbindungslösung des EuGH durchsetzen wird.[485]

d) Das Verhältnis zu Art. 16 AEUV

Neben Art. 7 und Art. 8 GRCh normiert Art. 16 AEUV ebenfalls Anforderungen an das unionale Datenschutzrecht. Ferner normiert Art. 16 AEUV erstmalig eine Datenschutzkompetenz der Union.[486] Art. 16 I AEUV ist hierbei wortgleich zu Art. 8 I GRCh und umschreibt die Grundsätze des Datenschutzrechts.[487] In Abs. II des Art. 16 AEUV werden die Kompetenzen der Union sowie das Verfahren zum Erlass von Datenschutzvorschriften geregelt. Vorschriften, die aufgrund dieser Grundlage erlassen worden, lassen gem. UAbs. II die spezifischen Regelungen des Art. 39 EUV jedoch unberührt.[488] Art. 39 EUV regelt das Verfahren für den Erlass von datenschutzrechtlichen Regelungen durch die Mitgliedstaaten bei Tätigkeiten der gemeinsamen Außen- und Sicherheitspolitik. Zuständig für den Erlass von Sekundärrecht ist hierbei der Rat.[489] Art. 16 II UAbs. I 1 1. HS AEUV setzt die Normsetzungsbefugnis und somit die Rechtsgrundlage, auf die sich die DS-GVO begründet.[490]

Die Artikel der GRCh sowie der Verträge (EUV und AEUV) sind gem. Art. 6 I EUV gleichrangig und stellen jeweils europäisches Primärrecht dar.[491] Die doppelte Gewährleistung des Rechts auf Datenschutz stellt die Frage nach dem Verhältnis der beiden Normen zueinander. Der übereinstimmende Wortlaut des Art. 8 I CRCh und des Art. 16 I AEUV könnte auf das Bestehen zweier Datenschutz-Grundrechte hindeuten.[492] Hiergegen spricht jedoch die Schrankenfreiheit des Art. 16 AEUV, der somit als Grundrecht eine grenzenlose Gewährleistung des Datenschutzes mit sich bringen würde, da auch die allgemeinen Schranken des Art. 52 GRCh nicht anwendbar wären.[493] Zudem enthält Art. 16 II AEUV eine ausdrückliche Ermächtigung für eingreifende Regelungen und würde seine Bedeutung verlieren, wenn Art. 16 I AEUV als Grundrecht schrankenlos gewährleistet werden würde.[494] Art. 16 I AEUV hat folglich lediglich eine deklaratorische Funktion. Er wiederholt vielmehr das Grundrecht auf Datenschutz, dass

---

[483] Michl, *DuD 2017, 349 (352).*
[484] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 34.*
[485] Michl, *DuD 2017, 349 (353).*
[486] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen, Rn 13.*
[487] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch I. Kapitel 2. Rn 24.*
[488] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen, Rn 13.*
[489] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 16.*
[490] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 38.*
[491] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 51.*
[492] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 37.*
[493] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 36 ff.*
[494] Schantz/Wolff, *Das neue Datenschutzrecht, A. Verfassungs- und unionsrechtliche Grundlagen Rn 36 ff.*

durch Art. 8 II und Art. 52 II GRCh eingeschränkt werden kann. Der wesentliche Aspekt des Art. 16 AEUV ist sein Abs. II, der die Kompetenzen der Union sowie die Verfahrensweise zum Erlass von datenschutzrechtlichem Sekundärrecht näher definiert.[495]

e) Das Verhältnis zu Art. 8 EMRK

Mit Inkrafttreten des Vertrages von Lissabon am 01. Dezember 2009 wurde der Grundrechte-Charta primärrechtlicher Charakter zugesprochen. Bis zu diesem Zeitpunkt zitierte der EuGH überwiegend die EMRK sowie die Rechtsprechung des EGMR, wenn es um grundrechtliche Ausführungen ging.[496] Dies ist durch Art. 6 III EUV möglich, der die EMRK als „allgemeine Rechtserkenntnisquelle" in das unionale Recht eingliedert.[497] Da völkerrechtliche Verträge in die europäische Rechtsordnung eingegliedert werden müssen, stehen sie hierarchisch zwar unter dem Primärrecht, werden dogmatisch aber als nebeneinander stehend betrachtet.[498] Dass diese dogmatische Einordnung vor allem im Verhältnis von der GRCh zur EMRK Gültigkeit hat, zeigt Art. 52 II GRCh: demnach haben diejenigen Grundrechte der Charta, „die den durch die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen, {…} die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird".

Zwar wird das Recht auf Datenschutz durch Art. 16 AEUV und Art. 7 und 8 der GRCh mittlerweile ausdrücklich normiert, jedoch gibt es in Bezug auf Art. 8 EMRK schon langjährige datenschutzrechtliche Auslegungen und Konkretisierungen durch die Rechtsprechung des EGMR. Diese muss auch weiterhin bei der Auslegung der GRCh berücksichtigt werden.[499]

3. Zusammenfassung

Wird von Mitgliedstaaten der EU zwingendes Unionsrecht umgesetzt oder vollzogen, so ist das mitgliedstaatliche Handeln an der europäischen Grundrechte-Charta zu bemessen. Dies gilt für weite Teile der DS-GVO. Für die Öffnungsklauseln der DS-GVO und den damit einhergehenden mitgliedstaatlichen Gestaltungsspielräumen ist der Anwendungsvorrang der europäischen Grundrechte-Charta vor den nationalen Grundrechtskatalogen jedoch strittig.

Zwar binden die europäischen Grundrechte-Charta sowie das deutsche Grundgesetz unmittelbar nur die Mitgliedstaaten beziehungsweise den deutschen Staat und bilden Abwehrrechte und Schutzrechte gegen staatliches Handeln, jedoch ist auf beiden Ebenen eine mittelbare Drittwirkung der Grundrechte auf Privatrechtssubjekte anerkannt. Folglich müssen sich auch

---

[495] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, Kap. § 2 Rn 37;* Grabitz u. a., *Das Recht der Europäischen Union: EUV/AEUV, Kap. AEUV Art. 16 Rn 8.*
[496] Michl, *DuD 2017, 349 (350).*
[497] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 40.*
[498] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht, § 2 Rn 51.*
[499] Gersdorf/Paal, *BeckOK Informations- und Medienrecht, Kap. EU-GRCharta Art. 7 Rn 7.*

Privatrechtssubjekte bei der Verarbeitung personenbezogener Daten an der jeweils vorrangigen Verfassung messen lassen. Zudem kann die Europäische Union beziehungsweise der Mitgliedstaat gezwungen sein, Schutzmaßnahmen in Form eines Gesetzes zu erlassen.

Angriffserkennungssysteme analysieren den gesamten Datenverkehr in den Netzwerken und Systemen, in denen sie eingesetzt werden. Je umfassender Daten zur Verfügung stehen, desto höher ist die Wirksamkeit der Angriffserkennung. Somit werden auch personenbezogenen und -beziehbare Daten in den Angriffserkennungssystemen verarbeitet.

Grundrechte stellen in erster Linie Abwehrrechte gegenüber staatlichen Eingriffen dar und binden auf nationaler Ebene nur die drei Staatsgewalten unmittelbar sowie auf unionsrechtlicher Ebene die Organe der Union und die Mitgliedstaaten bei der Durchführung des Rechts der Union. Bereits durch die einfachrechtlichen Rechtsgrundlagen, die im Verlauf dieser Abhandlung auf eine Ermächtigungsgrundlage zur Nutzung von Angriffserkennungssystemen durch Privatrechtssubjekte untersucht werden, wird in die Schutzbereiche der datenschutzrelevanten Grundrechte der betroffenen Personen auf unions- sowie mitgliedstaatlicher Ebene eingegriffen. Namentlich sind dies Art. 7 und 8 GRCh sowie Art. 2 I i.V.m. Art. 1 I 1 GG. Zudem wird in das Fernmeldegeheimnis nach Art. 10 I GG eingegriffen. Dieser staatliche Eingriff in die Grundrechte kann auf zweiter Ebene sogleich die Legitimation des tatsächlichen, mittelbaren Eingriffs in die Rechte der betroffenen Personen durch die Nutzung von Angriffserkennungssysteme durch Privatrechtssubjekte darstellen. Im Folgenden gilt es somit zu prüfen, ob eine solche Legitimation für den mittelbaren Eingriff in die betroffenen Grundrechte durch Privatrechtssubjekte auf national- sowie unionsrechtlicher Ebene tatsächlich vorliegt.

IV. Die Rechtmäßigkeit des Einsatzes von Angriffserkennungssystemen nach dem Telekommunikationsgesetz (TKG)

Eine mögliche Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft könnte auf nationalrechtlicher Ebene das Telekommunikationsgesetz (TKG) enthalten.

Zum Zeitpunkt dieser Arbeit ist das TKG im Umbruch. Der Deutsche Bundestag hat in seiner 224. Sitzung am 22. April 2021 den von der Bundesregierung eingebrachten Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz) angenommen. Das Telekommunikationsmodernisierungsgesetz (TKMoG) tritt zum 01. Dezember 2021 in Kraft und ist mit weitreichenden Änderungen des Telekommunikationsgesetzes (TKG) verbunden. Dieses tritt gleichzeitig in seiner alten Fassung außer Kraft.

Da von dieser Änderung auch die datenschutzrechtlichen Regelungen des TKG betroffen sind und aufgrund der Aktualität keine vertiefende Literatur zum Stand der Bearbeitung vorhanden ist, wird im Folgenden die Rechtmäßigkeit des Einsatzes von Angriffserkennungssystemen in privatrechtlich organisierten Krankenhäusern nach dem TKG a.F. sowie dem TKG neu geprüft. Der hierdurch erfolgende Rechtsvergleich erleichtert das Verständnis des TKG neu im Kontext des Datenschutzes und der Datensicherheit.

A. Die Rechtmäßigkeit nach dem TKG a.F.

Durch das TKG a.F. sollte durch Wettbewerbsregulierung und Förderung eine angemessene TK-Dienstleistung gewährleistet werden. Hierzu gehörten ebenfalls Regelungen zum Fernmeldegeheimnis, zum Datenschutz und zur Öffentlichen Sicherheit.[500] Durch das in § 88 TKG a.F. geregelte Fernmeldegeheimnis wurde der grundrechtliche Schutz des Art. 10 I GG im Bereich der Telekommunikationsdienstleistungen auf das Verhältnis zwischen Privatrechtssubjekten untereinander übertragen. Der Schutzbereich entsprach hierbei dem des Art. 10 I GG und erstreckte sich auf den Zeitraum der Nachrichtenübermittlung und eventuelle Zwischenspeicherungen.[501]

§ 88 TKG a.F. verpflichtete jedoch ausdrücklich in Absatz II nur Telekommunikations-Diensteanbieter (TK-Diensteanbieter) i.S.d. § 3 Nr. 6 TKG a.F..

Im Folgenden beschäftigt sich die Arbeit zunächst mit dem Anwendungsverhältnis der datenschutzrechtlichen Regelungen des TKG a.F. zur DS-GVO. In einem weiteren Schritt wird geklärt, ob privatrechtlich organisierte Krankenhäuser öffentlich zugängliche TK-Diensteanbieter i.S.d. § 3 Nr. 6 TKG a.F. darstellten und falls ja, ob es bereits eine Ermächtigungsgrundlage zur Nutzung von IDS in den Netzwerken dieser Krankenhäuser im TKG a.F. gab.

1. Verhältnis des TKG a.F. zur DS-GVO

Seit Inkrafttreten der DS-GVO stellte sich die Frage, inwieweit die Regelungen des TKG a.F. zum Datenschutz noch anwendbar waren. Art. 95 DS-GVO sah in diesem Fall einen Anwendungsvorrang der in der RL 2002/58/EG (**ePrivacy-Richtlinie**) normierten Pflichten vor, die u.a. durch Vorschriften im TKG a.F. und TMG umgesetzt wurden.[502] Dies hatte zur Folge, dass TKG-Vorschriften als lex speciales der DS-GVO dort vorgezogen wurden, wo diese die ePrivacy-Richtlinie umsetzten.[503] Ging das TKG a.F. über die Regelungen der RL hinaus, griff der Anwendungsbereich der DS-GVO.[504] Somit wurden Anbietern von öffentlich zugängigen Kommunikationsdiensten, die ihre Dienste über öffentliche Kommunikationsnetze

[500] BfDI, *Datenschutz und Telekommunikation - Info 05, S. 16.*
[501] BfDI, *Datenschutz und Telekommunikation - Info 05, S. 21.*
[502] BfDI, *Datenschutz und Telekommunikation - Info 05, S. 18.*
[503] Schramm/Shvets, *MMR 2019, 228 (229).*
[504] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kap. 3 Rn 5.*

bereitstellten und dem Anwendungsbereich der ePrivacy-Richtlinie unterlagen, keine zusätzliche Pflichten durch die DS-GVO auferlegt. Welche Vorschrift Anwendungsvorrang genossen, war daher jeweils im konkreten Einzelfall zu prüfen.[505]

Allerdings ist geplant, die ePrivacy-Richtlinie durch eine **E-Privacy-Verordnung** (ePV) zu ersetzen, um eine europaweite Harmonisierung des Datenschutzrechtes weiter voranzutreiben und sogleich geltendes Recht an die Anforderungen der fortwährenden Digitalisierung anzugleichen.[506] Laut Art. 1 III ePV-Vorschlag sollen die Bestimmungen der ePV die der DS-GVO in Bezug auf „*die Bereitstellung und Nutzung elektronischer Kommunikationsdienste sowie den freien Verkehr elektronischer Kommunikationsdaten und elektronischer Kommunikationsdienste in der EU*" präzisieren und ergänzen.[507] Sie bildet somit die sekundärrechtliche Grundlage zur Umsetzung des grundrechtlichen Schutzes der Vertraulichkeit dienstgestützter Kommunikation.[508] Die ePV wird in der europäischen Normenhierarchie ebenbürtig zur DS-GVO stehen und ist grundsätzlich als Ergänzung ebendieser vorgesehen. Da beide Verordnungen auf den Schutz personenbezogener Daten abzielen, muss die Abgrenzung der Zuständigkeit über den jeweiligen materiellen Anwendungsbereich erfolgen.[509] Da bei Diensten von Informationsgesellschaften mit dem Fokus auf elektronisch erbrachte kommerzielle Dienstleistungsangebote die Art sowie der Umstand der Übertragung sekundär sind, wird weiterhin die DS-GVO angewendet werden müssen. (Tele-)Kommunikationsdienste hingegen haben ihren Schwerpunkt im Transport bzw. der Vermittlung von Signalen. Bei der Verarbeitung der hierbei anfallenden Nutzerdaten wird über Art. 95 DS-GVO in unbestimmter Zukunft die ePV Anwendungsvorrang genießen.[510] Ein weiteres Abgrenzungskriterium wird der in Art. 95 DS-GVO geforderte Öffentlichkeitsaspekt des Übertragungssystems und der darüber genutzten Dienste sein.[511]

Die Verhandlungen über den Entwurf der ePV dauern derzeit noch an[512] und aufgrund zu erwartender Entwurfsablehnungen und einer geplanten 24-monatigen Übergangszeit, ist mit dem Inkrafttreten der ePV in den kommenden Jahren nicht zu rechnen.[513] Aktueller Stand zum Zeitpunkt der Bearbeitung ist die Einigung des Rates auf einen Entwurf der ePV am 10. Februar 2021. Es stehen nur die Trilog-Verhandlungen mit dem Parlament und der Kommission an.[514]

Bevor abschließend über das Verhältnis des TKG a.F. zur DS-GVO gesprochen wird, gilt es zunächst zu prüfen, ob privatrechtlich organisierte Krankenhäuser überhaupt in den

[505] Böhm/Halim, *MMR 2020, 651 (653).*
[506] BfDI, *Datenschutz und Telekommunikation - Info 05, S. 18.*
[507] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 95 Rn 4.*
[508] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 101.*
[509] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 82.*
[510] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 94.*
[511] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 100.*
[512] *Stand Februar 2021.*
[513] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 95 Rn 11.*
[514] Schumacher u. a., *MMR, 603 (605).*

Anwendungsbereich des TKG a.F. gefallen sind. Hierfür müssen Krankenhäuser zu den TK-Diensteanbieter i.S.d. TKG a.F. gezählt haben und öffentlich zugänglich i.S.d. Art. 95 DS-GVO sein.

2. Krankenhäuser als öffentlich zugängliche TK-Diensteanbieter nach dem TKG a.F.

Ob privatrechtliche Krankenhäuser neben der DS-GVO auch das Fernmeldegeheimnis aus § 88 TKG a.F. beachten mussten und die entsprechenden Normen des TKG a.F. auch neben der DS-GVO anwendbar waren, hing davon ab, ob Krankenhäuser als TK-Diensteanbieter i.S.d. § 3 Nr.6 TKG a.F. einzustufen waren, die zudem öffentlichen zugänglich sind.

Gem. § 3 Nr. 6 TKG a.F. war **TK-Diensteanbieter**, wer *„ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt“.* Telekommunikationsdienste waren gem. § 3 Nr. 24 TKG a.F. *„in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen“.* Unter der geforderten Geschäftsmäßigkeit wurde hierbei gem. § 3 Nr. 10 TKG a.F. *„das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“* verstanden. Da Telekommunikationsdienste somit auch ohne Gewinnerzielungsabsicht unter den Begriff des TK-Dienstanbieters fallen konnten und zudem nur eine teilweise Erbringung dieser Dienste verlangt wurde, konnten auch Unternehmen, die zugleich Infrastruktur- oder Inhaltsdienstleister sind, TK-Diensteanbieter i.S.d. § 3 Nr. 6 TKG a.F. sein. Somit konnten auch Krankenhäuser TK-Diensteanbieter sein, soweit Patienten und Patientinnen eine Möglichkeit zur Nutzung von TK-Diensten gewährt wird.[515]

Die Vorgaben der §§ 88 ff TKG a.F. galten zudem nur, wenn das in § 3 Nr. 10 TKG a.F. geforderte Mindestmaß an Außenwirkung gegeben war.[516] Dies war der Fall, wenn das TK-Angebot für Dritte zugänglich war. Fraglich ist, ob dieses Mindestmaß durch eine geschäftsmäßige Privatnutzung von Telekommunikationsnetzen gegeben war. Dient eine TK-Anlage ausschließlich der unternehmensinternen Kommunikation, einschließlich dienstlicher Telefongespräche ins öffentliche Fernmeldenetz, und sind keine privaten Gespräche zulässig, war dieses Mindestmaß an Außenwirkung nicht gegeben.[517] Wurden allerdings auch Außenstehenden (beispielsweise Gästen und Gästinnen) TK-Dienstleistungen über die TK-Anlage angeboten, so war das nach § 3 Nr. 10 TKG a.F. geforderte Mindestmaß erfüllt.[518] Strittig war indes, ob Mitarbeitende eines Unternehmens, die die TK-Anlage privat nutzen dürfen, auch unter den Begriff des „Dritten“ fielen. Die vormalig herrschende Meinung in der Literatur bejahte dies

[515] Spindler/Schuster, *Recht der elektronischen Medien TKG § 3 Rn 10.*
[516] Hoeren u. a., *Multimedia-Recht Teil 22.1 Rn 76.*
[517] BfDI, *Datenschutz und Telekommunikation - Info 05, S. 87.*
[518] BfDI, *Datenschutz und Telekommunikation - Info 05, S. 88.*

unter Bezugnahme auf die Gesetzgebungsgeschichte und den Wortlaut der §§ 3 Nr. 6, 10 und 24, 88 I, 91 II TKG a.F..[519] In der Rechtsprechung hingegen manifestierte sich eine ablehnende Haltung gegenüber der Anwendbarkeit des TKG a.F. bei erlaubter Privatnutzung.[520] Diese gründete sich u.a. auf den Ergebnissen der teleologischen Auslegung des TKG a.F.. Dieses sei als *„Gesetz zur Förderung des privaten Wettbewerbs im Bereich der Telekommunikation"* (§ 1 I TKG a.F.) zur Regelung der Rechtsbeziehung zwischen Staat und TK-Anbieter sowie TK-Anbieter und TK-Anbieter untereinander vorgesehen gewesen und nicht zur Regelung von unternehmensinternen Rechtsbeziehungen.[521] Von einem Streitentscheid kann vorliegend abgesehen werden. Da Gästen und Gästinnen bzw. Patienten und Patientinnen in Krankenhäusern Zugang zu den TK-Diensten gewährt wird (Nutzung der Telefonanlage und des WLANs), konnte das geforderte Mindestmaß an Außenwirkung gem. § 3 Nr. 10 TKG a.F. unabhängig von der Privatnutzung der TK-Dienste durch die Mitarbeitenden des Krankenhauses bejaht werden.

Übrig blieb hinsichtlich des Anwendungsvorrangs gegenüber der DS-GVO letztlich die Frage, ob die TK-Dienste des Krankenhauses auch **öffentlich zugänglich** i.S.d. Art. 95 DS-GVO sind. Laut § 3 Nr. 17a TKG a.F. waren öffentlich zugängliche Telekommunikationsdienste *„der Öffentlichkeit zur Verfügung stehende Telekommunikationsdienste"*. Der Terminus „öffentlich zugängliche Telekommunikationsdienste" hat im Rahmen der TKG-Novelle 2012 den damaligen Terminus „Telekommunikationsdienste für die Öffentlichkeit" ersetzt, wobei hierdurch ausdrücklich keine inhaltlichen Änderungen des Begriffes erfolgte, sondern lediglich eine Angleichung des Sprachgebrauchs im TKG a.F. angestrebt wurde.[522] Jedoch ist das Merkmal der Öffentlichkeit in diesem Kontext weder auf nationaler[523] noch auf europäischer Ebene[524] definiert wurden. Auf europäische Ebene konnte durch die Orientierung der ePrivacy-Richtlinie und der späteren E-Privacy-Verordnung an Art. 7 GRCh der Grundsatz der Gewährleistung der Vertraulichkeit der Kommunikation zur Auslegung des Begriffs herangezogen werden. Demnach können Betreibende von unternehmenseigenen Kommunikationsnetzwerken, welche die Kommunikation lediglich den Beschäftigten zu geschäftlichen Zwecken gestatten, nicht als öffentlich zugängliche Telekommunikationsdienste gelten.[525] Werden Kommunikationsnetze hingegen einer zuvor nicht festgelegten Anzahl Dritter zugänglich gemacht, sind diese öffentlich i.S.d. ePrivacy-Richtlinie.[526]

Auf nationaler Ebene galt der Begriff der öffentlichen Zugänglichkeit im TKG a.F. stets als umstritten.[527] Ähnlich zum unionsrechtlichen Verständnis des Begriffs konnte das Merkmal der

---

[519] Thüsing, *Beschäftigtendatenschutz und Compliance§ 3 Rn 74.*
[520] *Siehe: OLG Karlsruhe MMR 2005, 178; VGH Kassel NJW 2009, 2470; LAG Berlin-Brandenburg NZA-RR 2011, 342; LAG Niedersachsen MMR 2010, 639.*
[521] Fülbier/Splittgerbe, *NJW 2012, 1995 (2000).*
[522] Geppert/Schütz, *Beck'scher TKG-Kommentar TKG § 110 Rn. 10.*
[523] Geppert/Schütz, *Beck'scher TKG-Kommentar TKG § 110 Rn. 17.*
[524] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 101.*
[525] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 102.*
[526] Jandt/Steidle, *Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 104.*
[527] Spindler/Schuster, *Recht der elektronischen Medien TKG § 91 Rn 18.*

Öffentlichkeit bei ausschließlich privaten Netzwerken mit ausschließlich interner Kommunikation verneint werden. Für die Auslegung nach nationaler Auffassung war entscheidend, dass vom Gesetzgeber keine marktregulatorische Funktion verfolgt wurde, sondern eine Begrenzung des Adressaten- und Adressatinnenkreises zur Wahrung des Verhältnismäßigkeitsgrundsatzes in Hinblick auf mögliche Kosten vorgenommen wurde.[528]

Wenn Krankenhäusern Patienten und Patientinnen sowie Besuchenden die Möglichkeit gaben, die krankenhauseigenen TK-Dienste nutzen zu können, konnte die öffentliche Zugänglichkeit nach unionsrechtlichen sowie nationalen Maßstäben bejaht werden.

Krankenhäuser konnten somit als öffentlich zugängliche TK-Diensteanbieter i.S.d. TKG a.F. gesehen werden und folglich waren die datenschutzrechtlichen Sondernormen des TKG a.F. anwendbar.

3. Rechtmäßigkeit des Einsatzes von Angriffserkennungssystemen nach dem TKG a.F.

Da Krankenhäuser grundsätzlich unter den Begriff des TK-Diensteanbieters i.S.d. § 3 Nr. 6 TKG a.F. fielen, ist in einem weiteren Schritt zu erörtern, ob durch die Nutzung von Angriffserkennungssystemen in Krankenhaus-Netzwerken ein Eingriff in den bereits erläuterten Schutzbereichs des Fernmeldegeheimnisses nach § 88 TKG a.F. vorlag. Ist dies der Fall, so ist die Anwendbarkeit des datenschutzrechtlichen Abschnittes des TKG a.F. (§§ 91 ff TKG a.F.) zu prüfen und in Frage kommende rechtfertigende Rechtsgrundlagen sind zu betrachten.

Das Fernmeldegeheimnis in § 88 TKG a.F. verfolgte dasselbe Ziel, wie das in Art. 10 GG verankerte Fernmeldegeheimnis und bildete eine einfachgesetzliche Ausprägung von eben diesem. Anders als bei Art. 10 GG waren durch § 88 TKG a.F. jedoch nicht nur Staatsorgane, sondern auch Privatrechtssubjekte direkt verpflichtet.[529]

Vom sachlichen Schutzbereich des § 88 I TKG a.F. umfasst waren der Inhalt sowie die näheren Umstände von Telekommunikation. Laut § 3 Nr. 22 TKG a.F. fiel unter den Begriff Telekommunikation *„der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen“*. Unter näheren Umständen waren sämtliche Verkehrsdaten sowie sonstige Umstände, die einen Telekommunikationsvorgang individualisierbar machen inklusive erfolgloser Verbindungsversuche zu verstehen.[530] Bestandsdaten waren laut BVerfG hingegen nicht vom Schutzbereich des Fernmeldegeheimnisses umfasst.[531] Ein Telekommunikationsvorgang war individuell, wenn sich dessen Inhalte nicht an die Öffentlichkeit richteten (wie beispielsweise beim Rundfunk).[532] Zweck des Fernmeldegeheimnis war es,

[528] Geppert/Schütz, *Beck'scher TKG-Kommentar TKG § 110 Rn. 21.*
[529] Geppert/Schütz, *Beck'scher TKG-Kommentar TKG § 88 Rn. 1.*
[530] Spindler/Schuster, *Recht der elektronischen Medien TKG § 88 Rn. 11.*
[531] Spindler/Schuster, *Recht der elektronischen Medien TKG § 88 Rn. 12.*
[532] Geppert/Schütz, *Beck'scher TKG-Kommentar§ 88 Rn. 12, 13.*

unbemerkte Kenntnisnahme von Kommunikationsinhalten durch technikspezifische Risiken auszugleichen.[533] Zudem waren automatisierte Telekommunikationswege zwischen Computern und anderen Geräten vom Schutzbereich des § 88 TKG a.F. eingeschlossen.[534]

§ 88 TKG a.F. enthielt keine Definition darüber, welche Personen in den persönlichen Schutzbereich des Fernmeldegeheimnisses fielen. Unstreitig fielen jedoch natürliche Personen als Beteiligte an einem Telekommunikationsvorgang in den persönlichen Schutzbereich.[535] Zudem waren juristische Personen durch § 88 TKG a.F. geschützt, soweit sie an der Telekommunikation beteiligt waren.[536]

Verpflichtet zur Wahrung des Fernmeldegeheimnisses waren nach § 88 II TKG a.F. jeder Diensteanbieter. Diensteanbieter war nach § 3 Nr. 6 TKG a.F. jeder, *„der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt“.*

Bei der Erbringung und bei der Nutzung von TK-Diensten werden zahlreiche Daten (Vertragsbeginn, Produktbuchungen, etc.) und insbesondere Verkehrsdaten erzeugt. Diese fielen in der Regel in den Schutzbereich des Fernmeldegeheimnisses.[537] Da all diese Datenpakete aus den Kommunikationsvorgängen an einem Netzwerkknotenpunkt durch Angriffserkennungssysteme erhoben werden müssen und diese Erhebung bereits einen Eingriff in das Fernmeldegeheimnis darstellen konnte, bedurfte es somit einer rechtfertigenden Rechtsgrundlage.[538]

Diese hätte in den datenschutzrechtlichen Regelungen der §§ 91 ff. TKG a.F. zu finden sein können. § 91 TKG a.F. regelte den Anwendungsbereich des Datenschutzes. Vom Schutzbereich erfasst waren die *„personenbezogenen Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken“.* Im Unterschied zur DS-GVO war der Anwendungsbereich weiter gefasst, da § 91 II 2 TKG a.F. auch die Daten von Personen schützte, die grundsätzlich dem Fernmeldegeheimnis unterlagen.[539] Somit war neben den TK-Diensteanbietern jedes Unternehmen und jede natürliche Person, die an der Erbringung der Dienste, beispielsweise durch das Bereitstellen von Netzen, verpflichtet, personenbezogene Daten zu schützen sowie das Fernmeldegeheimnis zu wahren.[540]

---

[533] Spindler/Schuster, *Recht der elektronischen Medien TKG § 88 Rn. 13.*
[534] Geppert/Schütz, *Beck'scher TKG-Kommentar TKG § 88 Rn. 20.*
[535] Geppert/Schütz, *Beck'scher TKG-Kommentar TKG § 88 Rn. 19.*
[536] Spindler/Schuster, *Recht der elektronischen Medien TKG § 88 Rn. 24, 25.*
[537] Schramm/Shvets, *MMR 2019, 568 (568).*
[538] Krügel, *MMR 2017, 795 (797).*
[539] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kapitel 3 Rn 8.*
[540] BfDI, *Datenschutz und Telekommunikation - Info 05, S. 43.*

Im Folgenden werden mögliche Rechtfertigungsgrundlagen aus dem TKG a.F. vorgestellt und auf ihre Anwendbarkeit geprüft.

a) Maßnahme nach § 100 i.V.m. § 109 TKG a.F.

Zur Gewährleistung eines störungs- und problemfreien Betriebes von TK-Anlagen ist die permanente Analyse der Datenströme notwendig.[541] Eine Erlaubnisnorm hierfür konnte in § 100 I TKG a.F. gefunden werden: Gem. § 100 I 1 TKG a.F. durften Diensteanbieter, soweit erforderlich, *„die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen“.* In § 100 I 1 TKG a.F. explizit nicht erwähnt waren indes die Inhaltsdaten. Auch der, durch das Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 dem Satz hinzugefügte und nicht näher definierte, Begriff der Steuerdaten umfasste nicht die Inhaltsdaten.[542]

Zudem erlaubte § 100 III TKG a.F. zum Aufdecken oder Unterbinden von rechtswidriger Inanspruchnahme von TK-Netzen die Verwendung der *„Bestandsdaten und Verkehrsdaten, die erforderlich sind, um die rechtswidrige Inanspruchnahme des Telekommunikationsnetzes oder -dienstes aufzudecken und zu unterbinden“.* Allerdings war die Datennutzung ausschließlich an den eben genannten Zweck gebunden.[543] Netzbetreibende hatten somit die grundsätzliche Möglichkeit, eine Missbrauchsbekämpfung durchzuführen, durften allerdings erst bei einem dokumentierten konkreten Tatverdacht handeln, der auf Tatsachen gestützt wurde.[544]

Eng verknüpft mit den datenschutzrechtlichen Regelungen des TKG a.F. waren die Regelungen zur öffentlichen Sicherheit, die in den §§ 109-115 TKG a.F. aufgeführt waren. Diese führten Schutzmaßnahmen sowie Überwachungsmaßnahmen und Auskunftspflichten gegenüber berechtigten Stellen auf.[545] Insbesondere § 109 I TKG a.F. verpflichtete Diensteanbieter, unter Berücksichtigung des Standes der Technik, technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten zu treffen. Hierunter zählte insbesondere der Schutz der TK-Anlagen gegen Störungen, Beeinträchtigungen und äußere Angriffe.[546]

---

[541] BfDI, *Datenschutz und Telekommunikation - Info 05, S. 36.*
[542] Krügel, *MMR 2017, 795 (795).*
[543] BfDI, *Datenschutz und Telekommunikation - Info 05, S. 36.*
[544] Scheurle/Mayen, *Telekommunikationsgesetz - Kommentar TKG § 100 Rn 38;* Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kapitel 3 Rn 59.*
[545] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kapitel 3 Rn 71.*
[546] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kapitel 3 Rn 72.*

Fiel ein privatrechtlich organisiertes Krankenhaus unter den Begriff des TK-Anbieters I.S.d. § 3 Nr. 6 TKG a.F. und nutzt dieses Angriffserkennungssysteme, werden in unterschiedlicher Intensität die gesamten Datenströme des Netzwerkes und somit auch Inhaltsdaten erfasst. Da diese nicht unter § 100 I TKG a.F. fielen, war die Verwendung von Inhaltsdaten zur Angriffserkennung nicht über § 100 I TKG a.F. gerechtfertigt.[547] Da nicht ausgeschlossen werden kann, dass im Rahmen einer Datenanalyse des IDS auch Inhaltsdaten verwendet werden, konnte die Nutzung von Angriffserkennungssystemen in Netzwerken von privatrechtlich organisierten Krankenhäusern nicht vollumfassend über § 100 i.V.m. § 109 TKG a.F. gerechtfertigt werden. Zudem ist fraglich, ob die Erkennung eines Angriffs überhaupt unter die in § 100 I 1 TKG a.F. festgelegte Zweckbindung gefallen ist. § 100 I 1 TKG a.F. erlaubte die Datenverarbeitung, um Störungen oder Fehler an TK-Anlagen zu erkennen, einzugrenzen oder zu beseitigen. Die Erkennung eines Angriffes muss jedoch nicht zwangsläufig zu Störungen und Fehlern der TK-Anlagen führen, was die Zweckbindung des § 100 I 1 TKG a.F. in Bezug auf den Einsatz von Angriffserkennungssystemen zu vage erscheinen lässt.

b) Maßnahme nach § 88 III 1 TKG a.F.

Als weitere Erlaubnisnorm hätte der § 88 III 1 TKG a.F. herangezogen werden können. Dieser besagte, dass es den Verpflichteten untersagt war, *„sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen“.* Dies bedeutete im Umkehrschluss, dass sich TK-Diensteanbieter Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen durften, wenn nur so der Schutz der technischen Systeme und Netzwerke gewährleistet werden konnte.[548] Für weitere Zwecke war gem. § 88 III 3 TKG a.F. die Verwendung dieser Kenntnisse nur zulässig, soweit das TKG a.F. oder eine andere gesetzliche Vorschrift dies vorsah und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezog. Da § 88 III 1 TKG a.F. nicht näher definierte, wann die Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation erforderlich war, musste die Norm als mögliche Rechtfertigungsgrundlage im jeweiligen Einzelfall subsumiert werden. Da die benötigte Erforderlichkeit bereits für den Einsatz von Viren- und Spamfiltern umstritten war[549], war die Rechtfertigung der Nutzung von Angriffserkennungssystemen über den Umkehrschluss des § 88 III 1 TKG a.F. stark zu bezweifeln, da diese den gesamten Datenstrom analysieren. Da § 88 III 1 TKG a.F. als Rechtfertigungsgrundlage zu einzelfallbezogen und somit mit Rechtsunsicherheit behaftet war, konnte die Nutzung von Angriffserkennungssystemen in Netzwerken von privatrechtlich organisierten Krankenhäusern hierüber nicht gerechtfertigt werden.

[547] Krügel, *MMR 2017, 795 (795).*
[548] Krügel, *MMR 2017, 795 (795).*
[549] Krügel, *MMR 2017, 795 (795).*

Zwar sah § 88 III 4 TKG a.F. die Möglichkeit der Befreiung des Diensteanbieters von der Pflicht zur Wahrung des Fernmeldegeheimnisses vor, allerdings nur, wenn dieser von der Planung oder Ausführung einer Straftat nach § 138 StGB erfuhr. Da Angriffe auf Netzwerke nicht in der Regel, sondern nur in Ausnahmefällen die geforderten Straftatbestände des § 138 StGB erfüllen, konnte § 88 III 4 TKG a.F. nicht als Ermächtigungsgrundlage zur Befreiung der Wahrungspflicht des Fernmeldegeheimnisses und somit zur Rechtfertigung der Nutzung von Angriffserkennungssystemen dienen.[550]

4. Zwischenergebnis

Es ist festzustellen, dass eine Rechtfertigung der Nutzung von Angriffserkennungssystem in Krankenhäusern in privater Trägerschaft nach dem TKG a.F. mit großen Rechtsunsicherheiten behaftet war.

Zum einen war und ist das Verhältnis der datenschutzrechtlichen Normen zur DS-GVO ungeklärt, da eine Verabschiedung der, das Verhältnis abschließend regelnde, ePV in den kommenden Jahren nicht zu erwarten ist.

Zum anderen kann zwar die grundsätzliche Aussage getroffen werden, dass privatrechtlich organisierte Krankenhäuser als öffentlich zugängliche TK-Diensteanbieter i.S.d. TKG a.F. zu qualifizieren sind. Aber gerade die nach Art. 95 DS-GVO geforderte öffentliche Zugänglichkeit kann in Einzelfällen nicht gegeben sein.

Dass Krankenhäuser, die TK-Diensteanbieter i.S.d. TKG a.F. waren und mit Mechanismus zur Angriffserkennung arbeiten, hierdurch in den Schutzbereich des Fernmeldegeheimnisses nach § 88 TKG a.F. eingriffen, ist hingegen unumstritten. Als mögliche Rechtfertigungsgrundlagen kamen § 100 i.V.m. § 109 TKG a.F. sowie § 88 III 1 TKG a.F. in Betracht, die jedoch keine vollumfassende Rechtfertigung garantierten bzw. in ihrer Reichweite beschränkt waren und somit ebenfalls mit Rechtsunsicherheiten behaftet waren.

B. Die Rechtmäßigkeit nach dem TKG neu

Mit der Gesetzesänderung des TKG zum 01. Dezember 2021 veränderte sich der Datenschutz in der Telekommunikation grundlegend. Im Folgenden werden anhand von gezielten Gegenüberstellungen der alten und der neuen Fassung des TKG die einschlägigen Regelungen verglichen und es wird geprüft, ob es eine Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen im TKG neu gibt und ob diese im konkreten Fall anwendbar ist.

[550] Schlegel*, MMR 2020, 3 (5).*

1. Krankenhäuser als TK-Diensteanbieter i.S.d. TKG neu

Die Legaldefinition des TK-Diensteanbieters findet sich im TKG neu in § 3 Nr. 1 und ist allgemeiner als die Definition des TKG a.F.. So ist „*Anbieter von Telekommunikationsdiensten jeder, der Telekommunikationsdienste erbringt*“. Die nach § 3 Nr. 10 TKG a.F. verlangte Geschäftsmäßigkeit bei der Erbringung von TK-Diensten fällt in § 3 TKG neu weg. Auch nach dieser Definition wird ein Krankenhaus in privater Trägerschaft, welches seinen Patienten und Patientinnen und deren Besuchenden Zugang zu den TK-Diensten des Hauses gewährt, als Anbieter von TK-Diensten i.S.d. TKG neu eingestuft.

Eine detailliertere Ausgestaltung hat hingegen die Legaldefinition des Telekommunikationsdienste-Begriffs erhalten. Während in § 3 Nr. 24 TKG a.F. Telekommunikationsdienste als „*in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen*“ definiert wurden, konkretisiert das TKG neu in § 3 Nr. 61 Telekommunikationsdienste als „*in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die folgende Dienste umfassen: Internetzugangsdienste, interpersonelle Telekommunikationsdienste und Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine- Maschine-Kommunikation und für den Rundfunk genutzt werden*“. Eine Ausnahme gilt für „*Dienste, die Inhalte über Telekommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben*“. Die umfassendere Ausgestaltung wird wohl dem Fortschritt der Telekommunikationstechnik geschuldet sein und hat auf die Prüfung keine Auswirkung.

2. Rechtmäßigkeit des Einsatzes von Angriffserkennungssystemen nach dem TKG neu

Das in § 2 II TKG a.F. normierte Ziel des TKG, das Fernmeldegeheimnis zu wahren, ist in den Zielsetzungen des TKG neu nicht mehr enthalten. Auch findet das in § 88 I TKG a.F. normierte Fernmeldegeheimnis und die damit einhergehende Verpflichtung eines jeden Diensteanbieters zur Wahrung des Fernmeldegeheimnisses in § 88 II TKG a.F. im TKG neu kein Pendant mehr.

Damit einhergehend ist auch der Abschnitt zum Datenschutz gestrichen worden. So gibt es kein Gegenstück im TKG neu zu § 91 I TKG a.F., der die Regelungen zum „*Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken*“, einleitet. Ebenfalls ersatzlos im TKG neu gestrichen ist § 100 TKG a.F., der in Absatz 1 den Diensteanbietern unter Vorbehalt der Erforderlichkeit erlaubte, „*die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer sowie die Steuerdaten eines*

informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, {zu} erheben und {zu} verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen".

§ 109 I TKG a.F., der Diensteanbieter verpflichtete, unter Berücksichtigung des Standes der Technik „*erforderliche technische Vorkehrungen und sonstige Maßnahmen zu treffen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten*" und i.V.m. § 100 I TKG a.F. in der vorherigen Prüfung eine mögliche Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen dargestellt hatte, findet im TKG neu in § 165 eine Entsprechung. § 165 I TKG neu stimmt mit § 109 I TKG a.F. nahezu wörtlich überein. Einzig Abweichung ist, dass die technische Vorkehrung oder sonstige Maßnahme nach § 165 I TKG neu nicht „*erforderlich*", sondern „*angemessen*" zu sein hat. Zudem verpflichtet § 165 I TKG neu nicht nur die Diensteanbieter, sondern jeden, der „*Telekommunikationsdienste erbringt oder daran mitwirkt*". Laut § 165 II TKG neu haben Betreibende von öffentlichen Telekommunikationsnetzen oder Erbringer von öffentlich zugänglichen Telekommunikationsdiensten „*bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische und organisatorische Vorkehrungen und sonstige Maßnahmen zu treffen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch, sofern diese Störungen durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten*". Eine angemessene Maßnahme i.S.d. Absatz 2 sind laut § 165 III TKG neu „*Systeme zur Angriffserkennung im Sinne des § 2 Absatz 9b des BSI-Gesetzes*". Als Anforderungen an die Angriffserkennungssysteme führt § 165 III TKG neu zudem an, dass „*die eingesetzten Systeme zur Angriffserkennung in der Lage sein {müssen}, durch kontinuierliche und automatische Erfassung und Auswertung Gefahren oder Bedrohungen zu erkennen. Sie sollen zudem in der Lage sein, erkannte Gefahren oder Bedrohungen abzuwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen.*"

Prüft man die neue Gesetzeslage nur auf eine Ermächtigungsgrundlage hinsichtlich des Einsatzes von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft, kommt nur **§ 165 TKG** neu in Betracht, der im TKG neu in Teil 10 Öffentliche Sicherheit und Notfallvorsorge im Abschnitt 1 mit der Unterüberschrift Öffentliche Sicherheit verortet ist. § 165 TKG neu stellt technische Anforderungen an TK-Diensteanbieter, um die Sicherheit der Daten und somit den Schutz des Fernmeldegeheimnisses und der personenbezogenen Daten zu gewährleisten. Zwar verpflichtet § 165 TKG neu die TK-Dienstanbieter zur Umsetzung angemessener technischer Vorkehrung, allerdings erlaubt er hierdurch nicht die damit eventuell einhergehende Verarbeitung personenbezogener Daten. In der bisherigen Fassung des TKG kann § 109 I TKG a.F. nur i.V.m. § 100 I TKG a.F. einen Rechtfertigungsgrund darstellen, da § 100 I TKG

a.F. eine Verarbeitung bestimmter Daten gestattet. Da § 100 I TKG a.F. im neuen TKG keinen Gegenpart findet, kann § 165 TKG neu weder alleine noch i.V.m. einer weiteren Norm des TKG neu eine Ermächtigungsgrundlage darstellen. Da weder das Fernmeldegeheimnis noch die Verarbeitung bestimmter Datengruppen (§ 88 und 91 TKG a.F.) Einzug in das TKG neu gefunden haben, lässt darauf schließen, dass diese Lücke vom Gesetzgeber beabsichtigt ist.

Eine Rolle bei der Rechtfertigung des Einsatzes von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft könnte § 165 TKG neu allenfalls in Verbindung mit den Erlaubnistatbeständen des Art. 6 I DS-GVO sowie den Ausnahmetatbeständen des Art. 9 II DS-GVO spielen. Ob hierrüber eine Rechtfertigung möglich ist, wird in den entsprechenden Kapiteln dieser Untersuchung behandelt.

3. Zwischenergebnis

Eine Rechtfertigung des Einsatzes von Angriffserkennungssystemen in Krankenhäuser privater Trägerschaften kann – auch wenn Krankenhäuser TK-Diensteanbieter i.S.d. § 3 Nr. 1 TKG neu sind – über das TKG neu nicht erfolgen, da keine Norm als Ermächtigungsgrundlage in Betracht kommt.

