Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

11
K&R

24. Jahrgang November 2021 Seiten 685 – 756

dfv Mediengruppe · Frankfurt am Main

besteht.[34] Das richtet sich danach, ob zur Prüfung des Anspruchs die Prüfung des geschlossenen Vertrags unerlässlich ist. Hierzu stellt die Wikingerhof-Rechtsprechung auch klar, dass in derartigen Fällen regelmäßig den Geschäftspartnern keine Wahl bleibt als der Abschluss der entsprechenden Geschäftsbeziehungen. Ebenso argumentativ dies stützend ist der Hinweis auf den Gleichlauf zwischen Entsperransprüchen und einem Kontrahierungszwang auf erstmalige Herstellung einer Geschäftsbeziehung. Das Marktmachmissbrauchsverbot stellt die deliktsrechtlichen Schranken eines jeden Vertrags des marktbeherrschenden Unternehmens dar. Was jedoch missbräuchlich ist, richtet sich nach dem gesetzlichen Abwägungsmaßstab und dem Erfolgsort. Die zwar vertraglichen Plattform-Bedingungen stellen hierbei lediglich tatsächlich in wettbewerblicher Hinsicht berücksichtigungsfähige tatsächliche Umstände dar. Beeinträchtigt wird der Wettbewerb durch die Sperre jedoch in Deutschland.

Diese Argumente nicht ansprechend nimmt das LG Hannover seine internationale Zuständigkeit nach Art. 7 Nr. 1 Brüssel-Ia-VO an.[35] Die Frage der vertraglichen Berechtigung des Verkäufers zum Vertrieb über die Amazon-Plattform lasse sich nicht losgelöst von den vertraglichen Regelungen des Vertriebsvertrags beurteilen. Der Erfüllungsort dieses Vertrags liege allerdings in diesem Fall in Deutschland, da neben den Dienstleistungen in Luxembourg auch Logistik und Warenversendung in Deutschland Gegenstand des Vertrags waren. Dieses Ergebnis mag den Besonderheiten dieses Verfügungsverfahrens geschuldet sein, das auch die Sperre der Logistikleistungen und Androhung der Vernichtung in Deutschland eingelagerter Waren umfasste. Bei einem reinen Abstellen auf die Vermittlungsleistung wäre deshalb auch hier eine Ablehnung der internationalen Zuständigkeit zu befürchten gewesen.

Sowohl bei der internationalen Zuständigkeit nach Art. 7 Nr. 2 Brüssel-Ia-VO wie auch dem besonderen Gerichtsstand der unerlaubten Handlung nach § 32 ZPO kommt es auf den Begehungsort an. Dies ist jeder Ort, an dem nur eines der maßgeblichen Merkmale der unerlaubten Handlung begangen wurde, damit also jeder Handlungs- und jeder Erfolgsort.[36] Kommt es bei der hier begehrten Wiederzulassung als Amazon-Verkäufer auf den Zugang zu den vermittelten Absatzmärkten an, so ist jede verweigerte Vermittlung zu einem potenziellen Amazon-Kunden Erfolg der deliktischen Handlung. Da diese wiederum überall sitzen können, wird auch die Sperre an jedem Ort begangen. Der Verkäufer hat damit gemäß § 35 ZPO die Wahl unter den örtlich zuständigen Gerichten an jedem dieser Orte.[37]

3. Antrag

Im Zusammenhang mit kartellrechtlichen Entsperransprüchen können sich Fragen nach dem zivilprozessualen Bestimmtheitserfordernis stellen. Da sie sich materiellrechtlich auf die Anspruchsgrundlage aus § 33 Abs. 1 GWB stützen, ist den dabei geltenden Besonderheiten Rechnung zu tragen. Hiernach genügt es aber, wenn die Hauptleistungspflichten des Kontrahierungszwangs hinreichend bestimmt beschrieben sind, sodass eine Vollstreckung aus einem Titel ohne inhaltliche Fortsetzung des Streits möglich ist.[38] Es reicht demnach bei einem Entsperranspruch gegenüber Amazon aus, die vorgenommene Sperre und das Verkäuferkonto zu beschreiben und die begehrte Unterlassung darzustellen.

IV. Zusammenfassung

Gegen sachlich nicht gerechtfertigte Sperren ihrer Amazon-Verkäuferkonten können sich Unternehmen erfolgversprechend gerichtlich zur Wehr setzen. Dies kann auch im Wege des einstweiligen Rechtsschutzes erfolgen, wenn zusätzlich zu den allgemeinen Voraussetzungen existenzbedrohende Umstände glaubhaft gemacht werden können. Gerichtliche Anträge können dabei regelmäßig in Deutschland gestellt werden, da es auf die Auslegung eines Vertrags nicht ankommt, sondern durch das Marktmachtmissbrauchsverbot lediglich die deliktsrechtlichen Grenzen eines möglichen Sperrverhaltens durch Amazon bestimmt werden.

34 EuGH, 24. 11. 2020 – C-59/19, K&R 2021, 41 ff. = GRUR 2021, 116 = ECLI:EU:C:2020:950, Rn. 33 – Wikingerhof; BGH, 10. 2. 2021 – KZR 66/17 – Wikingerhof, Rn. 11.

35 LG Hannover, 22. 7. 2021 – 25 O 221/21.

36 *Toussaint*, in: Vorwerk/Wolf, BeckOK ZPO, 41. Ed. 2021, § 32 ZPO Rn. 9.

37 Mit diskutierten Einschränkungen aber *Heinrich*, in: Musielak/Voit, ZPO 18. Aufl. 2021, § 32 Rn. 18.

38 *Ollerdißen*, in: Wiedemann (Fn. 29), § 61 Rn. 62.

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

Update IT-Sicherheitsrecht

Kurz und Knapp

Die Autoren stellen für das IT-Sicherheitsrecht relevante legislative und judikative Entscheidungen aus dem Zeitraum 2020/2021 vor.

I. Einführung und Abgrenzung zum IT-Sicherheitsrecht

Die Informatik hat die IT-Sicherheit längst als eigenen, wichtigen Schwerpunkt etabliert. Sie nennt Sicherheitslücken „vulnerabilities“, deren Ausnutzung „exploit“ und das daraus resultierende Risiko „threat“. Die Rechtswissenschaft dagegen streitet noch um Existenz und Definition des IT-Sicherheitsrechts. Nach dem Verständnis der Autoren umfasst es alle Rechtsnormen und Rechtssätze, die die Verfügbarkeit, Integrität und Vertraulichkeit (= Schutz-

* Mehr über die Autoren erfahren Sie auf S. VIII. Der Beitrag geht auf einen Vortrag bei der DSRI-Herbstakademie 2021 zurück, der veröffentlicht wurde im Tagungsband von Taeger (Hrsg.), Im Fokus der Rechtsentwicklung – Die Digitalisierung der Welt, 2021, S. 321 ff. Er ist überarbeitet und aktualisiert zum Stand November 2021. Alle zitierten Internetquellen wurden zuletzt abgerufen am 9. 10. 2021.

ziele) von informationstechnischen Systemen (= Schutzobjekte) betreffen.[1] Diese Betrachtung passt auch zu § 2 Abs. 6 BSIG,[2] der eine Legaldefinition für Sicherheitslücken liefert. Die Folgen unzureichender IT-Sicherheit zeigt eine Wahlkampf-App: Unbefugte konnten Daten auslesen, die Wahlhelfer in Bürgergesprächen gesammelt hatten, insbesondere Namen, Anschrift und politische Einstellung.[3] Außerdem beziffert der BSI-Lagebericht 2020 u. a. wirtschaftliche Schäden durch Ransomware.[4] Angriffe nutzen Programmierfehler aus, die von Softwareentwicklern verursacht sind, sowie schlechte Systemadministration und Sicherheitslücken in Fernwartungs- und VPN-Zugängen.[5]

II. IT-Sicherheit in der Gesetzgebung und Rechtsprechung

Im Zeitraum 2020/21 betreffen folgende nationale und europäische Gesetzesakte und Gerichtsentscheidungen die IT-Sicherheit.

