Veröffentlichungen der
Hamburger Gesellschaft
zur Förderung des Versicherungswesens mbH, Hamburg

Jan Lüttringhaus

Internationale Aspekte der Cyber-Haftpflicht und der Cyber-Versicherung

Verlag Versicherungswirtschaft

Prof. Dr. Jan Lüttringhaus

Internationale Aspekte der Cyber-Haftpflicht und der Cyber-Versicherung

Veröffentlichungen der
Hamburger Gesellschaft
zur Förderung des Versicherungswesens mbH, Hamburg

Prof. Dr. Jan Lüttringhaus

Internationale Aspekte der Cyber-Haftpflicht und der Cyber-Versicherung

Verlag Versicherungswirtschaft

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Gleichstellungshinweis

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

ISSN 0947-6067
ISBN 978-3-96329-561-4

Vorwort

Die vorliegende Arbeit beleuchtet ein Thema, das erst durch die Digitalisierung in den Fokus des internationalen Haftungs- und Versicherungsrechts gerückt ist. Im Kern geht es um die Herausforderungen, welche die im Cyberspace – und damit weltweit grenzüberschreitend – stattfindenden Angriffe auf IT-Systeme für diese beiden Rechtsgebiete bringen.

Dabei gilt es zunächst die international-privatrechtlichen Grundlagen zu klären, und zwar sowohl für die Cyber-Haftpflicht als auch für die daraus erwachsenden versicherungsrechtlichen Deckungsstreitigkeiten. Hier stellen sich zahlreiche Einzelfragen, etwa diejenige, welche Cyber-Sicherheitsstandards haftungsrechtlich maßgeblich sind. Sodann ist zu erörtern, inwiefern Geldbußen wegen Verstößen gegen Cybersicherheits- und Datenschutzbestimmungen versicherbar sind und welche nationalen Regelungen es dafür heranzuziehen gilt. Ein weiteres gleichermaßen praxisrelevantes und komplexes Themenfeld betrifft die Versicherbarkeit und Erstattungsfähigkeit von Lösegeldern bei Ransomware-Angriffen. Besonders lebhaft diskutiert wird überdies – auch angesichts der jüngsten Überarbeitung der Musterbedingungen des GDV zur Cyberrisiko-Versicherung – der Ausschluss von Kriegsrisiken. Zudem bieten weitere Ausschlüsse, die gleichfalls dem gesteigerten Kumulrisiko bei der Cyberversicherung Rechnung tragen sollen, auch in der internationalen Perspektive spannende Herausforderungen.

Die Hamburger Gesellschaft zur Förderung des Versicherungswesens mbH schätzt sich glücklich, für die Behandlung dieser gleichermaßen anspruchsvollen und praxisrelevanten Themen einen führenden Experten des internationalen Haftungs- und Versicherungsrechts gewonnen zu haben. *Jan Lüttringhaus*, Ordinarius an der Leibniz Universität Hannover, ist bereits durch zahlreiche einschlägige Veröffentlichungen hervorgetreten, darunter etwa die profunde Kommentierung des Internationalen Versicherungsvertragsrechts im Beck-Online-Großkommentar zur Rom I-VO. Das vorliegende Werk legt ein beeindruckendes Zeugnis von der hohen Kompetenz des

Autors in der Materie ab. Es füllt eine Lücke und bietet eine überaus solide Grundlage für die weitere Diskussion.

Hamburg, im September 2025

Der Beirat
Hamburger Gesellschaft zur
Förderung des
Versicherungswesens mbH

Inhaltsverzeichnis

A. Einführung

Das Internet ist mittlerweile in vielerlei Hinsicht mit den sieben Weltmeeren vergleichbar: Hier wie dort haben wir es mit einem internationalen Raum zu tun, mithilfe dessen Werte geschaffen, Industrien und Lieferketten vernetzt und Waren und Dienstleistungen in aller Welt vertrieben werden. Sowohl auf hoher See als auch im Cyber-Space lauern dabei viele Risiken: Im Seehandel sind stets Ladung und Schiff – im Versicherungsjargon also Casco und Cargo – bedroht. Im Cyber-Space stehen nun gleichermaßen die Verfügbarkeit, Integrität und Vertraulichkeit sowohl eigener Daten als auch der sie „transportierenden", speichernden und verarbeitenden IT-Systeme im Fokus. Und ebenso wie der – schon aufgrund seiner Ausdehnung – faktisch dem lückenlosen Zugriff hoheitlicher Stellen entzogene Raum der See seit jeher Piraten zu Beutezügen, Entführungen und Erpressungen einlädt, so ist auch der grenzenlose und damit ähnlich staatsferne und schwer zu kontrollierende Cyber-Space ein Tummelplatz für allerlei Daten-Piraten. Das Spektrum reicht hier von ganz gewöhnlichen Kriminellen über mit hoheitlicher „*Lettre de marque*" handelnde „Cyber-Kaperfahrer"[1] bis hin zu genuin staatlichen Akteuren. Mit der wachsenden gesellschaftlichen, wirtschaftlichen und politischen Bedeutung des Cyber-Space ist dieser virtuelle Raum zudem längst zur Kampfzone in internationalen Konflikten geworden: Seit jeher haben sich die Schlachtfelder mit den technischen Möglichkeiten der Kombattanten beständig ausgeweitet und reichen vom traditionellen Land- und Seekrieg nun über den Luft- und Weltraumkrieg bis hin zu einem veritablen „Cy-

[1] Vgl. zu Kaperbriefen („*Lettres de marques*") und Kaperfahrten auf See nur den Auszug aus *Guidon de la mer* (16. Jahrhundert) Chapitre X Art. I (abgedruckt in: *Pardessus*, Collection de Lois Maritimes Antérieures au XVIIIe Siècle, part 2, Paris 1831, Neuabdruck Bad Feilnach 1997, S. 377 ff.): „Lettres de marques ou représailles, se concèdent par le Roy, Prince, Potentats, ou Seigneurs Souverains en leurs terre… contenant permission d'apprehender, saisir par force ou autrement, les biens & marchandises des sujets, de celuy qui a toléré, ou passé sous silence le premier tort".

ber-Krieg“.[2] Hier stellen sich dann rechtlich wie praktisch gleichermaßen diffizile Fragen, etwa ob der Cyber-Angriff in den – meist grenzüberschreitenden – Haftungsszenarien als „*acta iure imperii*“ zu qualifizieren ist[3] und ob im Rahmen eines Cyber-Versicherungsvertrags der Ausschluss für „Krieg“ oder „Cyber-Operations“ greift.[4]

Wenn im Folgenden – zur Vermeidung von Wiederholungen – von „Cyber-Vorfällen“, „Cyber-Incidents“ oder „Cyber-Attacken“ die Rede ist, sind damit zum einen obstruktive Angriffe, wie *Distributed Denial of Service* (DDoS)-Attacken gemeint, die die Arbeitsfähigkeit des Betroffenen blockieren. Zum anderen gibt es auch finanziell motivierte Angriffe: Hierzu zählen das Ausspionieren von Geschäftsgeheimnissen oder von Zugangs- und Kundendaten durch Phishing.[5] Besonders stechen freilich Ransomware-Attacken hervor, bei denen die Daten des Angegriffenen verschlüsselt und nur gegen Zahlung eines Lösegelds wieder entschlüsselt werden.[6] Dank „*Ransomware as service*“ aus dem Darknet ist das mittlerweile ein Geschäftsmodell sowohl für organisierte als auch für kleine Kriminelle.

Die für die Zwecke dieser Abhandlung wichtigste Parallele zwischen Hoher See und Internet ist die Schwierigkeit, von Natur aus internationale Sachverhalte mit nationalem Recht zu erfassen. Denn das Internet ist seinem Wesen und seiner Funktion nach von der Territorialität der Staatsgebiete entkoppelt. Entsprechend machen auch

---

2 Der Begriff „Cyberkrieg“ hat mittlerweile zwar nicht nur Eingang in den Sprachgebrauch, sondern auch in Wikipedia gefunden, vgl. https://de.wikipedia.org/wiki/Cyberkrieg. Allerdings differenziert die englischsprachige – anders als die deutschsprachige – Artikelfassung zutreffend zwischen dem Einsatz von „cyberwarfare“ und einem reinen „cyberwar“ andererseits und führt richtigerweise aus: „A cyber war could accurately describe a protracted period of back-and-forth cyber attacks (including in combination with traditional military action) between warring states. To date, no such action is known to have occurred.“ Siehe https://en.wikipedia.org/wiki/Cyberwarfare (jeweils zuletzt abgerufen am 1.5.2025).

3 Dies wird schon bei der internationalen Zuständigkeit und dem anwendbaren Recht für Haftpflichtansprüche relevant, siehe nur den – insoweit jeweils wortlautgleichen – Auszug aus Art. 1 Abs. 1 Brüssel Ia-VO und Art. 1 Abs. 1 Rom II-VO: „Diese Verordnung … gilt insbesondere nicht für … die Haftung des Staates für Handlungen oder Unterlassungen im Rahmen der Ausübung hoheitlicher Rechte (acta iure imperii).“ Siehe dazu eingehend unter C II. und III.

4 Siehe dazu eingehend unter F.

5 Vgl. zu Schäden durch Phishing-E-Mails und Fragen der (Organ)Haftung nur OLG Zweibrücken NJW 2023, 1589 ff.

6 Vgl. aus der ausländischen Rechtsprechungspraxis etwa *AA v. Persons Unknown et al.*, [2019] EWHC 3556 (Comm).

Cyber-Risken nicht an Staatsgrenzen halt. Im Cyber-Space sind IT-System- und Netzwerkgrenzen deshalb weitaus bedeutsamer als Staatsgrenzen: Je nach Branche nutzen Unternehmen weltweit einheitliche Strukturen, in denen sich Malware ausbreiten kann – und z.B. im Fall der jeweils durch *NotPetya*-Schadcode betroffenen Reederei *Maersk*, des Pharma-Konzerns *Merck* sowie des Lebensmittel-Herstellers *Mondelez* auch tatsächlich international ausgebreitet hat.[7] Zudem werden die Wertschöpfungsketten vermehrt auch unternehmensübergreifend vernetzt: Durch das *Internet of Things* (IoT), das *Industrial Internet of Things* (IIoT) und zahlreiche Formen des Outsourcings kommen viele weitere Verbindungen mit unterschiedlichen Zulieferern, Abnehmern und Dienstleistern hinzu. So kann sich auch der Schad-Code potentiell entlang der gesamten Wertschöpfungskette auf unterschiedlichen Ebenen verbreiten. Dadurch vervielfältigen sich die Orte, an denen Schäden weltweit auftreten können. Hinzu tritt die Simultanität der Schadensfälle, was wiederum immense Cumul-Risiken birgt.[8] Im Extremfall droht angesichts dieser Ubiquität und Simultanität ein weltumspannendes „Schadens-Mosaik", dessen Bausteinchen unterschiedliche Schadenskategorien auf diversen Stufen der Wertschöpfungskette sind.

Soweit nun Versicherer eine diesem Mosaik entsprechende Deckung für Cyber-Vorfälle bieten wollen, müssen die Cyber-Versicherungsprodukte der Internationalität der Risiken und Schadensszenarien Rechnung tragen. Das Deckungsversprechen lautet – üblicherund sinnvollerweise – deshalb im Ausgangspunkt auf „weltweiten" Cyber-Versicherungsschutz.[9] Doch das ist leichter gesagt als getan. Die globale Ausdehnung ebenso wie etwaige territoriale und rechtliche Einschränkungen[10] des Deckungsumfangs werfen vielfältige Probleme auf und zwingen dazu, stets das anwendbare Recht ebenso wie die internationale Zuständigkeit im Blick zu behalten: Denn ob das Versprechen „weltweiter Deckung" eingelöst werden

---

7 Anschaulich dazu etwa *Insurance Institute*, Cyber Insurance Research Findings, 2022, S. 216 f.

8 Vgl. etwa *BSI*, Mitteilung v. 6.2.2023: Weltweiter Ransomware-Angriff: tausende Server verschlüsselt (Schwachstelle CVE-2021-21974).

9 Vgl. nur Ziff. A1-11 Abs. 1 AVB Cyber 2024: „Versicherungsschutz besteht für Versicherungsfälle weltweit".

10 Vgl. beispielsweise Ziff. A1-11 Abs. 2 AVB Cyber 2024: „Dies gilt jedoch nur, soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht werden.".

kann, hängt im Streitfall entscheidend davon ab, welches Recht auf den Cyber-Versicherungsvertrag anwendbar und welches Gericht für die Deckungsstreitigkeit international zuständig ist (**dazu unter B**). So entscheiden Zuständigkeits- und Kollisionsrecht z.B. nicht zuletzt über die Werthaltigkeit bestimmter Deckungsbausteine – etwa in Bezug auf die Erstattung von Geldbußen nach Datenschutz- und Cyber-Sicherheitsverstößen oder Lösegelddeckungen bei Ransomware-Attacken.[11]

Besondere Aufmerksamkeit verdient sodann auch die internationalprivatrechtliche Dimension der Haftpflicht für Cybervorfälle (**hierzu unter C**): Wer Schad-Code – beispielsweise als Zulieferer oder Dienstleister – (fahrlässig) weiterverbreitet, sieht sich gerade bei grenzüberschreitenden Wertschöpfungsketten potentiell weltweit den Ansprüchen seiner Geschäftskontakte ausgesetzt. Prominente Opfer solcher weltweiten Vorfälle waren in jüngerer Zeit etwa *British Airways* und die Hotelkette *Marriott* mit ihrem globalen Kundenstamm. Hier stehen auf der einen Seite die betroffenen Flug- und Hotelgäste und auf der anderen die in Anspruch genommenen Anbieter jeweils vor der Frage, welches Recht denn auf etwaige Schadensersatzansprüche anwendbar ist. Abgesehen davon, dass einige Cyber-Bedingungswerke den Umfang des Versicherungsschutzes an die internationale Zuständigkeit und an das anwendbare Recht koppeln,[12] ist die Rechtsanwendungsfrage stets für den Regress des Cyber-Versicherers relevant.

Ausgehend von der Haftpflichtdimension beleuchtet diese Abhandlung sodann die Deckungsseite und nimmt grundlegende internationale Aspekte der Cyber-Versicherung in den Blick: Besondere Herausforderungen stellen sich hier nicht zuletzt bei grenzüberschreitenden Deckungskonzepten für Geldbußen wegen Verstößen gegen Cyber-Sicherheits- und Datenschutzgesetzen (**hierzu unter D**). Die empfindlichen Geldbußen innerhalb und außerhalb der EU bieten Anlass genug, die Versicherbarkeit von Geldbußen an der Schnittstelle von Kollisions- und Versicherungsvertragsrecht zu

[11] Dazu eingehend unter D II, IV sowie unter E II.
[12] Vgl. erneut Ziff. A1-11 Abs. 2 AVB Cyber 2024.

beleuchten.[13] Bei einem globalen Kundenstamm – wie bei internationalen Hotelketten, Fluglinien, Social-Media-Plattformen usw. – droht die Verhängung von Geldbußen weltweit: Ein Cyber-Incident mag dann zugleich den Tatbestand des kalifornischen CCPA,[14] der DSGVO sowie des chinesischen PIPL[15] erfüllen. Hier ist mit Blick auf die Cyber-Deckung zu fragen, inwieweit die Erstattung von Geldbußen durch den Cyber-Versicherer jeweils rechtlich zulässig ist und welches (supra)nationale Recht darüber entscheidet. Parallelfragen stellen sich auch bei Geldbußen, die wegen Verstößen gegen die Cyber-Sicherheitsstandards verhängt werden, zumal durch die Umsetzung der NIS-2-RL[16] der Kreis der erfassten Unternehmen deutlich erweitert und die Cyber-Risikomanagementvorgaben in der EU inhaltlich verschärft worden sind.

Unter ähnlichen Vorzeichen ist sodann auch die Versicherbarkeit und Erstattungsfähigkeit von „Lösegeldern" bei Ransomware-Attacken näher zu untersuchen: Neben international-privatrechtlichen Fragen zeigen sich hier rechtsvergleichend sehr unterschiedliche Tendenzen in den einzelnen Rechtsordnungen (**dazu unter E**).

Von großer praktischer Bedeutung für den Deckungsschutz ist schließlich auch der Umgang mit Cumul-Risiken in Cyber-Versicherungsbedingungen: Besondere Aufmerksamkeit verdienen hier die jüngst durch die *Lloyd's Market Association* (LMA) und durch den Gesamtverband der *Deutschen Versicherungswirtschaft* (GDV) vorgeschlagenen und nun in marktgängigen AVB implementierten Ausschlüsse von Cyber-Attacken, die Bestandteil eines „Krieges" oder sogenannter „Cyber-Operationen" sind (**hierzu unter F**).

---

13 Allein in der EU haben Datenschutzbehörden 2022 Bußgelder in Höhe von € 1,64 Milliarden verhängt, vgl. *DLA Piper*, GDPR fines and data breach survey (Januar 2023), S. 3.

14 Titel 1.81.5. *California Consumer Privacy Act of 2018*, sec. 1798.100 bis 1798.199.100 *California Civil Code*.

15 *Personal Information Protection Law* (PIPL) v. 20.8.2021, in Kraft getreten zum 1.11.2021.

16 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. EU 2022 L 333/80.

Eine Zusammenfassung der Ergebnisse rundet die Betrachtungen der internationalen Aspekte der Cyber-Versicherung und der Cyber-Haftpflicht ab (**dazu schließlich unter G**).

B. Cyber-Versicherungsvertragsstatut und international-privatrechtliche Grundlagen

Das Internationale Privatrecht umfasst das sogenannte Kollisionsrecht und als eng verzahntes Nachbargebiet das Internationale Zuständigkeitsrecht: Das Kollisionsrecht beantwortet die Frage, welches Recht in Sachverhalten mit Auslandsbezug zur Anwendung kommt, und löst damit den Konflikt auf, der in solchen Fallgestaltungen durch – potentiell kollidierende – Anwendungsansprüche von in- und ausländischen Rechtsnormen besteht.[17] Das Internationale Zuständigkeitsrecht hingegen entscheidet darüber, welche Gerichte bei grenzüberschreitenden Streitigkeiten zuständig sind.[18] Beide Fragestellungen sind bei Cyber-Versicherungen angesichts des Versprechens „weltweiter Deckung“[19] unmittelbar relevant: Denn ob dieses Deckungsversprechen eingelöst werden kann, hängt im Streitfall entscheidend davon ab, welches Recht das jeweils zuständige Gericht anwendet. Obschon Cyber-Versicherungsverträge regelmäßig sowohl Gerichtsstands- als auch Rechtswahlklauseln enthalten, sind solchen parteiautonomen Bestimmungen des zuständigen Gerichts und des anwendbaren Rechts durchaus Grenzen gesetzt. So können bzw. müssen Gerichte beispielsweise auch ungeachtet des eigentlich durch die Parteien gewählten Rechts bestimmte (international) zwingende Normen einer anderen Rechtsordnung anwenden.[20] Zu denken ist etwa an Versicherungsverbote und an Sanktions- oder Embargobestimmungen.

Darüber hinaus verknüpft zumindest die AVB-Cyber des GDV den „Geltungsbereich“ des Haftpflicht-Deckungsschutzes ausdrücklich mit den Fragen der internationalen Zuständigkeit und des anwendbaren Rechts: Versicherungsschutz soll nur bestehen, „soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht

---

17 Statt vieler m.w.N. *Kegel/Schurig*, Internationales Privatrecht, 9. Aufl. 2004, S. 4 ff.; MünchKommBGB/*von Hein*, 9. Aufl. 2024, Einl. IPR Rn. 1 ff.

18 Statt vieler m.w.N. *von Bar/Mankowski*, Internationales Privatrecht, 2. Aufl. 2003, S. 346 ff.; MünchKommBGB/*von Hein*, 9. Aufl. 2024, Einl. IPR Rn. 342.

19 Vgl. nur A1-11 AVB-Cyber 2024.

20 Vgl. nur Art. 3 Abs. 3 sowie Art. 9 Rom I-VO.

werden“.[21] Hier sind damit international-privatrechtliche Überlegungen schon inzident bei der Klärung der Frage relevant, ob ein Versicherungsfall eingetreten ist. Ähnliche Verschränkungen zwischen dem Deckungsversprechen einerseits und Aspekten des Internationalen Privatrechts andererseits finden sich z.B. auch bei manchen Bußgeldbausteinen in Cyber-Versicherungsverträgen: Dabei wird die Ersatzfähigkeit des nach Auftreten einer Datenschutz- oder Cyber-Sicherheitsverletzung gegen den Versicherungsnehmer verhängten Bußgelds davon abhängig gemacht, dass die Zahlung nach bestimmten beteiligten Rechtsordnungen – wie etwa dem Recht des das Bußgeld verhängenden Staates – zulässig ist.[22]

Im Rahmen dieser Abhandlung wird vorrangig die Perspektive eines Gerichts in der Europäischen Union (EU) und insbesondere eines deutschen Gerichtes eingenommen. Die hierbei gewonnenen Erkenntnisse sind allerdings auf die EU, den Europäischen Wirtschaftsraum (EWR) und auch auf das Vereinigte Königreich (UK) übertragbar, weil sowohl die Regelungen zur internationalen Zuständigkeit als auch zum Kollisionsrecht durch EU-Sekundärrecht, staatsvertragliche Übereinkommen und – wo erforderlich – nationale Umsetzungsrechtsakte angeglichen worden sind. Darüber hinaus werden auch abweichende Regelungen aus drittstaatlichen Rechtsordnungen – wie etwa bestimmte cyber-bezogene Verbotstatbestände in US-amerikanischen Bundesstaaten – in die Untersuchung einbezogen.[23] Das Augenmerk gilt im Folgenden zunächst den international-zuständigkeitsrechtlichen (**dazu unter I**) und den kollisionsrechtlichen Grundlagen (**dazu unter II**).

---

21 A1-11 („Geltungsbereich“) AVB-Cyber 2024: „Versicherungsschutz besteht für Versicherungsfälle weltweit. Dies gilt jedoch nur, soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht werden.“

22 Hierzu sowie zu gängigen AVB-Klauselgestaltungen in Cyber-Versicherungsverträgen eingehend zu Geldbußendeckungen unter D sowie zu Lösegelddeckungen unter F.

23 Eingehend unter F II 1 c).

I. Internationale Zuständigkeit für Cyber-Deckungsstreitigkeiten

Das anwendbare Internationale Zuständigkeitsrecht als Teilbereich des Internationales Zivilverfahrensrechts (IZVR) unterscheidet sich, je nachdem wo der Beklagte seinen Wohnsitz oder im Fall eines Versicherers eine Haupt- oder sonstige Niederlassung hat.[24] So findet das revidierte Luganer Übereinkommen (LugÜ 2007) grundsätzlich Anwendung, wenn der Beklagtensitz in einem der EFTA-Staaten Island, Norwegen oder der Schweiz liegt.[25] Soweit bei einem Beklagtensitz in einem Drittstaat weder das LugÜ noch die sogleich näher zu beleuchtende Brüssel Ia-VO anwendbar sind, und auch keine anderen speziellen (staatsvertraglichen) Regelungen existieren, muss auf das autonome deutsche IZVR zurückgegriffen werden: Die internationale Zuständigkeit folgt dann nach dem Grundsatz der Doppelfunktionalität aus der entsprechenden Anwendung der Regelungen zur örtlichen Zuständigkeit, was bei Versicherungssachen regelmäßig zu § 215 VVG führt.[26]

Liegt der Beklagtensitz dagegen innerhalb der EU-Mitgliedstaaten,[27] ist die Brüssel Ia-VO auf Zivil- und Handelssachen ausweislich ihres Art. 1 Abs. 1 S. 1, Art. 4 Abs. 1 i.V.m. Art. 62 f. anwendbar, soweit nicht eine der Ausnahmen nach Art. 1 Abs. 1 S. 2, Abs. 2 Brüssel Ia-VO eingreift.[28] Dem Grundsatz *actor sequitur forum rei* folgend ist der Beklagte zunächst stets an seinem (Wohn)Sitz i.S.d. Art. 4 Abs. 1 Brüssel Ia-VO innerhalb der EU-Mitgliedstaaten gerichtspflichtig. Bei Klagen gegen Versicherer ohne Sitz in der EU reicht es nach Art. 11 Abs. 2 Brüssel Ia-VO bereits aus, dass der Versi-

---

24 BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 206 ff.

25 Luganer Übereinkommen über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen v. 30.10.2007, ABl. 2007 L 339, 3. Zu den Parallelen und Unterschieden zur Brüssel Ia-VO statt vieler Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Vorbemerkung Brüssel Ia-VO Rn. 12 f.

26 Vgl. BGH NJW 1997, 2245; BGH NJW 2016, 3369.

27 Dänemark ist zwar ausweislich des Erwägungsgrundes Nr. 41 nicht an die Brüssel Ia-VO gebunden, die Regelungen der Verordnung können dort aber aufgrund eines völkerrechtlichen Abkommens angewendet werden, vgl. ABl. 2005 L 299/62 und siehe näher Geimer/Schütze/*Geimer*, EuZivilVerfR, 4. Aufl. 2020, Art. 1 EuGVVO Rn. 248 ff.

28 Zu Art. 1 Abs. 1 S. 2 Brüssel Ia-VO – insbesondere im Kontext von möglichen *acta iure imperii* im Kontext eines „Cyber-Kriegs" – noch ausführlich unter C II 1 a).

cherer zumindest eine Zweigniederlassung, Agentur oder sonstige Niederlassung innerhalb der Mitgliedstaaten unterhält und sich die Streitigkeit aus dem Betrieb der konkreten Niederlassung ergibt.[29] Die Brüssel Ia-VO ist nach Art. 6 Abs. 1 darüber hinaus auch dann auf Beklagte ohne Sitz in den Mitgliedstaaten anwendbar, wenn eine ausschließliche Zuständigkeit nach Art. 24 Brüssel Ia-VO oder eine den Anforderungen des Art. 25 Brüssel Ia-VO genügende Gerichtsstandsvereinbarung besteht. Cyber-Versicherungsverträge mit solchen Gerichtsstandsklauseln (**dazu unter 1**) bilden den Regelfall in der Praxis und sind bei Deckungsstreitigkeiten deshalb vor den allgemeinen Regelungen zur internationalen Gerichtszuständigkeit (**dazu unter 2**) in den Blick zu nehmen.

1. Gerichtsstandsvereinbarungen in Cyber-Versicherungsverträgen

Cyber-Versicherungsverträge enthalten regelmäßig eine Gerichtsstandsvereinbarung, die ein näher bezeichnetes – bei einem Versicherungsnehmer mit (Haupt)Sitz in Deutschland üblicherweise deutsches – Gericht für zuständig erklärt. Die Freiheit, den Gerichtsstand zu bestimmten, schränkt Art. 15 Brüssel Ia-VO jedoch erheblich ein, um insbesondere bei formularmäßigen Gerichtsstandsklauseln eine Umgehung des Schutzregimes für Versicherungsnehmer, Versicherte und Geschädigte nach Art. 11 bis 14 Brüssel Ia-VO zu verhindern.[30] Umfassende Parteiautonomie gewährt Art. 15 Nr. 5 i.V.m. Art. 16 Brüssel Ia-VO in Versicherungssachen in erster Linie für die Gerichtsstandswahl bei Großrisiken.[31] Ähnlich verhält es sich bei der Prorogation von Gerichten aus Nicht-EU-Mitgliedstaaten, die dem von der EU gezeichneten Haager

[29] Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 11 EuGVVO Rn. 4.

[30] Vgl. EuGH 30.6.2022 – Rs. C-652/20 (*Allianz Elementar Versicherung*) ECLI:EU:C:2022:514 Rn. 50; Prölss/Martin/*Piontek*, 32. Aufl. 2024, Art. 15 VO (EU) 1215/2012 Rn. 1.

[31] Gleiches gilt nach Art. 16 Brüssel Ia-VO u.a. für See- und Luftfahrtversicherungen vgl. nur EuGH 27.4.2023 – Rs. C-352/21 (*A1, A2*) ECLI:EU:C:2023:344.

Übereinkommen v. 30.6.2005 über Gerichtsstandsvereinbarungen angehören.[32]

Cyber-Versicherungsverträge beziehen sich dabei keineswegs ausnahmslos nur auf Großrisiken, wie sie nunmehr Art. 13 Nr. 27 Solvency II-RL[33] definiert:[34] Gerade im wachsenden KMU-Markt spielen Nicht-Großrisiken eine Rolle. Bei solchen Risiken sieht Art. 15 i.V.m. Art. 25 Brüssel Ia-VO unter dem Gesichtspunkt des „zuständigkeitsrechtlichen Schwächerenschutzes" Einschränkungen für die Gerichtsstandswahl in Versicherungssachen und damit auch für Cyber-Versicherungsverträge vor: Vereinbarungen über das international zuständige Gericht sind hier nur zulässig, wenn sie entweder nach Entstehung der Streitigkeit getroffen werden (Nr. 1), die Wahlmöglichkeiten des Gegners des Versicherers erweitern (Nr. 2), die Zuständigkeit der Gerichte des gemeinsamen Wohnsitz- oder Aufenthaltsstaates begründen (Nr. 3) oder aber unter bestimmten Voraussetzungen mit Versicherungsnehmern aus einem Nicht-Mitgliedstaat getroffen werden (Nr. 4). Auf der Einhaltung dieser Vorgaben sollte auch in Cyber-Versicherungsverträgen besonderes Augenmerk liegen, denn wenn eine Gerichtsstandsvereinbarung den Voraussetzungen des Art. 15 Brüssel Ia-VO nicht entspricht, ist die Vereinbarung gemäß Art. 25 Abs. 4 Brüssel Ia-VO rechtlich wirkungslos. Zu beachten ist zudem, dass Gerichtsstandsvereinbarungen grundsätzlich nur relativ im Verhältnis der Parteien wirken.[35] Wird eine Cyber-Versicherung – wie in der Praxis häufig – (auch) auf fremde Rechnung geschlossen und sind Versicherungsnehmer und Versicherter (teilweise) personenverschieden, kann der Versicherte den Versicherer bei Streitigkeiten aus dem Versicherungs-

---

32 Vgl. Deklaration der EU vom 11.6.2015, dazu BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 233 f.

33 Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit, ABl. EG 2009 L 335/1.

34 Zur Definition des Großrisikos bezieht sich Art. 16 Nr. 5 Brüssel Ia-VO ebenso wie im Kollisionsrecht Art. 7 Abs. 2 Rom I-VO auf den mittlerweile in Art. 13 Nr. 27 Solvency II-RL aufgegangenen Art. 5 lit. d 1. Schadensversicherungs-RL. In das deutsche Recht sind diese unionsrechtlichen Vorgaben durch § 210 Abs. 2 VVG iVm Anlage 1 zum VAG umgesetzt worden, vgl. nur EuGH 27.4.2023 – Rs. C-352/21 (*A1, A2*) ECLI:EU:C:2023:344 Rn. 31 ff.

35 Vgl. nur EuGH 12.5.2005 – Rs. C-112/03 (*Société financière et industrielle du Peloux/Axa Belgium*) ECLI:EU:C:2005:280 Rn. 40 ff.; EuGH 13.7.2017 – Rs. C-368/16 (*Assens Havn*) ECLI:EU:C:2017:546; EuGH 27.2.2020 – C-803/18 (*AAS Balta*) ECLI:EU:C:2020:123.

verhältnis auch vor dem im Verhältnis zum Versicherungsnehmer wirksam nach Art. 25, Art. 15 Brüssel Ia-VO prorogierten Gericht verklagen, da hierdurch seine Wahlmöglichkeiten nach Art. 15 Nr. 2 Brüssel Ia-VO erweitert werden. Fraglich erscheint, ob eine wirksame Gerichtsstandsvereinbarung zwischen dem Cyber-Versicherer und Cyber-Versicherungsnehmer sodann auch den Versicherten bindet: Denn schließlich leitet der Versicherte seine Rechte allein vom Versicherungsnehmer als Vertragspartner des Versicherers her und erscheint damit bereits nicht als außerhalb dieser Vereinbarung stehender „Dritter". Allerdings hat der EuGH eine Bindungswirkung ohne ausdrückliche Zustimmung des daran nicht Beteiligten bislang nur bei vollständigen „Substitutionsverhältnissen" bejaht, wenn der an der Vereinbarung Unbeteiligte nach dem anwendbaren nationalen Recht in alle Rechte und Pflichten der ursprünglichen Vertragspartei eintritt.[36]

2. Zuständigkeit für (Deckungs)Klagen gegen den Versicherer

Sollte eine Gerichtsstandsvereinbarung fehlen, unwirksam oder im Verhältnis zum Kläger nicht bindend sein, so kann der Versicherer zunächst nach Art. 11 Abs. 1 lit. a an seinem Sitz oder nach lit. b Brüssel Ia-VO am Wohnsitz des Versicherungsnehmers, Versicherten oder Begünstigten verklagt werden. Mitversicherer können gem. lit. c auch vor dem Gericht in Anspruch genommen werden, bei dem der führende Versicherer verklagt wird, wobei die praktische Bedeutung der Bestimmung aus zweierlei Gründen gering sein dürfte: Erstens bildet in der offenen Mitversicherung eine Prozessführungsklausel den Regelfall.[37] Zweitens sind bei den – jedenfalls bei großen Deckungsstrecken erforderlichen – Exzedentenversicherungen zum einen Schiedsklauseln üblich und zum anderen existieren hier

[36] Vgl. zum „Begünstigten" eines Versicherungsvertrags grundsätzlich EuGH 12.5.2005 – Rs. C-112/03 (*Société financière et industrielle du Peloux/Axa Belgium*) ECLI:EU:C:2005:280 Rn. 40 ff. Vgl. auch EuGH 9.11.2000 – Rs. C-387/98 (*Coreck Maritime*) Slg. 2000, I-9337 Rn. 22 ff. Vgl. ferner zu weiteren „Substitutionsverhältnissen" nur Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 25 EuGVVO Rn. 4a ff. m.w.N.

[37] Prölss/Martin/*Piontek*, 32. Aufl. 2024, Art. 11 Brüssel Ia-VO Rn. 6

ohnehin keine layer-übergreifenden Führungsklauseln und damit „federführende Versicherer“ i.S.d. Art. 11 Abs. 1 lit. c Brüssel Ia-VO.

Jenseits von Art. 11 Abs. 1 lit. a-c erstreckt Art. 10 i.V.m. Art. 7 Nr. 5 Brüssel Ia-VO die Gerichtspflichtigkeit der innerhalb der EU ansässigen Versicherer überdies auf die Gerichte am Ort ihrer Zweigniederlassung, Agentur oder sonstigen Niederlassung, wenn es sich um eine Streitigkeit aus dem Betrieb dieser Niederlassung handelt.[38] Auch sofern der Versicherer selbst keinen EU-Sitz hat, wird er gemäß Art. 11 Abs. 2 Brüssel Ia-VO dennoch dadurch in der EU gerichtspflichtig, dass er eine Zweigniederlassung, Agentur oder sonstige Niederlassung innerhalb der Mitgliedstaaten unterhält und sich die Streitigkeit gerade aus dem Betrieb der konkreten Niederlassung ergibt: In diesem Fall sind die Gerichte des Mitgliedstaats international zuständig, in dem sich die fragliche Niederlassung befindet.[39]

Mit Blick auf den in der Cyber-Versicherung enthaltenen Haftpflicht-Baustein kann zudem Art. 12 S. 1 Brüssel Ia-VO für die Zuständigkeit relevant werden: Die Norm erweitert die Gerichtspflichtigkeit des Versicherers über Art. 11 Brüssel Ia-VO hinaus bei Haftpflichtversicherungen auf das Gericht des Ortes, an dem das schädigende Ereignis eingetreten ist.[40] Nach ständiger Rechtsprechung des EuGH ist darunter sowohl der Handlungsort, d.h. also der Ort des dem Schaden zugrunde liegenden ursächlichen Geschehens, als auch der Erfolgsort und somit der Ort des primären Schadenseintritts zu verstehen. Diese weite Konzeption des EuGH hat zur Folge, dass der Kläger bei Distanzdelikten frei wählen kann.[41]

---

38 Rauscher/*Staudinger*, Europäisches Zivilprozess- und Kollisionsrecht I, 5. Aufl. 2021, Art. 10 Brüssel Ia-VO Rn. 8 f.; BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 226.

39 Langheid/Wandt/*Looschelders*, VVG, 3. Aufl. 2024, IntVersR Rn. 270.

40 Zu Auslegung des Begriffs des „Ortes, an dem das schädigende Ereignis eingetreten ist“ in Übereinstimmung mit Art. 7 Nr. 2 Brüssel Ia-VO z.B. Rauscher/*Staudinger*, Europäisches Zivilprozess- und Kollisionsrecht I, 5. Aufl. 2021, Art. 12 Brüssel Ia-VO Rn. 3.

41 Vgl. grundlegend EuGH 30.11.1976 – Rs. 21/76 (*Mines de potasse d'Alsace*) ECLI:EU:C:1976: 166 Rn. 24 f. Siehe auch z.B. BGH VersR 2008, 1129 Rn. 17. Näher Prölss/Martin/*Piontek*, 32. Aufl. 2024, Art. 12 Brüssel Ia-VO Rn. 3.

Während sowohl die EU-Versicherungsaufsichtsbehörde EIOPA[42] und die Agentur der Europäischen Union für Cybersicherheit ENISA[43] als auch vereinzelte Stimmen im Schrifttum[44] wiederholt eine Pflichtversicherung für Cyber-Risiken ins Spiel gebracht haben, scheint diese Diskussion vorerst in den Hintergrund getreten zu sein.[45] Sollte allerdings in einem weiter ausgereiften Cyber-Versicherungsmarkt angesichts erheblich wachsender Bedrohungsszenarien eine Pflichtversicherung eingeführt werden, so hätte dies auch Auswirkungen auf die internationale Zuständigkeit: Jedenfalls bei einer Insolvenz des Versicherungsnehmers sieht das deutsche Recht in § 115 i.V.m. § 113 VVG nämlich einen Direktanspruch des Geschädigten gegen den Versicherer des Haftpflichtigen vor. Soweit eine solche Direktklage nach nationalem Recht zulässig ist, eröffnet auf Ebene des IZVR dann Art. 13 Abs. 2 Brüssel Ia-VO dem Geschädigten den Gerichtsstand der Direktklage (*action directe*) gegen den Versicherer.[46]

II. Internationales Cyber-Versicherungsvertragsrecht unter der Rom I-VO

Steht die internationale Zuständigkeit für einen Cyber-Deckungsstreit fest, muss das Gericht in Sachverhalten mit Auslandsbezug das anwendbare Recht bestimmen. Aus der Perspektive eines deutschen Gerichts bilden dabei die Kollisionsnormen des internationa-

---

42 Vgl. nur *EIOPA*, Cyber Security and Cyber Risk: A universal Challenge, Keynote speech by Gabriel Bernardino at the 3rd Annual FinTech and Regulation Conference on „Taking innovation to the next level" on 26 February 2019 in Brussels, S. 6: „As cyber-insurance markets mature, we should start to discuss if cyber insurance should also be mandatory. This would provide a further level of security for companies and consumers in the digital world."

43 Vgl. nur die von der European Network and Information Security Agency (ENISA) herausgegebene Studie von *Anderson/Böhme/Clayton/Moore*, Security Economics and the Internal Market (2008), S. 84 f. siehe dort aber auch – kritisch – S. 86 f.

44 Programmatisch titelt etwa *Lemnitzer*, Journal of Cyber Policy 6(2) (2021), 118 ff.: „Why cybersecurity insurance should be regulated and compulsory". Siehe zuvor schon *Trang*, Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches, 18 Minnesota Journal of Law, Science & Technology 389 (2017).

45 Dezidiert gegen eine Versicherungspflicht im Bereich der Cyber-Versicherung auch z.B. *Insurance Europe*, Insurers' role in EU cyber resilience (2019), S. 9 f.

46 Dabei hat das nationale Gericht das jeweilige nationale Recht auszulegen, ob darin eine „unmittelbare Klage" i.S.d. Art. 13 Abs. 2 Brüssel Ia-VO gestattet wird, vgl. nur EuGH 13.7.2017 – Rs. C-368/16 (*Assens Havn*) ECLI:EU:C:2017:546 Rn. 32.

len Vertragsrechts unter der Rom I-VO den Ausgangspunkt (**dazu unter 1**). Das Versicherungsverhältnis kann darüber hinaus in Bezug auf bestimmte Deckungsbausteine auch durch besondere kollisions- oder sachrechtliche Normen beeinflusst werden, insbesondere soweit es um etwaige künftige Versicherungspflichten (**hierzu unter 2**) oder um die Zulässigkeit der Versicherung geht (**dazu unter 3**). Die aus der Perspektive eines international zuständigen deutschen Gerichts maßgeblichen Kollisionsnormen finden sich dabei für vertragliche Streitigkeiten zuvörderst in der Verordnung (EG) Nr. 593/2008 (Rom I-VO).[47]

1. Grundanknüpfung nach Art. 7 Rom I-VO

Die Kollisionsnorm des Art. 7 Rom I-VO erfasst nur Erst- bzw. Direktversicherungsverträge, wohingegen Rückversicherungsverträge gemäß Art. 7 Abs. 1 S. 2 Rom I-VO ausgenommen und nach Art. 3 bzw. Art. 4 angeknüpft werden.[48] Das auf Erstversicherungsverträge anwendbare Recht wird im Fall von Großrisiken grundsätzlich nach Art. 7 Abs. 1, Abs. 2 i.V.m. Art. 3 Rom I-VO ermittelt (**dazu unter a**). Bei Cyber-Versicherungsverträgen, die Massenrisiken zum Gegenstand haben, ist anhand der Belegenheit der Risiken innerhalb oder aber außerhalb der EU-Mitgliedstaaten zu differenzieren: Während innerhalb der EU belegene Massenrisiken grundsätzlich nach Art. 7 Abs. 3 anzuknüpfen sind (**dazu unter b**), unterfallen außerhalb der EU belegene Cyberrisiken in Gestalt von Massenrisiken ausweislich des Art. 7 Abs. 1 S. 1 den allgemeinen Kollisionsnormen in Art. 3 und Art. 4 Rom I-VO. Bei Cyber-Versicherungsverträgen, die Risiken in mehreren Staaten decken, können sich sodann besondere Herausforderungen bei der als Obliegenheit formulierten Einhaltung von IT-Sicherheitsvorschriften ergeben (**dazu unter c**).

---

47 Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17.6.2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I), ABl. 2008 L 177/6.