V. Die Rechtmäßigkeit des Einsatzes von Angriffserkennungssystemen nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)

Wie soeben festgestellt, findet sich im TKG neu keine Ermächtigungsgrundlage mehr, die für eine Rechtfertigung des Einsatzes von Angriffserkennungssystemen in privatrechtlich organisierten Krankenhäusern in Betracht kommt. Dies liegt daran, dass der Gesetzgeber im Rahmen der Neuausrichtung von TKG und TMG einen gemeinsamen Regelungsort für die Verarbeitungsvoraussetzungen bestimmter Daten schaffen wollte.[551] Hierfür wurde das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) geschaffen, das am 20. Mai 2021 vom Deutschen Bundestag verabschiedet wurde und zum 01. Dezember 2021 in Kraft tritt.[552] Neben der DS-GVO und dem BDSG besteht nun mit dem TTDSG ein weiteres Gesetz mit Vorschriften zum Datenschutz und der Wahrung der Privatsphäre. Im Verhältnis untereinander geht nach wie vor die DS-GVO als Verordnung i.S.d. Art. 288 II AEUV vor, soweit keine Öffnungsklausel vorliegt, die eine nationale Regelung neben der DS-GVO gewährt.[553]

Gem. § 1 Nr. 2 TTDSG regelt dieses Gesetz „*besondere Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und Telemedien*“. Zunächst muss auch hier geprüft werden, ob Krankenhäuser in privaten Trägerschaften in den

[551] GDD, *GDD-Praxishilfe Das neue Telekommunikation-Telemedien- Datenschutz-Gesetz (TTDSG) im Überblick, S. 3.*
[552] Schumacher u. a., *MMR, 603 (603).*
[553] Golland, *NJW 2021, 2238 Rn 2.*

Anwendungsbereich des TTDSG fallen. Anschließend werden die Regelungen zum Datenschutz im TTDSG auf eine Rechtfertigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern geprüft.

1. Krankenhäuser als TK-Diensteanbieter nach § 2 I TTDSG

Das TTDSG verweist in § 2 I auf die Begriffsbestimmungen des TKG neu und des TMG neu, soweit in § 2 II TTDSG keine abweichenden Begriffsbestimmungen getroffen wurden. Da dies für den Begriff des TK-Diensteanbieters nicht zutrifft, gilt für das TTDSG die Definition nach § 3 Nr. 1 TKG neu.

Somit fallen, wie bereits behandelt, Krankenhäuser in privaten Trägerschaften unter den Begriff des TK-Dienstanbieters nach § 2 I TTDSG i.V.m. § 3 Nr. 1 TKG neu.

2. Rechtmäßigkeit des Einsatzes von Angriffserkennungssystemen nach dem TTDSG

Teil 2 des TTDSG enthält Regelungen zum Datenschutz und Schutz der Privatsphäre in der Telekommunikation. Von Teil 2 umfasst sind die §§ 3 – 18 TTDSG. Sie stellen eine Überführung der bisherigen Regelungen der §§ 88 ff. TKG a.F. dar, die an die DS-GVO angepasst wurden.[554]

Gemäß § 3 I TTDSG unterliegt „*der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war*“ dem Fernmeldegeheimnis. Es erstreckt sich zudem auch „*auf die näheren Umstände erfolgloser Verbindungsversuche*“. Laut § 3 II TTDSG sind zur Wahrung des Fernmeldegeheimnisses „*Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken, Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken, Betreiber öffentlicher Telekommunikationsnetze und Betreiber von Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden*“, verpflichtet. Wie schon in § 88 TKG a.F. stellt § 3 TTDSG eine einfachgesetzliche Ausprägung des in Art. 10 GG verankerten Fernmeldegeheimnisses dar und verpflichtet nicht nur Staatsorgane, sondern auch Privatrechtssubjekte.

Als mögliche Rechtsgrundlage für die Rechtfertigung des Einsatzes von Angriffserkennungssystemen in Krankenhäusern kommt **§ 12 I TTDSG** in Betracht.

---

[554] GDD, *GDD-Praxishilfe Das neue Telekommunikation-Telemedien- Datenschutz-Gesetz (TTDSG) im Überblick, S. 4.*

Vergleicht man § 12 TTDSG mit seinem Vorgänger § 100 TKG a.F., so fällt auf, dass die Betitelung der Paragraphen gleichgeblieben ist. Zudem ähneln sich § 12 I 1 TTDSG und § 100 I 1 TKG a.F. sehr. In beiden Sätzen ist die Verarbeitung von „*Verkehrsdaten der Endnutzer (§ 12 I 1 TTDSG) bzw. der Teilnehmer und Nutzer (§100 I 1 TKG a.F.) sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind*“ erlaubt, „*um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen*.“ Auffällig ist, dass § 12 I 1 TTDSG keine Bestandsdaten aufzählt, wohingegen in § 100 I 1 TKG a.F. auch Bestandsdaten verarbeitet werden dürfen. Nach beiden Paragraphen gilt die Verarbeitungserlaubnis zudem wortgleich „*auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Telekommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können*“.

§ 100 I TKG a.F. kam als Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in privatrechtlich organisierten Krankenhäusern bereits nicht in Frage, da unter § 100 I TKG a.F. keine Inhaltsdaten erfasst sind, diese aber von Angriffserkennungssystemen analysiert werden. Bezogen auf § 12 I TTDSG zeigt sich dasselbe Problem, da auch hier keine Inhaltsdaten aufgeführt werden. So hat auch der Branchenverband der deutschen Informations- und Telekommunikationsbranche e.V. (bitkom) in seiner Stellungnahme vom April 2021 zum TTDSG-Entwurf § 12 TTDSG als Erlaubnisnorm zur Nutzung von Angriffserkennungssystemen abgelehnt, da es für eine effektive Abwehr erforderlich sei, dass diese „Verkehrs-, Steuer und Inhaltsdaten des Datenverkehrs nach Mustern und Indizien für Angriffe“ auswerten dürfen.[555]

3. Zwischenergebnis

Zwar fallen Krankenhäuser in den Regelungsbereich des TTDSG, jedoch enthält § 12 I TTDSG keine ausreichende Rechtfertigung der Nutzung von Angriffserkennungssystemen. Die Norm umfasst Inhaltsdaten nicht, deren Analyse für die Effektivität der Angriffserkennungssysteme unumgänglich ist.

Weder in den Regelungen des TKG neu noch im TTDSG findet sich somit eine Ermächtigungsgrundlage, die den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft rechtfertigt.

Im Folgenden wird geprüft, ob eine solche Rechtfertigung aus der DS-GVO uneingeschränkt erfolgen kann.

[555] Bitkom, *Stellungnahme TTDSG April 2021, S. 11.*

VI. Die Rechtmäßigkeit des Einsatzes von Angriffserkennungssystemen nach der Datenschutz-Grundverordnung (DS-GVO)

Die DS-GVO folgt dem Grundsatz des „Verbots mit Erlaubnisvorbehalts“, nachdem eine Datenverarbeitung bei bestehendem Personenbezug grundsätzlich einer Legitimation bedarf. Diese kann durch die Einwilligung der betroffenen Person in die Datenverarbeitung erlangt werden oder auf Grundlage einer Gesetzesnorm.[556] Zudem gibt es an mehr als 70 Stellen in der DS-GVO die Möglichkeit für die Mitgliedstaaten, innerhalb des Anwendungsbereiches der DS-GVO deren Vorgaben konkretisieren oder ergänzen zu können.[557] Diese sogenannten **Öffnungsklauseln** können umsetzungspflichtig sein oder den Mitgliedstaaten fakultative Gestaltungsspielräume anbieten.[558] Werden Öffnungsklauseln genutzt, stehen die daraus resultierenden nationalen Rechtsnormen nicht neben dem Unionsrecht, sondern bilden eine Konkretisierung des Unionsrechts.[559]

Neben der Normierung des materiellen Datenschutzrechtes regelt die DS-GVO ebenso die technische Durchsetzung.[560] Beide Komponenten werden in diesem Kapitel in Bezug auf die Nutzung von Angriffserkennungssystemen beleuchtet.

Im Folgenden wird zunächst geprüft, ob die DS-GVO überhaupt Anwendung findet. Dies ist der Fall, wenn es sich bei den Daten, die in Angriffserkennungssystemen i.S.d. DS-GVO verarbeitet werden, um personenbezogene Daten handelt. Anschließend werden die Erlaubnistatbestände der DS-GVO nach einer Ermächtigungsgrundlage für die Nutzung von Angriffserkennungssystemen im privatrechtlichen Krankenhauskontext untersucht. Hierbei wird insbesondere auf die Besonderheiten und gesonderten Ausnahmetatbestände bei Gesundheitsdaten eingegangen. Abschließend wird auf den technischen Datenschutz, die damit einhergehenden Maßnahmenkataloge der DS-GVO und die Rolle von Angriffserkennungssystemen hierbei eingegangen.

A. Der Personenbezug

Vom Schutz der DS-GVO sind lediglich personenbezogene Daten umfasst, die somit das zentrale Tatbestandsmerkmal des europäischen Datenschutzrechts bilden. Der Begriff verbindet die technische Seite des Datenschutzes mit den Grundrechtspositionen betroffener natürlicher Personen.[561] Somit kennt die DS-GVO nur zwei Zustände: die Verarbeitung eines Datums fällt entweder vollständig oder gar nicht in den Schutzbereich der DS-GVO. Dreh- und Angelpunkt

[556] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch, Teil I. Kapitel 2. Rn 18.*
[557] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht§ 4 Rn 10.*
[558] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht§ 4 Rn 12.*
[559] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 38.*
[560] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar Rn 1.*
[561] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 4 Nr. 1 Rn 1.*

ist hierbei der Personenbezug.[562] Wirtschaftliche oder sonstige Interessen am Schutz der Daten spielen hingegen keine Rolle bei deren Verarbeitung nach der DS-GVO.[563]

1. Grundlagen

Der **Begriff des Datums** nach der DS-GVO ist grundsätzlich weit zu verstehen und umfasst jede Art der Information über eine betroffene Person unabhängig von ihrer Verkörperung. Kann die Information verarbeitet werden i.S.d. Art. 4 Nr. 2 DS-GVO, fällt diese unter den Begriff des Datums im Verständnis der DS-GVO.[564] Somit unterscheidet sich der Begriff im Datenschutz von dem Begriff des Datums in der Informatik, die hierrunter ein sie repräsentierendes Zeichen oder Signal versteht.[565]

Personenbezogene Daten sind nach Art. 4 Nr.1 DS-GVO alle Informationen, „*die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen*“, wobei eine Person insbesondere dann identifizierbar ist, wenn sie „*direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann*“. Der Personenbezug muss hierbei nicht durch eine einzelne Information erfolgen. Dieser kann auch erst durch die Kombination mehrere Informationen entstehen, die im Einzelnen nicht notwendigerweise einen Personenbezug aufweisen müssen.[566]

Es war lange strittig, ob sich der Umfang des Personenbezug nach der **relativen oder objektiven Theorie** bestimmt. Kernfrage hierbei war, welches Zusatzwissen und welche Mittel sich der oder die Verarbeitende zurechnen lassen muss, wenn es um die Bestimmbarkeit des Personenbezugs geht. Aufsichtsbehörden sowie Teile der Literatur vertraten mit der objektiven Theorie die Ansicht, dass ein Personenbezug als gegeben anzusehen ist, wenn mithilfe aller weltweit verfügbaren Informationen ohne Bezugnahme auf die individuellen technischen Fähigkeiten und Mittel des oder der Verarbeitenden ein Personenbezug herstellbar ist. Dies hätte zur Folge, dass nur bei einer absolut ausschließbaren Verknüpfungsmöglichkeit zwischen dem Datum und der möglichen betroffenen Person ein Personenbezug abzulehnen wäre. Die mittlerweile herrschende relative Theorie hingegen richtet die Bestimmbarkeit des Personenbezugs danach aus, welche Mittel und welches Zusatzwissen dem oder der Verarbeitenden im konkreten Einzelfall tatsächlich zur Verfügung stehen. Hierzu zählen u.a. auch Arbeitsaufwand, Zeit

[562] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 4 Nr. 1 Rn 14.*
[563] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 4 Rn 7.*
[564] Gola, *Datenschutz-Grundverordnung Kommentar Art. 5 Rn 6;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG Art. 4 Nr. 1 Rn 25.*
[565] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 4 Rn 8.*
[566] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 4 Nr. 1 Rn 52.*

und Kosten. Hinzugezogen werden können zudem auch Mittel, die bei Dritten vorhanden sind. Ausreichend ist bereits die abstrakte Möglichkeit der Herstellung eines Personenbezugs.[567]

Der EuGH sowie die DS-GVO verfolgen die relative Theorie. So heißt es in Erwägungsgrund 26 der DS-GVO, dass bei der Ermittlung der Identifizierbarkeit alle Mittel berücksichtigt werden müssen, „*die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren*". Hierbei müssen insbesondere die Kosten, der Zeitaufwand und die verfügbare Technologie bedacht werden.

Einen besonderen Fall der personenbezogenen Daten stellt die in Art. 4 Nr. 5 DS-GVO erwähnte **Pseudonymisierung** dar. Art. 4 Nr. 5 DS-GVO definiert den Vorgang der Pseudonymisierung als „*Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden*". Nach der DS-GVO ist ein Personenbezug jedoch auch bei pseudonymisierten Daten gegeben. So steht in Erwägungsgrund 26 der DS-GVO, dass pseudonymisierte Daten, „*die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten,*" als personenbezogene Daten betrachtet werden sollen. Zwar kann laut Erwägungsgrund 28 die „*Anwendung der Pseudonymisierung auf personenbezogene Daten die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen*", die Verarbeitung der Daten richtet sich jedoch dennoch nach den Grundsätzen des Art. 5 DS-GVO. Risiken für die betroffene Person werden dadurch gesenkt, dass die unmittelbare Kenntnis der Identität der betroffenen Person bei der Verarbeitung der pseudonymisierten Daten nicht erforderlich ist, zudem wird eine Zuordnung der pseudonymisierten Daten zu der betroffenen Person bei Drittzugriff erschwert.[568] Von der Pseudonymisierung abzugrenzen ist die Verschlüsselung von Daten. Hierbei behält der Datenbestand sämtliche Attribute und Informationen, diese werden lediglich besser vor einem unbefugten Zugriff geschützt.[569]

Können die Daten durch Heranziehung zusätzlicher Informationen einer Person nicht zugeordnet werden, liegt eine **Anonymisierung** vor. Um zu prüfen, ob im konkreten Fall eine Pseudonymisierung oder eine Anonymisierung vorliegt, sind die Maßstäbe der relativen Theorie zum Personenbezug anzuwenden.[570] Erwägungsgrund 26 der DS-GVO definiert anonymisierte Daten als „*Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche*

---

[567] Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht§ 3 Rn 14;* Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG Art. 4 Nr. 1 Rn 58 ff.*

[568] Gola*, Datenschutz-Grundverordnung Kommentar Art. 4 Rn 39;* Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht§ 3 Rn 16.*

[569] Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 4 Rn 34.*

[570] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 4 Rn 40.*

Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann". Wurden Daten anonymisiert, scheidet die Anwendung der DS-GVO aus, wobei sich die Frage gestellt werden muss, ob es durch den wachsenden Einsatz von Algorithmen und KI-Verfahren in der Zukunft überhaupt noch die Möglichkeit einer vollständigen Anonymisierung gibt.[571]

Besteht ein Personenbezug oder ist ein Datum personenbeziehbar, fällt es unter den Schutzbereich der DS-GVO und es bedarf einer Ermächtigungsgrundlage, um dieses Datum **verarbeiten** zu dürfen. Unter den weit gefassten Begriff der Verarbeitung fällt nach Art. 4 Nr. 2 DS-GVO jeder „*mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe {…} wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung*". Zur Datenverarbeitung gehört folglich jeder Vorgang, der im Zusammenhang mit personenbezogenen Daten steht. Ob dieser Vorgang einen Einzelfall darstellt oder mit einer Reihe von Vorgängen verknüpft ist, wie viele Schritte zeitlich und räumlich verteilt hierfür stattfinden und ob diese in den internen oder externen Sphären des oder der Verarbeitenden stattfinden, ist rechtlich irrelevant. Ebenso spielen die Intensität und die Dauer der Verarbeitung keine Rolle, es existieren im europäischen Datenschutzrecht keine „belanglosen personenbezogenen Informationen".[572]

Gem. Art. 4 Nr. 18 sind **Unternehmen** i.S.d. DS-GVO „*natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen*". Die Zuordnung von Personengesellschaften zum Unternehmensverständnis des Unionsrechtsgebers erspart eine Auseinandersetzung über den rechtlichen Umfang von Personengesellschaften nach dem jeweiligen mitgliedstaatlichen Verständnis. Ebenso fallen auch juristische Personen des öffentlichen Rechts unter den Begriff, solange sie einer wirtschaftlichen Tätigkeit nachgehen.[573]

Intensiv diskutiert wurde die Frage, ob **IP-Adressen** zu den personenbezogenen Daten i.S.d. DS-GVO gehören. Damit ein Computersystem über das Internet erreichbar ist, muss es über eine öffentliche IP-Adresse verfügen. Internetzugangsanbieter weisen den Geräten ihrer Kunden und Kundinnen IP-Adressen zu. Diese IP-Adressen können dauerhaft (statisch) oder in regelmäßigen Abständen erneut (dynamisch) zugewiesen werden. Die IP-Adressen unter IPv4 sind also teilweise statisch zugewiesen, teilweise dynamisch.[574] Laut Erwägungsgrund 30 der

---

[571] Schneider, *Datenschutz nach der EU-Datenschutz-Grundverordnung, S. 67.*
[572] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG Art. 4 Nr. 2 Rn 11;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG Art. 4 Nr. 1 Rn 22.*
[573] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 4 Nr. 18 Rn 1.*
[574] Schantz/Wolff, *Das neue Datenschutzrecht C. Die unterschiedlichen Kodifikationen des Datenschutzrechts Rn. 285.*

DS-GVO können „*natürlichen Personen unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern {…} zugeordnet*“ werden. Dies kann gem. Erwägungsgrund 30 Spuren hinterlassen, die in Kombination mit weiteren Informationen zur Profilbildung und Identifikation von natürlichen Personen genutzt werden können. Hieraus lässt sich schließen, dass der Unionsgesetzgeber in Bezug auf die Personenbezogenheit von IP-Adressen dem Ansatz der relativen Theorie folgt.[575] Im Breyer-Urteil hat zudem der EuGH im Jahr 2016 Stellung zu der Frage genommen, ob dynamischen IP-Adressen aus Sicht eines oder einer Webseitenbetreibenden einen Personenbezug aufweisen. Der EuGH bejaht den Personenbezug bzw. die Möglichkeit der Personenbeziehbarkeit und verweist auf die rechtlichen Möglichkeiten, die dem oder der Webseitenbetreibenden zur Verfügung stehen, um beim Internetzugangsanbieter die Identität des oder der Betroffenen zu erfragen. Somit folgt der EuGH auch hier dem relativen Theorieansatz und konzentriert sich auf die Auslegung des Erwägungsgrundes 26 der DS-GVO, lässt aber Elemente der objektiven Theorie ebenfalls einfließen, indem er die abstrakte Möglichkeit der Ermittlung des Personenbezugs durch Strafverfolgungsbehörden ebenfalls als ausreichend zur Bejahung einer Personenbeziehbarkeit bewertet.[576]

2. Personenbezug im konkreten Fall

Wie bereits im technischen Teil dieser Arbeit erörtert, analysieren Angriffserkennungssysteme grundsätzlich sämtliche Datenströme innerhalb des zu sichernden Netzwerkes oder Systems in Echtzeit. Je umfangreicher der Zugriff der Angriffserkennungssysteme auf die Daten eines Netzwerkes ist, desto effizienter und wirksamer können diese arbeiten. So stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) fest, dass insbesondere bei der Überwachung von internen Netzen durch Angriffserkennungssysteme eine Vielzahl von personenbezogenen Daten verarbeitet werden. [577] Werden diese also in IT-Infrastrukturen eingesetzt, die personenbezogene Daten verarbeiten und werten IDS und SIEM-Systeme den gesamten Datenverkehr aus, verarbeiten diese somit umfangreich personenbezogene Daten in Form von unter anderem log files, Verkehrs-, Inhalts- und Bestanddaten, die wie bereits festgestellt in den Schutzbereich der Datenschutzgrundrechte nach dem Grundgesetz sowie der Europäische Grundrechtecharte fallen.[578] So weisen Telekommunikationsdaten nicht nur auf die Nutzer und Nutzerinnen der Telekommunikation, sondern auch auf Verhaltensweisen und Tagesabläufe

[575] Schantz/Wolff*, Das neue Datenschutzrecht C. Die unterschiedlichen Kodifikationen des Datenschutzrechts Rn. 289.*
[576] Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Kap. 4 Rn 33-37;* Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 4 Nr. 1 Rn 66;* Schantz/Wolff*, Das neue Datenschutzrecht C. Die unterschiedlichen Kodifikationen des Datenschutzrechts Rn 287.*
[577] BSI*, BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen (IDS) - Rechtliche Aspekte beim Einsatz von IDS.*
[578] Jandt/Steidle*, Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG B. III. Rn 314;* Niedersächsisches Ministerium für Inneres und Sport*, NDIG und OZG: Rechtsrahmen für die digitale Verwaltung in Niedersachsen.*

hin. Die in SIEM-Systemen aufgenommenen Daten können zudem IP-Adressen oder User-IDs enthalten.[579] Auch wenn in der Datenbank des SIEM-Systems einzelne Daten ohne Personenbezug geführt werden, können diese zusammen einen Personenbezug entstehen lassen.

IT-Systeme in Krankenhäusern nutzen vorrangig und unmittelbar der Versorgung und Behandlung von Patienten und Patientinnen. Auf Grundlage der in den Systemen gespeicherten und verarbeiteten Informationen wird der Krankenhausalltag koordiniert und Behandlungsentscheidungen getroffen. Ihre Nutzung ist unabdingbar für einen ordnungsgemäßen Krankenhausbetrieb.[580] Die Daten, die in den IT-Systemen verarbeitet werden, weisen somit in vielen Fällen einen direkten Personenbezug zu betroffenen Patienten und Patientinnen auf oder lassen Rückschlüsse auf diese zu. Auch wenn einzelne Informationen keinen Personenbezug aufweisen, kann durch Zusatzinformationen, die ebenfalls in den IT-Systemen eines Krankenhauses verarbeitet werden, ein Personenbezug hergestellt werden. Werden Online-Kennungen für Mitarbeitende oder Patienten und Patientinnen genutzt, so kann auch hier ein Personenbezug hergestellt werden (siehe Urteil zu IP-Adressen).

Werden auf den IT-Systemen eines Krankenhauses Angriffserkennungssysteme genutzt, untersuchen diese automatisiert Daten aus den zu schützenden Systemen. Dass hierbei personenbezogene Daten von Mitarbeitenden sowie Patienten und Patientinnen untersucht und somit i.S.d. DS-GVO verarbeitet werden, ist teilweise notwendig beziehungsweise unvermeidbar. Angesichts der letzten Schadprogramm-Angriffe auf Krankenhäuser[581] ist eine wirksame Überwachung eines Krankenhaus-Netzes mit IDS und SIEM-Systemen ohne die Verarbeitung von personenbezogenen Daten wohl nicht realisierbar.

Um eine flächendeckende Absicherung der Nutzung von Angriffserkennungssystemen erhalten zu können, bedarf es also einer Ermächtigungsgrundlage aus der DS-GVO. Um den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft rechtfertigen zu können, gilt es zunächst zu prüfen, wer in diesem Kontext die datenschutzrechtliche Verantwortung i.S.d. DS-GVO innehat und an wen folglich die möglichen Ermächtigungsgrundlagen zu adressieren sind.

B. Datenschutzrechtliche Verantwortlichkeit

Laut **Art. 4 Nr. 7 DS-GVO** ist datenschutzrechtlicher Verantwortlicher oder Verantwortliche „*die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet*“. Grundlegendes Kriterium bei der Bestimmung eines oder einer datenschutzrechtlichen Verantwortlichen ist folglich die Entscheidungsgewalt über Zweck und Mittel der Datenverarbeitung, wobei die Verarbeitung an sich nicht von dem oder der

[579] Kort, *NZA 2011, 1319 (1319).*
[580] Jorzig/Sarangi, *Digitalisierung im Gesundheitswesen, S. 82.*
[581] *Siehe hierzu die Ausführungen in der Einleitung.*

Verantwortlichen getätigt werden muss.[582] Anhand der Entscheidungsgewalt erfolgt auch die Abgrenzung zwischen Verantwortlichem bzw. Verantwortlicher und Auftragsverarbeiter bzw. -verarbeiterin.[583] Der oder die datenschutzrechtliche Verantwortliche ist Adressat oder Adressatin der Pflichten aus der DS-GVO und muss nach Art. 5 II DS-GVO nachweisen, dass personenbezogene Daten rechtmäßig verarbeitet werden.[584]

Die weitere Ausgestaltung des Begriffs findet in **Art. 24 DS-GVO** statt. Art. 24 DS-GVO stellt unter dem Prinzip des risikobasierten Ansatzes die allgemeingültige, horizontal wirkende Rechenschaftspflicht des oder der Verantwortlichen auf. Zur Sicherstellung der zulässigen Datenverarbeitung sind technische und organisatorische Maßnahmen zu treffen.[585] Adressat oder Adressatin der Pflichten ist ausdrücklich nur der oder die Verantwortliche. Für Auftragsverarbeiter und -verarbeiterinnen gilt die Pflicht zur sicheren Datenverarbeitung durch Art. 32 DS-GVO.[586]

Im Auftrag des oder der Verantwortlichen können weitere „*natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen"* personenbezogene Daten verarbeiten. Dies sind nach **Art. 4 Nr. 8 DS-GVO** sogenannte „*Auftragsverarbeiter*". Die Begriffsbestimmungen nach Art. 4 Nr. 7 und 8 DS-GVO dienen zuvorderst dem Zweck, die am Verarbeitungsvorgang beteiligten Parteien im Hinblick auf die datenschutzrechtliche Verantwortlichkeit voneinander abzugrenzen.[587] Der Auftragsverarbeiter oder die Auftragsverarbeiterin ist kein Dritter i.S.d. Art. 4 Nr. 10 DS-GVO.[588] Ein wichtiges Merkmal im Verhältnis zum oder zur Verantwortlichen ist die Weisungsgebundenheit des Auftragsverarbeiters oder der -verarbeiterin gegenüber dem oder der Verantwortlichen. Diese ergibt sich nicht direkt aus Art. 4 Nr. 8 oder Art. 28 DS-GVO, sondern kann aus Art. 29 DS-GVO abgeleitet werden.[589] Durch die Weisungsgebundenheit des Auftragsverarbeiters oder der -verarbeiterin gelten nur für den oder die Verantwortlichen die datenschutzrechtlichen Voraussetzungen für eine rechtmäßige Verarbeitung personenbezogener Daten, er oder die trägt die volle datenschutzrechtliche Verantwortung. Wird nach der Rechtmäßigkeit der Verarbeitung gesucht, so steht nicht der Auftragsverarbeiter oder die -verarbeiterin, sondern der oder die Verantwortliche im Mittelpunkt der Regelungen.[590]

Die nähere Ausgestaltung des Verhältnisses zwischen Verantwortlichem bzw. Verantwortlicher und Auftragsverarbeiter bzw. -verarbeiterin regelt **Art. 28 DS-GVO**. Hiernach steht es den Beteiligten frei, in welcher Rechtsform das Auftragsverhältnis begründet wird. Möglich sind „Dienstverträge, Werkverträge, Geschäftsbesorgungsverträge aber auch Gestaltungen im

---

[582] Taeger/Gabel*, Kommentar DSGVO - BDSG DS-GVO Art. 4 Rn 169;* Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 4 Rn 36.*
[583] Taeger/Gabel*, Kommentar DSGVO - BDSG DS-GVO Art. 4 Rn 168.*
[584] Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 4 Rn 114,.*
[585] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 4 Rn 49, Art. 24 Rn 1.*
[586] Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 24 Rn 3.*
[587] Taeger/Gabel*, Kommentar DSGVO - BDSG DS-GVO Art. 4 Rn 204.*
[588] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 4 Rn 74.*
[589] Forgó u. a.*, Betrieblicher Datenschutz - Rechtshandbuch Teil VII. Kap. 2 Rn 18;* Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 4 Rn 40.*
[590] Paal/Pauly*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 4 Rn 56;* Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 28 Rn 11.*

Rahmen bestehender Geschäftsbeziehungen".[591] Überschreitet der Auftragsverarbeiter bzw. die -verarbeiterin die Grenzen des Auftragsverhältnisses und bestimmt Zweck und Mittel der Verarbeitung neu, so gilt dieser nach Art. 28 X DS-GVO selbst als Verantwortlicher oder Verantwortliche.[592] Innerhalb des Auftragsverhältnisses hat der Auftragsverarbeiter oder die -verarbeiterin jedoch einen gewissen Grad ein Eigenständigkeit. So kann dieser oder diese beispielsweise über die Hard- und Softwareinfrastruktur entscheiden beziehungsweise mitentscheiden.[593]

Grundsätzlich ist der Auftragsarbeiter oder die -verarbeiterin in der Systematik der DS-GVO als „verlängerter Arm" des oder der Verantwortlichen zu betrachten, der oder die zwar die tatsächliche Herrschaft über den Verarbeitungsprozess innehat, jedoch nicht über Zweck und Mittel der Verarbeitung entscheidet. Diese Weisungsgebundenheit überlässt dem oder der Verantwortlichen die alleinige Verantwortung für die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten.[594]

Bezogen auf Krankenhäuser liegt es nahe, dass Arbeiten außerhalb der Kernkompetenzen eines Krankenhausbetriebes an externe Dienstleister oder Dienstleisterinnen delegiert werden. Im Hinblick auf Kosten- und Risikosenkungen, Mangel an IT- und Fachpersonal sowie fehlender internen Kompetenzen bei datenschutzrechtlichen Themen, werden häufig externe IT-Dienstleister oder -Dienstleisterinnen beauftragt.[595]

Wird von der krankenhausinternen IT-Abteilung die IT-Sicherheit und somit auch der Einsatz von Angriffserkennungssystemen übernommen, ist der oder die Betreibende des Krankenhauses in privater Trägerschaft der oder die Verantwortliche i.S.d. DS-GVO. Dies ändert sich nicht, wenn für die IT-Sicherheit externe Dienstleister oder Dienstleisterinnen beauftragt werden und diese weisungsgebunden sind und somit Auftragsverarbeiter oder -verarbeiterinnen i.S.d. DS-GVO sind.

C. Rechtmäßigkeit der Datenverarbeitung durch die DS-GVO

Die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten nach der DS-GVO richtet sich primär nach Art. 5 und 6 DS-GVO. Werden besondere Kategorien personenbezogener Daten verarbeitet, müssen zudem die Ausnahmetatbestände des Art. 9 DS-GVO beachtet werden. Dass generell eine Ermächtigungsgrundlage für die Verarbeitung von personenbezogener Daten notwendig ist, ergibt sich, wie bereits im verfassungsrechtlichen Teil dieser Arbeit erörtert, aus den unionsrechtlichen Datenschutzgrundrechten, vordergründlich aus Art. 8 II 1 GRCh.

[591] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 4 Rn 76.*
[592] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 24 Rn 19.*
[593] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 28 Rn 3.*
[594] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 28 Rn 2.*
[595] Management & Krankenhaus, *Das Outsourcing ist kein Selbstläufer.*

Im Folgenden werden die Grundsätze der Datenverarbeitung vorgestellt, die in Art. 5 DS-GVO geregelt sind und bei jeder Verarbeitung von personenbezogener Daten Anwendung finden. Anschließend werden die Erlaubnistatbestände des Art. 6 DS-GVO auf ihre Anwendbarkeit bei der Nutzung von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft geprüft. Da in Krankenhäusern unter anderem Gesundheitsdaten verarbeitet werden können und diese zu den Kategorien besonderer personenbezogener Daten des Art. 9 I DS-GVO zählen, werden zudem die verschärften Ermächtigungsgrundlagen des Art. 9 II DS-GVO geprüft. Das Kapitel schließt mit einer Übersicht über die technische Komponente des Datenschutzsystems der DS-GVO und stellt die Maßnahmenkataloge und Sicherheitsstandards vor, die in den Art. 24, 25 und 32 DS-GVO bei der Verarbeitung von personenbezogenen Daten gefordert werden.

1. Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO

Art. 5 I DS-GVO enthält die Grundsätze der Datenverarbeitung nach der DS-GVO. Diese sind nicht im klassischen Aufbau in Tatbestand und Rechtsfolge unterteilt, sondern geben ein allgemeines Strukturprinzip vor, dass sich durch die Einzelregelungen der gesamten DS-GVO zieht und in den nachfolgenden Artikeln weiter konkretisiert wird.[596] Es sind fundamentale Regeln für die Verarbeitung personenbezogener Daten, die trotz ihrer sehr allgemein gehaltenen Formulierung eine Konkretisierung der Ziele aus Art. 1 DS-GVO sowie der Grundrechte aus Art. 16 II AEUV und Art. 8 EMRK darstellen.[597] Trotz ihrer Bezeichnung als „Grundsätze“ sind die Vorgaben in Art. 5 DS-GVO unmittelbar geltende Pflichten, die laut Art. 5 II DS-GVO insbesondere die Verarbeitenden zur Einhaltung verpflichten.[598] Jede Datenverarbeitung, die in den Schutzbereich der DS-GVO fällt, muss kumulativ sämtlichen Grundsätzen des Art. 5 I DS-GVO entsprechen.[599] Verstöße gegen Art. 5 DS-GVO werden nach Art. 83 V DS-GVO besonders hart sanktioniert.

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Gemäß Art. 5 I lit. a DS-GVO müssen personenbezogene Daten „*auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden*“.

Der hier verankerte Grundsatz der **Rechtmäßigkeit** der Verarbeitung personenbezogener Daten ist der oberste Grundsatz des Art. 5 DS-GVO und entspricht dem datenschutzrechtlichen

[596] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 4.*
[597] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 3, 20.*
[598] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 5 Rn 1;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 4.*
[599] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 5.*

Erlaubnisvorbehalt aus Art. 8 II 1 GRCh[600] Der Grundsatz der Rechtmäßigkeit hat keine spezifische rechtliche Wirkung, er bringt jedoch programmatisch die Grundrechtssensitivität der Datenverarbeitung zum Ausdruck.[601] Dies beinhaltet nicht nur die Forderung nach einer gesetzliche Grundlage für die Verarbeitung personenbezogener Daten, sondern dass auch das „wie" der Datenverarbeitung rechtmäßig sein muss.[602] Gesetzliche Grundlagen zu Verarbeitung personenbezogener Daten sind in Art. 6 und 9 DS-GVO verankert.[603] Zudem können sich Rechtsgrundlagen aus dem Recht der Mitgliedstaaten oder weiterem Unionsrecht ergeben, wenn die DS-GVO entsprechende Öffnungsklauseln hierfür vorgesehen hat.[604]

Personenbezogene Daten müssen zudem nach **Treu und Glauben** verarbeitet werden. Die Übersetzung des englischen Begriffs „fairness" in Treu und Glauben wird stark kritisiert, da Assoziationen mit dem Begriff Treu und Glauben aus dem deutschen Zivilrecht nahe liegen und der Begriff entsprechend geprägt ist.[605] So wird der englischsprachige Begriff im französischen mit loyautè und im italienischen mit correttezza („richtig", „fehlerfrei", „fair") übersetzt, was für eine deutsche Übersetzung als „Fair" oder „Fairness" sprechen würde.[606] Die Verarbeitung personenbezogener Daten nach Treu und Glauben bezieht sich auf die „Art und Weise der Rechtsausübung im Verhältnis zwischen Verantwortlichem und betroffener Person"[607] und wirkt unfairen Verhaltensweisen und unzulässiger Rechtsausübung entgegen.[608] Vom Grundsatz erfasst werden solche Situationen, die dem Kräftegleichgewicht zwischen Verantwortlichem oder Verantwortlicher und betroffener Person widersprechen oder den grundsätzlichen Erwartungen der betroffenen Personen an die Verarbeitung nicht entsprechen.[609]

Der Grundsatz der **Transparenz** entspricht der Feststellung des BVerfG von 1983, in der es heißt: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."[610] Ohne den Grundsatz der Transparenz würde der Datenschutz ins Leere laufen, weil Rechtsverstöße dem oder der Betroffenen unter Umständen nicht bekannt werden würden.[611] Die Transparenz umfasst hierbei nicht nur die Retrospektive, also die

---

[600] Albrecht/Jotzo, *Das neue Datenschutzrecht der EU Teil 2 Rn 2.*
[601] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 33.*
[602] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 38.*
[603] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 8.*
[604] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 6.*
[605] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 5 Rn 13.*
[606] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 18;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 47;* Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 14.*
[607] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 44.*
[608] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 8;* Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 9.*
[609] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 17;* Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 5 Rn 14.*
[610] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 50.*
[611] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 11.*

Nachvollziehbarkeit der bereits stattgefundenen Datenverarbeitung, sondern auch die Prospektive, also Transparenz zukünftiger Datenverarbeitung.[612] Gemäß Erwägungsgrund 39 S. 3 der DS-GVO setzt der Grundsatz der Transparenz voraus, „*dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind*". Der Grundsatz betrifft nicht nur die Art und Weise der Information, sondern auch den Inhalt dieser.[613] Konkretisierungen finden sich in der DS-GVO unter anderem in Art. 12 bis 15 sowie in Art. 32 und 25.[614]

b) Zweckbindung

Art. 5 I lit. b DS-GVO normiert den Grundsatz der Zweckbindung. Hiernach müssen personenbezogene Daten „*für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden*". Der Grundsatz der Zweckbindung stellt den zentralen Grundsatz des europäischen Datenschutzrechts dar und ist auf Grundrechtsebene in Art. 8 II 1 GRCh verankert.[615] Der Zweck der Datenverarbeitung ist mit der Zulässigkeit der Datenverarbeitung eng verbunden, da die Erlaubnistatbestände der Art. 6 und 9 DS-GVO an die Verarbeitungszwecke anknüpfen.[616]

Gemäß Erwägungsgrund 39 S. 6 der DS-GVO muss bei der Erhebung von personenbezogenen Daten der Zweck der Datenverarbeitung bereits festgelegt sein. Der Zweck bestimmt unter anderem, welche Daten verarbeitet werden dürfen und wie lange diese gespeichert werden dürfen.[617] Hierbei muss es sich nicht nur um einen Zweck handeln, sondern kann mehrere Zwecke umfassen, die jedoch alle eindeutig bestimmt sein müssen.[618] Ist der Zweck der Datenverarbeitung nicht explizit oder konkret genug, so ist die Datenverarbeitung verboten.[619] Dies bezieht sich vor allen Dingen auf unklare Umschreibungen und vage Zweckfestlegungen.[620] Es gibt zudem keine zweckfreie Datenverarbeitung, da jede Verarbeitung ein Ziel verfolgt.[621] Die Zulässigkeit der gesamten Datenverarbeitung ist an den festgelegten Zweck gebunden und die Einhaltung dieses Zweckes ist in jeder Phase der Verarbeitung durch den Verantwortlichen oder die Verantwortliche zu überprüfen.[622] Die Zweckbindung erlischt erst zum Zeitpunkt der Zweckerfüllung, was zu einer Löschpflicht führt.[623]

---

[612] Paal/Pauly*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 21;* Taeger/Gabel*, Kommentar DSGVO - BDSG DS-GVO Art. 5 Rn 16.*
[613] Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 11.*
[614] Kühling/Buchner*, Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 19.*
[615] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 63, 64.*
[616] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 13.*
[617] Kühling/Buchner*, Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 21.*
[618] Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 13.*
[619] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 72.*
[620] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 14.*
[621] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 70.*
[622] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 92.*
[623] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 17.*

Der Zweck der Datenverarbeitung ist zudem der Bezugspunkt für die Erforderlichkeitsprüfung.[624] So besagt Erwägungsgrund 39 der DS-GVO in Satz 9, dass „*personenbezogene Daten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann*".

Die Zweckbindung erstreckt sich auch auf Folgenutzer und -nutzerinnen, die die Daten von dem Erstverantwortlichen oder der Erstverantwortlichen übermittelt bekommen haben.[625] Erhalten die Folgenutzer und -nutzerinnen die Daten ohne, dass sie diese erheben müssen, setzt die Zweckbindung mit dem Speichern der Daten ein.[626]

Der Grundsatz der Zweckbindung wird flankiert von den Grundsätzen der Datenminimierung und der Speicherbegrenzung.[627]

Die Zweckbindung erstreckt sich grundsätzlich auch auf die **Weiterverarbeitung** der Daten.[628] Eine Weiterverarbeitung der Daten zu Zwecken, die nicht identisch mit dem ursprünglichen Zweck sind, ist unter der in Art. 5 I lit. b DS-GVO aufgeführte Bedingung, dass diese „*nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise"* weiterverarbeitet werden, möglich.[629] Der Primärzweck ist folglich der Maßstab zur Beurteilung der Vereinbarkeit der Weiterverarbeitung.[630]

Dies wird durch die Öffnungsklausel des **Art. 6 IV DS-GVO** gestützt, wonach eine Verarbeitung, die „*zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden*" und die „*nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt*" beruht, möglich ist, wenn diese „*zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist*". Zudem bestimmt auch Erwägungsgrund 50 S. 1 der DS-GVO, dass die Verarbeitung personenbezogener Daten für andere Zwecke als die ursprünglichen nur zulässig sein sollte, „*wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist*".