1. EU-Cybersicherheitsstrategie 2020

Die EU will die Widerstandsfähigkeit (Resilienz) kritischer Infrastrukturen gegen Sicherheitsvorfälle erhöhen, dazu die Prävention, Abschreckung und Reaktion verbessern und dabei einen globalen, offenen Cyberraum fördern. Diese „Cybersicherheitsstrategie für die digitale Dekade" vom 16. 12. 2020 ist als „Soft Law" nicht verbindlich, aber für die Auslegung von Rechtsakten relevant. Dazu stehen die Novellierung der NIS-Richtlinie (RL) 2016/1148 und Regulierungen für das Internet der Dinge auf dem Plan, ebenso wie die verstärkte Vernetzung von Sicherheitseinsatzzentren, Normungen und Standards zur IT-Sicherheit, die Förderung der IT-Sicherheit in Unternehmen und der kurzfristige Ausbau des 5G-Instrumentariums. Kriminalitätsbekämpfung und diplomatische Reaktionen auf Cyberangriffe i. S. d. Art. 215 AEUV (z. B. das Einfrieren von Konten ermittelter Täter) ergänzen das Paket.[6]

2. Europäisches Kompetenzzentrum für Cybersicherheit und Joint Cyber Unit

Die Verordnung (EU) 2021/887 (gilt seit 28. 6. 2021) schafft das Kompetenzzentrum für Cybersicherheit mit Sitz in Bukarest mit dem Ziel, Forschung, Innovation und Realisierung im Bereich der Cybersicherheit zu fördern (so Art. 3 der Verordnung). Wissenschaftliche Kritikpunkte, insbesondere zur Abgrenzung der neuen Behörde von der Agentur der EU zur Netz- und Informationssicherheit (ENISA), sind nicht berücksichtigt. Zur koordinierten Abwehr EU-weiter IT-Angriffe gibt es einen Vorschlag für eine „Joint Cyber Unit".[7]

3. Entwicklungen zum Cybersecurity Act

Der „Cybersecurity Act" (VO (EU) 2019/881) sieht u. a. vor, ein System EU-weiter IT-Sicherheitszertifizierungen zu schaffen (dort die Artt. 46 ff.).

Der erste hierzu veröffentlichte Zertifizierungsrahmen ist das „EUCC Scheme V.1.1.1", das die ENISA gemäß den Artt. 48 Abs. 2, 49 VO (EU) 2019/881 auf der Grundlage einschlägiger ISO-Normen und den Common Criteria erstellt hat.[8] Es definiert Kriterien für Zertifizierungsstellen sowie zur Entwicklung und den Eigenschaften eines IT-Produkts. Die kritische Auseinandersetzung damit bleibt einer gesonderten Betrachtung vorbehalten, die Autoren vermissen indes z. B. bei den „Minimum Site Security Requirements" für Softwareentwickler[9] klare Qualitätsvorgaben zur Softwareerstellung wie z. B. Coding-Standards und Vorgaben zu verpflichtenden Penetration-Tests: In einigen Fällen soll es aus Sicht des EUCC ausreichen, nur zu prüfen, ob die verwendeten Softwareprodukte bekannte Sicherheitslücken haben. Gleichzeitig schlägt das EUCC eine komplexe Metrik zur Bewertung von so entdeckten Problemen vor, die jeder Erfahrung aus der IT-Sicherheit zuwiderläuft: Ungepatchte Vulnerabilities bleiben ein Einfallstor für Angreifer, egal wie „alt" oder kompliziert.[10]

---

1 Führende Fachverbände wie z. B. die Gesellschaft für Informatik (GI, https://fb-sicherheit.gi.de/), die Association of Computing Machinery (ACM, https://www.acm.org/special-interest-groups/sigs/sigsac) und das Institute of Electrical and Electronics Engineers (IEEE, https://www.computer.org/communities/technical-committees/tcsp) haben Fachgruppen für IT-Sicherheit. Informatik-Literatur zur IT-Sicherheit bieten z. B. *Stallings/Brown*, Computer Security, Master-Studiengänge haben den Schwerpunkt IT-Sicherheit (z. B. https://www.rwu.de/studieren/studiengaenge/informatik). Zur fehlenden Abgrenzung aus rechtlicher Sicht z. B. *Voigt*, IT-Sicherheitsrecht, 2018, Einleitung Rn. 2 („Ein Recht der IT-Sicherheit … gibt es nicht"); mit einem Definitionsvorschlag *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechtshandbuch, 36. Erg.-Lfg., 2021, IT-Sicherheit, Rn. 233; ähnlich *Hornung/Schallbruch*, IT-Sicherheitsrecht, 2021, Kap. 1 Rn. 11 - 15.

2 BSIG = Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

3 *Wittmann*, Wenn die CSU und die Volkspartei digitalen Wahlkampf machen…, https://lilithwittmann.medium.com/wenn-die-csu-und-die-volkspartei-digitalen-wahlkampf-machen-6d9e245efefc; üblich ist bei der Entdeckung derartiger Sicherheitslücken das sogenannte „Responsible Disclosure-Verfahren", bei dem die Lücke zunächst nur dem Verantwortlichen und gegebenenfalls den Behörden angezeigt wird; nachdem der Verantwortliche die Behebung der Lücke gemeldet hat, darf sie vom Entdecker publiziert werden. An dieses Vorgehen hielt sich die Entdeckerin der Sicherheitslücke, dennoch erstattete die betroffene Partei Strafanzeige gegen sie. Die StA hat das Verfahren mangels Tatverdacht eingestellt. Bemerkenswert an der Einstellungsverfügung ist die Aussage, dass kein Schutz der Daten im Sinne des § 202a StGB vorlag, sondern diese ungeschützt erreichbar gewesen seien, https://netzpolitik.org/2021/cdu-connect-ermittlungsverfahren-gegen-sicherheitsforscherin-lilith-wittmann-eingestellt/.

4 Ransomware verschlüsselt Datenträger und fordert zum Entschlüsseln ein Lösegeld.

5 Zum Ganzen: *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 31 ff.; beispielhaft für Vorfälle: VPN-Sicherheitslücken: https://thehackernews.com/2021/06/north-korea-exploited-vpn-flaw-to-hack.html, Lösegeldzahlung des Fleischkonzerns JBS: https://www.handelsblatt.com/unternehmen/handel-konsumgueter/cyberkriminalitaet-fleischproduzent-jbs-zahlt-hackern-rund-11-millionen-dollar-loesegeld/27272370.html, Angriff auf eine Ölpipeline: https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices; Lagebericht des BSI 2020, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html (dort S. 14, 33, 34).

6 Cybersicherheitsstrategie der EU für die digitale Dekade (JOIN(2020) 18 final): https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020JC0018&from=EN, bestätigt durch den Beschluss des Rates der EU vom 22. 3. 2021 (Dokument 6722/21): https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/de/pdf; zur EU-Cybersicherheitsstrategie 2017 sowie zur Strategie für eine Sicherheitsunion und dem Charakter als Soft Law *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 269, 272, 280; am 17. 5. 2021 hat der Rat der EU Sanktionen gemäß Art. 215 AEUV verlängert, https://www.consilium.europa.eu/de/press/press-releases/2021/05/17/cyber-attacks-council-prolongs-framework-for-sanctions-for-another-year/; außerdem gibt es verschiedene EU-Strategien zur Digitalisierung, auf denen u. a. der Entwurf für eine KI-Verordnung beruht (COM(2021) 206 final vom 21. 4. 2021, dazu *Grützmacher/Füllsack*, ITRB 2021, 159 - 164).