48 BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 151 ff.

a) Großrisiken nach Art. 7 Abs. 2 UAbs. 1 i.V.m. Art. 3 Rom I-VO

Im Fall von Großrisiken können die Parteien des Versicherungsvertrags nach Art. 7 Abs. 2 UAbs. 1 i.V.m. Art. 3 Rom I-VO das auf den Vertrag anwendbare Recht im Ausgangspunkt frei wählen. Großrisiken definiert Art. 7 Abs. 2 UAbs. 1 Rom I-VO noch unter Verweis auf den nunmehr in Art. 13 Nr. 27 Solvency II-RL[49] aufgegangenen Art. 5 lit. d 1. Schadensversicherungs-RL,[50] die in Deutschland jeweils durch § 210 Abs. 2 VVG i.V.m. Anlage 1 zum VAG umgesetzt worden sind. Die Großrisikoeigenschaft folgt entsprechend entweder aus der Versicherungssparte und/oder der wirtschaftlichen Größe des Versicherungsnehmers.[51] Sollte zukünftig eine – u.a. durch EIOPA befürwortete – Versicherungspflicht für Cyberrisiken aufgestellt werden,[52] wäre bei solchen Pflichtversicherungen nach Art. 7 Abs. 4 Rom I-VO ggf. auch das Recht des EU-Mitgliedstaats zu beachten, der die Versicherungspflicht vorschreibt.[53]

aa) (Teil)Rechtswahl in Cyber-Versicherungsverträgen

Ausweislich des Art. 3 Abs. 1 Rom I-VO können die Parteien das auf den Cyber-Versicherungsvertrag anwendbare Recht ausdrücklich oder auch konkludent wählen. Indizien für eine konkludente Rechtswahl der Parteien können bei Versicherungsverträgen beispielsweise die Bezugnahme auf nach einem bestimmten nationalen Recht gestaltete AVB oder eine Gerichtsstandsvereinbarung liefern.[54] Dabei ist eine Rechtswahl gemäß Art. 3 Abs. 1 S. 2 Rom I-VO sowohl für den ganzen Versicherungsvertrag als auch nur für einen Teil desselben möglich.

---

49 Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II), ABl. 2009 L 335/1.

50 Erste Richtlinie 73/239/EWG des Rates vom 24. Juli 1973 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend die Aufnahme und Ausübung der Tätigkeit der Direktversicherung (mit Ausnahme der Lebensversicherung), ABl. 1973 L 228/3.

51 Eingehend statt vieler BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 92 ff.

52 Vgl. erneut nur *EIOPA*, Cyber Security and Cyber Risk: A universal Challenge, Keynote speech by Gabriel Bernardino at the 3rd Annual FinTech and Regulation Conference on „Taking innovation to the next level" on 26 February 2019 in Brussels, S. 6.

53 Dazu noch eingehend unter 2.

54 BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 97.

Eine Teilrechtswahl mag im Cyber-Kontext zumindest punktuell bei Geldbußendeckungen in Betracht kommen: Vor allem in der anglo-amerikanischen Vertragspraxis ist zuweilen eine Klausel anzutreffen, die für bestimmte Deckungsbausteine, wie insbesondere die Löse- und/oder Geldbußendeckung, vorsieht, dass die Leistungspflicht des Versicherers hier dem Recht desjenigen Staates unterliegen soll, der solche Deckungskonzepte zulässt. Solche „*Most Favorable Venue*"- und „*Most-Favorable-Jurisdiction*"-Ansätze sind aus dem US-amerikanischen Markt auch bei „*Punitive-Damages*"-Deckungen bekannt.[55] Eine für Cyber-Deckungen angepasste Klausel mag den Versicherungsschutz beispielsweise wie folgt auch auf die Erstattung von Geldbußen erstrecken:

> *„(This policy covers the) reimbursement of fines and penalties where insurable under the laws of an applicable jurisdiction most favorable to the insured".*[56]

In der Sache bezwecken die Parteien mit dieser Gestaltung eine Rechtswahl der „permissivsten" Rechtsordnung, d.h. also desjenigen Rechts, das in Bezug auf den gewünschten Versicherungsschutz keine oder zumindest möglichst geringe rechtliche Schranken enthält. Aus der Warte des unionalen Internationalen Privatrechts handelt es sich bei solchen Abreden dann zunächst um eine Teilrechtswahl, wie sie im Ausgangspunkt Art. 3 Abs. 1 S. 2 Rom I-VO gestattet. Allerdings mögen sich hier nicht nur Wirksamkeitshindernisse aus zwingenden Normen ergeben,[57] sondern es wird im weiteren Verlauf der Abhandlung noch darzulegen sein, dass diese Gestaltung quer zum internationalen Unionsprivatrecht und insbesondere zu Art. 3 Abs. 1 Rom I-VO steht.[58]

---

55 *Lüttringhaus*, Punitive Damages and Insurance, in: Lutzi, Punitive Damages, Mohr Siebeck (im Erscheinen).

56 Vgl. zu solchen „meistbegünstigenden" Wordings in Cyber-Policen nur *OECD*, Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation, 2020, S. 19.

57 Vgl. neben Art. 9 Rom I-VO vor allem Art. 3 Abs. 3 und Abs. 4 Rom I-VO und siehe dazu sogleich unter bb).

58 Dazu eingehend unter D IV 2.

bb) Grenzen der Rechtswahl nach Art. 3 Rom I-VO

Den oben beispielhaft skizzierten Vertragsgestaltungen können indes jeweils international-privatrechtliche Rechtswahlgrenzen entgegenstehen – und zwar auch jenseits der *Ex-ante*-Durchsetzung von Eingriffsnormen nach Art. 9 Rom I-VO und der *Ex-post*-Korrektur über den materiell-rechtlichen *ordre public* gemäß Art. 21 Rom I-VO: Denn Art. 3 Abs. 3 Rom I-VO beschränkt die Parteiautonomie in Sachverhalten, die ausschließlich Bezüge zum Inland aufweisen, und Art. 3 Abs. 4 Rom I-VO überträgt diese Ratio auf Konstellationen, in denen alle Sachverhaltselemente im EU-Binnenmarkt belegen sind.[59] Hinter beiden Regelungsansätzen steht der Gedanke, dass die Parteien durch Rechtswahl bei „rein (binnenmarkt)internen" Sachverhalten jedenfalls nicht diejenigen Vorschriften sollen ausschalten können, von denen sachrechtlich nicht durch Vereinbarung abgewichen werden kann.

Während bei Cyber-Versicherungen schon aufgrund der fast notwendig grenzüberschreitenden Natur der (Haftpflicht)Risiken kaum je die Rede von einem i.S.d. Art. 3 Abs. 3 Rom I-VO nur auf einen Staat bezogenem Vertrag wird sein können, könnte hingegen die sog. Binnenmarktklausel des Art. 3 Abs. 4 Rom I-VO durchaus zur Anwendung kommen. Dies wäre insbesondere der Fall, wenn die Parteien eines Cyber-Versicherungsvertrags durch die Wahl eines besonders „permissiven" drittstaatlichen Rechts gerade von den nicht-dispositiven Bestimmungen des Unionsrechts abweichen wollen, obschon alle relevanten Sachverhaltselemente innerhalb des EU-Binnenmarkts belegen sind. Zu denken ist etwa an die Deckung von Geldbußen wegen Verstößen gegen unionsrechtliche Vorgaben, wie sie die DSGVO[60] oder die NIS-2-RL[61] enthalten: Liegen die aus der Perspektive dieser Rechtsakte relevanten Sachverhaltsbe-

---

59 BeckOGK BGB/*Wendland*, 1.9.2022, Art. 3 Rom I-VO Rn. 227 ff.

60 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO), ABl. 2016 L 119/1.

61 Richtlinie des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. 2022 L333/80.

züge in einem oder mehreren EU-Mitgliedstaaten, so können sich die Parteien durch die Wahl eines drittstaatlichen Rechts – d.h. also des Rechts eines Nicht-EU-Staates – nicht ohne Weiteres dem Anwendungsbereich derjenigen Bestimmungen der EU-Rechtsordnung entziehen, die innerhalb der EU nicht zur Disposition der Parteien stehen.[62]

cc) Objektive Anknüpfung bei fehlender Rechtswahl

Falls die Parteien keine Rechtswahl getroffen haben, unterliegt ein Cyber-Versicherungsvertrag, der Großrisiken zum Gegenstand hat, nach Art. 7 Abs. 2 UAbs. 2 S. 1 Rom I-VO dem Recht des Staats, in dem der Versicherer seinen gewöhnlichen Aufenthalt hat. Nach der Ausweichklausel des Art. 7 Abs. 2 UAbs. 2 S. 2 Rom I-VO soll dies nur dann nicht gelten, wenn sich aus der Gesamtheit der Umstände ergibt, dass der Versicherungsvertrag eine offensichtlich engere Verbindung zu einem anderen Staat aufweist: In diesem – eng auszulegenden – Ausnahmefall ist das Recht dieses anderen Staates anzuwenden.

b) Massenrisiken: KMU unterhalb der Großrisiko-Schwelle

Korrespondierend mit der wachsenden Nachfrage von kleinen und mittleren Unternehmen (KMU) nach Cyber-Versicherungslösungen gewinnt die Frage an Bedeutung, wie solche Verträge bei Auslandsbezügen international-privatrechtlich sachgerecht zu erfassen sind. Auch auf Ebene des internationalen Versicherungsvertragsrechts verläuft die Trennlinie zwischen sog. Groß- und Massenrisiken: Direktversicherungsverträge über Massenrisiken sind all jene Verträge, durch die ein Risiko abgedeckt wird, das kein Großrisiko i.S.d. Art. 7 Abs. 2 Rom I-VO i.V.m. Art. 13 Nr. 27 Solvency II-RL ist. Damit entspricht die Großrisiko-Definition § 210 Abs. 2 VVG i.V.m. Anlage 1 zum VAG. Gerade bei KMU erscheint es gut möglich,

[62] Vgl. dazu auch unten D II und IV.

dass zwei der drei dort genannten Kennzahlen nicht überschritten werden.[63]

Während Art. 7 Abs. 1 i.V.m. Art. 3 Rom I-VO für Großrisiken umfassende Rechtswahlfreiheit gewährt, sind die Grenzen der Parteiautonomie bei Massenrisiken deutlich enger gefasst: Jedenfalls bei innerhalb der EU belegenen Massenrisiken sieht Art. 7 Abs. 3 UAbs. 1 Rom I-VO Beschränkungen vor.[64] Ist eine juristische Person Versicherungsnehmerin, verortet Art. 7 Abs. 6 Rom I-VO i.V.m. Art. 13 Nr. 13 lit. d (ii) Solvency II-RL das Risiko bei Nicht-Lebensversicherungsverträgen in dem Mitgliedstaat, in welchem die Niederlassung liegt, auf die sich der Vertrag bezieht. Soll ein Cyber-Versicherungsvertrag zwei oder mehr Risiken aus der Tätigkeit eines KMU abdecken, die in unterschiedlichen EU-Mitgliedstaaten belegen sind, so können die Parteien nach Art. 7 Abs. 3 UAbs. 1 lit. e Rom I-VO den gesamten Vertrag einheitlich dem Recht des Staates unterstellen, in dem entweder eines der versicherten Risiken belegen ist oder in dem der Versicherungsnehmer seinen gewöhnlichen Aufenthalt hat.[65] Diese Konzentration des Versicherungsvertragsstatuts auf ein anwendbares Recht erscheint gerade bei der Cyber-Versicherung als Multi-Line-Produkt sinnvoll. Denn zum einen sind Cyberrisiken schon ihrem Wesen nach ubiquitär und damit schwer zu lokalisieren, was insbesondere bei der Nutzung von – mittlerweile häufig mitversicherten –[66] Cloud-Diensten klar zutage tritt: Hier können Datenfragmente je nach verfügbarer Speicherkapazität in Sekundenbruchteilen nahezu beliebig zu Serverstandorten überall auf der Welt verschoben werden.[67] Zum anderen sind die in den einzelnen Bausteinen für Haftpflicht, Eigenschäden und Forensik-/

---

63 § 210 Abs. 2 Nr. 3 VVG nennt neben einer Bilanzsumme von 6.600.000 EUR auch Nettoumsatzerlöse von 13.600.000 EUR sowie im Durchschnitt 250 Arbeitnehmer pro Wirtschaftsjahr.

64 Dagegen besteht für außerhalb der EU belegene Massenrisiken zumindest im KMU-Kontext keine derartige Schranke: Art. 7 Rom I-VO ist hier unanwendbar und die Rechtswahl unterliegt damit in erster Line Art. 3 Rom I-VO, siehe nur BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 38.

65 BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 125 und 127.

66 Vgl. nur Ziff. A1-2.2 AVB-Cyber 2024.

67 Vgl. statt vieler *Nordmeier,* MMR 2010, 151 ff.; *Schneidereit*, Haftung für Datenverlust im Cloud Computing, 2017, S. 71 f.

Service-Kosten gedeckten Risiken sowie insbesondere auch „Assistance“-Leistungen bereits sachrechtlich durchaus heterogen.[68]

Schon unter diesen Gesichtspunkten erscheint die Wahl eines einheitlichen Versicherungsvertragsstatuts nach Art. 7 Abs. 3 UAbs. 1 lit. e Rom I-VO dringend geboten und der objektiven Anknüpfung unbedingt vorzugswürdig. Denn nach Art. 7 Abs. 3 UAbs. 3 und Abs. 5 Rom I-VO würde der Cyber-Versicherungsvertrag in Ermangelung einer Rechtswahl zwar dem Recht des Mitgliedstaats unterliegen, in dem zum Zeitpunkt des Vertragsschlusses das Risiko belegen ist. Jedoch sieht Art. 7 Abs. 5 Rom I-VO bei (Cyber-)Risiken, die in mehr als einem Mitgliedstaat belegen sind, eine wenig sachgerechte Aufspaltung des Versicherungsvertragsstatuts vor. Infolgedessen ist der Cyber-Versicherungsvertrag „als aus mehreren Verträgen bestehend anzusehen, von denen sich jeder auf jeweils nur einen Mitgliedstaat bezieht“. Unterhält beispielsweise ein deutsches KMU neben seiner deutschen auch eine französische Niederlassung, die unter einem einheitlichen Cyber-Versicherungsvertrag versichert werden soll, so unterlägen nach Art. 7 Abs. 3 UAbs. 3 und Abs. 5 Rom I-VO die in Deutschland belegenen Risiken deutschem und die in Frankreich belegenen Risiken französischem (Versicherungs)Recht. Nach Art. 7 Abs. 5 Rom I-VO droht damit eine Aufspaltung nach Risikobelegenheit, die im Extremfall zu einem „Mosaik“ aus unterschiedlichen Rechtsordnungen führen kann.

c) Sonderfrage: Einzuhaltende Sicherheitsvorschriften und vertragliche Obliegenheiten bei Auslandsbezügen

Ziff. A1-16.1 AVB-Cyber 2024 stellt eine Reihe von vertraglichen Obliegenheiten i.S.d. § 28 Abs. 1 und Abs. 2 VVG auf, die den Versicherungsnehmer zur Gewährleistung der IT-Sicherheit anhalten sollen.[69] Darüber hinaus verpflichtet Ziff. A1-16.2 lit. a AVB-Cyber 2024 den Versicherungsnehmer, „alle gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften einzuhalten“.

---

[68] Zur Einordnung unterschiedlicher Assistance-Bausteine eingehend z.B. *Koch*, VersR 2019, 449 ff.; *Fortmann*, r+s 2019, 429, 440.

[69] Die Rechtsfolgen i.S.d. § 28 Abs. 1 bzw. Abs. 2-3 und Abs. 5 VVG werden in Ziff. B3-4 AVB-Cyber 2024 dargestellt.

Eine solche Klausel-Formulierung begegnet schon in innerstaatlichen Konstellationen unter dem Gesichtspunkt der Transparenz i.S.d. § 307 Abs. 1 S. 1 BGB erheblichen Bedenken, weil ein durchschnittlicher Versicherungsnehmer i.d.R. gar nicht hinreichend klar erkennen können wird, an welchen konkreten Vorgaben er sein Verhalten nun ausrichten soll; entsprechend läuft die verhaltenssteuernde Funktion der – mit einer Verschlechterung der Rechtsstellung sanktionierten – Obliegenheit hier leer.[70] Zu diesen berechtigten Kritikpunkten treten in Sachverhalten mit Auslandsbezug weitere Herausforderungen hinzu: Denn je nach Fallgestaltung ist genau zu hinterfragen, welcher Rechtsordnung die gesetzlichen und behördlichen IT-Sicherheitsvorgaben entnommen werden müssen. Diese Frage ist angesichts des im Ausgangspunkt weltweiten Deckungsversprechens in Ziff. A1-11 AVB-Cyber 2024 keineswegs nur theoretischer Natur. Die Klausel lautet:

> *„Versicherungsschutz besteht für Versicherungsfälle weltweit. Dies gilt jedoch nur, soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht werden."*

Schwierigkeiten bereitet dies zunächst im Kontext des Haftpflichtbausteins (**dazu unter aa**), wobei der genaue Inhalt der vertraglichen Obliegenheiten nach Ziff. A1-16.2 lit. a AVB-Cyber 2024 sodann auch im Rahmen aller weiteren Deckungsbausteine fraglich erscheinen wird (**dazu unter bb**).

aa) Relevanz der maßgeblichen IT-Sicherheitsstandards im Haftpflichtbaustein: Law-mix voraus?

Der zweite Satz von Ziff. A1-11 AVB-Cyber 2024 adressiert zunächst den Haftpflichtbaustein, wenn dort auf „Ansprüche in EWR-

[70] Vgl. zu ähnlichen Klausel-Formulierungen in der Wohngebäudeversicherung OLG Schleswig VersR 2019, 1557 f.; OLG Celle 15.09.2022 – 8 U 259/21, wobei der BGH 25.9.2024 – IV ZR 350/22, BeckRS 2024, 27326, hierin weder einen Verstoß gegen das Transparenzgebot nach § 307 Abs. 1 S. 2 BGB noch eine unangemessene Benachteiligung i.S.d. § 307 Abs. 1 S. 1 BGB erblickt hat. Vgl. zur Cyber-Versicherung auch die berechtigte Kritik von Prölss/Martin/*Klimke*, 32. Aufl. 2024, AVB Cyber A1-16 Rn. 18 f.; Bruck/Möller/*Koch*, 10. Aufl. 2023, AVB Cyber A1-16 Rn. 10 f. Offener – allerdings jeweils ohne eingehende Auseinandersetzung mit den einzelnen Problemen – z.B. *Fortmann*, r+s 2019, 429, 436; Langheid/Wandt/*Rudkowski*, VVG, 4. Aufl. 2024, AVB Cyber Rn. 194.

Staaten und nach deren Recht“ abgestellt wird.[71] Diese Klausel scheint vorauszusetzen, dass Haftpflichtansprüche stets nur einem einzigen Recht unterstehen. Das ist jedoch gerade bei grenzüberschreitenden Cyber-Delikten keineswegs zwingend, weil hier der Staat, an dem der Schädiger Schad-Code (weiter)verbreitet (sog. Handlungsort), sich fast schon regelmäßig von dem Staat unterscheiden wird, in dem der unmittelbare Schadenserfolg eintritt (sog. Erfolgsort). Im Fall derartiger „Cyber-Distanz-Delikte“, die sich z.B. entlang einer Liefer- und Abnehmerkette über Staatsgrenzen hinweg auswirken, können die Haftpflichtansprüche dann zwar einerseits kraft kollisionsrechtlicher Verweisung dem Recht eines EU-/EWR-Staates am Erfolgsort unterliegen,[72] andererseits aber durchaus nach dem IT-Sicherheitsstandard eines anderen (Dritt)Staates am Handlungsort des Schädigers zu bewerten sein. Denn über Art. 17 Rom II-VO sind

> *„(b)ei der Beurteilung des Verhaltens der Person, deren Haftung geltend gemacht wird, … faktisch und soweit angemessen die Sicherheits- und Verhaltensregeln zu berücksichtigen, die an dem Ort und zu dem Zeitpunkt des haftungsbegründenden Ereignisses in Kraft sind.“*

Der Ort des haftungsbegründenden Ereignisses bezeichnet gerade den Handlungsort,[73] so dass also die Haftpflicht durchaus dem Recht des EU-/EWR-Staates A unterstehen kann, während für die maßgeblichen IT-Sicherheitsstandards nach Art. 17 Rom II-VO the-

---

71 Die Bezugnahme auf „Ansprüche“ mag zwar begrifflich neben Haftpflichtansprüchen auch die Leistungsansprüche des Cyber-Versicherungsnehmers – und damit die Deckungsseite – umfassen. Aufgrund der auch in anderen Cyber-Bedingungswerken marktüblichen Wahl zugunsten deutschen Rechts und der die internationale Zuständigkeit deutscher Gerichte begründenden Gerichtsstandsklausel in Ziff. B4-5 und Ziff. B4-6 AVB-Cyber 2024 liefe diese Klausel indes i.d.R. leer. Etwas anderes dürfte sich auch nicht bei internationalen Versicherungsprogrammen unter Einbindung von Lokalpolicen mit abweichender Rechtswahl ergeben, weil etwaige Differenzdeckungen (DIC/DIL) und auch die Versicherung des Finanzinteresses (FINC) regelmäßig unter einer deutschem Recht unterliegenden Masterpolice erfolgen, vgl. dazu statt aller *Armbrüster*, Privatversicherungsrecht, 2. Aufl. 2019, S. 688 ff. Der theoretisch verbleibende Anwendungsbereich wären damit Deckungsbausteine, die aufgrund gezielter (Teil)Rechtswahl nicht dem Recht eines EU/EWR-Staates bzw. nicht der internationalen Zuständigkeit der Gerichte eines solchen Staates unterstehen, wie z.B. spezielle Geldbußendeckungen, die dann jedoch auch unter anderen Aspekten Bedenken begegnen könnten, siehe dazu noch eingehend unten D.

72 I.d.R. nach der allgemeinen Anknüpfung des Art. 4 Rom II-VO, siehe zu den Anknüpfungen im internationalen Cyber-Haftpflichtrecht noch eingehend unten C.

73 Statt vieler BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 43 ff.

oretisch das Recht des Nicht-EU-/EWR-Staates B zu „berücksichtigen“ sein mag.[74] Dieses Beispiel zeigt schon die Limitationen und Schwächen des Ansatzes in Ziff. A1-11 S. 2 AVB-Cyber 2024 auf: Werden die Ansprüche bei einem solchen „law-mix“ nur nach dem Recht von EU-/EWR-Staaten „geltend gemacht“?

Während Art. 17 Rom II-VO allein außervertragliche Haftungsverhältnisse erfasst, können – z.B. bei der Weiterverbreitung von Schad-Code entlang der Lieferkette – auch vertragliche Haftungsansprüche und damit die Einhaltung von Cyber-Sicherheitsstandards innerhalb von Vertragsverhältnissen relevant werden: Selbst wenn es an einer – wohl mittlerweile üblichen – expliziten vertraglichen Vereinbarung zwischen den Vertragspartnern hinsichtlich des einzuhaltenden IT-Sicherheitsniveaus fehlen sollte, dürften die jeweils am Ort des Handelnden maßgeblichen Cyber-Sicherheitsstandards zumindest als sog. *local data*[75] auf Ebene des Sachrechts berücksichtigungsfähig sein.[76] Auch hier droht potentiell ein „law-mix“, weil dieser Handlungsort rasch jenseits der eigenen Betriebsstätte des Versicherungsnehmers zu lokalisieren sein kann: So läge der Fall z.B. bei einer durch einen Außendienstmitarbeiter des Versicherungsnehmers bei einem Kunden im Nicht-EWR-Ausland verursachten Informationssicherheitsverletzung, die zugleich die (IT-) Infrastruktur des Kunden im EWR beeinträchtigt und entsprechend Haftpflichtansprüche am Erfolgsort (i.S.d. Art. 4 Abs. 1 Rom II-VO) nach dem Recht eines EWR-Staates auslöst. Hier wäre u.a. zu fragen, ob die dann kollisionsrechtlich als Deliktsstatut am Erfolgsort geltenden Regeln einerseits und am Handlungsort im Wege des Art. 17 Rom II-VO anwendbaren Cyber-Sicherheitsregeln andererseits auch für die Einhaltung der Obliegenheit zur Beachtung der „gesetzlichen und behördlichen“ Sicherheitsstandards i.R.d. Haftpflichtbausteins relevant werden sollen. In Ermangelung einer näheren Spezifikation in Ziff. A1-16.2 lit. a AVB-Cyber 2024 dürfte zwar durchaus naheliegen, dass die für die Haftpflicht einerseits und für

---

74 Siehe dazu im Kontext der internationalen Cyber-Haftpflicht sogleich eingehend unter C IV.

75 Vgl. zur Funktion des Art. 17 Rom II-VO und der Sachnähe zur „Datumtheorie“ nur BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 17 Rom II-VO Rn. 1; BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 4. Siehe dazu im Kontext der internationalen Cyber-Haftpflicht sogleich auch unter C IV.

76 Vgl. *Bach* in: Spindler/Schuster, Elektron. Medien, 4. Aufl. 2019, Art. 40 EGBGB Rn. 9 f.

die Haftpflichtdeckung andererseits relevanten Cyber-Sicherheitsstandards korrespondieren. Aus der Warte eines durchschnittlichen und um Verständnis bemühten – gewerblich tätigen – Cyber-Versicherungsnehmers, der auch den erkennbaren, systematischen Zusammenhang der Klausel im Bedingungswerk berücksichtigt, dürfte das aber spätestens nach einem kurzen Seitenblick auf die übliche Rechtswahlklausel zugunsten deutschen Rechts mehr als fraglich erscheinen: Denn wenn „für diesen Vertrag … deutsches Recht" gelten soll, erscheint es explizit begründungs- und vor allem klarstellungsbedürftig, wenn für die inhaltliche Ausgestaltung von Obliegenheiten dann plötzlich „gesetzliche und behördliche" Cyber-Sicherheitsstandards einer anderen Rechtsordnung maßgeblich sein sollten.[77] Diese Frage gilt es hinsichtlich der durch den Versicherungsnehmer zu beachtenden vertraglichen Obliegenheiten sogleich noch zu vertiefen.[78] Festzuhalten bleibt, dass im Haftpflichtbaustein gleich in zweierlei Hinsicht Friktionen drohen: Erstens erscheint der in Ziff. A1-11 AVB-Cyber 2024 mit dem anwendbaren Recht von EU-/EWR-Staaten verknüpfte territoriale Deckungsumfang immer dann fraglich, wenn ein „law-mix" in Betracht kommt. Zweitens birgt gerade das Zusammenspiel von Rechtswahlklausel und Ziff. A1-16.2 lit. a AVB-Cyber 2024 in grenzüberschreitenden Sachverhalten Potential für ein – wohl auch durch die Cyber-Versicherer unerwünschtes – Auseinanderfallen der für die Haftpflicht einerseits und sodann für vertragliche Obliegenheiten andererseits maßgeblichen IT-Sicherheitsstandards. Insoweit erscheint eine Präzisierung der Regelung für grenzüberschreitende Konstellationen ratsam.

bb) Vertragliche Obliegenheiten zur Einhaltung von IT-Sicherheitsstandards in grenzüberschreitenden Sachverhalten

Soweit es um die Einhaltung vertraglicher Obliegenheiten in grenzüberschreitenden Sachverhalten geht, ist die soeben skizzierte Problematik keineswegs auf den Haftpflichtbaustein beschränkt, son-

[77] Vgl. zur Bestimmung des anwendbaren Rechts nur die Rechtswahlklausel in Ziff. B4-6 AVB-Cyber 2024.

[78] Siehe unten bb).

dern stellt sich angesichts des weltweiten Deckungsversprechens in Ziff. A1-11 S. 1 AVB-Cyber 2024 bei sämtlichen Cyber-Deckungsbausteinen: Entsprechend könnte der Pauschalverweis auf „alle gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften“ in Ziff. A1-16.2 lit. a AVB-Cyber 2024 in Sachverhalten mit Auslandsberührung jeweils Abgrenzungsschwierigkeiten begründen, welcher der – potentiell unterschiedlichen – nationalen IT-Sicherheitsstandards für die Einhaltung der Obliegenheiten maßgeblich sein soll. Hier müsste für den Versicherungsnehmer hinreichend ersichtlich sein, welchem Recht die „gesetzlichen und behördlichen“ Sicherheitsvorschriften jeweils zu entnehmen und wie infolgedessen die vertraglich vereinbarten Obliegenheiten konkret ausgestaltet sind. Im Ausgangspunkt beschränkt Ziff. A1-10 Abs. 1 AVB-Cyber 2024 das Deckungsversprechen in territorialer Hinsicht auf die Bundesrepublik Deutschland, soweit es um Betriebsstätten und informationsverarbeitende Systeme geht, die der Versicherungsnehmer selbst betreibt. Allerdings lässt Ziff. A1-10 Abs. 2 AVB-Cyber 2024 die individualvertragliche Erstreckung des Versicherungsschutzes auch auf vom Versicherungsnehmer selbst betriebene ausländische Betriebsstätten zu. Abgesehen davon, dass grenzüberschreitend tätige Unternehmen eine solche territoriale Deckungserweiterung wohl standardmäßig gegen Mehrprämie vereinbaren werden, gewährt Ziff. A1-2.2 AVB-Cyber 2024 ohnehin international unbegrenzten Versicherungsschutz, soweit der Versicherungsnehmer externe Dienstleister – wie beispielsweise Cloud- oder sonstige IT-Infrastruktur-Anbieter – heranzieht: Aus dem Zusammenspiel von Ziff. A1-2.2 und Ziff. A1-10 Abs. 2 AVB-Cyber 2024 geht hervor, dass solche externen Dienstleister und deren informationsverarbeitende Systeme auch im Ausland ansässig sein und von dort aus ihre jeweiligen (IT-)Dienstleistungen erbringen können.[79]

[79] Statt vieler Looschelders/Pohlmann/*Malek*, 4. Aufl. 2023, F. AVB Cyber Rn. 93; Langheid/Wandt/*Rudkowski*, VVG, 4. Aufl. 2024, Kap. 37: AVB Cyber Rn. 65. Kein Versicherungsschutz soll aber gemäß A1-2.2 Abs. 2 AVB-Cyber 2024 für Schäden bestehen, die infolge des „Ausfalls, der Unterbrechung oder Störung der Dienstleistung entstehen, soweit sie zu einer Beeinträchtigung der Verfügbarkeit der elektronischen Daten oder informationsverarbeitenden Systeme des Versicherungsnehmers führen“.

Dieser im Wortlaut und in der Systematik der AVB angelegte territoriale Deckungsumfang lässt für einen durchschnittlichen Cyber-Versicherungsnehmer deshalb womöglich den Schluss zu, dass Ziff. A1-16.2 lit. a AVB-Cyber 2024 potentiell verlangt, dass weltweit ausnahmslos „alle gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften“ beachtet werden. Schließlich können neben den jeweiligen in- und ausländischen Standorten der Betriebsstätten und informationsverarbeitenden Systeme des Versicherungsnehmers selbst auch alle Standorte und IT-Systeme seiner externen Dienstleister betroffen sein. Weder Ziff. A1-16.2 lit. a noch eine andere Klausel der AVB-Cyber 2024 stellen jedoch klar, in welchem Verhältnis die jeweiligen IT-Sicherheitsstandards und sonstigen (unter)gesetzlichen und vertraglichen Sicherheitsstandards nun zueinander stehen sollen: Müssen ausländische Standards nun immer ergänzend zu den im deutschen Inland maßgeblichen Sicherheitsvorschriften eingehalten werden? Oder soll insoweit eine präzise Trennlinie zwischen den jeweiligen in- und ausländischen Betriebsstätten gezogen werden, obschon dies gerade bei grenzüberschreitend vernetzten Produktions- und Arbeitsprozessen kaum immer technisch-organisatorisch lückenlos gangbar erscheint? Zusätzliche Verwirrung dürfte aus der Perspektive eines durchschnittlichen Cyber-Versicherungsnehmers sodann stiften, dass die Parteien für den gesamten Cyber-Versicherungsvertrag gemäß Ziff. B4-6 AVB-Cyber 2024 ausnahmslos „deutsches Recht“ gewählt haben.[80] Schon aus Art. 3 Abs. 3 und Abs. 4 sowie natürlich auch aus Art. 9 Rom I-VO folgt zwar, dass die Vertragsparteien kraft einer solchen Rechtswahl nicht von den im Übrigen anwendbaren (international) zwingenden Bestimmungen abweichen können. Auch bezweckt die Ziff. A1-16.2 lit. a AVB-Cyber 2024 in der Sache keine abweichende (Teil)Rechtswahl gemäß Art. 3 Abs. 1 S. 3 Rom I-VO zugunsten bestimmter IT-Sicherheitsstandards, sondern nur die Formulierung von – wenn auch sehr allgemein gehaltenen – vertraglichen Obliegenheiten. Dessen ungeachtet, muss mit Fug und Recht bezweifelt werden, ob sich diese überaus diffizile rechtliche Unterscheidung einem durchschnittlichen Cyber-Versicherungsnehmer ohne Weiteres erschließt. Selbst die üblicherweise hochgradig

[80] Vgl. erneut Ziff. B4-6 AVB-Cyber 2024.

geschäftserfahrenen Nachfrager von Cyber-Versicherungen werden kaum aus dem Zusammenspiel von Ziff. A1-2.2, Ziff. A1-10 Abs. 2 und Ziff. A1-16.2 lit. a AVB-Cyber 2024 eine klare territoriale Eingrenzung der maßgeblichen IT-Sicherheitsstandards entnehmen können, noch dürfte Ihnen die Reichweite und Bedeutung der Rechtswahlklausel in diesem Zusammenhang direkt erkennbar sein. Anders gewendet, sind die maßgeblichen IT-Sicherheitsstandards jedenfalls bei Bezügen zu multiplen Rechtsordnungen zunächst unklar, wobei auch die Auslegungsregel des § 305c Abs. 2 BGB kaum jemals zu eindeutigen Ergebnissen führen dürfte. Dann liegt das Verdikt nahe, dass Ziff. A1-16.2 lit. a AVB-Cyber 2024 jedenfalls bei Einbeziehung ausländischer Dienstleister und/oder im Fall der Mitversicherung zahlreicher im Ausland belegenen Betriebsstätten gemäß Ziff. A1-10 Abs. 2 AVB-Cyber 2024 nach § 307 Abs. 1 S. 2 BGB intransparent und infolge dessen unwirksam ist. Hier kann und muss der Cyber-Versicherer entsprechend nachschärfen. Das erscheint auch zumutbar, zumal die unionale, ebenso wie die nationale Rechtsprechung Klauselverwendern auch in anderem Kontext aufgibt, die Reichweite einer Rechtswahl klarzustellen und zugleich all jene Normen und Standards gesondert zu erwähnen, die für den Vertragsinhalt besonders relevant und zugleich der Parteidisposition entzogen sind.[81] In der Internationalität der rechtlichen wie auch der tatsächlichen Verhältnisse liegt zugleich der entscheidende Unterschied zu einer jüngst durch den BGH im Kontext der Wohngebäudeversicherung getroffenen Entscheidung: Während der Wortlaut von Ziff. A1-10 Abs. 2 AVB-Cyber 2024 und der korrespondierenden Klausel in der Wohngebäudeversicherung sich noch ähneln, wird das Verständnis für einen durchschnittlichen Cyber-Versicherungsnehmer gerade durch die multiplen Auslandsbezüge in einer Weise erschwert, dass dieser schon gar nicht nachvollziehen kann, an welchen – einzelnen oder womöglich sogar ku-

[81] Vgl. zum persönlich-sachlich hier nicht einschlägigen Verbrauchervertragsrecht z.B. im Kontext der FlugastrechteVO nur LG Frankfurt NJW-RR 2020, 1312, 1313; LG Frankfurt 19.1.2023 – 2-24 S 74/22O, BeckRS 2023, 2187 Rn. 28 f.; LG Köln NZV 2021, 196, 197 ff. sowie zu den günstigeren Bestimmungen i.S.d Art. 6 Rom I-VO im Kontext der Klauselkontrolle grundlegend EuGH 28.7.2016 – Rs. C-191/15 (*Amazon*) ECLI:EU:C:2016:612 Rn. 61 ff.

mulierten – nationalen IT-Sicherheitsstandards er sein Verhalten nun ausrichten soll.[82]

2. Art. 7 Abs. 4 Rom I-VO

Während neben der EU-Versicherungsaufsichtsbehörde EIOPA[83] und der Agentur der Europäischen Union für Cybersicherheit ENISA[84] auch manche Stimmen im Schrifttum[85] eine Pflichtversicherung für Cyber-Risiken gefordert haben, ist zumindest für den EU-Raum derzeit keine derartige Initiative absehbar.[86] Ein Seitenblick auf die wellenförmige Diskussion über die Pflichtversicherung für Elementarschäden zeigt jedoch, dass mit wiederholten und wachsenden Bedrohungsszenarien die Debatte über Versicherungspflichten wiederkehren könnte. Eine Versicherungspflicht bliebe dann nicht ohne Folgen für das auf Cyber-Versicherungsverträge anwendbare Recht: Denn nach Art. 7 Abs. 4 Rom I-VO ist ggf. das Recht des EU-Mitgliedstaats zu beachten, der die Versicherungspflicht vorschreibt. Soweit Nicht-EU-Staaten aktuell oder künftig Versicherungspflichten aufstellen sollten, ist zwar Art. 7 Abs. 4 Rom I-VO schon nach seinem Wortlaut („Mitgliedstaat") nicht unmittelbar anwendbar. Auch wenn man keine analoge Anwendung in Betracht ziehen möchte, erscheint es grundsätzlich sinnvoll,

---

82 Vgl. im Kontext einer ähnlichen Klausel-Formulierung in der Wohngebäudeversicherung BGH 25.9.2024 – IV ZR 350/22, BeckRS 2024, 27326 entgegen OLG Celle 15.09.2022 – 8 U 259/21; OLG Schleswig VersR 2019, 1557 f. Vgl. zur Cyber-Versicherung auch die berechtigte Kritik von Prölss/Martin/*Klimke*, 32. Aufl. 2024, AVB Cyber A1-16 Rn. 18 f.; Bruck/Möller/*Koch*, 10. Aufl. 2023, AVB Cyber A1-16 Rn. 10 f. Offener z.B. *Fortmann*, r+s 2019, 429, 436; Langheid/Wandt/*Rudkowski*, VVG, 4. Aufl. 2024, AVB Cyber Rn. 194.

83 Vgl. nur *EIOPA*, Cyber Security and Cyber Risk: A universal Challenge, Keynote speech by Gabriel Bernardino at the 3rd Annual FinTech and Regulation Conference on „Taking innovation to the next level" on 26 February 2019 in Brussels, S. 6: „As cyber-insurance markets mature, we should start to discuss if cyber insurance should also be mandatory. This would provide a further level of security for companies and consumers in the digital world."

84 Vgl. nur die von der European Network and Information Security Agency (ENISA) herausgegebene Studie von *Anderson/Böhme/Clayton/Moore*, Security Economics and the Internal Market (2008), S. 84 f. siehe dort aber auch – kritisch – S. 86 f.

85 Programmatisch titelt etwa *Lemnitzer*, Journal of Cyber Policy 6(2) (2021), 118 ff.: „Why cybersecurity insurance should be regulated and compulsory". Siehe zuvor schon *Trang*, Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches, 18 Minnesota Journal of Law, Science & Technology 389 (2017).

86 Dezidiert gegen eine Versicherungspflicht im Bereich der Cyber-Versicherung auch z.B. *Insurance Europe*, Insurers' role in EU cyber resilience (2019), s. 9 f.

drittstaatliche Versicherungspflichten in der Praxis einzuhalten und den Vertrag entsprechend auszugestalten.[87]

3. Eingriffsnormen und ordre public Art. 9, Art. 21 Rom I-VO

Bestimmte Vorschriften können als sog. Eingriffsnormen i.S.d. Art. 9 Rom I-VO ungeachtet des nach Art. 3 ff. und Art. 7 bestimmten Versicherungsvertragsstatuts zur Anwendung kommen. Zu dieser Normkategorie zählt nur eine zwingende Vorschrift, „deren Einhaltung von einem Staat als so entscheidend für die Wahrung seines öffentlichen Interesses, insbesondere seiner politischen, sozialen oder wirtschaftlichen Organisation, angesehen wird, dass sie ungeachtet des nach Maßgabe dieser Verordnung auf den Vertrag anzuwendenden Rechts auf alle Sachverhalte anzuwenden ist, die in ihren Anwendungsbereich fallen".[88] Eingriffsnormen werden somit von vornherein unabhängig von den allgemeinen Kollisionsnormen angewendet.

Bei Art. 9 Abs. 2 Rom I-VO handelt es sich um eine Öffnungsklausel, die es dem Mitgliedstaat des angerufenen Gerichts ermöglicht, sein nationales – in aller Regel einseitiges und häufig ungeschriebenes – Kollisionsrecht für Eingriffsnormen anzuwenden.[89] Neben den Eingriffsnormen des Gerichtsstaats nach Art. 9 Abs. 2 ermöglicht es Art. 9 Abs. 3 Rom I-VO dem Gericht zudem, den Eingriffsnormen am Erfüllungsort des Versicherungsvertrages „Wirkung zu verleihen".[90] International zuständige deutsche Gerichte können darüber hinaus ausländische Eingriffsnormen zumindest auf Ebene des Sachrechts über die privatrechtlichen Generalklauseln – und

---

87 Vgl. schon *Basedow/Scherpe,* FS Heldrich, 2005, 511, 526. Für eine Analogie zu Art. 7 Abs. 4 Rom I-VO Staudinger/*Armbrüster*, 2021, Art. 7 Rom I-VO Rn. 22.

88 Art. 9 Abs. 1 Rom I-VO.

89 *Sonnenberger,* FS Kropholler, 2008, 227, 241 ff. Siehe auch BeckOGK BGB/Lüttringhaus, 1.12.2023, Art. 7 Rom I-VO Rn. 183.

90 BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 9 Rom I-VO Rn. 92 ff.; BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 188 ff. Vgl. zuletzt etwa OLG Frankfurt VersR 2024, 1347, 1352.

damit insbesondere über § 138 Abs. 1 BGB – berücksichtigen.[91] Diese Form der materiell-rechtlichen Berücksichtigung ausländischer Eingriffsnormen ist nach Auffassung des EuGH insbesondere mit Art. 9 Abs. 3 Rom I-VO vereinbar.[92] Anders als bei der materiell-rechtlichen Berücksichtigung drittstaatlicher Eingriffsnormen über § 138 Abs. 1 BGB setzt die Anwendung von Art. 9 Abs. 3 Rom I-VO nicht zwingend voraus, dass hinsichtlich der mit der Norm verfolgten Zwecke ein weitgehender Wertungsgleichlauf im Erlassstaat einerseits und im Forumstaat andererseits besteht: Erforderlich und zugleich ausreichend ist hier vielmehr, dass der Forumstaat die Zielrichtung und das Schutzinteresse der Eingriffsnorm prinzipiell ebenfalls anerkennt, ohne die Wertung vollauf zu teilen oder gar korrespondierende eigene Normen vorzusehen.[93]

Zu den im Kontext der Cyber-Versicherung relevanten Anwendungsfeldern von Eingriffsnormen zählen neben etwaigen Verboten der Versicherung von Geldbußen[94] und von „Lösegeldern“ bei Ransomware-Attacken[95] nicht zuletzt Sanktions- und Embargoregelungen.[96] Die Wirkungsweise und die praktischen Auswirkungen solcher eingriffsrechtlichen Sonderanknüpfungen werden deshalb eingehend im Kontext dieser Fragestellungen erläutert.[97]

Im Gegensatz zu den Eingriffsnormen führt der kollisionsrechtliche Ordre-public-Vorbehalt gemäß Art. 21 Rom I-VO lediglich zu einer

---

91 Im „Nigerianischen Masken“-Fall hat der BGH bei einem deutschem Recht unterliegenden Transportversicherungsvertrag ein ausländisches Exportverbot für Kulturgüter im Rahmen des § 138 BGB herangezogen, vgl. BGHZ 59, 82, 85 f.