Der deutsche Gesetzgeber hat von der Öffnungsklausel des Art. 6 IV DS-GVO Gebrauch gemacht und in den §§ 23 und 23 BDSG Regelungen zur Zweckänderung erlassen.[631]

Für die Weiterverarbeitung von personenbezogenen Daten gilt jedoch auch weiterhin, dass diese den Grundsätzen des Art. 5 DS-GVO sowie den Anforderungen der Rechtgrundlage für

---

[624] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 23.*
[625] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 93.*
[626] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 16.*
[627] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 21.*
[628] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 29.*
[629] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 16.*
[630] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 30.*
[631] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 102.*

die Datenverarbeitung nach Art. 6 I sowie gegebenenfalls Art. 9 II DS-GVO entsprechen müssen. Dies gilt auch, wenn die mit der Weiterverarbeitung einhergehende Zweckänderung mit dem ursprünglichen Zweck vereinbar ist.[632] Art. 6 IV DS-GVO ist kein Erlaubnistatbestand für die Verarbeitung personenbezogener Daten.[633]

Strittig ist indes, ob die Weiterverarbeitung und der damit einhergehenden Zweckänderung einer besonderen Rechtsgrundlage bedarf (*siehe Kapitel 2.c)(6)(a) Verstoß gegen den Grundsatz der Zweckbindung?*).

c) Datenminimierung

Gemäß Art. 5 I lit. c DS-GVO müssen personenbezogene Daten „*dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein*". Diese drei Merkmale beschreiben den Grundsatz der Datenminimierung, wobei die einzelnen Begriffsdefinitionen fließend sind und ineinander übergehen. Daten sind dem Zweck angemessen, wenn diese einen Bezug zum festgelegten Verarbeitungszweck aufweisen. Eine Erheblichkeit liegt vor, denn die Verarbeitung zur Förderung dieses Zweckes geeignet ist. Die Beschränkung der Verarbeitung auf ein notwendiges Maß ist gegeben, wenn nicht mehr Daten verarbeitet werden, als zur Erreichung des Verarbeitungszwecks nötig sind.[634] Der Grundsatz der Datenminimierung gibt keine Beschränkung auf ein absolutes Minimum vor, sondern zielt auf ein dem Verarbeitungszweck angemessenes Niveau ab, das im Einzelfall zu bestimmen ist.[635] Durch die Orientierung am Verarbeitungszweck ergänzt der Grundsatz der Datenminimierung den Grundsatz der Zweckbindung.[636] Zudem beinhaltet der Grundsatz der Datenminimierung auch die Reduzierung der Datennutzung. Hierunter fallen Mehrfachauswertungen, die weitgehend gleich Informationen enthalten oder die Anzahl der betroffenen Personen möglichst gering zu halten.[637]

Eine konkrete Ausprägung des Grundsatzes der Datenminimierung ist in Art. 25 DS-GVO zu finden, der den Datenschutz durch Technikgestaltung (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) regelt sowie im Gebot der Speicherbegrenzung, das ebenfalls in Art. 5 DS-GVO normiert ist.[638]

---

[632] Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 19.*
[633] Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 19.*
[634] Kühling/Buchner*, Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 57.*
[635] Taeger/Gabel*, Kommentar DSGVO - BDSG DS-GVO Art. 5 Rn 27.*
[636] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 116;* Kühling/Buchner*, Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 56.*
[637] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 22.*
[638] Taeger/Gabel*, Kommentar DSGVO - BDSG DS-GVO Art. 5 Rn 29;* Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 23.*

d) Richtigkeit

Der Grundsatz der Richtigkeit nach Art. 5 I lit. d DS-GVO besagt, dass personenbezogene Daten „*sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein*“ müssen. Es sind zudem „*alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden*“. Der Grundsatz der Richtigkeit bezieht sich folglich auf die Qualität der verarbeiteten personenbezogenen Daten.[639] Daten sind „sachlich richtig“, wenn die gespeicherten Informationen über eine Person nach objektiven Kriterien mit der Realität übereinstimmen. Somit ist der Grundsatz nur auf Tatsachen anwendbar, die einem Beweis zugänglich sind, da Werturteile oberhalb der Beleidigungsgrenze nicht richtig oder falsch sein können.[640] Ob ein Datum „richtig“ ist, bestimmt sich einzelfallbezogen vom Kontext und dem jeweiligen Verwendungszweck. Der Grundsatz der Richtigkeit ist somit eng verbunden mit dem Grundsatz der Zweckbindung.[641] Dass Daten „auf dem neuesten Stand“ sind, ist nicht erforderlich, wenn es sich um „historische Daten“ handelt, die unmittelbar mit einem bestimmten Zeitpunkt verknüpft sind. So bleiben etwa Daten im Rahmen einer medizinischen Untersuchung „richtig“, auch wenn sich der Gesundheitszustand in der Zwischenzeit verändert hat.[642]

Der Grundsatz der Richtigkeit enthält zudem die Verpflichtung des oder der Verantwortlichen, aktiv die „Richtigkeit“ der verarbeiteten Daten zu überprüfen.[643] „Unrichtige“ Daten sind auch ohne Verlangen der betroffenen Person unverzüglich zu löschen oder zu berichtigen.[644]

Eine Konkretisierung erfährt der Grundsatz der Richtigkeit in Art. 16 DS-GVO, der der betroffenen Person ein Recht auf Berichtigung zuspricht.[645]

e) Speicherbegrenzung

Nach Art. 5 I lit. e DS-GVO müssen personenbezogene Daten „*in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist*“. Eine darüber hinaus gehende Speicherung der Daten ist nur gestattet, „*soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische*

---

[639] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 136.*
[640] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 139, 140;* Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 60.*
[641] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 62;* Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 5 Rn 37.*
[642] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 5 Rn 31.*
[643] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 24;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 143.*
[644] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 24.*
[645] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 5 Rn 32.*

Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden". Eine Definition des Begriffs „Speichern" gibt die DS-GVO nicht vor. Hierfür kann auf die Legaldefinition des Begriffs nach § 3 V Nr. 4 BDSG a.F. zurückgegriffen werden, wonach das Speichern ein „*technischer Vorgang und Zustand der Aufbewahrung von personenbezogenen Daten zum Zweck ihrer weiteren Verarbeitung oder Nutzung*" ist.[646]

Der Grundsatz der Speicherbegrenzung ist demnach eng verbunden mit dem Zweck der Datenverarbeitung, da dieser den Zeitraum der zulässigen Speicherung durch seinen Einfluss auf die Erforderlichkeit bestimmt.[647] Zudem findet der Grundsatz der Datenminimierung in der Speicherbegrenzung ein zeitliches Seitenstück.[648] Für die Speicherfrist ist gemäß Erwägungsgrund 39 S.8 der DS-GVO „*das unbedingt erforderliche Mindestmaß*" einzuhalten. Laut Satz 10 soll der oder die Verantwortliche Fristen für die Löschung vorsehen sowie regelmäßige Überprüfungen durchführen. Somit sind Vorratsdatenspeicherungen, um die Daten für zukünftig entstehende Zwecke nutzen zu können, unzulässig.[649] Dies ist auch in Bezug auf die Weiterverarbeitung zur Sekundärzwecken zu beachten, wenn diese zeitlich mit der Verarbeitung zur dem Primärzweck auseinanderfallen, da bei Primärzweckerfüllung die Pflicht zur Löschung der Daten greift.[650]

Eine Konkretisierung erfährt der Grundsatz der Speicherbegrenzung durch Art. 17 I DS-GVO, wonach die betroffene Person unter bestimmten Voraussetzungen die Löschung ihrer personenbezogenen Daten verlangen kann. Die Pflicht zur Löschung von Daten, die aufgrund ihrer Zweckerreichung obsolet geworden sind, besteht allerdings auch ohne ausdrückliches Begehren der betroffenen Person.[651] Daten müssen aber nicht grundsätzlich immer gelöscht werden. Der Wortlaut des Art. 5 I lit. e DS-GVO weist darauf hin, dass dem Grundsatz der Speicherbegrenzung auch genüge getan wird, wenn der Personenbezug vollkommen und unwiderrufbar aufgehoben wird.[652]

f) Integrität und Vertraulichkeit

Der Grundsatz der Integrität und Vertraulichkeit findet sich als letzter Grundsatz in Art. 5 I lit. f DS-GVO. Hiernach müssen personenbezogene Daten „*in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet*". Dies schließt den „*Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen*" ein. Durch die Vorgaben zur technischen und

[646] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 151.*
[647] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 65.*
[648] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 5 Rn 39.*
[649] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 25.*
[650] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 43.*
[651] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 5 Rn 37.*
[652] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 5 Rn 66.*

organisatorischen Sicherung werden die Grundsätze der Rechtmäßigkeit, der Zweckbindung, der Datenminimierung, der Richtigkeit und der Speicherbegrenzung unterstützt.[653]

Kritisiert wird die Bezeichnung des Grundsatzes, da er in seinem Schutzbereich weit über die technischen Ziele Integrität und Vertraulichkeit hinaus geht. So werden nach Erwägungsgrund 39 S. 12 der DS-GVO ebenfalls die Ziele der Verfügbarkeit und der Unversehrtheit der Daten sowie die Zugangs- und Zugriffsbeschränkungen aufgeführt.[654] So werden in diesem Grundsatz auch Aspekte des durch das BVerfG anerkannten Grundrechts auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme umgesetzt.[655]

Eine Konkretisierung erfährt der Grundsatz in den technischen und organisatorischen Vorgaben der Art. 25 und 32 DS-GVO.[656]

In Bezug auf Art. 5 DS-GVO ist zudem **Art. 23 DS-GVO** zu nennen, der als allgemeine Öffnungsklausel der Union und den Mitgliedstaaten die Möglichkeit gibt, die Betroffenenrechte nach Art. 12 bis 22 sowie 34 DS-GVO unter bestimmten Voraussetzungen zu beschränken und folglich auch mittelbar die Grundsätze des Art. 5 DS-GVO zu begrenzen[657], aber weder einen Erlaubnistatbestand zur Verarbeitung personenbezogener Daten enthält noch der Union oder den Mitgliedstaaten die Möglichkeit zur Schaffung eines solchen Erlaubnistatbestandes einräumt.

Im weiter Verlauf der DS-GVO kommen die Grundsätze des Art. 5 I DS-GVO vor allem in den Generalklauseln der Art. 6 und 9 DS-GVO zum Ausdruck. Im Folgenden werden diese beiden Artikel im Hinblick auf die Rechtmäßigkeit der Verarbeitung personenbezogener Daten bei der Nutzung von Angriffserkennungssystemen in privatrechtlichen Kontext im Gesundheitssektor beleuchtet.

2. Rechtmäßigkeit der Datenverarbeitung nach Art. 6 DS-GVO

Die zentrale Norm zur Regelung des Grundsatzes der Rechtmäßigkeit der Datenverarbeitung ist Art. 6 DS-GVO. Diese Norm befasst sich mit dem „Ob“ der Datenverarbeitung, also den Rechtfertigungsgründen, während Art. 5 DS-GVO das „Wie“ betrifft. Gemeinsam geben sie die Voraussetzungen für eine rechtmäßige Verarbeitung im Einzelfall vor.[658]

---

[653] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 168.*
[654] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 47;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 167.*
[655] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 170.*
[656] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 29;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 171.*
[657] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 23 Rn 2;* Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 23 Rn 1, 9.*
[658] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 1.*

Im Art. 6 I DS-GVO ist die Grundaussage verankert, dass die Verarbeitung personenbezogener Daten grundsätzlich nur zulässig ist, soweit der oder die Betroffene eingewilligt hat oder die Verarbeitung durch eine entsprechende Rechtsvorschrift legitimiert ist.[659] Die in Art. 6 I DS-GVO genannten Erlaubnistatbestände sind abschließend und stehen gleichberechtigt nebeneinander.[660] Es können zudem im Einzelfall auch mehrere der Erlaubnistatbestände zugleich verwirklicht sein, wobei zur Begründung der Rechtmäßigkeit die Erfüllung eines Tatbestandes genügt.[661]

Werden besondere Kategorien von personenbezogenen Daten verarbeitet, ist zudem Art. 9 DS-GVO hinzuzuziehen.[662]

Keine Rechtsgrundlagen für die Verarbeitung personenbezogener Daten stellen indes Art. 9 Absatz 2 bis 4 der DS-GVO dar. Absatz 2 und 3 geben Möglichkeiten und Voraussetzungen für Spezialgesetze im Rahmen des Absatz 1 vor, während Absatz 4 die Vereinbarkeitsvoraussetzungen der Verarbeitung bei Zweckänderung regelt.[663]

Im Folgenden werden die für den Einsatz von Angriffserkennungssystemen relevanten Erlaubnistatbestände des Art. 6 I DS-GVO auf ihre Anwendbarkeit geprüft.

a) Die Einwilligung nach Art. 6 I 1 lit. a i.V.m. Art. 7 DS-GVO

Einfachstes und verbraucherfreundlichstes Mittel für eine rechtmäßige Datenverarbeitung ist die Einwilligung der betroffenen Personen in die Nutzung von Angriffserkennungssystemen und der daraus resultierenden Verarbeitung von personenbezogenen Daten.

Die Einwilligung ist direkter Ausdruck des Grundrechtes auf informationelle Selbstbestimmung[664] und in Art. 6 I 1 lit. a DS-GVO verankert. Art. 7 und 8 der DS-GVO regeln ergänzend die Bedingungen für eine wirksam erteile Einwilligung. Laut Legaldefinition des Art. 4 Nr. 11 DS-GVO ist eine Einwilligung „*jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist*“. Gemäß Erwägungsgrund 42 S. 5 ist die in Art. 4 Nr. 11 DS-GVO geforderte Freiwilligkeit einer Einwilligung nur gegeben, wenn die betroffene Person „*eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile*

---

[659] Brink/Wolff, *BeckOK Datenschutzrecht, Teil DS-GVO Art. 6 Rn 11.*
[660] Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht§ 3 Rn 54.*
[661] Veil, *NVwZ 2018, 686 (689);* Veil, *NJW 2018, 686 (3337);* Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 8.*
[662] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 14;* Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 1.*
[663] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG Einführung zu Artikel 6 Rn 2.*
[664] Kühling/Buchner, *Datenschutzgrundverordnung Kommentar, Teil Art. 6 Rn 17.*

zu erleiden". Erwägungsgrund 43 stellt zudem klar, dass eine – aus einem Ungleichgewicht zwischen der betroffenen Person und des Verarbeiters oder der Verarbeiterin resultierende – Zwangssituation der Freiwilligkeit einer Einwilligung entgegenstehen kann. Zudem hat die betroffene Person nach Art. 7 III DS-GVO das Recht, die Einwilligung jederzeit widerrufen zu können. Ein wirksamer Widerruf wirkt ex-nunc, die Wirksamkeit der Einwilligung entfällt erst ab dem Zeitpunkt des Widerrufes und nicht für den gesamten Zeitraum der Einwilligung.[665]

Die Einwilligung steht in keinem Alternativverhältnis zu den übrigen Erlaubnistatbeständen des Art. 6 I DS-GVO. Fällt die Einwilligung durch einen Unwirksamkeitsgrund oder einen Widerruf weg, so kann die Verarbeitung von personenbezogenen Daten auf Grundlage eines andere Erlaubnistatbestandes rechtmäßig bleiben.[666]

Im konkreten Fall weist die Einwilligung als Ermächtigungsgrundlage zur Rechtfertigung der Nutzung von Angriffserkennungssystemen in privatrechtlich organisierten Krankenhäusern allerdings eine zu hohe Rechtsunsicherheit auf. Die Möglichkeit nach Art. 7 III 1 DS-GVO jederzeit eine erteile Einwilligung ohne Angabe von Gründen[667] widerrufen zu können, kann keine einheitliche rechtliche Absicherung bei der Verarbeitung personenbezogener Daten in einem größeren Personenkreis gewährleisten. Zudem besteht im Kontext der Nutzung solcher Systeme in privatrechtlich organisierten Krankenhäusern die Gefahr einer besonderen Abhängigkeit des oder der Einwilligenden[668], da dieser oder diese als Patient bzw. Patientin auf die Gesundheitsversorgung im Krankenhaus angewiesen ist. Dieses mögliche Ungleichgewicht kann die Erfüllung der Freiwilligkeit als Grundvoraussetzung der Einwilligung in Frage stellen.

Die Einwilligung als Ermächtigungsgrundlage zur Rechtfertigung der Verarbeitung personenbezogener Daten durch Angriffserkennungssysteme ist somit in ihrem Ansatz zu individuell und nicht auf die kollektive Masse an betroffenen Personen (Patienten und Patientinnen, Mitarbeitende, Besuchende) anwendbar, ohne ein hohes Wagnis an Rechtsunsicherheit und individuellen Einzelregelungen eingehen zu müssen. Individuelle Vereinbarungen sowie der Widerruf von diesen machen eine wirksame und wirtschaftliche Nutzung von Angriffserkennungssystemen technisch schwer möglich. Die Einwilligung kommt somit im vorliegenden Fall als beständige Ermächtigungsgrundlage nicht in Betracht.

---

[665] Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 7 Rn 48;* Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 7 Rn 54.*
[666] Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis§ 2 Rn 4.*
[667] Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 7 Rn 46.*
[668] Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 7 Rn 27.*

b) Die Verarbeitung für die Erfüllung eines Vertrages nach Art. 6 I 1 lit. b DS-GVO

Eine weitere Möglichkeit zur Rechtfertigung der Verarbeitung von personenbezogenen Daten im Rahmen der Nutzung von Angriffserkennungssystemen findet sich in Art. 6 I 1 lit. b DS-GVO.

Laut Art. 6 I 1 lit. b DS-GVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn „*die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich*“ ist. Art. 6 I 1 lit. b DS-GVO rechtfertigt die Datenverarbeitung also nur im Zusammenhang mit einem Vertrag oder einem vorvertraglichen Verhältnis, wobei hier auch sämtliche vertragsähnliche Konstellationen, die „gleichermaßen auf willentliche Entscheidungen des Betroffenen zurückgehen“, erfasst sind.[669] Unter den Begriff des Vertrages i.S.d. Art. 6 I 1 lit. b DS-GVO fallen privatrechtliche Verträge ebenso wie öffentlich-rechtliche Verträge. Kollektivverträge wie Betriebsvereinbarungen und Tarifverträge fallen laut Literatur nicht unter den Begriff, da die Bindung von z.B. Arbeitnehmenden in diesem Fall nicht denselben Grad der Freiwilligkeit aufweist, wie bei einem eigenen Vertragsschluss.[670]

Wäre eine Datenverarbeitung im Rahmen von vertraglichen Erfüllungspflichten nicht möglich, wäre der von der Privatautonomie geprägte Rechtsverkehr gehemmt bzw. komplett eingeschränkt.[671] Art. 6 I 1 lit. b DS-GVO stellt insoweit eine erweiterte Form der Einwilligung dar, da die notwendige Verarbeitung personenbezogener Daten im vertraglichen Kontext gewissermaßen von der Freiwilligkeit des Vertragsschluss mitumfasst ist.[672] Werden besondere Kategorien personenbezogener Daten nach Art. 9 I DS-GVO verarbeitet, gibt es in Art. 9 II DS-GVO kein vergleichbares Pendant zu Art. 6 I 1 lit. b DS-GVO. Aufgrund der Nähe zur Einwilligung liegt daher im Rahmen der Verarbeitung nach Art. 9 DS-GVO der Rückgriff auf die Einwilligung nach Art. 9 II lit. a DS-GVO nahe.[673]

Die Rechtmäßigkeit der Datenverarbeitung steht aber auch hier unter dem Grundsatz der Erforderlichkeit. Diese ist jedenfalls gegeben, wenn ein unmittelbarer Zusammenhang zwischen der Verarbeitungsnotwendigkeit und dem konkreten Zweck des Vertragsverhältnisses besteht.[674] Die Anforderungen an diesen unmittelbaren Zusammenhang sind indes fließend. So ist die Erforderlichkeit zwar nicht gegeben, wenn die Interessen der Vertragsparteien ohne die Kenntnis der personenbezogenen Daten gewahrt werden können. Allerdings verlangt die Erforderlichkeit

---

[669] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 6 Rn 13;* Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 6 Rn 30.*
[670] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 18.*
[671] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 6 Rn 29;* Kühling/Buchner, *Datenschutzgrundverordnung Kommentar Art. 6 Rn 26.*
[672] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 18.*
[673] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 1 Rn 15.*
[674] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 6 Rn 14;* Albrecht/Jotzo, *Das neue Datenschutzrecht der EU Teil 3 Rn 43.*

keine Absolutheit, also keine derartige Erforderlichkeit, dass ohne die Verarbeitung der personenbezogenen Daten eine Durchführung des Vertragsverhältnisses nicht möglich wäre.[675] Ob die Erforderlichkeit der Datenverarbeitung gegeben ist, ist somit einzelfallbezogen nach den vertragsspezifischen Anforderungen des jeweiligen Mitgliedsstaates zu überprüfen. [676] Eine Interessenabwägung ist hingegen nicht erforderlich.[677]

Dem Wortlaut der Norm zufolge, muss der oder die Betroffene die Vertragspartei sein.[678]

In Krankenhäusern wird ein Großteil der Daten in den internen Netzwerken und Systemen auf Vertragsabschlüssen (Arbeitsverträge, Behandlungsverträge sowie Schuldverhältnisse sämtlicher Art) basieren. Dass die Daten hierbei von einem Angriffserkennungssystem analysiert und verarbeitet werden, ist jedoch für den Vertragsschluss nicht erforderlich. Man könnte allenfalls argumentieren, dass für die Erfüllung eines Vertrages die Sicherheit der Datenverarbeitung notwendig ist. Da aber kein unmittelbarer Zusammenhang zwischen der Verarbeitung der Daten durch ein Angriffserkennungssystem und der eigentlichen Vertragserfüllung besteht, ist auch hier die Erforderlichkeit der Verarbeitung nicht gegeben. Zudem fordert Art. 6 I 1 lit. b DS-GVO auch hier wieder eine Einzelprüfung für jeden konkreten Fall, was in der Praxis kaum umsetzbar sein wird und erneut zu Rechtsunsicherheit führt. Außerdem kann nicht pauschal davon ausgegangen werden, dass sämtliche Daten in den Netzwerken und Systemen eines Krankenhauses auf Vertragsschlüssen beruhen.

Der Erlaubnistatbestand des Art. 6 I 1 lit. b DS-GVO kommt also als allgemeingültige Rechtfertigungsnorm für den Einsatz von Angriffserkennungssystemen nicht in Betracht.

c) Die Erfüllung einer rechtlichen Verpflichtung nach Art. 6 I 1 lit. c DS-GVO

Bestünde eine bestehende rechtliche Verpflichtung, die die Nutzung von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft erforderlich macht, könnte diese über Art. 6 I 1 lit. c DS-GVO deren Einsatz rechtfertigen. Diese Verpflichtung muss sich kraft objektiven Rechts ergeben, wobei unerheblich ist, ob sie im Gemeinschaftsrecht oder innerstaatlichem Recht wurzelt.[679] Zudem wird auch in Art. 6 I 1 lit. c DS-GVO die Erforderlichkeit als Grundvoraussetzung verlangt. Diese ist gegeben, wenn die geforderte rechtliche Verpflichtung ohne die Verarbeitung der betroffenen Daten nicht erfüllt werden kann.[680] Hierfür muss nicht jede einzelne Verarbeitung in der Gesetzesnorm benannt werden; es reicht vielmehr, wenn diese

[675] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 38.*
[676] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 37.*
[677] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art.6 Rn 20.*
[678] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 6 Rn 30.*
[679] Bretthauer, *EnWZ 2017, 56 (59).*
[680] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 28.*

teleologisch von dieser erfasst werden solange sich die Norm unmittelbar auf die Verarbeitung bezieht.[681]

Im Gegensatz zu Art. 6 I 1 lit. b DS-GVO ist die Rechtfertigungsgrundlage kein privatautonomes Schuldverhältnis, sondern eine Rechtsnorm.[682] Aus welchem Rechtsgebiet diese stammt, ist allerdings nicht entscheidend. So sind neben öffentlich-rechtlichen Vorgaben auch Normen aus dem zivilrechtlichen oder strafrechtlichen Spektrum möglich.[683] Art. 6 I 1 lit. c DS-GVO fungiert hierbei als sogenannte „Scharniernorm", die nur gemeinsam mit der geforderten „rechtlichen Verpflichtung" eine Rechtfertigung der Verarbeitung personenbezogener Daten darstellen kann,[684] wobei fraglich ist, ob die geforderte Rechtsnorm den eigentliche Erlaubnistatbestand stellt oder ob diese erst i.V.m. Art. 6 I 1 lit. c DS-GVO zu einem Erlaubnistatbestand wird.[685] Welche Anforderungen an den Begriff der „rechtlichen Verpflichtung" i.S.d. Art. 6 I 1 lit. c DS-GVO zu stellen sind, ist in der Literatur umstritten. Die Frage hierbei ist, ob eine bloße Verpflichtung i.V.m. Art. 6 I 1 lit. c DS-GVO zu einem wirksamen Erlaubnistatbestand zur Verarbeitung personenbezogener Daten führt oder ob an die mitgliedstaatliche spezifische Bestimmung ebenfalls das Merkmal des Erlaubnistatbestandes und nicht nur der Verpflichtung zu stellen ist.

Vertreter und Vertreterinnen der Auffassung, dass die geforderte rechtliche Verpflichtung ebenfalls die Merkmale einer Erlaubnistatbestandsnorm umfassen müsse, sehen in Art. 6 I 1 lit.c DS-GVO lediglich eine Anforderungsformulierung an den Inhalt mitgliedstaatlicher rechtlicher Verpflichtungen. Die eigentliche Legitimationsgrundlage sei im mitgliedstaatlichen Recht zu suchen.[686] Die Datenverarbeitung würde demnach nicht durch Art. 6 I 1 lit. c DS-GVO, sondern durch die rechtliche Verpflichtung erlaubt werden.[687] Als Minimalanforderung wird hierbei angesehen, dass die rechtliche Verpflichtung die Erlaubnis zur Datenverarbeitung zumindest teleologisch erfasse.[688]

Gegenstimmen in der Literatur sehen in der rechtlichen Verpflichtung nicht die Erlaubnisnorm für die Datenverarbeitung. Diese stelle Art. 6 I 1 lit. c DS-GVO dar, da an die rechtliche Verpflichtung kein Entschließungs- oder Handlungsermessen gestellt würde. Die geforderte rechtliche Verpflichtung würde lediglich die Rechtspflicht zur Datenverarbeitung begründen, diese aber nicht legalisieren.[689] Der in Art. 6 I 1 lit. c DS-GVO geforderten Erforderlichkeit stehe dieser Interpretation nicht im Weg, da sich eine Erforderlichkeit schon dann ergeben würde, wenn eine gesetzliche Verpflichtung vorliege.[690] Würde an die rechtliche Verpflichtung i.S.d.

---

681 Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht§ 3 Rn 60.*
682 Albrecht/Jotzo*, Das neue Datenschutzrecht der EU Teil 3 Rn 45.*
683 Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 43.*
684 Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 1 Rn 52.*
685 Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht§ 4 Rn 85.*
686 Kühling/Buchner*, Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 6 Rn 73.*
687 Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 1 Rn 52.*
688 Specht/Mantz*, Handbuch Europäisches und deutsches Datenschutzrecht§ 3 Rn 60.*
689 Forgó u. a.*, Betrieblicher Datenschutz - Rechtshandbuch Teil V. Kap. 1 Rn 20.*
690 Paal/Pauly*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 6 Rn 16;* Brink/Wolff*, BeckOK Datenschutzrecht DS-GVO Art. 6 Rn 34.*

Art. 6 I 1 lit. c DS-GVO die Anforderung einer Erlaubnisnorm gestellt werden, müsste sich zudem die Frage stellen, wie diese neben den datenschutzrechtlichen Anforderungen der DS-GVO bestehen könne.[691]

Eine herrschende Meinung zur Interpretation der Anforderungen an die rechtliche Verpflichtung nach Art. 6 I 1 lit. c DS-GVO hat sich zum Stand der Bearbeitung nicht abgezeichnet.

(1) Spezifischere Bestimmungen nach Art. 6 II, III DS-GVO

Die DS-GVO ermöglicht den Mitgliedstaaten nach Art. 6 II, III DS-GVO im Anwendungsbereich von Art. 6 I 1 lit. c und e DS-GVO spezifischere Bestimmungen beizubehalten oder einzuführen, indem sie Anforderungen für die Verarbeitung präziser bestimmen. Eine nationalstaatliche Normierung ist jedoch nur für solche Materien möglich, die bereits von der DS-GVO regulativ umfasst sind. Zudem setzen Art. 6 II und III DS-GVO voraus, dass die spezifische Rechtsvorschrift einen verpflichtenden bzw. ermächtigenden Charakter aufweist.[692] Während in Absatz III S. 1 und 2 ein Regelungsauftrag an die Mitgliedstaaten und die Union formuliert wurde, werden ins Absatz II sowie Absatz III S. 3 Regelungsoptionen vorgegeben.[693] Dass die Mitgliedstaaten nationale Spezifizierungen vornehmen können, betont zudem Erwägungsgrund 10, der einen „*Spielraum für die Spezifizierung, auch für die Verarbeitung besonderer Kategorien von personenbezogenen Daten*“ in der DS-GVO klar vorsieht. Mitgliedstaaten können somit Rechtsvorschriften erlassen, „*in denen die Umstände besonderer Verarbeitungssituationen festgelegt werden, einschließlich einer genaueren Bestimmung der Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist*“.

Fraglich ist, ob Absatz II und III des Art. 6 DS-GVO unter den Begriff der **Öffnungsklauseln** fallen, da es sich hier nicht um eine „Ermächtigung für Abweichungen von der DS-GVO“, sondern um eine eingeschränkte Spezifizierung im Geltungsbereich der DS-GVO handelt.[694] Da die Mitgliedstaaten vor allem unter den Vorgaben von Absatz III zwar eigenständige Regelungsspielräume haben, diese aber nur innerhalb eines beschränkten Gestaltungsspielraumes stattfinden können, wird man zwar von einer echten, aber beschränkten Öffnungsklausel ausgehen müssen.[695]

Das Verhältnis der beiden Absätze zueinander ist zudem **umstritten**. Während in Absatz II ein weiter Öffnungsrahmen für die Mitgliedstaaten formuliert wird, sind die Voraussetzungen in Absatz III spezieller und geben auch der Union die Möglichkeit rechtliche Bedingungen für

---

[691] Taeger/Gabel*, Kommentar DSGVO - BDSG DS-GVO Art. 6 Rn 64;* Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 42.*
[692] Albrecht/Jotzo*, Das neue Datenschutzrecht der EU Teil 3 Rn 46.*
[693] Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 6.*
[694] Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 6.*
[695] Albrecht/Jotzo*, Das neue Datenschutzrecht der EU Teil 3 Rn 46;* Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 3 Rn 19.*

Art. 6 I 1 lit. c und lit. e DS-GVO festzulegen.[696] Stimmen in der Literatur sehen Absatz II deswegen als „dem Grunde nach entbehrlich" an, da der Umfang des Absatz II vom spezielleren Absatz III umfasst ist. Gegenstimmen sehen in Absatz II indes eine „selbstständige Öffnungsklausel mit eigenständigem Regelungsgehalt", die dem Bestreben der Mitgliedstatten auf Autonomie bei nationalen Angelegenheiten Folge leistet und somit eine andere Zielsatzung als Absatz III verfolgt.[697] Es empfiehlt sich, die Absätze 2 und 3 des Art. 6 DS-GVO bei der Bearbeitung kumulativ zu betrachten und bei der Einführung spezifischer Normen sowie bei der Prüfung auf Vereinbarkeit von bereits bestehenden Normen im Rahmen des Absatz II die Vorgaben des Absatz III zu beachten.[698]

Im Folgenden werden mögliche rechtliche Verpflichtungen vorgestellt und auf ihre Anwendbarkeit im konkreten Fall geprüft.

(2) § 8a BSIG

Eine Möglichkeit für eine solche rechtliche Verpflichtung könnte § 8a BSIG darstellen, der oder die Betreibende kritischer Infrastrukturen dazu verpflichtet, „*angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind*". Kritische Infrastrukturen sind gem. § 2 Nr. 10 BSIG Einrichtungen, Anlagen oder Teile davon, die aus den Sektoren Energie, Informationstechnik, Telekommunikation, Transport/Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen von „*hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden*". In der Literatur wird diese Rechtsgrundlage jedoch als zu pauschal gewertet; sie biete den Unternehmen in ihrer Abwägungsentscheidung zu wenig Hilfestellung.[699] Zudem fallen in Deutschland nur lediglich 5 bis 10 Prozent der Krankenhäuser (Stand 2017) unter den Begriff der Kritischen Infrastruktur nach dem BSIG.[700] Es können sich somit nicht sämtliche Krankenhäuser auf die Rechtsgrundlage des § 8a BISG stützen.

---

[696] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 2 Rn 7.*
[697] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 2 Rn 17, 18.*
[698] Kühling/Buchner, *Datenschutzgrundverordnung Kommentar Art. 6 Rn 195, 196;* Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 39.*
[699] Krügel, *MMR 2017, 795 (799).*
[700] Jorzig/Sarangi, *Digitalisierung im Gesundheitswesen, S. 85.*

(3) Art. 14 I und Art. 16 I NIS-RL

Laut Art. 14 I und Art. 16 I der NIS-RL müssen „*die Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen*“. Ob eine Maßnahme geeignet ist, ist vom konkreten Einzelfall abhängig.[701] Jedoch richtet sich die Richtlinie nach Art. 27 NIS-RL nicht an die Betreibenden wesentlicher Dienste selbst, sondern an die Mitgliedsstaaten[702], die den innerstaatlichen Anbietern und Anbieterinnen technische und organisatorische Maßnahmen aufzuerlegen haben.[703] Sie fällt somit als mögliche rechtliche Verpflichtung i.S.d. Art. 6 I 1 lit. c DS-GVO weg.

(4) § 12 I TTDSG

Gemäß § 12 I TTDSG dürfen Verpflichtete i.S.d. TTDSG „*Verkehrsdaten der Endnutzer sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind, verarbeiten, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen*“, soweit dies erforderlich ist. „*Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Telekommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können*“. Da von § 12 I TTDSG allerdings keine Verarbeitung von Inhaltsdaten erfasst ist und diese für eine effektive Arbeit der Angriffserkennungssysteme ebenfalls analysiert werden müssen, kommt wie bereits bei den Ausführungen zur Rechtmäßigkeit des Einsatzes von Angriffserkennungssystemen nach dem TTDSG der § 12 I TTDSG auch nicht als rechtliche Verpflichtung i.S.d. Art. 6 I 1 lit. c DS-GVO für den konkreten Fall in Betracht.

(5) § 165 TKG neu

Laut § 165 I TKG neu sind Erbringende sowie Mitwirkende an TK-Diensten verpflichtet, „*angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen zum Schutz des Fernmeldegeheimnisses und gegen die Verletzung des Schutzes personenbezogener Daten*“. Konkretisiert wird diese Verpflichtung in Absatz 2, wonach Betreibende von öffentlichen Kommunikationsnetzen oder Erbringende öffentlich zugänglicher TK-Dienste „*bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische und*

[701] Krügel*, MMR 2017, 795 (799).*
[702] Forgó u. a.*, Rechtsgutachten zum Betrieb von IDS & Event Management-Systemen in Netzen der öffentlichen Verwaltung, S. 41.*
[703] Paal/Pauly*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 32 Rn 14.*

organisatorische Vorkehrungen und sonstige Maßnahmen zu treffen haben“. Die gilt zum einen „*zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch, sofern diese Störungen durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können*“ und zum anderen „*zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten*“. Als angemessen Maßnahme kommen hierfür nach Absatz 3 „*Systeme zur Angriffserkennung im Sinne des § 2 Absatz 9b des BSI-Gesetzes*“ in Betracht. Verpflichtend müssen diese bei erhöhtem Gefährdungspotential eingesetzt werden.

§ 165 TKG neu orientiert sich an der Legaldefinition des § 2 Abs. 9b des BSIG, wonach Angriffserkennungssysteme „*durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme*“ sind. „*Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten*“.

Da Krankenhäuser grundsätzlich unter den Begriff des TK-Diensteanbieters nach § 3 Nr. 1 TKG neu fallen können, kann Art. 6 I 1 lit. c DS-GVO i.V.m. § 165 TKG neu als Ermächtigungsgrundlage zur Rechtfertigung des Einsatzes von Angriffserkennungssystemen in Betracht kommen. Allerdings können nicht pauschal sämtliche Krankenhäuser unter den Begriff des TK-Diensteanbieters subsumiert werden. Dies hängt stark vom strukturellen Aufbau der Kommunikationsstrategie sowie der Unternehmensstruktur des jeweiligen Krankenhauses ab und von dem TK-Angebot, das den Patienten und Patientinnen, Besuchenden und Mitarbeitenden gemacht wird. Zudem liegt der Handlungsschwerpunkt eines Krankenhauses nicht in der Telekommunikation, sondern in der Gesundheitsversorgung. Fraglich ist, ob der Einsatz von Angriffserkennungssystemen in Krankenhäusern flächendeckend durch Art. 6 I 1 lit. c DS-GVO i.V.m. § 165 TKG neu gerechtfertigt werden kann oder ob diese Ermächtigungsgrundlage nur eine Rechtfertigung des Einsatzes solcher Systeme im Bereich von Telekommunikationsnetzen und -diensten darstellt. Hier stellt sich sodann die Frage, ob diese Elemente klar von den restlichen Datenströmen getrennt werden können bei der Analyse durch Angriffserkennungssysteme und ob es hierbei nicht zu Überschneidungen kommt.

Aufgrund der Unsicherheiten, die sich in der Praxis ergeben können, ist eine Rechtfertigung des Einsatzes von Angriffserkennungssystemen in Krankenhäusern nach Art. 6 I 1 lit. c DS-GVO i.V.m. § 165 TKG neu grundsätzlich denkbar, aber nicht empfehlenswert. Da gerade im Hinblick auf Verschlüsselungsangriffe und folgende Erpressungen die entscheidenden datenverarbeitenden Systeme nicht geschützt werden, ist diese Ermächtigung nicht praxisgerecht. Zudem können im Rahmen des Einsatzes von Angriffserkennungssystemen in Krankenhäusern auch besondere Kategorien personenbezogener Daten nach Art. 9 I DS-GVO verarbeitet werden. Dies würde eine weitere Rechtmäßigkeitsprüfung unter den verschärften Bedingungen des Art. 9 II DS-GVO bedeuten. Ob § 165 TKG neu auch nach den Maßstäben des Art. 9 II DS-

GVO als Ermächtigungsgrundlage zumindest für den Teilbereich der TK-Dienste eines Krankenhauses in Betracht kommt, wird im weiteren Verlauf der Arbeit geprüft.

(6) § 75c SGB V

Eine weitere Möglichkeit zur Rechtfertigung der Nutzung von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft könnte § 75c SGB V darstellen, der durch das Patientendaten-Schutz-Gesetz (PDSG) in das SGB V eingefügt wurde.[704] Er stellt eine Ergänzung des § 8a BSIG dar, da auch für Krankenhäuser unterhalb der KRITIS-Schwelle eine stetig wachsende Gefahr vor Angriffen auf die IT-Systeme besteht.[705]

Gemäß § 75c I SGB V sind Krankenhäuser ab dem 1. Januar 2022 dazu verpflichtet, „*nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind*“. Als angemessen i.S.d. § 75c I SGB V gelten Vorkehrungen, „*wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht*“. In Absatz 2 wird Krankenhäusern die Möglichkeit gegeben, die Verpflichtungen nach Absatz 1 durch die Anwendung von „*branchenspezifischen Sicherheitsstandards für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus*“ zu erfüllen. Die Eignung dieser Sicherheitsstandards muss allerdings vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a II BSIG festgestellt wurden sein. Ein solcher branchenspezifischer Sicherheitsstandard (B3S) stellt der B3S für medizinische Versorgung dar, der bereits vorgestellt wurde (*siehe II.C.1.a) BSIG und BSI-KritisV*). Dieser sieht in ANF-MN 106 und ANF-MN 107 die Implementierung von Angriffserkennungssystemen vor, stuft diese allerdings nicht als „Muss“-Vorkehrung, sondern lediglich als „Soll“-Vorkehrung ein.

Anders als bei § 8a BSIG gilt die Verpflichtung nicht nur für Krankenhäuser, die unter den Begriff der KRITIS fallen, sondern ausdrücklich nach Absatz 3 für sämtliche Krankenhäuser.

§ 75c I 1 SGB V ähnelt in seinem Wortlaut dem § 8a I 1 BSIG, erwähnt allerdings die Authentizität nicht. Zudem hat § 75c SGB V im Gegensatz zu § 8a I 1 BSIG nicht nur die Sicherung der Funktionsfähigkeit zum Ziel, sondern zudem auch die Sicherheit der verarbeiteten Patienten- und Patientinneninformationen.[706]

[704] Stoklas, *ZD-Aktuell 2020, 07308.*
[705] Dittrich, *GuP 2021, 165 (167).*
[706] Dittrich, *GuP 2021, 165 (169).*

Kritik wird derweil an der Platzierung des § 75c SGB V geäußert. So wird angemerkt, dass eine Änderung der KRITIS-Voraussetzungen bezogen auf die Schwellenwerte für Krankenhäuser einen ähnlichen rechtlichen Effekt gehabt hätte und thematisch eine bessere Verortung darstellen würde.[707]

Es ist allerdings festzustellen, dass § 75c SGB V trotz seiner Nähe zu § 8a BSIG Angriffserkennungssysteme als angemessene Vorkehrung nicht explizit vorschreibt. In § 8a Absatz 1a BSIG wird ab dem 1. Mai 2023 der Einsatz von Angriffserkennungssystemen ausdrücklich als Teil der in Absatz 1 Satz 1 aufgezählten Verpflichtungen umfasst. In § 75c SGB V, der § 8a BSIG in weiten Teilen ähnelt, werden Angriffserkennungssysteme nicht erwähnt, noch wird auf § 8a Absatz 1a BSIG verwiesen. Eine Schlussfolgerung hieraus kann sein, dass nach § 75c SGB V der Einsatz von Angriffserkennungssystemen nicht in jedem Fall eine angemessene organisatorische und technische Vorkehrung ist, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich ist. Dies würde eine Einzelfallprüfung für jedes Krankenhaus bedeuten. Damit kann § 75c SGB V i.V.m. Art. 6 I 1 lit.c DS-GVO keine einheitliche Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft darstellen.

Grundsätzlich ist der Einsatz von IDS und SIEM-Systemen zur Erkennung und Abwehr von Gefahren für die IT-Sicherheit erforderlich.[708] Stellt man ins Verhältnis, welche weitreichenden Folgen die Ausfälle oder Beeinträchtigungen des Krankenhaussystems auf den Betrieb und die Versorgung der Patienten und Patientinnen hat, so ist der Aufwand des Betriebes von Angriffserkennungssystemen, der im Zweifel von externen IT-Dienstleistern oder Dienstleisterinnen übernommen werden kann und folglich nur einen finanziellen Aufwand bedarf, angemessen, gerade unter Hinzuziehung der besonderen Schutzwürdigkeit der Sicherheit der Patienten- und Patientinneninformationen. Zudem zählen IDS und SIEM-Systeme zum aktuellen Stand der Technik und stellen somit keine außerordentlichen Anforderungen an das Krankenhaus, die sich außerhalb der technischen Norm befinden.[709]

(a) Verstoß gegen den Grundsatz der Zweckbindung?

Die Rechtfertigung des Einsatzes von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft durch Art. 6 I 1 lit. c DS-GVO i.V.m. § 75c I SGB V könnte jedoch gegen den Grundsatz der Zweckbindung aus Art. 5 I lit. b DS-GVO verstoßen.

---

[707] Dittrich, *GuP 2021, 165 (171).*
[708] Niedersächsisches Ministerium für Inneres und Sport, *NDIG und OZG: Rechtsrahmen für die digitale Verwaltung in Niedersachsen.*
[709] Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 38.*

So sind die Grundsätze aus Art. 5 DS-GVO unmittelbar geltendes Recht und durchsetzbar. Sie richten sich an den Verantwortlichen oder die Verantwortliche, unabhängig davon, ob die datenverarbeitende Stelle hoheitlich oder nicht hoheitlich ist.[710] Ihre Erfüllung ist Grundbedingung jeder Datenverarbeitung. Das heißt, dass jede Datenverarbeitung diesen Grundsätzen zu jeder Phase der Verarbeitung genügen muss,[711] was sie mehr zu „Grundpflichten" als zu „Grundsätzen" der Datenverarbeitung macht.[712] Zwar ordnet Art. 5 DS-GVO selbst keine unmittelbare Rechtsfolge bei einem Verstoß an, gemäß Art. 83 V DS-GVO werden Verstöße gegen Art. 5 DS-GVO allerdings besonders scharf sanktioniert.[713]

Nach dem Grundsatz der Zweckbindung müssen personenbezogene Daten „*für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden*". Gemäß Erwägungsgrund 39 S. 6 der DS-GVO muss bei der Erhebung von personenbezogenen Daten der Zweck der Datenverarbeitung bereits festgelegt sein. Die Zulässigkeit der gesamten Datenverarbeitung ist an den festgelegten Zweck gebunden.[714] Dieser erstreckt sich auch auf Folgenutzer und -nutzerinnen, die die Daten von dem oder der Erstverantwortlichen übermittelt bekommen haben.[715] Erhalten die Folgenutzer und -nutzerinnen die Daten ohne, dass sie diese erheben müssen, setzt die Zweckbindung mit dem Speichern der Daten ein.[716] Die Zweckbindung erstreckt sich somit also grundsätzlich auch auf die Weiterverarbeitung der Daten.[717]

Angriffserkennungssysteme analysieren den Datenstrom der Netzwerke und Systeme, in denen sie eingesetzt werden. Sie verarbeiten hierbei auch personenbezogene Daten, erheben diese jedoch nicht. Angriffserkennungssysteme nutzen die Daten, die bereits erhoben wurden und dadurch in die Netzwerke oder Systeme gelangt sind. Diese werden, bezogen auf Krankenhäuser, hauptsächlich im Rahmen von Behandlungsverträgen mit den Patienten und Patientinnen, Arbeitsverträgen mit den Mitarbeitenden des Krankenhauses sowie Dienstleistungsverträgen mit Zulieferern und Zulieferinnen oder sonstigen Dienstleistern erhoben worden sein und entsprechenden Zweckbindungen unterliegen. Werden Angriffserkennungssysteme eingesetzt, stellt dies folglich eine Weiterverarbeitung der Daten dar, auf die sich die ursprüngliche Zweckbindung erstreckt. Es ist zu bezweifeln, dass für sämtliche Datenerhebungen im Arbeitsalltag eines Krankenhauses die Analyse dieser Daten durch Angriffserkennungssysteme im Zweck der Datenverarbeitung enthalten ist. Auch wenn dies zukünftig für kommende Datenerhebungen geschieht, kann dies keine flächendeckende rechtliche Absicherung gewährleisten.

---

[710] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 23.*
[711] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 1.*
[712] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 5 Rn 2.*
[713] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 5 Rn 1;* Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 4.*
[714] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 92.*
[715] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 5 Rn 93.*
[716] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 16.*
[717] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 29.*

(b) Kompatibilität der Primär- und Sekundärzwecke

Eine Weiterverarbeitung der Daten zu Zwecken, die nicht identisch mit dem ursprünglichen Zweck sind, ist jedoch unter der in Art. 5 I lit. b DS-GVO aufgeführte Bedingung, dass diese „*nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise"* weiterverarbeitet werden, möglich.[718] Der Primärzweck bildet hierbei den Maßstab zur Beurteilung der Vereinbarkeit der Weiterverarbeitung.[719]

Eine Konkretisierung dieser Regelung stellt Art. 6 IV DS-GVO dar. Hiernach dürfen bei dem Verantwortlichen gespeicherte Daten, wie bereits in Art. 5 I lit. b DS-GVO normiert, weiterverarbeitet werden, soweit der ursprüngliche Zweck der Verarbeitung mit dem neuen Zweck der Weiterverarbeitung vereinbar ist. Ist dies nicht der Fall, enthält Art. 6 IV DS-GVO eine Öffnungsklausel, wonach Daten auch zu einem inkompatiblen Zweck weiterverarbeitet werden dürfen, wenn die betroffene Person einwilligt oder eine Rechtsgrundlage im Unionsrecht oder im Recht der Mitgliedstaaten vorliegt.[720] Keine Rolle spielt hierbei, ob die Weiterverarbeitung durch denselben Verantwortlichen bzw. dieselbe Verantwortliche oder durch einen neuen Verantwortlichen oder eine neue Verantwortliche vorgenommen wird.[721]

Eine Definition der geforderten „Vereinbarkeit" erfolgt in der DS-GVO nicht. Die in Art. 6 IV DS-GVO angeführten Kompatibilitätskriterien sind nicht abschließend und können als Beispiele bei der Prüfung herangezogen werden.[722] Art. 6 IV DS-GVO enthält dementsprechend keinen Erlaubnistatbestand für eine Zweckänderung, sondern gibt die Kriterien für die Beurteilung der Zweckvereinbarkeit vor.[723] Bei der Prüfung der Vereinbarkeit mit dem ursprünglichen Zweck muss dessen Verarbeitungskontext mit einbezogen werden. Je spezifischer und restriktiver dieser war, desto enger sind die Grenzen einer Weiterverarbeitung. Hierbei sind nach Erwägungsgrund 50 S. 6 der DS-GVO „*die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen*" zu beachten. Erforderlich ist somit eine Gesamtbetrachtung aller verfügbaren Informationen, die auch aus der Perspektive eines oder einer objektiven Dritten geprüft werden sollte.[724] Gemäß Art. 6 IV lit. c DS-GVO gilt zudem ein gesteigerter Rechtfertigungszwang, wenn besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO verarbeitet werden.