7 Zum Kompetenzzentrum: ABl. L 202/1 vom 8. 6. 2021; zur Kritik: *Von Wintzigerode/Müllmann*, in: Taeger (Hrsg.), Den Wandel begleiten, 2020, S. 475, 482, 484; zur geplanten „Joint Cyber Unit" COM (2021) 4520 final vom 23. 6. 2021, abrufbar unter https://digital-strategy.ec.europa.eu/en/library/recommendation-building-joint-cyber-unit.

8 EUCC = Common Criteria based European candidate cybersecurity certification scheme, seit 25. 5. 2021 abrufbar unter https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1/; dazu *Kowalski/Intemann/Mühlenbruch*, DuD 2021, 244, 246.

9 Seiten 78, 112 ff., Ziffer 9.6 EUCC.

10 Ein Beispiel für einen komplex auszunutzenden Exploit liefert CVE-2019-10149 (https://packetstormsecurity.com/files/153218/Exim-4.9.1-Remote-Command-Execution.html), i. Ü. zum Software-Qualitätsmanagement *Deusch/Eggendorfer*, in Taeger/Pohle (Fn. 1), Rn. 226; generell wäre analog zum Kfz-Bereich eine Art TÜV zu begrüßen, der vor Inverkehrbringen eine vollständige Qualitäts- und Sicherheitsprüfung durchführt.

In formeller Hinsicht ist durch das EUCC ein Standard geschaffen, den die EU-Kommission durch einen Durchführungsrechtsakt gemäß Art. 49 Abs. 7 VO (EU) 2019/881 zu einer rechtsverbindlichen Zertifizierungsvorgabe machen kann.

Neben dem EUCC hat die ENISA bereits den ersten Entwurf für einen Zertifizierungsrahmen für Cloud Services veröffentlicht und ein Schema für die Sicherheitszertifizierung von 5G-Produkten angekündigt.[11]

4. Aktualisierung der NIS-Richtlinie und Richtlinie über die Resilienz kritischer Einrichtungen

Im Dezember 2020 hat die Europäische Kommission eine überarbeitete NIS-Richtlinie (NIS 2) mit folgenden Novellierungen vorgeschlagen:[12]

Während die Artt. 14 und 16 der bisherigen NIS-RL (EU) 2016/1146 zwischen Betreibern wesentlicher Dienste (KRITIS-Unternehmen i. S. v. § 2 Abs. 10 BSIG) und Anbietern digitaler Dienste unterscheidet, benennt Art. 1 NIS 2 i. V. m. Anhängen I und II wesentliche und wichtige Einrichtungen (wozu die Anbieter digitaler Dienste zählen). Die Anhänge I und II NIS 2 adressieren die IT-Sicherheitspflichten auch an weitere Bereiche wie z. B. Teile der öffentlichen Verwaltung, die Infrastruktur für den Weltraum, Post, Abfallwirtschaft, Chemie und Lebensmittel, Teile des produzierenden Gewerbes einschließlich Kfz- und Maschinenbau.

Die behördlichen Strukturen werden verstärkt, etwa durch die Einrichtung eines Schwachstellenregisters und Vorgaben zum Krisenmanagement (Artt. 6 und 7 NIS 2), zum behördlichen Informationsaustausch einschließlich der Errichtung eines Europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe, Artt. 8 - 11, 12 - 14 NIS 2) und durch ein Berichts- und Peer Review-System zur Wirksamkeit der Sicherheitskonzepte (Artt. 15, 16 NIS 2).

Für die behördliche und unternehmerische Governance definiert Art. 17 NIS 2 die „Cybersicherheit" als Leitungs- und Kontrollaufgabe; die Leitungsorgane sollen für Sicherheitsverstöße ihrer Einrichtungen „rechenschaftspflichtig" sein. Art. 18 NIS 2 definiert Anforderungen an das Risikomanagement der IT-Sicherheit.

Gemäß Art. 20 NIS 2 müssen Einrichtungen wesentlicher und wichtiger Dienste wie bisher Sicherheitsvorfälle melden, aber künftig auch Bedrohungen als Vorstufe von Sicherheitsvorfällen.

Aufgrund der Pflicht der Mitgliedstaaten zu wirksamen Durchsetzungsmaßnahmen sind Ausweitungen der behördliche Befugnisse zu erwarten.

Ergänzend zu NIS 2 hat die EU-Kommission die Richtlinie über die Resilienz kritischer Einrichtungen vorgeschlagen.[13] Für diese Einrichtungen sollen den Behörden weitere Sicherheitsmaßnahmen ermöglicht werden, auch, soweit sie nicht die IT-Sicherheit betreffen.

5. Brexit und IT-Sicherheit

NIS 2 zeigt die Auswirkungen des Brexits auf das europäische IT-Sicherheitsrecht. Seit dem 1. 1. 2021 findet das EU-Recht in Großbritannien (UK) keine Anwendung mehr. Stattdessen gilt Teil 4, Titel II, Artt. 704 - 707 des Handels- und Kooperationsabkommens.[14] Danach sind Kooperation und Informationsaustausch zu IT-Sicherheitsfragen zwischen EU und UK weiterhin möglich, auch auf Ebene der Computer-Notfallteams der NIS-RL 2016/1146 und der ENISA, aber ausschließlich auf freiwilliger Basis.

Allerdings hat UK verschiedene Regelungen des EU-Rechts auf nationaler Ebene als sogenanntes „retained EU law" für verbindlich erklärt, darunter auch die NIS-RL 2016/1146 (ebenso den TK-Kodex der RL (EU) 2018/1972, allerdings ohne dessen IT-Sicherheitspflichten aus Titel V). Da das „retained EU law" den Stand zum 1. 1. 2021 „einfriert", nimmt UK nicht mehr an Rechtsänderungen teil, weshalb sich eine Divergenz im IT-Sicherheitsrecht ergeben wird.

Ob UK hiernach noch als sicheres Drittland i. S. d. DSGVO gelten kann, ist fraglich. Aufgrund der aktuellen Rechtslage hat die EU-Kommission dies durch ihren Angemessenheitsbeschluss gemäß Art. 45 DSGVO vom 28. 6. 2021 bejaht, trotz einer vorangegangenen Ablehnung durch das EU-Parlament.[15]

6. IT-Sicherheitsgesetz 2.0

Das IT-Sicherheitsgesetz 2.0 ist am 28. 5. 2021 in Kraft getreten (§§ 4a, 4b und 8 erst am 1. 12. 2021), insbesondere mit folgenden Änderungen:[16]

Zu den KRITIS-Sektoren zählt gemäß § 2 Abs. 10 S. 1 Nr. 1 BSIG nunmehr auch die Siedlungsabfallentsorgung. Die IT-Sicherheitsvorkehrungen der KRITIS-Betreiber müssen ab dem 1. 5. 2023 auch Angriffserkennungssysteme erfassen (§ 8a Abs. 1a BSIG).[17] KRITIS-Unternehmen müssen sich gemäß § 8b Abs. 3 BSIG beim BSI registrieren und tragen im meldepflichtigen Störfall gemäß § 8b Abs. 4a BSIG erweiterte Auskunftspflichten gegenüber dem BSI. Sie dürfen Kritische Komponenten (§ 2 Abs. 10 BSIG) nur nach Anmeldung bzw. bis zur Untersagung des Bundesinnenministeriums einsetzen (§ 9b Abs. 1 BSIG – ex ante-Verfahren bzw. § 9b Abs. 4 BSIG – ex post-Verfahren; für TK-Anbieter gilt eine Zertifizierungspflicht gemäß § 109 Abs. 2 S. 4 TKG – ab 1. 12. 2021: § 165 TKG). Die Pflichten des BSIG sind ausgedehnt auf Unternehmen im besonderen öffentlichen Interesse; sie haben sich beim BSI zu registrieren und eine Selbsterklärung ihrer IT-Sicherheitsvorkehrungen vorzulegen (§§ 2 Abs. 14, 8f BSIG).