92 EuGH 18.10.2016 – Rs. C-135/15 (*Nikiforidis*) ECLI:EU:C:2016:774 Rn. 40 ff. und 55. Siehe nur OLG Frankfurt NJW 2018, 3591 Rn. 31 ff. und insbesondere Rn. 43 ff.; OLG München BeckRS 2020, 15428 Rn. 31 ff.; OLG Frankfurt IPRax 2025, 184 Rn. 69 ff. Siehe zur h.M. im Schrifttum m.w.N. nur *Sonnentag*, VersR 2024, 201, 207 f. Kritisch und insbesondere zum Leistungsstörungsrecht differenzierend *Maultzsch*, FS Kronke, 2020, S. 363 ff.; *Maultzsch*, IPRax 2025, 164, 168 ff. Restriktiver z.B. auch Grüneberg/*Thorn* 84. Aufl. 2025, Art. 9 Rom I-VO Rn. 14. Noch vor Erlass der Entscheidung des EuGH in der Rechtssache *Nikiforidis* ablehnend Cour d’appel de Paris 25.2.2015 – n° 12/23757, Recueil Dalloz 2015, 1260, entgegen der vormaligen Rechtsprechungslinie der Cour de cassation 16.3.2010 – n° 08-21.511, zur offener formulierten Vorgängerregelung des Art. 9 Rom I in Art. 7 EVÜ.

93 Siehe nur *Max Planck Institute*, RabelsZ 68 (2004), 1, 76.

94 Dazu eingehend unter D.

95 Dazu näher unter F.

96 Dazu unter F I. Vgl. auch *Tehrani,* VersR 2016, 85 ff.

97 Siehe unten D II, IV sowie unter F II.

nachträglichen Ergebniskontrolle: Eine Korrektur nach Art. 21 Rom I-VO erfolgt nur, wenn das nach den allgemeinen Kollisionsnormen bestimmte Recht mit der öffentlichen Ordnung des Staates des angerufenen Gerichts offensichtlich unvereinbar ist.[98]

III. Ergebnis

Im Fall von Deckungsstreitigkeiten bei Cyber-Versicherungsverhältnissen ist das international zuständige Gericht zuvörderst anhand der in marktgängigen Cyber-Bedingungswerken üblichen Gerichtsstandsklauseln zu bestimmen. Nur wenn eine Gerichtsstandsvereinbarung fehlen oder den Anforderungen des Art. 25 Brüssel Ia-VO nicht genügen sollte, ist auf die allgemeinen Regelungen zur internationalen Gerichtszuständigkeit und damit insbesondere auf Art. 11 ff. Brüssel Ia-VO zurückzugreifen.

Das auf einen Cyber-Versicherungsvertrag in Sachverhalten mit Auslandsbezug anwendbare Recht bestimmt ein international zuständiges deutsches Gericht nach den allgemeinen Kollisionsnormen der Rom I-VO: Während der Rahmen der Parteiautonomie bei Großrisiken weiter gesteckt ist, wird die übliche Rechtswahl im Fall von Massenrisiken nicht nur in die Grenzen von Art. 3 Abs. 3 und Abs. 4, sondern auch in jene des Art. 7 Abs. 3 gefasst.

Bei Cyber-Versicherungsverträgen, die Risiken in mehreren Staaten decken, können sodann besondere Herausforderungen bei der als Obliegenheit formulierten Einhaltung von IT-Sicherheitsvorschriften bestehen: So mag es z.B. Transparenzbedenken begegnen, wenn der Versicherungsnehmer nach Ziff. A1-16.2 lit. a AVB-Cyber 2024 an „alle gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften“ gebunden wird, ohne dass der Kreis dieser nationalen Regelungen sachlich und räumlich-territorial präzisiert wird. Das Versicherungsverhältnis kann darüber hinaus auch durch besondere kollisions- und/oder sachrechtliche Vorgaben beeinflusst werden, etwa falls künftig eine Cyber-Ver-

[98] BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 192.

sicherungspflicht erlassen würde. Darüber hinaus mögen insbesondere in- und ausländische Eingriffsnormen Einfluss darauf nehmen, ob bestimmte Deckungszusagen – z.B. für Lösegelder oder Geldbußen – rechtlich zulässig und im Streitfall auch gerichtlich durchsetzbar sind.

C. Internationale Cyber-Haftpflicht und Verbindungslinien zur Cyber-Haftpflichtdeckung

Wer sich im Cyberspace bewegt, läuft Gefahr, sich Dritten gegenüber haftpflichtig zu machen: Zu denken ist beispielsweise an Szenarien, in denen Angreifer ein Unternehmen mit Malware attackieren und das Unternehmen den Schad-Code sodann in haftungsrelevanter Weise an seine Zulieferer, Abnehmer oder auch an unbeteiligte Dritte weiterleitet und diese dadurch schädigt. Deshalb zählt der Haftpflichtbaustein mit gutem Grund zu den integralen Bestandteilen eines jeden Cyber-Versicherungsvertrages. Aus Sicht des unionalen ebenso wie des deutschen Rechts kommen als haftungsbegründende Normen neben (vor)vertraglichen und deliktischen auch eine Reihe spezialgesetzlicher Tatbestände, wie Art. 82 DSGVO und § 10 GeschGehG[99] in Betracht (**dazu unter I**). Viele Unternehmen haben ihre Wertschöpfungsketten indes grenzüberschreitend vernetzt, so dass auch die Haftungsverhältnisse dem Recht unterschiedlicher ausländischer Staaten unterliegen können. In solchen Sachverhalten mit Auslandsbezug ist somit zunächst nach der international-privatrechtlichen Anknüpfung etwaiger Haftpflichtansprüche zu fragen. Dabei verzahnen manche Cyber-Versicherungsverträge das Internationale Privatrecht der Haftung für Cyberangriffe eng mit dem Cyber-Versicherungsschutz in Fällen mit Auslandsbezug: Denn während Cyber-Versicherungen üblicherweise – mit bestimmten Ausnahmen – Schäden weltweit zu decken versprechen, findet sich folgende Formulierung in den Allgemeinen Cyber-Muster-Versicherungsbedingungen des GDV:

> *„Versicherungsschutz besteht für Versicherungsfälle weltweit. Dies gilt jedoch nur, soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht werden.“*[100]

Obschon dieses Wording in der AVB-Praxis selten verwendet wird, geben diese Anforderungen doch sehr anschaulich die beiden zen-

[99] Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) v. 18.4.2019, BGBl. I 2019, S. 466.

[100] Ziff. A1-11 AVB-Cyber 2024 („Geltungsbereich“).

tralen Elemente der internationalen Dimension der Haftpflicht vor: Erstens ist nämlich zu fragen, unter welchen Voraussetzungen die internationale Zuständigkeit (**dazu unter II**) der Gerichte eines EWR-Mitgliedstaats begründet wird. Im Folgenden wird dabei in erster Linie die Perspektive eines deutschen Gerichts eingenommen und entsprechend neben der Brüssel Ia-VO und dem LugÜ auch das autonome Internationale Zuständigkeitsrecht herangezogen. Zweitens hängt die kollisionsrechtliche Anwendbarkeit des Rechts eines EWR-Staates von der Qualifikation und Anknüpfung solcher Rechtsfragen im unionalen und ggf. im autonomen Internationalen Privatrecht ab (**hierzu unter III**). Schwierigkeiten ergeben sich hier nicht zuletzt mit Blick auf die haftungsrechtlichen relevanten Cyber-Sicherheitsstandards: In grenzüberschreitenden Sachverhalten kann angesichts der Regelung in Art. 17 Rom II-VO auch ein von der *lex causae* abweichendes Recht zur Anwendung kommen (**dazu unter IV**). In der Zusammenschau werden damit die Schwächen des in Ziff. A1-11 AVB Cyber 2024 gewählten Ansatzes deutlich: Wird der Versicherungsschutz für potentiell weltumspannende Cyber-Risiken von der Gerichtszuständigkeit und dem anwendbaren Recht in EWR-Staaten abhängig gemacht, so stellt dies die Rechtsanwender vor große Herausforderungen.

I. Haftungsverhältnisse im Überblick

Infolge einer Cyber-Attacke kann der angegriffene Versicherungsnehmer seinerseits gegenüber Dritten – wie etwa seinen Kunden, Zulieferern und sonstigen Dienstleistern – haftpflichtig werden, wenn z.B. der Schad-Code fahrlässig weiterverbreitet und eine Informationssicherheitsverletzung bei den betroffenen Dritten hervorgerufen wird. Je nach rechtlicher Ausgestaltung der Beziehung zwischen den Beteiligten kommt eine Vielzahl von vorvertraglichen und vertraglichen (**dazu unter 1**) sowie von spezialgesetzlichen und außervertraglichen Haftungstatbeständen (**dazu unter 2**) in Betracht.

Demgegenüber werden die nun auch durch die NIS-2-Richtlinie[101] prominent adressierten gesellschaftsrechtlichen (Binnen)Haftungsfragen bei Cybersicherheitsverstößen vorrangig im Kontext der D&O-Versicherung relevant und sollen deshalb an dieser Stelle nur angedeutet werden.[102]

1. (Vor)vertragliche Haftung des angegriffenen Versicherungsnehmers gegenüber Dritten

Eine (vor)vertragliche Haftung kommt dabei im Rahmen bereits bestehender oder zumindest in Anbahnung befindlicher Geschäftskontakte in Betracht. Die Spannbreite ist hier denkbar weit und reicht innerhalb einer Vertragsbeziehung beispielsweise von Ansprüchen wegen einer durch den Cyber-Angriff bedingten Verzögerung der Leistung (nach §§ 280 Abs. 1, Abs. 2 i.V.m. § 286 BGB) über die teilweise oder vollständige Nichterfüllung oder Unmöglichkeit (§ 280 Abs. 1, Abs. 3 i.V.m. § 281 oder § 283 BGB) sowie die Mangelhaftigkeit (z.B. (Regress)Ansprüche wegen Mängeln einer Kaufsache i.S.d. § 434 BGB infolge von Fehlfunktionen der durch den Angriff betroffenen IIoT-gestützten Produktionslinie) bis hin zu Ansprüchen nach § 280 Abs. 1 BGB wegen Verletzung (vor)vertraglicher Schutzpflichten i.S.d. § 241 Abs. 2 BGB.[103] Solche besonderen Schutzpflichten in Bezug auf die durch den Vertragspartner verarbeiteten und verwahrten Daten liegen – neben ausdrücklicher gesetzlicher Anordnung, etwa bei personenbezogenen Daten i.S.d. DSGVO – immer dann nahe, wenn es sich um vertrauliche Daten

---

101 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333/80. Vgl. dazu auch den BMI-Referentenentwurf v. 6.4.2024 zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, NIS2UmsuCG).

102 Vgl. zu Binnenhaftung nur Art. 20 Abs. 1 NIS-2-Richtlinie sowie § 38 BSIG-E. Freilich kann sich hier durchaus die Frage eines – wiederum potentiell grenzüberschreitenden – Regresses des Cyberversicherers gegen Organe oder Mitarbeiter der Versicherungsnehmerin stellen, vgl. *Schilbach/Becker*, r+s 2023, 289 ff.

103 *Mehrbrey/Schreibauer*, MMR 2016, 75, 80; *Lesser*, Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken, 2021, S. 161 f.

handelt und die verarbeitende Vertragspartei kraft ihrer Stellung zu besonders sorgsamem Umgang und damit auch zu besonderen IT-Sicherheits- und Datenschutzmaßnahmen verpflichtet ist. So verhält es sich aufgrund berufsrechtlicher Vorgaben z.B. bei Steuerberatern, Rechtsanwälten, Notaren und Wirtschaftsprüfern.[104] Gleiches ist angesichts der weiteren aufsichtsrechtlichen IT-Sicherheitsregulierung von Banken, Versicherern und anderen Finanzunternehmen nach Inkrafttreten von DORA (Digital Operational Resilience Act)[105] sowie angesichts der Cybersicherheitsvorgaben für Betreiber kritischer Infrastruktur i.S.d. KRITIS-VO[106] und für die zahlreichen künftig dem NIS-2-Regime[107] unterworfenen Unternehmen unterschiedlichster Branchen anzunehmen. Durch ergänzende Vertragsauslegung wird sich aber auch jenseits solcher spezialgesetzlicher Vorgaben oftmals eine besondere Schutzpflicht nach § 241 Abs. 2 BGB dort begründen lassen, wo z.B. die Schwellenwerte des NIS-2-Regimes und/oder der KRITIS-VO nicht überschritten werden. Zu denken ist etwa an kleinere Online-Händler oder Unternehmen des produzierenden Gewerbes, die (Produkt)Entwürfe, technische Zeichnungen oder sonstige sensible Daten ihrer Geschäftspartner verarbeiten.[108] Ebenso betrifft dies die zunehmende Zahl von Dienstleistern und Zulieferern, die mittels 3D-

---

104 Vgl. etwa für Rechtsanwältinnen und Rechtsanwälte nur § 2 Abs. 2 BORA sowie für Steuerberatende Berufe nur § 11 StBerG.

105 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABl. 2022 L 333/1. Siehe zu DORA und dem Verhältnis und dem Übergang von den versicherungsaufsichtlichen Anforderungen an die IT (VAIT), Rundschreiben 10/2018 (VA) in der Fassung vom 3.3.2022, den Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo), Rundschreiben 2/2017 (VA) in der Fassung vom 2.3.2018 eingehend *BaFin*, DORA – Digital Operational Resilience Act (22.5.2024), abrufbar unter: https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html (zuletzt abgerufen am 1.5.2025). S. auch *Wirth/Schreier*, r+s 2024, 49, 54; *Dittrich/Heinelt*, RDi 2023, 164 ff.

106 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, BGBl. 2016 I 958.

107 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. L 333/80. Vgl. dazu auch den BMI-Referentenentwurf v. 6.4.2024 zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz).

108 *Lesser*, Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken, 2021, S. 26.

Druckverfahren konkrete Bauteile für Industriekunden nach deren Entwürfen fertigen oder Ersatzteile on-demand nachbauen.

Eine Verletzung (vor)vertraglicher Schutzpflichten mag sodann darin liegen, dass – z.B. aufgrund von IT-Sicherheitslücken beim primär Angegriffenen – auch die IT-Systeme von dessen Geschäftskontakten kompromittiert und weitere Daten durch die Cyber-Angreifer erbeutet werden. Eine grenzüberschreitende und potentiell sogar weltumspannende Dimension erhält die Haftpflicht infolge einer solchen Cyber-Attacke, wenn im Fall globaler Unternehmen – wie beispielsweise internationaler Hotelketten,[109] Fluglinien,[110] Social-Media-Dienste, Online-Händler oder auch Finanz- oder IT-Dienstleister – eine große Zahl sensibler Daten in die Hände von Cyber-Kriminellen fällt.

2. Deliktische Haftung des angegriffenen Versicherungsnehmers gegenüber Dritten

Zumindest aus Sicht des deutschen Sachrechts stellt sich bei einer Schädigung von Kunden, Zulieferern oder auch sonstigen Dritten durch ein cyberversichertes Unternehmen stets (auch) die Frage einer außervertraglichen und insbesondere deliktischen Haftung. Bereichsbezogen bestehen dabei spezialgesetzliche Anspruchsgrundlagen: So findet beispielsweise[111] der unionsrechtlich-autono-

---

[109] Vgl. nur die Geldbuße i.H.v. 18,4 Millionen GBP für Verstöße in UK *Information Commissioner's Office* (ICO) Penalty Notice (Case ref: COM0804337) v. 20.10.2020 wegen Verstößen gegen Sec. 155 Data protection Act 2018, die insgesamt rund 339 Millionen Hotelgäste von *Marriott International Inc*. betreffen könnten. Wegen derselben Verstöße hat nun auch in den USA u.a. die *Federal Trade Commission* (FTC) eine Geldbuße i.H.v. 52 Millionen USD verhängt. Siehe zum Ganzen nur *Tidy*, Marriott Hotels fined £18.4m for data breach that hit millions, BBC v. 30.10.2020, abrufbar unter: https://www.bbc.com/news/technology-54748843. Siehe auch *Veiga*, Marriott agrees to pay $52 million, beef up data security to resolve probes over data breaches, AP News v. 10.10.2024, abrufbar unter: https://apnews.com/article/marriott-data-breach-settlement-97534838b650bfc7a9e73a5336b2988e (jeweils zuletzt abgerufen am 1.5.2025).

[110] Siehe nur UK *Information Commissioner's Office* (ICO) Penalty Notice (Case ref: COM0783542) v. 16.10.2020 wegen Verstößen gegen Sec. 155 Data protection Act 2018 durch *British Airways plc*: Hier ist die Geldbuße von vormals 183 Millionen GPB auf 20 Millionen GPB herabgesetzt worden, siehe nur *Tidy*, British Airways fined £20m over data breach, BBC v. 16.10.2020, abrufbar unter: https://www.bbc.com/news/technology-54568784 (zuletzt abgerufen am 1.5.2025).

[111] Zu weiteren spezialgesetzlich geregelten Bereichen statt vieler *Lapp* in: Kipker, Cybersecurity, 2. Aufl. 2023, Kap. 10 Rn. 18 ff.; *Mehrbrey/Schreibauer*, MMR 2016, 75, 81.

me Haftungstatbestand des Art. 82 DSGVO nur auf Datenschutzverstöße in Bezug auf personenbezogene Daten natürlicher Personen Anwendung, wobei durch Art. 5 i.V.m. Art. 24 und Art. 32 DSGVO gerade auch die Unterschreitung des gebotenen IT-Sicherheitsniveaus für die Erfüllung des Haftungstatbestandes relevant werden kann. Denn unter bestimmten Voraussetzungen bürdet der EuGH dem verantwortlichen Unternehmen bzw. Auftragsdatenverarbeiter im Fall eines erfolgreichen Cyber-Angriffs, der zu Datenschutzverstößen führt, gerade die „Beweislast" dafür auf, dass die getroffenen technischen und organisatorischen Cyber-Risikomanagement-Maßnahmen „geeignet" i.S.d. Art. 24 und 32 DSGVO waren.[112] Überdies sieht Art. 82 Abs. 3 DSGVO eine Beweislastumkehr hinsichtlich des Verschuldens vor.[113] Ein Cybervorfall kann nicht nur bei unzureichenden IT-Sicherheitsmaßnahmen zu DSGVO-Verstößen führen, sondern auch im Gefolge des eigentlichen Cyber-Incidents sind haftungsrelevante Vorgänge denkbar, etwa wenn das angegriffene Unternehmen eine unverzügliche Mitteilung an die betroffenen Personen unterlässt, obwohl Art. 33 DSGVO dies gerade bei sensiblen Daten vorschreibt.

Im Gegensatz zu natürlichen Personen kommen – i.d.R. als juristische Personen organisierte – Unternehmen nicht in den Genuss der DSGVO, wenn unternehmensbezogene Daten von einem Cyber-Incident betroffen sind.[114] Hier rücken damit zunächst spezialgesetzliche Tatbestände in den Vordergrund: So ist beispielsweise auch durch die (fahrlässige) Weiterverbreitung von Schad-Code durch den Cyber-Versicherungsnehmer eine fahrlässige Verletzung von Geschäftsgeheimnissen der betroffenen Geschäftskontakte oder außenstehender Dritter denkbar. Hier sieht § 10 GeschGehG einen eigenen Haftungstatbestand vor, der auf Rechtsfolgenseite

---

112 EuGH 14.12.2023 – Rs. C-340/21 (*Natsionalna agentsia za prihodite*) ECLI:EU:C:2023:986 Rn. 24 ff. und 57; EuGH 25.1.2024 – Rs. C-687/21 (*MediaMarktSaturn Hagen-Iserlohn GmbH*) ECLI:EU:C:2024:72 Rn. 36 ff.

113 Dazu zuletzt z.B. LG Heidelberg 31.3.2023 – 7 O 9/22, Rn. 134 (juris). Siehe auch jurisPK-Internetrecht/*Heckmann*, 8. Aufl. 2024, Kap. 9 Rn. 681.

114 Das dürfte sich auch auf die Frage des Schutzgesetzcharakters der DSGVO-Bestimmungen i.R.d. § 823 Abs. 2 BGB auswirken: Insoweit fallen juristische Personen aus dem Schutzbereich dieser Datenschutzbestimmungen heraus, vgl. zur Anwendung nationaler Deliktstatbestände über Art. 82 DSGVO hinaus nur Erwägungsgrund Nr. 146 S. 4 DSGVO sowie zur Schutzgesetzeigenschaft statt vieler MünchKommBGB/Wagner, 9. Aufl. 2024, § 823 BGB Rn. 680.

nicht nur materiellen Schadensersatz, sondern auch eine Entschädigung in Geld für Nichtvermögensschäden wie z.B. Reputationsschäden umfasst.[115]

Darüber hinaus kommt stets eine Haftung aus unerlaubter Handlung und somit insbesondere § 823 BGB in Betracht. Allerdings sind zumindest die infolge eines Cyber-Vorfalls beeinträchtigten Daten als solche nach h.M. keine Sachen i.S.d. § 90 BGB und somit nicht vom Schutzgut „Eigentum" des § 823 Abs. 1 BGB umfasst.[116] Etwas anderes dürfte indes bei der durch einen Cyber-Incident bewirkten Datenlöschung oder Datenveränderung auf im Eigentum des Betroffenen stehenden und klar physisch abgrenzbaren Datenträgern gelten.[117] Die für viele wirtschaftsbezogene Anwendungen immer relevanter werdenden Cloud-Lösungen können damit indes gerade nicht erfasst und deliktisch geschützt werden.[118] Hier spricht viel dafür, Daten als „sonstige Rechte" i.S.d. § 823 Abs. 1 BGB zu begreifen, wobei diese ebenso umstrittene wie komplexe Thematik an dieser Stelle nicht weiter vertieft werden kann.[119] Gleiches gilt für die Frage, ob der Zugang zum Internet und damit auch zu unternehmenseigenen IIoT-Anwendungen in einer zunehmend digitalisierten Wertschöpfungskette nicht ebenfalls ein „sonstiges Recht" darstellen kann.[120] In jedem Fall aber dürfte bei gezielt gegen ein Unternehmen und dessen IT-Infrastruktur gerichteten Cyber-Attacken – etwa mittels Ransomware oder Social-Engineering – die Betriebsbezogenheit zu bejahen sein und damit ein Eingriff in den

---

115 Vgl. § 10 Abs. 2 und Abs. 3 GeschGehG.

116 Dazu statt vieler *Riehm*, VersR 2019, 714, 717 f.; MünchKommBGB/*Wagner*, 9. Aufl. 2024, § 823 BGB Rn. 285 ff.

117 BeckOGK BGB/*Voigt*, 1.7.2024, § 823 BGB Rn. 139. So konsequenterweise für die bei Ransomware-Attacken häufige Verschlüsselung von Daten, die auf einem im Eigentum – und nicht nur im Besitz – des Betroffenen befindlichen Datenträger gespeichert sind, auch *Lesser*, Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken, 2021, S. 32 ff. m.w.N.

118 Statt vieler BeckOGK BGB/*Voigt*, 1.7.2024, § 823 BGB Rn. 139 f.

119 Für die Anerkennung des Rechts an den eigenen Daten bzw. am eigenen Datenbestand i.R.d. § 823 Abs. 1 BGB etwa BeckOGK BGB/*Voigt* 1.7.2024, § 823 BGB Rn. 141 und 187; MünchKommBGB/*Wagner*, 9. Aufl. 2024, § 823 BGB Rn. 384 m.w.N. auch zur Gegenansicht.

120 BGHZ 196, 101 Rn. 17 ff. hat die Vereitelung des Internetzugangs als Vermögensschaden aufgefasst. Will man – etwa mit *Spindler*, JZ 2013, 897, 899 – darüber hinaus das Recht auf Internetzugang als sonstiges Recht i.S.d. § 823 Abs. 1 BGB anerkennen, so müsste dies konsequenterweise auch für IIoT-gestützte Produktions- oder Dienstleistungsprozesse gelten. Kritisch und m.w.N. zu den einzelnen Positionen MünchKommBGB/*Wagner*, 9. Aufl. 2024, § 823 BGB Rn. 386.

eingerichteten und ausgeübten Gewerbebetrieb vorliegen, der ebenfalls von § 823 Abs. 1 BGB erfasst wird.[121] Dies erscheint gerade angesichts der Judikatur des BGH zu unerwünschter digitaler Kommunikation mit Unternehmen als konsequente Fortschreibung dieser Rechtsprechungslinie.[122]

Bei einer (fahrlässigen) Weiterleitung von Schade-Code durch den Cyber-Versicherungsnehmer dürfte der Schwerpunkt der Vorwerfbarkeit zuweilen eher auf einem Unterlassen liegen, beispielsweise weil der Cyber-Versicherungsnehmer keinerlei (branchen)übliche IT-Sicherheitsmaßnahmen ergriffen oder gebotene Update-Intervalle ignoriert hat, wie sie z.B. der BSI-IT-Grundschutz rechtlich unverbindlich definiert. In solchen Konstellationen können den Schädiger durchaus Verkehrssicherungspflichten bezüglich seiner IT-Infrastruktur treffen, weil Dritte – wie Kunden und sonstige Geschäftskontakte – mit dieser üblicherweise in Kontakt kommen und den davon ausgehenden (Cyber-)Gefahren ausgesetzt sind.[123] Gerade gewerbliche IT-Nutzer, die intensiv mit zahlreichen Geschäftskontakten interagieren und dies insbesondere auf digitalem Wege tun, dürften Verkehrssicherungspflichten treffen, Schäden Dritter dadurch zu verhindern, dass sie durch ein angemessenes Cyberrisikomanagement IT-Sicherheitslücken minimieren. Allerdings bestehen Verkehrspflichten als deliktische Sorgfaltspflichten gerade nur zum Schutz der von § 823 Abs. 1 BGB erfassten Rechtsgüter; insoweit gleichen sich dann deliktische Verkehrspflichten und vertragliche Schutzpflichten i.S.d. § 241 Abs. 2 BGB inhaltlich an, wobei letztere sachlich freilich weitergehen können.[124] Dabei wird neben der expliziten gesetzlichen Verankerung branchen- und größenspezifischer IT-Sicherheitsvorgaben, z.B. im NIS-2-, KRITIS- oder DORA-Regime, stets auch auf die Intensität der Verzahnung der IT abzustellen sein: So dürften die Verkehrssicherungspflichten

---

121 Dafür schon *R. Koch*, NJW 2004, 801, 803. Siehe – mit Einschränkungen – auch *Lesser*, Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken, 2021, S. 39 ff.

122 Vgl. zur – freilich lauterkeitsrechtlich relevanten – unerwünschten Zusendung von E-Mails nur BGHZ 214, 204 Rn. 10 ff.; BGH VersR 2014, 1462 Rn. 15 ff. m.w.N.

123 In diesem Sinne *Lesser*, Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken, 2021, S. 162 ff. und 26 sowie schon zuvor *Mehrbrey/Schreibauer*, MMR 2016, 75, 81; *F. Koch*, CR 2009, 485 ff.; *R. Koch*, NJW 2004, 801, 805.

124 Allgemein MünchKommBGB/*Wagner*, 9. Aufl. 2024, § 823 BGB Rn. 498. Vgl. allgemein ferner nur BGH VersR 2023, 66 Rn. 10 ff.; BGH VersR 2021, 787 Rn. 24.

erheblich strenger ausfallen, wenn ein Unternehmen seine IT-Systeme und z.B. digital vernetzte Produktionsanlagen mit der IT-Infrastruktur seiner Zulieferer, Kunden und Dienstleister vernetzt.

Schließlich vermittelt § 823 Abs. 2 BGB i.V.m. unterschiedlichen Schutzgesetzen, wie insbesondere den daten- und IT-infrastrukturbezogenen Straftatbeständen der § 202a, § 202b, § 202c und § 202d StGB sowie der § 303a, § 303b StGB, weiteren deliktsrechtlichen Schutz unternehmenseigener Daten und IT-Infrastruktur u.a. gegenüber dem Ausspähen, Abfangen und Verändern von Daten sowie der Datenhehlerei und der Computersabotage.

II. Internationale Zuständigkeit für Cyber-Haftpflichtstreitigkeiten

Aus der hier gewählten Perspektive eines deutschen Gerichts richtet sich die internationale Zuständigkeit für individuelle Haftpflichtansprüche Dritter gegen den Angegriffenen vorrangig nach Brüssel Ia-VO (**dazu unter 1**).[125] Dies setzt allerdings grundsätzlich[126] einen Beklagtenwohnsitz – bzw. im Fall eines als juristische Person oder sonstiger Verband organisierten Unternehmens: eine Haupt- oder sonstige Niederlassung – in der EU voraus.[127] Nach dem in Art. 4 Abs. 1 Brüssel Ia-VO kodifizierten allgemeinen Grundsatz *actor sequitur forum rei* sind für Klagen stets die Gerichte am (Wohn)Sitz des Beklagten in einem EU-Mitgliedstaat international zuständig. Ist der Beklagte in einem der EFTA-Staaten ansässig, kommt das revi-

[125] Anders als bei einer – überhaupt nur im Fall der klaren „attribution" und Identifikation möglichen – direkten Inanspruchnahme eines (halb)staatlichen Cyber-Angreifers stellt sich in der hiesigen Konstellation die Frage nicht, ob die Brüssel Ia-VO womöglich nach ihrem Art. 1 Abs. 1 S. 2 unanwendbar ist, weil ein (halb)staatlicher Cyber-Angriff als Hoheitsakt anzusehen und die „die Haftung des Staates für Handlungen oder Unterlassungen im Rahmen der Ausübung hoheitlicher Rechte (*acta iure imperii*)" entsprechend ausgenommen ist, vgl. hierzu sowie zur Parallelfrage i.R.d. Art. 1 Abs. 1 S. 2 Rom II-VO sogleich unter II 1 a).

[126] Die Brüssel Ia-VO ist nach Art. 6 Abs. 1 darüber hinaus auf Beklagte ohne Sitz in den EU-Mitgliedstaaten anwendbar, wenn eine ausschließliche Zuständigkeit nach Art. 24 Brüssel Ia-VO oder eine den Anforderungen des Art. 25 Brüssel Ia-VO genügende Gerichtsstandsvereinbarung besteht.

[127] Vgl. Art. 62 f. Brüssel Ia-VO.

dierte LugÜ 2007[128] zur Anwendung. Bei einem Beklagtenwohnsitz in einem sonstigen Drittstaat folgt die internationale Zuständigkeit – vorbehaltlich staatsvertraglicher Abkommen – dann nach dem Grundsatz der Doppelfunktionalität aus der analogen Anwendung der Bestimmungen zur örtlichen Zuständigkeit, wie insbesondere § 12, § 32 ZPO.[129]

Hat der Angegriffene – etwa als europaweit tätige Fluglinie, Hotelkette oder Online-Händler – vor allem natürliche Personen als Kunden und erbeutet ein Cyber-Angreifer solche Kundendaten, könnten den natürlichen Personen Haftpflichtansprüche wegen Datenschutzverletzungen zustehen, die einen besonderen Gerichtsstand nach Art. 79 DSGVO eröffnen (**hierzu unter 2**). Je zahlreicher die Anspruchsteller und je überschaubarer die individuelle Anspruchshöhe ausfällt, desto attraktiver mag in solchen Konstellationen eine (grenzüberschreitende) kollektive Anspruchsdurchsetzung infolge des Cyber-Incidents erscheinen (**dazu unter 3**).

1. Gerichtsstände nach der Brüssel Ia-VO für die Inanspruchnahme des Angegriffenen durch geschädigte Dritte

Der sachliche Anwendungsbereich der Brüssel Ia-VO wird durch ihren Art. 1 abgesteckt, wobei dort prominent sog. *acta iure imperii* nach Art. 1 Abs. 1 S. 2 Brüssel Ia-VO ausgeklammert werden. Dies führt zur allgemeinen Frage, ob (halb)staatliche Cyber-Angriffe unter diesen Ausschlusstatbestand fallen (**dazu unter a**) und welche Folgen das für die Cyber-Haftpflicht bei bloß fahrlässiger Weiterverbreitung von Schad-Code hat. Schädigt der Angegriffene seine Geschäftskontakte oder sonstige Dritte, kann seine Haftpflicht – vorbehaltlich einer Gerichtsstandsvereinbarung nach Art. 25 Brüssel Ia-VO und der jeweiligen Ausgestaltung der Rechtsbeziehung – im

[128] Luganer Übereinkommen über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen v. 30.10.2007, ABl. 2007 L 339, 3. Zu den Parallelen und Unterschieden zur Brüssel Ia-VO statt vieler Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Vorbemerkung Brüssel Ia-VO Rn. 12 f.

[129] Vgl. nur BGH NJW 1997, 2245; BGH NJW 2016, 3369.

Vertragsgerichtsstand nach Art. 7 Nr. 1 Brüssel Ia-VO (**dazu unter b**) oder im Deliktsgerichtsstand nach Art. 7 Nr. 2 Brüssel Ia-VO (**hierzu unter c**) geltend gemacht werden. Weitere Gerichtsstände mögen im Einzelfall sodann insbesondere Art. 7 Nr. 5 sowie Art. 8 Nr. 1 Brüssel Ia-VO eröffnen (**dazu unter d**).

a) Haftung im Gefolge (halb)staatlicher Cyber-Attacken: acta iure imperii i.S.d. Art. 1 Abs. 1 S. 2 Brüssel Ia-VO ?

Bereits auf Ebene der gerichtlichen Durchsetzung der Haftpflicht für einen Cyber-Incident könnte der Anspruchsgegner versuchen, dem Anspruchssteller die Gerichtsstände der Brüssel Ia-VO mit dem Argument aus der Hand zu schlagen, dass die schadensursächliche Malware und/oder ihre ursprüngliche Verbreitung (halb)staatlichen Ursprungs seien. Denn ausweislich ihres Art. 1 Abs. 1 ist die Brüssel Ia-VO nur auf „Zivil- und Handelssachen“ anzuwenden. Dieser Begriff ist nach ständiger Rechtsprechung des EuGH unionsrechtlich-autonom auszulegen[130] und grenzt den Anwendungsbereich insbesondere mit Blick auf öffentlich-rechtliche Streitigkeiten ein, die in Art. 1 Abs. 1 S. 2 Brüssel Ia-VO näher umrissen werden. Ausgenommen werden insbesondere Steuer- und Zollsachen sowie verwaltungsrechtliche Angelegenheiten oder die Haftung des Staates für Handlungen oder Unterlassungen im Rahmen der Ausübung hoheitlicher Rechte (*acta iure imperii*).

Dies birgt potentiell Herausforderungen für die Zuständigkeit für Haftpflichtklagen infolge von Cyber-Angriffen: Schließlich wird manchem Schad-Code und mancher Attacke nachgesagt, dass sie einen (halb)staatlichen Ursprung haben oder zumindest von (halb) staatlichen Akteuren ersonnen und durchgeführt worden sind. Zu denken ist etwa an die sich selbst weiterverbreitende sog. „*StuxNet*“-Malware sowie in jüngerer Zeit etwa den „*Not Petya*“-Schadcode: Ersterer wurde als staatliches Angriffswerkzeug gegen

[130] Grundlegend EuGH 14.10.1976 – Rs. 29/76 (*Eurocontrol*) ECLI:EU:C:1976:137 Rn. 3. Siehe ferner nur EuGH 16.7.2020 – Rs. C-73/19 (*Belgische Staat*) ECLI:EU:C:2020:568 Rn. 33.

den Iran,[131] letzterer als ein Instrument der „Cyber-Kriegsführung“ Russlands gegen die Ukraine bezeichnet.[132] Zwar hat „*Not Petya*“ im Kontext von Kriegsausschlussklauseln in Versicherungsverträgen bereits US-amerikanische Gerichte beschäftigt, die jeweils dazu neigten, „Krieg“ i.S.d. Ausschlussklauseln zu verneinen.[133] Abgesehen davon, dass diese Verfahren mit Vergleichen endeten,[134] stand hier jeweils die Interpretation individueller versicherungsvertraglicher Formulierungen im Zentrum, wobei eine Mehrheit der bundesstaatlichen Gerichte in den USA ebenfalls auf die Perspektive eines durchschnittlichen Versicherungsnehmers abstellt.[135] Bereits dieser Auslegungsmaßstab ist indes deutlich von der Auslegung und Anwendung des Art. 1 Abs. 1 S. 2 Brüssel Ia-VO zu unterscheiden, weil die in dieser Norm verwendeten Begrifflichkeiten unionsrechtlich-autonom auszulegen sind.[136] Das beginnt schon mit der Kategorie der *acta iure imperii*, also der Ausübung genuiner Hoheitsrechte durch den Staat: Dieser Begriff muss ebenso wie die damit verbundene „Haftung des Staates für Handlungen oder Unterlassungen“ unionsrechtlich einheitlich und vor dem Hintergrund der EuGH-Judikatur interpretiert werden.[137] Der EuGH fasst hierunter u.a. Schadensersatzklagen privater gegen staatliche Akteure infolge

---

131 Vgl. nur *Markoff*, A Silent Attack, but Not a Subtle One, New York Times v. 26.9.2010, abrufbar unter: https://www.nytimes.com/2010/09/27/technology/27virus.html (zuletzt abgerufen am 1.5.2025).

132 Siehe nur *U.S. Department of Justice*, Press Release v. 19.10.2020: „Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace“, abrufbar unter: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (zuletzt abgerufen am 1.5.2025).

133 Vgl. *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co*., No. 2018-L-011008 (Ill. Cir. Ct.); *Merck & Co. v. ACE Am. Ins. Co.* 475 N.J. Super. 420 (App. Div. 2023) 293 A.3d 535; *Merck & Co., Inc. v. Ace Am. Ins. Co.*, No. UNN-L-002682-18 (N.J. Super. Ct. Law Div. 6.12.2021).

134 Vgl. zum Vergleich der Parteien v. 3.1.2024 *Merck Co., Inc. v. ACE Am. Ins. Co., N.J*., No. A-62/63-22 nur *Ebert*, Merck $1.4 Billion Cyberhack Settlement Ends 'Warlike' Act Claim, Bloomberg Law v. 4.1.2024, abrufbar unter: https://news.bloomberglaw.com/litigation/merck-1-4-billion-cyberhack-settlement-ends-warlike-act-claim. Durch Vergleich beigelegt worden ist auch *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co.*, No. 2018-L-011008 (Ill. Cir. Ct.), vgl. dazu nur *Adriano*, Zurich, Mondelez settle longstanding lawsuit over $100 million claim, abrufbar unter: https://www.insurancebusinessmag.com/us/news/cyber/zurich-mondelez-settle-longstanding-lawsuit-over-100-million-claim-426741.aspx (jeweils zuletzt abgerufen am 1.5.2025).

135 Vgl. nur m.w.N. *Merck & Co. v. ACE Am. Ins. Co.* 475 N.J. Super. 420 (App. Div. 2023) 293 A.3d 535.

136 Vgl. nur EuGH 16.7.2020 – Rs. C-73/19 (*Belgische Staat*) ECLI:EU:C:2020:568 Rn. 33 ff.

137 Vgl. nur EuGH 15.2.2007 – Rs. C-292/05 (*Lechouritou u.a./Bundesrepublik Deutschland*) Slg. 2007, I-1519 Rn. 27 ff.

von Kriegshandlungen: Kriegsführung durch den Einsatz von Streitkräften sei ein „typischer Ausdruck staatlicher Souveränität“ und zähle deshalb eindeutig zu den *acta iure imperii*.[138] Dabei soll es i.R.d. Art. 1 Abs. 1 S. 2 Brüssel Ia-VO grundsätzlich schon genügen, dass der streitgegenständliche Anspruch seinen Ursprung in einem genuin hoheitlichen Akt hat.[139]

Mit Blick auf die hier interessierenden Cyber-Attacken ist die Lage indes zumeist komplex und undurchsichtig: Denn zum einen sind die Cyber-Angreifer in der Regel allenfalls staatsnah, staatlich gesteuert oder (halb)staatlich organisiert, ohne selbst ein Organ oder eine Behörde des betreffenden Staates zu sein. Auch wenn dies freilich nicht ausnahmslos gilt, bleibt jedenfalls der Beweis staatlicher Urheberschaft schwierig.[140] Zum anderen ist eine Cyber-Attacke womöglich nicht ohne Weiteres unter den unionsrechtlichen Begriff der Kriegshandlung als „genuine“ Erscheinungsform der *acta iure imperii* zu fassen: Der EuGH hat sich in seiner bisherigen Rechtsprechung nur mit traditionellen, durch Waffengewalt vorgetragenen Kriegshandlungen auseinandergesetzt; ob hingegen auch ohne physische (Waffen)Gewalt ausgetragene „Cyber-Kriege“ für die Zwecke des Art. 1 Abs. 1 Brüssel Ia-VO einem konventionellen Krieg gleichgesetzt und damit als *acta iure imperii* vom Anwendungsbereich der Verordnung ausgenommen werden können, erscheint zweifelhaft.

Der EuGH differenziert zunächst anhand der – rechtlichen und faktischen – Möglichkeit eines Privaten, bestimmte Handlungen vorzunehmen: Können die Instrumente und Befugnisse „nicht von Privatpersonen ausgeübt werden“, sondern stehen sie nur staatlichen Hoheitsträgern als „Sonderrechte“ zu, so liegt ein Hoheitsakt i.S.d.

---

138 EuGH 15.2.2007 – Rs. C-292/05 (*Lechouritou u.a./Bundesrepublik Deutschland*) Slg. 2007, I-1519 Rn. 37. Eingehend dazu *Dutta*, ZZPInt 11 (2006), 208 ff.

139 Z.B. EuGH 15.2.2007 – Rs. C-292/05 (*Lechouritou u.a./Bundesrepublik Deutschland*) Slg. 2007, I-1519 Rn. 41. Siehe auch EuGH 14.10.1976 – Rs. 29/76 (*Eurocontrol*) ECLI:EU:C:1976:137 Rn. 3 ff. Dazu Geimer/Schütze/*Geimer*, EuZivilVerfR, 4. Aufl. 2020, Art. 1 EuGVVO Rn. 1c.

140 Dazu im Kontext jüngerer Ausschlüsse für Cyber-Attacken im Rahmen von „Krieg“ und „Cyber-Operationen“ unten F. Siehe zu staatlichen „ramsomware“-Attacken auch *Lyngaas*, Half of North Korean missile program funded by cyberattacks and crypto theft, White House says, CNN v. 10.5.2023, abrufbar unter: https://edition.cnn.com/2023/05/10/politics/north-korean-missile-program-cyberattacks/index.html (zuletzt abgerufen am 1.5.2025).