---

[718] Ehmann/Selmayr*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 5 Rn 16.*
[719] Paal/Pauly*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 30.*
[720] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 203.*
[721] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 204.*
[722] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 204.*
[723] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 9.*
[724] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 206.*

Sollte im konkreten Fall der neue Zweck mit dem ursprünglichen Zweck vereinbar sein, so stellt sich die Frage, ob es überhaupt einer gesonderten Rechtsgrundlage i.S.d. Art. 6 I DS-GVO bedarf oder ob sich die Zulässigkeit des Einsatzes von Angriffserkennungssystemen auf die jeweilige ursprüngliche Rechtsgrundlage zur Erhebung und Verarbeitung der Daten stützen kann. Ob dies möglich ist, ist in der Literatur umstritten.

Dass keine gesonderte Rechtsgrundlage mehr benötigt wird, wird zuvorderst durch Erwägungsgrund 50 der DS-GVO begründet, der in Satz 2 besagt, dass für den Fall der Kompatibilität von ursprünglichem Zweck und neuem Zweck „*keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten*“ ist.[725] Kritiker und Kritikerinnen dieser Meinung führen hierbei an, dass es sich bei Satz 2 des Erwägungsgrundes 50 um ein „redaktionelles Versehen“ handeln muss. Dies ergebe sich aus der Entstehungsgeschichte der DS-GVO, in der der Gesetzgebungsprozess dadurch bestimmt war, dass „bei der Zweckänderung ein Zurück hinter den Schutzstandard der Richtlinie unter keinen Umständen in Betracht kam“.[726] Befürworter und Befürworterinnen argumentieren hingegen, dass gerade die Regelungen zur Zweckbindung überdurchschnittlich genau während der Entwicklungsphase bearbeitet wurden.[727] Ist die Zweckänderung mit dem ursprünglichen Zweck vereinbar, bedarf es keiner neuen Erlaubnis zur Verarbeitung, eine gegenteilige Forderung würde gegen den Sinn und Zweck des Konzepts der Zweckvereinbarkeit verstoßen.[728]

Würde keine gesonderte Rechtsgrundlage benötigt werden, würde dies jedoch häufig zu unstimmigen Ergebnissen führen, da Weiterverarbeitungen thematisch keine Berührungspunkte mit der ursprünglichen Verarbeitung und deren Ermächtigungsgrundlage nach Art. 6 I DS-GVO haben könnten. So könnten Weiterverarbeitung über vertragliche Verpflichtungen nach Art. 6 I lit. b DS-GVO gerechtfertigt sein, obwohl kein Vertragsverhältnis zwischen Weiterverarbeitendem und der betroffenen Person besteht. Zudem sind bestimmte Betroffenenrechte nur bei bestimmten Ermächtigungsgrundlagen einschlägig.[729] Außerdem ergeben sich Probleme mit der Einhaltung des Grundsatzes der Rechtmäßigkeit aus Art. 5 I DS-GVO. Dieser verlangt, dass die Datenverarbeitung zur Zweckerreichung erforderlich ist. Bei der Weiterverarbeitung ergibt sich die Erforderlichkeit allerdings aus einem anderen (neuen) Zweck, an dem diese zu messen ist. Die datenschutzrechtliche Erlaubnis bezieht sich allerdings auf die Erforderlichkeit des ursprünglichen Zwecks.[730] Zudem spricht die Regelungssystematik und der Wortlaut für die Notwendigkeit einer neuen Rechtmäßigkeitsprüfung. So stehen die Erlaubnistatbestände des Art. 6 I DS-GVO vor Art. 6 IV DS-GVO. Ferner ist gemäß Art. 6 I DS-GVO die

[725] Paal/Pauly*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 5 Rn 31.*
[726] Kühling/Buchner*, Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 6 Rn 182.*
[727] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 210.*
[728] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 11, 12.*
[729] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 211;* Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 13.*
[730] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 14.*

Verarbeitung personenbezogener Daten „*nur*“ rechtmäßig, wenn eine der Bedingungen des Absatz 1 erfüllt ist.[731]

Von einem Streitentscheid kann abgesehen werden, wenn der Zweck des Einsatzes von Angriffserkennungssystemen in Krankenhäusern nicht kompatibel mit dem ursprünglichen Erhebungszweck der genutzten Daten ist. Dies wird im Folgenden geprüft.

Eine erste Schwierigkeit bei der Prüfung, ob der Zweck für die Datenverarbeitung im Rahmen des Einsatzes von Angriffserkennungssystemen in Krankenhäusern kompatibel mit dem Zweck der Erhebung sämtlicher Daten im Krankenhausbetrieb ist, liegt in der unbekannten Vielzahl an Zwecken, zu denen die Daten erhoben werden. So werden im Krankenhausbetrieb zum Zwecke der Gesundheitsversorgung Daten erhoben, aber auch im Rahmen des Arbeitsverhältnisses zwischen Mitarbeitenden und Krankenhaus. Zudem gibt es Verträge mit Zulieferern bzw. Zulieferinnen und Dienstleistern bzw. Dienstleisterinnen diverser Branchen. Da Angriffserkennungssysteme sämtliche Daten ungefiltert analysieren, ist es nicht möglich pauschal eine Kompatibilität mit sämtlichen Ursprungszwecken der Datenerhebung anzunehmen. Grundsätzlich lässt sich jedoch sagen, dass die Zielrichtung eine wesentlich andere ist. Während im Krankenhaus personenbezogene Daten vordergründig zur Patientenversorgung sowie zur Erhaltung des laufenden Betriebs aufgenommen und verarbeitet werden, verfolgt der Einsatz von Angriffserkennungssystemen die Zielsetzungen der IT-Sicherheit. So werden beispielsweise SIEM-Systeme vordergründig zu Zwecken der Datensicherung und der Datenschutzkontrolle eingesetzt.[732] Durch die Analyse der Krankenhausinfrastruktur soll die Funktionsfähigkeit dieser gewährleistet werden und damit einhergehend die sensiblen Patienten- und Patientinneninformationen geschützt werden. Aufgrund der unterschiedlichen Schutzziele der Verarbeitungen kann keine Kompatibilität der hiermit verknüpften Verarbeitungszwecken gezogen werden.

(c) Weiterverarbeitung auf Grundlage einer mitgliedstaatlichen Regelung

Trotz der Inkompatibilität des Weiterverarbeitungszwecks und der ursprünglichen Verarbeitungszwecke, ist eine Weiterverarbeitung nach Art. 6 IV DS-GVO möglich, wenn diese auf einer Rechtsgrundlage der Union oder eines Mitgliedstaates beruht.[733] Die Einwilligung oder die gesetzliche Regelung bilden somit eine eigene Legitimationsgrundlage, die eine Vereinbarkeit mit dem ursprünglichen Zweck obsolet machen und über die Öffnungsklausel des Art. 6 IV DS-GVO neben den Regelungen der DS-GVO stehen können.[734] Diese Rechtsgrundlage begründet jedoch nicht den Erlaubnistatbestand der eigentlichen Weiterverarbeitung. Hierfür bedarf es nach wie vor einer Ermächtigungsgrundlage nach Art. 6 I DS-GVO.[735] Die

[731] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 6 Rn 183.*
[732] Kort, *NZA 2011, 1319 (1319).*
[733] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 215.*
[734] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 17, 18.*
[735] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 48.*

mitgliedstaatliche Rechtsgrundlage muss kein formelles Gesetz sein, es genügt jede „rechtsverbindliche allgemeine Regelung mit Außenwirkung".[736] Gemäß Erwägungsgrund 50 S. 5 der DS-GVO kann die Rechtsgrundlage, die beispielsweise nach Art. 6 III DS-GVO eine Rechtsgrundlage für die Datenverarbeitung beinhaltet, auch zur Erlaubnis der zulässigen Zweckänderung genutzt werden.[737] Die Möglichkeit zur gesetzlichen Regelung beschränkt sich hierbei nicht nur auf die Anwendungsbereiche der Art. 6 I 1 lit. c und e DS-GVO, sondern gilt für sämtliche Erlaubnistatbestände des Art. 6 I DS-GVO, was sich bereits aus der fehlenden Bezugnahme in Absatz 4 auf bestimmte Erlaubnistatbestände des Absatz 1 ergibt. Zudem schränkt Absatz 4 seine Reichweite durch den Verweis auf Art. 23 I DS-GVO ein. Allerdings erlangt Absatz 4 in seiner Gesamtheit nur da Bedeutung, wo bereits aus einem anderen Grund eine eigene Regelungskompetenz angeordnet wurde, wie beispielsweise in Art. 6 I 1 lit. c und e DS-GVO.[738] Liegen sämtliche der Voraussetzungen vor, darf der Verantwortliche nach Erwägungsgrund 50 S. 7 der DS-GVO „*die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten*".

Gemäß Art. 6 IV DS-GVO muss die gesetzliche Regelung eine „*notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellen*". Art. 23 I DS-GVO stellt ebenfalls eine Öffnungsklausel zur Einschränkung der Verarbeitungsgrundsätze dar und wirkt in diesem Fall gemeinsam mit Art. 6 IV DS-GVO.[739] Gemäß Art. 23 I DS-GVO darf eine Gesetzgebungsmaßnahme die Regelungen der DS-GVO beschränken, „*sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt*". Welche Ziele die Maßnahme schützen soll, werden ebenfalls in Art. 23 I DS-GVO genannt.

Der Einsatz von Angriffserkennungssystemen in Krankenhäusern und die damit einhergehende Verarbeitung personenbezogener Daten könnte dem Ziel der sonstigen wichtigen Ziele des allgemeinen öffentlichen Interesses im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit nach Art. 23 I lit. e DS-GVO unterfallen. Die Datenverarbeitung selbst muss hierbei nicht zwingend dazu dienen, das öffentliche Interesse zu verwirklichen, weshalb der oder die Verantwortliche für diese Datenverarbeitung nicht notwendigerweise hoheitliche Befugnisse ausüben muss.[740]

Machen die Mitgliedstaaten von der Öffnungsklausel des Art. 23 I DS-GVO Gebrauch, so dürfen die Beschränkungen der Rechte der betroffenen Personen um das notwendige, verhältnismäßige Mindestmaß zur Wahrung des Verarbeitungszweckes nicht hinausgehen. Dies schließt pauschale Ausnahmen aus. Zudem sind hierdurch erlassene deutsche Rechtsvorschriften an den

[736] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 24.*
[737] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 25.*
[738] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 19.*
[739] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 26.*
[740] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 23 Rn 23.*

Vorgaben des deutschen Verfassungsrechts zu messen.[741] So hat der EuGH in der „Schrems"-Entscheidung eine anlasslose Massenüberwachung als unverhältnismäßig in Bezug auf das Grundrecht zur Achtung des Privatlebens erachtet.[742] Bezogen auf die flächendeckende Überwachung der Krankenhausinfrastruktur durch den Einsatz von Angriffserkennungssystemen ist somit eine genaue Abgrenzung und Begrenzung der Verpflichtungen und des Verarbeitungsrahmens nötig, um eine verhältnismäßige Beschränkung der Betroffenenrechte zu erreichen.

Mit **§§ 23 und 24 BDSG** hat der deutsche Gesetzgeber von der Öffnungsklausel des Art. 6 IV Gebrauch gemacht. Während § 23 BDSG die „*Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung*" regelt, befasst § 24 BDSG sich mit der „*Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nichtöffentliche Stellen*". Da Krankenhäuser in privater Trägerschaft keine öffentlichen Stellen darstellen, fallen diese unter den Anwendungsbereich des § 24 BDSG. Hiernacht ist die Weiterverarbeitung zu einem anderen Zweck zulässig, „*wenn sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen*". Da im Verhältnis zwischen Privaten die Grundrechte und somit der Grundsatz der Verhältnismäßigkeit nicht direkt greift, fordert § 24 I BDSG eine Abwägungsentscheidung.[743]

Die Legitimation des § 24 BDSG ist jedoch höchst umstritten. So sehen Stimmen in der Literatur bereits in Art. 6 IV DS-GVO keine Öffnungsklausel, da dort lediglich Anforderungen normiert würden.[744] § 24 I Nr. 1 BDSG könnte seine Legitimation jedoch durch die Öffnungsklausel aus Art. 6 I 1 lit. e i.V.m. Art. 6 II, III DS-GVO erreichen, da der Verarbeitungszweck der Norm im öffentlichen Interesse liege und nach Art. 6 I 1 lit. e DS-GVO die Verarbeitung auch nicht-öffentliche Stellen umfasse, wenn diese im öffentlichen Interesse liegen. Hiernach sei § 24 I Nr. 1 BDSG zulässig und ist mit dem Unionsrecht vereinbar.[745] Im Unterschied hierzu gäbe es für § 24 I Nr. 2 BDSG jedoch keine Öffnungsklausel in der DS-GVO, weswegen § 24 I Nr. 2 BDSG nicht mehr dem Unionsrecht vereinbar sei und folglich nicht angewendet werden könne.[746] Andere Stimmen sehen den gesamten Absatz 1 des § 24 BDSG für unionsrechtswidrig, da der deutsche Gesetzgeber keine Kompetenz besäße, um die Datenverarbeitung privater Verantwortlicher zu regeln.[747] Gegenmeinungen hingegen sehen in der unionsrechtlichen Vereinbarkeit keine Probleme und sehen zudem sogar die Möglichkeit, dass der nationale

[741] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 23 Rn 4.*
[742] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 23 Rn 17.*
[743] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar BDSG § 24 Rn 4.*
[744] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar BDSG § 24 Rn 10.*
[745] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar BDSG § 24 Rn 10.*
[746] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar BDSG § 24 Rn 13.*
[747] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 29.*

Gesetzgeber weitere Regelungen zur Weiterverarbeitung durch nicht-öffentliche Stellen neben § 24 BDSG unter den Vorgaben des Art. 6 IV DS-GVO treffen darf.[748]

Eine Rechtfertigung der Zweckänderung bei der Weiterverarbeitung der Daten durch Art. 6 IV DS-GVO i.V.m. § 24 BDSG ist aufgrund der großen Rechtsunsicherheit bezüglich der Vereinbarkeit mit dem Unionsrecht folglich nicht empfehlenswert.

Eine weitere Rechtsgrundlage für die Zweckveränderung bei der Weiterverarbeitung der Daten beim Einsatz von Angriffserkennungssystemen in Krankenhäusern könnte **§ 67c SGB X** darstellen. Dessen unionsrechtliche Vereinbarkeit wird auf Art. 6 I 1 lit. c und e i.V.m. Art. 9 II lit. b bzw. h sowie j DS-GVO gestützt.[749]

§ 67c SGB X bezieht sich auf die Speicherung, Veränderung oder Nutzung von Sozialdaten durch die in § 35 SGB I genannten Stellen. In § 35 I SGB I werden diverse Stellen aufgeführt, die dem Sozialgeheimnis unterliegen. Gemäß Absatz 6 Nr. 1 zählen hierzu auch Verantwortliche oder deren Auftragsverarbeiter und -verarbeiterinnen, „*die Sozialdaten im Inland verarbeiten, sofern die Verarbeitung nicht im Rahmen einer Niederlassung in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erfolgt*“. Krankenhäuser dürften als Verarbeiter von Sozialdaten im Inland somit als „Stelle“ i.S.d. § 35 SGB I zu zählen sein, folglich ist § 67c SGB X anwendbar.

§ 67c II Nr. 1 SGB X bestimmt, dass die nach Absatz 1 gespeicherten Daten „*von demselben Verantwortlichen für andere Zwecke nur gespeichert, verändert oder genutzt werden*“ dürfen, wenn „*die Daten für die Erfüllung von Aufgaben nach anderen Rechtsvorschriften dieses Gesetzbuches als diejenigen, für die sie erhoben wurden, erforderlich sind*“. Eine solche Aufgabe nach einer anderen Rechtsvorschrift könnte § 75c SGB V darstellen. Zur Erinnerung: Gemäß § 75c I SGB V sind Krankenhäuser ab dem 1. Januar 2022 dazu verpflichtet, „*nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind*“. Um dieser Aufgabe nachzukommen, müssen Daten verarbeitet werden, die bereits nach anderen Rechtsvorschriften erhoben wurden. Der oder die Verantwortliche bleibt hierbei gleich, da der oder die Betreibende eines Krankenhauses der oder die Verantwortliche sämtlicher datenschutzrechtlich relevanten Handlungen im Zusammenhang mit dem Betrieb des Krankenhauses ist und sich dies auch nicht durch Auftragsverarbeitung ändert. Dass sich das Krankenhaus in privater Trägerschaft befindet ist hierbei kein Problem, da § 75c SGB V dahingehend nicht unterscheidet, ebenso wenig wie § 67c SGB X.

[748] Gola, *Datenschutz-Grundverordnung Kommentar BDSG § 24 Rn 2.*
[749] Körner u. a., *Kasseler Kommentar Sozialversicherungsrecht SGB X § 67c Rn 11.*

Eine Zweckänderung bei der Weiterverarbeitung von bereits erhobenen Daten ist beim Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft demnach über § 67c II Nr. 1 SGB X i.V.m. § 75c I SGB V möglich. Die unionsrechtliche Zulässigkeit dieser Normen erfolgt über Art. 6 I 1 lit. c und e i.V.m. Art. 9 II lit. b bzw. h sowie j DS-GVO beziehungsweise Art. 6 IV DS-GVO, je nachdem, welche Meinung vertreten wird.

(d) Zusammenfassung

Art. 6 I 1 lit. c DS-GVO i.V.m. § 75c SGB V kommt somit grundsätzlich als Ermächtigungsgrundlage in Betracht. Die damit einhergehende Zweckänderung der Verarbeitung ist über die Regelungen der § 67c II Nr. 1 SGB X i.V.m. § 75c I SGB V zulässig, die aufgrund verschiedener Öffnungsklauseln neben der DS-GVO gültig sind.

Jedoch gilt auch hier, dass zusätzlich zu den Rechtfertigungsgründen des Art. 6 I DS-GVO geprüft werden muss, ob bei dem Einsatz von Angriffserkennungssystemen besondere Kategorien personenbezogener Daten nach Art. 9 I DS-GVO verarbeitet werden und, ob in diesem Fall ein Einsatz von Angriffserkennungssystemen auch nach Art. 9 II DS-GVO gerechtfertigt wäre.

(7) §§ 330 I 1, 331 III, IV SGB V

Eine weitere Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern könnte Art. 6 I 1 lit. c DS-GVO i.V.m. §§ 330 I 1, 331 III, IV SGB V darstellen. Die Vorschriften wurden im Rahmen des Patientendaten-Schutz-Gesetz (PDSG) erlassen und sind zum 20. Oktober 2020 in Kraft getreten.[750] §§ 330 I 1, 331 III, IV SGB V sind Teil des Elften Kapitels des SGB V, welches die Regelungen zur Telematikinfrastruktur beinhaltet. Bevor auf die mögliche Ermächtigungsgrundlage genauer eingegangen wird, wird zunächst der Begriff der Telematikinfrastruktur erläutert. Anschließend wird geprüft, ob Krankenhäuser grundsätzlich zu den Gesellschaftern der Gesellschaft der Telematik zu subsumieren sind und wer im konkreten Anwendungsfall datenschutzrechtlicher Verantwortlicher oder Verantwortliche ist. Diese Erkenntnisse werden auf die Tatbestandsvoraussetzungen der Ermächtigungsgrundlage angewandt und es wird abschließend geprüft, ob §§ 330 I 1, 331 III, IV SGB V im konkreten Fall eine Ermächtigungsgrundlage i.V.m. Art. 6 I 1 lit. c DS-GVO darstellen kann.

(a) Die Telematikinfrastruktur

Als Teil des Digitalisierungsprozesses im Gesundheitswesen ist mit dem Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) die Einführung der sogenannten Telematikinfrastruktur beschlossen wurden. Dazugehörige

[750] Körner u. a., *Kasseler Kommentar Sozialversicherungsrecht SGB V § 330 Rn 1.*

Regelungen, wie beispielsweise zum Datenschutz und zur Datensicherheit innerhalb dieser Infrastruktur, sind seitdem durch verschiedene gesetzliche Maßnahmen, zum Beispiel dem Terminservice- und Versorgungsgesetz (TSVG), dem Gesetz für mehr Sicherheit in der Arzneimittelversorgung (GSAV), dem Digitale-Versorgung-Gesetz (DVG) oder dem Patientendaten-Schutz-Gesetz (PDSG) sowie dem im Juni 2021 in Kraft tretenden Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) erlassen wurden.

Eine Legaldefinition der Telematikinfrastruktur findet sich in **§ 306 SGB V**. Hiernach ist laut Absatz 1 die Telematikinfrastruktur „*die interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur, die der Vernetzung von Leistungserbringern, Kostenträgern, Versicherten und weiteren Akteuren des Gesundheitswesens sowie der Rehabilitation und der Pflege dient*". Zu den Spitzenorganisationen, die Teil der Schaffung der Telematikinfrastruktur sind, gehört gemäß § 306 I 1 SGB V auch die Deutsche Krankenhausgesellschaft.

Im Referentenentwurf des PDSG wird die Telematikinfrastruktur als „Datenautobahn des Gesundheitswesens" betitelt. Durch die umfassende Vernetzung soll eine sicherere, schnellere und übergreifende Kommunikation zwischen den diversen Akteuren und Akteurinnen des Gesundheitswesens geschaffen werden.[751]

Gemäß § 306 II SGB V besteht die Telematikinfrastruktur aus der dezentralen und zentralen Infrastruktur sowie einer Anwendungsinfrastruktur. Die dezentrale Infrastruktur umfasst beispielsweise die elektronische Gesundheitskarte, die Konnektoren und die E-Health-Kartenterminals zum Lesen der Karten und Ausweise. Diese ermöglicht den Nutzern und Nutzerinnen einen Zugang zur zentralen Infrastruktur. Diese beinhalten die zentralen Dienste. Durch VPN-Zugangsdienste gelangen die Nutzer und Nutzerinnen an das geschlossene Netz, welches beispielsweise Verzeichnis- und Identifikationsdienste enthält. Zudem gehört zur Telematikinfrastruktur die Anwendungsinfrastruktur mit Anwendungen im Rahmen der digitalen Gesundheitsversorgung. Hierzu gehören laut Referentenentwurf unter anderem „die elektronische Patientenakte, die elektronische Verordnung, der elektronische Organspendeausweis, Hinweise zu Vorsorgevollmachten oder Patientenverfügungen, die elektronischen Notfalldaten und der elektronische Medikationsplan".[752]

§ 306 III SGB V regelt die Anforderungen an die Datensicherheit. So soll ein besonders hohes Schutzniveau durch „*entsprechende technische und organisatorische Maßnahmen im Sinne des Artikels 32 DS-GVO*" erreicht werden. Auf die Nennung konkreter Vorgaben wird mit dem Ziel der „technikneutralen Gesetzgebung" hierbei verzichtet. Die Festlegung von erforderlichen technischen und organisatorischen Maßnahmen ist vielmehr gesetzlicher Auftrag der Gesellschaft für Telematik. Die dabei einzuhaltenden Ziele sind laut Gesetzesentwurf die

[751] Bundesministerium für Gesundheit, *Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, S. 83.*
[752] Bundesministerium für Gesundheit, *Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, S. 104.*

„Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit“.[753]

§ 310 SGB V regelt die Organisationsstruktur der Gesellschaft für Telematik und legt den Gesellschafterkreis sowie deren Geschäftsanteile fest.[754] Angaben zur Rechtsform der Gesellschaft werden hierbei nicht getätigt. Die Gesellschaft besteht seit dem 11. Januar 2005 als juristische Person des Privatrechts in der Rechtsform der GmbH. Zunächst als „Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH“ firmiert, trägt sie seit dem 02. Oktober 2019 den Firmennamen „gematik GmbH“.[755] Trotz ihrer privatrechtlichen Rechtsform ist die gematik GmbH gemeinnützig i.S.d. AO (BT-Drs. 15/4924, 9), weil sie mit qualifizierter Mehrheit sozialversicherungsrechtlich verbindliche Entscheidungen treffen kann. Somit kann die gematik GmbH Verwaltungsakte und Allgemeinverfügungen erlassen sowie öffentlich-rechtliche Verträge abschließen.[756]

Gemäß § 310 I SGB V sind die „*Bundesrepublik Deutschland, vertreten durch das Bundesministerium für Gesundheit, und die in § 306 Absatz 1 Satz 1 genannten Spitzenorganisationen Gesellschafter der Gesellschaft für Telematik*“. Gemäß Absatz 2 hält die Bundesrepublik Deutschland die Mehrheitsanteile der Gesellschaft. Die restlichen Gesellschaftsanteile entfallen je zur Hälfte auf die Leistungserbringer und die Kostenträger des deutschen Gesundheitswesens.[757]

Die Telematikinfrastruktur ist derzeit im Aufbau. So muss die elektronische Patientenakte (ePA) seit Januar 2021 von den gesetzlichen Krankenkassen angeboten werden und seit Juli 2021 besteht ein Anspruch der Patienten und Patientinnen auf Befüllung der ePA durch ihren Arzt oder ihre Ärztin. Seit Oktober 2021 wird die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) eingeführt, die zunächst nur den Versand an die Krankenkassen betrifft und ab 2022 auch die Weiterleitung an den Arbeitgebenden. Zudem können Ärzte und Ärztinnen seit Oktober 2021 direkt über die Telematikinfrastruktur die elektronischen Arztbriefe (eArztbriefe) versenden und empfangen und zudem wird der elektronische Medikationsplan (eMP) in der Telematikinfrastruktur gespeichert. Sämtliche Ärzte und Ärztinnen sowie Apotheker und Apothekerinnen sind zur Aktualisierung verpflichtet. Ab Januar 2022 kommt zudem das elektronische Rezept (eRezept), das Notfalldatenmanagement (NFDM) und das Versichertenstammdatenmanagement (VSDM) verpflichtend.[758]

---

[753] Rolfs u. a., *BeckOK Sozialrecht SGB V § 306 Rn 8.*
[754] Rolfs u. a., *BeckOK Sozialrecht SGB V § 310 Rn 1.*
[755] Körner u. a., *Kasseler Kommentar Sozialversicherungsrecht SGB V § 310 Rn 3-5;* Rolfs u. a., *BeckOK Sozialrecht SGB V§ 310 Rn 3.*
[756] Rolfs u. a., *BeckOK Sozialrecht SGB V § 310 Rn 6.*
[757] Körner u. a., *Kasseler Kommentar Sozialversicherungsrecht SGB V § 310 Rn 7.*
[758] Kassenärztliche Bundesvereinigung, *Anwendungen Digitale Praxis.*

(b) Krankenhäuser als Gesellschafter der Gesellschaft der Telematik

Gemäß § 306 I SGB V gehört die Deutsche Krankenhausgesellschaft zu den Leistungserbringern, die nach § 310 II Nr. 3 SGB V 24,5 Prozent der Anteile der Gesellschaft der Telematik halten.

Laut § 341 VII SGB V sind Krankenhäuser verpflichtet, „*sich bis zum 1. Januar 2021 mit den für den Zugriff auf die elektronische Patientenakte erforderlichen Komponenten und Diensten auszustatten und sich an die Telematikinfrastruktur nach § 306 anzuschließen*". Kommen Krankenhäuser dieser Verpflichtung nicht nach, sind ab dem 01. Januar 2022 Sanktionierungen nach § 5 IIIe 1 KHEntgG möglich.

Ob sich bereits sämtliche Krankenhäuser der Telematikinfrastruktur angeschlossen haben, ist nicht bekannt. Die Verlängerung des Übergangszeitraumes von ehemals Ende 2020 auf Ende 2021 lässt jedoch darauf schließen, dass der Anschluss der Krankenhäuser an die Telematikinfrastruktur schleppend verlief. Es kann jedoch davon ausgegangen werden, dass in naher Zukunft sämtliche Krankenhäuser der Telematikinfrastruktur beitreten. Der Anschluss an die Telematikinfrastruktur macht Krankenhäuser allerdings nicht zu Gesellschaftern. Hierzu müssten sie Mitglied der Deutschen Krankenhausgesellschaft (DKG) sein, die gemäß § 306 I SGB V zu den Gesellschaftern der Gesellschaft für Telematik gehört. Laut Angaben der DKG vertritt diese 16 Landesverbände und 12 Spitzenverbände und vertritt die „gesamte Breite der Krankenhausinteressen". Sie ist der Dachverband der Krankenhausträger und vertritt die Krankenhäuser bei sämtlichen gesundheitspolitischen Entscheidungen.[759] Es kann davon ausgegangen werden, dass zumindest ein Großteil der deutschen Krankenhäuser über die Landesverbände zu den Mitgliedern der DKG gehören, die wiederrum Gesellschafterin der Gesellschaft für Telematik ist.

(c) Der verantwortliche Anbieter

§ 307 SGB V legt die datenschutzrechtliche Verantwortlichkeit fest. So liegt nach Absatz 1 bei der Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur nach § 306 II Nr. 1 SGB V die Verantwortung bei denjenigen, die „*diese Komponenten für die Zwecke der Authentifizierung und elektronischen Signatur sowie zur Verschlüsselung, Entschlüsselung und sicheren Verarbeitung von Daten in der zentralen Infrastruktur nutzen, soweit sie über die Mittel der Datenverarbeitung mitentscheiden*". Die Verantwortung für den „*Betrieb der durch die Gesellschaft für Telematik spezifizierten und zugelassenen Zugangsdienste nach § 306 II Nr. 2 a SGB V*" liegt nach Absatz 2 bei dem jeweiligen Anbieter des Zugangsdienstes. Gemäß Absatz 3 ist der Anbieter eines gesicherten Netzes innerhalb des gesicherten Netzes „*verantwortlich für die Übertragung von personenbezogenen Daten,*

[759] DKG*, Aufgaben und Ziele.*

insbesondere von Gesundheitsdaten der Versicherten, zwischen Leistungserbringern, Kostenträgern sowie Versicherten und für die Übertragung im Rahmen der Anwendungen der elektronischen Gesundheitskarte". Bezogen auf die Anwendungsinfrastruktur ist der jeweilige Anbieter nach Absatz 4 verantwortlich. Absatz 5 formuliert einen Auffangtatbestand, der die Gesellschaft für Telematik als Verantwortliche für die Verarbeitung personenbezogener Daten in der Telematikinfrastruktur benennt, soweit „*keine Verantwortlichkeit nach den vorstehenden Absätzen begründet ist*".

Datenschutzrechtliche Einschränkungen erfahren Anbieter der Zugangsdienste nach Absatz 2, die gemäß Satz 2 personenbezogene Daten der Versicherten zweckgebunden nur für den Aufbau und den Betrieb des Zugangsdienstes verarbeiten dürfen. Anbieter gesicherter Netze dürfen nach Absatz 3 Satz 2 personenbezogene Daten nur zum Zwecke der Datenübertragung verarbeiten.

Fraglich ist, ob der aufgefächerte Begriff des Verantwortlichen mit dem Verständnis des datenschutzrechtlichen Verantwortlichen nach der DS-GVO vereinbar ist. Nach Art. 4 Nr. 7 DS-GVO ist datenschutzrechtlicher Verantwortlicher „*die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet*". Wer die Entscheidungsgewalt über Zweck und Mittel der Datenverarbeitung hat, ist der Adressat bzw. die Adressatin der datenschutzrechtlichen Pflichten. Dies gilt auch für die Datenverarbeitung, so lange der oder die Verarbeitende weisungsgebunden gegenüber dem oder der Verantwortlichen ist. Gemäß Art. 4 Nr. 7 HS 2 DS-GVO kann durch Unionsrecht oder das Recht der Mitgliedstaaten jedoch ein Verantwortlicher oder eine Verantwortliche bestimmt werden, wenn Zweck und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben sind. Von dieser Öffnungsklausel wurde in § 307 SGB V Gebrauch gemacht, um den verschiedenen Rollen der Beteiligten bei den arbeitsteiligen Datenverarbeitungsprozessen innerhalb der Telematikinfrastruktur gerecht zu werden.[760]

Auf den Einsatz von Angriffserkennungssystemen in Krankenhäusern bezogen, wird die hierfür nötige Datenverarbeitung als Datenverarbeitung im gesicherten Netz i.S.d. § 306 II Nr 2 b SGB V zu subsumieren sein, da die Angriffserkennungssysteme im gesicherten Netz des jeweiligen Krankenhauses installiert werden und dort sämtliche Datenströme analysieren, also verarbeiten. Gemäß § 307 III SGB V ist der oder die Betreibende des gesicherten Netzes alleinverantwortlich. Der oder die Betreibende ist im vorliegenden Fall das Krankenhaus in privater Trägerschaft. In der Begründung zum Gesetzesentwurf des PDSG wird nochmals klargestellt, dass die Gesellschaft für Telematik weder Anbieter des gesicherten Netzes ist, noch die Betreibenden der gesicherten Netze Auftragsverarbeiter der Gesellschaft für Telematik darstellen.[761]

---

[760] Bundesministerium für Gesundheit, *Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, S. 100.*

[761] Bundesministerium für Gesundheit, *Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, S. 101.*

Krankenhäuser sind somit verantwortliche Anbieter nach § 307 III SGB V. Sollten diese im Innenverhältnis den Einsatz von Angriffserkennungssysteme an externe IT-Dienstleister oder -Dienstleisterinnen delegieren, ändert dies nichts an der datenschutzrechtlichen Verantwortlichkeit, da diese Auftragsverarbeiter und -verarbeiterinnen i.S.d. Art. 4 Nr. 8 DS-GVO darstellen.

(d) Rechtfertigung nach §§ 330 I 1, 331 III, IV SGB V

Gemäß **§ 330 I 1 SGB V** sind die Gesellschaft für Telematik sowie verantwortliche Anbieter und Anbieterinnen verpflichtet, „*angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der Telematikinfrastruktur zu treffen und fortlaufend zu aktualisieren*“. Angemessen ist eine Vorkehrung nach § 330 I 3 SGB V, „*wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der Telematikinfrastruktur insgesamt oder von solchen Diensten der Telematikinfrastruktur steht, die durch Störungen verursacht werden können*“. Prozesse i.S.d. § 330 I 1 SGB V sind „Verfahren zum Austausch von Daten in der Telematikinfrastruktur, z.B. zwischen Komponenten oder Systemen“.[762] Wie schon bereits §75c SGB V, orientiert sich auch § 330 SGB V an § 8a I BSIG.[763]

Vergleich man den Wortlaut des § 75c I mit § 330 I 1 SGB V, so sind die dort enthaltenen Verpflichtungen sehr ähnlich. Beide Paragraphen verpflichten zu angemessenen organisatorischen und technischen Vorkehrungen zur Gewährleistung der IT-Sicherheit und orientieren sich an § 8a I BSIG. Während in § 330 I 1 SGB V Krankenhäuser in privaten Trägerschaften nur indirekt über deren Gesellschafterstatus der Gesellschaft der Telematik beziehungsweise deren IT-Dienstleister als verantwortliche Anbieter verpflichtet werden, verpflichtet § 75c I SGB V die Krankenhäuser direkt und namentlich. § 75c I SGB V dürfte somit als lex specialis-Norm bei der Frage der Rechtmäßigkeit von Angriffserkennungssystemen in Krankenhäusern die Verpflichtung nach § 330 I 1 SGB V verdrängen.

§ 331 III SGB V konkretisiert die geforderten organisatorischen und technischen Vorkehrungen dergestalt, dass die in § 330 I 1 SGB V normierte Verpflichtung der Gesellschaft für Telematik „*auch den Einsatz von geeigneten Systemen zur Erkennung von Störungen und Angriffen*“ umfasst. Ein Grund, warum die Konkretisierung des § 330 I 1 SGB V in § 331 SGB V verortet wurde, ist aus dem Gesetzeskontext nicht ersichtlich. Auch in der Begründung zum Gesetzesentwurf ist keine Erklärung gegeben. § 331 III SGB V ähnelt § 8a Ia BSIG, der die

[762] Körner u. a., *Kasseler Kommentar Sozialversicherungsrecht SGB V § 330 Rn 3.*
[763] Bundesministerium für Gesundheit, *Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, S. 107.*

Verpflichtungen nach § 8a I BSIG ebenfalls in Bezug auf den Einsatz von Angriffserkennungssystemen konkretisiert.

Zudem erlaubt **§ 331 IV SGB V** der Gesellschaft für Telematik die Verarbeitung der „*für den Einsatz der Systeme nach Absatz 3 erforderlichen Daten*". Somit liegt für den Einsatz von Systemen nach § 331 III SGB V nicht nur eine rechtliche Verpflichtung nach § 330 I 1 SGB V, sondern ebenfalls eine Ermächtigung nach § 331 IV SGB V vor. In dieser Hinsicht unterscheiden sich §§ 330 I 1, 331 III, IV SGB V von § 75c I SGB V, da dort nur eine rechtliche Verpflichtung verortet ist. Aufgrund des oben dargestellten offenen Streites, welchen Rechtscharakter die in Art. 6 I 1 lit. c DS-GVO geforderte „*rechtliche Verpflichtung*" aufweisen muss, wird aufgrund des Ermächtigungselements sowie der Konkretisierung eine Prüfung der §§ 330 I 1, 331 III, IV SGB V trotz des allgemeineres Regelungsumfangs vorgenommen.

Auffällig ist, dass § 330 I 1 SGB V die Gesellschaft für Telematik sowie die verantwortlichen Anbieter und Anbieterinnen verpflichtet, die Konkretisierung nach § 331 III SGB V sowie die Ermächtigungsgrundlage des § 331 IV SGB V jedoch nur die Gesellschaft für Telematik adressieren und nicht die verantwortlichen Anbieter und Anbieterinnen. Auch hierzu ist in der Begründung zum Gesetzesentwurf keine Stellungnahme enthalten. Die unterschiedlichen Adressaten- und Adressatinnenkreise lassen die Schlussfolgerung zu, dass zwar verantwortliche Anbieter und Anbieterinnen verpflichtet sind, angemessene organisatorische und technische Vorkehrungen zur Gewährleistung der IT-Sicherheit zu treffen, damit aber nicht zwingend der Einsatz von Angriffserkennungssystemen erfasst ist und ihnen eine hierbei notwendige Verarbeitung von personenbezogenen Daten nicht durch § 331 IV SGB V erlaubt ist.

Wie bereits erörtern, sind Krankenhäuser Anbieter gesicherter Netze und somit verantwortliche Anbieter nach § 307 III SGB V. Der Einsatz von Angriffserkennungssystemen in den internen Netzwerken eines Krankenhauses fällt somit in den datenschutzrechtlichen Verantwortungsbereiches des jeweiligen Krankenhauses und nicht in die Verantwortung der Gesellschaft der Telematik. Da die Gesellschaft für Telematik ausdrücklich keine datenschutzrechtliche Verantwortung für Verarbeitungen nach § 307 I bis IV SGB V übernimmt, kommt im konkreten Fall nur die rechtliche Verpflichtung des § 330 I SGB V zum Tragen. Die Konkretisierung sowie die Verarbeitungserlaubnis nach § 331 III und IV SGB V finden keine Anwendung, da diese nur die Gesellschaft der Telematik ansprechen, nicht jedoch die verantwortlichen Anbieter und Anbieterinnen.

Da § 330 I SGB V alleinstehend hinter der lex specialis-Norm § 75c SGB V zurücktritt und § 75c SGB V – wie zuvor geprüft – grundsätzlich eine Rechtfertigung des Einsatzes von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft i.V.m. Art. 6 I 1 lit. C DS-GVO darstellen kann, ist eine Rechtfertigung weder nach Art. 6 I 1 lit. c DS-GVO i.V.m. §§ 330 I 1, 331 III, IV SGB V noch nach Art. 6 I 1 lit. c DS-GVO i.V.m. § 330 I 1 SGB V möglich.

(8) Zwischenergebnis

Als Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft kommt Art. 6 I 1 lit. c DS-GVO i.V.m. § 75c SGB V in Betracht. Da § 75c SGB V (ebenso wie die zuvor geprüften § 8a I 1 BSIG, Art. 14 I und Art. 16 I NIS-RL, § 165 I TKG neu und § 330 I SGB V) eine rechtliche Verpflichtung, spezifische organisatorische und technische Vorkehrungen zu treffen, darstellt und keine Erlaubnis der damit einhergehenden Datenverarbeitung beinhaltet, muss auf den Streit verwiesen werden, welche Anforderungen an die rechtliche Verpflichtung nach Art. 6 I 1 lit. c DS-GVO zu stellen sind (*siehe c) Die Erfüllung einer rechtlichen Verpflichtung nach Art. 6 I 1 lit. c DS-GVO*). Wie dort bereits ausgeführt, gibt es bisher keine herrschende Meinung in der Literatur. Je nach Standpunkt genügt § 75c SGB V den Anforderungen des Art. 6 I 1 lit. c DS-GVO oder eben nicht. Art. 6 I 1 lit.c DS-GVO i.V.m. § 75c SGB V kann deswegen erst als verlässliche Ermächtigungsgrundlage anerkannt werden, wenn ein Streitentscheid vorliegt.

Zusätzlich muss geprüft werden, ob bei dem Einsatz von Angriffserkennungssystemen besondere Kategorien personenbezogener Daten nach Art. 9 I DS-GVO verarbeitet werden. Dies hätte zur Folge, dass sich die Rechtmäßigkeit des Einsatzes nicht nur nach Art. 6 I DS-GVO, sondern auch nach den verschärften Voraussetzungen des Art. 9 II DS-GVO richtet.

d) Erforderlichkeit der Wahrnehmung der Aufgabe aufgrund des öffentlichen Interesses nach Art. 6 I 1 lit. e DS-GVO

Eine andere Möglichkeit der Rechtfertigung könnte Art. 6 I 1 lit. e DS-GVO darstellen. Hiernach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn diese „*für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde*“.

Ähnlich wie Art. 6 I 1 lit. c DS-GVO ist auch Art. 6 I 1 lit. e DS-GVO eine „Scharniernorm“, die nach Erwägungsgrund 45 S. 1 eine konkrete Rechtsgrundlage im Unionsrecht oder im Recht des betroffenen Mitgliedstaates fordert und alleine stehend keine Basis für eine Rechtfertigung für die Verarbeitung personenbezogener Daten stellen kann. Während bei Art. 6 I 1 lit. c DS-GVO ein klares Ge- oder Verbot vorliegen muss, genügen im Rahmen des Art. 6 I 1 lit. e DS-GVO jedoch bereits Ermächtigungsgrundlagen, bei denen der oder die Verantwortliche über das Tätigwerden im Rahmen der Norm selbst entscheiden kann.[764]

Var. 1 des Art. 6 I 1 lit. e DS-GVO ist sehr weit gefasst ist und erfährt eine Einschränkung erst durch die erforderliche Rechtsgrundlage. So liegt ein „öffentliches Interesse“ nach dem Maßstab der DS-GVO beispielsweise bei der „*Verarbeitung zu Zwecken der sozialen Sicherheit und*

[764] Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 46.*

der öffentlichen Gesundheit" (Art. 36 V DS-GVO) oder bei „*gesundheitlichen Zwecken, wie der öffentlichen Gesundheit oder der sozialen Sicherheit*" (Erwägungsgrund 45 S. 6) vor.[765] Für privatrechtlich organisierte Unternehmen kommt der Erlaubnistatbestand des Art. 6 I 1 lit. e DS-GVO nur in Betracht, wenn Aufgaben, die im öffentlichen Interesse liegen, an sie übertragen wurden.[766] So sieht Erwägungsgrund 45 in Satz 6 natürliche oder juristische Personen des Privatrechts explizit bei „*gesundheitlichen Zwecken, wie der öffentlichen Gesundheit oder der sozialen Sicherheit oder der Verwaltung von Leistungen der Gesundheitsfürsorge*" vor. Eine Verarbeitung personenbezogener Daten, die dem Streben nach Gewinn dient ist derweilen nicht über Art. 6 I 1 lit. e DS-GVO zu rechtfertigen. Hier ist Art. 6 I 1 lit. f DS-GVO einschlägig.[767]

Als mögliche nationale Rechtsgrundlagen käme hier ebenfalls **§ 8a BSIG, § 12 I TTDSG, § 165 I TKG neu** und **§ 75c SGB V** in Betracht. Da in den jeweiligen Normen jedoch klare Gebote formuliert wurden, fallen diese somit bereits unter die spezifischeren Bedingungen des Art. 6 I 1 lit. c DS-GVO, da dieser engere Voraussetzungen an die Rechtsgrundlage formuliert.