---

11 Zu 5G: https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification; zu den Cloud-Diensten: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme.

12 Dokument COM(2020) 823 final, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0823&from=EN mit Begründung des Entwurfs, siehe auch die Stellungnahme des Europäischen Datenschutzbeauftragten vom 11. 3. 2021 unter https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-cybersecurity-strategy-and-nis-20_en mit kritischen Anmerkungen zur Terminologie (dort Ziffer 32 zu „Cybersicherheit") und zu Tendenzen, Ende-zu-Ende-Verschlüsselungen zu umgehen (dort Ziffern 62, 63), ebenso *Kipker/Birreck/Niewöhner/Schnorr*, MMR 2021, 214 ff.

13 COM 2020/829 final, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0829&from=EN.

14 ABl. EU Nr. L 149/10 vom 30. 4. 2021.

15 *Walden/Michels*, Int. Cybersecur Law Rev., 2021, 19, 20, 21; zur Ablehnung des Angemessenheitsbeschlusses durch das EU-Parlament *Scheuch*, ITRB 2021, 150; zum dennoch gefassten Angemessenheitsbeschluss der EU-Kommission: https://www.juris.de/jportal/portal/page/homerl.psml?nid=jnachr-JUNA210602508&wt_mc=pushservice&cmsuri=%2Fjuris%2Fde%2Fnachrichten%2Fzeigenachricht.jsp.

16 BGBl. I-2021 vom 27. 5. 2021, S. 1122 ff.; für einen Überblick über die einzelnen Änderungen und weitere Nachweise *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 408 sowie *Hornung*, NJW 2021, 1985 - 1991, *Niemann/Karniyevich*, K&R 2021, 441 - 448; *Schallbruch*, CR 2021, 450 - 455 und 516 - 523.

17 Eine systematische Angriffserkennung durch Intrusion Detection Systeme (IDS) war nach Auffassung der Autoren bereits bislang gemäß Art. 33 DSGVO bzw. § 13 TMG und § 109 TKG geboten, *Deusch/Eggendorfer*, in: Taeger (Hrsg.), Rechtsfragen digitaler Transformation, 2018, S. 741, 750; ergänzt in: K&R 2018, 753, 757.

Schließlich sind dem BSI neue Aufgaben und Befugnisse zur Gefahrenabwehr zugeschrieben worden, zum Beispiel um Portscans durchzuführen in der – technisch unbegründeten – Hoffnung, damit Sicherheitslücken zu entdecken.[18] Die §§ 7c und b BSIG räumen dem BSI die Befugnis ein, gegenüber Anbietern von Telekommunikation und Telemedien Maßnahmen zur Abwehr konkreter Gefahren anzuordnen. Eingriffe in Endgeräte, zum Teil ohne Kenntnis der Nutzer ermöglicht § 7c Abs. 1 Nr. 2 BSIG. Hiernach kann das BSI TK-Anbieter anweisen, Bereinigungsbefehle zur Löschung von Schadsoftware an informationstechnische Systeme zu verteilen, die an ihr Kommunikationsnetz angeschlossen sind. Da weder das BSI noch die TK-Anbieter wissen, welche Endgeräte mit welchen Eigenschaften von den Bereinigungsbefehlen betroffen sind, besteht die Gefahr von Kollateralschäden, was sich insbesondere in sensiblen IT-Anwendungen wie z. B. in Krankenhäusern als schwierig erweisen könnte.

Neben dem Bundesgesetzgeber versprechen sich einige Länder eine Erhöhung der IT-Sicherheit durch entsprechende Landesgesetze, zum Beispiel durch das Cybersicherheitsgesetz Baden-Württemberg.[19]

7. IT-Sicherheitsaspekte im TK-ModG

Das Telekommunikationsmodernisierungsgesetz (TK-ModG) dient der Umsetzung der Richtlinie des TK-Kodex (RL (EU) 2018/1972).[20] Das Gesetz tritt gemäß dessen Art. 61 am 1. 12. 2021 in Kraft; durch Art. 1 erhält das bisherige TKG eine vollständige Neufassung. Das Telekommunikationsgeheimnis und der TK-Datenschutz sind im TKG-neu nicht mehr geregelt, sondern im Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG, siehe unten Ziffer 8). Die IT-Sicherheitspflichten sind in den §§ 164 - 183 TKG-neu geregelt; Verstöße sind je nach Tatbestand mit Bußgeldern zwischen € 10 000,00 und € 1,0 Mio. bzw. mit 1 - 2 % des Jahresumsatzes bewehrt (§ 228 Abs. 2 Nr. 35 - 61 und Abs. 7 und 8 TKG-neu).

Die technischen Vorkehrungen der Normadressaten (gemäß § 3 Nr. 61 TKG-neu auch sogenannte „OTT-Anbieter“[21]) gegen Störungen müssen statt bislang „erforderlich“ (§ 109 TKG) künftig „angemessen“ sein (§ 165 Abs. 1, 2 TKG-neu). Die Angemessenheit definiert § 165 Abs. 6 TKG-neu. Dabei können auch Angriffserkennungssysteme i. S. d. § 2 Abs. 9b BSIG eingesetzt werden, bei „erhöhtem Gefährdungspotential“ ist dies sogar Pflicht (§ 165 Abs. 3 TKG-neu). Gemäß § 165 Abs. 3 S. 4 TKG-neu sollen Angriffserkennungssysteme erkannte Gefahren oder Bedrohungen abwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen.[22]

Die §§ 166 ff. TKG-neu regeln die bisherige Systematik der §§ 109 ff. TKG aus Sicherheitskonzept, (IT-) Sicherheitsbeauftragtem, Meldepflichten bei Sicherheitsvorfällen und Datenschutzverletzungen, Sicherheitskatalog und Aufsicht der Bundesnetzagentur bis hin zur Befugnis für eine Untersagung des TK-Dienstes gemäß § 183 TKG-neu.

8. TTDSG

Das TTDSG (Telekommunikation-Telemedien-Datenschutzgesetz) wird zeitgleich mit dem TK-ModG (siehe Ziffer 7.) ab 1. 12. 2021 in Kraft treten. Es soll die Vertraulichkeit und den Datenschutz in der Telekommunikation und bei der Nutzung von Telemedien regeln.[23]

Das Fernmeldegeheimnis und den TK-Datenschutz regelt Teil 2 des TTDSG, mit der überfälligen Entscheidung des Gesetzgebers, die Erben zum Zugriff auf die Daten aus der Kommunikation des Verstorbenen mit Dritten zu berechtigen (§ 4 TTDSG).[24] § 12 TTDSG erlaubt die Verarbeitung von TK-Daten zur Erkennung und Beseitigung von Störungen der Telekommunikation.[25]

In Teil 3 ist der Telemedien-Datenschutz geregelt. Die technischen und organisatorischen Vorkehrungen regelt § 19 TTDSG (statt bislang § 13 Abs. 7 TMG).[26] Auffallend sind die umfangreichen Regelungen zur Auskunft gegenüber Behörden über Bestands-, Zugangs- und Nutzungsdaten. Technische Fragen wirft § 23 Abs. 1 TTDSG auf. Hiernach soll ein Diensteanbieter zur Beantwortung behördlicher Auskunftsverlangen auf Passwörter seiner Nutzer zugreifen dürfen. Diensteanbieter, die ihre Pflichten aus § 19 TTDSG erfüllen und die Passwörter ihrer Nutzer nicht im Klartext aufbewahren, sondern „hashen“,[27] werden § 23 TTDSG nicht erfüllen können.