Art. 1 Abs. 1 Brüssel Ia-VO nahe.[141] Nimmt man dies als Ausgangspunkt, so sind Cyber-Attacken, die auf lediglich staatlich tolerierte oder staatlich unterstützte Akteure zurückgehen, keine *acta iure imperii*, weil hier keine rechtlich oder auch tatsächlich nur von staatlichen Stellen auszuübenden Befugnisse, sondern üblicherweise auch für Private handhabbare Schadprogramme genutzt werden. Darüber hinaus postuliert der EuGH in seiner bisherigen Judikatur zu „Kriegen" als *acta iure imperii* zum einen wohl noch unmittelbar physisch vermittelten Zwang und damit militärische Gewalt durch „Operationen von Streitkräften".[142] Zum anderen will der Gerichtshof konventionelle Kriegshandlungen gerade deswegen als „typische(n) Ausdruck staatlicher Souveränität" behandeln, weil solche Maßnahmen „von den zuständigen staatlichen Stellen einseitig und zwingend beschlossen werden und sich als mit der Außen- und Verteidigungspolitik von Staaten untrennbar verknüpft zeigen".[143] Zumindest mit dieser dezisionistischen Komponente lässt der EuGH durchaus Raum für andere als mit physisch vermittelter Gewalt geführte „Cyber-Kriege", soweit sie durch expliziten Beschluss der staatlichen Stelle zu Instrumenten der Außen- und Sicherheitspolitik werden.

Führt man diese Anforderungen zusammen und subsumiert die bisherigen Erscheinungsformen von Cyber-Angriffen darunter, so ergibt sich folgendes Bild: Als *acta iure imperii* dürften nur Cyber-Attacken gelten, die als Teil eines konventionellen, mit militärischen Gewaltmitteln geführten Krieges durch staatliche Behörden oder sonstige Hoheitsträger selbst angeordnet und ausgeführt werden. Anders gewendet sind also auch die „Beimischungen" von Cyber-Attacken zu einem konventionell geführten Krieg selbst Teil der Kriegshandlungen und damit *acta iure imperii* i.S.d. Art. 1 Abs. 1 Brüssel Ia-VO. Dagegen dürften staatlich nur tolerierte oder – z.B. durch die Nicht-Pönalisierung von Angriffen auf „westliche" Ziele – durch die staatliche Rechtsetzung inzentivierte Cyber-Attacken

141 EuGH 22.12.2022 – Rs. C-98/22 (*Eurelec*) ECLI:EU:C:2022:1032 Rn. 26.
142 EuGH 15.2.2007 – Rs. C-292/05 (*Lechouritou u.a./Bundesrepublik Deutschland*) Slg. 2007, I-1519 Rn. 37.
143 EuGH 15.2.2007 – Rs. C-292/05 (*Lechouritou u.a./Bundesrepublik Deutschland*) Slg. 2007, I-1519 Rn. 37.

durch private Akteure nicht unter Art. 1 Abs. 1 Brüssel Ia-VO fallen, weil diese Angreifer keine genuinen Hoheitsrechte ausüben, sondern sich – wie gewöhnliche Kriminelle auch – Schadprogrammen wie z.B. Ransomware bedienen, die privaten Akteuren meist über das sog. „Dark Net" gleichermaßen zur Verfügung stehen. Hier wird man im Lichte der EuGH-Rechtsprechung deshalb kaum davon sprechen können, dass ein solcher Beklagter „Befugnisse ausübt, die von den im Verhältnis zwischen Privatpersonen geltenden allgemeinen Regeln abweichen."[144]

Selbst wenn man den Kreis des hoheitlichen Handelns bei Cyber-Attacken deutlich weiter ziehen und – mit teils beachtlichen Argumenten – z.B. auch die *NotPetya*-Malware[145] und jüngere Malware-Attacken, u.a. auf ein Düsseldorfer Krankenhaus, durch die „DoppelPaymer"- bzw. „Indrik Spider"-Gruppe,[146] einbeziehen möchte, wird sich hier zum einen ein ähnliches Problem stellen, wie es auch bei den – nach wie vor umstrittenen – Ansätzen zum Ausschluss von „Krieg" und „Cyber-Operationen" im Rahmen überkommener und neuer (Kriegs)Ausschlussklauseln auftaucht: Die Zuordnung („*attribution*") der Cyber-Attacke zu einem Staat und dessen Organen ist mit einem erheblichen forensischen (Zeit)Aufwand verbunden, und der Vollbeweis dürfte – trotz der Prüfung der internationalen Zuständigkeit von Amts wegen in jedem Rechtszug –[147] allen-

144 Vgl. nur EuGH 16.7.2020 – Rs. C-73/19 (*Movic*) ECLI:EU:C:2020:568, Rn. 36; EuGH 22.12.2022 – Rs. C-98/22 (*Eurelec*) ECLI:EU:C:2022:1032 Rn. 22.

145 Siehe nur *U.S. Department of Justice*, Press Release v. 19.10.2020: „Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace", abrufbar unter: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and sowie ferner U.S. District Court for the Western District of Pennsylvania, CriminalNo. 20-316 v. 15.10.2020 (*United States of America v. Yuriy Sergeyevich Andrienko and others*), abrufbar unter: https://www.justice.gov/d9/press-releases/attachments/2020/10/19/2020_10_19_unsealed _indictment_0.pdf (jeweils zuletzt abgerufen am 1.5.2025).

146 Vgl. *Burger*, Die Spur führt nach Russland, FAZ v. 6.3.2023: „NRW-Innenminister Herbert Reul (CDU) äußerte, auch wenn viele Angriffe der Gruppe dazu dienten, sich selbst zu bereichern, sehe man auch Verbindungen zum russischen Inlandsgeheimdienst FSB und der Söldnertruppe Wagner. Das ergebe sich aus öffentlich zugänglichen Quellen. „Daher liegt die Vermutung nahe, dass die Attacken ‚mindestens staatlich geduldet' werden", so Reul. „Gleichzeitig ist nicht auszuschließen, dass die abgeschöpften Daten und Gelder auch für staatliche Zwecke genutzt werden."

147 Siehe nur BGH EuZW 2022, 622 Rn. 8; BGH NJOZ 2011, 1278 Rn. 15 sowie statt vieler MünchKommZPO/*Patzina*, 6. Aufl. 2020, § 12 ZPO Rn. 69.

falls in Ausnahmefällen überhaupt zu führen sein.[148] Vor allem aber wird bei der Inanspruchnahme von Geschäftspartnern oder sonstigen Dritten, die z.B. fahrlässig Schad-Code an ihre Kunden weiterverbreitet haben, keine Rede davon sein können, dass diese privaten Akteure selbst in irgendeiner Form hoheitliche Befugnisse i.S.d. Art. 1 Abs. 1 S. 1 Brüssel Ia-VO ausüben. Anders gewendet, ist also beispielsweise die mangelnde Cyber-Sicherheit in einem Unternehmen oder das fahrlässige Weiterverbreiten von Schad-Code – und mag letzterer auch staatlichen Ursprungs sein – niemals „typischer Ausdruck staatlicher Souveränität",[149] sondern die Schädiger handeln und haften gerade nach den „im Verhältnis zwischen Privatpersonen geltenden allgemeinen Regeln".[150] Damit sind für die Cyber-Haftpflicht unter Privaten stets die Gerichtsstände der Brüssel Ia-VO eröffnet.

b) Zuständigkeit für Haftpflichtansprüche in Vertragsbeziehungen: Art. 25 und Art. 7 Nr. 1 Brüssel Ia-VO

Wird der Beklagte im Rahmen einer bereits bestehenden vertraglichen Beziehung haftpflichtig, kann die internationale Zuständigkeit vorrangig durch eine Gerichtsstandsvereinbarung nach Art. 25 Brüssel Ia-VO begründet werden.[151] Die im Vertrag enthaltene Gerichtsstandsvereinbarung kann dabei neben vertraglichen – je nach Formulierung, Auslegung anhand des Parteiwillens und je nach anwendbarem Recht – auch etwaig konkurrierende außervertragliche Haftpflichtansprüche erfassen.[152] Durch eine Gerichtsstandsverein-

---

148 Siehe mit Blick auf die Umsetzung der Vorgaben in LMA 5564 a, b bis LMA 5567a, b sowie zur Lösung in den AVB-Cyber 2024 eingehend unter F. Den besonders großen (Zeit)Aufwand illustriert auch der Angriff auf das deutsche Bundesamt für Kartographie und Geodäsie der – trotz erheblicher Ermittlungsressourcen – erst nach drei Jahren (staatsnahen) chinesischen Akteuren zugeordnet werden konnte, vgl. BMI Pressemitteilung v. 31.7.2024, abrufbar unter: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/cyberangriff-bkg.html (zuletzt abgerufen am 1.5.2025).

149 EuGH 15. 2. 2007 – Rs. C-292/05 (*Lechouritou u.a./Bundesrepublik Deutschland*) Slg. 2007, I-1519 Rn. 37. Eingehend dazu *Dutta*, ZZPInt 11 (2006), 208 ff.

150 Vgl. nur EuGH 16.7.2020 – Rs. C-73/19 (*Movic*) ECLI:EU:C:2020:568, Rn. 36; EuGH 22.12.2022 – Rs. C-98/22 (*Eurelec*) ECLI:EU:C:2022:1032 Rn. 22.

151 Zu den Voraussetzungen und Einschränkungen von Gerichtsstandsvereinbarungen statt aller Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 25 EuGVVO Rn. 1 ff.

152 OLG Frankfurt a. M. BeckRS 2015, 14693. Statt vieler m.w.N. MünchKommZPO/*Gottwald*, 6. Aufl. 2022, Art. 25 Brüssel Ia-VO Rn. 64 f.; Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 25 Brüssel Ia-VO Rn. 15.

barung können Beklagte stets gemäß Art. 25 Brüssel Ia-VO auch ungeachtet ihres (Wohn)Sitzes inner- oder außerhalb der EU-Mitgliedstaaten vor dem vereinbarten Gericht gerichtspflichtig werden. Fehlt eine solche Vereinbarung oder ist sie unwirksam, ist zunächst der besondere Vertragsgerichtsstand nach Art. 7 Nr. 1 in den Blick zu nehmen, zumal dieser nach ständiger Rechtsprechung des EuGH grundsätzlich Vorrang vor dem Deliktsgerichtsstand nach Art. 7 Nr. 2 Brüssel Ia-VO hat.[153]

Gemäß Art. 7 Nr. 1 Brüssel Ia-VO ist für Ansprüche aus einem Vertrag das Gericht des EU-Mitgliedstaates international zuständig, in dem die vertragliche Verpflichtung erfüllt worden ist oder zu erfüllen wäre. Der Vertragsbegriff ist unionsrechtlich-autonom auszulegen und damit von den Kategorien des nationalen Rechts zu entkoppeln: Erforderlich und zugleich ausreichend für einen Vertrag oder Ansprüche aus einem solchen i.S.d. Art. 7 Nr. 1 Brüssel Ia-VO ist stets eine „von einer Partei gegenüber einer anderen freiwillig eingegangene Verpflichtung".[154] Der Vertragsgerichtsstand kann jedenfalls dann relevant werden, wenn anlässlich der vertraglich geschuldeten Leistungserbringung ein Schaden entsteht. Als Beispiel mag ein Unternehmen dienen, dass Verpackungsmaschinen herstellt und eine IIoT-gesteuerte Fernwartung der Maschinen anbietet. Werden nun die Kunden aufgrund fehlerhafter Programmierung der Fernwartungssoftware Opfer von Hackerangriffen, kann darin – grundsätzlich – eine Schlechtleistung unter dem (Maschinenwartungs)Vertrag liegen,[155] die den Vertragsgerichtsstand nach Art. 7 Nr. 1 Brüssel Ia-VO begründet. In solchen Konstellationen ist allerdings nach dem Verhältnis von Vertrags- und Deliktsgerichtsstand zu fragen.[156] Gerade bei Haftpflichtansprüchen hat der EuGH

---

153 Siehe nur EuGH 3.3.2014 – Rs. C-548/12 (*Brogsitter*) ECLI:EU:C:2014:148 Rn. 18 ff.; EuGH 10.9.2015 – Rs. C-47/14 (*Holterman Ferho Exploitatie*) ECLI:EU:C:2015:574 Rn. 70 f.

154 Vgl. nur EuGH 17.6.1992 – Rs. C-26/91 (*Handte*) Slg. 1992, I-3967 Rn. 15; EuGH 27.10.1998 – Rs. C-51/97 (*Réunion européenne*) Slg. 1998, I-6511 Rn. 17; EuGH 18.7.2013 – Rs. C-147/12 (*ÖFAB*) ECLI:EU:C:2013:490 Rn. 33; EuGH 11.11.2020 – Rs. C-433/19 (*Ellmes Property Services*) ECLI:EU:C:2020:900 Rn. 35 ff.

155 Auf Deckungsebene ist üblicherweise i.R.d. Cyber-Haftpflichtbausteins ein Ausschluss für Erfüllungsansprüche und deren Derivate vorgesehen: Ausgeschlossen wäre nach A3-2 lit. a AVB Cyber 2024 insbesondere der Schadensersatz statt der Leistung. Je nach Fallgestaltung mag indes eine Nebenpflichtverletzung i.S.d. § 241 Abs. 2 BGB vorliegen.

156 Dazu zuletzt eingehend etwa *Junker*, FS Schack, 2022, 653 ff.

hier zur Abgrenzung durchaus unterschiedliche Ansätze verfolgt: So sollte nach der *Brogsitter*-Entscheidung der vorrangige Vertragsgerichtsstand bereits dann eröffnet sein, wenn die Auslegung der vertraglichen Verpflichtungen unerlässlich erscheint, um zu bestimmen, ob ein Verhalten rechtmäßig oder widerrechtlich ist.[157] Von dieser Linie ist der Gerichtshof in seiner *Wikingerhof*-Entscheidung abgewichen und fragt nunmehr, ob der Vertrag hinweggedacht werden könne, ohne dass die Haftung des Beklagten entfiele.[158] In der Praxis dürfte bei Haftpflichtansprüchen infolge von Cyber-Vorfällen schon aufgrund dieser vergleichsweise restriktiven Handhabung des Vertragsgerichtsstands durch den EuGH nun der Deliktsgerichtsstand nach Art. 7 Nr. 2 Brüssel Ia-VO weitaus relevanter sein.[159] Sach- und parteiinteressengerechte Anwendungsfelder verbleiben freilich dort, wo die Parteien das Daten- bzw. Geschäftsgeheimnisschutz- und/oder IT-Sicherheitsniveau zum Gegenstand von – im Vergleich zu etwaigen gesetzlichen Vorgaben strengeren – vertraglichen Abreden gemacht haben.[160] Auf Deckungsseite wäre dann freilich die Interaktion von A1-17.11, A3-1, A3-2, A3-4.3 und insbesondere A3-3 AVB Cyber 2024 zu potentiell haftungserweiternden vertraglichen Abreden der Parteien zu beachten.

c) Deliktsgerichtsstand nach Art. 7 Nr. 2 Brüssel Ia-VO

Für Klagen, mit denen ein außervertraglicher Haftpflichtanspruch aus „unerlaubter Handlung" geltend gemacht wird, begründet Art. 7 Nr. 2 Brüssel Ia-VO die Zuständigkeit der Gerichte am „Ort des

---

157 Vgl. EuGH 3.3.2014 – Rs. C-548/12 (*Brogsitter*) ECLI:EU:C:2014:148 Rn. 18 ff. Vgl. auch OLG Köln ZVertriebsR 2016, 202.

158 Vgl. EuGH 24.11.2020 – Rs. C-59/19 (*Wikingerhof*) ECLI:EU:C:2020:950 Rn. 33 und dazu näher *Wurmnest*, IPRax 2021, 340, 343; *Rieländer*, RIW 2021, 103, 110.

159 Vgl. erneut EuGH 24.11.2020 – Rs. C-59/19 (*Wikingerhof*) ECLI:EU:C:2020:950 Rn. 33. Vgl. auch BGH VersR 2022, 122 Rn. 15 ff.; BGH NJW 2024, 514 Rn. 17.

160 Vgl. erneut auch EuGH 3.3.2014 – Rs. C-548/12 (*Brogsitter*) ECLI:EU:C:2014:148 Rn. 24 f.; EuGH 24.11.2020 – Rs. C-59/19 (*Wikingerhof*) ECLI:EU:C:2020:950 Rn. 33. Dazu treffend auch BGH NJW 2024, 514 Rn. 17: „Eine Vertragsbeziehung zwischen den Parteien schließt die Anwendbarkeit von Art. 7 Nr. 2 EuGVVO … indessen nicht aus. Beruft sich der Kl. in einem solchen Fall auf die Regeln der Haftung aus unerlaubter Handlung … und erscheint es nicht unerlässlich, den Inhalt des mit dem Bekl. geschlossenen Vertrags zu prüfen, um zu beurteilen, ob das diesem vorgeworfene Verhalten rechtmäßig oder rechtswidrig ist, da diese Verpflichtung unabhängig von diesem Vertrag besteht, so bildet eine unerlaubte Handlung … den Gegenstand der Klage iSv Art. 7 Nr. 2 EuGVVO."

schädigenden Ereignisses“.[161] Nach ständiger Rechtsprechung des EuGH ist darunter sowohl der Ort des Schadenseintritts (*Erfolgsort*) als auch der Ort des ursächlichen Handelns oder Unterlassens (*Handlungsort*) zu verstehen.[162] Dieser Ansatz wird auch als „Ubiquitätsprinzip“ bezeichnet, weil der Kläger im Fall des Auseinanderfallens von Handlungs- und Erfolgsort bei sogenannten Streu- oder Distanzdelikten die Wahl zwischen den Gerichtsständen hat.[163] Ein Erfolgsort wird dann häufig am (Wohn)Sitz des Geschädigten liegen und damit einen Klägergerichtsstand begründen.[164] Demgegenüber deckt sich der Handlungsort oftmals mit dem allgemeinen Gerichtsstand des Beklagten.[165]

Bei potentiell weltumspannenden Streudelikten wie Cyber-Attacken ergibt sich mit Blick auf die Kognitionsbefugnis des international nach Art. 7 Nr. 2 Brüssel Ia-VO zuständigen Gerichts allerdings eine Besonderheit: Am Gerichtsstand des Handlungsortes soll der Kläger nach Auffassung des EuGH nämlich seinen gesamten Schaden einklagen können, wohingegen das Gericht des jeweiligen Mitgliedstaats, in dem ein Erfolgsort liegt, grundsätzlich nur für den dort lokalisierten Schaden international zuständig sei.[166] Der EuGH gesteht dem Erfolgsortgericht in der Regel nur eine eingeschränkte Kognitionsbefugnis zu, was bei Streuschäden durch einen Cyber-Vorfall in mehreren Mitgliedsstaaten zu einer komplizierten Mosaik-Betrachtung zwingt: Der geschädigte Kläger muss dann grundsätzlich mehrere Verfahren in unterschiedlichen Staaten führen, was nicht nur einen höheren Verfahrens- und Kostenaufwand, sondern auch widersprüchliche Entscheidungen zur Folge haben kann.[167]

---

[161] Siehe zum auch insoweit stets unionsrechtlich-autonomen Begriffsverständnis z.B. EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 25; EuGH 10.9.2015 – Rs. C-47/14 (*Holterman Ferho Exploitatie*) ECLI:EU:C:2015:574 Rn. 66 ff.

[162] Grundlegend EuGH 30.11.1976 – Rs. 21/76 (*Mines de potasse d'Alsace*) ECLI:EU:C:1976:166 Rn. 24 f.

[163] Vgl. erneut EuGH 30.11.1976 – Rs. 21/76 (*Mines de potasse d'Alsace*) ECLI:EU:C:1976:166 Rn. 24 f.

[164] Vgl. EuGH 28.1.2015 – Rs. C-375/13 (*Kolassa*) ECLI:EU:C:2015:37 Rn. 50 ff.

[165] Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 7 Brüssel Ia-VO Rn. 19.

[166] Vgl. EuGH 7.3.1995 – Rs. C-68/93 (*Shevill*) ECLI:EU:C:1995:61 Rn. 33.

[167] Zur sogenannten Mosaiktheorie bei Persönlichkeitsrechtsverletzungen durch die Medien grundlegend EuGH 7.3.1995 – Rs. C-68/93 (*Shevill*) ECLI:EU:C:1995:61 Rn. 33. Siehe zur Kritik an diesem Ansatz eingehend statt vieler *Lutzi*, Private International Law Online (2020), Rn. 4.72–4.83.

Der EuGH hält an diesem Ansatz jedoch auch für im Cyber-Space begangene Delikte grundsätzlich fest,[168] weshalb über den Handlungsortgerichtsstand (**dazu unter aa**) hinaus gerade im Fall der Cyber-Haftpflicht zu fragen ist, ob unter bestimmten Voraussetzungen eine umfassende Zuständigkeit des Erfolgsortgerichtsstands begründet werden kann (**dazu unter bb**).

aa) Handlungsort und Cyberhaftpflicht

Der Handlungsort i.S.d. Art. 7 Nr. 2 Brüssel Ia-VO befindet sich grundsätzlich dort, wo das für den Schaden ursächliche Geschehen stattgefunden hat.[169] Das ist der Ort, an dem der Schädiger entweder aktiv die schadensstiftende Handlung vornimmt[170] oder, im Fall eines Unterlassens, der Ort, an dem der Schädiger in tatbestandsmäßiger Weise die gebotene Handlung unterlässt.[171] Mit Blick auf den Handlungsort bei Cyberdelikten und -angriffen gilt im Ausgangspunkt Folgendes: Bei aktiver Verbreitung von Schad-Code ist der Handlungsort grundsätzlich der „Absendeort", also z.B. der Ort des Einspeisens einer Malware.[172] Das dürfte auch auf die unbeabsichtigte (fahrlässige) Weiterverbreitung von Schad-Code zutreffen: Nimmt der Geschädigte beispielsweise einen mit ihm in Geschäftsverbindung stehenden Schädiger in Anspruch, weil dieser eine Malware z.B. per E-Mail oder aber mittels eines Updates für die von ihm gestellte Fernwartungssoftware versehentlich weiterverbreitet hat, so liegt der Handlungsort am Sitz des Schädigers, der die

---

168 Siehe aus der ständigen Rechtsprechung nur EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 42 f.; EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 31; EuGH 17.6.2021 – Rs. C-800/19 (*Mittelbayerischer Verlag*) ECLI:EU:C:2021:489 Rn. 24 ff.; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv*) ECLI:EU:C:2021:1036 Rn. 24 ff. Vgl. auch EuGH 22.1.2015 – Rs. C-441/13 (*Hejduk*) ECLI:EU:C:2015:28 Rn. 38.

169 EuGH 9.7.2020 – Rs. C-343/19 (*VKI/Volkswagen AG*) ECLI:EU:C:2020:534 Rn. 23 f.

170 Statt vieler Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 7 Brüssel Ia-VO Rn. 19a.

171 EuGH 18.7.2013 – Rs. C-147/12 (*ÖFAB*) ECLI:EU:C:2013:490 Rn. 52 ff.; EuGH 28.1.2015 – Rs. C-375/13 (*Kolassa*) ECLI:EU:C:2015:37 Rn. 51 ff.

172 Vgl. zum Ort der Ausrüstung mit manipulierender Software EuGH 9.7.2020 – Rs. C-343/19 (*VKI/Volkswagen AG*) ECLI:EU:C:2020:534 Rn. 24. Vgl. zum Auslösen einer – markenrechtsverletztenden – Internetanzeige EuGH 19. 4. 2012 – Rs. C-523/10 (*Wintersteiger*) ECLI:EU:C:2012:220 Rn. 34 ff. Allgemein lokalisiert z.B. auch BeckOK ZPO/*Thode*, 54. Ed. 1.9.2024, Art. 7 Brüssel Ia-VO Rn. 87, den Handlungsort im Cyber-Space dort, wo die jeweiligen Daten (in das Internet) hochgeladen werden. Vgl. zum Kollisionsrecht ferner BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 40 EGBGB Rn. 42.

E-Mail dort versendet oder das Software-Update von dort aus übermittelt hat. Freilich lässt sich hier im Einzelfall jeweils auf den Schwerpunkt der Vorwerfbarkeit abstellen und fragen, ob nicht beispielsweise das zeitlich noch vorgelagerte Unterlassen objektiv gebotener Cyber-Sicherheitsmaßnahmen ursächlich für die Weiterverbreitung ist.[173] Schließlich mag das Unterlassen zu einem anderen Ort – z.B. zur in einem anderen Staat belegenen Konzern-IT-Zentrale – und damit zu einem anderen international zuständigen Gericht führen.

Nicht als Handlungsort einzuordnen ist dagegen nach wohl vorherrschender und grundsätzlich auch zutreffender Meinung der Ort des jeweiligen Zielrechners oder -servers.[174] Eine Ausnahme erscheint aber sachgerecht, wenn ein vorsätzlich handelnder Cyber-Angreifer sich z.B. Botnetze baut, also Rechner, IoT-, IIoT-Geräte oder sonstige IT-Infrastruktur kapert, um dadurch sodann mithilfe dieser dezentral ein anderes Ziel attackieren zu können. Hier können Handlungsorte sehr wohl am Standort der jeweils gekaperten Rechner oder IoT-Geräte lokalisiert werden, die sodann für Angriffe auf weitere Rechner verwendet werden.[175] Der Angreifer ist insoweit auch nicht schutzwürdig, da er sich gezielt die Dezentralität und

---

173 Auf Deckungsebene führt dies unweigerlich zur Frage, ob Obliegenheiten vor Eintritt des Versicherungsfalls zur Gewährleistung der IT-Sicherheit verletzt worden sind, vgl. nur A1-16 AVB Cyber.

174 Vgl. EuGH 19.4.2012 – Rs. C-523/10 (*Wintersteiger*), ECLI:EU:C:2012:220 Rn. 36: „Das Auslösen des technischen Anzeigevorgangs durch den Werbenden erfolgt zwar letztlich auf einem Server des Betreibers der von dem Werbenden verwendeten Suchmaschine. Gleichwohl kann im Hinblick auf das mit den Zuständigkeitsregeln verfolgte Ziel der Vorhersehbarkeit der Standort dieses Servers für die Zwecke der Anwendung von Art. 5 Nr. 3 der Verordnung Nr. 44/2001 nicht als Ort des ursächlichen Geschehens angesehen werden, denn es ist unklar, wo er sich befindet." Vgl. auch *Dicey, Morris and Collins on the conflict of laws*, 16th ed. 2022, Rn. 35-120; BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 40 EGBGB Rn. 43 f.; *Mankowski*, RabelsZ 63 (1999), 203, 267 f. und 281 f.; anders war bei Internet-Delikten die Praxis wohl in China, wo auf den Serverstandort abgestellt worden ist, vgl. nur *Jie Huang*, Personal Jurisdiction based on the Location of a Server: Chinese Territorialism in the Internet Era?, 36 Wisconsin International Law Journal 87 (2019); *Jeanne Huang*, Chinese Private International Law and Online Data Protection, 15 Journal of Private International Law 186, 196 (2019).

175 Anders als in Konstellationen, in denen gefährliche und dem Einfluss des Handelnden sodann entzogene Elemente – etwa Radioaktivität durch Explosion eines Kernkraftwerks – außer Kontrolle geraten, werden hier vom Täter ganz gezielt weitere Rechner und sonstige Bestandteile fremder IT-Infrastruktur infiziert und sodann als „Bot-Netz" instrumentalisiert; das rechtfertigt die Multiplikation der Handlungsorte und eine grundsätzliche Wahlbefugnis des Geschädigten, vgl. nur *Freitag/Leible*, ZVglRWiss 99 (2000), 101, 138 f.; BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 40 EGBGB Rn. 23 und dort in Rn. 22 auch zur Abgrenzung zu anderen Szenarien.

Ubiquität des Internets für sein Delikt zunutze macht. Er muss damit rechnen, überall dort wo er attackiert, zum einen gerichtspflichtig und zum anderen auch (in der Regel: nach dem Recht des jeweiligen Handlungsorts) für den gesamten angerichteten Schaden haftbar zu sein.[176] Auch der EuGH erkennt grundsätzlich an, dass im Einzelfall mehrere Handlungsorte bestehen können.[177] Zugleich fordert der Gerichtshof in seiner *Melzer*-Entscheidung aber, dass der Schädiger selbst und nicht nur ein Dritter auf dessen Geheiß am potentiellen Handlungsort tätig wird.[178] Die Situation ist indes zumindest beim gezielten Einsatz von Malware, die der vorsätzlich handelnde Angreifer unmittelbar steuert, in der hier diskutierten Konstellation eine andere. Letztverbindlich kann dies allerdings nur der EuGH entscheiden.

bb) Erfolgsort und Cyberhaftpflicht: Ort des Primärschadens bei multiplen Angriffsrouten, „Würmern“ und (reinen) Vermögensschäden

Der Erfolgsort bezeichnet grundsätzlich den Ort, an dem durch die (bevorstehende) Verwirklichung des Schadenserfolges in Rechtsgüter des Geschädigten eingegriffen wird.[179] Allerdings differenziert der EuGH hier zwischen der unmittelbaren Verletzung des Rechtsguts einerseits und dem sich hieraus mittelbar ergebenden Folgeschaden: Bei Personen- und Sachschäden soll der Erfolgsort nur am Ort der Rechtsgutsverletzung als sogenannter Ort des „Erst-

[176] In diese Richtung auch *Mankowski*, RabelsZ 63 (1999), 203, 270 f.: Der Täter „macht sich die Vorteile eines weltweiten Kommunikationsnetzes zunutze ... und weiß das auch“.

[177] So zum internationalen Kartelldeliktsrecht EuGH 5.7.2018 – Rs. C-27/17 (*flyLAL*) ECLI:EU:C:2018:533 Rn. 57 und 35, der allerdings eine Schwerpunktbetrachtung vornimmt und fragt, welchem Handlungsort „besonders große Bedeutung zukommt“. Vgl. auch GA *Bobek* v. 28.2.2018 – Rs. C-27/17 (*flyLAL*) ECLI:EU:C:136 Rn. 87 ff. Dazu Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 7 Brüssel Ia-VO Rn. 19a.

[178] Vgl. EuGH 16.5.2013 – Rs. C-228/11 (*Melzer*) ECLI:EU:C:2013:305 Rn. 29 ff. Vgl. ferner BGH IPRax 2017, 480 Rn. 17 ff.

[179] Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 7 Brüssel Ia-VO Rn. 19.

schadens“ liegen.[180] Etwaige mittelbare Folgeschäden begründen dagegen keinen Erfolgsortgerichtsstand.[181] Gleiches gilt grundsätzlich für den Ort, an dem der Schaden lediglich erstmalig entdeckt wird.[182] Das wirft freilich gerade bei der Einspeisung und (Selbst) Verbreitung von Malware in – nicht selten über Staatsgrenzen und ganze Wertschöpfungsketten hinweg – verzweigten und verbundene Firmennetzwerken Fragen auf: Hier lässt sich der primäre Ort der Einschleusung selbst innerhalb eines betroffenen Unternehmens allenfalls mit aufwendiger Forensik rekonstruieren und der effektive Einschleusungspunkt dürfte gerade bei ganz gezielter Verwendung von multiplen Angriffs- und Verbreitungswegen zudem fast zufälliger Natur sein. Es spricht deshalb viel dafür, dass zumindest beim Einsatz und auch bei der Weiterleitung von selbstverbreitender Malware (z.B. eines Wurms wie „*Stuxnet*“)[183] *jeder* betroffene Computer, Server oder sonstiger Bestandteil der IT-Infrastruktur als eigenständiger „Erstschaden“ und damit als ein Erfolgsort i.S.d. Art. 7 Nr. 2 Brüssel Ia-VO zu behandeln ist. Dies entspricht sowohl dem Wesen als auch der Wirkungsweise solcher gezielt streuender Cyber-Angriffsmittel, die sodann eine vom Angreifer intendierte unübersehbare Vielzahl von „Cyber-Streuschäden“ hervorrufen. Auch hier nutzt der Angreifer bewusst und gewollt Instrumente, die potentiell überall auf der Welt (Primär)Schäden hervorrufen können, so dass der Cyber-Angreifer billigerweise auch damit rechnen muss,

---

180 Z.B. EuGH 29.7.2019 – Rs. C-451/18 (*Tibor Trans*) ECLI:EU:C:2019:635 Rn. 28; EuGH 9.7.2020 – Rs. C-343/19 (*VKI/Volkswagen AG*) ECLI:EU:C:2020:534 Rn. 26. Vgl zum Kollisionsrecht auch Erwägungsgrund Nr. 17 Rom II-VO: „Das anzuwendende Recht sollte das Recht des Staates sein, in dem der Schaden eintritt, und zwar unabhängig von dem Staat oder den Staaten, in dem bzw. denen die indirekten Folgen auftreten könnten. Daher sollte bei Personen- oder Sachschäden der Staat, in dem der Schaden eintritt, der Staat sein, in dem die Verletzung erlitten beziehungsweise die Sache beschädigt wurde.“.

181 Z.B. EuGH 11.1.1990 – Rs. C-220/88 (*Dumez France*) ECLI:EU:C:1990:8 Rn. 14 und 22; EuGH 9.7.2020 – Rs. C-343/19 (*VKI/Volkswagen AG*) ECLI:EU:C:2020:534 Rn. 27. Entsprechend kann z.B. die französische Muttergesellschaft eines deutschen Tochterunternehmens, das unmittelbar in Deutschland durch ein anderes deutsches Unternehmen geschädigt wird, nicht ihre mittelbaren Schäden nach Art. 7 Nr. 2 Brüssel Ia-VO an einem „Erfolgsort“ in Frankreich einklagen, vgl. EuGH 11.1.1990 – Rs. 220/88 (*Dumez France*) Slg. 1990, I-49 Rn. 22; Geimer/Schütze/*Geimer*, EuZivilVerfR, 4. Aufl. 2020, Art. 7 EuGVVO Rn. 281.

182 Vgl. nur Anders/Gehle/*Schmidt*, ZPO, 82. Aufl. 2024, Art. 7 Brüssel Ia-VO Rn. 22 f.

183 *Rieger*, Trojaner „stuxnet“: Der digitale Erstschlag ist erfolgt, FAZ v. 22. 9.2010.

an ausnahmslos jedem dieser Erfolgsorte gerichtspflichtig zu sein.[184]

Die Differenzierung zwischen „Erstschaden“ und daraus hervorgehendem mittelbaren Folgeschaden versagt ohnehin immer dann, wenn von vornherein nur ein „reiner“ bzw. „echter“ Vermögensschaden eintritt. Im Kontext von Cyber-Haftpflichtansprüchen ist etwa an die Betriebsunterbrechung infolge einer Verschlüsselung von – nicht im Besitz oder Eigentum des Betroffenen stehenden – IT-Systemen und insbesondere von Cloud-Lösungen zu denken: Je nach dem, wie das anwendbare Recht diesen Vorgang rechtsdogmatisch erfasst,[185] mag das primär geschädigte Rechtsgut allein das Vermögen sein, wobei die besondere Herausforderung gerade bei Betriebsunterbrechungsschäden darin bestehen dürfte, das jeweils konkret betroffene und geminderte (Teil)Vermögen für die Zwecke des Art. 7 Nr. 2 Brüssel Ia-VO zu lokalisieren.[186]

cc) Sachgerechte Erfolgsortzuständigkeit für den Gesamtschaden am „Mittelpunkt des Interesses“

Während am Handlungsort stets der Gesamtschaden eingeklagt werden kann, soll am jeweiligen Erfolgsort nach der Judikatur des EuGH jedoch gerade bei Streuschäden, wie sie im Fall von Cyber-Attacken und auch bei der Weiterleitung von Schadcode eintreten, grundsätzlich nur der dort eingetretene Teilschaden zu liquidieren sein.[187] Der EuGH begründet diese „*Shevill*-Doktrin“ bzw. „Mosaiktheorie“ mit der auf den jeweiligen Erfolgsort beschränkten Sach-

---

184 Vgl. zum Handlungsort bereits *Mankowski*, RabelsZ 63 (1999), 203, 270 f.

185 Bei einer durch einen Cyber-Incident bewirkten Datenlöschung oder Datenveränderung auf im Eigentum des Betroffenen stehenenden und klar physisch abgrenzbaren Datenträgern mag das Eigentum beeinträchtigt sein, was bei Ransomware-Attacken auch die häufige Verschlüsselung von Daten umfassen dürfte, vgl. nur *Lesser*, Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken, 2021, S. 32 ff. m.w.N. Bei den immer relevanter werdenden – und gerade nicht im Eigentum des Angegriffenen stehenden – Cloud-Lösungen dürfte aus Sicht des deutschen Rechts der Fall anders liegen.

186 Vgl. zu anderen Fällen reiner Vermögensschäden nur EuGH 28.1.2015 – Rs. C-375/13 (*Kolassa*) ECLI:EU:C:2015:37 Rn. 54 ff.; EuGH 6.6.2016 – C-12/15 (*Universal Music International Holding*) ECLI:EU:C:2016:449 Rn. 40.

187 Vgl. grundlegend EuGH 7.3.1995 – Rs. C-68/93 (*Shevill*) ECLI:EU:C:1995:61 Rn. 33; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv/DR*) ECLI:EU:C:2021:1036 Rn. 34 ff. Dazu statt vieler *Lutzi*, NJW 2022, 768 ff.; *Engel*, EuZW 2022, 226 ff.

nähe des Gerichts.[188] Daraus folgt bei der Einschleusung und Weiterverbreitung von Malware in der IT-Infrastruktur internationaler Unternehmen ein potentiell riesiges „Mosaik“ aus einzelnen Erfolgsorten, an denen das betroffene Unternehmen seine jeweiligen Teilschäden sodann mit großem Aufwand einzeln gerichtlich durchsetzen müsste.

Noch weitaus komplexer wird das Bild, wenn die mittlerweile in fast allen Unternehmen üblichen und beständig um Anwendungsfelder erweiterten Cloud-Lösungen in die Betrachtung einbezogenen werden. Obschon die Fragmentierung und Verschlüsselung der Daten i.R.d. Cloud-Computing eine zusätzliche Sicherheitsebene schaffen mag,[189] sind auch hier bereits erfolgreiche Cyber-Angriffe zu verzeichnen, durch die Daten kompromittiert worden sind.[190] Wesensmerkmal des Cloud-Computing ist, dass einheitliche Datenbestände auf diverse und – je nach Anbieter – europa- oder weltweit verstreute Server je nach verfügbarer Speicherkapazität fragmentweise verteilt und gespeichert werden.[191] Lokalisiert man hier nun den Erfolgsort am jeweils zur Datenspeicherung verwendeten Server, wo Datenfragmente durch den Cyber-Angriff konkret betroffen sind,[192] würde dem Nutzer die Rechtsdurchsetzung nahezu unmöglich gemacht: Zum einen lässt sich kaum nachvollziehen, wo und zu welchem exakten Zeitpunkt ein konkreter Datensatz – oder präziser gefasst: ein konkretes Datenfragment – abgespeichert worden ist.[193] Auch existieren für einen einheitlich betroffenen Datensatz, der in zufälliger Weise auf Server verteilt wird, dann potentiell zahlreiche Erfolgsorte und damit zersplitterte Gerichtszuständigkeiten – nämlich jeweils dort, wo das jeweilige kompromittierte Datenfragment

---

188 Grundlegend wiederum EuGH 7.3.1995 – Rs. C-68/93 (*Shevill*) ECLI:EU:C:1995:61 Rn. 33.

189 Zu den Hintergründen und Methoden z.B. *Google Cloud Architecture Center*, Mitigating ransomware attacks using Google Cloud, 15.11.2021, abrufbar unter: https://cloud.google.com/architecture/mitigating-ransomware-attacks (zuletzt abgerufen am 1.5.2025).

190 Zu den Angriffswegen z.B. *Balassiano/Shaty*, Ransomware in the Cloud: Breaking Down the Attack Vectors, 29.11.2023, abrufbar unter: https://www.paloaltonetworks.com/blog/prisma-cloud/ransomware-data-protection-cloud/ (zuletzt abgerufen am 1.5.2025).

191 Vgl. statt vieler *Nordmeier,* MMR 2010, 151 ff.; *Schneidereit*, Haftung für Datenverlust im Cloud Computing, 2017, S. 71 f.

192 Dafür im Grundsatz *Schneidereit*, Haftung für Datenverlust im Cloud Computing, 2017, S. 70 f. Dagegen *Nordmeier*, MMR 2010, 151, 153 ff.

193 *Borges* in: Borges/Meents, Cloud Computing, 2016, § 12 II Rn. 21; *Schneidereit*, Haftung für Datenverlust im Cloud Computing, 2017, S. 72.

belegen war.[194] Keiner dieser Erfolgsorte weist dabei eine besondere enge sachliche Verbindung zum Datensatz selbst oder gar zum betroffenen Unternehmen auf: Die Verteilung erfolgt anhand der vorhandenen Speicherkapazitäten, und je nach Verfügbarkeit kann sich die Allokation binnen Sekundenbruchteilen wieder ändern, und ein zuvor in den USA gespeichertes Datenfragment mag auf einen Server nach Indien verschoben werden. Eine gesteigerte Sach- oder Beweisnähe des Gerichts am jeweiligen – völlig arbiträren – Speicherort im Zeitpunkt einer Informationssicherheitsverletzung ist hier erst recht nicht gegeben, wenn der Datensatz bzw. das Datenfragment bereits in der Sphäre des Cloud-Nutzers kompromittiert (und so z.B. durch *ransomware* verschlüsselt) und dann im Wege rollierender Aktualisierungen in die Cloud geladen wird.[195]

Vor diesem Hintergrund ist für Cyber-Attacken insgesamt zu fragen: Kann hier das Mosaikprinzip der Erfolgsorte aufgelockert werden, damit der Geschädigte nicht zu den Gerichten der zahllosen Erfolgsorte laufen muss, um seine Ansprüche dort jeweils gewissermaßen häppchenweise durchzusetzen? Einen Lösungsansatz mag hier die *eDate- und Martinez-* Rechtsprechung des EuGH bieten: In dieser Rechtssache hatte der EuGH dem durch Persönlichkeitsrechtsverletzungen im Internet Geschädigten im Ergebnis einen Klägergerichtsstand am „Mittelpunkt seines Interesses“ gewährt, wo der Gesamtschaden liquidiert werden kann.[196]

Für eine ähnliche Lösung bei Cyber-Attacken auf Unternehmen ließe sich die Nähe von unternehmensbezogenen Daten zum Unternehmenspersönlichkeitsrecht und zur Privatsphäre anführen: Insoweit hat der EuGH in seiner *Svensk-Handel*-Entscheidung nämlich bereits eine Übertragung der *eDate*-Grundsätze auf Unternehmen

---

194 Vgl. erneut zum „Mosaikprinzip“, wonach in den einzelnen Erfolgsortgerichtsständen jeweils nur der dort entstandene Schaden geltend gemacht werden kann EuGH 17.6.2021 – Rs. C-800/19 (*Mittelbayerischer Verlag*) ECLI:EU:C:2021:489 Rn. 24 ff.; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv*) ECLI:EU:C:2021:1036 Rn. 24 ff.