Ob Krankenhäuser in der Hand privater Trägerschaften eine Aufgabe des öffentlichen Interesses wahrnehmen und ob hierunter auch die Sicherung der internen Netzwerke durch den Einsatz von Angriffserkennungssystemen subsumiert werden kann, kann somit dahinstehen. Zudem stellt sich hier ebenfalls wieder die Frage, ob besonderen Kategorien der dort verarbeiteten personenbezogenen Daten vorliegen und eine weitere mögliche mitgliedstaatliche Rechtsgrundlage über die speziellere Scharniernorm des Art. 9 II lit. g DS-GVO gefunden werden muss.

e) Erforderlichkeit der Verarbeitung zur Wahrung der berechtigten Interessen des oder der Verantwortlichen oder eines Dritten nach Art. 6 I 1 lit. f DS-GVO

Letztlich ist in Art. 6 DS-GVO noch lit. f des ersten Absatzes auf seine Anwendbarkeit zu prüfen. Der Erlaubnistatbestand des Art. 6 I 1 lit. f DS-GVO ist neben der Einwilligung aus Art. 6 I 1 lit. a DS-GVO die praxisrelevanteste Rechtsgrundlage für die Verarbeitung personenbezogener Daten im privatrechtlichen Bereich.[768] Sein Verhältnis zu den anderen Erlaubnistatbeständen des Art. 6 I DS-GVO ist allerdings umstritten. Während einige Stimmen in der Literatur den Art. 6 I 1 lit. f DS-GVO als Auffangtatbestand betrachten[769], lehnen andere Meinungen dies mit der Begründung ab, dass Datenverarbeitungen, deren Zulässigkeit bereits abschließend festgelegt wurde (z.B. im Rahmen von Vertragserfüllungen), in ihrem Umfang nicht durch weitere Erlaubnistatbestände erweitert werden dürften. Die Interessenabwägung im Rahmen

---

[765] Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 39.*
[766] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 51;* Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis§ 2 Rn 33.*
[767] Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 39.*
[768] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 1 Rn 86.*
[769] Gola*, Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 13;* Laue/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis§ 2 Rn 37.*

des Art. 6 I 1 lit. f DS-GVO müsse in solchen Fällen dementsprechend enger ausgelegt werden.[770] Als einziger Erlaubnistatbestand des Art. 6 I DS-GVO wird in I 1 lit. f eine Interessenabwägung zwischen den gegensätzlichen Interessen von Verarbeitendem oder Verarbeitender und Betroffenem bzw. Betroffener vorgenommen.[771]

Laut Art. 6 I 1 lit. f DS-GVO ist eine Verarbeitung personenbezogener Daten rechtmäßig, wenn „*die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt*." Laut Erwägungsgrund 47 S. 1 sind hierbei „*die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen*". Gemäß S. 3 wird ein eher restriktiver Ansatz verfolgt, da „*das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen*" ist. Im Zweifelsfall müsse somit das Recht des oder der Betroffenen Vorzug genießen.[772] Was unter den Begriff des berechtigten Interesses fällt, wird in Art. 6 I 1 lit. f DS-GVO nicht näher definiert. Von Interessen, Grundrechten und Grundfreiheiten des oder der Betroffenen wird ausgegangen, ebenso von einem Zusammenhang zur Schutzerfordernis personenbezogener Daten. Zu den berechtigten Interessen zählen nicht nur rechtliche, sondern auch tatsächliche, wirtschaftliche oder ideelle Interessen.[773] Das bloße Streifen von Rechten der betroffenen Personen macht eine Datenverarbeitung nach Art. 6 I 1 lit. f DS-GVO nicht per se unrechtmäßig. Auch bei einem gleichwertigen Interesse beider Seiten darf eine Verarbeitung stattfinden.[774] Ein berechtigtes Interesse kann nur vorliegen, wenn die Verarbeitung der personenbezogenen Daten im konkreten Einzelfall erforderlich ist, es also keine ebenso effektive, aber weniger grundrechtseinschneidende Alternative gibt.[775] Auf der Interessenseite des oder der Betroffenen sind insbesondere die Grundrechte aus Art. 7 und 8 GRCh zu berücksichtigen.[776]

Im Laufe des Gesetzgebungsverfahrens wurde u.a. über die Formulierung eines Unterartikels diskutiert, der eine Datenverarbeitung rechtfertige, wenn diese für die IT-Sicherheit erforderlich sei. Der Vorschlag konnte sich zwar nicht durchsetzen, jedoch hat der Aspekt der IT-Sicherheit in Erwähnungsgrund 49 einen Platz gefunden.[777] Laut Erwägungsgrund 49 S. 1 stellt die Verarbeitung von personenbezogenen Daten zur Netz- und Informationssicherheit als überwiegendes berechtigtes Interesse „*in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist*". Gemäß Satz 2 des Erwägungsgrundes 49 könnte ein

[770] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 13.*
[771] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 6 Rn 59.*
[772] Albrecht/Jotzo, *Das neue Datenschutzrecht der EU Teil 3 Rn 51.*
[773] Kühling/Buchner, *Datenschutzgrundverordnung Kommentar Art. 6 Rn 146.*
[774] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 58.*
[775] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 1 Rn 100.*
[776] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 28.*
[777] Kühling/Buchner, *Datenschutzgrundverordnung Kommentar Art. 6 Rn 167.*

solches berechtigtes Interesse „*beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren*". Obwohl in Erwägungsgrund 49 nur von unbefugtem Zugang und nicht von unbefugten Zutritten oder Zugriffen gesprochen wird, ist anzunehmen, dass der Begriff Zugang hier als Oberbegriff steht und somit auch den Schutz vor unbefugtem Zutritt und Zugriff erfasst. Somit fallen auch Datenverarbeitungen in den Kreis des berechtigten Interesses des Erwägungsgrundes 49, die vor unbefugtem Zugriff oder Zutritt schützen sollen, wie beispielsweise Angriffserkennungssysteme.[778] IT-Sicherheit kann somit ein berechtigtes Interesse bei der Verarbeitung personenbezogener Daten darstellen. Dies macht die DS-GVO zudem in Art. 5 I lit. f, Art. 24 sowie Art. 32 deutlich. Entscheidend ist im Rahmen des Art. 6 I 1 lit. f DS-GVO aber vor allen Dingen die Frage, ob zur Wahrung der IT-Sicherheit die Verarbeitung personenbezogener Daten überhaupt erforderlich und verhältnismäßig ist.[779]

Erwägungsgrund 49 richtet sich an Behörden, Computer-Notdienste, Betreibende von elektronischen Kommunikationsnetzen und -diensten sowie Anbieter und Anbieterinnen von Sicherheitstechnologien und -diensten. Ob es sich hierbei um eine abschließende oder eine beispielhafte Aufzählung handelt, wird nicht deutlich gemacht. Gegen eine beispielhafte Aufzählung spricht das Fehlen eines Indikators wie „insbesondere". Jedoch bieten die aufgezählten Begriffe einen großen Interpretationsspielraum, weswegen von einer nicht abschließenden Aufzählung in Erwägungsgrund 49 ausgegangen werden kann.[780]

Aufgrund der in Art. 6 I 1 lit. f DS-GVO verlangten Interessen- und Grundrechtsabwägung, ist eine Verhältnismäßigkeitsprüfung für jeden Einzelfall erforderlich.[781] Zudem lässt die Flexibilität des Art. 6 I 1 lit. f DS-GVO, die mit dem Ausgleichsgebot zwischen den Rechten der betroffenen Personen und Dritter einhergeht, keine verlässliche Vorhersehbarkeit für den Verantwortlichen oder die Verantwortliche zu, was zu einem hohen Maß an Rechtsunsicherheit führt.[782] Des Weiteren gilt auch bei diesem Erlaubnistatbestand in Bezug auf die Verarbeitung von personenbezogenen Daten in Krankenhäusern, dass Daten, die unter den speziellen Tatbestand des Art. 9 DS-GVO fallen, nicht von Art. 6 I 1 lit. f DS-GVO alleine erfasst werden. Die Zulässigkeit der Verarbeitung bestimmt sich in solchen Fällen immer zudem nach den spezielleren Ausnahmetatbeständen des Art. 9 II DS-GVO.[783]

---

[778] Jandt/Steidle*, Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 327, 328.*
[779] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG Art. 6 Abs. 1 Rn 119;* Jandt/Steidle*, Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 306.*
[780] Jandt/Steidle*, Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG Rn 309.*
[781] Krügel*, MMR 2017, 795 (799).*
[782] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 1 Rn 86;* Brink/Wolff*, BeckOK Datenschutzrecht DS-GVO Art. 6 Rn 14.*
[783] Schneider*, Datenschutz nach der EU-Datenschutz-Grundverordnung, S. 133.*

Wegen der Einzelfallcharakteristik des Art. 6 I 1 lit. f DS-GVO kann dieser als verlässliche und beständige Rechtfertigungsnorm zur Nutzung von Angriffserkennungssystemen in privatrechtlich organisierten Krankenhäusern nicht genutzt werden. Hier ist zudem zu beachten, dass in den zu sichernden Netzwerken auch Daten verarbeitet werden, für die die Voraussetzungen des Art. 9 DS-GVO ebenfalls vorliegen müssen.

f) Zwischenergebnis

Während des Einsatzes von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft werden personenbezogene Daten verarbeitet. Eine Rechtfertigung dieser Verarbeitung kann allenfalls durch Art. 6 I 1 lit. c DS-GVO i.V.m. § 75c I SGB V erfolgen, der jedoch nach jetziger Rechtslage mit Rechtsunsicherheiten behaftet ist, da noch strittig ist, ob die Voraussetzungen des Art. 6 I 1 lit. c DS-GVO zur Gänze erfüllt sind. Werden im Rahmen des Einsatzes von Angriffserkennungssystemen in Krankenhäusern besondere Kategorien personenbezogener Daten nach Art. 9 I DS-GVO verarbeitet, ist eine Rechtfertigung der Nutzung dieser Systeme über Art. 6 I 1 lit. c DS-GVO i.V.m. § 75c I SGB V allein nicht möglich, da zusätzlich die spezielleren Voraussetzungen des Art. 9 II DS-GVO erfüllt sein müssen.

Ob besondere Kategorien personenbezogener Daten verarbeitet werden und ob es Rechtfertigung der Nutzung von Angriffserkennungssystemen auch nach Art. 9 DS-GVO vorliegt, wird im Folgenden geprüft.

3. Rechtmäßigkeit der Verarbeitung von Gesundheitsdaten nach Art. 9 DS-GVO

In Netzwerken von Krankenhäusern werden insbesondere besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO verarbeitet, wodurch dieser eine maßgebliche Bedeutung beim Einsatz von Angriffserkennungssystemen hat. Zwar gibt es laut BVerfG im Volkszählungsurteil „*unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr*" – was auch auf unionsrechtlicher Ebene durch Art. 8 GRCh festgehalten wurde – , dennoch gibt es laut DS-GVO bestimmte Arten von Daten, die eine besonders hohe Schutzbedürftigkeit aufweisen, wobei Art. 9 DS-GVO hierbei keine Unterscheidung zwischen einer Verarbeitung dieser Daten durch öffentliche oder nicht öffentliche Stellen macht.[784] Die Gründe für diese hohe Schutzbedürftigkeit der Datenkategorien liegen in ihrem höchstpersönlichen, identitätsstiftenden Charakter und dem damit einhergehenden erhöhten Diskriminierungsrisiko und Schadenspotenzial.[785] Praktisch spiegelt sich die Schutzintensivierung zudem in einer höheren Geldstrafe bei einem Verstoß gegen Art. 9 DS-GVO nach Art. 83 V DS-GVO wieder.[786]

[784] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 169.*
[785] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 15, 17.*
[786] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 1.*

Zwar verfolgt Art. 9 DS-GVO primär den Schutz des Grundrechts auf Datenschutz nach Art. 8 GRCh, jedoch werden durch die Intensivierung des Schutzes der Datenkategorien aus Art. 9 DS-GVO ebenfalls unter anderem Art. 7 (Privat- und Familienleben), Art. 1 (Würde des Menschen), Art. 10 (Gedanken-, Gewissens- und Religionsfreiheit), Art. 11 (Freiheit der Meinungsäußerung), Art. 12 (Versammlungsfreiheit), Art. 21 (Nichtdiskriminierung), Art. 22 (Vielfalt der Kulturen, Religionen und Sprachen) sowie Art. 27 und 28 GRCh (Rechte im Unternehmen, Tarifverträge) geschützt.[787]

Absatz 1 des Art. 9 DS-GVO stellt ein grundsätzliches Verarbeitungsverbot für die aufgeführten Datenkategorien auf. Ausnahmetatbestände hiervon führt Absatz 2 auf, die unter bestimmten Voraussetzungen eine Verarbeitung rechtfertigen können. Absatz 3 schafft eine weitere Verschärfung der Rahmenbedingungen für die rechtmäßige Verarbeitung von Daten im Gesundheitsbereich nach Art. 9 II lit. h DS-GVO und Absatz 4 gibt den Mitgliedstaaten die Möglichkeit eigener spezifischer Regelungen innerhalb des Schutzniveaus des Art. 9 DS-GVO.[788]

Im Folgenden wird Art. 9 im Verhältnis zu Art. 5 und 6 DS-GVO eingeordnet, bevor die relevanten Datenkategorien aus dem Katalog des Art. 9 I DS-GVO vorgestellt werden. Analog der Prüfung des Art. 6 I DS-GVO als Erlaubnisnorm für den Einsatz von Angriffserkennungssystemen werden auch hier die einschlägigen Ausnahmetatbestände des Art. 9 II DS-GVO vorgestellt und auf ihre Anwendbarkeit geprüft.

a) Verhältnis zu Art. 5 und 6 DS-GVO

Gemäß Erwägungsgrund 51 S. 5 der DS-GVO gelten bei der Anwendung eines der Ausnahmetatbestände des Art. 9 II DS-GVO zusätzlich „*die allgemeinen Grundsätze und andere Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung*“. Hiermit sind vor allem die Grundsätze des Art. 5 DS-GVO sowie die allgemeine Rechtmäßigkeit der Verarbeitung personenbezogener Daten aus Art. 6 I DS-GVO gemeint.[789] Eine Datenverarbeitung kann folglich rechtswidrig sein, obwohl sie einen Tatbestand des Art. 9 II DS-GVO verwirklicht, aber nicht auf eine der Grundlagen des Art. 6 I DS-GVO gestützt werden kann.[790]

[787] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 14, 16;* Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 9 Rn 1.*
[788] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 9 Rn 3;* Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 7;* Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 8.*
[789] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 5.*
[790] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 26.*

b) Datenkategorien

Art. 9 I DS-GVO beinhaltet einen abschließenden Katalog besonders geschützter Daten.[791] Diese sind namentlich „*Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person*“. Die Formulierung, dass diese Merkmale aus Daten „hervorgehen“, lässt darauf schließen, dass vom Schutzbereich des Art. 9 I DS-GVO nicht nur Daten umfasst sind, die direkt die Katalogmerkmale beschreiben, sondern auch Daten, die mittelbare Rückschlüsse auf diese Merkmale zulassen.[792] Die Platzierung der Formulierung „hervorgehen“ lässt zudem auf eine zweigliedrige Struktur schließen: Während bei Daten mit Merkmalen über „*die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit*“ aus abstrakten Bezugspunkten durch mittelbarer Interpretation hervorgehen, sieht der Gesetzgeber bei Daten mit Merkmalen über „*genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person*“ die Schutzbedürftigkeit bereits in ihrer Existenz begründet.[793]

Für die Fragestellung dieser Arbeit sind aus dem Katalog des Absatz 1 die genetischen Daten sowie die Gesundheitsdaten von Bedeutung, da diese in Netzwerken von Krankenhäusern verarbeitet werden und somit auch von dort installierten Angriffserkennungssystemen verarbeitet werden können.

Gemäß der Legaldefinition des Art. 4 Nr. 13 DS-GVO sind **genetische Daten** „*personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden*“. Erwägungsgrund 34 der DS-GVO ergänzt diese Definition noch diesbezüglich, dass diese Daten „*aus der Analyse einer biologischen Probe der betreffenden natürlichen Person, insbesondere durch eine Chromosomen, Desoxyribonukleinsäure (DNS)- oder Ribonukleinsäure (RNS)-Analyse oder der Analyse eines anderen Elements, durch die gleichwertige Informationen erlangt werden können, gewonnen werden.*“ Dies

[791] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 19.*
[792] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 9 Rn 6;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 11;* Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 22.*
[793] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 9 Rn 19;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 2.*

schließt reine äußere Merkmale, wie die Augen- oder Haarfarbe einer Person als genetische Daten i.S.d. DS-GVO aus.[794]

Der besondere Schutz von Gesundheitsdaten entspringt dem Grundrecht auf Leben und Gesundheit nach Art. 2, 3 GRCh sowie dem Recht auf Gesundheitsschutz nach Art. 35 GRCh.[795] **Daten über die Gesundheit** sind laut Art. 4 Nr. 15 DS-GVO „*personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen*". Hierzu gehören nach Erwägungsgrund 35 S. 1 „*Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person*". Als Gesundheitsdaten zählen laut Erwägungsgrund 35 S. 2 auch „*Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-Vitro-Diagnostikum stammen*." Zudem können „Bestands-, Verkehrs- wie auch Inhaltsdaten des Telekommunikationsverkehrs zwischen Betroffenen und Gesundheitseinrichtungen wie auch Kommunikationsinhalte generell" vom Begriff der Gesundheitsdaten umfasst sein.[796] Finanzdaten sowie Angaben über das Alter und das Geschlecht einer Person gelten hingegen nicht als Gesundheitsdaten.[797] Ferner können Gesundheitsdaten durch die Kombination diverser Daten entstehen, die einzeln betrachtet nicht in den Schutzbereich des Art. 9 I DS-GVO fallen.[798]

Da Angriffserkennungssysteme sämtliche Datenströme des zu schützenden Netzwerkes auf Angriffsmuster analysieren, werden in Netzwerken und Systemen von Krankenhäusern auch besondere Kategorien personenbezogener Daten nach Art. 9 I DS-GVO verarbeitet, insbesondere genetische Daten und Daten über die Gesundheit. Somit ist in Bezug auf die Prüfung der Rechtmäßigkeit des Einsatzes von Angriffserkennungssystemen in Krankenhäusern Art. 9 DS-GVO neben den allgemeinen Erlaubnistatbeständen des Art. 6 DS-GVO zu prüfen. Eine Rechtfertigungsnorm könnte sich in Art. 9 II, III DS-GVO finden.

---

[794] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 31;* Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 9 Rn 13.*
[795] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 34.*
[796] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 39.*
[797] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 15.*
[798] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 9 Rn 15;* Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 9 Rn 15.*

c) Die Ausnahmetatbestände des Art. 9 II, III DS-GVO

Absatz 2 des Art. 9 DS-GVO sieht abschließend Ausnahmen zu dem grundsätzlichen Verarbeitungsverbot aus Absatz 1 vor. Teilweise können diese Ausnahmen von den Mitgliedstaaten unter strengen Anforderungen selbst bestimmt werden.

Eine nationale Bestimmung in Bezug auf Art. 9 II lit. b, g und h DS-GVO findet sich in **§ 22 BDSG**. § 22 I BDSG ist eine allgemeine Erlaubnisnorm, die neben den Tatbestandsvoraussetzungen des Art. 9 II DS-GVO steht und als Generalklausel die Öffnungsklauseln des Art. 9 II DS-GVO auf nationaler Ebene abdeckt.[799] In § 22 II BDSG werden Sicherheitsanforderungen an die Verarbeitung der personenbezogenen Daten formuliert, die den Maßnahmenkatalog des Art. 32 DS-GVO ergänzen.[800]

Im Folgenden werden die Ausnahmetatbestände des Art. 9 II DS-GVO vorgestellt, nach denen eine Nutzung von Angriffserkennungssystemen in den Netzwerken privatrechtlich organisierter Krankenhäuser gerechtfertigt sein könnte.

(1) Die Einwilligung nach Art. 9 II lit. a DS-GVO

Laut Art. 9 II lit. a DS-GVO gilt das Verarbeitungsverbot des Absatzes 1 nicht, wenn die betroffene Person „*in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt*“. Die Einwilligung muss sich hierbei explizit auf die Verarbeitung der besonderen Daten nach Art. 9 I DS-GVO beziehen, sonst greift der allgemeinere Tatbestand des Art. 6 I lit. a DS-GVO. Die Wirksamkeitsvoraussetzungen des Art. 7 und 8 DS-GVO sind auf die Einwilligung nach Art. 9 II lit. a DS-GVO anwendbar.[801] Gerade in der digitalen Gesundheitswelt erlangt die Einwilligung eine große Bedeutung, da Betreibende von Gesundheits-Apps mit e-health Angeboten oftmals nicht der sonst geforderten Geheimhaltungspflicht unterliegen.[802]

Im Gegensatz zu Art. 6 I lit. a DS-GVO ist in Art. 9 II lit. a DS-GVO eine „*ausdrückliche*“ Einwilligung verlangt, was die Möglichkeit der konkludenten Einwilligung im Fall der Verarbeitung besonderer Kategorien personenbezogener Daten ausschließt.[803]

Ebenso wie nach Art. 6 I lit. a DS-GVO muss die Einwilligung in die Verarbeitung freiwillig erfolgen. Diese kann bei bestehendem Ungleichgewicht zwischen betroffener Person und Verarbeitendem oder Verarbeitender gefährdet sein. Im Gesundheitsbereich kommt zudem das

[799] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 25.*
[800] Dochow u. a., *Datenschutz in der ärztlichen Praxis, S. 175.*
[801] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 47, 53.*
[802] Dochow u. a., *Datenschutz in der ärztlichen Praxis, S. 63.*
[803] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 33.*

vordergründliche Interesse der medizinischen Behandlung hinzu, welches das Interesse an der informationellen Selbstbestimmung überlagern bzw. verdrängen kann.[804]

Da eine Einwilligung nach Art. 9 II lit. a DS-GVO nach Art. 7 III DS-GVO jederzeit widerrufen werden kann, kommt diese mit einer hohen Rechtsunsicherheit daher. Zudem ist die einzelne Einwilligungsabfrage mit einem entsprechenden Mehraufwand verbunden und die Freiwilligkeit ist unter dem Aspekt der eventuellen gesundheitlichen Notfallsituationen und dem daraus resultierenden Abhängigkeitsverhältnis der Patienten und Patientinnen zur medizinischen Versorgung im Krankenhaus fraglich und in Einzelfällen nicht gegeben. Eine beständige Rechtfertigung der Nutzung von Angriffserkennungssystemen in den Netzwerken privatrechtlich organisierter Krankenhäuser ist folglich nach Art. 9 II lit. a DS-GVO nicht möglich.

(2) Das erhebliche öffentliche Interesse nach Art. 9 II lit. g DS-GVO

Eine weitere Ausnahme des Verarbeitungsverbotes aus Absatz 1 liegt gem. Art. 9 II lit. g DS-GVO vor, wenn „*die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats {…} aus Gründen eines erheblichen öffentlichen Interesses erforderlich*“ ist. Die Rechtsgrundlage muss hierbei „*in angemessenem Verhältnis zu dem verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen*“. Art. 9 II lit. g DS-GVO ist folglich kein eigenständiger Erlaubnistatbestand, sondern eine sog. horizontale Öffnungsklausel.[805] Die geforderte Rechtsgrundlage muss laut Erwägungsgrund 41 der DS-GVO jedoch „*nicht notwendigerweise ein von einem Parlament angenommener Gesetzgebungsakt*“ sein. Es genügt, wenn die „*entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme klar und präzise und ihre Anwendung für die Rechtsunterworfenen gemäß der Rechtsprechung des Gerichtshofs der Europäischen Union und des Europäischen Gerichtshofs für Menschenrechte vorhersehbar“* ist.

Im Vergleich zum allgemeineren Pendant in Art. 6 I lit. e DS-GVO fordert Art. 9 II lit. g DS-GVO ein „*erhebliches*“ öffentliches Interesse und stellt somit deutlich höhere Anforderungen an die Rechtfertigung der Datenverarbeitung.[806] So führt Erwägungsgrund 46 der DS-GVO in Satz 3 beispielhaft die „*Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen*“ als Gründe des öffentlichen Interesses an. Entsprechend hoch liegt im Gefahrenabwehrrecht die Eingriffshürde. Erst bei einer Gefahr für konkret benannte, hochrangige und besonders schützenswerte Rechtsgüter der Allgemeinheit kann eine Maßnahme zur Gefahrabwehr

[804] Dochow u. a., *Datenschutz in der ärztlichen Praxis, S. 64.*
[805] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 30, 31.*
[806] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 69.*

über Art. 9 II lit. g DS-GVO i.V.m. einer entsprechenden national- oder unionsrechtlichen Rechtsgrundlage gerechtfertigt sein.[807]

Während in lit. g das generelle öffentliche Interesse gemeint ist, also schützenswerte Belange des Gemeinwohls sowie der Gemeinschaftsgüter, behandeln lit. h und i spezifisch das öffentliche Gesundheitsinteresse.[808]

Art. 9 II lit. g DS-GVO i.V.m. § 22 I Nr. 2 BDSG kommt als Rechtfertigungsgrundlage für den Einsatz von Angriffserkennungssystemen nicht in Betracht, da die hohe Eingriffshürde, die durch das geforderte „erhebliche" Interesse gesetzt wird, nicht erreicht wird. Vergleicht man den Zweck des Einsatzes von Angriffserkennungssystemen in den Netzwerken von Krankenhäusern mit den in Erwägungsgrund 46 S. 3 aufgezählten Beispielen, so wird zwar von einem öffentlichen Interesse grundsätzlich ausgegangen werden können, ein erhebliches öffentliches Interesse liegt indes nicht vor. Zudem wird weder in Art. 9 II lit. g DS-GVO noch in § 22 I Nr. 2 BDSG die Datensicherheit erwähnt. In Bezug auf die Wahrung der Integrität und Vertraulichkeit von IT-Systemen und Netzwerken ist § 22 I Nr. 2 BDSG als mitgliedstaatliche Regelung zu allgemein. Hinzu kommt, dass es sich im konkreten Fall um die Verarbeitung besonderer Kategorien personenbezogener Daten im Gesundheitsbereich handelt und somit die spezielleren Art. 9 II lit. h und lit. i DS-GVO einschlägig sind.

(3) Die Versorgung im Gesundheitsbereich nach Art. 9 II lit. h DS-GVO

Die in der Praxis bedeutsamste Vorschrift im Bereich der Verarbeitung von Gesundheitsdaten stellt Art. 9 II lit. h DS-GVO dar.[809] So wird eine Ausnahme des generellen Verarbeitungsverbotes für „*Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich*" vorgesehen. Lit. h erfasst folglich sämtliche Phasen einer medizinischen Behandlung (Diagnose, Behandlung, Nachversorgung inklusive Rehabilitation) sowie die präventive Arbeit im Gesundheitssektor. Die Anforderungen an der Verarbeitung richten sich an die behandelnde Einrichtung selbst, also an die Arztpraxis, die Apotheke, das Krankenhaus oder ähnliches. Umfasst ist nach lit. h ebenfalls die mit der Behandlung zusammenhängende Verwaltung, die beispielsweise die Abrechnung, Buchführung und Statistik umfasst.[810] Die Begriffe Gesundheits- sowie Sozialbereich sind nicht klar voneinander abzugrenzen. Während im Gesundheitsbereich der Schwerpunkt auf dem körperlichen und

[807] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 54.*
[808] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 88;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 68.*
[809] Dochow u. a., *Datenschutz in der ärztlichen Praxis, S. 40.*
[810] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 35;* Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 98.*

seelischen Wohlbefinden liegt, befasst sich der Sozialbereich mit sozialer Gerechtigkeit und Sicherheit und öffentliche Leistungen oder staatliche Regulierungen. Eine klare Abgrenzung wird nach dem Wortlaut des lit. h allerdings auch nicht gefordert.[811]

Art. 9 II lit. h DS-GVO ist ebenfalls kein eigenständiger Erlaubnistatbestand, sondern fordert eine zusätzliche „*Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder einen Vertrag mit einem Angehörigen eines Gesundheitsberufs*".

Zudem müssen die in **Art. 9 III DS-GVO** enthaltenen Bedingungen und Garantien eingehalten werden.[812] Dieser schränkt eine Verarbeitung nach Art. 9 II lit. h DS-GVO derart ein, dass die Daten nur „*von Fachpersonal oder unter dessen Verantwortung verarbeitet werden*" dürfen und „*dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt*". Demnach ist die Verarbeitung von personenbezogenen Daten nicht nur durch Fachpersonal zulässig, sondern auch von weiteren Personen, so lange diese ebenfalls einer Geheimhaltungspflicht unterliegen. Da Art. 9 III DS-GVO keine Anforderungen an das Berufsgeheimnis stellt, ist davon auszugehen, dass jede Regelung eines Berufsgeheimnisses den Anforderungen genügt.[813] Zudem ist auch die Verarbeitung durch einen Auftragsverarbeiter oder einer -verarbeiterin abgedeckt, wenn die Geheimhaltungspflicht gesichert ist.[814] Eine vertraglich vereinbarte Verpflichtung zur Geheimhaltung genügt nach Abs. III hingegen nicht.[815]

Das von Art. 9 III DS-GVO erfasste Fachpersonal unterliegt im deutschen Recht primär dem Berufsgeheimnis aus § 203 I, II Nr. 1 StGB.[816] Gemäß § 203 III StGB liegt zudem keine Offenbarung eines Geheimnisses vor, wenn die nach Absatz 1 und 2 dem Berufsgeheimnis unterliegenden Personen „*Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen*". Zudem dürfen sie „*fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist*". Dies gilt auch für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit mitwirken und die dem Berufsgeheimnis unterliegen. Unter § 203 III 2 StGB fallen unter anderem Auftragsverarbeiter und -verarbeiterinnen i.S.d. Art. 28 DS-GVO. Diese unterliegen

[811] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 114.*
[812] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 9 Rn 42.*
[813] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 138.*
[814] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 89.*
[815] Dochow u. a., *Datenschutz in der ärztlichen Praxis, S. 42.*
[816] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 9 Rn 32.*

somit ebenfalls einer gesetzlichen Verschwiegenheitspflicht.[817] Zudem haben Berufsgeheimnisträger und -trägerinnen gemäß § 53 StPO ein Zeugnisverweigerungsrecht.

Zu den Berufsgeheimnissen gehört auch das Sozialgeheimnis aus § 35 SGB I.[818] Gemäß Absatz 1 Satz 1 umfasst die Wahrung des Sozialgeheimnisses „*die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden*". Das Sozialgeheimnis erstreckt sich zudem gemäß § 80 SGB X auch auf Auftragsverarbeiter und -verarbeiterinnen i.S.d. Art. 28 DS-GVO.

Durch lit. h des Art. 9 II DS-GVO können weder die Verarbeitung besonderer Kategorien personenbezogener Daten für die medizinische Forschung (Regelung in lit. j) noch die Durchsetzung für Zahlungsansprüche (Regelung in lit. f) gerechtfertigt werden.[819] Lit. h deckt das individuelle Interesse der betroffenen Person bei medizinischen Behandlungen ab, während lit. i das öffentliche Gesundheitsinteresse zum Regelungsgegenstand hat.[820]

(a) Anforderungen an die rechtliche Grundlage

Bevor einzelne Normen auf ihre Anwendbarkeit geprüft werden, muss sich auch hier die Frage gestellt werden, welche Anforderungen an die in Art. 9 II lit. h DS-GVO geforderte „*Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats*" gestellt werden. Vergleicht man den Wortlaut des Art. 9 II lit. h DS-GVO mit dem Wortlaut in Art. 6 I 1 lit. c DS-GVO („*rechtliche Verpflichtung*"), so ist auf den ersten Blick erkennbar, dass der Gesetzgeber unterschiedliche Voraussetzungen an die mitgliedstaatlichen Regelungen stellt. So ist der Regelungsinhalt einer Rechtsgrundlage umfassender als der einer rechtlichen Verpflichtung. Da bereits bei Art. 6 I 1 lit. c DS-GVO darüber gestritten wird, ob der Begriff „rechtliche Verpflichtung" das Erfordernis einer bloßen Verpflichtung oder einer Ermächtigungsgrundlage beinhaltet, kann bei Art. 9 II lit. h DS-GVO eine bloße rechtliche Verpflichtung als „*Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats*" nicht ausreichen. Der Erlaubnistatbestand ergibt sich nicht nur aus Art. 9 II lit.h DS-GVO, sondern muss ebenfalls in der unionsrechtlichen oder mitgliedstaatlichen Norm verankert sein. Für diese Auffassung spricht zudem, dass in der Literatur, anders als bei Art. 6 I 1 lit.c DS-GVO, die Auslegung der „*Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats*" nicht strittig ist. So spricht Ehmann/Selmayr klar von einer „gesetzliche Anordnung bzw. Erlaubnis einer solchen Verarbeitung im Unionsrecht oder im Recht der Mitgliedstaaten" [821], ebenso wie Taeger/Gabel.[822]

---

[817] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 149.*
[818] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 92.*
[819] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 78;* Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 93.*
[820] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 9 Rn 78.*
[821] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 60.*
[822] Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 9 Rn 30.*

Art. 9 II lit. h DS-GVO kann somit nur i.V.m. einem unionsrechtlichen beziehungsweise mitgliedstaatlichen Ermächtigungstatbestand eine Rechtfertigung der Verarbeitung besonderer Kategorien personenbezogener Daten darstellen.

Im Folgenden werden mögliche rechtliche Grundlagen auf ihre Anwendbarkeit als Rechtfertigungsgrundlage für dein Einsatz von Angriffserkennungssystemen in Krankenhäusern geprüft. Da § 8a BSIG sowie § 12 I TTDSG bereits i.V.m. Art. 6 I DS-GVO keine Ermächtigungsgrundlage für eine Rechtfertigung bilden, eine Rechtfertigung von besonderen Kategorien personenbezogener Daten die Voraussetzungen von Art. 6 I sowie Art. 9 II DS-GVO erfüllen muss und § 165 TKG neu nur eine partielle Rechtfertigung i.V.m. Art. 6 I 1 lit.c DS-GVO gewährleisten kann, werden diese nicht auf ihre Anwendbarkeit geprüft.

(b) § 22 I Nr. 1 lit. b BDSG

Auf nationaler Ebene wurde durch Art. 9 II lit. h, III DS-GVO i.V.m. § 22 I Nr. 1 lit. b BDSG ein Erlaubnistatbestand geschaffen, der nahezu wortgleich zu lit. h die Verarbeitung von Gesundheitsdaten in Arztpraxen und Kliniken im Rahmen von individuellen Behandlungsverhältnissen unter den Voraussetzungen der Geheimhaltungspflicht erlaubt.[823]

Jedoch stellt sich die Frage, ob dem geforderten Erforderlichkeitsgrundsatz genüge getan wird. So ist eine Verarbeitung nach lit. h erforderlich, wenn die Daten in direktem Zusammenhang mit der medizinischen Fachaufgabe stehen.[824] Dies hat zum Beispiel zur Folge, dass externe IT-Dienstleister und -Dienstleisterinnen, die die Praxisverwaltungssysteme installieren und warten, nicht unter lit. h fallen, sondern unter Umständen unter lit. i.[825] Auch hier steht die Installation von Angriffserkennungssystemen nur in einem mittelbaren Zusammenhang, da der primäre Grund – die Gewährleistung der Funktionsfähigkeit der Netzwerke und Systeme – auf sekundärer Ebene einen störungsfreien Krankenhausbetrieb ermöglichen kann. Ferner könnte die Anforderung aus Art. 9 III DS-GVO und § 22. I Nr. 1 lit. b BDSG in der Praxis zu Problemen führen, da bei der Verarbeitung der Daten Personal vorausgesetzt wird, das einer entsprechenden Geheimhaltungspflicht unterliegt. Zwar ist hierfür nicht ausdrücklich medizinisches Fachpersonal gefordert, jedoch müssen die verarbeitenden Personen aufgrund einer bestehenden Rechtsgrundlage der Geheimhaltungspflicht unterliegen. Eine vertragliche Verpflichtung hierzu reicht nicht aus.

Laut Erwägungsgrund 53 S. 1 der DS-GVO dürfen besondere Kategorien personenbezogener Daten für „*gesundheitsbezogene Zwecke*“ insbesondere dann verarbeitet werden, wenn ein Zusammenhang „*mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen und*

[823] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 37.*
[824] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 88.*
[825] Dochow u. a., *Datenschutz in der ärztlichen Praxis, S. 44.*

der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des Sozialsystems und zwecks Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen" besteht. Die Nutzung von Angriffserkennungssystemen in Netzwerken privatrechtlicher organisierter Krankenhäuser dient der Erkennung und Abwehr von Cyber-Angriffen und soll folglich die Funktionsfähigkeit und Integrität der zu schützenden Netzwerke gewährleisten. Dieses hierdurch verfolgt Ziel könnte unter die „*Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge*" subsumiert werden. Allerdings wird in Erwägungsgrund 53 S. 1 ein Bezug zur Gesundheit beim Zwecke der Verarbeitung gefordert. Direkt wird man einen gesundheitsbezogenen Zweck beim Einsatz von Angriffserkennungssystemen nicht bejahen können. Angriffserkennungssysteme werden nicht installiert, um die Behandlung der Patienten und Patientinnen oder die damit einhergehende Verwaltung zu unterstützen, sondern um die Funktionsfähigkeit von Netzwerken zu schützen und zu erhalten. Hieraus ließe sich allenfalls ein mittelbarer Zweck zur Gesundheitsversorgung ziehen, da die Funktionsfähigkeit des Krankenhaus-Netzwerkes für die Versorgung und Administration der Patienten und Patientinnen von Bedeutung ist.

Zusammengefasst ist eine Rechtfertigung der Nutzung von Angriffserkennungssystemen in privatrechtlich organisierten Krankenhäusern nach Art. 9 II lit. h, III DS-GVO i.V.m. § 22. I Nr. 1 lit. b BDSG mit zu viel Rechtsunsicherheit bezüglich der Zweckgebundenheit, der Erforderlichkeit und der geforderten Maßstäbe an die Geheimhaltungspflicht behaftet. Zudem sind die beiden Normen, die sich inhaltlich kaum unterscheiden, zu allgemein formuliert, um eine verlässliche Erlaubnisnorm in diesem konkreten Fall darstellen zu können.

(c) § 75c SGB V

Gemäß § 75c I SGB V sind Krankenhäuser ab dem 1. Januar 2022 dazu verpflichtet, „*nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind*". Wie bereits unter Art. 6 I 1 lit. c DS-GVO behandelt, umfasst § 75c SGB V grundsätzlich den Einsatz von Angriffserkennungssystemen und dies explizit in Krankenhäusern.

Fraglich ist jedoch, ob § 75c SGB V den Anforderungen aus Art. 9 III DS-GVO gerecht wird. Hiernach kann eine Datenverarbeitung über Art. 9 II lit. h DS-GVO nur gerechtfertigt sein, wenn der Verarbeiter einer Geheimhaltungspflicht unterliegt. Wie bereits zuvor erwähnt, nutzen Krankenhäuser je nach Größe und Kostenfaktor externe IT-Dienstleister oder -

Dienstleisterinnen, um die komplexe EDV betreiben zu können.[826] Diese sind, wenn sie weisungsgebunden sind, Auftragsverarbeiter und -verarbeiterinnen i.S.d. Art. 28 DS-GVO. Die datenschutzrechtliche Verantwortung verbleibt beim Krankenhausbetreibenden. Seit dem Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017 umfasst § 203 StGB durch den Absatz 3 auch „*sonstige mitwirkende Personen*“, die an der Tätigkeit des Geheimnisträgers oder der -trägerin mitwirken, ohne in dessen oder deren Sphäre eingegliedert zu sein.[827] Hierzu gehören auch Auftragsverarbeiter und -verarbeiterinnen i.S.d. Art. 28 DS-GVO. Da die Mitarbeitenden der krankenhausinternen IT-Abteilung als „Gehilfen“ und externe IT-Dienstleister und -Dienstleisterinnen als „sonstige mitwirkende Personen“ i.S.d. § 203 III StGB zu bewerten sind, entspricht § 75c SGB V den Anforderungen des Art. 9 III DS-GVO, obwohl hier keine expliziten Regelungen zur Geheimniswahrung getroffen wurden.

Allerdings ist § 75c SGB V eine reine Verpflichtungsnorm und ähnelt im Aufbau und Formulierung Art. 32 DS-GVO, der Anforderungen an die Datensicherheit stellt, aber keine Verarbeitungserlaubnis enthält. § 75c SGB V verpflichtet Krankenhäuser zwar, Maßnahmen zur Gewährleistung der Datensicherheit auszuführen und hat durch seine Nähe zu § 8a BSIG, in dem die Nutzung von Angriffserkennungssystemen thematisiert wird, auch einen Bezug hierzu. Jedoch erlaubt er in dem Zusammenhang keine Verarbeitung von personenbezogenen Daten. Auch im Zehnten Kapitel des SGB V, das unter anderem Regeln zum Datenschutz aufführt, ist keine Ermächtigungsgrundlage zur Verarbeitung personenbezogener Daten enthalten, die i.V.m. § 75c SGB V einen Erlaubnistatbestand darstellen kann.

Da Art. 9 II lit. h DS-GVO eine Ausnahme des Verarbeitungsverbotes aus Art. 9 I DS-GVO nur i.V.m. einer Ermächtigungsgrundlage aus Unionsrecht oder mitgliedstaatlichem Recht bilden kann und § 75c SGB V lediglich eine rechtliche Verpflichtung darstellt, genügt § 75c SGB V den Anforderungen des Art. 9 II lit. h DS-GVO nicht.

In Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 I DS-GVO, insbesondere von Gesundheitsdaten und genetischen Daten, stellt Art. 9 II lit. h DS-GVO i.V.m. § 75c SGB V keine Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft dar.

(d) § 330 I SGB V

Gemäß § 330 I 1 SGB V sind die Gesellschaft für Telematik sowie verantwortliche Anbieter und Anbieterinnen verpflichtet, „*angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der Telematikinfrastruktur*

[826] Redaktion KWM*, Datenschutz: Wie Kliniken Patientendaten bei externen Aufträgen schützen können.*
[827] Frhr. von dem Bussche*, Konzerndatenschutz Teil 3 Kapitel 4 Rn 12.*

zu treffen und fortlaufend zu aktualisieren". Angemessen ist eine Vorkehrung nach § 330 I 3 SGB V, „*wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der Telematikinfrastruktur insgesamt oder von solchen Diensten der Telematikinfrastruktur steht, die durch Störungen verursacht werden können*".

Auch hier scheitert diese mögliche Ermächtigungsgrundlage an den Anforderungen der rechtlichen Grundlage des Art. 9 II lit. h DS-GVO, da § 330 I SGB V lediglich eine rechtliche Verpflichtung darstellt. Im Zusammenhang mit § 330 I SGB V erlaubt § 331 IV SGB V zwar die Verarbeitung der personenbezogenen Daten, jedoch gilt diese Verarbeitungserlaubnis nur für die Gesellschaft der Telematik und nicht für die verantwortlichen Anbieter und Anbieterinnen i.S.d. SGB V, zu denen die Krankenhäuser bezogen auf ihre eigenen Netzwerke gehören. Zudem ist § 75 c SGBV lex specialis zu § 330 I SGB V.

Art. 9 II lit. h DS-GVO i.V.m. § 330 I SGB V kommt somit nicht als Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft in Betracht.

(4) Die öffentlichen Gesundheitsdienste nach Art. 9 II lit. i DS-GVO

Ist „*die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit {...} erforderlich*" so kann gemäß Art. 9 II lit. i DS-GVO „*auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht*" die Verarbeitung besonderer Kategorien personenbezogener Daten gerechtfertigt sein. Lit. i nennt beispielhaft den „*Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren*" oder die „*Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten*". Die Beispiele sind als Konkretisierung des Begriffs der öffentlichen Gesundheit zu interpretieren und nicht als abschließender Katalog.[828]

Art. 9 II lit. i DS-GVO ist folglich ebenfalls eine Öffnungsklausel und findet sein nationalrechtliches Pendant in **§ 22 I Nr. 1 lit. c BDSG**, der inhaltlich fast deckungsgleich zum lit. i ist.

In Abgrenzung zu lit. g und lit. h bezieht sich lit. i spezifisch auf das öffentliche Gesundheitsinteresse. Laut Erwägungsgrund 54 S. 3 der DS-GVO soll der Begriff der öffentlichen Gesundheit i.S.d Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates ausgelegt werden und „*alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der*

[828] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 9 Rn 46.*

Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen". Ein Beispiel hierfür ist die elektronische Patientenakte, die bereits in viele Mitgliedstaaten der EU eingeführt wurde.[829] Im Gegensatz zu lit. g fordert lit. i ein einfaches öffentliches Interesse, das allerdings dem Bereich des öffentlichen Interesses zuzuschreiben sein muss. In anderen Fällen ist lit. g anzuwenden und somit ein erhebliches öffentliches Interesse gefordert.[830]

Für private Verarbeiter und Verarbeiterinnen setzte Erwägungsgrund 54 in Satz 4 strenge Voraussetzungen. Sie dürfen sich nur auf lit. i berufen, wenn der Zweck der Datenverarbeitung im öffentlichen Interesse liegt.