Die §§ 25 und 26 TTSG sollen die „Cookie-Regelung“ aus Art. 5 Abs. 3 E-Privacy-RL 2002/58/EG umsetzen. Dienste zur Verwaltung von Einwilligungen für die Speicherung von Informationen auf Endgeräten der Nutzer (sogenannte „PIMS“) sollen gemäß § 26 TTDSG Zertifizierungen erhalten, wenn sie unter anderem die Sicherheit und Zuverlässigkeit ihres Dienstes nachweisen können.[28]

9. Umsetzung der Digitale-Inhalte-Richtlinie und Planungen zum Produktsicherheitsrecht

Aufgrund der Digitale-Inhalte-RL (EU) 2019/770 haben Verbraucher gemäß § 327f BGB – neu ab dem 1. 1. 2022

18 Ein Portscan findet über das Netz verfügbare Dienste, soweit keine Firewall den Zugang dorthin verhindert. Er kann außerdem die Software-Version des Dienstes erkennen. Darüber lassen sich bekannte Sicherheitslücken erkennen. Allerdings ist das Verfahren sehr grob und kann problemlos von betroffenen Unternehmen verhindert werden – vielfach automatisch, da Firewall-Systeme kombiniert mit Network-Intrusion-Detection-Systemen Portscans erkennen und unterbinden, *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 34f., 408. Wer unter diesen Bedingungen bei einem Portscan Auffälligkeiten liefert, dürfte daher schwerwiegendere Probleme haben.

19 Cybersicherheitsgesetz Baden-Württemberg vom 4. 2. 2021 (GBl. 2021, 182).

20 BGBl. I-2021, S. 1858 ff.; eine hilfreiche Synopse zum bisherigen TKG und dem beschlossenen Gesetz liefert *Louven* unter https://louven.legal/wp-content/uploads/2021/06/Louven_TKG-Synopse.pdf; zum Referentenentwurf vom 9. 12. 2020 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 433 - 437 zum TK-Kodex der EU Rn. 289, jeweils m. w. N.

21 Zu den OTT („Over-the-top“)-Anbietern siehe z. B. *Deusch/Eggendorfer*, K&R 2017, 93 - 99, 96 f.

22 Ob sich der Gesetzgeber damit von dem Einsatz eines Intrusion Detection Systems nicht zu viel verspricht? Zur Funktionsweise von IDS: *Deusch/Eggendorfer*, in: Taeger (Fn. 19), S. 741, 750 und K&R 2018, 753, 757.

23 BGBl. I-2021, S. 1982 ff.; Regierungsentwurf mit Begründung: BT-Drs. 19/27441 v. 9. 3. 2021; zum TTDSG im Überblick: *Hanloser*, ZD 2021, 121; *Golland*, NWB 2021, 1818 - 1825; detailliert *Taeger/Gabel* (Hrsg.), DSGVO, BDSG, TTDSG, 4. Aufl. 2021.

24 Dazu BGH, 12. 7. 2018 – III ZR 183/17, K&R 2018, 633 ff. = NJW 2018, 3178 und *Deusch*, Digitales Sterben – das Erbe im Web 2.0 in: Taeger (Hrsg.), Law as a Service, 2013, S. 429, 438, 446.

25 Die Begründung des Regierungsentwurfs (BT-Drs. 19/27441 v. 9. 3. 2021. S. 35 f.) erlaubt die Folgerung, dass damit auch die Datenverarbeitung durch Angriffserkennungssysteme (Intrusion Detection Systems) gemeint ist. Wünschenswert wäre, der Gesetzgeber hätte die Begriffe aus TKModG und dem IT-SicherheitsG 2.0 verwendet.

26 Seite 37 der Gesetzesbegründung: BT-Drs. 19/27441 v. 9. 3. 2021.

27 Ein Hash erzeugt eine nicht umkehrbare Umrechnung des Passwortes, der Klartext ist also nicht wiederherstellbar. Dies hindert ein unbefugtes Lesen der Passwörter, dazu *Eggendorfer*, Gesalzen und gepfeffert. Hashes, Salz und Pfeffer, Linux Magazin 10/2015.

28 Zu den zahlreichen Fragen, die dabei noch offen sind siehe zum Beispiel *Golland*, NWB 2021, 1818, 1823 - 1825.

einen sogenannten „Update-Anspruch“ bei digitalen Produkten. Laut Gesetzesbegründung geht es v. a. um „Sicherheitsaktualisierungen“. Dies darf aber nicht als Freibrief verstanden werden, unsichere Produkte erst nach Inverkehrbringen durch „Sicherheitsupdates“ „sicher“ zu machen.[29]

Teilweise wird der Sicherheitsaspekt der digitale Inhalte-RL als Element in der unionsrechtlichen Gesetzgebung zu digitalisierten Produkten gesehen. In diesem Zusammenhang ist die EU mit der Novellierung der Produktsicherheitsrichtlinie 2001/95/EG befasst, die insbesondere eine Verbesserung der IT-Sicherheit von Produkten zum Ziel hat. Ein Abschluss des Verfahrens zur Richtliniensetzung ist indes noch nicht in Sicht.[30]

10. Patientendatenschutzgesetz vom 19. 10. 2020

Das Patientendatenschutzgesetz (PDSG) soll digitale Angebote der Gesundheitsversorgung ermöglichen, insbesondere durch Novellierungen im SGB V.[31] Für die IT-Sicherheit relevant sind die Regelungen zur Telematikinfrastruktur (TI, §§ 306, 307 SGB V). Dies sind die Komponenten, mit denen die „eHealth-Services“ genutzt werden sollen wie z. B. Lesegeräte für die elektronische Gesundheitskarte und Anwendungsdienste wie die elektronische Patientenakte (ePA). Der Aufbau der TI ist Aufgabe der Gesellschaft für Telematik, der Gematik GmbH (§ 311 SGB V). Deren datenschutzrechtliche Einordnung als Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO ist umstritten. § 307 SGB V (Datenschutzrechtliche Verantwortlichkeiten) bleibt daher unklar.[32]

Die Sicherheit der TI regeln die §§ 329 - 333 SGB V. Die Gematik GmbH ist zur Gefahrenabwehr verpflichtet und berechtigt, Diensteanbieter zur Gefahrenbeseitigung anzuweisen bis hin zur Sperrung von Diensten (§ 329 Abs. 1, 3 SGB V). Die Anbieter der Anwendungsdienste haben Störungen an die Gematik GmbH zu melden, welche die Meldungen an das BSI weiterleitet (§ 329 Abs. 2, 4 SGB V). Die Gematik GmbH und die Diensteanbieter müssen organisatorische und technische Vorkehrungen zur IT-Sicherheit treffen (§ 330 Abs. 1 SGB V). Die Gematik GmbH hat dem BSI Nachweise zur Erfüllung der Sicherheit zu erbringen und es über erkannte Sicherheitsmängel zu informieren (§ 330 Abs. 2, 3 SGB V).[33]

Im Vergleich zur Sicherheitsarchitektur des TKG fällt auf, dass die Meldepflichten bei Störungen nur gegenüber der Gematik GmbH gelten, aber nicht gegenüber den Betroffenen (wie in § 109a Abs. 1 TKG ab 1. 12. 2021: § 168 Abs. 6 bzw. § 169 Abs. 1 TKG-neu). Eine Meldepflicht der Gematik GmbH fehlt möglicherweise deshalb, weil der Gesetzgeber diese nicht als Verantwortliche i. S. d. Art. 4 Nr. 7 DSGVO ansieht. Ein Verzeichnis für Störungen (§ 109a Abs. 3 TKG ab dem 1. 12. 2021: § 169 Abs. 3 TKG-neu) ist nicht geregelt, auch nicht die Pflicht zur Benennung eines Sicherheitsbeauftragten (§ 109 Abs. 4 TKG ab 1. 12. 2021: § 166 Abs. 1 TKG-neu).