195 Zu den Kriterien der Sach- und Beweisnähe m.w.N. etwa EuGH 18.7.2013 – Rs. C-147/12 (*ÖFAB*) ECLI:EU:C:2013:490 Rn. 50 f.

196 EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 52 ff.

befürwortet.[197] Diese Linie verfolgen auch die nationalen Gerichte und in Frankreich z.B. die Cour de cassation.[198] Für die Anwendung auch auf Cyber-Attacken, die Weiterleitung von Schad-Code und die daraus hervorgehenden Informationssicherheitsverletzungen spricht zunächst auf Ebene des EU-Primärrechts, dass der EuGH in seiner ständigen Rechtsprechung Art. 7 GRCh als Fundament des unionsrechtlichen Schutzes von vertraulichen Daten ansieht und dieses Unionsgrundrecht insbesondere auch ausdrücklich auf Unternehmen erstreckt.[199] In unionsgrundrechtsdogmatischer Hinsicht beruhen also das Unternehmenspersönlichkeitsrecht, um das es in *Svensk Handel* ging, einerseits und der Schutz von Datenvertraulichkeit andererseits zumindest partiell auf derselben Basis.[200] Anders ausgedrückt: Auch Unternehmen haben ein durch Art. 7 GRCh geschütztes Recht auf Privatheit – und aus Sicht der Unionsrechtsordnung betreffen Cyberangriffe, bei denen die Verfügbarkeit, Integrität und Vertraulichkeit von Unternehmensinformationen verletzt werden, just diese geschützte Sphäre der Privatheit.[201]

EU-Sekundärrechtakte wie die Brüssel Ia-VO sind stets im Lichte des EU-Primärrechts und damit auch der Unionsgrundrechte auszulegen und anzuwenden. Die dogmatische Verortung der Vertraulichkeit von Unternehmensinformationen i.R.d. Art. 7 GRCh spricht dafür, dass auf Ebene des Art. 7 Nr. 2 Brüssel Ia-VO Cyber-Angriffe und deren Folgen ähnlich wie alle anderen gegen die Vertraulichkeit von Unternehmensinformationen gerichteten Verletzungshandlungen zu behandeln sind. Gerade im Interesse einer kohärenten Systematik des Internationalen Zivilverfahrensrechts der EU sollten

---

197 EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 30 ff. Siehe sodann auch EuGH 17.6.2021 – Rs. C-800/19 (*Mittelbayerischer Verlag*) ECLI:EU:C:2021:489 Rn. 24 ff.; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv/DR*) ECLI:EU:C:2021:1036 Rn. 31 und 39.

198 Cass. com. 16.3.2022 – n° 20.22.000, Rev. crit. DIP 2023, 807 ff. m. Anm. *El Hage*.

199 Vgl. nur EuGH 14.2.2008 – Rs. C-450/06 (*Varec*) ECLI:EU:C:2008:91 Rn. 48; GA *Wathelet* v. 16.9.2015 – Rs. C-419/14 (*WebMindLicenses*) ECLI:EU:C:2015:606 Rn. 111.

200 Vgl. erneut nur EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 30 ff. einerseits und EuGH 14.2.2008 – Rs. C-450/06 (*Varec*) ECLI:EU:C:2008:91 Rn. 48 andererseits.

201 Im Übrigen bezieht der EuGH juristische Personen zumindest teilweise in den Schutzbereich des Datenschutzgrundrechts nach Art. 8 GRCh ein, wenn der Name der juristischen Personen sich auf eine oder mehrere natürliche Personen bezieht, vgl. EuGH 9.11.2010 – Rs. C-92/09 (*Schecke*) ECLI:EU:C:2010:662 Rn. 53; EuGH 17.12.2015 – Rs. C-419/14 (*WebMindLicenses*) ECLI:EU:C:2015:832Rn. 79.

daher die in der Rechtsprechung des EuGH in den Rechtssachen *eDate und Martinez* und *Svensk Handel* entwickelten Grundsätze auch auf Schadensersatzansprüche infolge von Cyber-Angriffen übertragen werden. Eine solche Übertragung hat auch der EuGH-Generalanwalt *Szpunar* zumindest im Kontext der E-Commerce-Richtlinie[202] vorgeschlagen, wobei es in der Rechtssache *Facebook Ireland Limited* gerade um die Zuständigkeit für den Erlass von Verfügungen zur Verhinderung von Schäden ging, die über den Verbreitungsweg „Cyber-Space" ubiquitär eintreten können.[203] Das mag ebenfalls für die Verallgemeinerungsfähigkeit dieses Ansatzes streiten.

Nach der hier befürworteten Lesart kann auch bei Haftpflichtansprüchen im Gefolge von Cyber-Attacken ein Gerichtsstand am „Mittelpunkt des Interesses" des betroffenen Unternehmens entsprechend der durch den EuGH in den Rechtssachen *eDate und Martinez* und *Svensk Handel* entwickelten Maßstäbe begründet werden.[204] In diesen Entscheidungen argumentiert der EuGH zur Begründung des Gerichtsstandes nicht vorrangig mit dem Schutz des Klägers, sondern mit dem Interesse an einer geordneten Rechtspflege, das bei ubiquitären und zumeist eher beliebigen Erfolgsorten andernfalls beeinträchtigt würde.[205] Dies trifft auch bei der Schädigung von Unternehmen durch Cyber-Attacken oder durch die Weiterverbreitung von Schad-Code und dadurch ausgelöste Informationssicherheitsverletzungen zu: Hier ist die Lokalisation der Erfolgsorte bei einheitlicher, grenzüberschreitend vernetzter IT zum einen diffizil und zum anderen hängt es meist von Kostenerwägungen ab, in welchen Staaten zentrale Teile der unternehmenseigenen IT-Infrastruktur ansässig sind. Vor allem ist die Frage nach den

---

202 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG L 178/1.

203 Vgl. GA *Szpunar* Schlussanträge v. 4.6.2019 – Rs. C-18/18 (*Facebook Ireland Limited*) ECLI:EU:C:2019:458 Rn. 82 ff.

204 Vgl. EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 30 ff. und Rn. 36 f., wobei der Gerichtsstand laut EuGH ungeachtet dessen eröffnet sein soll, ob der geltend gemachte Schaden materieller oder immaterieller Natur ist. Vgl. zur Rezeption der Entscheidung in den Mitgliedstaaten erneut nur Cass. com. 16.3.2022 – n° 20.22.000, Rev. crit. DIP 2023, 807 ff. m. Anm. *El Hage*.

205 EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 37.

Erfolgsorten bei Cloud-Lösungen ohnehin kaum zu beantworten. Hinzu kommt, dass ohnehin weniger die – allein zuständigkeitsbegründenden – „Primärschäden" an den Datensätzen und IT-Anlagen,[206] als vielmehr die dadurch hervorgerufenen Vermögensfolgeschäden, etwa infolge von Betriebsunterbrechungen und deren Folgen, besonderes wirtschaftliches Gewicht haben.[207] Hier den Blick mit dem EuGH auf den „Mittelpunkt des Interesses" des angegriffenen Unternehmens zu lenken, erscheint daher umso sachgerechter, als der Gerichtshof diesen Mittelpunkt grundsätzlich dort lokalisiert, wo die juristische Person „den wesentlichen Teil ihrer wirtschaftlichen Tätigkeit ausübt".[208] Dies wird in der Regel der Ort der Hauptverwaltung sein, der sich häufig – wenn auch keineswegs zwingend – mit dem Satzungssitz deckt.[209] Zu beachten ist zudem die Hauptniederlassung, die zuständigkeitsrechtlich nicht zuletzt Gesellschaften aus Drittstaaten in der EU gerichtspflichtig macht: Sie liegt am „Schwerpunkt der externen – auf den Markt bezogenen – Geschäftstätigkeit", die wiederum anhand der „dort vorhandenen Personal- und Sachmittel, die für den Umfang des Geschäftsvolumens maßgeblich sind", zu bestimmen ist.[210] Fasst man unter diese „Sachmittel" gerade auch die IT-Infrastruktur eines Unternehmens, so wird die tatsächliche und wirtschaftliche Beeinträch-

---

206 Deutlich etwa EuGH 29.7.2019 – Rs. C-451/18 (*Tibor Trans*) ECLI:EU:C:2019:635 Rn. 27: „Die Antwort auf die Frage, wo sich der Ort befindet, an dem sich ein solcher Schadenserfolg verwirklicht hat, hängt davon ab, ob es sich um einen sich unmittelbar aus dem kausalen Ereignis ergebenden Erstschaden handelt, dessen Eintrittsort die Zuständigkeit im Hinblick auf Art. 7 Nr. 2 der Verordnung Nr. 1215/2012 begründen könnte, oder um die darauffolgenden nachteiligen Konsequenzen, die keine Zuständigkeitszuweisung gemäß dieser Vorschrift begründen können".

207 In diesem Sinne auch Schlussanträge GA *Bobek* v. 13.7.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:554 Rn. 80 ff.

208 EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 37: Am Mittelpunkt des wirtschaftlichen Interesses eines Unternehmens will der EuGH in der Rechtssache Svensk Handel auch die internationale Zuständigkeit für Beseitigungs- und Unterlassungsklagen konzentrieren. Dabei argumentiert der Gerichtshof gerade mit der „weltumspannenden Verbreitung" und folglich mit einem Kriterium, dass man auch bei Cybervorfällen in international tätigen Unternehmen anlegen kann, vgl. dort Rn. 48.

209 Vgl. zu Art. 63 Abs. 1 lit. a un b Brüssel Ia-VO statt aller Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 63 EuGVVO Rn. 1.

210 Siehe zur Hauptniederlassung i.S.d. Art. 63 Abs. 1 lit. c Brüssel Ia-VO nur BGH IPRax 2024, 145 f. Siehe auch *Schwemmer*, IPRax 2024, 130 ff.

tigung durch die Cyberattacke auch an ebendiesem Hauptsitz typischerweise am stärksten ausfallen.[211]

Dieser Ort ist für haftpflichtige Schädiger auch weitaus vorhersehbarer als der Standort einzelner betroffener Server oder gar von Datenfragmenten in einer Cloud.[212] Ganz ähnliche Überlegungen lassen sich bei Unternehmen aus Branchen anstellen, die ihre Mitarbeiter ständig rund um die Welt verstreut – z.B. als Berater, Vertriebs- oder Außendienstmitarbeiter – einsetzen. Denn sind auf solchen Reisen sodann die einzelnen Dienstlaptops oder sonstigen Endgeräte jeweils z.B. von der fahrlässigen Weiterverbreitung von Schad-Code durch Geschäftskontakte betroffen, so können die Erfolgsorte ohne Weiteres auf unterschiedlichen Kontinenten liegen, einschließlich auf mehr oder minder zufälliger Zwischenstopps oder Durchreisestationen. In solchen Szenarien erscheinen die Erfolgsorte ebenfalls vollkommen arbiträr.

Zwar gilt auch bei der internationalen Zuständigkeit: Wer fahrlässig – z.B. infolge eines zu geringen IT-Sicherheitsniveaus – Schadsoftware potentiell weltweit in Umlauf bringt oder weiterverbreitet, muss damit rechnen, überall dort gerichtspflichtig zu sein, wo sich Schäden materialisieren.[213] Jedoch erscheint das Gericht am Hauptsitz – und damit am „Mittelpunkt des Interesses“ – des betroffenen Unternehmens nicht nur leichter vorhersehbar, sondern es ist regelmäßig auch besonders sach- und beweisnah, weil in der Unternehmenszentrale schon aus Gründen der – nunmehr branchenspezifisch auch in der NIS-2-Richtlinie und den Umsetzungsrechtsakten wie dem BSIG-E[214] niedergelegten – Cyber-Risikomanagement-Pflichten alle Informationen zur IT und zur Schadensentwicklung

---

211 Vgl. im Ergebnis zu Cloud-Lösungen auch *Schneidereit*, Haftung für Datenverlust im Cloud Computing, 2017, S. 76; *Borges* in: Borges/Meents, Cloud Computing, 2016, § 12 II Rn. 21 a.E.; BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 4 Rom II-VO Rn. 41.

212 Zum Kriterium der Vorhersehbarkeit z.B. EuGH 17.6.2021 – Rs. C-800/19 (*Mittelbayerischer Verlag*) ECLI:EU:C:2021:489 Rn. 25; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv*) ECLI:EU:C:2021:1036 Rn. 25.

213 Vgl. EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 50; EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 35 ff.

214 Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) (Stand: 2.10.2024), BT-Drucks. 20/13184.

zusammenlaufen und rasch verfügbar sind: Dies folgt schon aus dem Erfordernis einer unternehmensweiten Cyber-Sicherheits- und -Risiko-Management-Strategie und den entsprechenden Organisations-, Überwachungs- und Compliance-Pflichten und Reporting-Wegen.[215] Eine Konzentration auf den Gerichtsstand am Hauptsitz als „Mittelpunkt der Interessen" entspricht zudem gerade der *ratio* des Art. 7 Nr. 2 Brüssel Ia-VO, weil hier „zwischen der Streitigkeit und den Gerichten … eine besonders enge Beziehung besteht, die aus Gründen einer geordneten Rechtspflege und einer sachgerechten Gestaltung des Prozesses eine Zuständigkeit dieser Gerichte rechtfertigt."[216] Zudem muss der Beklagte gerade vernünftigerweise auch damit rechnen, an diesem Gerichtsstand in Anspruch genommen zu werden.[217]

Inwieweit die Erwägungen aus den *eDate*- und *Svensk Handel*-Entscheidungen auf Cyber-Vorfälle übertragen werden können, vermag letztverbindlich freilich nur der EuGH zu klären. Soweit das verneint werden sollte, wäre eine mühsame und für den von einer Informationssicherheitsverletzung betroffenen Kläger zudem kostspielige Mosaikbetrachtung der Erfolgsorte unausweichlich.

d) Gerichtsstände nach Art. 7 Nr. 5, Art. 8 Nr. 1 Brüssel Ia-VO

Die internationale Zuständigkeit für Cyber-Haftpflichtklagen kann auch am besonderen Gerichtsstand der Niederlassung des Schädigers nach Art. 7 Nr. 5 Brüssel Ia-VO begründet werden, wenn es sich um Streitigkeiten aus dem Betrieb einer in einem anderen als dem (Wohn)Sitzmitgliedstaat belegenen EU-Niederlassung handelt.[218] Zu denken ist etwa an den Fall, dass eine französische Zweigniederlassung eines deutschen Unternehmens sorgfaltswidrig Schad-Code an internationale Kunden weiterverbreitet hat und nun

---

215 So gibt es i.R.d. NIS-2-Regimes eine umfassende Verantwortlichkeit und „Rechenschaftspflicht" für Cyber-Risikomanagementmaßnahmen nach Art. 21 i.V.m. Art. 20 NIS-2-RL dergestalt, dass „dokumentiert(e) Cybersicherheitskonzepte" und „Nachweis(e) für die Umsetzung der Cybersicherheitskonzepte" vorzuhalten sind, vgl. Art. 32 Abs. 2 lit. e und lit. g NIS-2-RL.

216 EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 26 f.; EuGH 17.6.2021 – Rs. C-800/19 (*Mittelbayerischer Verlag*) ECLI:EU:C:2021:489 Rn. 24 ff.; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv*) ECLI:EU:C:2021:1036 Rn. 24 ff.

217 So auch EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv*) ECLI:EU:C:2021:1036 Rn. 25.

218 Z.B. Musielak/Voit/*Stadler/Krüger*, ZPO, 22. Aufl. 2025, Art. 7 Brüssel Ia-VO Rn. 25 f.

von diesen Kunden auf Schadensersatz in Anspruch genommen wird. Hingegen dürfte durch die i.d.R. nur fahrlässige Weiterverbreitung von Schad-Code durch das Opfer einer Cyber-Attacke schon mangels Vorsatz keiner der IT- bzw. datenbezogenen Straftatbestände verwirklicht werden.[219] Infolgedessen wäre der Gerichtsstand der Adhäsionsklage nach Art. 7 Nr. 3 Brüssel Ia-VO in dieser Konstellation regelmäßig nicht eröffnet.

Soweit der Angegriffene und weitere Personen – wie etwa der Cyber-Angreifer oder auch ein IT-Dienstleister des Angegriffenen – ausnahmsweise als Gesamtschuldner für eine Informationssicherheitsverletzung bei Dritten haften, kommt schließlich der Gerichtsstand des Sachzusammenhangs nach Art. 8 Nr. 1 Brüssel Ia-VO in Betracht: Danach können insbesondere gesamtschuldnerisch haftende Beklagte mit Sitz in der EU im Wohnsitzmitgliedstaat nur eines der Beklagten verklagt werden, wenn zwischen den Klagen eine so enge Beziehung gegeben ist, dass eine gemeinsame Verhandlung und Entscheidung geboten erscheint, um zu vermeiden, dass in getrennten Verfahren widersprechende Entscheidungen ergehen.[220] Demgegenüber scheidet dieser Gerichtsstand aus, sobald einer der Beklagten seinen Sitz in einem Drittstaat hat,[221] weshalb Anspruchsgegner international-zuständigkeitsrechtlich besonders schwer zu erfassen sind, die aus mehreren Staaten heraus Ursachenbeiträge setzen oder gar – als unmittelbare Cyber-Angreifer – gezielt zusammenwirken, wie dies z.B. bei der Ransomware-Gruppe „*Radar/Dispossessor*“ der Fall war.[222]

---

219 Vgl. zum Vorsatzerfordernis bei §§ 202a, 202b, 202c, 202d StGB sowie zu §§ 303a, 303b StGB statt vieler BeckOK StGB/*Weidemann*, 65. Ed. 1.5.2025, § 202a StGB Rn. 21 sowie § 303a StGB Rn. 17 f. und § 303b StGB Rn. 17 f.

220 Vgl. nur EuGH 21.5.2015 – Rs. C-352/13 (*CDC Hydrogen Peroxide*) ECLI:EU:C:2015:335 Rn. 20; EuGH 20.4.2016 – Rs. C-366/13 (*Profit Investment*) ECLI:EU:C:2016:282 Rn. 59 ff.

221 Vgl. nur OLG Stuttgart IPRax 2015, 430 Rn. 144; Anders/Gehle/*Schmidt*, ZPO, 82. Aufl. 2024, Art. 8 Brüssel Ia-VO Rn. 2 f.

222 Vgl. *FAZ* v. 13.8.2024, Polizei zerschlägt internationale Hacker-Bande, abrufbar unter: https://www.faz.net/aktuell/wirtschaft/unternehmen/polizei-zerschlaegt-internationale-bande-von-cyberkriminellen-19916507.html (zuletzt abgerufen am 1.5.2025), wonach dieser Gruppierung mindestens „zwölf Tatverdächtige aus Deutschland, der Ukraine, Russland, Kenia, Serbien, Litauen, den Vereinigten Arabischen Emiraten“ angehörten. Bei strafrechtlicher Verfolgung der jeweiligen Akteure in mehreren Staaten scheitert hier auch der Gerichtsstand der Adhäsionsklage nach Art. 7 Nr. 3 Brüssel Ia-VO.

2. Art. 79 DSGVO bei Datenschutzverletzung infolge des Cyber-Vorfalls

Wird der Angegriffene, der als Verantwortlicher oder Auftragsverarbeiter i.S.d. DSGVO Daten in der EU verarbeitet, seinerseits durch natürliche Personen – und so z.B. durch seine Endkunden – wegen Datenschutzverstößen in Anspruch genommen, hält die DSGVO in Art. 79 Abs. 2 besondere internationale Zuständigkeitsvorschriften bereit. Dabei setzt der Gerichtsstand des Art. 79 Abs. 2 S. 2 DSGVO nicht voraus, dass der Beklagte eine Niederlassung in der EU hat, solange nur der räumlich-territoriale Anwendungsbereich der Verordnung nach Art. 3 DSGVO eröffnet ist.[223] Art. 79 Abs. 2 DSGVO regelt die internationale Zuständigkeit für Schadensersatzklagen, die auf Verstößen gegen die DSGVO oder ergänzende mitgliedstaatliche Datenschutzbestimmungen beruhen. In diesem Gerichtsstand sind damit nicht nur der unionsrechtlich-autonome Schadensersatzanspruch aus Art. 82 DSGVO, sondern auch konkurrierende deliktische und vertragliche Schadenersatzansprüche nach nationalem Privatrecht – etwa aus § 823 oder § 280 Abs. 1 BGB – sowie Beseitigungs- und Unterlassungsansprüche einklagbar.[224] Im Gerichtsstand des Art. 79 DSGVO können somit grundsätzlich auch alle Folgeschäden eines Datenschutzverstoßes, wie etwa die aus einer Veränderung, Preisgabe, Verschlüsselung und des Missbrauchs der Daten folgenden Einbußen, eingeklagt werden.

Nach Art. 79 Abs. 2 S. 1 DSGVO ist der Anspruchsgegner dabei zunächst in allen Mitgliedstaaten gerichtspflichtig, in denen er eine Niederlassung unterhält. Vor allem kann die von Datenschutzverstößen betroffene Person gemäß Art. 79 Abs. 2 Satz 2 DSGVO wahlweise auch an ihrem gewöhnlichen Aufenthaltsort klagen. Damit sieht die DSGVO einen leicht zugänglichen Klägergerichtsstand vor. Vor diesem Hintergrund hat die Brüssel Ia-VO neben der DSGVO in der Praxis wohl allenfalls noch eine Ergänzungsfunktion,

---

223 *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 68; *Hoffmann*, IPRax 2024, 7, 15.

224 Dafür LG Frankfurt 28.6.2019 – 2-03 O 315/17 (juris) Rn. 41; *Lüttringhaus* in: Gebauer/Wiedmann, Europäisches Zivilrecht, 3. Aufl. 2021, Kap. 30 Rn. 82 ff. Siehe zur Vorlagefrage an den EuGH nur BGH GRUR 2023, 1724, 1726; BGH NJW 2024, 1577, 1585.

obschon die allgemeinen Gerichtsstände – wie z.B. der Deliktsgerichtsstand nach Art. 7 Nr. 2 Brüssel Ia-VO – dem Kläger freilich weiterhin zur Verfügung stehen.[225] Denn ausweislich des Erwägungsgrundes Nr. 147 DSGVO sollen, soweit in der DSGVO „spezifische Vorschriften über die Gerichtsbarkeit (…) enthalten sind, die allgemeinen Vorschriften (…) der Anwendung dieser spezifischen nicht entgegenstehen". Dies eröffnet strategisch vorgehenden Klägern durchaus Möglichkeiten zum *forum-shopping*: Sie wählen ganz gezielt einen internationalen Gerichtsstand, in dem sie – z.B. aufgrund der dortigen Präjudizen und Rechtssprechungstendenzen – für ihren Haftpflichtanspruch die größten Erfolgsaussichten sehen. Diese Vorgehensweise mag grundsätzlich auch für die – aus Sicht des Anspruchsgegners besonders schadensträchtige – kollektive Rechtsverfolgung attraktiv erscheinen, obschon hier das internationale Privat- und Zuständigkeitsrecht insoweit Hürden aufstellt.

3. Grenzüberschreitende kollektive Anspruchsdurchsetzung infolge eines Cyber-Incidents

Während die kollektive Durchsetzung von Ansprüchen infolge von Datenschutz- oder Cybersicherheitsverstößen zwar nicht in der EU-Verbandsklage-Richtlinie[226] vorgegeben wird, sieht die deutsche Umsetzung im VDuG[227] eine Verbandsklage in Form der „Abhilfeklage" jedenfalls insoweit vor, als in solchen „bürgerlichen Rechtsstreitigkeiten" Ansprüche und Rechtsverhältnisse von einer Vielzahl von Verbrauchern gegen einen Unternehmer geltend gemacht werden.[228] § 2 Abs. 2 Nr. 13 UKlaG zählt Ansprüche nach der DSGVO zu den mit einer Verbandsklage durchsetzbaren „Verbrau-

---

225 LG Berlin 24.8.2023 – 16 O 420/19, Rn. 40 f. (juris); Rechtbank Amsterdam 30.6.2021, ECLI:NL:RBAMS:2021:3307 Rn. 5.42. Eingehend *Heinze/Warmuth*, ZZPInt 21 (2016), 175, 186 f.; *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 67 f.; *Oster*, IPRax 2023, 198, 203 f. Im Verhältnis zu EWR-Staaten kommen zudem die Bestimmungen des LugÜ und insbesondere Art. 5 Nr. 3 LugÜ in Betracht.

226 Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25. November 2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG, ABl. 2020 L 409/1.

227 Gesetz zur gebündelten Durchsetzung von Verbraucherrechten (Verbraucherrechtedurchsetzungsgesetz – VDuG) v. 8.10.2023, BGBl. Nr. 272

228 Vgl. § 1 VDuG.

cherschutzgesetzen“. Auf sachrechtlicher Ebene ist i.R.d. Schadensersatzanspruches nach Art. 82 DSGVO freilich mit Blick auf die nach § 15 Abs. 1 VDuG erforderliche Gleichartigkeit der Ansprüche gerade bei immateriellem Schadensersatz kritisch zu hinterfragen, ob dem Gericht wirklich eine schablonenhafte Prüfung der Anspruchsvoraussetzungen in tatsächlicher und rechtlicher Hinsicht möglich ist.[229] Art. 80 Abs. 1 DSGVO führt dabei zu keiner Erweiterung, sondern sieht die Möglichkeit einer kollektiven Durchsetzung privatrechtlicher Ansprüche infolge von Datenschutzverstößen nur „sofern dieses im Recht der Mitgliedstaaten vorgesehen ist“. Damit setzt Art. 80 Abs. 1 DSGVO bestehende mitgliedstaatliche Verbandsklagebestimmungen voraus, ohne diese vorzugeben.[230]

Mangels Normierung in der EU-Verbandsklage-RL bzw. im VDuG ergibt sich die internationale Zuständigkeit für eine grenzüberschreitende Verbandsklage aus den Zuständigkeitsregeln der Brüssel Ia-VO[231] bzw. bei Verbandsklagen gegen drittstaatliche Akteure aus dem jeweils anwendbaren staatsvertraglichen oder aber aus dem autonomen deutschen Zuständigkeitsrecht (z.B. § 32 ZPO analog).[232] Der Verbrauchergerichtsstand ist dabei Verbänden nicht eröffnet,[233] so dass unter der Brüssel Ia-VO der Rückgriff auf den allgemeinen Beklagtengerichtsstand nach Art. 4 am Unternehmenssitz i.S.d. Art. 63 Brüssel Ia-VO oder ggf. am Handlungsort nach Art. 7 Nr. 2 Brüssel Ia-VO jeweils besonders nahe liegt: Auf diesem Wege lässt sich grundsätzlich eine uniforme internationale Zuständigkeit für alle gebündelten Ansprüche sicherstellen.[234] Darüber hinaus sind auch Zessionsmodelle denkbar, um eine gebündelte

---

229 Offener im Anschluss an EuGH 11.4.2024 – Rs. C-741/21 (*GP/juris GmbH*) ECLI:EU:C:2024:288 nun BGH GRUR 2024, 1878 Rn. 31. Offen Musielak/Voit/*Stadler*, ZPO, 22. Aufl. 2025, § 15 VDuG Rn. 5. Kritisch noch *Pohle/Adelberg*, ZD 2024, 312, 317; *Stadler*, ZZP 136 (2023) 129, 142; *Thönissen*, r+s 2023, 749, 755. Zur Gleichartigkeit allgemein Anders/Gehle/*Schmidt*, ZPO, 82. Aufl. 2024, § 15 VDuG Rn. 2.

230 Vgl. auch *Silvas de Freitas*, NIPR 2023, 227 ff.

231 Musielak/Voit/*Stadler*, ZPO, 22. Aufl. 2025, Vorbem. VDuG Rn. 30.

232 Vgl. im Einzelnen *Hoffmann*, IPRax 2024, 7 ff.; *Oster*, IPRax 2023, 198, 203.

233 Vgl. EuGH 1.10.2002 – Rs. C-167/00 (*Henkel*) Slg. 2002, I-8111 Rn. 33; EuGH 19.1.1993 – Rs. C-89/91 (*Shearson Lehmann Hutton*) Slg. 1993, I-139 Rn. 23.

234 Musielak/Voit/*Stadler*, ZPO, 22. Aufl. 2025, Vorbem. VDuG Rn. 30; *Thönissen*, EuZW 2023, 637 ff. und 640 für einen eigenen materiell-rechtlichen Anspruch des Verbandes und damit eine auf diesen bezogene Internationale Zuständigkeit; dagegen *Domej*, FS Schack, 2022, 564, 567; *Janal*, GRUR 2023, 985.

Anspruchsdurchsetzung insbesondere der Haftpflicht nach Art. 82 DSGVO zu erreichen, wobei die international-privatrechtliche Dimension hier eine uniforme Durchsetzung womöglich erschweren könnte.[235] Es dürfte gerade bei multiplen Auslandsbezügen eine große Herausforderung für die Sachwalter darstellen, jeweils kollisionsrechtlich zutreffende (Unter)Gruppen entlang des anwendbaren Rechts zu bilden.[236] Unterbleibt aber eine solche – stets komplexe und anspruchsvolle – Differenzierung, wird durch die unterschiedlichen Anforderungen des jeweiligen anwendbaren Rechtes womöglich die Gleichartigkeit i.S.d. § 15 VDuG infrage gestellt, so dass die Unzulässigkeit der Klage droht.[237]

Schließlich ist das auf die Haftung infolge eines Cyber-Incidents – z.B. wegen Datenschutzverstößen – anwendbare Recht nach den für die jeweiligen Rechtsverhältnisse maßgeblichen Kollisionsnormen zu ermitteln. Dies führt zur übergreifenden Frage der kollisionsrechtlichen Anknüpfung der Cyber-Haftpflicht.

III. Kollisionsrecht der Cyber-Haftpflicht

Das cyberversicherte Unternehmen kann infolge eines Cyber-Incidents z.B. durch die fahrlässige Weiterverbreitung des in die eigenen Systeme eingeschleusten Schad-Codes eine erhebliche Zahl von Dritten schädigen. Sind diese geschädigten Zulieferer, Abnehmer, Dienstleister oder sonstigen Geschäftskontakte im Ausland ansässig, führt dies zur Frage, welches Recht auf die Haftpflichtansprüche solcher Dritter anwendbar ist. Die Antwort liefert das Internationale Privatrecht, wobei sich die kollisionsrechtliche Anknüpfung von Schadensersatzansprüchen infolge von Cyber-Attacken unterscheidet, je nachdem, ob es sich bei den Geschädigten um juristische Personen handelt, die sich vertraglicher oder außervertraglicher Haftpflichtansprüche berühmen (**dazu unter 1**) oder, ob natürliche Personen infolge des Cyber-Incidents Schadensersatzansprü-

---

235 Zur grenzüberschreitenden Durchsetzung eingehend *Stadler*, FS Schack, 2022, 499 ff.; *Oster*, IPRax 2023, 198 ff. Vgl. auch *Paal/Kritzer*, NJW 2022, 2433 ff.

236 Statt vieler *Maultzsch,* ZZP 137 (2024), 119, 142 f.

237 Musielak/Voit/*Stadler*, ZPO, 22. Aufl. 2025, Vorbem. VDuG Rn. 31 m.w.N.

che, insbesondere wegen Datenschutzverstößen i.R.d. DSGVO, geltend machen (**hierzu unter 2**). Gerade bei Datenschutzverstößen durch Online-Händler, Airlines, Hotelketten oder Social-Media-Plattformen bilden grenzüberschreitende Sachverhalte mit Auswirkungen in unterschiedlichen Mitgliedstaaten den Regelfall.[238] Damit drängt sich die international-privatrechtliche Frage auf, welches nationale Recht eigentlich in solchen grenzüberschreitenden Konstellationen anzuwenden ist, zumal der unionsrechtlich-autonome Tatbestand des Art. 82 DSGVO keineswegs alle für die Haftpflicht und den Schadensersatz relevanten Fragen regelt. Die kollisionsrechtliche Rechtsanwendungsfrage stellt sich schließlich auch bei der kollektiven Durchsetzung solcher Ansprüche infolge von Cyber-Incidents (**dazu unter 3**).

1. IPR der Cyber-Haftpflicht gegenüber Unternehmen

Die Herausforderungen bei der Ermittlung des auf Haftpflichtansprüche infolge eines Cyber-Vorfalls anwendbaren Rechts beginnen schon bei den maßgeblichen Kollisionsnormen: Denn das Internationale Unionsprivatrecht unter der Rom II-VO ist unanwendbar, sofern der Datenbestand und die Integrität der IT-Infrastruktur von Unternehmen als Aspekte der „Privatsphäre oder der Persönlichkeitsrechte“ i.S.d. Art. 1 Abs. 2 lit. g Rom II-VO einzuordnen wären (**dazu unter a**). Die Rechtsanwendungsfrage stellt sich sodann, wenn der durch einen Cyber-Incident Geschädigte gegenüber dem dafür (mit)verantwortlichen Cyber-Versicherungsnehmer (vor)vertragliche (**dazu unter b**) und/oder deliktische bzw. sonstige spezialgesetzliche außervertragliche Ansprüche (**dazu unter c**) geltend macht. Dabei ist jeweils die Möglichkeit einer Sonderanknüpfung der zu beachtenden Cyber-Sicherheitsstandards im Blick zu behalten (**dazu unter d**).

[238] Vgl. nur EuGH 25.1.2018 – Rs. C-498/16 (*Schrems/Facebook Ireland*) ECLI:EU:C:2018:37.

a) Rom I-VO und Rom II-VO als maßgebliches Kollisionsrechtsregime

Je nach Ausgestaltung der Rechtsverhältnisse mit dem für den Cyber-Incident (mit)verantwortlichen Cyber-Versicherungsnehmer stehen vertragliche oder außervertragliche Haftpflichtansprüche im Vordergrund. Die Qualifikation erfolgt dabei schon angesichts des Vorrangverhältnisses unionsrechtlich-autonom: Maßgeblich ist also nicht das nationale, sondern ein eigenständiges unionales Begriffsverständnis.[239] Ebenso wie im internationalen Zuständigkeitsrecht unter Art. 7 Nr. 1 Brüssel Ia-VO setzt eine vertragliche Qualifikation stets eine „von einer Partei gegenüber einer anderen freiwillig eingegangene Verpflichtung“ voraus.[240] Kann demnach die vertragliche Natur eines Cyber-Haftpflichtanspruchs bejaht werden, sind die Kollisionsnormen der Rom I-VO anwendbar, zumal diese Verordnung in ihrem Art. 1 keine speziellen Ausnahmetatbestände für daten-, IT- oder auch nur (unternehmens)persönlichkeitsrechts-bezogene Schuldverhältnisse vorsieht.[241]

Anders liegt der Fall aber bei der außervertraglichen Haftung infolge eines Cyber-Incidents: Abgrenzungsprobleme ergeben sich hier durch Art. 1 Abs. 2 lit. g Rom II-VO, der außervertragliche Schuldverhältnisse aus der „Verletzung der Privatsphäre oder der Persönlichkeitsrechte“ explizit vom Anwendungsbereich der Verordnung ausnimmt, so dass insoweit das autonome Kollisionsrecht – in Deutschland damit die Art. 40-42 EGBGB – maßgeblich wären. Dies führt zur Frage, ob Art. 1 Abs. 2 lit. g Rom II-VO auch Haftpflichtansprüche von Unternehmen erfasst, die infolge eines Cyber-Vorfalls eine Verletzung der Integrität, Vertraulichkeit und Verfügbarkeit ihrer Daten und IT-Infrastruktur zu beklagen haben. Den Dreh-

---

239 Vgl. nur EuGH 21.1.2016 – verb. Rs. C-359/14 und C-475/14 (*ERGO Insurance und Gjensidige Baltic*) ECLI:EU:C:2016:40 Rn. 43; EuGH 5.9.2024 – Rs. C-86/23 (*HUK COBURG II*) ECLI:EU:C:2024:689 Rn. 38 ff. sowie zur Brüssel Ia-VO z.B. EuGH 16.7.2020 – Rs. C-73/19 (*Belgische Staat*) ECLI:EU:C:2020:568 Rn. 33. Vgl zum Vorrangverhältnis gegenüber dem autonomen deutschen Internationalen Privatrecht auch Art. 3 EGBGB.

240 Vgl. nur EuGH 17.6.1992 – Rs. C-26/91 (*Handte*) Slg. 1992, I-3967 Rn. 15; EuGH 27.10.1998 – Rs. C-51/97 (*Réunion européenne*) Slg. 1998, I-6511 Rn. 17; EuGH 11.11.2020 – Rs. C-433/19 (*Ellmes Property Services*) ECLI:EU:C:2020:900 Rn. 35 ff.

241 Vgl. zu Art. 1 Abs. 2 Rom I-VO und dem Ausnahmekatalog nur Ferrari/*Lüttringhaus*, Concise Commentary on the Rome I Regulation, 2nd ed. 2020, Art. 1 Rome I Rn. 37 ff.

und Angelpunkt bildet das unionsrechtliche Begriffsverständnis von „Privatsphäre“ und „Persönlichkeitsrechten“.

aa) Art. 1 Abs. 2 lit. g Rom II-VO: Bereichsausnahme für Persönlichkeitsdelikte

Blickt man zunächst auf die Gesetzgebungshistorie und den ursprünglichen kompromisshaften Charakter des Art. 1 Abs. 2 lit. g Rom II-VO, so ist diese Bereichsausnahme primär für grenzüberschreitende Persönlichkeitsverletzungen, insbesondere durch die Medien, konzipiert worden, um der je nach Mitgliedstaat sehr unterschiedlichen Gewichtung von Persönlichkeitsschutz einerseits und Presse- und Äußerungsfreiheit andererseits Rechnung zu tragen.[242] Seinem Wortlaut nach nimmt Art. 1 Abs. 2 lit. g Rom II-VO indes ausnahmslos alle Ansprüche wegen Verletzungen „der Privatsphäre“ aus dem Anwendungsbereich von Rom II-VO aus, ohne eine Eingrenzung auf Mediendelikte vorzunehmen. Dies betrifft womöglich auch datenbezogene Haftpflichtansprüche: Zum einen erwähnt die Überprüfungsklausel in Art. 30 Abs. 2 Rom II-VO – in der es gerade um die Untersuchung solcher von der Verordnung ausgeklammerter Bereiche gehen soll – nämlich die EU-Datenschutzrichtlinie und damit den Vorgängerrechtsakt der DSGVO als eine bei der Überprüfung zu betrachtende Materie. Zum anderen hatte die EU-Kommission ursprünglich einen eigenen Tatbestand für alle datenbezogenen Delikte in Art. 6 Rom II-Entwurf vorgesehen und sodann verworfen.[243] Weder die Gesetzgebungshistorie noch der Wortlaut Art. 30 Abs. 2 Rom II-VO können jedoch ein eindeutiges Auslegungsergebnis stützen, weil Art. 6 Rom II-Entwurf gerade unter dem Aspekt von Mediendelikten nicht konsensfähig war und Art. 30 Abs. 2 Rom II-VO lediglich die „Berücksichtigung“ der Rechtsakte zum Datenschutz fordert, ohne klar für oder gegen die

[242] Zu den Hintergründen und der zentralen Rolle der sog. „yellow press“ aus UK statt vieler *R. Wagner*, FS Kropholler, 2008, 715, 720 f.; BeckOGK BGB/*Schulze/Fervers*, 1.8.2021, Art. 30 Rom II-VO Rn. 15 ff.

[243] Vgl. den Kommissionsentwurf v. 22.7.2003, KOM(2003) 427 endg. (2003/0168 (COD)) einerseits und sodann den geänderten Kommissionsentwurf v. 21.2.2006, KOM(2006) 83 endg. (2003/0168 (COD)), andererseits.

Einbeziehung datenbezogener Ansprüche in Rom II-VO zu plädieren.

Orientierung bietet deshalb vorrangig das unionsrechtliche Begriffsverständnis der „Privatsphäre“ und der „Persönlichkeitsrechte“ sowie das Telos der Bereichsausnahme in Art. 1 Abs. 2 lit. g Rom II-VO. Zunächst steht nach der bisherigen Judikatur des EuGH im international-privatrechtlichen Kontext stets der Ehrschutz im Vordergrund: Es geht darum, dass „das Ansehen des Betroffenen … beeinträchtigt worden ist“,[244] und zwar auch dann, wenn die Ehrverletzung mithilfe des Internets begangen und potentiell weltweit verbreitet wird.[245] Gerade im Gefolge dieser Entscheidungslinie im Anschluss an das *Shevill*-Urteil ist auch die Nennung der „Privatsphäre“ und der „Persönlichkeitsrechte“ in der Bereichsausnahme des Art. 1 Abs. 2 lit. g Rom II-VO zu sehen. Während sich dies im Ausgangspunkt auf natürliche Personen bezog, hat der EuGH nunmehr die international-privatrechtliche Dimension des Schutzes des Unternehmenspersönlichkeitsrechts ausgeleuchtet, bei der ebenfalls „die Beeinträchtigung des Ansehens und der Wertschätzung einer juristischen Person durch eine ehrverletzende Veröffentlichung“ und damit der Ehrschutz im Fokus steht.[246]

Allen Fragen des so verstandenen Schutzes der „Privatsphäre“ und der „Persönlichkeitsrechte“ ist gemein, dass hier bei Presse- und Mediendelikten inner- und außerhalb der EU große Unterschiede bei der Gewichtung und Abwägung zwischen Persönlichkeitsschutz einerseits und Presse- und Äußerungsfreiheit andererseits bestehen.[247] Aus diesen divergierenden, zumeist durch nationales Verfassungsrecht grundierten Lösungsansätzen erwächst ein Konflikt, der zugleich die zentrale Begründung für die Existenz des kompro-

---

244 Vgl. zum internationalen Zuständigkeitsrecht grundlegend EuGH 7.3.1995 – Rs. C-68/93 (*Shevill*) ECLI:EU:C:1995:61 Rn. 33. Siehe auch EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 42 ff.

245 Grundlegend EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 42 ff. und 52.

246 Grundlegend EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 17 ff. Siehe auch EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv/DR*) ECLI:EU:C:2021:1036 Rn. 17, 29 ff. und 39.