(a) Anforderungen an die rechtliche Grundlage

Da Art. 9 II lit. i DS-GVO wortgleich zu Art. 9 II lit. h DS-GVO eine „*Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats*" fordert, kann hier auf die Ausführungen bei Art. 9 II lit. h DS-GVO verwiesen werden. Eine bloße rechtliche Verpflichtung reicht nicht aus, um i.V.m. Art. 9 II lit. i DS-GVO eine Rechtfertigungsgrundlage zur Verarbeitung personenbezogener Daten zu bilden.[831] Das Element des Erlaubnistatbestandes muss vielmehr auch in der Grundlage aus dem Unionsrecht oder dem mitgliedstaatlichem Recht zu finden sein.

Zudem verlangt Art. 9 II lit. i DS-GVO ähnlich wie in Art. 9 III DS-GVO spezifische Schutzmechanismen wie die Einhaltung des Berufsgeheimnisses.[832]

Da § 75c und § 330 I SGB V lediglich rechtliche Verpflichtungen darstellen, kommen diese nicht als Ermächtigungsgrundlage i.S.d. Art. 9 II lit. i DS-GVO nicht in Betracht.

Im Folgenden wird § 22 I Nr. 1 lit. c BDSG auf seine Anwendbarkeit als Rechtfertigungsgrundlage für dein Einsatz von Angriffserkennungssystemen in Krankenhäusern i.V.m. Art. 9 II lit. i DS-GVO geprüft.

(b) § 22 I Nr. 1 lit. c BDSG

Gemäß § 22 I Nr. 1 lit. c BDSG ist die Verarbeitung besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 I DS-GVO zulässig „*aus Gründen des öffentlichen Interesses im Bereich der*

---

[829] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 39;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 95.*
[830] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 9 Rn 82;* Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 9 Rn 47.*
[831] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 9 Rn 84.*
[832] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 118;* Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 41.*

öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist". Da sich § 22 I Nr. 1 lit. c BDSG beinah wortgleich an Art. 9 II lit. i DS-GVO orientiert, sind die entsprechenden Auslegungen der Begrifflichkeiten auch hier anwendbar. Wie zuvor ausgeführt ist es fraglich, ob der Einsatz von Angriffserkennungssystemen in Krankenhäusern überhaupt in den Anwendungsbereich des Art. 9 II lit. i DS-GVO und somit auch in den Anwendungsbereich des § 22 I Nr. 1 lit. c BDSG fällt.

Die Ausnahmevorschrift des Art. 9 II lit. i DS-GVO steht in inhaltlichem Zusammenhang mit Art. 168 AEUV. Dieser zielt gemäß Absatz 1 auf „*die Verbesserung der Gesundheit der Bevölkerung, die Verhütung von Humankrankheiten und die Beseitigung von Ursachen für die Gefährdung der körperlichen und geistigen Gesundheit*" ab. Dies umfasst „*die Bekämpfung der weit verbreiteten schweren Krankheiten, wobei die Erforschung der Ursachen, der Übertragung und der Verhütung dieser Krankheiten sowie Gesundheitsinformation und -erziehung gefördert werden; außerdem umfasst sie die Beobachtung, frühzeitige Meldung und Bekämpfung schwerwiegender grenzüberschreitender Gesundheitsgefahren*". Hieraus entstand beispielsweise die Einrichtung eines Netzwerks zur Überwachung übertragbarer Krankheiten.[833] Als Sicherheitsanliegen formuliert Art. 168 AEUV in Absatz 4 „*Maßnahmen zur Festlegung hoher Qualitäts- und Sicherheitsstandards für Organe und Substanzen menschlichen Ursprungs sowie für Blut und Blutderivate*", „*Maßnahmen in den Bereichen Veterinärwesen und Pflanzenschutz, die unmittelbar den Schutz der Gesundheit der Bevölkerung zum Ziel haben*" und „*Maßnahmen zur Festlegung hoher Qualitäts- und Sicherheitsstandards für Arzneimittel und Medizinprodukte*".

Die Gewährleistung von Sicherheitsstandards i.S.d. Art. 9 II lit. i DS-GVO umfasst folglich die medizin- und produktrechtliche Komponente des Gesundheitswesens, wohingegen unter Art. 9 II lit. h DS-GVO die infrastrukturellen und systemischen Aspekte fallen.[834] Beispiele für Grundlagen i.S.d. Art. 9 II lit. i DS-GVO, die durch mitgliedstaatliches Recht umgesetzt wurden, sind das Krebsregister nach § 65c SGB V und die Regelungen zur elektronischen Gesundheitskarte §§ 291ff. SGB V sowie Regelungen im Arzneimittelgesetz, Medizinproduktegesetz und Meldepflichten im Infektionsschutzgesetz.[835] So fallen Regelungen im Arzneimittelgesetz unter die „*Gewährleistung hoher Qualitäts- und Sicherheitsstandards*" und die Meldepflicht im Infektionsschutzgesetz unter den „*Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren*".[836]

---

[833] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 94.*
[834] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 62.*
[835] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 95;* Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 119;* Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 41.*
[836] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 9 Rn 85.*

Der Einsatz von Angriffserkennungssystemen in Krankenhäusern soll die IT-Sicherheit der Gesundheitsinfrastruktur gewährleisten und die besonders schützenswerten Patienten- und Patientinneninformationen vor zum Zugriff Dritter schützen. Die IT-Sicherheit fällt jedoch nicht unter den „*Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren*“, da hierunter medizinische Gefahren i.S.v. Epidemien verstanden werden und keine technischen Gefahren, die eine Gesundheitsgefährdung daherbringen könnten. Auch unter der „*Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten*“ kann nicht die IT-Sicherheit subsumiert werden, da auch hier ausschließlich medizinische Aspekte berücksichtigt werden, wie aus Art. 168 IV AEUV und bereits erlassenen rechtlichen Grundlagen i.S.d. Art. 9 II lit. i DS-GVO entnommen werden kann.

Da der Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft nicht in den Anwendungsbereich des Art. 9 II lit. i DS-GVO i.V.m. § 22 I Nr. 1 lit. c BDSG fällt, kann dieser nicht hierrüber gerechtfertigt werden.

(5) Die Öffnungsklausel des Art. 9 IV DS-GVO

Art. 9 IV DS-GVO gibt den Mitgliedstaaten die Möglichkeit, zusätzliche Bedingungen oder Beschränkungen einzuführen oder aufrecht zu erhalten, „*soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist*“. Die allgemeine Öffnungsklausel formuliert keine Voraussetzungen an die nationalen Bestimmungen. Allerdings dürfen hierdurch keine neuen Ausnahmetatbestände des Verarbeitungsverbots etabliert werden. Durch Absatz 4 können die Anforderungen des Absatzes 2 allenfalls verschärft und spezifiziert werden. Dies könne aus dem Wortlaut des Absatzes 4 interpretiert werden, der gerade nicht von Ausnahmen spricht.[837] Die nach Absatz 4 erlaubten nationalen Bedingungen und Beschränkungen müssen nicht notwendigerweise Verarbeitungsanforderungen beinhalten, sondern können auch rechtliche Entlastungen unter angemessenen Garantiebestimmungen anführen.[838] Sämtliche Anforderungen müssen jedoch verhältnismäßig in Bezug auf ihren Schutzzweck sein.[839]

In Bezug auf Art. 9 II lit. b und g bis j DS-GVO entfaltet Absatz 4 keine Wirkung, da hier bereits Öffnungsklauseln vorgesehen sind[840], weswegen Art. 9 IV DS-GVO in der Prüfung der Rechtmäßigkeit der Nutzung von Angriffserkennungssystemen in privatrechtlich organisierten Krankenhäusern keine Anwendung findet.

[837] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 9 Rn 64.*
[838] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 154.*
[839] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 150.*
[840] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 9 Rn 59.*

d) Zwischenergebnis

Um besondere Kategorien personenbezogener Daten rechtmäßig verarbeiten zu können, muss diese nach Art. 6 sowie Art. 9 DS-GVO erlaubt sein. In Netzwerken von Krankenhäusern werden unter anderem genetische Daten und Gesundheitsdaten i.S.d. Art. 9 I DS-GVO verarbeitet. Da Angriffserkennungssysteme sämtliche Datenströme des Netzwerkes oder des Systems, in dem sie installiert wurden, analysieren und somit verarbeiten, muss für den Einsatz von Angriffserkennungssystemen in Krankenhäusern auch eine Rechtfertigung der Verarbeitung nach Art. 9 II DS-GVO vorliegen.

Der Einsatz von Angriffserkennungssystemen in Krankenhäusern könnte zwar unter die Versorgung im Gesundheitsbereich nach Art. 9 II lit. h DS-GVO fallen, jedoch entsprechen die möglichen Rechtsnormen aus dem mitgliedstaatlichen Recht nicht den Anforderungen des Art. 9 II lit. h DS-GVO.

4. Zusammenfassung

Der Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft kann grundsätzlich über Art. 6 I 1 lit. c DS-GVO i.V.m. § 75c I SGB V gerechtfertigt werden. Werden hierbei jedoch besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO verarbeitet, fehlt es an einer Ermächtigungsgrundlage. Da eine solche Verarbeitung in Krankenhausnetzwerken unvermeidbar ist, gibt es zum jetzigen Stand der Gesetzgebung keine umfassende Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft.

D. Datensicherheit

Neben den Regelungsinhalten zur Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten, verfolgt die DS-GVO den Ansatz des Datenschutzes durch Technikgestaltung – auch Datensicherheit genannt. Ziel ist hierbei, Datenschutzgrundsätze nicht erst bei der eigentlichen Verarbeitung zu beaufsichtigen und zu kontrollieren, sondern bereits bei der Planung und Implementierung von Systemen zu verankern.[841] Dies verdeutlicht Erwägungsgrund 78 S. 1, wonach es für den „*Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen erforderlich ist, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden*“. Dieser prägt auch in S. 2 die Begriffe Datenschutzes durch Technik (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default). Die folgenden Normen zur Datensicherheit sind bloße Verfahrensvorschriften und bilden keine

[841] Sydow*, Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 25 Rn 2;* Kühling/Buchner*, Datenschutzgrundverordnung Kommentar Art. 32 Rn 1.*

Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten. Diese richtet sich allein nach Art. 6 I und Art. 9 I DS-GVO.[842]

Lex generalis ist **Art. 24 DS-GVO**, wonach in S. 1 der oder die Verantwortliche „*unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen {...}*" umzusetzen hat. Art. 24 DS-GVO greift den allgemeinen Verarbeitungsgrundsatz aus Art. 5 Abs. 1 lit. f. DS-GVO auf, der Integrität und Vertraulichkeit bei der Verarbeitung personenbezogener Daten fordert. Der in Art. 24 DS-GVO erwähnte Begriff der „technischen und organisatorischen Maßnahmen" stellt eine Verknüpfung der Datensicherheit mit dem Datenschutz dar, da ein umfassender Schutz von personenbezogenen Daten nur dann gewährleistet werden kann, wenn diese auch vor unberechtigtem Zugriff und missbräuchlicher Nutzung geschützt werden.[843]

Konkretisierung erfährt Art. 24 DS-GVO in den **Art. 25 und 32 DS-GVO**. Während Art. 25 DS-GVO die Berücksichtigung des Datenschutzes schon im Vorfeld der Datenverarbeitung anordnet, regelt Art. 32 DS-GVO technische und organisatorische Sicherheitsanforderung für die Verarbeitung. Das von Art. 25 und Art. 32 DS-GVO geforderte Datenschutzniveau ist einzelfallabhängig[844] und muss für jeden konkreten Fall anhand einer Risikoabschätzung geprüft werden. Beide Normen hängen eng zusammen und zeigen eine ähnliche Gesinnung auf, da beispielsweise die Pseudonymisierung in beiden Artikeln als geeignete Sicherheitsmaßnahmen angesehen wird.[845] Der Unterschied zwischen den beiden Normen ist in dem Normzweck zu finden: So sollen nach Art. 32 DS-GVO Schutzmaßnahmen anhand einer Risikoanalyse getroffen und primär der Grundsatz aus Art. 5 I lit. f DS-GVO gewährleistet werden, wohingegen Art. 25 DS-GVO die wirksame Umsetzung sämtlicher Grundsätze des Art. 5 DS-GVO verfolgt.[846] Zudem besteht hinsichtlich des jeweiligen Normadressaten ein Unterschied, da Art. 25 DS-GVO nur den Verantwortlichen oder die Verantwortliche in die Pflicht nimmt, Art. 32 DS-GVO zudem auch den Auftragsverarbeiter oder die -verarbeiterin.[847] Hersteller, Herstellerinnen sowie Produzenten und Produzentinnen von Systemen gehören nicht unmittelbar zum Normadressatenkreis der DS-GVO, können aber aufgrund der geforderten Maßnahmen aus Art. 25 und Art. 32 mittelbar verpflichtet werden.[848]

---

[842] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 25 Rn 3.*
[843] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kap.1 Rn 44.*
[844] Frhr. von dem Bussche, *Konzerndatenschutz Kap. 3 Rn 1.*
[845] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 32 Rn 9;* Sydow, *Europäische Datenschutzgrundverordnung Handkommentar Art. 25 Rn 83.*
[846] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 25 Rn 8;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 32 Rn 12.*
[847] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 32 Rn 8.*
[848] Kühling/Buchner, *Datenschutzgrundverordnung Kommentar Art. 25 Rn 13.*

Inwieweit neben der Frage der Rechtmäßigkeit der Nutzung von Angriffserkennungssystemen in privatrechtlich organisierten Krankenhäusern eine Nutzung solcher Angriffserkennungssysteme nach der DS-GVO gefordert bzw. vorgesehen ist, wird in diesem Kapitel erörtert.

Zunächst einmal wird der risikobasierte Ansatz der DS-GVO erläutert, bevor die Anforderungen des Art. 32 und 25 DS-GVO hinsichtlich der technischen Ausgestaltung zur Gewährleistung von Datensicherheit vorgestellt und auf den Einsatz von Angriffserkennungssystemen bezogen werden.

a) Der Risikobegriff der DS-GVO

Eine Neuerung im Datenschutzrecht ist der durch die DS-GVO eingeführte risikobasierte Ansatz, an dem sich sowohl Art. 25 als auch Art. 32 DS-GVO orientieren.[849] Das Risiko bezieht sich hier nach Art. 24 I DS-GVO auf die Gefährdung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Eine Legaldefinition des Risikobegriffs ist in Art. 4 der DS-GVO nicht erfolgt. Laut Erwägungsgrund 75 der DS-GVO sind jedoch potentielle physische, materielle sowie immaterielle Schäden bei der Risikoeinschätzung zu beachten, maßgeblich ist hierbei die Verletzung Betroffener in ihren Grundrechten, wie auch Erwägungsgrund 94 S. 2 unterstreicht. Erwägungsgrund 75 stellt eine sehr verschachtelt Auflistung der Risiken sowie Bewertungsaspekte dar. Nach Erwägungsgrund 76 soll zudem die „*Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt*." Kritiker und Kritikerinnen werfen der DS-GVO hier eine „Zirkelschlüssigkeit" vor, da nach Erwägungsgrund 75 und 76 das Risiko selbst mit einer Eintrittswahrscheinlichkeit und Schwere beurteilt werden soll, in der Informationssicherheit aber oftmals anhand der Eintrittswahrscheinlichkeit und Schwere des möglichen Schadens das Risiko bestimmt wird. Die Risikoformel aus der Informationssicherheit ist aber mit der DS-GVO nicht kompatibel, da diese in Erwägungsgrund 94 S. 2 nicht nur auf Schäden, sondern auch auf Grundrechtsbeeinträchtigungen verweist.[850] Zudem sei die Zusammenstellung der Aufzählung von potentiellen Risiken in Erwägungsgrund 75 von einer unsystematischen Willkürlichkeit geprägt.[851]

Allgemein lässt sich sagen, dass je höher die Wahrscheinlichkeit und die Schwere einer möglichen Verletzung der Rechte und Freiheiten von natürlichen Personen ist, desto höher sind die Anforderungen, die an die datenschutzrechtlichen Pflichten des oder der Verarbeitenden zu stellen sind.[852]

---

[849] Schröder, *ZD 2019, 503 (503).*
[850] Bieker, *DuD 2018, 27 (29).*
[851] Schröder, *ZD 2019, 503 (503).*
[852] Bieker, *DuD 2018, 27 (30);* Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kap. 2 Rn 6.*

b) Art. 32 DS-GVO

Art. 32 DS-GVO ist eine Ausformung des allgemeinen datenschutzrechtlichen Grundsatzes der Integrität und Vertraulichkeit aus Art. 5 I lit. f DS-GVO und konkretisiert den Generalauftrag des Art. 24 DS-GVO.[853] Zudem erfüllt Art. 32 DS-GVO das – durch den EuGH anerkannte und konkretisierte – Schutzgebot von personenbezogenen Daten im technischen und organisatorischen Sinn aus Art. 8 Abs. 1 GRCh.[854] Ferner stellt Art. 32 DS-GVO die Grundlagennorm für die Melde- und Benachrichtigungspflichten aus Art. 33 und 34 DS-GVO dar.[855]

Während Art. 6 DS-GVO die Erlaubnistatbestände enthält, die eine Verarbeitung personenbezogener Daten rechtfertigen und Art. 5 DS-GVO die allgemeingültigen Grundsätze hierbei formuliert, gibt Art. 32 DS-GVO „regulatorische Leitplanken" für die Sicherheit der Verarbeitung vor. Die Rechtmäßigkeit der Verarbeitung wird in Art. 32 DS-GVO somit nicht geregelt und ein Verstoß gegen Art. 32 DS-GVO führt nicht zur Rechtswidrigkeit ebendieser.[856]

Dabei liegen die geforderten Sicherheitsmaßnahmen des Art. 32 DS-GVO nah an den Maßnahmen des Kataloges des BSIG und der NIS-Richtlinie.[857] **Abs. 1 des Art. 32 DS-GVO** fordert, dass der oder die Verantwortliche und der Auftragsverarbeiter bzw. die -verarbeiterin bei der Datenverarbeitung geeignete technische und organisatorische Maßnahmen zu treffen haben, „*um ein dem Risiko angemessenes Schutzniveau zu gewährleisten*". Dieses hat „*unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen*" zu erfolgen. Zielrichtung dieses Absatzes ist der Schutz des oder der Einzelnen vor einer unzulässigen Verwendung seiner oder ihrer Daten mit der Folge, dass die Infrastruktur zu sichern ist und nicht die Sicherheit und Funktionsfähigkeit der Informations- und Kommunikationsinfrastruktur an sich.[858] Hierbei gilt es stets, den Schutzaufwand mit dem Risiko ins Verhältnis zu setzen.[859] Art. 32 I DS-GVO ist folglich multipolar ausgerichtet und gibt im Verhältnis der einzelnen Faktoren zueinander keine Hierarchie vor.[860] Die in Art. 32 I HS. 2 lit. a bis d DS-GVO aufgezählten Maßnahmen sind nicht abschließend („*unter anderem*") und verankern lediglich einen Mindeststandard, der den Verarbeitenden oder die Verarbeitende nicht in seinem oder ihrem Ausmaß der Sicherheitsvorkehrungen beschränkt.[861] Zudem sind die aufgezählten Maßnahmen nicht statisch, sondern können individuell bei den konkreten Risikobewertungen

---

[853] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 32 Rn 2;* Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 32 Rn 1.*
[854] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 32 Rn 6;* Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 32 Rn 33.*
[855] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 32 Rn 3.*
[856] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 32 Rn 2,3.*
[857] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kap. 4 Rn 28.*
[858] Forgó u. a., *Rechtsgutachten zum Betrieb von IDS & Event Management-Systemen in Netzen der öffentlichen Verwaltung, S. 47.*
[859] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 32 Rn 7.*
[860] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 32 Rn 26.*
[861] Frhr. von dem Bussche, *Konzerndatenschutz Kap. 3 Rn 2.*

variieren.[862] Es ergibt sich somit ein großer Ermessensspielraum beim Adressaten bzw. bei der Adressatin.[863]

Bei dem in Art. 32 I DS-GVO geforderten Stand der Technik handelt es sich um bekannte, bewährte und verfügbare technische Maßnahmen und nicht notwendigerweise um die neusten und leistungsfähigsten technischen Produkte oder Entwicklungen. Zudem muss der Stand der Technik regelmäßig anhand der technologischen Weiterentwicklung überprüft und gegebenenfalls angepasst werden, da dieser Begriff auf einer gegenwärtigen Bewertung basiert und sich in seinen Ansprüchen verändern kann.[864] Der aktuelle Stand der Technik lässt sich unter Zuhilfenahme diverser Standards und Normen (beispielsweise ISO/IEC 27000-Normenreihe oder NIS Cybersecurity-Framework) sowie des IT-Grundschutzes des BSI ermitteln.[865]

Abs. 2 des Art. 32 DS-GVO stellt bei der Beurteilung eines angemessenen Schutzniveaus nach Abs. 1 die Risiken in den Vordergrund, „*die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden*“ und stellt somit eine Konkretisierung des Abs. 1 dar. Abs. 2 ist bei der Risikobewertung und der Maßnahmenfindung nach Art. 1 verpflichtend zu berücksichtigen.[866]

c) Art. 25 DS-GVO

Während Art. 32 I DS-GVO sich auf die Sicherheit während der Verarbeitung personenbezogener Daten bezieht, setzt der Regelungsgehalt des Art. 25 DS-GVO noch vor der eigentlichen Verarbeitung an, wobei der in beiden Artikeln vorkommende Begriff der „technischen und organisatorischen Maßnahmen“ identisch ist.[867] Art. 25 DS-GVO ist ebenso wie Art. 32 DS-GVO als Konkretisierung zu Art. 24 DS-GVO zu sehen, wobei im Verhältnis zueinander wiederum Art. 32 DS-GVO lex specialis zu Art. 25 DS-GVO ist.[868]

Art. 25 DS-GVO sieht Schutzmaßnahmen bei der Produktentwicklung und -implementierung und somit schon vor der Erhebung personenbezogener Daten vor.[869] Er folgt dem Konzept eines Datenschutzes durch Technik („privacy by design“), begleitet von datenschutzfreundlichen Voreinstellungen („privacy by default“).[870] Die Betitelung der Regelungen des Art. 25 DS-

---

[862] Frhr. von dem Bussche, *Konzerndatenschutz Kap. 3 Rn 15.*
[863] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 32 Rn 10.*
[864] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 32 Rn 5;* Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 32 Rn 18, 19.*
[865] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kap. 1 Rn 48, 49.*
[866] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kap. 2 Rn 25;* Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 32 Rn 38, 39.*
[867] Frhr. von dem Bussche, *Konzerndatenschutz Kap. 3 Rn 51,52.*
[868] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 25 Rn 8.*
[869] Bartsch/Rieke, *EnWZ 2017, 435 (437);* Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 25 Rn 1.*
[870] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 25 Rn 8.*

GVO als „privacy by design“ und „privacy by default“ werden in der Literatur jedoch kritisiert. So würden diese Umschreibungen zu Missverständnissen führen, da das Schutzgut des Art. 25 DS-GVO nicht der Schutz der Privatsphäre (Privacy) sei, sondern der Schutz personenbezogener Daten, also der Datenschutz. Dies würde sich auch in der englischsprachigen Fassung wiederspiegeln, in der von „data Protection by design“ gesprochen wird. Der Begriff „Privacy“ kommt lediglich in Art. 7 GRCh vor, der zwar eine Verwandtschaft zu Art. 8 GRCh aufweist, die DS-GVO allerdings auf dem Datenschutzgrundrecht des Art. 8 GRCh fußt.[871] Dies wird auch verdeutlicht durch Erwägungsgrund 78 der DS-GVO, in der in Satz 2 von „data protection by design“ und „data protection by default“ gesprochen wird.

Datenschutz durch Technikgestaltung wird in Art. 25 DS-GVO bereits als „Bestandteil der Systementwicklung“ verstanden, also ex ante betrachtet.[872] Diese Maßnahmen sollen bei der Umsetzung von den Datenverarbeitungsgrundsätzen des Art. 5 DS-GVO wie beispielsweise der Datenminimierung und der Datenvermeidung helfen.[873] Hintergrund der ex ante-Sicht ist die Feststellung, dass viele Verarbeitungsvorgänge bereits durch Voreinstellungen der genutzten Hard- und Software vorgegeben sind und folglich bei einem Ansätzen des technischen Datenschutzes im Konzeptions- und Entwicklungsprozess möglich Verstöße gänzlich oder zumindest effektiver vermieden werden können.[874]

Adressat bzw. Adressatin des Art. 25 DS-GVO ist trotz des ex ante-Ansatzes der oder die Verantwortliche und nicht der Hersteller oder die Herstellerin. Für die Hersteller und Herstellerinnen von Software oder Verarbeitungstechnik kann Art. 25 DS-GVO lediglich als „Aufruf zur datenschutzfreundlichen Gestaltung“ verstanden werden.[875] Der oder die Verantwortliche hat somit bei der „*Festlegung der Mittel für die Verarbeitung*“, spätestens aber „*zum Zeitpunkt der eigentlichen Verarbeitung*“ die Vorgaben des Art. 25 DS-GVO zu beachten. Seiner oder ihrer Verantwortung kann er oder sie sich auch nicht durch eine Auftragsverarbeitung entziehen, da der oder die Verantwortliche laut Art. 28 I DS-GVO bei der Auswahl eines Auftragsverarbeiters oder einer -verarbeiterin sicherstellen muss, dass dieser oder diese „*die hinreichend Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet*“.

Während Art. 25 I DS-GVO die Pflicht zum Datenschutz durch Technikgestaltung behandelt, werden in Art. 25 II DS-GVO datenschutzfreundliche Voreinstellungen gefordert. Abs. 2 ist aufgrund seiner Regelungen in besonderen Anwendungsfällen lex specialis zu Abs. 1, der

---

[871] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 25 Rn 2;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 25 Rn 23.*
[872] Frhr. von dem Bussche, *Konzerndatenschutz Kap. 3 Rn 53.*
[873] Bartsch/Rieke, *EnWZ 2017, 435 (437);* Kühling/Buchner, *Datenschutzgrundverordnung Kommentar Art. 25 Rn 15.*
[874] Ehmann/Selmayr, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 25 Rn 1.*
[875] Schneider, *Datenschutz nach der EU-Datenschutz-Grundverordnung, S. 255;* Laue/Kremer, *Das neue Datenschutzrecht in der betrieblichen Praxis§ 7 Rn 8.*

allgemeine organisatorische und technische Verpflichtungen enthält und dem oder der Verantwortlichen einen weiten Gestaltungsspielraum einräumt.[876] Die recht abstrakte Anforderungsformulierung des Art. 25 DS-GVO ist der Dynamik des Datenschutzes geschuldet, um offen und beständig für zukünftige Entwicklungen zu sein.[877]

In **Abs. 1 des Art. 25 DS-GVO** wird der oder die Verantwortliche unter der Möglichkeit der Abwägung[878] verpflichtet, bereits bei der Konzipierung[879] „*geeignete technische und organisatorische Maßnahmen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen*" und trägt der Erkenntnis Rechnung, dass ein umfassender Datenschutz nur durch eine entsprechende Technikgestaltung bereits bei der Konzipierung möglich ist.[880] Diese technische Gestaltung trifft alle physischen Vorkehrungen, sowie die Software- und Hardwareprozesse. Organisatorische Maßnahmen beziehen sich auf die äußeren Rahmenbedingungen für die technische Gestaltung.[881] Welche organisatorischen und technischen Maßnahmen der oder die Verantwortliche konkret treffen muss, ist kontext-, risiko- und kostenabhängig und gibt dem oder der Verantwortlichen einen entsprechend weiten Entscheidungsspielraum.[882]

Dem Art. 25 DS-GVO zugeordnet ist Erwägungsgrund 78, der sich thematisch allerdings überwiegend mit Absatz 1 auseinandersetzt.[883] So können laut Erwägungsgrund 78 S. 3 geeignete technische Maßnahmen etwa „*unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern*".

Durch **Abs. 2 des Art. 25 DS-GVO** wird der oder die Verantwortliche verpflichtet durch geeignete technische und organisatorische Maßnahmen sicherzustellen, „*dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden*". Dies entspricht dem im Datenschutzrecht allgegenwärtigen Grundsatz der Erforderlichkeit.[884] Der oder die Verantwortliche muss demensprechend dem Grundsatz der Datenminimierung aus Art. 5 DS-GVO durch Abs. 2 Folge leisten.[885]

---

[876] Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 25 Rn 9.*
[877] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 25 Rn 59.*
[878] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 25 Rn 4.*
[879] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 25 Rn 34.*
[880] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 25 Rn 10.*
[881] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 25 Rn 28.*
[882] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 25 Rn 36.*
[883] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 25 Rn 2.*
[884] Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 25 Rn 9.*
[885] Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar Art. 25 Rn 49;* Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 25 Rn. 12.*

d) Kritik

Kritiker und Kritikerinnen bemängeln die unübersichtliche Ausgestaltung des Art. 32 I DS-GVO, da die dort aufgezählten Maßnahmen weder aufeinander abgestimmt noch abschließend sind und zudem noch von anderen Artikeln der DS-GVO ergänzt werden müssen.[886] Allgemein bieten Art. 32 und 25 DS-GVO wenige konkrete Anhaltspunkte, die Ausgestaltung der Datensicherheit bleibt letztendlich eine Entscheidung des oder der Verantwortlichen. Dies ermöglicht zwar eine enorme Flexibilität, führt allerdings auch zu Unsicherheiten bei der Auswahl der Maßnahmen.[887] Es fehle an klaren Vorgaben bezüglich Leistungsanforderungen, Produkten, Konzeption und Gestaltung. Einzig die Bußgelddrohungen des Art. 83 IV und V DS-GVO würden den Artikeln zur Datensicherheit ein Gewicht geben.[888]

Eine Möglichkeit, um zumindest branchenspezifische konkrete Verhaltensregeln für die Datensicherheit zu generieren, stellt Art. 40 DS-GVO dar. Hiernach können laut Art. 40 II DS-GVO „*Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln ausarbeiten oder ändern oder erweitern*“. Dies gilt laut Nr. h auch für „*die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32*“.

e) Datensicherheit durch die Nutzung von Angriffserkennungssystemen

Die Nutzung von Angriffserkennungssystemen wie IDS oder SIEM-Systeme ist eine Maßnahme nach Stand der Technik, um ein Schutzniveau zu gewährleisten, wenn es um die in Art. 32 I lit. b DS-GVO aufgeführte „*Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen*“ geht. Dies deckt sich bezogen auf Krankenhäuser mit dem IT-Sicherheitsgesetz 2.0, das in der Ergänzung des § 8a BSIG um den Absatz Ia festlegt, dass der oder die Betreibende der Kritischen Infrastrukturen dazu verpflichtet werden, Systeme zur Angriffserkennung einzusetzen.

Privatrechtlich organisierte Krankenhäuser sollten Angriffserkennungssysteme nutzen, um dem geforderten Schutzniveau der Art. 24, 25 und 32 DS-GVO Genüge zu tun. Es gilt jedoch im jeweiligen Einzelfall eine Risikoabwägung, insbesondere für die Rechte und Freiheiten natürlicher Personen, durchzuführen.

Die Artikel der DS-GVO zur Datensicherheit haben jedoch keinen Einfluss auf die Rechtmäßigkeit der Datenverarbeitung. Diese richtet sich ausschließlich nach den Grundsätzen der Datenverarbeitung aus Art. 5 und den Erlaubnistatbeständen aus Art. 6 I DS-GVO. Auch wenn

---

[886] Schneider, *Datenschutz nach der EU-Datenschutz-Grundverordnung, S. 264.*
[887] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Kap. 2 Rn 34, 35.*
[888] Schneider, *Datenschutz nach der EU-Datenschutz-Grundverordnung, S. 212.*

sich aus Art. 24, 25 und 32 DS-GVO schließen lässt, dass Krankenhäuser Angriffserkennungssysteme nutzen sollten oder sogar müssten, um den dort geforderten Sicherheitsmaßstäben gerecht zu werden, ist dies keine Rechtfertigung für die Nutzung an sich.

E. Zusammenfassung

Der Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft kann grundsätzlich – wenn auch mit Rechtsunsicherheiten – über Art. 6 I 1 lit. c DS-GVO i.V.m. § 75c I SGB V gerechtfertigt werden. Werden jedoch besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO hierbei verarbeitet, fehlt es an einer Ermächtigungsgrundlage. Somit besteht jetzigen Stand der Gesetzgebung keine umfassende Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft.

Die fehlende Erlaubnisgrundlage steht im Kontrast zu den technischen Vorgaben des Art. 32 DS-GVO. Werden keine geeigneten technischen und organisatorischen Maßnahmen zum Schutze der Datenverarbeitung getroffen, drohen den Krankenhausbetreibenden Sanktionen nach den Art. 82 ff DS-GVO. Kommen sie den technischen Anforderungen des Art. 32 DS-GVO nach, verarbeiten sie wiederum personenbezogene Daten, ohne hierfür ermächtigt zu sein, und riskieren ebenfalls Sanktionen. Um diesen Zwiespalt lösen zu können, bedarf es einer verlässlichen Ermächtigungsgrundlage, wonach Krankenhäuser nach Art. 6 und 9 DS-GVO Angriffserkennungssysteme installieren und betreiben dürfen.

Im Folgenden wird aus den Erkenntnissen der vorangegangenen Kapitel und anhand beispielhafter Vergleiche der rechtlichen Situation in ähnlicher Fallkonstellationen eine Gestaltungsmöglichkeit für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft entwickelt.

VII. Gestaltung einer spezifischen nationalen Bestimmung

Da nach der aktuellen Rechtslage keine umfassende Rechtfertigung für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft besteht, wird in diesem Kapitel der Untersuchung eine Möglichkeit für eine umfassende Ermächtigungsgrundlage vorgestellt. Diese beruht auf § 75c SGB V, der entsprechend novelliert wird. Für die Novellierung werden zwei Beispiele für eine Rechtfertigung der Nutzung von Angriffserkennungssystemen aus anderen Einsatzbereich herangezogen, die im Folgenden vorgestellt werden. Anschließend folgt der Entwurf der Novellierung des § 75c SGB V-E mit einer Erläuterung der Änderungen und Anpassungen. Zudem wird die Novellierung des § 75c SGB V-E auf die verfassungs- und datenschutzrechtliche Vereinbarkeit geprüft.

A. Beispiele aus bereits bestehenden Regelungen

Auf Landesebene werden im Folgenden die sehr detaillierten Regelungen zur Informationssicherheit in Landesbehörden nach dem Niedersächsischen Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) vorgestellt. Als Pendant hierzu folgt auf Bundesebene der allgemeinere Erlaubnistatbestand des § 5 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), welcher die Befugnisse des Bundesamtes zur Abwehr von Cyber-Angriffen regelt.

1. Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit (NDIG)

Nicht nur in der Gesundheitsversorgung, sondern auch in der Exekutive schreitet die Digitalisierung voran und mit ihr die vermehrte Nutzung von IT-Systemen. Angriffe auf die Infrastrukturen der öffentlichen Verwaltung mehren sich und werden komplexer, auch steigt die Professionalität dieser Angriffe. Um die Funktionsfähigkeit der Exekutive zu gewährleisten und die Daten der Bürger und Bürgerinnen schützen zu können, bedarf es der Implementierung von Anwendungen, die die IT-Sicherheit der Netzwerke schützen.[889]

Ein Beispiel hierfür enthält das Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit (NDIG). Es wurde vom Niedersächsischen Landtag am 23. Oktober 2019 verabschiedet und beinhalten im dritten Teil umfassende Regelungen zur Informationssicherheit. Schwerpunkt ist hierbei eine Rechtsgrundlage „für den Einsatz einer geeigneten Sensorik zur Abwehr von Angriffen auf die IT-Infrastruktur des Landes".[890]

Laut **§ 19 I 1 NDIG** kann jede Behörde „*auf den von ihr betriebenen, mit dem Landesdatennetz verbundenen IT-Systemen die dort zum Erkennen und Nachverfolgen von Auffälligkeiten gespeicherten personenbezogenen Daten nach Maßgabe der Sätze 2 und 3 automatisiert auswerten, soweit dies zu dem Zweck, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren, erforderlich ist*." Dies bedeutet eine Zweckänderung der Datenverarbeitung, mit der der Umgang mit bereits erhobenen Daten geregelt wird. Die in Rede stehenden Daten sind zuvor im Rahmen der Tätigkeit der Behörden auf gesonderten Ermächtigungsgrundlagen für entsprechende festgesetzte Zwecke erhoben und in den Netzwerken der Behörden verarbeitet wurden. Bei den Daten handelt es sich abschließend die automatisierte Ereignisdokumentationen. Hierfür dürfen nach Satz 3 die Daten zusammengeführt und gemeinsam verarbeitet werden. Unter den Begriff der „automatisierten Ereignisdokumentation" fallen die Protokolldaten, die in Protokolldateien automatisch abgelegt

[889] Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 36.*
[890] Niedersächsisches Ministerium für Inneres und Sport, *NDIG und OZG: Rechtsrahmen für die digitale Verwaltung in Niedersachsen.*

werden. Diese werden auch „log files“ genannt.[891] So nimmt beispielsweise bei Webservern eine spezielle Software wie der Apache HTTP Server Anfragen der Nutzer entgegen und verarbeitet und beantwortet diese. Über diese Tätigkeiten wird standardgemäß von der Software ein Ereignisprotokoll geführt, das „log file“.[892]

Die Erlaubnisnorm für die Verarbeitung der Daten aus der automatisierten Ereignisdokumentation stellt **§ 19 II 2 NDIG** dar. Nach Satz 1 kann jede Behörde „*an den von ihr betriebenen, mit dem Landesdatennetz verbundenen Übergabe- und Knotenpunkt*“ nach auffälligem Datenverkehr suchen, solange dies für den in Absatz 1 formulierten Zweck erforderlich ist. Hierfür darf nach Satz 2 der an den Übergabe- und Knotenpunkten anfallende personenbezogene Datenverkehr „*automatisiert erhoben, entschlüsselt und unverzüglich automatisiert ausgewertet werden*“. Übergabe- und Knotenpunkte sind „IT-Systeme, die den Datenverkehr mit einem anderen Netz sicherstellen oder ihn innerhalb des eigenen Netzes verteilen“[893], was in der Praxis eine flächendeckende Verarbeitungserlaubnis des Datenverkehrs eines Netzwerkes zum Zwecke der Gefahrenabwehr bedeutet. Die Erlaubnisnorm des § 19 II 2 NDIG gilt zudem auch für die beiden Eskalationsstufen der §§ 20 und 21 NDIG.

Absatz 3 des § 19 NDIG schränkt Absatz 1 und 2 dergestalt ein, dass die Auswertung der kommunikativen Bedeutung von Inhaltsdaten unzulässig ist. Eine Auswertung dieser ist nur nach den strengeren Voraussetzungen des § 21 NDIG möglich.

§ 19 IV 1 NDIG verkörpert den Grundsatz der Speicherbegrenzung aus Art. 5 DS-GVO und gibt vor, dass die „*nach Absatz 1 oder 2 erhobenen und ausgewerteten Daten sowie die Auswertungsergebnisse unverzüglich zu löschen*“ sind, wenn „*die Auswertung nach Absatz 1 oder 2 keine zureichenden tatsächlichen Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit*“ ergibt, wobei die ursprünglichen Daten zum ursprünglichen Verwendungszweck gemäß Satz 2 weiterhin gespeichert und verarbeitet werden dürfen.

In §§ 20 und 21 NDIG werden erweiterte Auswertungsoptionen als zweite und dritte Eskalationsstufen festgelegt.[894] So eröffnet **§ 20 I 1 NDIG** als zweite Eskalationsstufe die Möglichkeit, bei „*zureichenden tatsächlichen Anhaltspunkten für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit*“ die erhobene und ausgewerteten Daten – mit der Ausnahme von Inhaltsdaten – sowie die Auswertungsergebnisse zusammenzuführen und für maximal 30 Tage zu speichern. In diesem Zeitraum dürfen die gespeicherten Daten „*weiter einzelfallbezogen automatisiert auswerten, soweit dies zur Erkennung oder Abwehr der Gefahr erforderlich ist*“. Der an die StPO angelehnte Begriff des

[891] Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 41.*
[892] Auer-Reinsdorff/Conrad, *Handbuch IT- und Datenschutzrecht§ 36 Rn 125.*
[893] Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 41.*
[894] Miller, *NdsVBl 2021, 1 (3).*

„zureichenden tatsächlichen Anhaltspunktes“ meint hierbei einen Anfangsverdacht für eine Gefahr für die IT-Sicherheit. Dieser Anfangsverdacht liegt vor, wenn die Gefahr zumindest möglich erscheint.[895] Ergibt die Auswertung nach § 20 I 1 NDIG keine „*hinreichenden tatsächlichen Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit*“, so sind die gespeicherten Daten sowie die Auswertungsergebnisse nach Satz 3 unverzüglich zu löschen. Im Vergleich zu „zureichenden tatsächlichen Anhaltspunkten“ liegen „hinreichende tatsächliche Anhaltspunkte“ vor, wenn die Wahrscheinlichkeit höher ist, dass eine Gefahr vorliegt, als dass keine vorliegt.[896] An die hinreichenden Anhaltspunkte sind folglich strengere Maßstäbe zu setzen, als an die zureichenden Anhaltspunkte.

Liegen „*hinreichende tatsächliche Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit*“ vor, so greift die dritte Eskalationsstufe und die Daten gemäß Absatz 1 dürfen laut **§ 20 II 1 NDIG** über die in Absatz 1 angegebene 30-Tages-Frist hinaus gespeichert und zudem auch nicht automatisiert ausgewertet werden. Hierfür bedarf es nach Satz 2 jedoch der Anordnung der Behördenleitung. § 20 II 4 NDIG regelt zudem den Umgang mit „Beifang“, also mit tatsächlichen Anhaltspunkten für weitere Gefahren für die IT-Sicherheit, die sich erst im Laufe der Auswertung nach Satz 1 ergeben haben. Diese dürfen sodann auch nach den Vorgaben des § 20 II 1 NDIG und unter dem Vorbehalt der Anordnung durch die Behördenleitung verarbeitet werden, also über die 30 Tages-Frist hinaus und zudem auch nicht automatisiert.

§ 21 NDIG regelt die Verarbeitung von Inhaltsdaten parallel zu den Eskalationsstufen des § 20 NDIG. Dabei setzen die Ermächtigungen der Vorschrift nicht voraus, dass zuvor der § 20 erfolgreich durchlaufen werden muss. So kann die Behörde als zweite Eskalationsstufe zu § 19 NDIG gemäß **§ 21 I 1 NDIG** auch Inhaltsdaten und Auswertungsergebnisse maximal 30 Tage speichern und in dieser Zeit einzelfallbezogen und automatisiert auswerten, wenn „*zureichende tatsächliche Anhaltspunkte dafür {bestehen}, dass die ausgewerteten Inhaltsdaten zur Erkennung oder Abwehr einer durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachten Gefahr für die IT-Sicherheit erforderlich sind*“. Eine Auswertung der kommunikativen Bedeutung der Inhaltsdaten ist jedoch weiterhin unzulässig. Im Vergleich zu § 20 II 2 NDIG bedarf es hier nicht einer Anordnung, sondern nach § 21 I 3 NDIG der unverzüglichen nachträglichen Genehmigung der Behördenleitung. Liegt diese nicht vor oder ergibt die Auswertung nach Satz 1 keine hinreichenden tatsächlichen Anhaltspunkte für eine Gefahr für die IT-Sicherheit, sind die gespeicherten Inhaltsdaten sowie die Ergebnisse der Auswertung nach Satz 5 und 6 unverzüglich zu löschen.

---

[895] Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 42.*
[896] Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 42.*

Ergeben sich jedoch „*hinreichende tatsächliche Anhaltspunkte*“ für die Erforderlichkeit der Auswertung von Inhaltsdaten, so dürfen die Daten gemäß **§ 21 II 1 NDIG** i.S.d. dritten Eskalationsstufe länger als 30 Tage gespeichert werden und auch nicht automatisiert ausgewertet werden. Hierfür ist jedoch gemäß Satz 2 die Anordnung der Behördenleitung nötig. Ergibt sich bei der Auswertung nach § 21 II 1 NDIG eine andere Gefahr für die IT-Sicherheit („Beifang“), so dürfen nach Satz 4 die Daten für die Erkennung oder Abwehr dieser Gefahr ebenfalls nach den Maßgaben des Satz 1 und unter dem Vorbehalt der Anordnung der Behördenleitung (Satz 2 und 3) ausgewertet werden.

Eine weitere Einschränkung findet sich in **§ 21 IV 1 NDIG**. Hiernach dürfen Daten, die „*dem Kernbereich privater Lebensgestaltung oder besonderen Kategorien personenbezogener Daten (Artikel 9 der Datenschutz-Grundverordnung) zuzurechnen {sind} oder geeignet {sind}, die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen*“ nicht gespeichert, verändert, genutzt oder übermittelt werden und sind unverzüglich zu löschen.