11. Legislative Tendenzen zur Umgehung von Verschlüsselung

Verschiedene legislative Akte streben an, die Verschlüsselung von Daten und Kommunikationssystemen zu umgehen, insbesondere folgende:

- Entschließung des Rates der Europäischen Union zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung,[34]
- Auskunftspflicht von TK- und Telemediendienste-Anbietern zu Passwörtern, § 8d BVerfSchG[35] und Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität vom 30. 3. 2021.[36]
- Am 29. 4. 2021 einigten sich das Europäische Parlament und der Rat darauf, per Verordnung Eingriffe in die Vertraulichkeit der Kommunikation zur Bekämpfung von sexuellem Missbrauch von Kindern zuzulassen.[37]
- Erweiterung polizeilicher Zugriffsrechte durch Quellen-TKÜ:

Der Gesetzesentwurf zu § 27d BPolG sah vor, die Rechte der Bundespolizei zum Einsatz der Quellen-TKÜ zu erweitern.[38]

Zudem änderte der Bundestag am 23. 6. 2021 § 86 StGB. Verboten ist künftig nicht nur, Propagandamittel von Organisationen zu verbreiten, die in Deutschland als verfassungswidrig eingestuft wurden (zum Beispiel aufgrund eines Vereinsverbots); vom Verbot wird zudem Material von Organisationen erfasst sein, die aufgrund der Benennung des Rates der EU auf der sogenannten „EU-Terrorliste“ stehen, aber nicht durch eine deutsche Behörde bzw. ein deutsches Gericht verboten worden sind. Die Erweiterung der Quellen-TKÜ erfolgt dabei mittelbar, da § 100a StPO den Einsatz des „Staatstrojaners“ bei Straftaten gemäß § 86 StGB zulässt. Mithin kann die Quellen-TKÜ künftig auch dann eingesetzt werden, wenn Material von Organisationen der „EU-Terrorliste“ verwendet wird, unabhängig davon, ob es dazu in Deutschland ein Verbotsverfahren gegeben hat.[39]

---

29 BGBl. I-2021, S. 2123 ff., 2126; zur Billigung des Gesetzesentwurfs BT-Drs. 19/27653 v. 17. 3. 2021 (mit Begründung zu den „Sicherheitsaktualisierungen“ auf S. 58) siehe BR-Drs. 568/21 v. 25. 6. 2021 (Ende der Umsetzungsfrist der RL war am 30. 6. 2021); zum Entwurf *Deusch/Eggendorfer*, in Taeger/Pohle (Fn. 1) Rn. 446, 447.

30 *Reusch*, BB 2021, 1218, 1222.

31 BGBl. 2020-I v. 19. 10. 2020, S. 2115; digitale Gesundheitsdienste sind bereits zuvor geregelt worden, zum Beispiel durch das „Digitale Versorgungsgesetz“, dazu *Dochow*, MedR 2020, 979.

32 Gematik GmbH: www.gematik.de, zur Verantwortlichkeit *Dochow*, MedR 2020, 979, 983, 984.

33 Zur einheitlichen Auslegung dieses Begriffs („TOM“) im IT-Sicherheitsrecht *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 284.

34 https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf; die Idee ist schon technisch nicht schlüssig: Verschlüsselung mit Hintertür ist per se unsicher. Sichere Verschlüsselung bietet keinen Zweitzugang. Mithin beauftragt der Rat der EU hier Forschung zur Quadratur des Kreises und verschwendet erheblich EU-Mittel.

35 BGBl. 2021-I, v. 1. 4. 2021, S. 448 ff.; dort auch auf S. 460 die Änderung zur Auskunftspflicht von TK-Anbietern gegenüber dem Zoll gemäß § 30 ZFdG. Die Idee scheitert hoffentlich schon daran, dass Anbieter klug genug sind, Passwörter nicht im Klartext, sondern durch eine Einwegfunktion, einen Hash (s. o. Fn. 27), geschützt ablegen. Damit ist ein Zugriff auf Passwörter technisch unmöglich. Ein Umstand, der jedem Informatikerstsemester auffallen sollte – und somit erst recht dem Gesetzgeber.

36 BGBl. 2021-I, v. 1. 4. 2021, S. 441 ff.

37 Pressemitteilung der EU-Kommission: https://ec.europa.eu/germany/news/20210430-sexueller-missbrauch-von-kindern_de; zum Verordnungstext (COM(2020) 568 final) https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0568&from=DE; auch hier ignoriert der Rat elegant die technischen Sachverhalte, s. o. Fn. 34.

38 Zum Gesetzesentwurf BT-Drs.19/26541 v. 9. 2. 2021, der jedoch vom Bundesrat abgelehnt wurde (BR-Drs. 515/21(B) v. 25. 6. 2021, Berlin hat die Streichung von § 27d BPolG-E beantragt); Quellen-TKÜ setzt voraus, dass Betriebssystemhersteller Hintertüren für den Start in ihre Systeme einbauen, was erhebliche Sicherheitsrisiken bedeutet, oder aber, dass der Staat noch nicht veröffentlichte Sicherheitslücken aufkauft und nutzt – auch ein erhebliches IT-Sicherheitsrisiko.

39 Zur „EU-Terrorliste“: Der Rat der EU kann aufgrund der Verordnung EG Nr. 2580/2001 Personen und Organisationen durch Durchführungsverordnungen entsprechend einstufen, wie zum Beispiel in der Durchführungsverordnung Nr. 2021/138 des Rates der EU vom 5. 2. 2021 erfolgt. Zur Novellierung des § 86 StGB: BGBl. I-2021, S. 4250.

Staatliche Eingriffe in Verschlüsselungen sind aus Sicht der IT-Sicherheit problematisch, weil die technischen Mittel dazu (Quellen-TKÜ, Bundestrojaner) nicht nur von den Behörden zu den legitimen Zwecken nutzbar sind, sondern auch von Kriminellen.[40] Jüngst bestätigte auch der EGMR seine kritische Haltung zur Überwachung von „Ende-zu-Ende-Verschlüsselungen".[41] Dass diese Kritik berechtigt ist, zeigt auch die Affäre um die sogenannte Pegasus-Software, die durch ein israelisches Unternehmen entwickelt und vom marokkanischen Geheimdienst zur Ausspähung des französischen Staatspräsidenten verwendet wurde.[42]

12. BVerfG: Grundrechtliche Schutzpflicht des Staates zur IT-Sicherheit

Durch den Beschl. v. 8. 6. 2021 bestätigte das BVerfG die grundrechtliche Schutzpflicht des Staates, elektronische Kommunikation und informationstechnische Systeme vor Angriffen Dritter zu schützen.[43]

Dem Beschluss lag eine Verfassungsbeschwerde gegen § 54 Abs. 2 Polizeigesetz Baden-Württemberg zugrunde. Hiernach darf die Polizei die Quellen-TKÜ zur Abwehr bestimmter polizeilicher Gefahren einsetzen, zum Beispiel einer dringenden und erheblichen Gefahr für Leib und Leben, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für wesentliche Infrastruktureinrichtungen, ebenso wenn Tatsachen die Annahme rechtfertigen, dass eine bestimmte Straftat (insbesondere terroristischer Natur) innerhalb eines überschaubaren Zeitraums begangen wird (§ 54 Abs. 1 Polizeigesetz Baden-Württemberg). Die Quellen-TKÜ soll sich dabei gegen die „verantwortliche Person" (das heißt, den polizeirechtlichen „Störer" oder den vermeintlichen Täter) richten; betroffen sind aber auch die Kommunikationspartner des Störers, was § 54 Abs. 1 S. 3 Polizeigesetz Baden-Württemberg ausdrücklich benennt. Um den „Staatstrojaner" für die Quellen-TKÜ einzusetzen, nutzt die Polizei sogenannte „Sicherheitslücken" (vulnerabilities, siehe oben Abschnitt I) in Software auf dem Endgerät des Betroffenen (siehe dazu auch oben Ziffer 11). Das Gericht befasst sich dabei ausdrücklich nur mit Sicherheitslücken, die dem Hersteller noch unbekannt, aber der Polizei bekannt sind. Nach Auffassung der Beschwerdeführer gefährdet dieses staatliche Vorgehen die Vertraulichkeit und Integrität ihrer informationstechnischen Systeme, da es das Interesse des Staates darauf lenke, Sicherheitslücken für Quellen-TKÜ gegen Störer auszunutzen, statt sie den Herstellern zu melden und damit seiner Schutzpflicht für sichere IT-Systeme gerecht zu werden.