247 Zu den Hintergründen und der zentralen Rolle der sog. „yellow press“ aus UK statt vieler *R. Wagner*, FS Kropholler, 2008, 715, 720 f.; BeckOGK BGB/*Schulze/Fervers*, 1.8.2021, Art. 30 Rom II-VO Rn. 15 ff.

misshaften Ausschlusstatbestands in Art. 1 Abs. 2 lit. g Rom II-VO ist.

bb) Konfliktlagen nach Art. 1 Abs. 2 lit. g Rom II-VO bei Cyber-Incidents

Im Rahmen einer systematisch-teleologischen Betrachtung des Art. 1 Abs. 2 lit. g Rom II-VO ist zu fragen, ob der soeben skizzierte Konflikt in gleichem Maße auch bei Cyber-Incidents besteht, die *ein Unternehmen* – z.B. durch fahrlässig Schad-Code weiterleitende Mitarbeiter oder wegen eines zu geringen IT-Sicherheitsniveaus – verursacht, und die sodann zu einer Informationssicherheitsverletzung bei *einem anderen Unternehmen* führen. Obgleich Cyber-Vorfälle ein Reputations-Risiko bedeuten mögen, steht bei den Haftpflichtansprüchen des geschädigten Unternehmens keineswegs ein – wie auch immer gearteter – „Ehrschutz" im Vordergrund. Vielmehr wird der Geschädigte die infolge des Cyber-Incidents erlittenen wirtschaftlichen Einbußen, wie z.B. IT-Forensik- und Wiederherstellungskosten sowie Betriebsunterbrechungsschäden geltend machen. Beeinträchtigt wird durch die Informationssicherheitsverletzung i.d.R. die Funktions- und Arbeitsfähigkeit des Unternehmens als solche. Insoweit bedarf es zur Feststellung der Haftpflicht des Schädigers – anders als bei Presse- oder sonstigen (Internet)Medien- oder Äußerungsdelikten – gerade keiner komplexen Abwägung von geschützten Grundrechtspositionen gegeneinander. Anders ausgedrückt ist eine fahrlässige Weiterverbreitung von Schad-Code an Zulieferer nun einmal keine „Meinungsäußerung" oder sonst grundrechtlich – jenseits der allgemeinen Handlungsfreiheit – besonders geschützte Tätigkeit, sondern der Schädiger ist hier dem geschädigten Unternehmen i.d.R. nach dem anwendbaren nationalen allgemeinen Vertrags- und/oder Deliktsrecht haftpflichtig. Daran ändert auch ein etwaiger Zugriff von Hackern auf personenbezogene Daten natürlicher Personen beim geschädigten Unternehmen nichts: Ist das geschädigte Unternehmen seinerseits z.B. gegenüber seinen Geschäftskontakten und/oder Mitarbeitern haftpflichtig – in der EU regelmäßig nach Art. 82 DSGVO –, so kann es sodann gegen das für den Cyber-Incident (mit)verantwortliche Un-

ternehmen i.d.R. nach allgemeinen Regeln des Vertrags- und Deliktsrechts Regress nehmen. Die Durchsetzung solcher Ansprüche erfordert indes keinerlei grundrechtliche Abwägung: Denn es geht auch hier gerade nicht um grundrechtssensible „Mediendelikte", wie man sie bei der Abfassung der Kompromissvorschrift in Art. 1 Abs. 2 lit. g Rom II-VO im Blick hatte, sondern um allgemeine Haftpflichtansprüche.

Das gilt erst recht, soweit die Informationssicherheitsverletzung allein nicht-personenbezogene Unternehmensdaten, Geschäftsgeheimnisse und sonstige (gewerbliche) Schutzrechte des geschädigten Unternehmens betrifft. Insoweit liefert gerade auch die Systematik der Rom II-VO ein besonders tragfähiges Argument: Denn aus Art. 8 Rom II-VO folgt, dass der Unionsgesetzgeber eine Trennlinie zwischen den von der Rom II-VO erfassten unternehmenseigenen Rechtspositionen einerseits und den durch Art. 1 Abs. 2 lit. g Rom II-VO ausgeschlossenen Fällen der „Privatsphäre" und der „Persönlichkeitsrechte" andererseits ziehen möchte: Rechte des geistigen Eigentums, gewerbliche Schutzrechte, aber auch z.B. (gewerblich genutzte) Domain-Namen und Datenbanken werden von Art. 8 und damit dem sachlichen Anwendungsbereich der Rom II-VO umfasst, wobei nach h.M. dazu selbst das unternehmerisch genutzte Urheber- und Erfinderpersönlichkeitsrecht[248] sowie Handelsnamen und geschäftliche Bezeichnungen zählen sollen.[249] Obschon die Vertraulichkeit, Verfügbarkeit und Integrität von Unternehmensdaten und IT-Infrastruktur sowie von Geschäftsgeheimnissen[250] keineswegs zwingend von Art. 8 Rom II-VO erfasste Schutzgüter betrifft, so zeigt diese Norm doch, dass die Rom II-VO nach der Konzeption dieser Verordnung gerade auf den Schutz wirtschaftlich relevanter immaterieller Rechte und Rechtsgüter anwendbar sein soll. Es erscheint vor diesem Hintergrund systematisch-teleologisch konse-

[248] Vgl. OGH GRUR Int 2012, 468.

[249] Statt vieler m.w.N. MünchKommBGB/*Drexl*, 9. Aufl. 2025, Art. 8 Rom II-VO Rn. 179; BeckOK BGB/*Spickhoff,* 73. Ed. 1.8.2024, Art. 8 Rom II-VO Rn. 2 f., die hingegen bestimmte vermögensrechtliche Bestandteile des Persönlichkeitsrechts unter Verweis auf Art. 1 Abs. 2 lit. g Rom II-VO ausklammern.

[250] Den Geschäftsgeheimnisschutz erkennt der EuGH spätestens seit EuGH 14.2.2008 – Rs. C-450/06 (*Varec*) ECLI:EU:C:2008:91 Rn. 49 als einen allgemeinen Grundsatz des Unions (privatrechts) an und verortet diesen tendenziell ebenfalls vermögensrechtlich.

quent, die Haftpflicht infolge von Informationssicherheitsverletzungen – jedenfalls bei Unternehmen als geschädigten Anspruchstellern – der Rom II-VO zu unterstellen und derartige Schuldverhältnisse nicht als solche i.S.d. Art. 1 Abs. 2 lit. g Rom II-VO zu qualifizieren.[251] Dabei kann es keine Rolle spielen, ob sodann eine Anknüpfung nach Art. 8 Rom II-VO oder aber nach anderen Kollisionsnormen von Rom II-VO – und insbesondere der allgemeinen Kollisionsnorm des Art. 4 Rom II-VO – erfolgt: Besonders deutlich wird dies etwa bei der Verletzung des Geschäftsgeheimnisschutzes infolge eines Cyber-Angriffs: Haftpflichtansprüche wegen des Abflusses oder der Offenlegung von zum „know-how" des betroffenen Unternehmens zählenden Daten müssen nämlich aus Sicht der Rom II-VO denknotwenig immer die Hürde des Art. 1 Abs. 2 lit. g Rom II-VO nehmen, gleichviel ob sie sodann nach Art. 8,[252] Art. 6[253] oder aber Art. 4 Rom II-VO[254] anzuknüpfen sind. Das Statut der außervertraglichen Haftung umfasst dann grundsätzlich das Bestehen sowie Inhalt und Umfang des (Schutz)Rechts, die Rechtsinhaberschaft des Verletzten sowie Tatbestand und Rechtsfolgen einer Rechtsverletzung.[255] Besonderheiten bestehen jedoch hinsichtlich des maßgeblichen Cyber-Sicherheitsniveaus, das sowohl für die Verschuldens- als auch für die Mitverschuldensfrage relevant werden kann.[256]

cc) Zwischenergebnis

Festzuhalten bleibt, dass nach der hier vertretenen Ansicht die Kollisionsnormen der Rom II-VO auf Haftpflichtansprüche wegen Informationssicherheitsverletzungen nach einem Cyber-Incident An-

---

[251] Vgl. im Ergebnis ähnlich *Bach* in: Spindler/Schuster, Elektron. Medien, 4. Aufl. 2019, Art. 1 Rom II-VO Rn. 9, der allerdings anhand des Personenbezugs der betroffenen Daten differenzieren möchte. Das kann aber zumindest in der Rückgriffskonstellation eines geschädigten Unternehmens gegen ein für den Cyber-Incident (mit)verantwortliches anders Unternehmen – wie gezeigt – kaum ausschlaggebend für die Bereichsausnahme in Art. 1 Abs. 2 lit. g Rom II-VO sein.

[252] Dafür mit beachtlichen Agrumenten etwa BeckOGK BGB/*McGuire*, 1.7.2023, Art. 8 Rom II-VO Rn. 125 ff.

[253] Siehe nur MünchKommBGB/*Drexl*, 9. Aufl. 2025, Art. 8 Rom II-VO Rn. 3, 171 f.; *Bach* in: Spindler/Schuster, Elektron. Medien, 4. Aufl. 2019, Art. 1 Rom II-VO Rn. 13, dort auch zur Fallgruppe des vorsätzlichen Einschleusens von Malware bei Wettbewerbern zum Zweck der Sabotage.

[254] Vgl. jurisPK-BGB/*Heinze*, 8. Aufl. 2017, Art. 8 Rom II-VO Rn. 26 und 25.

[255] Vgl. mit Blick auf Art. 8 Rom II-VO nur BGH GRUR 2022, 1324 Rn. 14 m.w.N.

[256] Dazu noch eingehend unter IV.

wendung finden. Zu differenzieren ist dann allerdings zwischen Ansprüchen, die bei der Anbahnung oder im Rahmen einer vertraglichen Geschäftsbeziehung geltend gemacht werden, und solchen, die außerhalb einer solchen Sonderverbindung stehen.

b) Kollisionsrechtliche Anknüpfung (vor)vertraglicher Haftpflichtansprüche

Sofern der – z.B. durch Weiterverbreitung von Schad-Code – für eine Informationssicherheitsverletzung bei einem Dritten verantwortliche Cyber-Versicherungsnehmer mit diesem Dritten bereits durch einen Vertrag verbunden ist, bestimmt sich das in Sachverhalten mit Auslandsbezug auf vertragliche Haftpflichtansprüche anwendbare Recht aus der Perspektive eines deutschen Gerichts nach der Rom I-VO.[257] Nach Art. 3 Abs. 1 Rom I-VO unterliegt der Vertrag dem durch die Parteien gewählten Recht,[258] vorbehaltlich der Einschränkungen durch Art. 3 Abs. 3 und Abs. 4 sowie der Art. 9 und Art. 21 Rom I-VO. Eine solche Rechtswahl wird im unternehmerischen Verkehr den Regelfall bilden, so dass die objektiven Anknüpfungen nach Art. 4 ff. Rom I-VO ebenso wie die zugunsten bestimmter Akteure, wie Verbrauchern, Arbeitnehmern und Versicherungsnehmern,[259] bestehenden Einschränkungen an dieser Stelle nicht weiter zu vertiefen sind.

Verursacht der Cyber-Versicherungsnehmer eine Informationssicherheitsverletzung hingegen bereits im Stadium der Anbahnung eines Vertrages mit einem Dritten, ist das auf solche Haftpflichtansprüche anwendbare Recht nicht nach der Rom I-VO, sondern aufgrund der unionsrechtlich-autonomen Qualifikation solcher Rechtsverhältnisse als „außervertraglich“ vielmehr nach der Rom II-VO zu ermitteln: Sofern die Parteien keine Rechtswahl gemäß Art. 14 Rom II-VO getroffen haben, ist nach der Art des betroffenen Interesses zu differenzieren: Die akzessorische Anknüpfung an das – ggf. nur

---

257 Vgl. zum Charakter als *loi universelle*, die auch auf drittstaatliches Recht verweisen kann nur Art. 2 Rom I-VO.

258 Zu den Modalitäten einer solchen (Teil)Rechtswahl statt aller BeckOGK BGB/*Wendland*, 1.9.2022, Art. 3 Rom I-VO Rn. 118 ff.

259 Vgl. nur Art. 6, 7 und Art. 8 Rom I-VO.

hypothetische – Vertragsstatut nach Art. 12 Abs. 1 Rom II-VO ebenso wie die subsidiäre Anknüpfungsleiter des Art. 12 Abs. 2 Rom II-VO erfassen nur den Ausgleich enttäuschter Leistungserwartungen,[260] wohingegen die – z.B. bei der Weiterleitung von Schad-Code üblicherweise gegebene – Verletzung des Integritätsinteresses dem Deliktsstatut unterliegt und nach Art. 4 Rom II-VO anzuknüpfen ist.[261]

c) Kollisionsrechtliche Anknüpfung außervertraglicher Haftpflichtansprüche

Aus der Warte eines international zuständigen deutschen Gerichts sind außervertragliche Haftpflichtansprüche infolge von Informationssicherheitsverletzungen nach der Rom II-VO anzuknüpfen. Das gilt im Ausgangspunkt auch in Konstellationen, in denen die Beteiligten bereits durch eine vertragliche Vereinbarung verbunden sind.[262]

aa) Geringe Relevanz der Rechtswahl nach Art. 14 Rom II-VO

Hier lenkt die Rechtsanwendungsfrage den Blick zuvörderst auf die bereits zwischen Schädiger und Geschädigtem – z.B. in Rahmenverträgen für Lieferbeziehungen oder Dienstleistungen – vereinbarten Rechtswahlklauseln. Zumindest wenn alle Beteiligten einer „kommerziellen Tätigkeit“ i.S.d. Art. 14 Abs. 1 lit. b Rom II-VO nachgehen, können sie auch das auf ihre außervertraglichen Rechtsbeziehungen anwendbare Recht zwar schon vor Eintritt des schadensbegründenden Ereignisses durch eine „frei ausgehandelte

---

260 Nach der Anknüpfungsleiter des Art. 12 Abs. 2 lit. a–c Rom II-VO ist das Erfolgsortrecht maßgeblich, wenn nicht ein gemeinsamer gewöhnlicher Aufenthalt von Schädiger und Geschädigten oder aber im Einzelfall eine offensichtlich engere Verbindung zum Recht eines anderen Staates besteht, vgl. zu den Einzelheiten und Fallgruppen statt vieler BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 12 Rom II-VO Rn. 7 ff.

261 Siehe auch Erwägungsgrund 30 S. 4 Rom II-VO sowie statt vieler BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 12 Rom II-VO Rn. 7 ff.; *Lüttringhaus*, RIW 2008, 193 ff.

262 Vgl. zum potentiellen Zusammentreffen deliktischer und vertraglicher Ansprüche aus zuständigkeitenrechtlicher Perspektive nur EuGH 3.3.2014 – Rs. C-548/12 (*Brogsitter*) ECLI:EU:C:2014:148 Rn. 24 f.; EuGH 24.11.2020 – Rs. C-59/19 (*Wikingerhof*) ECLI:EU:C:2020:950 Rn. 33; BGH NJW 2024, 514 Rn. 17.

Vereinbarung“ wählen.[263] In der Vertragspraxis werden die Rechtswahlklauseln jedoch zum einen nicht immer ausreichend klar auch auf deliktische Ansprüche gemünzt, obschon Art. 14 Abs. 1 S. 2 Rom II-VO entweder eine explizite oder aber mit hinreichender Sicherheit aus den Umständen des Falles ersichtliche Rechtswahl fordert. Vor allem muss zum anderen eine im Vorhinein getroffene Rechtswahl nach Art. 14 Rom II-VO individuell vereinbart werden, wohingegen in der unternehmerischen Praxis zumeist ausschließlich Rechtswahlklauseln in Allgemeinen Geschäftsbedingungen (AGB) verwendet werden. Nach ganz h.M. stellen solche Rechtswahlklauseln in AGB keine „frei ausgehandelte Vereinbarung“ i.S.d. Art. 14 Rom II-VO dar.[264] Deshalb bleibt zur parteiautonomen Bestimmung des auf außervertragliche Schuldverhältnisse anwendbaren Rechts nur eine nach Eintritt des schadensbegründenden Ereignisses getroffene Rechtswahl gemäß Art. 14 Abs. 1 lit. a Rom II-VO. Eine solche Rechtswahl dürfte aber gerade in einer streitig geführten (gerichtlichen) Auseinandersetzung über die Haftpflichtansprüche in der Praxis kaum zwischen den Beteiligten zustande kommen.[265]

bb) Objektive Grundanknüpfung nach Art. 4 Rom II-VO

Damit kommt der objektiven Anknüpfung außervertraglicher Haftpflichtansprüche nach Art. 4 ff. Rom II-VO auch im Rahmen bestehender Vertragsverhältnisse Bedeutung zu. Die Grundanknüpfung nach Art. 4 Abs. 1 Rom II-VO stellt im Unterschied zur internationalzuständigkeitsrechtlichen Regelung des Art. 7 Nr. 2 Brüssel Ia-VO nur auf den Erfolgsort ab: Anwendbar ist also das Recht an dem Ort, wo der Primärschaden eintritt.[266] Dieses Recht erfasst dann auch grundsätzlich alle daraus hervorgehenden Folgeschäden –

---

263 Zu den Modalitäten einer solchen Rechtswahl statt aller BeckOGK BGB/*Rühl*, 1.4.2025, Art. 14 Rom II-VO Rn. 44 ff. und 65 ff.

264 BeckOGK BGB/*Rühl*, 1.4.2025, Art. 14 Rom II-VO Rn. 70 ff. m.w.N.

265 Anders mag der Fall dann liegen, wenn die Parteien durch eine besonders enge und lange Geschäftsbeziehung verbunden und zudem an der Fortführung dieser Geschäftsverbindung interessiert sind.

266 Vgl. Art. 4 Abs. 1 Rom II-VO a.E., wonach das Recht am Primärschadensort anwendbar ist, „unabhängig davon, in welchem Staat das schadensbegründende Ereignis oder indirekte Schadensfolgen eingetreten sind“.

mögen sie auch in anderen Staaten eintreten. Bei Cyber-Delikten besteht indes die besondere Herausforderung, dass Primärschäden potentiell überall auf Welt entstehen können: Denn gemäß Art. 2 Abs. 3 lit. b Rom II-VO ruft schon die bloße Einschleusung von Schad-Code einen eigenen Primärschaden auf jedem befallenen Rechner, Server, IIoT-Gerät oder sonstigen Bestandteil der IT-Infrastruktur hervor, weil nach der Malware-Einschleusung dort ein Schadenseintritt fraglos „wahrscheinlich" i.S.d. Norm ist.[267] Darüber hinaus erfasst die Rom II-VO ausweislich ihres Art. 2 Abs. 2 gerade auch „außervertragliche Schuldverhältnisse, deren Entstehen wahrscheinlich ist". Entsprechend kann an jedem Rechner- und Serverstandort – sowie potentiell auch auf jedem Element von Cloud-Infrastruktur –[268] jeweils ein eigener Erfolgsort bereits dadurch begründet werden, dass Schad-Code dort erfolgreich auf ein Element der IT-Infrastruktur geladen worden ist.

(1) Multiplikation der Erfolgsorte bei Cloud-Computing-Diensten

Die in Art. 2 Abs. 3 lit. b Rom II-VO angelegte Multiplikation der Primär- und damit der Erfolgsorte führt zu nachgerade absurden Ergebnissen beim Einsatz von Cloud-Computing-Diensten: Denn wie bereits im Kontext der internationalen Zuständigkeit ausgeführt,[269] werden hier Datensätze fragmentiert und – je nach Kapazität – in kürzester Zeit an unterschiedlichsten Server-Standorten europa- oder auch weltweit abgelegt. Gelingt es den Angreifern, Daten in der Cloud (z.B. ein Back-Up) ebenfalls zu kompromittieren, dann liegen die weltweit „atomisierten" Erfolgsorte potentiell an allen Serverstandorten des Cloud-Diensteanbieters. Vor allem wäre das dort jeweils anwendbare Recht – der „Mosaiktheorie" des EuGH folgend – nur für die konkret kompromittierten Datenfragmente am jeweiligen Serverstandort maßgeblich.[270] Ähnliche Komplikationen er-

[267] Nach Art. 2 Abs. 3 Rom II-VO gelten „(s)ämtliche Bezugnahmen in dieser Verordnung auf a) ein schadensbegründendes Ereignis … auch für schadensbegründende Ereignisse, deren Eintritt wahrscheinlich ist, und b) einen Schaden … auch für Schäden, deren Eintritt wahrscheinlich ist.".

[268] Dazu sogleich eingehend unter (1).

[269] Siehe erneut oben II 1 c) bb) (2).

[270] Grundlegend dazu wiederum im Kontext der internationalen Zuständigkeit EuGH 7.3.1995 – Rs. C-68/93 (*Shevill*) ECLI:EU:C:1995:61 Rn. 33. Vgl. zu Art. 7 Nr. 2 Brüssel Ia-VO erneut oben II 1 c) bb).

geben sich z.B. auch bei grenzüberschreitend arbeitenden Vertriebs- oder Außendienstmitarbeitern, deren mobile Endgeräte bei internationalen Kunden im Ausland über das Firmennetzwerk kompromittiert werden: Auch an all diesen Orten läge jeweils ein Erfolgsort.

Festzuhalten bleibt, dass das Internationale Deliktsrecht Mühe hat, solche Streuschäden im grenzenlosen Cyber-Space sachgerecht zu erfassen. Dabei erscheint die Mosaikbetrachtung auch und gerade bei den typischerweise durch Cyber-Vorfälle hervorgerufenen Folgeschäden – wie Betriebsunterbrechungen – kaum praktikabel. Denn das Recht am jeweiligen Erfolgsort findet nicht nur auf den dort lokal entstandenen Primärschaden, sondern auch auf die daraus konkret hervorgehenden Folgeschäden Anwendung. Professionelle Angreifer verbreiten indes den Schad-Code üblicherweise erst in der gesamten IT-Infrastruktur des Unternehmens und warten mitunter geduldig – viele Monate und teils sogar mehr als ein Jahr – bis zum finalen Angriff. Schleusen die Angreifer Schad-Code über mehrere Verbreitungswege – beispielsweise über in verschiedenen Staaten ansässige Zulieferer des Angegriffenen – in die IT-Infrastruktur eines Unternehmens ein, so wirken dann potentiell mehrere Primärschäden in unterschiedlichen Staaten zusammen und führen zu einheitlichen Folgeschäden, etwa in Form von Betriebsunterbrechungen. Hier nun mehrere Rechte an den jeweiligen Erfolgsorten nur anteilig auf einen einheitlichen Folgeschaden anzuwenden, erscheint weder sachgerecht noch praktikabel.

(2) Art. 4 Abs. 3 Rom II-VO: Parallele zum „Mittelpunkt des Interesses“ im internationalen Zuständigkeitsrecht

Die dringliche Frage lautet also, wie hier ein solches Mosaik der Rechte vermieden und eine sachgerechte Lösung gefunden werden kann. Abhilfe schafft die Ausweichklausel des Art. 4 Abs. 3 Rom II-VO: Danach kann das Recht des Staates zur Anwendung kommen, mit dem der Sachverhalt eine offensichtlich engere Verbindung aufweist. Das kann wiederum ein zwischen Schädiger und Geschädigtem bestehender Vertrag sein, sofern er enge Bezüge zum Schadensfall aufweist. Das ist ein gangbarer Weg, wenn z.B.

ein Rahmenvertrag zwischen Zulieferer und Hersteller auch den IIoT-Einsatz regelt und letzterer das Einfallstor für die Weiterverbreitung von Schad-Code ist. Auch wenn vertragliche Abreden zur Cyber-Sicherheit entlang der Lieferkette insbesondere im Zuge der Umsetzung der NIS-2-RL beständig zunehmen,[271] lässt sich eine derart klare Verbindung eines Cyber-Incidents zu einem Vertrag wohl nicht immer konstruieren.[272]

Dessen ungeachtet dürfte bei Cyber-Streudelikten ohnehin eine engere Verbindung auch zum Recht am „Mittelpunkt der Interessen" des Geschädigten bestehen: Dies entspricht dem Ansatz des EuGH beim internationalen Deliktsgerichtsstand für Internetdelikte in der *eDate*- und *Svensk Handel*-Entscheidungslinie.[273] Danach soll der Geschädigte seinen gesamten, in aller Welt erlittenen Schaden auch bei den Gerichten am „Mittelpunkt" seines Interesses geltend machen können. Das gilt nach der EuGH-Entscheidung in der Rechtssache *Svensk Handel* auch für Unternehmen: Hier soll für die Zwecke der internationalen Zuständigkeit der Mittelpunkt der Interessen regelmäßig am Hauptsitz des Geschädigten liegen.[274]

Angesichts der ähnlich gelagerten Problematik bei der kollisionsrechtlichen Erfassung von Cyber-Delikten und -Schäden sollte dieser international-zuständigkeitsrechtliche Ansatz auch auf das Kollisionsrecht übertragen werden. Denn das Medium Internet birgt hier jeweils gleichermaßen die Gefahr einer uferlosen Verbreitung der Erfolgsorte. Die Anknüpfung an den Hauptsitz als „Mittelpunkt des Interesses" ist bei Cyber-Vorfällen auch sachgerecht: Dort laufen alle Informationen zum Umfang und zur Art der jeweiligen Cyber-Incidents sowie der hierdurch hervorgerufenen bzw. potentiell noch drohenden Schäden zusammen. Dies folgt wiederum aus dem

---

271 Vgl. dazu nur die unionsrechtlichen Vorgaben in Art. 21 Abs. 2 lit. d, Abs. 3 NIS-2-RL.

272 Vgl. – freilich unter einem anderen Aspekt im Kontext des Art. 7 Nr. 2 Brüssel Ia-VO – nur EuGH 24.11.2020 – Rs. C-59/19 (*Wikingerhof*) ECLI:EU:C:2020:950 Rn. 33 sowie z.B. BGH VersR 2022, 122 Rn. 15 ff.; BGH NJW 2024, 514 Rn. 17.

273 Vgl. EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 30 ff. sowie EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 52 ff.

274 EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 30 ff. Vgl. sodann auch EuGH 17.6.2021 – Rs. C-800/19 (*Mittelbayerischer Verlag*) ECLI:EU:C:2021:489 Rn. 24 ff.; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv/DR*) ECLI:EU:C:2021:1036 Rn. 31 und 39.

durch die BSI-KritisV sowie z.B. künftig die DORA-VO[275] und vor allem die NIS-2-RL für mehr Unternehmen sichtbar normierten Erfordernis einer unternehmensweiten IT-Sicherheitsstrategie und den Reporting-Wegen.[276] Hier kann – muss aber freilich nicht – auch der Ort liegen, an dem (bzw. von dem aus) die durch den Cyber-Incident betroffenen Daten und IT-Systeme schwerpunktmäßig genutzt werden, so dass hier ein Großteil der Schäden eintritt.[277]

In jedem Fall ist der Hauptsitz als „Mittelpunkt der Interessen" auch aus Sicht des Schädigers weitaus vorhersehbarer als die Multiplikation beliebig auf der Welt lokalisierter Erfolgsorte. Denn der Schädiger kann fraglos erkennen, wo sich der Hauptsitz eines geschädigten Geschäftskontakts befindet, nicht aber, wo im Einzelnen die Bausteine seiner IT-Infrastruktur betrieben oder Cloud-Computing-Dienste von Anbietern mit potentiell weltweit verstreuten Servern in Anspruch genommen werden.

In der Summe dürfte dies grundsätzlich eine offensichtlich engere Verbindung i.S.d. Art. 4 Abs. 3 Rom II-VO begründen können, wobei hier freilich eine Einzelfallbetrachtung geboten ist.[278] Festzuhalten bleibt, dass dieser Ansatz zudem einen weitgehenden Gleichlauf von internationaler Zuständigkeit und anwendbarem Recht ermöglicht: Denn die international zuständigen Gerichte am Mittelpunkt des Interesses des Geschädigten können grundsätzlich auch das am dortigen *forum* geltende Recht als Deliktsstatut auf die

---

275 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011, ABl. EU 2022 L 333/1.

276 Auch jenseits der durch die speziellen Cyber-Sicherheitsvorgaben des NIS-2-Regimes oder der BSI-KritisV gebundenen Unternehmen bestehen freilich gesellschaftsrechtliche Vorgaben zur Gewährleistung eines risiko-angemessenen Cyber-Sicherheitsniveaus: So besteht nach § 91 Abs. 2 AktG insbesondere die Pflicht, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

277 Für die kollisionsrechtliche Relevanz des „üblichen Verwendungsortes" gerade bei betroffenen Daten in der Cloud z.B. *Bach* in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Rn. 14; Rauscher/*Pabst*, Europäisches Zivilprozess- und Kollisionsrecht, 5. Aufl. 2023, Art. 4 Rom II-VO Rn. 134a.

278 Generell zurückhaltender aber z.B. Rauscher/*Pabst*, Europäisches Zivilprozess- und Kollisionsrecht, 5. Aufl. 2023, Art. 4 Rom II-VO Rn. 51, wobei der sodann unter Rn. 134a gerade bei Cloud-Diensten befürwortete Rückgriff auf den Ort, „an dem die Daten üblicherweise verwendet werden", zu ähnlichen Ergebnissen führen dürfte.

Haftpflichtansprüche anwenden. Das reduziert für alle Beteiligten die Rechtsermittlungs- und Rechtsanwendungskosten.

cc) Zwischenergebnis

Auch im Internationalen Privatrecht der Cyber-Haftpflicht führt die Grundanknüpfung an den Erfolgsort nach Art. 4 Abs. 1 Rom II-VO potentiell zu einer Multiplikation der anwendbaren Rechte: Gerade beim weit verbreiteten Einsatz von Cloud-Computing-Diensten, aber auch bei weltweit tätigen Vertriebs- und Außendienstmitarbeitern, können Informationssicherheitsverletzungen Geschäftskontakte an zahlreichen Primärschadensorten betreffen. Für das Kollisionsrecht der Cyber-Haftpflicht gegenüber Unternehmen erscheint hier eine Lösung in Parallele zur internationalen Zuständigkeit nach Art. 7 Nr. 2 Brüssel Ia-VO erstrebenswert: Nach den Grundsätzen der *Svensk Handel*-Entscheidung des EuGH sollte eine Konzentration auf das Recht am „Mittelpunkt des Interesses“ des Geschädigten nach Art. 4 Abs. 3 Rom II-VO erfolgen, wobei dies bei betroffenen Unternehmen regelmäßig zu deren Hauptsitz führen dürfte. Hierfür sprechen neben der Vorhersehbarkeit für den Schädiger auch die Sach- und Beweisnähe, weil am Hauptsitz angesichts des Erfordernisses einer unternehmensweiten IT-Sicherheitsstrategie und der Reporting-Wege üblicherweise alle Informationen zu einem Cyber-Incident zusammenlaufen. Darüber hinaus kann so ein weitgehender Gleichlauf von internationaler Zuständigkeit und anwendbarem Recht erreicht werden, was die Rechtsermittlungs- und Rechtsanwendungskosten reduziert und die Rechtdurchsetzung insgesamt beschleunigen und vereinfachen dürfte.

2. IPR der Cyber-Haftpflicht bei DSGVO-Verstößen gegenüber natürlichen Personen

Die Geschäftsmodelle zahlreicher Branchen – vom Online-Marktplatz und Internetversandhandel über Social-Media-Unternehmen bis hin zu internationalen Hotelketten und Fluglinien – beruhen auf dem unmittelbaren Geschäftskontakt mit natürlichen Personen aus

unterschiedlichen Staaten, wobei notwendigerweise umfangreiche personenbezogene Daten verarbeitet werden. Werden solche personenbezogenen Daten nun im Rahmen eines Cyber-Angriffs durch Hacker erbeutet, stellt sich in Sachverhalten mit – gerade bei Airlines und Online-Plattformen multiplen – Auslandsbezügen die Frage, nach welchem Recht die von der Datenschutzverletzung Betroffenen (Schadensersatz)Ansprüche geltend machen können. Der Fokus der nachfolgenden Betrachtungen liegt dabei auf Informationssicherheitsverletzungen, die durch die DSGVO geschützte Daten natürlicher Personen in der EU betreffen, wobei – gerade bei einem internationalen Kundenstamm – auch weitere Rechtsordnungen und damit Datenschutzgesetze berührt sein mögen.

Das auf Haftpflichtansprüche infolge von Datenschutzverstößen anwendbare Recht wird – szenarienbasiert und keineswegs lückenlos – durch Art. 3 DSGVO bestimmt: Hierbei handelt es sich um eine verordnungsautonome einseitige Kollisionsnorm des IPR, obschon Art. 3 DSGVO zugleich auch international-verwaltungsrechtliche und ordnungswidrigkeitenrechtliche Funktionen erfüllt.[279] Dieser Ansatz hat nunmehr als Vorbild für weitere einseitige Kollisionsnormen in Rechtsakten des digitalen Binnenmarktes gedient, wie z.B. Art. 2 Abs. 1 Digital Services Act,[280] Art. 1 Abs. 3 Data Act[281] und Art. 1 Abs. 2 Digital Markets Act,[282] sowie nun auch in Art. 2 Abs. 1 AI Act[283] als einem der zentralen Pfeiler zur Regulierung künstlicher Intelligenz.[284]

---

279 *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 60 ff. und 72 ff.; *Oster*, ZEuP 2021, 275 ff.

280 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, ABl. EU 2022 L 277/1.

281 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13.12.2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828, ABl. EU 2023 L 2023/2854.

282 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14.9.2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828, ABl. EU 20222 L 265/1.

283 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828, ABl. EU 2024 L 2024/1689.

284 Eingehend *Lutzi*, IPRax 2024, 262, 264 ff.; *Hennemann/Steinrötter*, NJW 2024, 1, 8 f.

a) Verweisungsumfang des Art. 3 DSGVO

Soweit die Tatbestandsvoraussetzungen des Art. 3 DSGVO erfüllt sind, führt dies zur Anwendbarkeit des unionsrechtlich-autonomen Schadensersatzanspruchs nach Art. 82 DSGVO. Als spezielle einseitige Kollisionsnorm bleibt Art. 3 DSGVO sodann auch durch das allgemeine internationale Unionsprivatrecht „unberührt", wie Art. 27 Rom II-VO in Bezug auf außervertragliche Schuldverhältnisse ausdrücklich feststellt.[285]

Wird ein Datenverantwortlicher Opfer eines Cyberangriffs, ist auf die Haftung des Angegriffenen immer Art. 82 DSGVO anwendbar, wenn der Angegriffene eine Niederlassung i.S.d. Art. 3 Abs. 1 DSGVO in der EU unterhält oder das Marktortprinzip nach Art. 3 Abs. 2 DSGVO greift. Die DSGVO lässt insoweit keine Parteiautonomie zu. Deshalb ändert z.B. die in AGB oder Nutzungsbedingungen anzutreffende Rechtswahl für alle Haftungsfragen nichts an der Anwendbarkeit des Art. 82 DSGVO.[286]

Damit sind insbesondere auch Unternehmen ohne Hauptsitz in der EU potentiell einer Haftung nach Art. 82 DSGVO ausgesetzt, wenn sie Opfer von Cyber-Angriffen werden und entweder über eine Niederlassung i.S.d. Art. 3 Abs. 1 DSGVO in der EU verfügen oder aber in einer vom Marktortprinzip nach Art. 3 Abs. 2 DSGVO erfassten Weise ihre Tätigkeit auf die EU erstrecken. Soweit Art. 3 DSGVO den räumlich-territorialen Anwendungsbereich der Verordnung eröffnet, unterliegen dann auch die datenschutzrechtlichen Standards – einschließlich des in Art. 5 i.V.m. Art. 24 und Art. 32 DSGVO bezüglich der Cyber-Sicherheit geforderten „Stands der Technik" – grundsätzlich allein dem Unionsrecht. Soweit jedoch nationale Umsetzungs- oder Gestaltungsfreiräume hinsichtlich der Cy-

---

[285] *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 73 ff., wobei die Normen der DSGVO angesichts ihres unbedingten Anwendungsanspruchs wohl auch als Eingriffsnormen qualifiziert und über die entsprechenden Öffnungsklauseln, wie etwa Art. 9 Rom I-VO und Art. 16 Rom II-VO, ungeachtet der allseitigen Kollisionsnormen gemäß dem einseitigen Verweisungsbefehl des Art. 3 DSGVO durchgesetzt werden können, vgl. bereits *de Miguel Asensio*, REDI 69 (2017), 75, 104; Gola/Heckmann/*Piltz*, 3. Aufl. 2022, DS-GVO Art. 3 Rn. 56 ff.

[286] So schon *Piltz*, K&R 2012, 640, 644 f. Siehe auch Gola/Heckmann/*Piltz*, 3. Aufl. 2022, DS-GVO Art. 3 Rn. 56 ff.

ber-Sicherheitsstandards bestehen, erlangt die Frage Bedeutung, welches mitgliedstaatliche Recht insoweit anwendbar ist.[287]

b) Anknüpfung der nicht in Art. 82 DSGVO geregelten Fragen

Durch Art. 3 DSGVO werden indes bei Weitem nicht alle international-privatrechtlichen Fragen erschöpfend beantwortet, die sich im Fall einer grenzüberschreitenden Haftpflicht nach Art. 82 DSGVO stellen können. Denn insbesondere schweigt Art. 82 DSGVO – ebenso wie auch der Rest der Verordnung – zu einer ganzen Reihe von Punkten, die für die Haftpflicht zentral sind. Dies betrifft z.B. ein etwaiges Mitverschulden des Betroffenen sowie die Verjährung.[288] Zudem setzt die Haftung nach Art. 82 DSGVO tatbestandlich voraus, dass der Schaden, „durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde". Dies ist bei Cyber-Angriffen auf einen Datenverantwortlichen, bei denen dann Daten Dritter unter Verstoß gegen die DSGVO erbeutet werden, insbesondere der Fall, wenn der Angegriffene die Cyber-Sicherheitsstandards nach Art. 32, 24 DSGVO nicht einhält.[289] Soweit selbst innerhalb der EU noch divergierende Regelungen bestehen können, wird man in grenzüberschreitenden Konstellationen klären müssen, welche Standards hier ausschlaggebend sind.[290] Hinzu kommt, dass die DSGVO rund 70 Öffnungsklauseln für abweichende mitgliedstaatliche Gestaltungen enthält, die z.B. nach Art. 8 Abs. 1 DSGVO auch die Altersgrenze für die wirksame Einwilligung in die Datenverarbeitung betreffen können. Im haftungsrechtlichen Kontext ebenfalls besonders relevant ist, dass sich die Schadensbemessung i.R.d. Art. 82 DSGVO nach dem nationalen Privatrecht der Mitgliedstaaten richtet: Nach der Rechtsprechung des EuGH in der Rechtssache *Österreichische Post AG* haben

---

287 Vgl. zur Ausfüllung durch nationales Recht nur EuGH 14.12.2023 – Rs. C-340/21 (*Natsionalna agentsia za prihodite*) ECLI:EU:C:2023:986 Rn. 22 ff.

288 Näher *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 75 ff.

289 Art. 32 verlangt „technische und organisatorische" Maßnahmen, die u.a. dem „Stand der Technik" genügen und dazu geeignet sein müssen, „die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen".

290 Siehe dazu noch eingehend unter IV.

„die nationalen Gerichte bei der Festsetzung der Höhe des Schadensersatzes, der aufgrund des in diesem Artikel verankerten Schadensersatzanspruchs geschuldet wird, die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung anzuwenden …, sofern die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden."[291]

In diesen zentralen Punkten bedarf der unionsrechtlich-autonome Schadensersatzanspruch somit notwendig der Ergänzung durch nationales Zivilrecht.[292] In Sachverhalten mit Auslandsbezügen muss deshalb stets das anwendbare mitgliedstaatliche Recht ermittelt werden. Art. 3 DSGVO hilft an dieser Stelle nicht weiter: Diese Norm knüpft nur an Elemente „in der Union" an und kann somit nicht auf das Recht eines konkreten Mitgliedstaats verweisen.[293] Deshalb wird das international zuständige Gericht eines EU-Mitgliedstaats auf sein Kollisionsrecht (*lex fori*) – zu welchem selbstredend auch die europäisch harmonisierten Kollisionsnormen zählen – zurückzugreifen.[294]

aa) Umfang der Bereichsausnahme in Art. 1 Abs. 2 lit. g Rom II-VO

Die Haftung für Verstöße gegen EU-Datenschutzrecht besteht unabhängig von einer freiwillig eingegangenen vertraglichen Verpflichtung. Entsprechend ist sie im Internationalen Unionsprivatrecht außervertraglich zu qualifizieren. Maßgeblich wären somit im Grundsatz die Kollisionsnormen der Rom II-VO. Allerdings nimmt die Rom II-VO in Art. 1 Abs. 2 lit. g alle Ansprüche wegen Verletzungen „der Privatsphäre oder der Persönlichkeitsrechte" aus. Fraglich er-

[291] EuGH 4.5.2023 – Rs. C-300/21 (*Österreichische Post AG*) ECLI:EU:C:2023:370 Rn. 53 f. und Rn. 59; EuGH 21.12.2023 – Rs. C-667/21 (*Krankenversicherung Nordrhein*) ECLI:EU:C:2023:1022 Rn. 83.

[292] EuGH 4.5.2023 – Rs. C-300/21 (*Österreichische Post AG*) ECLI:EU:C:2023:370 Rn. 53 f. und Rn. 59. Deutlich bereits zuvor *Lloyd v Google LLC* [2019] EWCA Civ 1599 (2.10.2019, *Davis* LJ) Rn. 66: „Moreover, user damages are a domestic concept, which might be regarded as a method of assessment of loss and, therefore, properly within the scope of domestic law, even where they are being used to compensate for breach of an EU law right".

[293] *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 75 ff.; *Oster*, ZEuP 2021, 275, 289.

[294] Vgl. wiederum nur Rechtbank Amsterdam 30.6.2021, ECLI:NL:RBAMS:2021:3307 Rn. 8.21.

scheint, ob auch Ansprüche wegen Datenschutzverletzungen infolge von Cyber-Incidents unter diese Ausnahme fallen.

(1) Historisch-teleologische Annäherung

Darunter werden durch die instanzgerichtliche Rechtsprechung und das Schrifttum vielfach auch Haftpflichtansprüche infolge von Datenschutzverstößen gefasst, weil zum einen in Art. 6 Rom II-Entwurf[295] eine spezielle Kollisionsnorm vorgesehen war und zum anderen nun Art. 30 Abs. 2 Rom II-VO neben einer Untersuchung des IPR der Persönlichkeitsrechtsverletzungen auch die „kollisionsrechtlichen Aspekte im Zusammenhang mit der (Datenschutzrichtlinie)[296]“ als Vorgängerrechtsakt der DSGVO „berücksichtig(t)“ wissen will.[297] Wie bereits ausgeführt,[298] sind diese Indizien für sich genommen jedoch jeweils wenig belastbar: Zunächst war Art. 6 Rom II-Entwurf allein unter dem Aspekt von Mediendelikten nicht konsensfähig, während Datenschutzverstöße gar nicht im Mittelpunkt der Debatte standen.[299] Sodann trifft die in Art. 30 Abs. 2 Rom II-VO gewünschte „Berücksichtigung“ von Datenschutzfragen bei der Überprüfung der kollisionsrechtlichen Rechtsentwicklung in den EU-Mitgliedstaaten keine Aussage über den Ein- oder Ausschluss dieser Frage i.R.d. Rom II-VO. Auch aus der auf Grundlage dieser Überprüfungsklausel im Jahr 2021 vorgelegten „Study on the Rome II Regulation“ ergeben sich keinerlei abweichende Anhaltspunkte: Vielmehr widmet sich die gesamte Studie gar nicht dem Kollisionsrecht im Bereich

295 Vgl. den Kommissionsentwurf v. 22.7.2003, KOM(2003) 427 endg. (2003/0168 (COD)).

296 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG 1995 L 281/31.

297 LG Frankfurt 28.6.2019 – 2-03 O 315/17 (juris) Rn. 74; Rechtbank Amsterdam 30.6.2021, ECLI:NL:RBAMS:2021:3307 Rn. 8.21. So schon *Brkan*, EDPLR (2016), 324, 330; *Kohler*, RDIPP 52 (2016), 653, 673f.; *de Miguel Asensio*, REDI 69 (2017), 75, 105. Vgl. auch Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality (Final Report), JLS/2007/C4/028, S. 61 ff.