Gemäß **§ 23 I NDIG** kann jede Behörde „*den nach § 19 Abs. 2 erhobenen Datenverkehr zu dem Zweck, durch Schadprogramme oder Angriffe verursachte, im Hinblick auf das Ausmaß des zu erwartenden Schadens und die Wahrscheinlichkeit des Schadenseintritts erhöhte Gefahren für die IT-Sicherheit im gesamten Landesdatennetz (dringende Gefahren für die IT-Sicherheit) abzuwehren, automatisiert speichern*“. Die Daten sind, wenn möglich, zu verschlüsseln und nach 30 Tagen zu löschen. Ist es zur Abwehr einer dringenden Gefahr für die IT-Sicherheit unerlässlich, dürfen die gespeicherten Daten nach § 23 II NDIG automatisiert und nicht automatisiert ausgewertet und länger als 30 Tage gespeichert werden. Hierfür bedarf es nach Absatz 3 jedoch der Anordnung des Amtsgerichts, in dessen Bezirk die Behörde ihren Sitz hat.

Die Speicherung ist notwendig, da sonst nicht überprüft werden kann, ob mögliche Angriffe stattgefunden, aber unerkannt geblieben sind. Bei Angriffswellen, wie mit dem Schadprogramm „Emotet“, das ab 2018 in kürzester Zeit Kliniken, Gerichte, Universitäten und Stadtverwaltungen lahmlegte und gegen das herkömmliche Virenscanner weitgehend wirkungslos waren[897], ist es gerade in der öffentlichen Verwaltung von dringender Wichtigkeit prüfen zu können, ob die Systeme ebenfalls infiltriert wurden. Dies kann bei der Echtzeiterkennung mit anschließender Löschpflicht nach § 19 II – IV NDIG jedoch nicht mehr geprüft werden, weswegen § 23 NDIG die begrenzte Speicherung unter verschärften Voraussetzungen zulässt.

§ 25 NDIG stellt zudem besonders hohe Anforderungen an die Datensicherheit der nach den §§ 18 bis 23 NDIG verarbeiteten Daten sowie deren Auswertungsergebnisse und formuliert in Absatz 2 einen nicht abgeschlossenen Anforderungskatalog. Zudem ist nach Absatz 4 jeder Zugriff auf die Daten zu protokollieren.

Mit Blick auf den Untersuchungsgegenstand ist festzustellen, dass der Adressat des NDIG die öffentliche Verwaltung ist und privatrechtlich organisierte Unternehmen, wie ein Krankenhaus

[897] Wölbert*, c’t 2020, 14 (14).*

in privater Trägerschaft, nicht umfasst sind.[898] Da aufgrund der unmittelbaren Bindung der öffentliche Verwaltung an die Grundrechte ein strenger Maßstab an die Rechtfertigung von Eingriffen zu setzen ist, kann sich bei der Formulierung einer Rechtfertigungsnorm bezogen auf Krankenhäuser gut an den Regelungen des NDIG orientiert werden.

2. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes und für die Gestaltung einer sicheren Digitalisierung in Deutschland zuständig. Die rechtliche Grundlage der Arbeit des BSI ist im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) verankert, dass 2009 in Kraft trat und seitdem mehrmals novelliert wurde. Das BSI ist zuständig für den Schutz der Regierungsnetze und die Sicherung zentraler Netzübergänge. Zudem ist das BSI die zentrale Meldestelle für IT-Sicherheit innerhalb der Bundesverwaltung.[899]

§ 5 BSIG ermächtigt das Bundesamt für Sicherheit in der Informationstechnik zu Protokollierungs- und Überwachungsmaßnahmen im Bereich der Kommunikationstechnik der Bundesverwaltung, um Gefahren für die Kommunikationstechnik des Bundes abzuwehren und wird im Folgenden vorgestellt.

Gemäß **§ 5 I BSIG** darf das Bundesamt für Sicherheit in der Informationstechnik (BSI) „*zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist*“. Nach der Legaldefinition des § 2 Nr. 8 S. 1 BSIG sind Protokolldaten „*Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind*“. Weiterhin darf das BSI „*die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist*“. Hiervon sind auch Inhaltsdaten umfasst. Die automatisierte Auswertung der Daten hat hierbei unverzüglich zu erfolgen und die Daten sind im Anschluss sofort zu löschen.

Bestehen tatsächlich Anhaltspunkte, dass personenbezogene Daten über ein Schadprogramm übermittelt wurden und müssen Protokolldaten zur Abwehr der Gefahr beziehungsweise zur Erkennung weiterer Schadprogramme automatisiert ausgewertet werden, so greift die

[898] Zickler, *NordOer 2020, 441 (441).*
[899] BSI, *Auftrag des BSI.*

Verlängerungsoption des Verarbeitungszeitraumes des Absatz 1 nach **§ 5 II BSIG**. Hiernach dürfen die Protokolldaten bis zu 18 Monate gespeichert werden. Es muss sichergestellt werden, dass die Daten ausschließlich automatisiert ausgewertet werden können. Wenn möglich, sind die gespeicherten Daten automatisiert zu pseudonymisieren.

§ 5 III BSIG weitet den Verwendungszweck der Absätze 1 und 2 dahingehend aus, dass die Verwendung personenbezogener Daten auch dann zulässig ist, wenn ein auf bestimmte Tatsachen begründetet Verdacht vorliegt, dass „*diese ein Schadprogramm enthalten, diese durch ein Schadprogramm übermittelt wurden oder sich aus ihnen Hinweise auf ein Schadprogramm ergeben können, und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen*". Bestätigt sich dieser Verdacht, dürfen die personenbezogenen Daten weiterhin verarbeitet werden, wenn dies „*zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist*".

§ 5 IV BSIG regelt die Benachrichtigungspflicht der Beteiligten im Falle eines Abwehrvorganges von Schadprogrammen oder vergleichbaren Gefahren, wohingegen **§ 5 V BSIG** die Übermittelung der nach Absatz 3 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden regelt. Die Daten können zudem gemäß **§ 5 VI BSIG** für sonstige Zwecke an die Strafverfolgungsbehörden, die Polizeien des Bundes und der Länder, die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst und an den Bundesnachrichtendienst unter bestimmten Bedingungen übermittelt werden.

„*Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte*" ist nach **§ 5 VII BSIG** nicht zulässig. Zudem dürfen Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des Artikels 9 I DS-GVO, die bei der automatisierten Auswertung erlangt werden, nicht verwendet werden und sind unverzüglich zu löschen. Zudem ist die Tatsache der Erlangung und Löschung dieser Daten zu dokumentieren.

Vor der Aufnahme der Datenerhebung und -verwendung hat das Bundesamt nach **§ 5 VIII BSIG** ein Datenerhebungs- und -verwendungskonzept zu erstellen.

§ 5 BSIG enthält eine Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen für öffentliche Stellen, namentlich mit dem BSI als einzigem Adressaten. Im Vergleich zum NDIG ist das BSIG sehr stark auf die Verhältnisse der Bundesverwaltung und Beschaffenheit der dortigen IT abgestellt. Zudem ist das Eskalationsmodell des NDIG im Hinblick auf einen kontrollierbaren stufenweisen Eingriff in die betroffenen Grundrechte klarer und für den Untersuchungsgegenstand anwendbarer.

Die Regelungen des NDIG gehen in Umfang und Detailschärfe weit über die Bundesregelungen des § 5 BSIG hinaus. Mit den Vorschriften des NDIG hat der Gesetzgeber „die ihm von der Verfassung gesetzten Grenzen weitestgehend eingehalten“.[900]

B. Implikationen für den Gesetzgeber

Die im Rahmen dieser Untersuchung festgestellten Unzulänglichkeiten in Bezug auf die Rechtfertigung des Einsatzes von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft zeigen auf, dass ein gesetzgeberischer Novellierungsbedarf besteht. Im Folgenden wird § 75c SGB V angepasst, um Regelungslücken zu schließen. Als Beispiel und Vorlage dienen hierzu die bereits bestehenden Normen aus dem NDIG sowie § 5 BSIG. Die Novellierungen werden im Anschluss begründet und auf ihre verfassungs- sowie datenschutzrechtliche Vereinbarkeit geprüft.

1. Novellierung des § 75c SGB V-E – IT-Sicherheit in Krankenhäusern

(1) [1]Ab dem (Zeitpunkt) sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind, zu treffen. [2]Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. [3]Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.

(1a) Die angemessenen organisatorischen und technischen Vorkehrungen nach Absatz 1 Satz 1 umfassen auch den Einsatz von Systemen zur Angriffserkennung nach § 8a Absatz 1a des BSI-Gesetzes.

(1b) Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

[900] Miller, *NdsVBl 2021, 1, 13 (1).*

(1c) Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.

(2) [1]Krankenhäuser können auf denen von ihnen betriebenen IT-Systemen die dort zum Erkennen und Nachverfolgen von Auffälligkeiten gespeicherten personenbezogenen Daten nach Maßgabe der Sätze 2 und 3 automatisiert auswerten, soweit dies zu dem Zweck, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren, erforderlich ist. [2]Für die Auswertung nach Satz 1 dürfen ausschließlich die automatisierten Ereignisdokumentationen herangezogen werden. [3]Zum Zweck der Auswertung dürfen die in Satz 2 genannten Daten zusammengeführt und gemeinsam verarbeitet werden.

(2a) [1]Krankenhäuser dürfen den an den Übergabe- und Knotenpunkten der von ihnen betriebenen Datennetze anfallenden personenbezogenen Datenverkehr automatisiert erheben, entschlüsseln und unverzüglich automatisiert auswerten, soweit dies zu dem Zweck, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren, erforderlich ist. [2]Sämtliche Verantwortliche müssen dem Sozialgeheimnis nach § 35 Absatz 1 Erstes Buch Sozialgesetzbuch oder § 80 Zehntes Buch Sozialgesetzbuch oder einem sonstigen Berufsgeheimnis im Sinne des Artikel 9 Absatz 3 der Verordnung (EU) 2016/679 unterliegen.

(2b) [1]Ergibt die automatisierte Auswertung nach Absatz 2 Satz 1 oder Absatz 2a Satz 1 keine zureichenden tatsächlichen Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahren für die IT-Sicherheit, so sind die hierfür erhobenen und ausgewerteten Daten sowie die Auswertungsergebnisse unverzüglich zu löschen. [2]Die Speicherung und sonstige Verarbeitung der ausgewerteten Daten nach dem ursprünglichen Verwendungszweck bleiben von Satz 1 unberührt.

(2c) [1]Ergibt die automatisierte Auswertung nach Absatz 2 Satz 1 oder Absatz 2a Satz 1 zureichende tatsächliche Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahren für die IT-Sicherheit, so kann das Krankenhaus die erhobenen und ausgewerteten Daten sowie die Auswertungsergebnisse zusammenführen, höchstens 30 Tage speichern und in dieser Zeitspanne weiter einzelfallbezogen automatisiert auswerten, soweit dies zur Erkennung oder Abwehr der Gefahr erforderlich ist. [2]Soweit es sich um die Speicherung von Inhaltsdaten handelt, bedarf es der unverzüglichen Genehmigung des Verantwortlichen im Sinne des Artikel 4 Nummer 7 der Verordnung (EU) 2016/679. [3]Die nach Satz 1 gespeicherten Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym sind. [4]Ergibt die Auswertung nach Satz 1 keine hinreichenden tatsächlichen Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so sind die gespeicherten Daten sowie die Auswertungsergebnisse unverzüglich zu löschen.

(2d) [1]Ergibt die automatisierte Auswertung nach Absatz 2 Satz 1 oder Absatz 2a Satz 1 oder eine weitere automatisierte Auswertung nach Absatz 2c Satz 1 hinreichende tatsächliche Anhaltspunkte für eine durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahren für die IT-Sicherheit, so dürfen die Daten über den Ablauf der in Absatz 2c Satz 1 bestimmten Frist hinaus gespeichert, auch nicht automatisiert ausgewertet und entpseudonymisiert werden, soweit und solange dies zur Erkennung oder Abwehr der Gefahr erforderlich ist. [2]Hierzu bedarf es der vorherigen Zustimmung des Verantwortlichen im Sinne des Artikel 4 Nummer 7 der Verordnung (EU) 2016/679. [3]Ergibt die Auswertung nach Satz 1 tatsächliche Anhaltspunkte für eine andere durch eine Sicherheitslücke, ein Schadprogramm oder einen Angriff verursachte Gefahr für die IT-Sicherheit, so dürfen die Daten auch gespeichert und nicht automatisiert ausgewertet werden, soweit und solange dies zur Erkennung oder Abwehr der anderen Gefahr erforderlich ist.

(2e) [1]Werden nach Absatz 2, 2a oder 2c Inhalte einer Telekommunikation (Inhaltsdaten) verarbeitet, so ist die Auswertung ihrer kommunikativen Bedeutung unzulässig. [2]Werden aufgrund der Maßnahmen des Absatzes 1 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 erlangt, dürfen diese nicht verwendet werden. [3]Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. [4]Dies gilt auch in Zweifelsfällen. [5]Die Tatsache, dass in den Sätzen 1 und 2 genannte Daten ausgewertet wurden, und die Löschung dieser Daten sind zu dokumentieren. [6]Die in der Dokumentation enthaltenen Daten dürfen ausschließlich zur Datenschutzkontrolle verwendet werden.

(3) [1]Die nach den Absätzen 2 bis 2e verarbeiteten Daten sowie die Auswertungsergebnisse sind durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme, Veränderung und Verwendung zu schützen. [2]Bei der Umsetzung dieser Maßnahmen ist ein besonders hohes Maß an Datensicherheit zu gewährleisten. [3]Insbesondere

1. sind der Zutritt zu den und der Zugriff auf die Datenverarbeitungsanlagen auf Personen zu beschränken, die durch den jeweiligen Krankenhausbetreiber hierzu besonders ermächtigt sind,

2. ist organisatorisch sicherzustellen, dass eine Kenntnisnahme der nach den Absätzen 2 bis 2e verarbeiteten Daten sowie der Auswertungsergebnisse durch andere als die nach Nummer 1 ermächtigten Personen ausgeschlossen ist,

3. ist sicherzustellen, dass die für Datenverarbeitung nach den Absätzen 2 bis 2e verwendeten IT-Systeme von den für die üblichen betrieblichen Aufgaben verwendeten IT-Systemen getrennt sind, insbesondere die Speicherung in gesonderten Speichereinrichtungen erfolgt,

4. sind besondere Sicherungsmaßnahmen gegen den unberechtigten Zugriff aus anderen Netzen, insbesondere aus dem Internet, zu treffen,

5. sind nach dem Stand der Technik als besonders sicher geltende Verschlüsselungsverfahren zur Gewährleistung der Vertraulichkeit der gespeicherten Daten einzusetzen und

6. ist technisch und organisatorisch sicherzustellen, dass der Zugriff auf die Daten nur gemeinsam durch mindestens zwei nach Nummer 1 ermächtigte Personen erfolgen kann.

(4) [1]Krankenhäuser dürfen von den Ermächtigungen der §§ 2 bis 2d nur Gebrauch machen, wenn sie ein Sicherheitskonzept für die dazu eingesetzten technischen Systeme erstellt und die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen aktenkundig gemacht haben. [2]Das Sicherheitskonzept ist alle zwei Jahre einer Revision zu unterziehen. [3]Für jede Veränderung der eingesetzten technischen Systeme gilt Satz 1 entsprechend.

(5) [1]Jeder Zugriff, insbesondere das Lesen, Kopieren, Ändern, Übermitteln, Löschen und Sperren von nach den Absätzen 2 bis 2e verarbeiteten Daten sowie von Auswertungsergebnissen ist zu protokollieren. [2]Das Protokoll enthält Zeitpunkt, Art und Zweck des Zugriffs sowie eine eindeutige Kennung der auf die Daten zugreifenden Person. [3]Das Protokoll darf ausschließlich zur Datenschutzkontrolle verwendet werden. [4]Jeder Eintrag in das Protokoll ist zwei Jahre nach seiner Aufnahme zu löschen.

(6) [1]Betroffene Personen sind spätestens nach dem Erkennen und der Abwehr einer Gefahr für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. [2]Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde, und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat.

2. Erläuterungen

Zu Absatz 1:

Absatz 1 entspricht der Originalfassung des § 75c I SGB V. Er umfasst die Verpflichtung zum Technikeinsatz, nicht jedoch die Ermächtigung zur Datenverarbeitung im Rahmen des Technikeinsatzes. § 75c I 1 SGB V regelt den Technikeinsatz zur „*Vermeidung von Störungen*“ für die klassischen und weitere, nicht aufgeführte Sicherheitsziele, auch etwa durch technische Fehler, Ausfälle, falsche Bemessung von Komponenten oder Fehlbedienungen. Dagegen führt die Novellierung ab Absatz 2 eine klarer begrenzte Zweckbindung ein, um Daten im Rahmen einer Zweckänderung (Absatz 2) bzw. Ermächtigung (Absätze 2a bis 2d) verarbeiten zu dürfen, soweit dies zu dem Zweck, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren, erforderlich ist. Diese Änderung entspricht auch der Tatsache, dass Angriffserkennungssysteme nicht erst zur Vermeidung oder Beseitigung von Störungen eingesetzt werden, sondern bereits zur Ermittlung von Gefahren, die zu einer Störung durch Angriffe, Schadprogramme oder Sicherheitslücken führen können.

Zu Absatz 1a:

Da § 75c SGB V in seiner Originalfassung bereits in Absatz 2 auf § 8a BSIG verweist und dieser in Absatz 1a festlegt, dass auch Angriffserkennungssysteme zu den organisatorischen und technischen Maßnahmen explizit gehören, ist es zum Erreichen eines Mindestsicherheitsstandards nötig, die Nähe zu den Regelungen des BSIG auch im Bereich der Angriffserkennung aufzuzeigen.

Zu Absatz 1b:

Absatz 1b ist die Originalfassung des Absatz 2 des § 75c SGB V.

Zu Absatz 1c:

Absatz 1c ist die Originalfassung des Absatz 3 des § 75c SGB V.

Zu Absatz 2:

Bei Absatz 2 handelt es sich um eine Zweckänderungsnorm, die es zulässt, dass bereits gespeicherte Datenbestände ausgewertet werden können. Für § 75c SGB V besteht zwar eine Zweckänderungsnorm in § 67c II Nr. 1 SGB X, die wohl über die Öffnungsklauseln der Art. 6 I 1 lit. c und e i.V.m. Art. 9 II lit. beziehungsweise h sowie j DS-GVO beziehungsweise Art. 6 IV DS-GVO neben dem europäischen Datenschutzrecht bestehen kann, jedoch ist diese sehr allgemein gehalten (*siehe VI.C.2.c)(6)(a) Verstoß gegen den Grundsatz der Zweckbindung?*). Um dem Grundsatz der Zweckbindung Genüge zu tun, wurde für die Weiterverarbeitung der Daten nach § 75 c SGB V eine entsprechende und klar begrenzte Zweckänderung formuliert. Um die Übersichtlichkeit in der Normfülle des Sozialgesetzbuches nicht zu verlieren wurde diese ebenfalls in § 75 c SGB V verortet und nicht im SGB X.

Die Zwecksetzung für die Weiterverarbeitung in Absatz 2 unterscheidet sich von der Zwecksetzung für die Maßnahmenverpflichtung aus Absatz 1. Absatz 2 orientiert sich an § 19 I 1 NDIG und begrenzt den Verarbeitungszweck auf die Abwehr von Gefahren für die IT-Sicherheit. Zudem erfährt die Zweckänderung in Satz 2 und 3 klare Grenzen. Der Zweck für die Datenweiterverarbeitung nach Absatz 2 ist gegenüber dem Zweck für die Maßnahmenbereitstellung nach Absatz 1 strenger ausgelegt, da an eine Zweckänderung zur Weiterverarbeitung engere Voraussetzungen zu stellen sind, als an eine primäre Zwecksetzung. Während der Zweck für die Maßnahmenverpflichtung auch organisatorische Maßnahmen zur Verhinderung von beispielsweise Mängeln in der Systemadministration, Ausbildungsdefizite, Personalmangel oder Managementdefizite umfasst, geht es bei der Zweckänderung zur Datenweiterverarbeitung in Absatz 2 ausschließlich um Gefahren, die durch Sicherheitslücken, Schadprogramme und Angriffe entstehen und somit in den Einsatzbereich von Angriffserkennungssystemen fallen.

Bei der Auslegung des Begriffes IT-Sicherheit folgt die Novellierung der Legaldefinition aus § 1 Nr. 7 NDIG, wonach IT-Sicherheit „*die Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten*“ darstellt.

Zu Absatz 2a:

Während Absatz 2 die automatisierte Auswertung bestimmter bereits erhobener und gespeicherter Daten regelt, dient Absatz 2a dazu, eine Rechtsgrundlage zu schaffen, um den Datenverkehr in den Netzwerken von Krankenhäusern durch Angriffserkennungssysteme durchsuchen zu können. Bisher stellt § 75c SGB V eine reine Verpflichtungsnorm und keine Erlaubnisnorm dar (*siehe VI.C.2.c) Die Erfüllung einer rechtlichen Verpflichtung nach Art. 6 I 1 lit. c DS-GVO*). Die Erlaubnis ist begrenzt auf die Übergabe- und Knotenpunkte der von dem jeweiligen Krankenhaus betriebenen Datennetze und schließt damit jedwede Durchsuchung von Datenverkehren außerhalb dieses Netzes aus. Ein vom Krankenhaus betriebenes Netz kann etwa über die Administration aktiver Netzkomponenten, die Vergabe von IP-Adressen und Routingregeln eingegrenzt werden. Die Durchsuchung und Auswertung des Datenverkehrs darf nur hinsichtlich vorhandener Sicherheitslücken, Schadprogrammen oder Angriffen zur Abwehr von Gefahren für die IT-Sicherheit erfolgen.

Satz 2 entspricht den Anforderungen des Art. 9 II lit. h, III DS-GVO, wonach Daten im Gesundheitsbereich nur von Fachpersonal oder Personen verarbeitet werden dürfen, die einem Berufsgeheimnis oder einer Geheimhaltungspflicht unterliegen. Gemäß Art. 9 III DS-GVO dürfen hierfür Rechtsgrundlagen in der Union oder den Mitgliedstaaten geschaffen werden, weswegen Absatz 2a Satz 2 neben der DS-GVO bestehen kann.

Zu Absatz 2b:

Da in § 75c SGB V bisher keine Vorgaben für Speicher- und Löschfristen gemacht wurden, wird in Absatz 2b – angelehnt an § 19 IV NDIG und § 5 I 2 BSIG – eine Pflicht zur unverzüglichen Löschung der verarbeiteten Daten sowie der daraus entstandenen Ergebnisse normiert, um den Anforderungen des Grundsatzes der Speicherbegrenzung gerecht zu werden.

Zu Absatz 2c:

Absatz 2c sowie 2d orientieren sich am Eskalationsstufenmodell der §§ 20 und 21 des NDIG. Da das Modell im NDIG systematisch sehr unübersichtlich gestaltet wurde mit vielen Querverweisen über mehrere Paragraphen, werden die Eskalationsregelungen zur Speicher- und Löschpflicht hier übersichtlicher in zwei aufeinanderfolgenden Absätzen gefasst.

Ergibt die Auswertung der Protokolldaten oder des Netzwerkverkehrs zureichende tatsächliche Anhaltspunkt für eine Gefahr für die IT-Sicherheit, so dürfen die entsprechenden Daten, mit den Auswertungsergebnissen nach Absatz 2c Satz 1 zusammengeführt, 30 Tage gespeichert und automatisiert verarbeitet werden. Bei der Speicherfrist wurde sich an die Vorgaben des NDIG gehalten, die sich von den Speicherfristen des BSIG (18 Monate) stark unterscheiden. Da im Zweifel das Mittel mit der geringeren Eingriffsintensität in die Grundrechte der Betroffenen zu wählen ist, sind hier 30 Tage als Speicherfrist festgesetzt wurden. Sind von der automatisierten Auswertung auch Inhaltsdaten umfasst, bedarf es gemäß Satz 2 aufgrund der erhöhten Eingriffsintensität einer Kontrollinstanz in Form einer unverzüglichen Genehmigung zur Verarbeitung vom jeweiligen Verantwortlichen i.S.d. DS-GVO. Da die erstmalige Aufzeichnung des verdächtigen Datenverkehrs in Echtzeit erfolgen muss, kann in dieser Vorschrift nicht mit

einer „vorherigen Zustimmung“ wie in Absatz 2d gearbeitet werden. Zudem ist durch den Verweis auf die Verantwortlichkeit nach den Maßgaben der DS-GVO den Ausführungen in Erwägungsgrund 74 Satz 1 der DS-GVO genüge getan, wonach die Verantwortung und Haftung geregelt werden sollte.

Zu Absatz 2d:

Absatz 2d erweitert die Verarbeitungserlaubnis in Fällen des hinreichenden Verdachtes für eine Gefahr auch auf die nicht automatisierte Verarbeitung und stellt die höchste Stufe des Eskalationsmodells dar. Da der Grundrechtseingriffes auf dieser Stufe am intensivsten ist, muss für die Verarbeitung nach Absatz 2d für sämtliche Daten, also auch für Nicht-Inhaltsdaten, eine vorherige Zustimmung des Verantwortlichen i.S.d. DS-GVO eingeholt werden.

Zudem enthält Absatz 2d in Satz 1 eine Sprungeskalation. Findet sich bei der Auswertung in der vorherigen Eskalationsstufe nach Absatz 2c Satz 1 hinreichende tatsächliche Anhaltspunkte für eine weitere Gefahr, so muss diesbezüglich nicht erneut das Eskalationsmodell in sämtlichen Abstufungen durchlaufen werden. Die betroffenen Maßnahmen können direkt nach den Maßgaben der Eskalationsstufe des Absatz 2d verarbeiten werden.

Der Auffangtatbestand zum „Beifang“ wurde in Absatz 2d Satz 3 aus dem NDIG übernommen.

Zu Absatz 2e:

Um das Fernmeldegeheimnis zu schützen, ist angelehnt an § 19 III NDIG die Auswertung der kommunikativen Bedeutung der erlangten Inhaltsdaten unzulässig. Zudem wird, angelehnt an § 5 VII BSIG, das Verbot der Datenverwendung auf Erkenntnisse aus dem Kernbereich privater Lebensgestaltung und Daten i.S.d. Art. 9 I DS-GVO ausgeweitet, da in den Netzwerken von Krankenhäusern genetische Daten sowie Gesundheitsdaten der Patienten und Patientinnen verarbeitet werden (*siehe VI.C.3.b) Datenkategorien*), die Schlüsse auf die private Lebensgestaltung von einzelnen Personen zulassen können.

Wurden entsprechende Daten doch ausgewertet, so ist im Sinne des Grundsatzes der Transparenz der Vorfall sowie die Löschung der Daten nach Satz 5 und 6 zu dokumentieren.

Zu Absatz 3:

Absatz 3 beinhaltet besondere Vorgaben zur Datensicherheit, die für die im Rahmen des Einsatzes von Angriffserkennungssystemen gespeicherten Daten sowie der Auswertungsergebnisse im Hinblick auf die Grundrechtseingriffe angewendet werden müssen. Die hier aufgeführten Maßnahmen stellen zusätzliche Sicherheitsbarrieren dar, die einen unzulässigen Eingriff in den Schutzbereich der tangierten Grundrechte verhindern sollen.

Zu Absatz 4:

Krankenhäuser sind nach Absatz 4 verpflichtet, ein Sicherheitskonzept auf Basis der bekannten Standards zu erstellen, in dem die Verantwortung nach der DS-GVO dokumentiert in Handlungen umgesetzt wird. Hier wurde sich an § 25 III NDIG orientiert.

Zu Absatz 5:

In diesem Absatz wird eine Protokollierungspflicht verankert, um den Grundsatz der Transparenz zu wahren.

Zu Absatz 6:

Angelehnt an § 5 IV BSIG beinhaltet Absatz 7 eine Benachrichtigungspflicht von betroffenen Personen.

3. Verfassungskonformität

Die Novellierung des § 75c SGB V-E muss mit der nationalen sowie unionsrechtlichen Verfassung konform sein.

a) Nationale Ebene

Die Verfassungskonformität setzt insbesondere voraus, dass die Novellierung des § 75c SGB V-E dem Verhältnismäßigkeitsgrundsatz genügt[901], da durch den Einsatz von Angriffserkennungssystemen in Krankenhäusern in das Fernmeldegeheimnis aus Art. 10 I GG sowie das Recht auf Informationelle Selbstbestimmung nach Art. 2 I i.V.m. Art. 1 I 1 GG eingegriffen wird (*siehe III.C Betroffene Grundrechte*). Dazu muss die Novellierung einem legitimen Zweck dienen, zur Erreichung des Gesetzeszweckes geeignet und erforderlich sowie verhältnismäßig i.e.S. sein.[902]

Die Novellierung des § 75 c SGB V beinhaltet zwei Zwecksetzungen. Während Absatz 1 den Zweck für die Implementierung organisatorischer und technischer Maßnahmen festsetzt, findet sich in Absatz 2 sowie 2a eine Zweckänderung zur Weiterverarbeitung von Daten durch Angriffserkennungssysteme.

Gemäß Absatz 1 der Novellierung haben Krankenhäuser zum Zweck der „*Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind,*“ entsprechende organisatorische und technische Vorkehrungen zu treffen. Wie bereits in der Einleitung dieser Untersuchung erörtert, sind in den vergangenen Jahren diverse Krankenhäuser in Deutschland Opfer von Angriffen geworden mit teils verheerenden Folgen (*siehe I.A Cyber-Angriffe auf Krankenhäuser*). Der Zweck des Absatz 1 der Novellierung besteht darin, durch die Installation von organisatorischen und technischen Vorkehrungen die Funktionsfähigkeit der Krankenhäuser zu gewährleisten und damit einhergehen die in den

[901] Maunz u. a., *GG – Kommentar Art. 10, Rn. 143, Art. 2, Rn. 130.*
[902] Gersdorf/Paal, *BeckOK Informations- und Medienrecht GG Art. 2 Rn 75.*

Netzwerken der Krankenhäuser verarbeiteten Patienten- und Patientinnendaten zu schützen. Dies dient zum einen der Vertraulichkeit der Kommunikation und schützt zum anderen personenbezogene Daten i.S.d. DS-GVO. Absatz 1 der Novellierung verfolgt daher einen **legitimen Zweck**.

Da Angriffserkennungssysteme Daten analysieren, die bereits in IT-Systemen gespeichert sind und die auf Grundlage anderer, unterschiedlicher Zwecksetzungen erhoben wurden, bedarf es einer Zweckänderung für die Weiterverarbeitung dieser Daten im Rahmen der Nutzung von Angriffserkennungssystemen in Absatz 2. Diese Zweckformulierung findet auch in den Absätzen 2a ff Anwendung, wonach Daten verarbeitet werden dürfen, wenn dies zum Zweck „*durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren*" geschieht. Angriffserkennungssysteme werten den gesamten Datenstrom des Systems oder Netzwerkes auf Angriffsmuster aus und können dadurch Angriffe auf das System oder Netzwerk, vorhandene Sicherheitslücken und das Auftreten von Schadprogrammen erkennen. Hierdurch schützen sie die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten sowie die Funktionsfähigkeit der Systeme und verhindern den unerlaubten Zugriff durch Dritte. Der Einsatz von Angriffserkennungssystemen in Krankenhäusern und der damit einhergehende Zweck, Gefahren für die IT-Sicherheit abzuwehren, stellt ebenfalls einen legitimen Zweck dar.

Die Novellierung muss zudem auch **geeignet** sein. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts genügt hierfür, dass die Wahrscheinlichkeit der Erreichung des legitimen Zwecks durch die Maßnahme erhöht wird.[903] Gemäß § 2 Nr. 9b BSIG sind Angriffserkennungssysteme „*durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme".* Die zu den Angriffserkennungssystemen gehörenden IDS können Angriffe erkennen, protokollieren und melden, aber nicht abwehren.[904] SIEM-Systeme können zudem in Echtzeit die sicherheitsrelevanten Ereignisse analysieren, die in den automatisiert erhoben logfiles protokolliert sind.[905] Der Einsatz von IDS und SIEM-Systemen ist Stand der Technik.[906] Da angesichts der fortschreitenden Hackerangriffe auf die IT von Krankenhäusern die Funktionsfähigkeit eines Krankenhauses und die damit einhergehende Sicherheit der verarbeiteten Patienten- und Patientinneninformationen nur sichergestellt werden kann, wenn Angriffe überhaupt erkannt werden, ist der Einsatz von Angriffserkennungssystemen zur Zweckerreichung nach Absatz 1 sowie nach Absatz 2 und 2a geeignet.

Der Einsatz von Angriffserkennungssystemen muss zur Zweckerreichung zudem auch **erforderlich** sein. Dies ist der Fall, wenn kein milderes Mittel zur Verfügung steht, das den Zweck

---

[903] Miller, *NdsVBl 2021, 1 (7).*
[904] Wendzel, *IT-Sicherheit für TCP/IP- und IoT-Netzwerke, S. 199.*
[905] Miller, *NdsVBl 2021, 1 (2).*
[906] Niedersächsisches Ministerium für Inneres und Sport, *Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, S. 38.*

mit einem geringeren Eingriffsgewicht und vergleichbarem Effekt erreichen könnte.[907] Angelehnt an das NDIG wird die Eingriffsintensität auf drei Eskalationsstufen verteilt. So darf der personenbezogene Datenverkehr gemäß Absatz 2a zunächst nur „*automatisiert erhoben, entschlüsselt und unverzüglich automatisiert ausgewertet werden*". Nach Absatz 2c der Novellierung des § 75c SGB V-E können dann bei zureichenden tatsächlichen Anhaltspunkten für eine Gefahr die erhobenen und ausgewerteten Daten sowie die Auswertungsergebnisse zusammengeführt werden, höchstens 30 Tage gespeichert und in dieser Zeitspanne weiter einzelfallbezogen automatisiert auswerten werden, wenn dies erforderlich ist und der Verantwortliche dies in Bezug auf Inhaltsdaten genehmigt. Erst wenn hinreichende tatsächliche Anhaltspunkte vorliegen, können nach Absatz 2d der Novellierung die Daten über den Ablauf der 30 Tage hinaus gespeichert und nicht automatisiert ausgewertet werden, wenn dies erforderlich ist und eine vorherige Zustimmung der Verantwortlichen vorliegt. Hierdurch wird sichergestellt, dass im Normalbetrieb lediglich automatisierte Auswertungsvorgänge erlaubt sind und erst bei einem ansteigenden Verdacht der Eingriff in den Schutzbereich stufenweise und kontrolliert intensiviert werden kann.

Damit Angriffserkennungssysteme am effizientesten arbeiten können, müssen sie sämtlichen Datenverkehr der Systeme oder Netzwerke analysieren. Würde man bestimmte Daten wie Inhaltsdaten von der Auswertung ausschließen, würde dies die Verlässlichkeit und Effizienz der Angriffserkennungssysteme stark einschränken und die Eignung der Maßnahme infrage stellen. Da die Weiterentwicklung von Angriffsmethoden gerade darauf abstellt, Sicherheits- und Detektionslücken zu finden und auszunutzen, ist eine lückenhafte Überwachung ungeeignet. Somit kann der Ausschluss bestimmter eingriffsintensiver Daten kein milderes Mittel darstellen, da hierdurch kein vergleichbarer Effekt erreicht werden kann. Zudem wird das Eingriffsgewicht durch das Stufenmodell auf ein realistisches Minimum reduziert. Der Einsatz von Angriffserkennungssystemen in Krankenhäusern nach der Novellierung des § 75c SGB V-E ist demnach auch erforderlich.

Schlussendlich müsste der Einsatz auch angemessen sein. Die Angemessenheitsprüfung stellt die **Verhältnismäßigkeit i.e.S.** dar. Die Novellierungen des § 75c SGB V-E sind angemessen, wenn der von ihnen verfolgte Zweck nicht außer Verhältnis zu den mit ihnen verbundenen Eingriffen steht.[908] Es ist folglich eine Zweck-Mittel-Relation durchzuführen, im Rahmen dessen in einer Gesamtschau die grundrechtsbeeinträchtigenden Maßnahmen den grundrechtsschützenden Maßnahmen gegenübergestellt werden.

Durch die Auswertung des gesamten Datenverkehrs der Systeme und Netzwerke eines Krankenhauses durch Angriffserkennungssysteme wird in das Fernmeldegeheimnis nach Art. 10 I GG sowie in das Recht auf informationelle Selbstbestimmung nach Art. 2 I i.V.m. Art. 1 I 1 GG der Patienten und Patientinnen, deren Besucher und Besucherinnen sowie der

[907] Miller, *NdsVBl 2021, 1 (7).*
[908] Miller, *NdsVBl 2021, 1 (8).*

Mitarbeitenden des Krankenhauses eingegriffen (*siehe III Verfassungsrechtliche Bewertung*). Aufgrund ihres lückenlosen Umfanges können die auszuwertenden Daten theoretisch dafür herangezogen werden, um aussagekräftige Rückschlüsse über persönliche und intime Lebensumstände der Nutzer und Nutzerinnen des Netzwerks, sowie auch von Patienten und Patientinnen des Krankenhauses ziehen zu können, weswegen der Einsatz von Angriffserkennungssystemen eine intensive **grundrechtsbeeinträchtigende Maßnahme** darstellt. Dieser Intensität werden in der Novellierung des § 75c SGB V-E **grundrechtsbeschützende Maßnahmen** gegenübergestellt. So ist in Absatz 2a eine strenge Zweckbindung verankert, die eine Verarbeitung der Daten ausschließlich zum Zweck der Abwehr von durch Sicherheitslücken, Schadprogrammen oder Angriffen verursachten Gefahren für die IT-Sicherheit ermöglicht. Zudem behandelt die Norm spezifisch den Bereich Krankenhaus und grenzt den Einsatzbereich auf die Übergabe- und Kontenpunkte des jeweiligen Krankenhausnetzwerks ein, so dass der Einsatz von Angriffserkennungssystemen nur präzise und begrenzt möglich ist und sich nicht auf andere Bereiche des Gesundheitssektors beziehen lässt. Gemäß der grundsätzlichen Erlaubnistatbestandsnorm des Absatzes 2a ist die Auswertung der Daten nur automatisiert erlaubt. Eine nicht automatisierte Verarbeitung ist gemäß dem Eskalationsmodell erst bei hinreichenden tatsächlichen Anhaltspunkten nach Absatz 2d möglich, wobei hier noch zusätzlich eine Kontrollinstanz der Auswertung zustimmen muss. Zudem wird der Sensibilität der krankenhaustypischen Daten Rechnung getragen, in dem eine Verarbeitung der Daten nach Absatz 2a Satz 2 nur Personen gestattet ist, die einem Berufsgeheimnis oder einer Geheimhaltungspflicht unterliegen. Gemäß Absatz 2c Satz 3 bestehen Pflichten zur Pseudonymisierung der Daten. Die Daten sind entweder unverzüglich zu löschen oder können bei zureichenden tatsächlichen Anhaltspunkten für eine Gefahr maximal 30 Tage gespeichert werden. Zudem normiert Absatz 3 einen Maßnahmenkatalog, wie die Daten sowie die Auswertungsergebnisse zu sichern sind. Absatz 4 fordert, ein Sicherheitskonzept vor dem Einsatz von Angriffserkennungssystemen. Sicherheitskonzepte stellen eine anerkannte, grundsätzliche Kontroll- und Organisationsmaßnahme nach den gültigen Sicherheitsstandards dar und dienen der Vermeidung der unrechtmäßigen Verarbeitung der Daten. Gemäß Absatz 2e der Novellierung dürfen weder die kommunikative Bedeutung von Inhaltsdaten noch Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des Art. 9 I DS-GVO ausgewertet werden. Derartige Zwischenergebnisse sind zudem unverzüglich zu löschen. Um Transparenz zu wahren, ist in Absatz 5 eine Protokollierungspflicht sämtlicher Vorgänge verankert. Zudem ist der oder die Betroffene gemäß Absatz 6 bei Verstößen oder Vorfällen zu informieren.

Durch die umfassenden grundrechtsbeschützenden Maßnahmen der Novellierung des § 75c SGB V-E, ist der Einsatz von Angriffserkennungssystemen in Krankenhäusern verhältnismäßig i.e.S..

b) Unionsrechtliche Ebene

Durch den Einsatz von Angriffserkennungssystemen wird auf unionsrechtlicher Ebene zudem in die in Art. 7 und 8 GRCh normierten Grundrechte eingegriffen. Die Novellierung des § 75c SGB V-E, die als Ermächtigungsgrundlage des Einsatzes von Angriffserkennungssystemen in Krankenhäusern fungiert, muss als eingreifende Regelung gemäß Art. 52 GRCh verhältnismäßig sein.[909] EuGH und EGMR teilen dasselbe Verständnis über die Anforderungen an den Verhältnismäßigkeitsgrundsatz, wonach auch hier eine Maßnahme verhältnismäßig ist, wenn diese ein legitimes Ziel verfolgt und hierfür geeignet, erforderlich und angemessen ist.[910]

Somit kann auf die Abhandlungen zu Verhältnismäßigkeit im nationalen Grundrechtskontext verwiesen werden (*siehe a) Nationale Ebene*).

Somit ist der nach der Novellierung des § 75c SGB V-E erlaubte Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft auf nationaler sowie unionsrechtlicher Ebene verfassungskonform.

4. Vereinbarkeit mit den Grundsätzen der Datenverarbeitung

Die Novellierung des § 75c SGB V-E muss zudem mit den Grundsätzen der Datenverarbeitung aus Art. 5 DS-GVO vereinbar sein.

Die aufgrund des in Art. 5 I lit. a DS-GVO verankertem Grundsatz der **Rechtmäßigkeit** der Verarbeitung personenbezogener Daten erforderliche Rechtsgrundlage ist in den Absätzen 2a, 2c sowie 2d verankert. Da diese als nationale Norm nur i.V.m. Art. 6 und 9 DS-GVO bestehen können, wird im Anschluss geprüft, ob eine Vereinbarkeit mit den Erlaubnistatbeständen vorliegt. Ist dies der Fall, ist dem Grundsatz der Rechtmäßigkeit genüge getan.

Personenbezogene Daten müssen zudem nach **Treu und Glauben** verarbeitet werden, wobei „Fairness“ als deutscher Begriff für diesen Grundsatz in der Literatur bevorzugt wird (*siehe VI.C.1 Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO*). Um dem Kräfteungleichgewicht zwischen Krankenhausbetreibenden und Patienten bzw. Patientinnen vorzubeugen, findet sich in der Novellierung des § 75c SGB V-E in Absatz 2a eine eng gefasste Zweckgebundenheit für die Verarbeitung der Daten. Zudem ist die Auswertung der kommunikativen Bedeutung von Inhaltsdaten nach Absatz 2e verboten und Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten i.S.d. Art. 9 I DS-GVO sind unverzüglich zu löschen. Vorfälle solcher Art sind zu dokumentieren. Zudem sind nach Absatz 3 eine Reihe von technisch-organisatorischen Sicherheitsmaßnahmen sowie nach Absatz 4 das Erstellen und Umsetzen eines Sicherheitskonzepts vorgesehen, um einen vertraulichen Umgang mit den

[909] Schantz/Wolff, *Das neue Datenschutzrecht D. Rn 600.*
[910] Sydow, *Europäische Datenschutzgrundverordnung Handkommentar DSGVO Art. 23 Rn 44.*

personenbezogenen Daten sicherzustellen. Ferner sind sämtliche Vorgänge nach Absatz 5 zu protokollieren, so dass Datenverarbeitungsvorgänge rekonstruiert werden können und betroffene Personen sind nach Absatz 6 zu benachrichtigen.

Die Voraussetzungen des Grundsatzes der **Transparenz** werden durch die Dokumentationspflicht des Absatzes 2e, der Protokollierungspflicht nach Absatz 5, der Benachrichtigungspflicht des Absatzes 6 sowie der Pflicht zu Erstellung eines Sicherheitskonzeptes nach Absatz 4 erfüllt. Zudem werden durch das Auswertungsverbot der sensiblen Daten in Absatz 2e auch aus inhaltlicher Sicht klare Grenzen der Verarbeitung gezogen.

Der in Art. 5 I lit. b DS-GVO normierte Grundsatz der **Zweckbindung** besagt, dass personenbezogene Daten nur für einen festgelegten, eindeutigen und legitimen Zweck erhoben werden dürfen. Da Angriffserkennungssysteme bereits zu anderen Zwecken erhobene Daten verarbeiten, liegt eine Weiterverarbeitung vor. Wie bereits erörtert, ist Zweck der Weiterverarbeitung nicht mit den Primärzwecken vereinbar, weswegen eine Weiterverarbeitung zu einem anderen Zweck nur möglich ist, wenn die Zweckänderung auf einer Rechtsgrundlage der Union oder eines Mitgliedstaates beruht und diese neben der DS-GVO Anwendung findet (*siehe VI.C.2.c)(6)(a) Verstoß gegen den Grundsatz der Zweckbindung?)*. Grundsätzlich könnte die Zweckänderung, die mit der Verpflichtung aus § 75c SGB V einhergeht, auf Grundlage des § 67c SGB X gerechtfertigt sein. Dieser findet seine Legitimation neben der DS-GVO durch die Öffnungsklauseln des Art. 6 I 1 lit. c und e i.V.m. Art. 9 II lit. b beziehungsweise h sowie j DS-GVO oder nach Art. 6 IV DS-GVO. Da § 67c SGB X jedoch sehr allgemein gehalten ist, wird durch das Einfügen der Absätze 2 und 2a des Novellierungsvorschlags ein eindeutiger Zweck i.S.d. Grundsatzes festgelegt. So wird festgelegt, dass Daten nach der Novellierung des § 75c SGB V-E nur weiterverarbeitet werden dürfen, wenn dies zur Abwehr von durch Sicherheitslücken, Schadprogrammen oder Angriffen verursachten Gefahren für die IT-Sicherheit erforderlich ist. Zudem benennt Absatz 2a klare Anwendungsgebiete (Übergabe- und Knotenpunkten der von ihnen betriebenen Datennetze), die durch Angriffserkennungssysteme überwacht werden sollen. Absatz 2 und 2a findet seine Legitimation im vorliegenden Fall durch die Öffnungsklauseln des Art. 6 I 1 lit. c i.V.m. Art. 9 II lit. h DS-GVO beziehungsweise Art. 6 IV DS-GVO.