Das BVerfG bestätigte den Beschwerdeführern, dass der Staat aufgrund der objektiven Werteordnung der Grundrechte (betroffen waren hier das IT-Grundrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG und das Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG) die Pflicht hat, die Vertraulichkeit und Integrität von informationstechnischen Systemen und die elektronische Kommunikation vor Zugriffen Dritter zu schützen (insbesondere Leitsätze 1 und 2a sowie Rn. 30 - 40 des Beschlusses). Damit hat das Gericht die Streitfrage, ob es eine grundrechtliche Schutzpflicht zur IT-Sicherheit gibt, zugunsten der IT-Sicherheit entschieden.[44]

Andererseits sieht das BVerfG den Schutzauftrag zur IT-Sicherheit in einem Zielkonflikt mit der Offenhaltung unbekannter Sicherheitslücken, um die Quellen-TKÜ zur Gefahrenabwehr zu ermöglichen. Der Gesetzgeber sei aufgerufen, diesen Zielkonflikt zu regeln (so Leitsatz 2 und Rn. 41 ff. des Beschlusses). Ob dem Gesetzgeber dies gelingen kann, kann zumindest bezweifelt werden. Denn die Lösung des benannten Zielkonflikts setzt voraus, dass es Sicherheitslücken gibt, die nur dem Staat bekannt sind. Der Gesetzgeber müsste bei der Auflösung des Zielkonflikts dafür sorgen, dass diese Sicherheitslücken nicht auch durch Kriminelle oder Organisationen anderer Staaten zu gesetzeswidrigen Zwecken ausgenutzt werden – eine Vorstellung, die zumindest aus Sicht der Informatik durchaus zu hinterfragen ist.

Im Ergebnis hat das BVerfG die Verfassungsbeschwerde als unzulässig zurückgewiesen, weil der Vortrag der Beschwerdeführer für die Verletzung der Schutzpflicht zur IT-Sicherheit und zur Erschöpfung des Rechtswegs nicht ausreichend waren. Das Gericht hielt es insbesondere für geboten, eine negative Feststellungsklage gegen mögliche Überwachungsmaßnahmen zu erheben; dabei hätte das angerufene Fachgericht die rechtmäßige Ausgestaltung des § 54 Polizeigesetz Baden-Württemberg prüfen müssen (siehe Rn. 73 des Beschlusses).

13. Pflicht zur beA-Nutzung trotz Sicherheitsmängeln

Anwälte hatten sich gegen die Pflicht zur beA-Nutzung gewehrt, weil keine Ende-zu-Ende-Verschlüsselung eingesetzt wird. Der BGH wies die Klage ab, weil § 31a BRAO nur die Sicherheit des Zugangs zum Postfach regle, aber nicht die Sicherheit der Datenübermittlung (was aus technischer Sicht aber nicht sinnvoll ist).[45]

Fraglich ist, ob und wie das BGH-Urteil vereinbar ist mit der grundrechtlichen Schutzpflicht des Staates, „elektronische Kommunikation und informationstechnische Systeme vor Angriffen Dritter zu schützen" (siehe oben Ziffer 12). Denn der BGH hält beim beA „behebbare Schwachstellen" für zumutbar (siehe Rn. 65 des Urteils), obwohl mit der Ende-zu-Ende-Verschlüsselung eine Kom-

40 Eine Spähsoftware entscheidet ja nicht danach, für wen sie eine Information ausspioniert, *Deusch/Eggendorfer*, in Taeger/Pohle (Fn. 1), Rn. 280, 385. Wer zudem den Stand der öffentlichen IT in der EU beobachtet, wird feststellen, dass Behörden häufig Mühe haben, mit den IT-Sicherheitsstandards der Wirtschaft mitzuhalten. Wie unter diesen Bedingungen eine staatlich genutzte Sicherheitslücke vor Dritten geheim gehalten werden soll, bleibt fraglich; dazu ebenfalls kritisch *Schiffner/Schmitz*, in: Taeger (Hrsg.), Die Digitalisierung der Welt, 2021, S. 289, 296, 300.

41 EGMR, 25. 5. 2021 – 58170/13, 62322/14, 24960/15, BeckRS 2021, 11635, dort zum Eingriff in die Vertraulichkeit (Art. 8 EMRK) und zum Missbrauchsrisiko, Rn. 350, 425.

42 https://www.faz.net/aktuell/politik/inland/pegasus-software-macrons-handy-im-visier-17446839.html.

43 BVerfG, 8. 6. 2021 – 1 BvR 2771/18, K&R 2021, 571, Ls. 1 und 2.

44 Zum Streitstand siehe auch *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 388 - 394.

45 BGH, 22. 3. 2021 – AnwZ (Brfg) 2/20, Rn. 39, 42, K&R 2021, 413 = NJW 2021, 2206 ff. mit sehr zutreffender Anmerkung von Degen auf S. 2218); ergänzend: VG Mainz, 17. 12. 2020 – 1 K 778/19 MZ (dazu *Schöttle*, BRAK-Mitteilungen 2021, 77 ff.) – TLS für anwaltliche E-Mails außerhalb des beA ausreichend (technisch aber fragwürdig, *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 1), Rn. 189 sowie Rn. 187 zur Sicherstellung der Vertraulichkeit der Kommunikation durch Ende-zu-Ende-Verschlüsselung). Neuerliche IT-Sicherheitsfragen stellen sich zum beA. Weil der Austausch der Signaturdatei mit den Gerichtspostfächern nicht funktioniert, hat das beA diese Funktion abgeschafft, siehe https://www.lto.de/recht/juristen/b/besonderes-elektronisches-anwaltspostfach-bea-sicherheitsluecke-zustellung-nachweis-signatur-brak-wiedereinsetzung/. Laut BRAK soll dies keine Auswirkungen haben, da die Funktion ohnehin fehlerhaft gewesen sei, https://portal.beasupport.de/external/c/release-informationen. Aus technischer Sicht jedoch muss diese Funktion fehlerfrei implementiert sein.

munikationstechnik mit angemessenem Sicherheitsstand verfügbar ist.[46]

14. DSGVO-Geldbußen wegen unzureichender IT-Sicherheit und § 30 OWiG

Für Verstöße gegen die IT-Sicherheitspflichten gemäß Art. 32 DSGVO sieht Art. 83 Abs. 4 DSGVO Geldbußen bis zu 2 % des Jahresumsatzes des Verantwortlichen oder bis zu € 10 Mio. vor, je nachdem, welcher Betrag höher ist. Richtet sich die Geldbuße gegen ein Unternehmen, so ist das Verhältnis von § 30 OWiG zu Art. 83 DSGVO unklar; hierzu gibt es zwei entgegengesetzte Entscheidungen des LG Bonn und des LG Berlin.