298 Siehe erneut oben III 1 a).

299 Vgl. wiederum Kommissionsentwurf v. 22.7.2003, KOM(2003) 427 endg. (2003/0168 (COD)) gegenüber Kommissionsentwurf v. 21.2.2006, KOM(2006) 83 endg. (2003/0168 (COD)).

„data protection“ und auch die nationalen Berichte sind insoweit weitgehend unergiebig.[300]

Betrachtet man Art. 1 Abs. 2 lit. g Rom II-VO unter historisch-teleologischen Gesichtspunkten, so ist diese Bereichsausnahme primär für grenzüberschreitende Persönlichkeitsverletzungen, insbesondere durch die Medien, konzipiert worden, um der – je nach Mitgliedstaat – sehr unterschiedlichen Gewichtung von Persönlichkeitsschutz einerseits und Presse- und Äußerungsfreiheit andererseits Rechnung zu tragen.[301] Diese Eingrenzung ist dem Wortlaut des Art. 1 Abs. 2 lit. g Rom II-VO indes nicht zu entnehmen, wenn dort alle Ansprüche aus der Verletzung „der Privatsphäre“ aus dem Anwendungsbereich von Rom II-VO ausgeschlossen werden. In teleologischer Hinsicht spricht entscheidend gegen eine Einbeziehung von Haftpflichtansprüchen wegen Datenschutzverstößen, dass es hier – anders als bei Mediendelikten – gerade nicht um komplexe grundrechtliche Abwägungsfragen geht, wobei die relevanten Grundrechte je nach beteiligtem EU-Mitgliedstaat sehr unterschiedlich gewichtet werden. Dies folgt schon daraus, dass der Unionsgesetzgeber einfachgesetzlich mit der DSGVO einen EU-weit einheitlichen Rahmen für den Datenschutz und damit zugleich für die Verwirklichung, Ausgestaltung und Eingrenzung des unionalen Grundrechts auf Datenschutz nach Art. 8 GRCh geschaffen hat. Es erscheint deshalb in Anbetracht des Telos und der Entstehungsgeschichte des Art. 1 Abs. 2 lit. g Rom II-VO gerade widersinnig, diese Bereichsausnahme auch auf die in zentralen tatbestandlichen Fragen vollharmonisierten und damit in allen Mitgliedstaaten weitgehend gleichförmig laufenden Haftpflichtansprüche für Datenschutzverstöße anzuwenden. Dies gilt in besonderem Maße, als der EuGH im Rahmen von Vorabentscheidungsverfahren selbst jene dem nationalen Recht überlassenen Bereiche der Haftpflicht nach Art. 82 DSGVO, wie z.B. die Schadensbemessung, ebenfalls durch

[300] Siehe jeweils die Fragen Nr. 26 und Nr. 30 und die Antworten der nationalen Berichterstatter in *European Union*, Study on the Rome II Regulation (EC) 864/2007 on the law applicable to non-contractual obligations (JUST/2019/JCOO_FW_CIVI_0167), 2021.

[301] Zu den Hintergründen wiederum statt vieler *R. Wagner*, FS Kropholler, 2008, 715, 720 f.

Anwendung des Äquivalenz- und Effektivitätsgrundsatzes in einen unionsrechtlichen Rahmen fasst.[302]

(2) Verschwimmende Grenzen zwischen Datenschutz und allgemeiner (Produkt)Haftung

Hinzu tritt eine weitere, an der unaufhaltsam voranschreitenden Digitalisierung und damit der Bedeutung von Daten(schutz) ansetzende Überlegung: Würde man jedwede Haftpflicht mit Bezug zu Daten nach Art. 1 Abs. 2 lit. g aus der Rom II-VO ausklammern, so ergeben sich unweigerlich unüberwindbare Abgrenzungsprobleme und möglicherweise auch kollisionsrechtlich sinnwidrige Aufspaltungen einheitlicher Lebens- und Haftungsverhältnisse. Denn wer sich z.B. durch Diebstahl eines Smartphones, Laptops, eines modernen Kfz oder eines sonstigen (persönliche) Daten verarbeitenden Geräts bemächtigt und sich damit deliktisch haftbar macht,[303] kann beim Zugriff auf die darauf gespeicherten persönlichen Daten fraglos dem Sacheigentümer nach Art. 82 DSGVO schadenersatzpflichtig sein. Schließlich schwingt sich der deliktisch Handelnde zum für die Datenverarbeitung i.S.d. Art. 4 Nr. 7 DSGVO „Verantwortlichen“ auf, der sodann den Vorgaben der Art. 5 ff. DSGVO sowie der Haftung nach Art. 82 DSGVO unterworfen ist. Soll in grenzüberschreitenden Sachverhalten dann die Anknüpfung der Ansprüche aus unerlaubter Handlung einerseits und aus datenschutzrechtlicher Haftung andererseits jeweils unterschiedlichen Kollisionsnormen unterstellt werden, weil Art. 1 Abs. 2 lit. g Rom II-VO – vermeintlich – Datenschutzfragen ausklammert? Dies erscheint wenig sachgerecht und in Anbetracht der wachsenden alltäglichen Bedeutung von Daten und Datenverarbeitung durch allerlei Geräte und (Produktions)Prozesse nachgerade aus der Zeit gefallen.

---

302 Vgl. erneut nur EuGH 4.5.2023 – Rs. C-300/21 (*Österreichische Post AG*) ECLI:EU:C:2023:370 Rn. 53 f. und Rn. 59; EuGH 21.12.2023 – Rs. C-667/21 (*Krankenversicherung Nordrhein*) ECLI:EU:C:2023:1022 Rn. 83, wonach „die nationalen Gerichte bei der Festsetzung der Höhe des Schadensersatzes, der aufgrund des in diesem Artikel verankerten Schadensersatzanspruchs geschuldet wird, die innerstaatlichen Vorschriften der einzelnen Mitgliedstaaten über den Umfang der finanziellen Entschädigung anzuwenden haben, sofern die unionsrechtlichen Grundsätze der Äquivalenz und der Effektivität beachtet werden.“.

303 Aus Sicht des deutschen Privatrechts wären deliktische Ansprüche nach § 823 Abs. 1 und Abs. 2 BGB i.V.m. § 242 StGB einschlägig, statt vieler MüchKommBGB/Wagner, 9. Aufl. 2024, § 823 BGB Rn. 302.

Darüber hinaus ist zu bedenken, dass Art. 1 Abs. 2 Rom I-VO keine mit Art. 1 Abs. 2 lit. g Rom II-VO vergleichbare Bereichsausnahme vorsieht. Soweit nun viele mitgliedstaatliche Rechtsordnungen – wie in Deutschland – grundsätzlich eine parallele vertragliche und außervertragliche Haftung für Datenschutzverstöße innerhalb bereits bestehender Vertragsbeziehungen zulassen,[304] läuft die Bereichsausnahme in der Rom II-VO zumeist ohnehin leer: Sind Schädiger (z.B. eine datenverarbeitende Airline) und Geschädigter (z.B. der Fluggast) vertraglich verbunden, werden die vertraglichen Schadensersatzansprüche dem Vertragsstatut gemäß Art. 3 ff. i.V.m. Art. 10 Rom I-VO unterstellt. Damit wird das gleiche Ergebnis erzielt, das auch im Wege der akzessorischen Anknüpfung nach Art. 4 Abs. 3 Rom II-VO erzielt würde. Anders ausgedrückt, gelangt hier dasselbe Recht zur Anwendung, das auch bei der notwendigen Ergänzung des Art. 82 DSGVO um nationale Regelungen – z.B. zur Schadensbemessung –, mithilfe der Rom II-VO anwendbar wäre. Eine solche bestehende vertragliche Verbindung dürfte gerade bei Datenverarbeitungen und entsprechend auch bei DSGVO-Verstößen wohl den Regelfall bilden. Auch insoweit erscheint dann eine abweichende Behandlung konkurrierender vertraglicher und außervertraglicher Haftpflichtansprüche infolge von DSGVO-Verstößen wenig stimmig.

Zu diesen Entwicklungen im allgemeinen Haftungsrecht treten nun auch eindeutig unionsrechtlich fundierte Wertungen hinzu, die für die Einbeziehung von außervertraglichen Ansprüchen wegen DSGVO-Verstößen in das System der Rom II-VO sprechen: Nach der novellierten Produkthaftungs-RL[305] zählen zu den ersatzfähigen Schäden nämlich fortan auch die Vernichtung oder Verfälschung nicht-beruflich genutzter Daten (Art. 6 Abs. 1 lit. c Produkthaftungs-RL). Das für den EU-Binnenmarkt besonders bedeutsame Kollisionsrecht der Produkthaftung ist indes in Art. 5 Rom II-VO unionsrechtlich harmonisiert worden. Sollte hier nun die einheitliche Haf-

[304] Vgl. nur BeckOK DatenschutzR/*Quaas*, 49. Ed. 1.8.2024, Art. 82 DSGVO Rn. 8. Vgl. zum grundsätzlichen *non-cumul* gleichgerichteter vertraglicher und deliktischer Haftpflichtansprüche in Frankreich dagegen z.B. Cass. civ. 1re, 28.6. 2012 – n° 10-28.492.

[305] Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, ABl. L, 2024/2853.

tungsfrage kollisionsrechtlich danach aufgespalten werden, ob derselbe Produktfehler einerseits Schäden an physischen Gegenständen wie Laptops (dann: Anwendung des Art. 5 Rom II-VO) oder aber an den darauf gespeicherten Daten (dann: Ausschluss nach Art. 1 Abs. 2 lit. g Rom II-VO und Anwendung abweichender mitgliedstaatlicher Kollisionsnormen) verursacht? Das erscheint aus der Warte des Unionsrechts sowohl auf Ebene des Kollisions- als auch des Sachrechts sinn- und systemwidrig.

(3) Restriktive Auslegung des Art. 1 Abs. 2 lit. g Rom II-VO

Es spricht vor diesem Hintergrund viel dafür, mit den obigen historisch-teleologischen und systematischen Argumenten die Bereichsausnahme nach Art. 1 Abs. 2 lit. g Rom II-VO zu überwinden und Haftpflichtansprüche infolge von Datenschutzverstößen gemäß Art. 82 DSGVO nach der Rom II-VO und insbesondere nach der allgemeinen Kollisionsnorm des Art. 4 Rom II-VO anzuknüpfen.[306] Maßgeblich wäre dann – vorbehaltlich eines deckungsgleichen gewöhnlichen Aufenthalts der Parteien oder einer z.B. durch einen Vertrag begründeten engeren Verbindung – das Recht des Staates, „in dem der Schaden eintritt, unabhängig davon, in welchem Staat das schadensbegründende Ereignis oder indirekte Schadensfolgen eingetreten sind."[307] Wie dieser Erfolgsort bei Datenschutzverstößen infolge von Cyber-Angriffen zu bestimmen ist, soll sogleich näher beleuchtet werden.[308]

Doch selbst wenn man der hier befürworteten Linie nicht folgen und die Bereichsausnahme des Art. 1 Abs. 2 lit. g Rom II-VO weiter fassen möchte, dürfte der Anwendungsbereich der Rom II-VO eröffnet bleiben, soweit bei einem Cyber-Incident Daten erbeutet werden, die keinen Personenbezug und damit auch keine Verbindung zur

---

306 So – zumindest im Ergebnis – auch Plath/*Becker*, DSGVO/BDSG/TTDSG, 4. Aufl. 2023, Art. 82 DSGVO Rn. 17. Anders indes z.B. OLG Köln MMR 2011, 394, 395; LG Frankfurt 28.6.2019 – 2-03 O 315/17 (juris) Rn. 74; Rechtbank Amsterdam 30.6.2021, ECLI:NL:RBAMS:2021:3307 Rn. 8.21 sowie z.B. *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 76 ff.; *Oster*, ZEuP 2021, 275, 289 ff.; BeckOGK BGB/*Fornasier*, 1.6.2022, Art. 40 EGBGB Rn. 98 ff., dort jeweils m.w.N.

307 Vgl. Art. 4 Abs. 1 Rom II-VO.

308 Dazu im Kontext des – insoweit vergleichbaren – Erfolgsorts nach Art. 40 EGBGB sogleich unter bb).

„Verletzung der Privatsphäre oder der Persönlichkeitsrechte“ aufweisen.[309] In solchen Konstellationen wäre freilich jeweils schon vor dem Hintergrund des Art. 4 Nr. 1 DSGVO kritisch zu prüfen, ob z.B. bei Maschinen-, Gebäude- oder Fahrzeugdaten in Kombination mit weiteren Informationen und unter Verwendung bestimmter Datenverarbeitungssysteme und Techniken (z.B. „KI“) nicht doch wieder ein Personenbezug hergestellt werden kann.[310]

bb) Anknüpfung nach der Rom II-VO

(1) Keine Rechtswahl nach Art. 14 Rom II-VO vor Schadenseintritt bei nicht-kommerzieller Tätigkeit

Die subjektive Anknüpfung nach Art. 14 Rom II-VO spielt gegenüber nicht-kommerziell tätigen natürlichen Personen jedenfalls dann keine nennenswerte Rolle, wenn die Rechtswahl – wie lange Zeit z.B. bei internationalen Social-Media-Plattformen üblich –[311] zum einen in AGB enthalten ist und zum anderen bereits vor Entstehung eines Schadens getroffen wurde: Denn nach Art. 14 Abs. 1 S. 1 lit. b Rom II-VO ist eine anfängliche Rechtswahl allein bei kommerziell tätigen Akteuren durch eine „frei ausgehandelte Vereinbarung“ möglich. Diesen Anforderungen wird nicht genügt, wenn Rechtswahlklauseln in AGB gegenüber Verbrauchern oder anderen nicht-kommerziell handelnden Personen verwendet werden.

---

309 Vgl. im Ergebnis auch *Bach* in: Spindler/Schuster, Elektron. Medien, 4. Aufl. 2019, Art. 1 Rom II-VO Rn. 9. Soweit dort dann auch erwogen wird, Ansprüche wegen „unberechtigten Abrufens oder Abfangens“ von Daten jedenfalls dann Rom II-VO zu unterstellen, wenn die Daten für sich genommen unpersönlich sind, dies etwa bei Passwörtern, PIN oder TAN anzunehmen sei, überzeugt dies nicht: Solche Daten lassen sich gerade i.S.d. Art. 4 Nr. 1 DSGVO individuellen Personen zuordnen (etwa über die IP-Adresse, Gerätekennung, Mobilnummer oder – bei physischen (Kredit)Karten – dort vorhandene Informationen). Zudem haben solche Formen der Informationssicherheitsverletzungen in der Regel gerade das Ziel, Daten wie TAN oder PIN mit bestimmten personenbezogenen Accounts in Verbindung zu bringen.

310 Art. 4 Nr. 1 DSGVO fasst unter personenbezogene Daten nämlich „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die 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“.

311 Vgl. zur Wahl kalifornischen Rechts in älteren Fassungen der Nutzungsbedingungen von Facebook nur *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 55 f. (dort in Fn. 19); *Piltz*, K&R 2012, 640, 644 f. Vgl. auch KG ZD 2014, 412, 416.

(2) Multiplikation der Erfolgsorte bei Cyber-Incidents und Relevanz des „Mittelpunkts der Interessen“ für Art. 4 Abs. 3 Rom II-VO

Nach der objektiven Regelanknüpfung des Art. 4 Abs. 1 Rom II-VO ist grundsätzlich das Recht des Staates anzuwenden, in dem der Schaden eintritt. Dies gilt jedoch nur, soweit Schädiger und Geschädigter keinen gemeinsamen gewöhnlichen Aufenthalt i.S.d. Art. 4 Abs. 2 Rom II-VO haben und sich auch aus der Gesamtheit der Umstände keine offensichtlich engere Verbindung ergibt, wie sie insbesondere durch ein bereits bestehendes Rechtsverhältnis (z.B. einen Vertrag) zwischen den Parteien entstehen kann.[312]

Der Schadens- bzw. Erfolgsort nach Art. 4 Abs. 1 Rom II-VO liegt in dem Staat, in dem die schädigenden Auswirkungen zu Lasten des Betroffenen eintreten, unabhängig davon, in welchem Staat das schadensbegründende Ereignis – und damit der Handlungsort – oder aber indirekte Schadensfolgen lokalisiert sind.[313] Wie bereits ausgeführt, kann dieser sog. Primärschadensort bei Cyber-Incidents potentiell überall auf der Welt liegen: Denn gemäß Art. 2 Abs. 3 lit. b Rom II-VO ruft schon die bloße Einschleusung von Schad-Code einen eigenen Primärschaden auf jedem befallenen Rechner, Server, IIoT-Gerät oder sonstigen Bestandteil der IT-Infrastruktur hervor.[314] Hinzu kommt, dass auch noch nicht materialisierte Schäden erfasst werden, wenn nur „deren Eintritt wahrscheinlich ist“.[315] Entsprechend kann an jedem Rechner- und Serverstandort jeweils ein eigener Erfolgsort bereits dadurch begründet werden, dass Schad-Code dort erfolgreich auf ein Element der IT-Infrastruktur geladen worden ist.[316] Korrespondierend dazu sind infolge von Cyber-Incidents auch Datenschutzverletzungen in diversen Staaten und damit mehrere Erfolgsorte denkbar, etwa wenn der geschädigte Betroffene und/oder der schädigende Datenverantwortliche Computer,

312 Zum Anknüpfungssystem statt vieler BeckOGK BGB/*Rühl*, 1.3.2025, Art. 4 Rom II-VO Rn. 46 ff.
313 Statt vieler BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 4 Rom II-VO Rn. 5 ff.
314 Siehe dazu erneut im Kontext der internationalen Zuständigkeit oben II 1 c) aa) (1) sowie mit Blick auf das Kollisionsrecht oben III 1 c) bb).
315 Vgl. Art. 2 Abs. 3 lit. b Rom II-VO.
316 Vgl. oben II 1 c) aa) (1).

Server, Cloud- oder sonstige IT-Infrastruktur für die Datenverarbeitung verwendet, die in verschiedenen Staaten belegen sind.

Bei solchen Streuschäden sind die jeweiligen Erfolgsorte zwar grundsätzlich gleichrangig und führen wiederum zu einem „Schadens-Mosaik". Wie schon im Kontext der internationalen Zuständigkeit und des allgemeinen Kollisionsrechts ausgeführt,[317] droht dann gerade bei der Nutzung von Cloud-Computing-Diensten eine Multiplikation der Primärschadens- und Erfolgsorte: Einheitliche Datensätze werden hier fragmentiert und – je nach verfügbaren Server-Kapazitäten – in kürzester Zeit an unterschiedlichsten Server-Standorten europa- oder auch weltweit abgelegt. Gelingt es den Angreifern, Daten in der Cloud (z.B. ein Back-Up) ebenfalls zu kompromittieren, dann liegen die jeweiligen Erfolgsorte potentiell an allen Serverstandorten des Cloud-Diensteanbieters. Nach der „Mosaiktheorie" im Gefolge der *Shevill*-Entscheidung des EuGH dürfte allerdings zumindest im Brüssel Ia-VO-System die zuständigkeitsrechtliche Kognitionsbefugnis hier auf den am jeweiligen Erfolgsort eingetretenen Schaden begrenzt sein.[318] Bei der Cloud-Nutzung wäre dann das am jeweiligen Serverstandort nach Art. 4 Abs. 1 Rom II-VO anwendbare Recht für die jeweiligen Datenfragmente maßgeblich.[319] Diese Vervielfältigung der Erfolgsorte erscheint für die Parteien ebenso wie für die Gerichte kaum beherrschbar und zudem eher willkürlich: Die von Rechen- und Speicherkapazitäten abhängige Belegenheit der Datenfragmente lässt sich weder eindeutig voraussehen, noch ist eine fragmentierte Anwendung unterschiedlicher Rechte auf einen einheitlichen Datenschutzverstoß kollisions- oder sachrechtlich sinnvoll. Besonders anschaulich zeigt sich dies z.B. bei der Schadensbemessung.[320]

Nach der hier vertretenen Ansicht sollte der Erfolgsort bei DSGVO-Verstößen infolge von Cyber-Incidents in Anlehnung an die zuständigkeitsrechtlichen Erwägungen des EuGH in der Rechtssache *eDate und Martinez* konzentriert werden können: Eine solche

317 Vgl. wiederum oben II 1 c) aa) (1) und oben III 1 c) bb).
318 Vgl. EuGH 7.3.1995 – Rs. C-68/93 (*Shevill*) ECLI:EU:C:1995:61 Rn. 33.
319 Vgl. erneut oben II 1 c) aa) (1) und oben III 1 c) bb).
320 Vgl. zur Anwendung mitgliedstaatlichen Rechts auf diese Frage erneut nur EuGH 14.12.2023 – Rs. C-340/21 (*Natsionalna agentsia za prihodite*) ECLI:EU:C:2023:986 Rn. 22 ff.

Schwerpunktbetrachtung ermöglicht die Ausweichklausel des Art. 4 Abs. 3 Rom II-VO im Fall einer offensichtlich engeren Verbindung. Letztere besteht nach der hier vertretenen Auffassung stets zum Recht des Staates, an dem der Geschädigte den „Mittelpunkt seiner Interessen" hat: Der infolge einer Cyberattacke Betroffene sollte seinen gesamten Schaden nach dem Erfolgsortrecht des EU-Mitgliedstaates geltend machen können, in dem ebendieser „Mittelpunkt seiner Interessen" liegt.[321] Dieser Interessenschwerpunkt wird bei der Haftung für Datenschutzverstöße in der Regel am gewöhnlichen Aufenthalt des Betroffenen zu lokalisieren sein. Ebendieser Interessensmittelpunkt ist für den Betroffenen und auch wie für den Datenverantwortlichen, der nun Opfer einer Cyberattacke wird, grundsätzlich vorhersehbar. Dieser Lösungsansatz bietet zugleich den Vorzug eines Gleichlaufs von *forum und ius*: Das nach Art. 79 Abs. 2 DSGVO regelmäßig zuständige Gericht am gewöhnlichen Aufenthalt des Betroffenen könnte dann nämlich das dort geltende Recht anwenden.

(3) Ausblick: Produkthaftung für „Daten" nach Art. 6 Abs. 1 lit. c der novellierten Produkthaftungs-RL und Art. 5 Rom II-VO

Nach Art. 6 Abs. 1 lit. c der novellierten Produkthaftungs-RL[322] soll künftig auch die Vernichtung oder Verfälschung nicht-beruflich genutzter Daten einen i.R.d. Produkthaftung ersatzfähigen Schadensposten darstellen. Soweit hierin zugleich ein DSGVO-Verstoß liegt, der einen Schadensersatzanspruch nach Art. 82 DSGVO begründet, wäre für die ergänzende Anwendung mitgliedstaatlichen Rechts (z.B. für die Frage der Schadensbemessung) wohl auf das gegenüber Art. 4 Rom II-VO speziellere kollisionsrechtliche Anknüpfungssystem für die Produkthaftung nach Art. 5 Rom II-VO zurückzugrei-

[321] Vgl. erneut oben III 1 c) bb). Vgl. EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 52 ff. sowie sodann auch EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 30 ff.; EuGH 17.6.2021 – Rs. C-800/19 (*Mittelbayerischer Verlag*) ECLI:EU:C:2021:489 Rn. 24 ff.; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv/DR*) ECLI:EU:C:2021:1036 Rn. 31 und 39. Vgl. auch – freilich ohne Fokus auf Cyber-Incidents – BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 4 Rom II-VO Rn. 11.

[322] Richtlinie (EU) 2024/2853 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, ABl. L, 2024/2853.

fen.[323] Auch i.R.d. sog. Anknüpfungsleiter sollte die hier befürwortete Konzentration[324] auf den „Mittelpunkt der Interessen" des von einer Datenschutzverletzung Betroffenen möglich sein: Sofern nicht auf der ersten „Sprosse" der Anknüpfungsleiter ohnehin das Recht des Staates am gewöhnlichen Aufenthalt des Geschädigten anwendbar ist (Art. 5 Abs. 1 lit. a Rom II-VO), kann jedenfalls mithilfe der an Art. 4 Abs. 3 Rom II-VO angelehnten Ausweichklausel des Art. 5 Abs. 2 Rom II-VO eine offensichtlich engere Verbindung zum Recht des Staates bejaht werden, an dem der Geschädigte den „Mittelpunkt seiner Interessen" hat. Dieser Mittelpunkt dürfte nach der hier vertretenen Auffassung bei Datenschutzverletzungen regelmäßig am gewöhnlichen Aufenthaltsort des Geschädigten zu lokalisieren sein.

cc) Nationales Kollisionsrecht als Auffangordnung

Nach der hier befürworteten restriktiven Auslegung der Bereichsausnahme in Art. 1 Abs. 2 lit. g Rom II-VO kann zur Ergänzung der nicht in Art. 82 DSGVO abschließend geregelten Rechtsfragen auf die unionsrechtlich autonomen Kollisionsnormen der Rom II-VO zurückgegriffen werden, um das jeweils – etwa für die Schadensbemessung – anwendbare mitgliedstaatliche Sachrecht zu ermitteln.[325] Will man mit einigen Stimmen aus dem Schrifttum und aus der instanzgerichtlichen Rechtsprechung Art. 1 Abs. 2 lit. g Rom II-VO jedoch auch auf Datenschutzverstöße erstrecken,[326] müsste insoweit auf das autonome Kollisionsrecht des jeweiligen *forums* zurückgegriffen werden. In Deutschland wären entsprechend die Art. 40 ff. EGBGB maßgeblich.[327] Vorbehaltlich einer nachträglichen Rechtswahl oder eines gemeinsamen gewöhnlichen Aufenthalts der Parteien gemäß Art. 40 Abs. 2 EGBGB kann der Betroffene dann i.R.d.

---

323 Vgl. nur *Müller-Berg*, IPRax 2025, 221, 226 f.

324 Siehe dazu erneut oben (2).

325 Eingehend dazu oben 2 b) aa).

326 Vgl. wiederum nur OLG Köln MMR 2011, 394, 395; LG Frankfurt 28.6.2019 – 2-03 O 315/17 (juris) Rn. 74; Rechtbank Amsterdam 30.6.2021, ECLI:NL:RBAMS:2021:3307 Rn. 8.21. So frühzeitig wiederum *Brkan*, EDPL 2016, 324 ff.; *Kohler*, RDIPP 52 (2016), 653, 673f.; *de Miguel Asensio*, REDI 69 (2017), 75, 105.

327 Näher *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 76 ff.; BeckOGK BGB/*Fornasier* 1.6.2022, Art. 40 EGBGB Rn. 99 ff. m.w.N.

Regelanknüpfung wählen, ob statt des Rechts des Handlungsortes (Art. 40 Abs. 1 S. 1 EGBGB) das des Erfolgsortes (Art. 40 Abs. 1 S. 2 EGBGB) anwendbar sein soll. Dies führt zur Frage, wo diese Orte bei Datenschutzverstößen infolge von Cyberattacken jeweils zu lokalisieren sind.

Während der Ort des jeweilig betroffenen Zielrechners oder -servers zumindest grundsätzlich nicht i.R.d. Art. 40 Abs. 1 S. 1 EGBGB relevant werden dürfte,[328] liegt der Handlungsort bei Cyber-Delikten regelmäßig am „Absendeort", also z.B. am Ort des Einspeisens einer Schadsoftware.[329] Allerdings erscheint bei Datenschutzverletzungen infolge von Cyber-Incidents der konkrete Ort der – mit der DSGVO nicht zu vereinbarenden – Datenverarbeitung aufgrund der weltweiten Übertragbarkeit und häufig technisch auch – z.B. mittels Cloud-Computing-Diensten – ausgelagerten Verarbeitung von Daten ebenfalls eher zufällig und als Handlungsort wenig vorhersehbar.[330] Kollisionsrechtlich relevant ist vielmehr – wie es der EuGH in seiner *Google-Spain*-Entscheidung für das EU-Datenschutzrecht bereits unter der EU-Datenschutz-RL vorgezeichnet hat –,[331] wo über die Zwecke und Mittel der Datenverarbeitung entschieden und davon wirtschaftlich profitiert wird.[332] Entsprechend wird der relevante Handlungsort regelmäßig an der EU-Niederlassung des Verantwortlichen oder des Auftragsverarbeiters liegen, welche die haf-

---

328 BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 40 EGBGB Rn. 43; *Mankowski*, RabelsZ 63 (1999), 203, 265 ff. und 281 f. Eine Ausnahme erscheint allenfalls dann sachgerecht, wenn ein unmittelbarer Cyber-Angreifer sich z.B. Botnetze baut, also Rechner oder auch IoT-Geräte kapert, um dadurch sodann mithilfe dieser dezentral ein anderes Ziel attackieren zu können. Hier können Handlungsorte sehr wohl am Standort der jeweils gekaperten Rechner, Server oder auch z.B. IoT-Geräte lokalisiert werden, die sodann für Angriffe auf weitere Rechner verwendet werden. Der Angreifer ist insoweit auch nicht schutzwürdig, da er sich gezielt die Dezentralität und Ubiquität des Internets für sein Delikt zunutze macht. Er muss damit rechnen, überall dort wo er attackiert, zum einen gerichtspflichtig und zum anderen nach dem Recht des jeweiligen *Handlungsorts* für den gesamten angerichteten Schaden haftbar zu sein. In diese Richtung auch *Mankowski*, RabelsZ 63 (1999), 203, 270 f.: Der Täter „macht sich die Vorteile eines weltweiten Kommunikationsnetzes zunutze ... und weiß das auch". Zumindest im internationalen Kartelldeliktsrecht erkennt auch der EuGH bereits die Möglichkeit mehrerer Handlungsorte an, vgl. EuGH 5.7.2018 – Rs. C-27/17 (*flyLAL*) ECLI:EU:C:2018:533 Rn. 57 und 35, wobei der EuGH hier eine Schwerpunktbetrachtung vornimmt und fragt, welchem Handlungsort „besonders große Bedeutung zukommt".

329 Vgl. nur BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 40 EGBGB Rn. 43 m.w.N.

330 *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 76.

331 Vgl. EuGH 13.5.2014 – Rs. C-131/12 (*Google Spain*) ECLI:EU:C:2014:317 Rn. 50 ff.; EuGH 1.10.2015 – Rs. C-230/14 (*Weltimmo*) ECLI:EU:C:2015:639 Rn. 24 ff.

332 *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 76. Vgl. auch OLG Köln MMR 2011, 394, 395.

tungsbegründende Datenverarbeitung für ihre Tätigkeit veranlasst und ökonomischen Nutzen aus den Daten zieht.[333]

Der Erfolgsort sollte sodann auch i.R.d. Art. 40 Abs. 1 S. 2 EGBGB in Anlehnung an die zuständigkeitsrechtlichen Erwägungen des EuGH in *eDate und Martinez* bestimmt werden: Danach könnte der infolge einer Cyberattacke Betroffene seinen gesamten Schaden nach dem Erfolgsortrecht des EU-Mitgliedstaates geltend machen, in dem der „Mittelpunkt seiner Interessen" liegt. Bei der Haftung für Datenschutzverstöße liegt der Interessenschwerpunkt in der Regel am gewöhnlichen Aufenthalt des Betroffenen. Der so verstandene Interessenmittelpunkt ist für den Betroffenen ebenso wie für den Datenverantwortlichen, der nun Opfer einer Cyberattacke wird, grundsätzlich vorhersehbar. Dieser Lösungsansatz bietet zugleich den Vorzug eines Gleichlaufs von *forum und ius*: Das nach Art. 79 Abs. 2 DSGVO regelmäßig zuständige Gericht am gewöhnlichen Aufenthalt des Betroffenen könnte dann nämlich das dort geltende Recht anwenden.

Allerdings ist i.R.d. Art. 40 Abs. 1 EGBGB zu beachten, dass bei der Anknüpfung an den Handlungsort und – nach wohl vorherrschender, wenn auch nicht unbestrittener Auffassung im Schrifttum – auch bei Anknüpfung an den Erfolgsort grundsätzlich von einer Gesamtverweisung i.S.d. Art. 4 Abs. 1 EGBGB auszugehen ist.[334] Entsprechend wäre stets auch noch das Internationale Privatrecht des Staates am jeweiligen Handlungs- oder Erfolgsort zu beachten, was gerade im Fall von Weiterverweisungen die Ermittlung des anwendbaren Rechts noch komplexer machen kann. Demgegenüber fällt bei der hier befürworteten Anwendung der Rom II-VO diese zusätzliche Ebene an Komplexität weg, weil die unionsrechtlich-autono-

[333] *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 76; BeckOGK BGB/*Fornasier*, 1.6.2022, Art. 40 EGBGB Rn. 102.

[334] Vgl. jeweils m.w.N. nur BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 40 EGBGB Rn. 47; *Bach* in: Spindler/Schuster, Elektron. Medien, 4. Aufl. 2019, Art. 40 EGBGB Rn. 7 f. Differenzierend hingegen BeckOGK BGB/*Fornasier*, 1.6.2022, Art. 40 EGBGB Rn. 159 ff.

men Kollisionsnormen gemäß Art. 24 Rom II-VO eine Sachnormverweisung aussprechen.[335]

c) Zwischenfazit

Der privatrechtliche Haftungstatbestand des Art. 82 DSGVO ist lückenhaft und bedarf hinsichtlich so zentraler Fragen wie Verschuldensmaßstab, Mitverschulden, Verjährung und Schadensbemessung der Ergänzung durch das nationale Privatrecht. Welches nationale Zivilrecht in Sachverhalten mit Auslandsbezügen anwendbar ist, muss anhand des Kollisionsrechts ermittelt werden. Allerdings ist umstritten, ob die Rom II-VO auf Ansprüche infolge von Datenschutzverletzungen anwendbar ist. Die besseren historisch-teleologischen ebenso wie auch systematischen Argumente sprechen hier für eine restriktive Auslegung der Bereichsausnahme in Art. 1 Abs. 2 lit. g Rom II-VO. Nach der hier vertretenen Auffassung sind die nicht in Art. 82 DSGVO geregelten und damit der Ergänzung durch nationales Recht bedürftigen Rechtsfragen nach der Rom II-VO anzuknüpfen. Der Rückgriff auf nationale Kollisionsnormen, wie Art. 40 ff. EGBGB, ist dann entbehrlich.

3. Kollektive Rechtsdurchsetzung und anwendbares Recht

Gerade bei massenhaften Haftpflichtansprüchen infolge eines Cyber-Incidents – etwa bei Datenschutzverstößen, die durch ein zu geringes Cyber-Security-Niveau einer in der EU tätigen Airline oder Hotelkette verursacht werden – liegt eine kollektive Verfolgung solcher Ansprüche nahe. In Ermangelung EU-weit einheitlicher prozessrechtlicher Möglichkeiten zur kollektiven Rechtsdurchsetzung

[335] Zum „Ausschluss der Rück- und Weiterverweisung“ bestimmt Art. 24 Rom II-VO Folgendes: „Unter dem nach dieser Verordnung anzuwendenden Recht eines Staates sind die in diesem Staat geltenden Rechtsnormen unter Ausschluss derjenigen des Internationalen Privatrechts zu verstehen.“.

im Wege einer Verbandsklage[336] und wegen den – nicht zuletzt kollisionsrechtlichen – Herausforderungen bei der Durchsetzung im Wege einer sog. Abhilfeklage[337] kann dann eine Abtretung der Ansprüche zum Zweck der gebündelten Geltendmachung sinnvoll sein (sog. Zessionsmodell),[338] der Art. 80 DSGVO nicht *per se* entgegensteht.[339] In solchen Fällen ist dann zwischen dem auf den Haftpflichtanspruch als „Forderungsstatut" anwendbaren Recht einerseits und dem für die Abtretung nach Art. 14 Abs. 1 Rom I-VO maßgeblichen „Zessionsgrundstatut" andererseits zu differenzieren.[340] Das „Zessionsgrundstatut" unterliegt dabei dem Recht, das nach der Rom I-VO auf den Vertrag zwischen Zedent und Zessionar anzuwenden ist. Im Regelfall wird dies das nach Art. 3 Rom I-VO gewählte Recht sein, wobei freilich die Korrektive nach Art. 3 Abs. 3 und Abs. 4 sowie insbesondere die Sonderanknüpfung nach Art. 6 Rom I-VO zu beachten sind.

Welches Recht auf die – ggf. abzutretenden –Haftpflichtansprüche selbst anwendbar ist, richtet sich zunächst nach den für die jeweilige Anspruchskategorie maßgeblichen Kollisionsnormen.[341] Bleibt

---

336 Art. 80 Abs. 1 DSGVO gestattet zwar grundsätzlich die Durchsetzung von Betroffenenrechten durch qualifizierte Verbände. Ein Verbandsklagerecht sieht die DSGVO damit jedoch nicht vor; vielmehr bedarf es einer gesonderten Regelung im Recht der EU-Mitgliedstaaten. Während der Kommissionsvorschlag für eine Verbandsklage-Richtlinie (Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG, KOM(2018) 184 endg.) in Art. 2 Abs. 1 iVm Anhang I Nr. 53 noch Verbandsklagen zur Durchsetzung der DSGVO vorsah, ist in der EU-Verbandsklage-Richtlinie (Richtlinie (EU) 2020/1828 des Europäischen Parlaments und des Rates vom 25. November 2020 über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher und zur Aufhebung der Richtlinie 2009/22/EG, ABl. 2020 L 409/1) keine entsprechende Regelung mehr enthalten. Vgl. dazu und zur Rechtslage unter dem VuDG erneut oben II 3.

337 Statt vieler *Maultzsch,* ZZP 137 (2024), 119, 142 f.; Musielak/Voit/*Stadler*, ZPO, 22. Aufl. 2025, Vorbem. VDuG Rn. 31 m.w.N.

338 Dabei treten Betroffene ihre Ansprüche – und insbesondere immaterielle Schadensersatzansprüche nach Art. 82 DSGVO – an kommerzielle Kläger ab, die sodann durch eine gebündelte Anspruchsdurchsetzung nicht nur Skaleneffekte, sondern vor allem eine effektive Rechtsverfolgung erzielen können, eingehend *Paal/Kritzer*, NJW 2022, 2433 ff. Zur grenzüberschreitenden Durchsetzung *Stadler*, FS Schack, 2022, 499 ff.

339 Abtretungsverbot verneint durch LG Essen 23.9.2021 – 6 O 190/21, ZD 2022, 50. Ebenso *Paal/Kritzer*, NJW 2022, 2433, 2434.

340 Art. 14 Rom I-VO erfasst dabei auch die Zession von Ansprüchen aus außervertraglichen Schuldverhältnissen, siehe statt vieler BeckOGK BGB/*Hübner*, 1.8.2022, Art. 14 Rom I-VO Rn. 1 ff.; Rauscher/*Freitag*, Europäisches Zivilprozess- und Kollisionsrecht III, 5. Aufl. 2023, Art. 14 Rom I-VO Rn. 1 ff.

341 Vgl. zum Forderungsstatut auch Art. 14 Abs. 2 Rom I-VO.

man beim innerhalb der EU praktisch besonders bedeutsamen Beispiel des Schadensersatzanspruchs für Datenschutzverstöße, so ergeben sich hier angesichts der unionsrechtlich-autonomen Natur des Art. 82 DSGVO zumindest auf den ersten Blick wenig Schwierigkeiten: Im durch Art. 3 DSGVO abgesteckten räumlich-territorialen Anwendungsbereich der Verordnung kommt Anspruchstellern dieser Haftpflichttatbestand stets zugute. Dies gilt angesichts der von Art. 3 Abs. 2 lit. a und b DSGVO erfassten Tatbestände der „Verhaltensbeobachtung in der EU" und dem „Angebot von Waren und Dienstleistungen in der EU" selbst für Drittstaatenangehörige, die sich nur kurz in den EU-Mitgliedstaaten aufhalten.

Allerdings muss in allen nicht durch Art. 82 DSGVO normierten Randbereichen – etwa bei der Verjährung und beim Mitverschulden – das nationale Privatrecht etwaige Lücken füllen.[342] Gleichviel, ob sodann die autonomen Kollisionsnormen der *lex fori* (in Deutschland damit Art. 40 ff. EGBGB) oder aber die Kollisionsnormen der Rom II-VO heranzuziehen sind,[343] können diese auf viele unterschiedliche Rechtsordnungen verweisen, wenn Betroffene aus diversen Mitgliedstaaten ihre Ansprüche mit einer Verbandsklage geltend machen.[344] Diese kollisionsrechtliche „Zersplitterung" kann auch auf die kollektive Rechtsdurchsetzung rückkoppeln: Denn beispielsweise verlangt in Deutschland § 15 Abs. 1 VDuG tatbestandlich gerade die Gleichartigkeit der geltend gemachten Ansprüche, um dem Gericht eine schablonenhafte Prüfung der Anspruchsvoraussetzungen in tatsächlicher und rechtlicher Hinsicht zu ermöglichen.[345] Gerade bei immateriellem Schadensersatz mag man dies schon auf sachrechtlicher und tatsächlicher Ebene hinterfragen. Wenn nun auch noch – und sei es nur für Fragen der Verjährung, des Mitverschuldens und der Schadensbemessung – bei Datenschutzvorfällen mit Betroffenen in vielen unterschiedlichen EU- und

---

342 Vgl. EuGH 14.12.2023 – Rs. C-340/21 (*Natsionalna agentsia za prihodite*) ECLI:EU:C:2023:986 Rn. 22 ff. sowie aus der mitgliedstaatlichen Rechtsprechung nur Rechtbank Amsterdam 30.6.2021, ECLI:NL:RBAMS:2021:3307 Rn. 8.21; LG Frankfurt 28.6.2019 – 2-03 O 315/17 (juris) Rn. 74.

343 Siehe dazu erneut eigehend oben III 2 b).

344 Zu den Herausforderungen statt vieler *Thönissen*, EuZW 2023, 637, 638 f.

345 Kritisch *Pohle/Adelberg*, ZD 2024, 312, 317; *Stadler*, ZZP 136 (2023), 129, 142; *Thönissen*, r+s 2023, 749, 755. Zur Gleichartigkeit allgemein Anders/Gehle/*Schmidt*, ZPO, 82. Aufl. 2024, § 15 VDuG Rn. 2.

Nicht-EU-Staaten dann unterschiedliche nationale Privatrechte die bei Art. 82 DSGVO bestehenden Lücken füllen müssen,[346] so dürfte dies eine schablonenartige Prüfung des Schadensersatzanspruchs nach Art. 82 DSGVO vereiteln.