Aus den Grundsätzen der **Datenminimierung** sowie der **Speicherbegrenzung** ergibt sich, dass personenbezogene Daten zu löschen sind, sobald sie nicht mehr zur Zweckerreichung erforderlich sind. Weisen Daten nicht auf besondere Vorkommnisse hin, sind diese unverzüglich zu löschen. Markieren personenbezogene Daten jedoch Gefahrenhinweise, sind diese weiterhin zum Erreichen des Verarbeitungszwecks erforderlich und dürfen weiterhin gespeichert werden. Das BAG hat in diesem Zusammenhang entschieden, dass personenbezogene Daten spätestens 60 Tage nach der Erhebung gelöscht werden müssen, so lange diese nicht noch zum Zweck der Beweissicherung benötigt werden.[911] Den Grundsätzen werden durch die Löschpflichten in

[911] Benner-Tischler*, ZD-Aktuell 2019, 06446.*

Absatz 2b, 2c und 2e sowie durch die zeitlichen Speicherbegrenzungen im Absatz 2c nachgekommen. Durch die Übernahme des Eskalationsstufenmodells aus dem NDIG wird nach der Wahrscheinlichkeit eines tatsächlichen Angriffes beziehungsweise Sicherheitsvorfalls hinsichtlich der Dauer der Speicherung der Daten entschieden, was die Speichermöglichkeiten für den oder die Krankenhausbetreibenden auf ein verhältnismäßiges Minimum reduziert. Zudem arbeiten die Angriffserkennungssysteme automatisiert mit bekannten Mustern und Schwellenwerten. Fallen Informationen nicht in diese Muster oder unter diese Schwellenwerte, werden sie nicht längerfristig erfasst. Der weitaus überwiegende Teil der Daten, die von einem Angriffserkennungssystemen analysiert werden, werden im Sinne der Datenminimierung somit nur kurzfristig erfasst.

Der Grundsatz der **Richtigkeit** nach Art. 5 I lit. d DS-GVO spielt bei dem Einsatz von Angriffserkennungssystemen nur eine untergeordnete Rolle, da die Systeme die Daten lediglich auf Auffälligkeiten untersuchen. Ob die Daten, die in den Krankenhausnetzwerken verarbeitet werden sachlich richtig sind, kann durch einen automatisierten Auswertungsvorgang nicht festgestellt werden. Die detaillierten Löschpflichten der Novellierung des § 75c SGB V-E garantieren jedoch, dass sämtliche Daten, die nicht mit einem detektieren Angriff in Zusammenhang stehen, umgehend gelöscht werden. Dies schließt somit auch unrichtige Daten ein. Da die Novellierung des § 75c SGB V-E nicht darauf ausgelegt ist, eine dauerhafte Datenspeicherung zu rechtfertigen, bedarf es somit keiner regelmäßigen Pflicht zur Überprüfung der Richtigkeit der Daten.

Der Grundsatz der **Integrität und Vertraulichkeit** findet sich als letzter Grundsatz in Art. 5 I lit. f DS-GVO. Hiernach müssen personenbezogene Daten „*in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet*“. Dies schließt den „*Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen*“ ein. Durch Absatz 3 wird sichergestellt, dass die Daten, die durch den Einsatz von Angriffserkennungssystemen ausgewertet und gespeichert werden, durch technische und organisatorische Maßnahmen gegen unbefugte Kenntnisnahme, Veränderung und Verwendung geschützt werden. Für eine bessere Umsetzung in der Praxis, führt Absatz 3 einen Maßnahmenkatalog auf. Zudem muss nach Absatz 4 ein Sicherheitskonzept für die eingesetzten technischen Systeme erstellt werden.

Folglich werden in den Novellierungen des § 75c SGB V-E sämtliche Grundsätze der Datenverarbeitung aus Art. 5 DS-GVO umgesetzt.

5. Vereinbarkeit mit den Erlaubnistatbeständen der DS-GVO

Die Novellierungen des § 75c SGB V-E müssen zudem den Erlaubnistatbeständen der DS-GVO entsprechen, um eine Rechtfertigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft darstellen zu können.

a) Art. 6 I 1 lit. c DS-GVO

Wie bereits bei der Prüfung des § 75c SGB V, könnte die Novellierung ebenfalls i.V.m. Art. 6 I 1 lit. c DS-GVO eine Ermächtigungsgrundlage zur Verarbeitung personenbezogener Daten darstellen (*siehe VI.C.2.c)(6) § 75c SGB V*). Hiernach ist die Verarbeitung rechtmäßig, wenn „*die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich {ist}, der der Verantwortliche unterliegt*".

Art. 6 I 1 lit. c DS-GVO wird erst in Verbindung mit einer rechtlichen Verpflichtung aus dem Recht der Union oder der Mitgliedstaaten zur Ermächtigungsgrundlage[912], wobei strittig ist, welche Anforderungen an den Begriff der rechtlichen Verpflichtung zu stellen sind. Stimmen in der Literatur fordern, dass die rechtliche Verpflichtung ebenfalls die Merkmale einer Erlaubnistatbestandsnorm umfassen müsse,[913] wohingegen andere Ansichten an die rechtliche Verpflichtung lediglich die Anforderung der Begründung zur Rechtspflicht zur Datenverarbeitung stellen und nicht die Legalisierung dieser.[914]

Die Anforderungen an diese rechtliche Verpflichtung geben Art. 6 II, III DS-GVO vor. Hiernach ist die nationalstaatliche Normierung nur für solche Materien möglich, die bereits von der DS-GVO regulativ umfasst sind. Zudem setzen Art. 6 II und III DS-GVO voraus, dass die spezifische Rechtsvorschrift einen verpflichtenden bzw. ermächtigenden Charakter aufweist.[915] Da die Mitgliedstaaten vor allem unter den Vorgaben von Absatz III zwar eigenständige Regelungsspielräume haben, diese aber nur innerhalb eines beschränkten Gestaltungsspielraumes stattfinden können, wird man zwar von einer echten, aber beschränkten Öffnungsklausel ausgehen müssen.[916]

Die Novellierung des § 75c SGB V-E beinhaltet in Absatz 1 die rechtliche Verpflichtung „*angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der*

---

[912] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 1 Rn 52.*
[913] Kühling/Buchner, *Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 6 Rn 73;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 1 Rn 52;* Specht/Mantz, *Handbuch Europäisches und deutsches Datenschutzrecht§ 3 Rn 60.*
[914] Forgó u. a., *Betrieblicher Datenschutz - Rechtshandbuch Teil V. Kap. 1 Rn 20;* Paal/Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar DS-GVO Art. 6 Rn 16;* Brink/Wolff, *BeckOK Datenschutzrecht DS-GVO Art. 6 Rn 34;* Taeger/Gabel, *Kommentar DSGVO - BDSG DS-GVO Art. 6 Rn 64;* Gola, *Datenschutz-Grundverordnung Kommentar DS-GVO Art. 6 Rn 42.*
[915] Albrecht/Jotzo, *Das neue Datenschutzrecht der EU Teil 3 Rn 46.*
[916] Albrecht/Jotzo, *Das neue Datenschutzrecht der EU Teil 3 Rn 46;* Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 3 Rn 19.*

Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind, zu treffen". Da die Absätze 2a, 2c sowie 2d zudem Erlaubnistatbestände zur Verarbeitung der hierfür notwendigen personenbezogenen Daten in Eskalationsstufen enthalten, kann der Streit über die Anforderungen an die rechtliche Verpflichtung i.S.d. Art. 6 I 1 lit. c DS-GVO (*siehe VI.C.2.c) Die Erfüllung einer rechtlichen Verpflichtung nach Art. 6 I 1 lit. c DS-GVO*) dahinstehen, da die Novellierung des § 75c SGB V-E nach beiden Meinungen eine rechtliche Verpflichtung darstellt.

Durch Absatz 1a der Novellierung, der unter Bezugnahme auf § 8a Ia BSIG den „*Einsatz von Systemen zur Angriffserkennung*" als angemessene organisatorische und technische Vorkehrung nach Absatz 1 Satz 1 der Novellierung sieht, fällt der Einsatz von IDS sowie SIEM-Systemen interpretationsfrei unter die Verpflichtung des Absatz 1.

Da der Einsatz von Angriffserkennungssystemen eine Weiterverarbeitung bereits erhobener Daten darstellt und der Weiterverarbeitungszweck mit dem ursprünglichen Verarbeitungszweck nicht kompatibel ist, bedarf es einer Rechtsgrundlage der Union oder eines Mitgliedstaates, die eine Zweckänderung zur Weiterverarbeitung erlaubt. Die Begründung der Legitimation dieser Rechtsgrundlage neben der DS-GVO ist umstritten. So sehen Stimmen in der Literatur Art. 6 IV DS-GVO als Öffnungsklausel, die Zweckänderungsnormen eine Legitimation neben den Bestimmungen der DS-GVO einräumt, wohingegen andere Meinungen den Normen eine Legitimation durch die Öffnungsklausel aus den Erlaubnistatbeständen des Art. 6 I 1 i.V.m II, III DS-GVO zusprechen (*siehe VI.C.2.c)(6)(a) Verstoß gegen den Grundsatz der Zweckbindung?*). Diese Rechtsgrundlage für die Zweckänderung begründet hierbei jedoch nicht den Erlaubnistatbestand der eigentlichen Weiterverarbeitung. Gemäß Erwägungsgrund 50 S. 5 der DS-GVO kann die Rechtsgrundlage, die beispielsweise nach Art. 6 III DS-GVO eine Rechtsgrundlage für die Datenverarbeitung beinhaltet, auch zur Erlaubnis der zulässigen Zweckänderung genutzt werden.[917]

Absatz 2 der Novellierung des § 75c SGB V-E enthält eine solche Zweckänderung. Hiernach können personenbezogene Daten „*zu dem Zweck, durch Sicherheitslücken, Schadprogramme oder Angriffe verursachte Gefahren für die IT-Sicherheit abzuwehren*" verarbeitet werden, worunter auch der Einsatz von Angriffserkennungssystemen fällt. Da bereits § 67c SGB X, der eine Zweckänderung ebenfalls erlaubt, mit den Regelungen der DS-GVO durch die Öffnungsklauseln des Art. 6 I 1 lit. c und e i.V.m. Art. 9 II lit. b bzw. h sowie j DS-GVO vereinbar ist[918], kann der Zweckänderungstatbestand in der Novellierung des § 75c SGB V-E ebenfalls durch die Öffnungsklausel des Art. 6 I 1 lit. c, II, III DS-GVO bestehen.

[917] Simitis u. a., *Datenschutzrecht - DGVO mit BDSG DSGVO Art. 6 Abs. 4 Rn 25.*
[918] Körner u. a., *Kasseler Kommentar Sozialversicherungsrecht SGB X § 67c Rn 11.*

Somit stellt die Novellierung des § 75c SGB V-E i.V.m. Art. 6 I 1 lit. c, II, III DS-GVO eine Rechtfertigungsnorm für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft dar.

b) Art. 9 II lit. h DS-GVO

Da in den Netzwerken von Krankenhäusern besondere Kategorien personenbezogener Daten i.S.d. Art. 9 I DS-GVO verarbeitet (*siehe VI.C.3 Rechtmäßigkeit der Verarbeitung von Gesundheitsdaten nach Art. 9 DS-GVO*) und diese somit ebenfalls von Angriffserkennungssystemen ausgewertet werden, bedarf es neben einer Erlaubnistatbestandsnorm aus Art. 6 I DS-GVO ebenfalls eine Rechtfertigung der Verarbeitung nach den strengeren Voraussetzungen des Art. 9 II DS-GVO.

Gemäß Art. 9 II lit. h DS-GVO wird eine Ausnahme des generellen Verarbeitungsverbotes für „*Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich*“ vorgesehen. Art. 9 II lit. h DS-GVO ist ebenfalls kein eigenständiger Erlaubnistatbestand, sondern fordert eine zusätzliche „*Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder einen Vertrag mit einem Angehörigen eines Gesundheitsberufs*“. Da bereits bei Art. 6 I 1 lit. c DS-GVO darüber gestritten wird, ob der Begriff rechtliche Verpflichtung das Erfordernis einer bloßen Verpflichtung oder einer Ermächtigungsgrundlage beinhaltet, kann bei Art. 9 II lit. h DS-GVO eine bloße rechtliche Verpflichtung als „*Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats*“ nicht ausreichen. Der Erlaubnistatbestand ergibt sich nicht nur aus Art. 9 II lit. h DS-GVO, sondern muss ebenfalls in der unionsrechtlichen oder mitgliedstaatlichen Norm verankert sein.

Im Gegensatz zum eigentlichen Normgehalt des § 75c SGB V enthält die Novellierung in Absatz 2, 2a, 2c sowie 2d Erlaubnistatbestände, die die Verarbeitung personenbezogener Daten zum Zweck der Abwehr von Gefahren für die IT-Sicherheit gemäß des Eskalationsstufenmodells erlauben. Da gemäß Absatz 1a der Einsatz von Angriffserkennungssystemen von den Regelungen der Novellierung umfasst und die Auswertung der Daten hierdurch erlaubt ist, kann die Novellierung des § 75c SGB V-E i.V.m. Art. 9 II lit. h DS-GVO eine Rechtfertigungsgrundlage darstellen.

Zusätzlich müssen jedoch die in Art. 9 III DS-GVO enthaltenen Bedingungen und Garantien eingehalten werden. Absatz 3 schränkt eine Verarbeitung nach Art. 9 II lit. h DS-GVO derart ein, dass die Verarbeitung von personenbezogenen Daten nur durch Fachpersonal zulässig ist sowie durch Personen, die einer Geheimhaltungspflicht oder einem Berufsgeheimnis unterliegen. Das von Art. 9 III DS-GVO erfasste Fachpersonal unterliegt im deutschen Recht primär

dem Berufsgeheimnis aus § 203 I, II Nr. 1 StGB.[919] Gemäß § 203 III StGB liegt zudem keine Offenbarung eines Geheimnisses vor, wenn die nach Absatz 1 und 2 dem Berufsgeheimnis unterliegenden Personen „*Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen*". Zudem dürfen sie „*fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist*". Dies gilt auch für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen die an der beruflichen oder dienstlichen Tätigkeit mitwirken, die dem Berufsgeheimnis unterliegen. Unter § 203 III 2 StGB fallen unter anderem Auftragsverarbeiter und -verarbeiterinnen i.S.d. Art. 28 DS-GVO. Diese unterliegen somit ebenfalls einer gesetzlichen Verschwiegenheitspflicht.[920] Zudem haben Berufsgeheimnisträger und -trägerinnen gemäß § 53 StPO ein Zeugnisverweigerungsrecht. Zu den Berufsgeheimnissen gehört auch das Sozialgeheimnis aus § 35 SGB I.[921] Gemäß Absatz 1 Satz 1 umfasst die Wahrung des Sozialgeheimnisses „*die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden*". Das Sozialgeheimnis erstreckt sich zudem gemäß § 80 SGB X auch auf Auftragsverarbeiter und -verarbeiterinnen i.S.d. Art. 28 DS-GVO.

Durch die Novellierung des § 203 StGB bedarf es für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft keine explizite Regelung mehr, um die Anforderungen in Art. 9 III DS-GVO zu erfüllen. Da die besonderen Kategorien personenbezogener Daten aus Art. 9 I DS-GVO jedoch eine hohe Schutzbedürftigkeit aufweisen, wird durch die Regelung in Absatz 2a Satz 2 zur Geheimhaltungspflicht dieser Schutzbedürftigkeit Genüge getan.

Somit ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Rahmen des Einsatzes von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft gemäß Art. 9 II lit. h, III DS-GVO i.V.m. der Novellierung des § 75c SGB V-E gerechtfertigt.

6. Zusammenfassung

Die Novellierung des § 75c SGB V-E ist sowohl auf nationaler als auch auf unionsrechtlicher Grundrechtsebene verfassungskonform. Zudem verstößt die Novellierung des § 75c SGB V-E nicht gegen die Grundsätze der Datenverarbeitung aus Art. 5 DS-GVO.

In Verbindung mit Art. 6 I 1 lit. c, II, III DS-GVO kann die Novellierung des § 75c SGB V-E neben den Regelungen der DS-GVO als Erlaubnistatbestand zum Einsatz von Angriffserkennungssystemen bestehen. Zudem dürfen in Verbindung mit Art. 9 II lit. h, III DS-GVO auch

[919] Taeger/Gabel*, Kommentar DSGVO - BDSG DS-GVO Art. 9 Rn 32.*
[920] Kühling/Buchner*, Datenschutz-Grundverordnung BDSG Kommentar DS-GVO Art. 9 Rn 149.*
[921] Simitis u. a.*, Datenschutzrecht - DGVO mit BDSG DSGVO Art. 9 Rn 92.*

die besonderen Kategorien personenbezogener Daten aus Art. 9 I DS-GVO nach den Maßgaben der Novellierung des § 75c SGB V-E verarbeitet werden.

VIII. Ergebnis

Durch den flächendeckenden Ausbau der digitalen Infrastruktur im Gesundheitswesen wird eine neue Qualität der Patienten- und Patientinnenversorgung und -behandlung ermöglicht. Mit dem Fortschritt der Digitalisierung und Vernetzung steigt jedoch auch die Abhängigkeit der Akteure des Gesundheitswesens von den dort eingesetzten IT-Systemen und Prozessen. Je größer die Vernetzung ist, desto breiter wird das Spektrum an Angriffsmöglichkeiten und Systemschwachstellen, die von Angreifern und Angreiferinnen genutzt werden können und in der jüngeren Vergangenheit bereits genutzt wurden. Um die Funktionalität des Gesundheitswesens, hier insbesondere der Krankenhäuser, gewährleisten zu können und Patienten- und Patienteninneninformationen angemessen vor dem unberechtigten Zugriff Dritter schützen zu können, ist es unerlässlich, angemessene technische und organisatorische Schutzvorkehrungen zu treffen. Eine etablierte Maßnahme stellt die Implementierung von Angriffserkennungssystemen, wie IDS oder SIEM-Systemen, dar. Diese werten die Datenströme der Netzwerke und Systeme automatisiert auf Angriffsmuster aus.

Nach aktueller Rechtslage gibt es weder auf nationaler noch auf unionsrechtlicher Ebene eine umfassende Ermächtigungsgrundlage für den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft. Aufgrund der mittelbaren Drittwirkung der unionsrechtlichen und nationalen Grundrechte ist diese aber auch im Verhältnis zwischen Privatrechtssubjekten erforderlich, zudem ist der Gesetzgeber durch seine verfassungsrechtlichen Schutzpflichten verpflichtet, die betroffenen Grundrechte gegen Eingriffe durch private Personen zu schützen.

Durch die Umsetzung der vorgeschlagenen Novellierung des § 75c SGB V-E würde eine umfassende Ermächtigungsgrundlage vorliegen, die den Einsatz von Angriffserkennungssystemen in Krankenhäusern in privater Trägerschaft rechtfertigen würde.

Eine spezifische Regelung zum Einsatz von Angriffserkennungssystemen in Krankenhäusern kann jedoch nicht genügen, um die IT-Sicherheit im Gesundheitswesen grundlegend datenschutzrechtlich zu manifestieren. Es bedarf zusätzlicher verwandter Regelungen für sämtliche Akteure und Akteurinnen des Gesundheitssektors, um rechtliche Grauzonen beim flächendeckenden Einsatz von Angriffserkennungssystemen zu vermeiden.

Kritisch zu betrachten ist zudem ein Grundproblem in der nationalen Umsetzung von unionsrechtlichen Öffnungsklauseln im Datenschutz, welches § 75c SGB V in seiner jetzigen Form beispielhaft aufweist. So wird zwar eine rechtliche Verpflichtung des Verantwortlichen bzw. der Verantwortlichen zum Handeln normiert, eine Ermächtigungsgrundlage für dieses Handeln fehlt jedoch. Dies führt – wie im vorliegenden Fall – dazu, dass ein Handeln nach dieser

Verpflichtung unrechtmäßig wäre, falls die DS-GVO in ihren Erlaubnistatbeständen nicht einschlägig ist beziehungsweise die Voraussetzungen der Öffnungsklauseln nicht vorliegen. Zudem ist fragwürdig, ob die reine rechtliche Verpflichtung ohne damit einhergehende Regelung des Erlaubnistatbestandes mit dem staatsrechtlichen Bestimmtheitsgrundsatz und dem Gebot der Normenklarheit des Grundgesetzes vereinbar ist. Es bietet sich an, die gesteckten Möglichkeiten der Öffnungsklauseln der Erlaubnistatbestände der Art. 6 und 9 DS-GVO in Gänze im nationalen Recht umzusetzen und im Sinne des Bestimmtheitsgrundsatzes nicht nur die rechtlichen Verpflichtungen zum Einsatz von Maßnahmen zum Schutze der IT-Sicherheit, sondern auch deren Ermächtigung hierzu auf nationaler Ebene zu regeln.

Literaturverzeichnis

aerzteblatt.de, Betrieb im Klinikum Fürth wegen Hacker-Attacke eingeschränkt, https://www.aerzteblatt.de/nachrichten/108189/Betrieb-im-Klinikum-Fuerth-wegen-Hacker-Attacke-eingeschraenkt (abgerufen am 10.12.2021)

Albrecht, Jan Philipp / Jotzo, Florian, Das neue Datenschutzrecht der EU, 2016

Ärzteblatt, Kritische Infrastruktur: Regierung legt Kriterien fürs Gesundheitswesen fest, https://www.aerzteblatt.de/nachrichten/76084/Kritische-Infrastruktur-Regierung-legt-Kriterien-fuers-Gesundheitswesen-fest (abgerufen am 15.11.2019)

Ärzteblatt, Kritische Infrastruktur: Schwellenwert für Kliniken „problematisch", https://www.aerzteblatt.de/nachrichten/76094/Kritische-Infrastruktur-Schwellenwert-fuer-Kliniken-problematisch (abgerufen am 15.11.2019)

Ärzteblatt, IT-Sicherheit und Datenschutz für Kliniken immer wichtiger, https://www.aerzteblatt.de/nachrichten/98987/IT-Sicherheit-und-Datenschutz-fuer-Kliniken-immer-wichtiger (abgerufen am 15.11.2019)

Auer-Reinsdorff, Astrid / Conrad, Isabell, Handbuch IT- und Datenschutzrecht, 2. Auflage, 2016

Bäcker, Matthias, Das Grundgesetz als Implementationsgarant der Unionsgrundrechte, EuR 2015, 389

Ballmann, Bastian, Network Hacks, 2012

Bartsch, Alexander / Rieke, Inga, Das neue Datenschutzrecht mit Auswirkungen auch auf Energieversorger, EnWZ 2017, 435

Bauer, Christoph / Eickmeier, Frank / Eckard, Michael, E-Health: Datenschutz und Datensicherheit, 2018

Becker, Florian, Grundrechtliche Grenzen staatlicher Überwachung zur Gefahrenabwehr, NVwZ 2015, 1335

Benner, Anja, DREI: Forschungsprojekt zur datenschutzkonformen Erkennung von Innentätern durch Softwaresysteme, ZD-Aktuell 2017, 05556

Benner-Tischler, Anja, Löschfristen in technischen Systemen zur Mitarbeiterüberwachung und ihre Auswirkung auf die Beweisverwertung, ZD-Aktuell 2019, 06446

Bergmann, Jan / Dienelt, Klaus, Ausländerrecht: AuslR, 12. Auflage, 2018

Berlth, Astrid, Artikel 1 GRCh – Die Menschenwürde im Unionsrecht, Münster 2012

BfDI (Hrsg.), Datenschutz und Telekommunikation - Info 05, 2020

Bieker, Felix, Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, DuD 2018, 27

Bitkom, Stellungnahme TTDSG April 2021, 2021

BKA, Cybercrime Bundeslagebild 2020, 2020

Bless, Roland / Mink, Stefan / Blaß, Erik-Oliver / Conrad, Michael / Hof, Hans-Joachim / Kutzner, Kendy / Schöller, Marcus, Sichere Netzwerkkommunikation, 2005

Böhm, Wolf-Tassilo / Halim, Valentino, Cookies zwischen ePrivacy und DS-GVO – was gilt?, MMR 2020, 651

Bratvogel, Karsten / Schmidt, Klaus, Netzwerke Grundlagen, 11. Auflage, 2019

Bretthauer, Sebastian, Smart Meter im Spannungsfeld zwischen Europäischer Datenschutzgrundverordnung und Messstellenbetriebsgesetz, EnWZ 2017, 56

Brink, Stephan / Wolff, Heinrich Amadeus, BeckOK Datenschutzrecht, 27. Auflage, 2019

Brink, Stephan / Wolff, Heinrich Amadeus (Hrsg.), BeckOK Datenschutzrecht, 37. Auflage, 2021

BSI, Die Lage der IT-Sicherheit in Deutschland 2020, 2020

BSI, BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen (IDS) - Rechtliche Aspekte beim Einsatz von IDS

BSI, Die Lage der IT-Sicherheit in Deutschland 2021, 2021

BSI, Über den IT-Grund-schutz, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-GrundschutzAbout/itgrundschutzAbout_node.html (abgerufen am 20.01.2021)

BSI, Auftrag des BSI, https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html;jsessionid=EB2135B8EECF879B35A2697971B6F551.internet081 (abgerufen am 07.12.2021)

Bundesamt für Sicherheit in der Informationstechnik, Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Leitfaden, 2013

Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2016, 2016

Bundesamt für Sicherheit in der Informationstechnik, Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS, 2017

Bundesamt für Sicherheit in der Informationstechnik, Kritische Infrastrukturen - Rechtsgrundlagen: BSI-Gesetz, IT-Sicherheitsgesetz, NIS-Richtlinie

Bundesministerium der Justiz (Hrsg.), Handbuch der Rechtsförmlichkeit, 3. Auflage, 2008

Bundesministerium für Gesundheit, Spahn: „Die Welt wartet nicht auf uns“, https://www.bundesgesundheitsministerium.de/presse/interviews/interviews/faz-141119.html (abgerufen am 10.12.2021)

Bundesministerium für Gesundheit, Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur

Bundesministerium für Gesundheit, Krankenhauszukunftsgesetz für die Digitalisierung von Krankenhäusern, https://www.bundesgesundheitsministerium.de/krankenhauszukunftsgesetz.html (abgerufen am 20.12.2021)

Calliess, Christian / Ruffert, Matthias (Hrsg.), EUV/AEUV Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta Kommentar, 5. Auflage, 2016

Casper, Mirko / Strobel, Stefan, Durchleuchtet - Software zum Schwachstellenmanagement, iX 2018

Darms, Martin / Haßfeld, Stefan / Fedtke, Stephen, IT-Sicherheit und Datenschutz im Gesundheitswesen – Leitfaden für Ärzte, Apotheker, Informatiker, und Geschäftsführer in Klink und Praxis, 2019

Dehn, Siegmund, Netzwerke Sicherheit, 11. Ausgabe, 2019

Deutsche Krankenhaus Gesellschaft, Krankenhäuser als kritische Infrastrukturen - Umsetzungshinweise der Deutschen Krankenhausgesellschaft, 2017

Deutsche Krankenhaus Gesellschaft, Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, 2019

Deutsche Krankenhaus Gesellschaft, Krankenhausstatistik - Eckdaten der Krankenhausversorgung, https://www.dkgev.de/fileadmin/default/Mediapool/3_Service/3.2._Zahlen-Fakten/Foliensatz_KHstatistik20210427.pdf (abgerufen am 02.12.2021)

Deutscher Bundestag, Ausarbeitung: Krankenhäuser in privater Trägerschaft – Rechtsgrundlagen, verfassungsrechtliche Vorgaben und Finanzierung, 2014

Dinger, Jochen / Hartenstein, Hannes, Netzwerk- und IT-Sicherheitsmanagement - Eine Einführung, 2008

Dittrich, Tilmann, Die Verankerung der IT-Sicherheit von Krankenhäusern im Sozialrecht – worin liegt der Nutzen des § 75 c SGB V?, GuP 2021, 165

DKG, Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, 2019

DKG, Aufgaben und Ziele, https://www.dkgev.de/dkg/aufgaben-ziele/ (abgerufen am 27.11.2021)

Dochow, Carsten / Dörfer, Bert-Sebastian / Halbe, Bernd / Hübner, Marlis / Ippach, Jan / Schröder, Jürgen / Schütz, Joachim / Strüve, Jakob, Datenschutz in der ärztlichen Praxis, 1. Auflage, 2019

Dürig, Markus / Fischer, Matthias, Cybersicherheit in Kritischen Infrastrukturen, DuD 2018, 209–213

Ehmann, Eugen / Selmayr, Martin (Hrsg.), Datenschutz-Grundverordnung Kommentar, 2. Auflage, 2018

Eigner, Martin / Gerhardt, Florian / Gilz, Torsten / Mogo Nem, Fabrice, Informationstechnologie für Ingenieure, 2012

Eisenreich, Frauke, Digitalisierung im Krankenhaus: Entwicklung und Validierung eines konzeptionellen Akzeptanzmodells im Rahmen der Implementierung eines Krankenhausinformationssystems in einer Universitätsklinik, 2020

Fezer, Karl-Heinz / Büscher, Wolfgang / Obergfell, Eva Inés (Hrsg.), Lauterkeitsrecht - Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG), 2016

Fischinger, Phillip S., Münchener Handbuch zum Arbeitsrecht, Bd. I, 4. Auflage, 2019

Forgó, Nikolaus / Helfrich, Marcus / Schneider, Jochen (Hrsg.), Betrieblicher Datenschutz - Rechtshandbuch, 3. Auflage, 2019

Forgó, Nikolaus / Krügel, Tina / Schmieder, Fabian, Rechtsgutachten zum Betrieb von IDS & Event Management-Systemen in Netzen der öffentlichen Verwaltung, 2016

Franck, Johannes, Smart Grids und Datenschutz: Verarbeitung von Energiedaten in intelligenten Stromnetzen aus datenschutzrechtlicher Perspektive, Bd. 18, , 2016

Franzen / Gallner / Oetker, Hartmut (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 3. Auflage, 2020

Franzetti, Claudio, Essenz der Infortmatik, 2019

Frhr. von dem Bussche, Axel, Konzerndatenschutz, 2019

Fülbier, Ulrich / Splittgerbe, Andreas, Keine (Fernmelde-)Geheimnisse vor dem Arbeitgeber?, NJW 2012, 1995

Gamer, Thomas, Dezentrale, Anomalie-basierte Erkennung verteilter Angriffe im Internet, 2010

GDD, GDD-Praxishilfe Das neue Telekommunikation-Telemedien- Datenschutz-Gesetz (TTDSG) im Überblick, 2021

Geppert, Martin / Schütz, Raimund (Hrsg.), Beck'scher TKG-Kommentar, 4. Auflage, 2013

Gersdorf, Hubertus / Paal, Boris P. (Hrsg.), BeckOK Informations- und Medienrecht, 26. Edition, 2019

Gersdorf, Hubertus / Paal, Boris P. (Hrsg.), BeckOK Informations- und Medienrecht, 23. Edition

Gola, Peter (Hrsg.), Datenschutz-Grundverordnung Kommentar, 2. Auflage, 2018

Gola, Peter / Schomerus, Rudolf / Klug, Christoph / Körffer, Barbara (Hrsg.), Bundesdatenschutzgesetz Kommentar, 12. Auflage, 2015

Golland, Alexander, Das Telekommunikation-Telemedien-Datenschutzgesetz Cookies und PIMS als Herausforderungen für Website-Betreiber, NJW 2021, 2238

Grabitz / Hilf / Nettesheim (Hrsg.), Das Recht der Europäischen Union: EUV/AEUV, 67. EL, 2019

Groß, Stephan, Kooperative Angriffserkennung in drahtlosen Ad-hoc- und Infrastrukturnetzen, 2008

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035

Härtel, Ines, Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren, LKV 2019, 49

heise online, Höhere Sicherheit mit wenig Aufwand: Wie innovative SIEM-Lösungen helfen, Cyber-Angriffe abzuwehren, https://www.heise.de/solutions/rapid7/hoehere-sicherheit-mit-wenig-aufwand-wie-innovative-siem-loesungen-helfen-cyber-angriffe-abzuwehren/ (abgerufen am 02.12.2021)

Hillgruber, Christian / Epping, Volker, BeckOK Grundgesetz, 40. Edition, 2019

Hirsch, Burkhard, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, NJOZ 2008, 1907

Hoeren, Thomas / Sieber, Ulrich / Holznagel, Bernd (Hrsg.), Multimedia-Recht, 54. EL, 2020

Hwang, Shu-Perng, Anwendungsvorrang statt Geltungsvorrang? Normlogische und institutionelle Überlegungen zum Vorrang des Unionsrechts, EuR 2016, 355

Jandt, Silke / Steidle, Roland (Hrsg.), Datenschutz im Internet - Rechtshandbuch zu DSGVO und BDSG, 1. Auflage, 2018

Jarass, Hans D., Charta der Grundrechte der Europäischen Union Kommentar, 3. Auflage, 2016

Jobst, Simon, Konsequenzen einer unmittelbaren Grundrechtsbindung Privater, NJW 2020, 11

Jorzig, Alexandra / Sarangi, Frank, Digitalisierung im Gesundheitswesen, 2020

Kappes, Martin, Netzwerk- und Datensicherheit, 2. Auflage, 2013

Kassenärztliche Bundesvereinigung, Anwendungen Digitale Praxis, https://www.kbv.de/html/it-anwendungen.php (abgerufen am 17.11.2021)

Katsivelas, Ioannis, Anwendbarkeit der Grundrechtecharta beim Einsatz von Adblockern, MMR 2017, 286

Keller, Andres, Breitbandkabel und Zugangsnetze, 2. Auflage, 2011

Kipker, Dennis-Kenji / Birrek, Piet / Niewöhner, Mario / Schnorr, Timm, NIS-Richtlinie und der Entwurf der NIS-2-Richtlinie - Überblick, Gemeinsamkeiten und Unterschiede, MMR 2021, 214

Kipker, Dennis-Kenji / Scholz, Dario, Das IT-Sicherheitsgesetz 2.0 - Neue Rahmenbedingungen für die Cybersicherheit in Deutschland, MMR 2019, 431

Kirchhof, Ferdinand, Nationale Grundrechte und Unionsgrundrechte, NVwZ 2014, 1537

Klein, Franz, Grundrechtliche Schutzpflicht des Staates, NJW 1989, 1633

Körner, Anne / Leitherer, Stephan / Mutschler, Bernd / Rolfs, Christian (Hrsg.), Kasseler Kommentar Sozialversicherungsrecht, Bd. Band 1, , 115. EG, 2021

Kort, Michael, Datenschutzrechtliche und betriebsverfassungsrechtliche Fragen bei IT-Sicherheitsmaßnahmen, NZA 2011, 1319

Krügel, Tina, Der Einsatz von Angrifferkennungssystemen im Unternehmen, MMR 2017, 795

Kugelmann, Dieter, Rahmenbedingungen für eine digitale Gesundheitsversorgung aktiv gestalten, DuD 2019, 398

Kühling, Jürgen / Buchner, Benedikt (Hrsg.), Datenschutzgrundverordnung Kommentar, 2. Auflage, 2018

Kühling, Jürgen / Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung BDSG Kommentar, 3. Auflage, 2020

Kulick, Andreas, „Drittwirkung" als verfassungskonforme Auslegung – Zur neuen Rechtsprechung des BVerfG, NJW 2016, 2236

Kutscha, Martin, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, 1042

Laue, Philip / Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Auflage, 2018

Luch, Anika, Das neue „IT-Grundrecht" - Grundbedingung einer „Online-Handlungsfreiheit", MMR 2011, 75

Management & Krankenhaus, Das Outsourcing ist kein Selbstläufer, https://www.management-krankenhaus.de/topstories/it-kommunikation/das-outsourcing-ist-kein-selbstlaeufer (abgerufen am 26.11.2021)

Mandl, Peter, Internet Internals - Vermittlungsschicht, Aufbau und Protokolle, 2018

Mandl, Peter / Bakomenko, Andreas / Weiß, Johannes, Grundkurs Datenkommunikation, 2. Auflage, 2010

Martini, Mario / Hohmann, Matthias, Der gläserne Patient: Dystopie oder Zukunftsrealität?, NJW 2020, 3573

Matz-Lück, Nele / Hong, Mathias (Hrsg.), Grundrechte und Grundfreiheiten im Mehrebenensystem - Konkurrenzen und Interferenzen, 2011

Maunz, Theodor / Dürig, Günter / Herdegen, Matthias, GG – Kommentar, 8. Auflage, 63. EL, 2011

Mehler-Bicher, Anett / Mehler, Frank / Kuntze, Nicolai / Kunz, Sibylle / Ostheimer, Bernhard / Steiger, Lothar / Weih, Hans-Peter (Hrsg.), Wirtschaftsinformatik Klipp und Klar, 2019

Meier, Michael, IntrusionDetection effektiv! - Modellierung und Analyse von Angriffsmustern, 2007

Meyer, Jürgen, Charta der Grundrechte der Europäischen Union Kommentar, 4. Auflage, 2014

Meyer, Jürgen / Hölscheidt, Sven (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Auflage, 2019

Michl, Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, DuD 2017, 349

Milenkoski, Aleksandar, Evaluation of Intrusion Detection Systems in Virtualized Environments, 2016

Miller, Dennis, Der Einsatz von IT-Systemen zur Erkennung und Abwehr von Cyberangriffen, NdsVBl 2021, 1

Nebel, Maxi, Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? - Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht, ZD 2015, 517

Niedersächsisches Ministerium für Inneres und Sport, Leitfaden für Behörden: Das NDIG und andere Gesetze zur digitalen Verwaltung, 2020

Niedersächsisches Ministerium für Inneres und Sport, NDIG und OZG: Rechtsrahmen für die digitale Verwaltung in Niedersachsen, https://www.mi.niedersachsen.de/startseite/themen/it_bevollmachtigter_der_landesregierung/recht/rechtliche-grundlagen-fuer-egovernment-62293.html (abgerufen am 28.11.2021)

Obermann, Kristof / Horneffer, Martin, Datennetztechnologien für Next Generation Networks, 2. Auflage, 2012

Oppel, Florian / Sendke, Thomas, Unionsrechtlicher Grundrechtsschutz beim internationalen Informationsaustausch, IStR 2018, 110

Paal, Boris P. / Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar, 2. Auflage, 2018

Paal, Boris P. / Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz Kommentar, 3. Auflage, 2021

Papier, Hans-Jürgen, Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft, NJW 2017, 3025

Pieper, Niels, Grundstrukturen des verfassungsrechtlichen Datenschutzes – Zum Schutz personenbezogener Daten durch die Grundrechte des Grundgesetzes bei Maßnahmen der Gefahrenabwehr, JA 2018

Plenk, Valentin, Angewandte Netzwerktechnik kompakt, 2. Auflage, 2018

Redaktion KWM, Datenschutz: Wie Kliniken Patientendaten bei externen Aufträgen schützen können, https://blog.klinik-wissen-managen.de/datenschutz-wie-kliniken-patientendaten-bei-externen-auftraegen-schuetzen-koennen/ (abgerufen am 26.11.2021)

Rolfs, Christian / Giesen, Richard / Kreikebohm, Ralf / Meßling, Miriam / Udsching, Peter (Hrsg.), BeckOK Sozialrecht, 62. Edition, 2021

Roßnagel, Alexander, Kein „Verbotsprinzip“ und kein „Verbot mit Erlaubnisvorbehalt“ im Datenschutzrecht, NJW 2019, 1

Roßnagel, Alexander / Schnabel, Christoph, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534

Safferling, Christoph, Der EuGH, die Grundrechtecharta und nationales Recht: Die Fälle Åkerberg Fransson und Melloni, NStZ 2014, 545

Schantz, Peter / Wolff, Heinrich Amadeus, Das neue Datenschutzrecht, 2017

Scheurle, Klaus-Dieter / Mayen, Thomas (Hrsg.), Telekommunikationsgesetz - Kommentar, 3. Auflage, 2018

Schill, Alexander / Springer, Thomas, Verteilte Systeme, 2. Auflage, 2011

Schlegel, Hendrik, Einsatz von sog. „Data Loss Prevention“-Software im Unternehmen - Automatisierte Überprüfung ausgehender E-Mails bei erlaubter Privatnutzung, MMR 2020, 3

Schmitz, Dominik, Die Grundrechtecharta als Teil der Verfassung der Europäischen Union, EuR 2004, 691

Schneider, Jochen, Datenschutz nach der EU-Datenschutz-Grundverordnung, 2. Auflage, 2019

Schramm, Marc / Shvets, Iryna, Umgang mit TK-Kundendaten nach Inkrafttreten der DS-GVO, MMR 2019, 228

Schramm, Marc / Shvets, Iryna, Verkehrsdaten zwischen ePrivacy-RL und ePrivacy-VO: Nutzung von TK-Diensten und personalisierter Werbung, MMR 2019, 568

Schröder, Markus, Der risikobasierte Ansatz in der DS-GVO - Risiko oder Chance für den Datenschutz?, ZD 2019, 503

Schumacher, Pascal / Sydow, Lennart / von Schönfeld, Max, Cookie Compliance, quo vadis? Datenschutzrechtliche Perspektiven für den Einsatz von Cookies und Webtracking nach TTDSG und ePrivacy-VO, MMR , 603

Simitis, Spiros, Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398

Simitis, Spiros / Hornung, Gerrit / Döhmann, Indra (Hrsg.), Datenschutzrecht - DGVO mit BDSG, 2019

Skistims, Hendrik / Roßnagel, Alexander, Rechtlicher Schutz vor Staatstrojanern?, ZD 2012, 3

Smart Grid Task Force EG2, Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection, https://ec.europa.eu/energy/sites/ener/files/documents/Recommendations%20regulatory%20requirements%20v1_0_clean%20%282%29.pdf (abgerufen am 15.11.2019)

Specht, Louisa / Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019

Spindler, Gerald / Schmitz, Peter / Liesching, Marc (Hrsg.), Telemediengesetz Kommentar, 2. Auflage, 2018

Spindler, Gerald / Schuster, Fabian (Hrsg.), Recht der elektronischen Medien, 4. Auflage, 2019

Stelkens, Paul / Bonk, Hein Joachim / Sachs, Michael, Verwaltungsverfahrensgesetz – Kommentar, 8. Auflage, 2014

Stoklas, Jonathan, Das Patientendaten-Schutz-Gesetz – Mehr Rechte für Patienten?, ZD-Aktuell 2020, 07308

Streinz (Hrsg.), EUV/AEUV Kommentar, 3. Auflage, 2018

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung Handkommentar, 2. Auflage, 2018

Taeger, Jürgen / Gabel, Detlev (Hrsg.), Kommentar DSGVO - BDSG, 3. Auflage, 2019

Thüsing, Gregor (Hrsg.), Beschäftigtendatenschutz und Compliance, 3. Auflage, 2021

Tschammler, Deniz, IT-Sicherheit im Gesundheitswesen – Schutz kritischer Infrastrukturen und Verifikation von Arzneimitteln, PharmR 2019, 509

Veil, Winfried, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686

Veil, Winfried, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, 686

Wendzel, Steffen, Tunnel und verdeckte Kanäle im Netz - Grundlagen, Protokolle, Sicherheit und Methoden, 2012

Wendzel, Steffen, IT-Sicherheit für TCP/IP- und IoT-Netzwerke, 2018

Wente, Jürgen, Informationelles Selbstbestimmungsrecht und absolute Drittwirkung der Grundrechte, NJW 1984, 1446

Winter, Philipp / Lampesberger, Harald / Zeilinger, Markus / Hermann, Eckehard, Anomalieerkennung in Computernetzen, DuD 2011, 235–239

Wölbert, Christian, Schmerzhafte Lektion: Was Emotet anrichtet – und welche Lehren die Opfer daraus ziehen, c't 2020, 14

zdf.de, IT-Ausfall war erpresserischer Hacker-Angriff, https://www.zdf.de/nachrichten/panorama/hacker-angriff-uniklinik-duesseldorf-100.html (abgerufen am 10.12.2021)

Zickler, Michael C., Die digitale Verwaltung in Niedersachsen, NordOer 2020, 441

Einführung von Intrusion-Detection-Systemen - Grundlagen, Version 1.0, 2002

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, 2020

Sachverständigengutachten zu 57 S 87/08, https://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2011-07-29_Sachverst_an_LG.pdf (abgerufen am 27.11.2021)