a) LG Bonn, Bußgeldbescheid Callcenter

Das LG Bonn hat einen Bußgeldbescheid gegen ein Callcenter (€ 9,55 Mio.; Verstoß gegen Art. 32 DSGVO wegen fehlender Authentifizierung von Kundenanfragen) dem Grunde nach bestätigt, aber der Höhe nach auf € 900 000,00 herabgesetzt. Das Gericht wandte § 30 OWiG wegen des Vorrangs der DSGVO nicht an.[47]

b) LG Berlin, Bußgeldbescheid Immobilienunternehmen

Ein Berliner Immobilienunternehmen unterhielt ein E-Mail-Archivsystem, in dem Daten einzelner Betroffener nicht gelöscht werden konnten. Dies führte zu einem Bußgeldbescheid der Datenschutzbehörde in Höhe von € 14,5 Mio. Das LG Berlin hob den Bescheid auf, weil nicht festgestellt werden konnte, welches Organ des Unternehmens für die Sicherheitsmängel verantwortlich war. Dies ist laut LG Berlin gemäß § 30 OWiG Voraussetzung für DSGVO-Bußgelder gegen Unternehmen (ausdrücklich entgegen der obigen Entscheidung des LG Bonn).[48]

15. OLG Stuttgart, Darlegungs- und Beweislast bei Schadensersatz wegen Hackerangriff

Das beklagte Tochterunternehmen eines Zahlungskartenanbieters war Opfer eines Hackerangriffs, bei dem personenbezogene Daten abgeflossen sind, unter anderem auch personenbezogene Daten der Klägerin. Diese verlangte immateriellen Schadensersatz gemäß Art. 82 DSGVO mit der Begründung, die Beklagte habe die Sicherheitsanforderungen des Art. 32 DSGVO nicht erfüllt. Das OLG wies die Klage jedoch ab, weil die Beklagte zu den „anzuwendenden und eingehaltenen sowie regelmäßig geprüften Standards eingehend vorgetragen habe (…)“, und zwar zum Zertifikat ISO IEC 27001:2017 und dem damit verbundenen Standard. Dabei hat sich der Senat ausdrücklich dagegen ausgesprochen, aus Art. 82 DSGVO eine Beweislastumkehr abzuleiten, nach der sich die Beklagte hätte vollumfänglich entlasten müssen. Vielmehr wendete das Gericht die Grundsätze der primären und sekundären Darlegungs- und Beweislast an. Hiernach war es zwar zunächst an der Beklagten, aufgrund des Datenabflusses ihre Sicherheitsvorkehrungen darzulegen; daraufhin hätte aber die Klägerin vortragen müssen, weshalb diese Vorkehrungen den erforderlichen Standard gemäß Art. 32 DSGVO nicht erfüllt haben oder weshalb die Sicherheitsvorkehrungen im konkreten Fall nicht eingehalten wurden. Dass die Klägerin hierfür nicht über die erforderlichen Angaben verfügte, ließ das Gericht nicht gelten: Der Klägerin sei es zumutbar gewesen, bei der Datenschutzbehörde nähere Informationen zu erhalten, etwa durch ein Beschwerde- oder Auskunftsverfahren oder durch die Benennung ihrer Mitarbeiter als Zeugen.

Im Ergebnis ist es der Beklagten somit in zweiter Instanz gelungen, den Anspruch abzuwehren, indem sie ihr Zertifikat gemäß ISO 27001 und die damit verbundenen Maßnahmen vorgetragen hat. Ob diese Argumentation letztlich trägt, wird der BGH zu entscheiden haben; die Revision ist unter dem Aktenzeichen VI ZR 111/21 anhängig.[49]

Kritisch anzumerken ist hierzu, dass die ISO 27001-Vorgaben vor allem Prozesse definieren, nicht aber konkrete Sicherheitsmaßnahmen oder deren Prüfung. Somit bleibt die Frage, ob der Standard ISO 27001 tatsächlich einen positiven Effekt auf die praktische IT-Sicherheit hat und nicht nur auf organisatorischer Ebene sensibilisiert. Diese Frage klammert das Verfahren bislang aus.

16. Verschlüsselte Kommunikation als Indiz zur Straftäterschaft?

Hinzuweisen ist auf verschiedene strafgerichtliche Entscheidungen, die aus der Verwendung von Krypto-Handys (Encrochat) einen dringenden Tatverdacht auf konspiratives Verhalten zur Begehung und Verdeckung von Straftaten ableiten. In diesem Zusammenhang drängt sich die Frage auf, in welchen weiteren Fällen die Verwendung von Verschlüsselungstechniken einen Tatverdacht begründen könnte; das LG Berlin hat sich deshalb ausdrücklich gegen die genannten Entscheidungen ausgesprochen und die TK-Daten eines Kryptohandys nicht als Beweismittel zugelassen, da zum Zeitpunkt der Anordnung der Datenüberwachung keine anderen Verdachtsmomente gegen den Betroffenen vorlagen als die Tatsache, dass er ein Encrochat-Handy verwendet hat.[50]

III. Fazit und Blick in die Zukunft

Die fortschreitende technische Entwicklung („Digitalisierung“) stellt den Gesetzgeber und den Rechtsanwender auf allen Ebenen vor weitere Herausforderungen. Dabei entsteht regelmäßig der Eindruck, dass die öffentliche IT und der Gesetzgeber noch weit hinterherhinken.

---

46 Auch aus technischer Sicht wirft das BGH-Urteil einige Fragen auf. Die Vorstellung, IT-Sicherheit lasse sich aufteilen in „Sicherheit des Zugangs zum Postfach“ und „Sicherheit der Datenübermittlung“, entspricht in keiner Weise dem Stand der Technik. Denn immer, wenn ein beA-Nutzer seinen Zugang zum Postfach nutzt, werden Daten zwischen den beteiligten Systemen übermittelt, unabhängig davon, ob Nachrichten lediglich abgerufen oder auch versendet werden. Gegen eine Aufteilung der IT-Sicherheit in „Sicherheit des Zugangs“ und „Sicherheit der Datenübermittlung“ spricht auch, dass die IT-Sicherheit stets auf ein bestimmtes informationstechnisches System insgesamt abstellt und dabei beurteilt, ob die Schutzziele (etwa Vertraulichkeit durch Verschlüsselung) erreicht werden. Die Aufteilung der Sicherheit in Zugang und Datenübermittlung steht dieser technischen Beurteilung entgegen. In dieser Weise könnte auch die Entscheidung des BVerfG (Nr. 12 in diesem Aufsatz) verstanden werden, da der Staat hiernach die elektronische Kommunikation und die informationstechnischen Systeme insgesamt zu schützen hat und nicht lediglich Teilbereiche hieraus. Eine vertiefte Auseinandersetzung mit dem BGH-Urteil muss jedoch vorbehalten bleiben.

47 LG Bonn, 11. 11. 2020 – 29 OWi 1/20, K&R 2021, 133 ff. = ITRB 2021, 85; laut Pressestelle rechtskräftig.

48 LG Berlin, 18. 2. 2021 – 526 OWiG LG 1/20, K&R 2021, 190 ff., Rechtsmittel eingelegt, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210303-PM-Deutsche_Wohnen.pdf; zu den genannten Entscheidungen auch *Nietsch/Osmanovics*, BB 2021, 1858 - 1865.

49 OLG Stuttgart, 31. 3. 2021 – 9 U 34/21, K&R 2021, 748 ff. = ZD 2021, 375.

50 OLG Rostock v. 23. 3. 2021 – 20 Ws 70/21, BeckRS 2021, 6824; ebenso OLG Bremen, 18. 12. 2020 – 1 Ws 166/20 und OLG Hamburg, 29. 1. 2021 – 1 Ws 2/21; die Entscheidungsgründe sind wegen den Verschlüsselungsanforderungen der DSGVO lebensfremd. Das LG Berlin (Beschl. v. 1. 7. 2021 – 525 KLs 254 – Js 592/20 – 10/21, BeckRS 2021, 17261) hat sich gegen diese Entscheidungen gestellt.