IV. Haftungsrechtlich maßgebliche Cyber-Sicherheitsstandards in grenzüberschreitenden Fällen

Die Bedeutung von Cyber-Sicherheitsmaßnahmen rückt zunehmend ins Bewusstsein nicht nur von Unternehmen, sondern auch von Gesetzgebern weltweit: In den USA wird auf Bundesebene vor allem die „*Critical Infrastructure Security and Resilience*" vorgegeben,[347] und die einzelnen US-Bundesstaaten erlassen Cybersicherheitsvorschriften für andere Akteure jenseits der kritischen Infrastruktur.[348] Im Vereinigten Königreich existiert – teils als Überleitung und Aktualisierung der NIS-1-RL[349] – ebenfalls ein umfassender gesetzlicher Cybersecurity-Rahmen.[350] Gleiches lässt sich z.B. auch über die Volksrepublik China sagen, wo bereits 2016 ein Cybersicherheitsgesetz verabschiedet worden ist.[351] Auch die Afrikanische Union (AU) hat für ihre Mitgliedstaaten frühzeitig ein Abkommen über Cyber-Sicherheit und Datenschutz aufgesetzt,[352] das allerdings

346 Vgl. erneut nur EuGH 14.12.2023 – Rs. C-340/21 (*Natsionalna agentsia za prihodite*) ECLI:EU:C:2023:986 Rn. 22 ff. sowie statt vieler *Lüttringhaus*, ZVglRWiss 117 (2018), 50, 75 ff.; *Oster*, ZEuP 2021, 275, 289.

347 Vgl. zu den ständig aktualisierten und erweiterten Maßnahmen im Überblick nur *Cybersecurity & Infrastructure Security Agency*, abrufbar unter: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience (zuletzt abgerufen am 1.5.2025).

348 Vgl. z.B. im Bundesstaat New York den *Stop Hacks and Improve Electronic Data Security Act* (SHIELD).

349 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. ABl. 2016 L 194/1.

350 Eingehender Überblick in *House of Commons*, Cybersecurity in the UK: Research Briefing v. 19.4.2024, abrufbar unter: https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf (zuletzt abgerufen am 1.5.2025), S. 43 ff.

351 Vgl. Cybersecurity Law of the People's Republic of China v. 7.11.2016.

352 African Union Convention on Cyber Security and Personal Data Protection, Recital 11, June 27, 2014, A.U. Doc. EX.CL/846 (XXV).

nicht von allen Mitgliedsnationen der AU ratifiziert worden ist.[353] In der EU gleicht nunmehr die NIS-2-RL[354] auf unionsrechtlicher Ebene die Cyber-Sicherheitsstandards für bestimmte besonders relevante Unternehmen und andere Entitäten an. Diese Mindestharmonisierung des Cyber-Sicherheitsrechts in den EU-Mitgliedstaaten führt jedoch keineswegs zu völliger Uniformität.[355] Entsprechend können sich in der EU – zumindest in Randbereichen – beispielsweise die für ein Unternehmen der „kritischen Infrastruktur" maßgeblichen Normen unionsweit durchaus unterscheiden, je nachdem, ob das deutsche BSIG[356] und die Kritis-VO[357] oder aber deren Entsprechungen in anderen Mitgliedstaaten zur Anwendung kommen. In Sachverhalten mit Auslandsbezug treffen somit potentiell diverse Cyber-Sicherheitsstandards aufeinander, die jeweils Anwendung beanspruchen. Das bleibt in grenzüberschreitenden Cyber-Haftpflichtszenarien womöglich nicht ohne Folgen: Hier können sowohl bei außervertraglichen als auch bei vertraglichen Haftungstatbeständen dann die Sicherheitsstandards am Handlungsort zu „berücksichtigen" sein (**dazu unter 1**), soweit dies im Einzelfall angemessen erscheint (**dazu unter 2**). Besonderes Augenmerk verdienen in diesem Zusammenhang drittstaatliche Handlungsorte, Intra-EU-Konstellationen sowie der Eingriffsnormcharakter vieler Cyber-Sicherheitsstandards (**dazu unter 3**).

---

353 Vgl. *AU*, List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, abrufbar unter: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ONCYBERSECURITYAND_PERSONAL_DATA_PROTECTIONO.pdf (zuletzt abgerufen am 1.5.2025).

354 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. EU 2022 L 333/80.

355 Art. 5 NIS-2-RL lautet: „Diese Richtlinie hindert die Mitgliedstaaten nicht daran, Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau gewährleisten, sofern diese Bestimmungen mit den Pflichten der Mitgliedstaaten nach dem Unionsrecht im Einklang stehen".

356 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist. Siehe zur Umsetzung der NIS-2-RL zudem den Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) (Stand: 2.10.2024), BT-Drucks. 20/13184.

357 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 23. Februar 2023 (BGBl. 2023 I Nr. 53) geändert worden ist.

1. Berücksichtigung abweichender Cyber-Sicherheitsstandards am Handlungsort

Während das auf die Haftung anwendbare Recht in der Regel nach der allgemeinen Kollisionsnorm des Art. 4 Rom II-VO zu bestimmen ist und damit – vorbehaltlich vorrangiger Anknüpfungen nach Art. 4 Abs. 3 und Abs. 2 – zum Recht des Erfolgsorts führt,[358] soll nach Art. 17 Rom II-VO den Sicherheitsstandards am Handlungsort des Schädigers Rechnung getragen werden:

> *„Bei der Beurteilung des Verhaltens der Person, deren Haftung geltend gemacht wird, sind faktisch und soweit angemessen die Sicherheits- und Verhaltensregeln zu berücksichtigen, die an dem Ort und zu dem Zeitpunkt des haftungsbegründenden Ereignisses in Kraft sind.“*[359]

Damit können ungeachtet des eigentlichen Deliktsstatuts die Sicherheits- und Verhaltensregeln am Handlungsort zum Zeitpunkt des haftungsbegründenden Ereignisses gerade für die Bewertung von Rechtswidrigkeit und Verschulden berücksichtigt werden.[360] Ist deutsches Sachrecht als *lex causae* anwendbar, so mögen die maßgeblichen Sicherheits- und Verhaltensregeln nicht zuletzt darüber entscheiden, ob ein Schutzgesetz i.S.d. § 823 Abs. 2 BGB i.V.m. Art. 2 EGBGB verletzt ist.[361] Hinzu kommt, dass insbesondere die haftungsrechtliche Beurteilung des Verhaltens des Schädigers von den kollisionsrechtlich anzulegenden IT-Sicherheitsstandards abhängt: Im Fall von sog. Cyber-Distanzdelikten können nämlich der Ort der schädigenden Handlung – d.h. also beispielsweise des Einspeisens oder Weiterleitens von Malware – einerseits und der Standort der schadensstiftenden IT-Infrastruktur andererseits durchaus auseinanderfallen. Hier wäre dann zu fragen, welche konkreten IT-Sicherheitsstandards für die Bewertung des Schädigerhandelns über Art. 17 Rom II-VO maßgeblich sein sollen. Eine weitere Di-

---

358 Vgl. zu Art. 4 Abs. 1 Rom I-VO erneut oben III 1 c) bb).

359 Art. 17 Rom II-VO.

360 Vgl. nur OLG Köln NJW-RR 2020, 847 Rn. 23 ff. Statt vieler Erman/*Stürner*, BGB, 17. Aufl. 2023, Art. 17 Rom II-VO Rn. 3 ff.; *Staudinger* in: Gebauer/Wiedmann, Europäisches Zivilrecht, 3. Aufl. 2021, Art. 17 Rom II-VO Rn. 1.

361 Vgl. jüngst in diese Richtung etwa BGH VersR 2024, 1306 Rn. 13 ff.

mension können solche internationalen Cyber-Haftpflichtszenarien durch grenzüberschreitende Vernetzung von Wertschöpfungs- und Produktionsketten erhalten: Wenn beispielsweise gleich mehrere Zuliefererebenen aus unterschiedlichen Staaten potentiell gleichrangig haftpflichtig sind, so müssen konsequenterweise über Art. 17 Rom II-VO IT-Sicherheitsstandards an den jeweiligen Handlungsorten der Schädiger berücksichtigt werden. Ähnliche Probleme können sich auch auf Seiten des Geschädigten stellen, wenn dessen Mitverschulden zu beurteilen ist: Anerkanntermaßen ist für den Mitverschuldensvorwurf gegenüber einem Geschädigten Art. 17 Rom II-VO (analog) anwendbar.[362] Zu denken wäre etwa an ein in der gesamten EU tätiges deutsches Unternehmen, das aus Gründen der Praktikabilität sein IT-Sicherheitskonzept einheitlich nach dem deutschen IT-Sicherheitsrecht ausrichtet und sodann aber infolge eines durch einen seiner Zulieferer ausgelösten Cyber-Vorfall einen Schaden an seiner finnischen und französischen Niederlassung erleidet: Kann diesem Unternehmen ein Mitverschuldensvorwurf gemacht werden, wenn es das jeweils abweichende – höhere oder auch sachlich-inhaltlich einfach um andere Anforderungen ergänzte – IT-Sicherheitsniveau in Finnland bzw. Frankreich nicht einhält? Dies ist trotz der Angleichung der Cyber-Sicherheitsbestimmungen in der EU keineswegs nur ein theoretisches Szenario, weil nach Art. 5 NIS-2-RL gerade unterschiedliche Regelungsstandards weiterhin zulässig sind.[363]

Während Art. 17 Rom II-VO allein auf die außervertragliche Cyber-Haftpflicht Anwendung findet, können die in grenzüberschreitenden Sachverhalten maßgeblichen IT-Sicherheitsvorschriften durchaus auch in vertraglichen Schuldverhältnissen relevant werden. Zu denken ist beispielsweise an die in internationalen Geschäftsbeziehungen möglichen vertraglichen Haftpflichtszenarien, etwa wenn ein Zulieferer oder Abnehmer Malware entlang der Wertschöpfungsket-

---

362 Vgl. allgemein nur OLG München 15.12.2017 – 10 U 2443/17 (juris) Rn. 5; Erman/*Stürner*, BGB, 17. Aufl. 2023, Art. 17 Rom II-VO Rn. 3 ff.; BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 17 Rom II-VO Rn. 4; *Staudinger* in: Gebauer/Wiedmann, Europäisches Zivilrecht, 3. Aufl. 2021, Art. 17 Rom II-VO Rn. 3; BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 17.

363 Die Norm lautet auszugsweise: „Diese Richtlinie hindert die Mitgliedstaaten nicht daran, Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau gewährleisten…“.

te weiterverbreitet und so seine Vertragspartner schädigt. Auch sofern die Vertragsparteien insoweit vertragliche Abreden getroffen und konkrete Standards vereinbart haben sollten, ist zum einen zu beachten, dass zumindest (international) zwingende IT-Sicherheitsstandards nicht zur Parteidisposition stehen.[364] Darüber hinaus mag sich – in Parallele zur außervertraglichen Sondernorm des Art. 17 Rom II-VO – bei vertraglichen Haftpflichttatbeständen gleichermaßen die Frage stellen, ob IT-Sicherheitsstandards am Sitz des Schädigers womöglich als sog. *local data*[365] sachrechtlich berücksichtigt werden können.[366]

2. Angemessenheit der Berücksichtigung von Sicherheitsstandards jenseits der lex causae

Art. 17 Rom II-VO durchbricht das Prinzip der einheitlichen Anknüpfung des Cyber-Deliktsstatuts, um bei Distanzdelikten zum einen die Interessen von Schädiger und Geschädigtem besser auszutarieren und zum anderen den öffentlichen Interessen des Staates am Handlungsort dadurch Rechnung zu tragen, dass dessen IT-Sicherheitsstandards zumindest „berücksichtigt" werden können.[367] Ein Korrektiv hält jedoch das Angemessenheitserfordernis bereit, das als unbestimmter unionsrechtlicher Rechtsbegriff vorrangig durch die Vorgaben des EU-(Primär)-Rechts mit Inhalt zu füllen ist. In diesem Zusammenhang sind sowohl die primärrechtlichen Grundfreiheiten und das Diskriminierungsverbot des Art. 18 AEUV als auch sämtliche zu deren Konkretisierung ergangenen EU-Sekundärrechtsakte, wie insbesondere Art. 3 E-Commerce-RL[368] und dessen

---

364 Vgl. erneut nur Art. 3 Abs. 3, Abs. 4 und Art. 9 Rom I-VO.

365 Siehe zur Funktion des Art. 17 Rom II-VO und der Sachnähe zur „Datumtheorie" nur BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 17 Rom II-VO Rn. 1; BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 4.

366 Vgl. i.R.v. Vertragsbeziehungen etwa BGH NJW 2019, 3374, 3375 f. Siehe auch *Bach* in: Spindler/Schuster, Elektron. Medien, 4. Aufl. 2019, Art. 40 EGBGB Rn. 9 f.

367 Statt aller BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 5.

368 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl. EG 2000 L 178/1.

deutsche Umsetzung in § 3 TMG, zu beachten.[369] Diese Normen bauen auf das „Herkunftslandsprinzip" im E-Commerce: Online-Händler, die von ihrem Hauptsitz in einem EU-Staat aus in der gesamten EU Waren und Dienste im elektronischen Geschäftsverkehr vertreiben, dürften gemäß Art. 3 E-Commerce-RL prinzipiell keinen strengeren Datenschutz- oder Cyber-Sicherheitsstandards aus anderen EU-Mitgliedstaaten unterworfen werden, als sie das Recht ihres jeweiligen Herkunftsmitgliedstaates vorsieht.[370] Soweit der Anwendungsbereich des Art. 3 E-Commerce-RL eröffnet ist,[371] ist hier eine sachrechtliche Korrektur möglich.[372]

Allerdings dürften derartige Vorgaben des unionalen Primär- und Sekundärrechts keineswegs den Regelfall bilden. Dann ist zu fragen, wie die „Angemessenheit" i.R.d. Art. 17 Rom II-VO bestimmt werden kann. Einige Stimmen im Schrifttum wollen darauf eine pauschale Antwort geben, in dem sie den strengeren – und damit per se „angemessenen" – Sicherheits- und Verhaltensregeln des Handlungsortrechts immer Vorzug vor den weniger strikten Vorgaben der *lex causae* – und damit regelmäßig dem Erfolgsortrecht i.S.d. Art. 4 Abs. 1 Rom II-VO – geben.[373] Demgegenüber seien weniger strenge Sicherheits- und Verhaltensstandards des Hand-

---

369 Vgl. nur *Mankowski* in: Basedow/Hopt/Zimmermann, EurPrivatR-HdWB I, 2009, 825; *Michaels*, FS Kropholler, 2008, 151, 161 ff.

370 Im Ausgangspunkt dürfte Art. 3 E-Commerce-RL auch Cyber-Sicherheits- und Datenschutzbestimmungen einschließen, weil im Anhang dieses Rechtsakts insoweit keine Ausnahme vorgesehen ist. Zu den „Diensten der Informationsgesellschaft" i.S.d. Art. 2 lit. a E-Commerce-RL zählt „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung". Darunter fallen z. B. auch „elektronisch erbrachte Dienstleistungen" und „auf individuellen Abruf eines Empfängers erbrachte Dienstleistungen" durch die Übertragung von Daten. Vgl. zum sog. Herkunftslandsprinzip und zu den Ausnahmen nur Ohly/Sosnitza/*Ohly*, UWG, 8. Aufl. 2023, Einf. Rn. 79 f.; MünchKommLauterkeitsrecht/*Mankowski*, 3. Aufl. 2020, Internationales Wettbewerbs- und Wettbewerbsverfahrensrecht Rn. 38 ff.

371 Zum Ausnahmetatbestand für Verbraucherverträge vgl. nur Art. 3 Abs. 3 i.V.m. Anhang (Ausnahmen), 6. Spiegelstrich E-Commerce-RL. Diese Ausnahme dürfte indes nur für vertragliche Ansprüche, nicht aber bei einer außervertraglichen Qualifikation der Haftung für Datenschutz- bzw. Cyber-Sicherheitsverstöße einschlägig sein, dazu *Heiderhoff* in: Dethloff/Nolte/Reinisch (Hrsg.), Freiheit und Regulierung in der Cyberwelt, 2016, S. 35, 64.

372 Zur Einordnung als Sach- und nicht als Kollisionsnorm EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 60 ff.; BGH GRUR 2017, 397 Rn. 37; BGH GRUR 2012, 830 Rn. 30.

373 BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 75. Vgl. auch *Dornis* in: Basedow/Rühl/Ferrari, Encyclopedia of Private International Law, Bd. II, 2017, 1166, 1171; *Dornis*, Georgia Journal of International & Comparative Law 44 (2016), 305, 335 f.

lungsortrechts nur dann „angemessen“ und zugunsten des Schädigers berücksichtigungsfähig, wenn der Schädiger die grenzüberschreitenden Auswirkungen seines Verhaltens – und damit nicht zuletzt die Überwirkung auf den tatsächlichen Erfolgsort – nicht habe vorhersehen können.[374]

Dieser pauschale Ansatz begegnet gerade im Fall von Cyber-Sicherheitsstandards und Cyber-Haftungsfragen jedoch gewichtigen Bedenken: Die Vernetzung der IT-Infrastruktur folgt regelmäßig der Vernetzung der Wertschöpfungsketten, so dass bei Cyber-Risiken extraterritoriale Auswirkungen schon bei vermeintlich „reinen“ Inlandssachverhalten kaum als unvorhersehbar einzustufen sein dürften. So gehört es zur Realität moderner Datenverarbeitung, dass eine große Bandbreite von Datenspeicherungs- und auch anderen IT-Lösungen „as a service“ mithilfe von Cloud-Systemen im In- und Ausland sichergestellt wird. Weder technisch-tatsächlich noch insbesondere kollisionsrechtlich erscheint es deshalb besonders überzeugend, in solchen Fällen auf die Vorhersehbarkeit grenzüberschreitender Auswirkungen des Tuns am Handlungsort abzustellen.[375] Denn andernfalls müsste die Antwort unisono lauten, dass im Vergleich zur *lex causae* weniger strenge Sicherheits- und Verhaltensstandards des Handlungsortrechts niemals berücksichtigt werden können. Hier erscheint eine deutlich differenziertere Herangehensweise wünschenswert.

3. Drittstaatliche Handlungsorte, Intra-EU-Konstellationen und der Eingriffsnormcharakter von Cyber-Sicherheitsstandards

Inwieweit es „angemessen“ erscheint, abweichende Cyber-Sicherheitsstandards des Handlungsortrechts zu „berücksichtigen“, dürfte aus der Perspektive mitgliedstaatlicher Gerichte zunächst entscheidend davon abhängen, ob sie einerseits mit dem Recht eines Hand-

[374] BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 76; jurisPK-BGB/*Engel*, 10. Aufl. 2023, Art. 17 Rom II-VO Rn. 12.

[375] Vgl. zur Produkthaftung bereits *Wandt*, Internationale Produkthaftung, 1995, Rn. 558 ff.

lungsorts in einem Nicht-EU-Staat (**dazu unter a**) oder aber andererseits mit dem – weitgehend durch EU-Sekundärrecht angeglichenen und damit häufig weitgehend vergleichbaren – Recht eines anderen EU-Mitgliedstaates konfrontiert werden (**dazu unter b**).

a) Cyber-Sicherheitsstandards am Handlungsort in Nicht-EU-Staaten

Bei der „Berücksichtigung" von IT-Standards aus Nicht-EU-Staaten ist zunächst zu beachten, dass der internationale Anwendungsbereich der innerhalb der EU teil-harmonisierten Cyber-Sicherheitsstandards durch die Unionsrechtsakte – insbesondere durch die DSGVO und NIS-2-RL – verbindlich vorgegeben wird: Z.B. verlangt das EU-Datenschutzrecht die Einhaltung aller „technischen und organisatorischen" IT-Sicherheitsvorgaben nach Art. 32, 24 DSGVO immer dann, wenn der Sachverhalt einen in Art. 3 DSGVO beschriebenen Bezug zur EU aufweist.[376] Dieser einseitige Verweisungsbefehl führt damit ausnahmslos und international zwingend zur Anwendung der DSGVO-Standards, ohne dass eine „Berücksichtigung" abweichender Cyber-Sicherheitsstandards an einem Handlungsort außerhalb der EU nach Art. 17 Rom II-VO in Betracht käme.[377] Einen vergleichbaren Ansatz wählt nun auch das novellierte EU-IT-Sicherheitsrecht in Gestalt des Art. 2 Abs. 1 NIS-2-RL: Die Cyber-Risikomanagementmaßnahmen und -sicherheitsstandards sind auf alle „Einrichtungen" anwendbar, die „ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben". Entsprechend müssen in solchen Konstellationen immer die der NIS-2-RL-Umsetzung dienenden Cyber-Sicherheitsstandards eines EU-Mitgliedstaates angewendet werden (seien es solche des Forum- oder des Erfolgsort-Staates). Damit ist zugleich der Weg über Art. 17 Rom II-VO vollständig versperrt, weil IT-Sicherheitsstandards, die an einem Handlungsort in einem Nicht-EU-Staat gelten, nicht auf den unionsrechtlichen Vorgaben der NIS-2-RL beruhen.

[376] Eingehend dazu Lüttringhaus ZVglRWiss 117 (2018), 50, 60 ff.
[377] Vgl. erneut nur Lüttringhaus ZVglRWiss 117 (2018), 50, 72 ff.

Raum für die „Berücksichtigung“ drittstaatlicher Sicherheitsstandards nach Art. 17 Rom II-VO bleibt damit allenfalls in Regelungsbereichen, für die das EU-Cyber-Sicherheitsrecht weder in der DSGVO- und der NIS-2-RL noch überhaupt in anderen Rechtsakten unionsrechtliche Vorgaben trifft. Zu denken ist in diesem Zusammenhang beispielsweise an Unternehmen, die aus dem sachlich-persönlichen Anwendungsbereich der NIS-2-RL und/oder der DSGVO herausfallen. Gleichviel, ob drittstaatliche Cyber-Sicherheitsstandards über Art. 17 Rom II-VO oder aber in vertraglichen Haftungsbeziehungen als *local data* berücksichtigt werden sollen, gilt es im Blick zu behalten, dass derartige Sicherheitsvorschriften in der Regel als Eingriffsnormen gemäß Art. 16 Rom II-VO bzw. Art. 9 Abs. 1 Rom I-VO zu qualifizieren sind. Art. 17 Rom II-VO erscheint vor diesem Hintergrund als eine spezielle Regelung für eingriffsrechtliche Sicherheitsstandards am Handlungsort.[378] Allerdings ist der Weg über Art. 17 Rom II-VO in dieser Konstellation voller Hürden: Denn auch bei den Cyber-Sicherheitsstandards der *lex fori* handelt es sich um Eingriffsnormen, die in außervertraglichen Schuldverhältnisses über Art. 16 Rom II-VO und in vertraglichen Haftpflichtszenarien über Art. 9 Abs. 2 Rom I-VO durch den Gerichtsstaat durchgesetzt werden können. Anders gewendet, trifft hier also die Eingriffsnorm eines Nicht-EU-Staates auf eine solche des Forumstaates. Es erscheint sehr zweifelhaft, dass ein mitgliedstaatliches Gericht nun fremde und noch dazu drittstaatliche IT-Sicherheitsstandards des Handlungsortrechts vorrangig über Art. 17 Rom II-VO „berücksichtigt“ und damit zugleich das heimische Cyber-Sicherheitsrecht verdrängt. Ungeachtet dessen, dass Art. 17 eine gegenüber Art. 16 Rom II-VO speziellere Vorschrift sein dürfte,[379] liegt es in der Praxis nahe, dass das Forum hier den forumseigenen IT-Sicherheitsstandards den Vorzug gibt, etwa unter Verweis auf die (vermeintlich) fehlende „Angemessenheit“ i.R.d. Art. 17 Rom II-VO. Ein solches „Heimwärtsstreben“ ist dem internationalen Entscheidungseinklang bei Cyber-Haftpflichtansprüchen allerdings wenig förderlich.

---

[378] Vgl. BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 87 ff. und Art. 16 Rom II-VO Rn. 35 ff.

[379] Dafür BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 17 Rom II-VO Rn. 2; BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 87.

Zusammenfassend ist festzuhalten, dass unter diesen Vorzeichen kaum praktische Anwendungsfälle denkbar sind, in denen forumsfremde IT-Sicherheitsstandards über Art. 17 Rom II-VO oder – in vertraglichen Cyber-Haftpflichtszenarien – als sog. *local data* berücksichtigt werden können: Diese „Berücksichtigung" erscheint allenfalls dort realistisch, wo weder unionsrechtliche Vorgaben die zwingende Anwendung (teil)harmonisierter Sicherheitsstandards eines EU-Mitgliedstaates gebieten noch der Anwendungsbereich der eingriffsrechtlichen Cyber-Sicherheitsnormen der *lex fori* eröffnet ist.

b) Intra-EU-Konstellationen

Der Raum für den Rückgriff auf Art. 17 Rom II-VO bzw. die allgemeinen Grundsätze der Berücksichtigung von *local data* ist jedoch deutlich größer, wenn es um „Intra-EU-Sachverhalte" geht, die nur Bezüge zu EU-Mitgliedstaaten aufweisen. Zu denken ist etwa an eine Konstellation, in welcher der ungewollt Schad-Code verbreitende Schädiger zwar die IT-Sicherheitsvorgaben an seinem Handlungsort in EU-Mitgliedstaat A, nicht aber jene am Erfolgsort in EU-Mitgliedstaat B einhält. Hier ist zu fragen, welche Cyber-Sicherheitsstandards im Einzelfall maßgeblich und ggf. über Art. 17 Rom II-VO berücksichtigungsfähig sind. Anders gewendet, bedarf es für derartige „Intra-EU-Konstellationen" also womöglich eines „Binnenkollisionsrechts", das darüber entscheidet, welches der – angesichts der unionalen (Teil)Harmonisierung dieser Materie zumindest im Ausgangspunkt gleichwertigen – nationalen Cyber-Sicherheitsrechte der EU-Mitgliedstaaten zur Anwendung berufen sein soll. Allerdings bestehen trotz der weitgehenden Angleichung durch das NIS-2-Regelungssystem zwischen den mitgliedstaatlichen Rechtsordnungen insoweit immer noch Unterschiede, zumal Art. 5 NIS-2-RL nur eine Mindestharmonisierung vorgibt und damit strengere nationale Vorschriften in den EU-Mitgliedstaaten weiterhin zulässt. Hinzu kommt, dass die überwiegende Mehrzahl der in der EU tätigen Unternehmen schon aufgrund ihrer Größe und/oder ihrer Branchenzugehörigkeit von vornherein nicht in den sachlich-persönlichen Anwendungsbereich des NIS-2-Regelungssystems fallen und

damit nur den mitgliedstaatlichen Vorschriften unterliegen. Auch die DSGVO sieht ihrerseits zahlreiche Öffnungsklauseln für mitgliedstaatliche Gestaltungen vor. Derartige Divergenzen zwischen den jeweiligen nationalen Sicherheitsstandards mögen dann aber dazu führen, dass der Schädiger zwar das an seinem Handlungsort (Mitgliedstaat A), nicht aber das im Mitgliedstaat B als Erfolgsort maßgebliche Cyber-Sicherheitsniveau einhält, wo sodann infolge eines von ihm – z.B. durch Weiterverbreitung von Malware – verursachten Cyber-Incidents Informationssicherheitsverletzungen und Schäden eintreten. Die Regelanknüpfung des Art. 4 Abs. 1 Rom II-VO würde zur Anwendung des Erfolgsortrechts im Mitgliedstaat B führen, das grundsätzlich gemäß Art- 15 lit. a) Rom II-VO auch „den Grund und den Umfang der Haftung" und somit die maßgeblichen Verhaltens- und IT-Sicherheitsstandards beherrscht. Allerdings könnten über Art. 17 Rom II-VO womöglich die Cyber-Sicherheitsstandards am Handlungsort in Staat A berücksichtigt werden, ohne dass dies z.B. den unionalen Vorgaben in der NIS-2-RL oder der DSGVO zuwiderliefe: Denn – u.a. im Fall der Ausübung von Tätigkeiten „in der Union" – geben sowohl Art. 2 Abs. 1 NIS-2-RL als auch Art. 3 DSGVO jeweils nur die Anwendung der sekundärrechtlichen Regelungsniveaus vor, ohne damit vorzugeben, welches nationale IT-Sicherheitsrecht in Sachverhalten mit Bezügen zu zwei oder mehr EU-Mitgliedstaaten maßgeblich sein soll. Insoweit bleiben diese Unionsrechtsakte vielmehr indifferent: Solange in Intra-EU-Konstellationen nur die Einhaltung des unionsrechtlich vorgegebenen (Mindest) Cyber-Sicherheitsniveaus gemäß der NIS-2-RL bzw. der DSGVO gewährleistet ist, erscheint damit ein Rückgriff auf Art. 17 Rom II-VO möglich.[380] Aus der Perspektive des Unionsrechts besehen, ist dies gerade deshalb hinnehmbar, weil sowohl das Datenschutz- als auch das Cyber-Sicherheitsrecht durch die DSGVO bzw. die NIS-2-RL sehr weitgehend angeglichen worden ist und – zumindest bei unionsrechtskonformer Ausgestaltung und nicht zuletzt auch durch die durch den EU-Effektivitätsgrundsatz determinierte Anwendung des nationalen Rechts – damit keine grundlegenden Abweichungen von den unionalen Werten zu befürchten sind. Auch aus der Warte des

[380] Dies steht gerade bei Datenschutzverstößen freilich unter dem Vorbehalt, dass die Ausnahme des Art. 1 Abs. 2 lit. g Rom II-VO nicht eingreift, siehe dazu eingehend oben III 1 a) aa).

jeweiligen mitgliedstaatlichen Rechts und Forums betrachtet, dürften hier deutlich weniger Friktionen drohen: Gerade angesichts der Teil-Harmonisierung und des Interessengleichlaufs mag es für den Forum-Staat deutlich leichter hinnehmbar sein, sein öffentliches Interesse an der Durchsetzung seines die DSGVO bzw. die NIS-2-RL übererfüllenden – und damit strengeren – IT-Sicherheitsrechts zurückzustellen, und über Art. 17 Rom II-VO stattdessen die großzügigeren, aber immer noch unionsrechtskonformen Standards anderer EU-Mitgliedstaaten zu „berücksichtigen". Für diese Lösung spricht, dass es zumindest i.S.d. Art. 17 Rom II-VO schwerlich begründbar erscheint, ein unionsrechtskonformes Regelungsniveau per se als nicht „angemessen" zu bewerten.

Allerdings handelt es sich auch bei den das Regelungsniveau der NIS-2-RL übererfüllenden (oder etwaige Gestaltungsspielräume der DSGVO nutzenden) mitgliedstaatlichen Regelungen regelmäßig um Eingriffsnormen i.S.d. Art. 9 Abs. 1 Rom I-VO und Art. 16 Rom II-VO.[381] Das führt zur Frage, ob mitgliedstaatliche Gerichte entsprechend ihre strengere *lex fori* stets anwenden und so den Weg über Art. 17 Rom II-VO zu den unionsrechtlich (mindest)harmonisierten Cyber-Sicherheitsstandards am Handlungsort in einem anderen EU-Mitgliedstaat verbauen können. In seinen *Unamar*- und *HUK COBURG II*-Entscheidungen hat der EuGH zwar grundsätzlich die Anwendung auch solcher Eingriffsnormen der *lex fori* gebilligt, durch die ein unionsrechtlich vorgegebenes Regelungsniveau übererfüllt wird.[382] Prägnant führt der EuGH in der Rechtssache *HUK COBURG II* aus,

> *„dass nach der Rechtsprechung des Gerichtshofs das Recht eines Mitgliedstaats, das den durch eine Richtlinie vorgeschriebenen Mindestschutz gewährt, zugunsten der lex fori wegen deren zwingenden Charakters unangewendet gelassen werden kann, wenn das angerufene Gericht nach eingehender Prüfung feststellt, dass der Gesetzgeber des Mitgliedstaats dieses Ge-*

[381] Vgl. dazu BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 17 Rom II-VO Rn. 87 ff. und Art. 16 Rom II-VO Rn. 35 ff.

[382] EuGH 17.10.2013 – Rs. C-184/12 (*Unamar*) ECLI:EU:C:2013:663 Rn. 50 ff.; EuGH 5.9.2024 – Rs. C-86/23 (*HUK COBURG II*) ECLI:EU:C:2024:689 Rn. 54 ff.

richts es im Rahmen der Umsetzung dieser Richtlinie für entscheidend erachtet hat, der betroffenen Person in seiner Rechtsordnung einen Schutz zu gewähren, der über den hinausgeht, der in der genannten Richtlinie vorgesehen ist, und dabei die Natur und den Gegenstand solcher zwingenden Vorschriften berücksichtigt".[383]

Allerdings gab der EuGH mit Blick auf die Handelsvertreter-RL schon in der Rechtssache *Unamar* aber zu bedenken, dass das anzuwendende Recht

„das eines anderen Mitgliedstaats wäre, der nach Ansicht aller Beteiligten sowie des vorlegenden Gerichts die Richtlinie … korrekt umgesetzt hat."[384]

Das lässt sich als Aufforderung verstehen, bei der Durchsetzung der Eingriffsnormen der *lex fori* jedenfalls dann größtmögliche Zurückhaltung zu üben, wenn das Recht eines anderen EU-Mitgliedstaates mit einem unionsrechtskonformen Regelungsniveau zuR Anwendung kommt.[385] Diese grundsätzliche Wertung sollte auch i.R.d. Art. 17 Rom II-VO beachtet werden: Soweit das mitgliedstaatliche Recht am Handlungsort des Schädiger das unionsrechtlich – z.B. durch die NIS-2-RL und die DSGVO – geforderte IT-Sicherheitsniveau einhält, können ebendiese Standards aus Sicht des Unionsrechts als „angemessen" i.S.d. Art. 17 Rom II-VO bewertet und damit auch grundsätzlich „berücksichtigt" werden. Es bleibt in der Cyber-Haftpflichtpraxis jedoch abzuwarten, inwieweit sich die Gerichte in den Mitgliedstaaten dieser Sichtweise anschließen und über Art. 17 Rom II-VO nicht nur die Interessen von Schädiger und Geschädigtem austarieren, sondern zugleich auch die öffentlichen Interessen des Forum-Staates an der Durchsetzung eigener IT-Sicherheitsstandards zurückzustellen. Gerade weil die Ermittlung und „Berücksichtigung" ausländischen Rechts immer einen gewis-

[383] Indes kommt der EuGH in HUK COBURG II sodann zu dem Ergebnis, dass weder ein von der Richtlinie harmonisierter Bereich noch überhaupt eine nach Art. 16 Rom II-VO im Wege der Sonderanknüpfung durchsetzungsfähige Eingriffsnorm vorliegen dürfte, EuGH 5.9.2024 – Rs. C-86/23 (*HUK COBURG II*) ECLI:EU:C:2024:689 Rn. 54 ff.

[384] EuGH 17.10.2013 – Rs. C-184/12 (*Unamar*) ECLI:EU:C:2013:663 Rn. 51.

[385] EuGH 17.10.2013 – Rs. C-184/12 (*Unamar*) ECLI:EU:C:2013:663 Rn. 51.

sen Aufwand bedeutet, mögen manche Gerichte versucht sein, direkt das eigene Cyber-Sicherheitsrecht des Forumstaates – sei es als *lex causae*, sei es als Eingriffsnormen – zur Anwendung zu bringen.

4. Zwischenfazit

Bei der grenzüberschreitenden Haftung infolge von Cyber-Vorfällen, die durch die Nichteinhaltung von IT-Sicherheitsstandards verursacht werden, kann es in gewissem, unionsrechtlich vorgezeichnetem Rahmen durchaus zu einem „Rechtsmix" kommen: Nach Art. 17 Rom II-VO können grundsätzlich die „Sicherheits- und Verhaltensregeln" am Handlungsort des Schädigers zu berücksichtigen sein. Darüber hinaus könnten auch in vertraglichen Schuldverhältnissen sowie bei der Frage eines etwaigen Mitverschuldens des Geschädigten die jeweiligen lokalen Cyber-Sicherheitsstandards grundsätzlich (analog Art. 17 Rom II-VO) als *local data* herangezogen werden.

Der Anwendungsbereich des Art. 17 Rom II-VO wird indes vor allem durch unionsrechtliche Vorgaben und insbesondere durch den in Art. 3 DSGVO und in Art. 2 Abs. 1 NIS-2-RL abgesteckten räumlich-territorialen Anwendungsbereich der EU-Cyber-Sicherheitsstandards begrenzt. Dies steht einer „Berücksichtigung" drittstaatlicher Standards an einem Handlungsort außerhalb der EU über Art. 17 Rom II-VO entgegen, zumal viele mitgliedstaatliche Cyber-Sicherheitsstandards auch als Eingriffsnormen zu qualifizieren sein dürften.

Zumindest grundsätzlich bleibt ein ergänzender Rückgriff auf Art. 17 Rom II-VO in Intra-EU-Konstellationen möglich, soweit hier jedenfalls die Einhaltung des unionsrechtlich vorgegebenen (Mindest) Cyber-Sicherheitsniveaus gewährleistet ist: Durch die (Teil)Harmonisierung in diesem Bereich durch die DSGVO bzw. die NIS-2-RL haben sich die mitgliedstaatlichen Cyber-Sicherheitsstandards zumindest stark angenähert. Orientierung bieten insoweit auch die Rechtssachen *Unamar* und *HUK COBURG II*, wenngleich der

EuGH es einem EU-Mitgliedstaat nicht verwehrt, sein EU-Richtlinien- bzw. EU-Verordnungsvorgaben übertreffendes Recht gegenüber den großzügigeren Standards anderer EU-Mitgliedstaaten durchzusetzen.[386]

V. Ergebnis

Wer sich im Cyberspace bewegt, läuft Gefahr, sich Dritten gegenüber haftpflichtig zu machen: Zu denken ist beispielsweise an Szenarien, in denen Angreifer ein Unternehmen mit Malware attackieren und das Unternehmen den Schad-Code sodann in haftungsrelevanter Weise an seine Zulieferer, Abnehmer oder auch an unbeteiligte Dritte weiterleitet und diese dadurch schädigt. Aus Sicht des unionalen ebenso wie des deutschen Rechts kommen als haftungsbegründende Normen neben (vor)vertraglichen und deliktischen auch eine Reihe spezialgesetzlicher Tatbestände, wie Art. 82 DSGVO und § 10 GeschGehG, in Betracht. Viele Unternehmen haben ihre Wertschöpfungsketten grenzüberschreitend vernetzt, so dass auch die Haftungsverhältnisse dem Recht unterschiedlicher ausländischer Staaten unterliegen können. Welches Recht im Einzelfall anwendbar und welches Gericht für Haftpflichtstreitigkeiten international zuständig ist, bestimmt das internationale Privat- und Zuständigkeitsrecht. Besondere Herausforderungen ergeben sich hier jeweils daraus, dass bei Cyber-Attacken ebenso wie bei der (fahrlässigen) Weiterverbreitung von Schad-Code sog. Streuschäden in vielen verschiedenen Staaten eintreten können.

Auf Ebene der Gerichtszuständigkeit sollte i.R.d. Deliktsgerichtsstands nach Art. 7 Nr. 2 Brüssel Ia-VO bei Cyber-Incidents zunächst ein Erfolgsort am „Mittelpunkt der Interessen“ des Geschädigten anerkannt werden. Während am Handlungsort des Schädigers stets der Gesamtschaden eingeklagt werden kann, soll laut EuGH bei Streuschäden am jeweiligen Erfolgsort grundsätzlich nur der dort eingetretene Teilschaden zu liquidieren sein.[387] Da-

[386] EuGH 17.10.2013 – Rs. C-184/12 (Unamar) ECLI:EU:C:2013:663 Rn. 50 ff.; EuGH 5.9.2024 – Rs. C-86/23 (HUK COBURG II) ECLI:EU:C:2024:689 Rn. 54 ff.

[387] Grundlegend EuGH 7.3.1995 – Rs. C-68/93 (*Shevill*) ECLI:EU:C:1995:61 Rn. 33.

raus folgt bei der Einschleusung und Weiterverbreitung von Malware in der IT-Infrastruktur internationaler Unternehmen ein potentiell riesiges „Mosaik“ aus einzelnen Erfolgsorten, an denen das betroffene Unternehmen seine jeweiligen Teilschäden sodann mit großem Aufwand einzeln gerichtlich durchsetzen müsste. Noch weitaus komplexer wird das Bild durch die mittlerweile üblichen Cloud-Lösungen: Hier werden einheitliche Datenbestände auf diverse und – je nach Anbieter – europa- oder weltweit verstreute Server je nach verfügbarer Speicherkapazität fragmentweise verteilt und gespeichert. Lokalisiert man hier nun den Erfolgsort am jeweils zur Datenspeicherung verwendeten Server, wo Datenfragmente durch den Cyber-Angriff konkret betroffen sind, würde die Zuständigkeit unnötig zersplittert, obwohl das Gericht am jeweiligen – aufgrund der Funktionsweise einer Cloud: arbiträren – Speicherort keine besondere Sach- oder Beweisnähe aufweist. Bei grenzüberschreitender Geltendmachung von Cyber-Haftpflichtansprüchen sollte deshalb i.R.d. Art. 7 Nr. 2 Brüssel Ia-VO ein Gerichtsstand am „Mittelpunkt des Interesses“ des geschädigten Unternehmens entsprechend der durch den EuGH in den Rechtssachen *eDate und Martinez* und *Svensk Handel* entwickelten Maßstäbe begründet werden. Dieser „Mittelpunkt des Interesses“ deckt sich in der Regel mit dem Ort der Hauptverwaltung.

Auch im internationalen Privatrecht der Cyber-Haftpflicht führt die Grundanknüpfung außervertraglicher Ansprüche an den Erfolgsort nach Art. 4 Abs. 1 Rom II-VO potentiell zu einer Multiplikation der anwendbaren Rechte: Gerade beim Einsatz von Cloud-Computing-Diensten sowie z.B. bei weltweit tätigen Vertriebs- und Außendienstmitarbeitern und der engen Vernetzung der IT entlang der Wertschöpfungskette kann ein einheitlicher Cyber-Vorfall zahlreiche Primärschadensorte am Sitz der jeweiligen Geschäftskontakte begründen. Für das Kollisionsrecht der Cyber-Haftpflicht gegenüber Unternehmen erscheint hier eine Lösung in Parallele zur internationalen Zuständigkeit erstrebenswert: Nach den Grundsätzen der *Svensk Handel*-Entscheidung des EuGH sollte eine Konzentration auf das Recht am „Mittelpunkt des Interesses“ des Geschädigten nach Art. 4 Abs. 3 Rom II-VO erfolgen, wobei dies bei betroffenen Unternehmen regelmäßig zu deren Hauptsitz führen dürfte. Hierfür

sprechen neben der Vorhersehbarkeit für den Schädiger auch die Sach- und Beweisnähe, weil am Hauptsitz angesichts des Erfordernisses einer unternehmensweiten IT-Sicherheitsstrategie und der Reporting-Wege üblicherweise alle Informationen zu einem Cyber-Incident zusammenlaufen. Darüber hinaus kann so ein weitgehender Gleichlauf von internationaler Zuständigkeit und anwendbarem Recht erreicht werden, was die Rechtsermittlungs- und Rechtsanwendungskosten reduziert und die Rechtsdurchsetzung insgesamt beschleunigen und vereinfachen dürfte.

Cyber-Incidents können auch zu Datenschutzverstößen und damit zu Ansprüchen einer Vielzahl von betroffenen natürlichen Personen führen. Gerade wenn die IT-Systeme von global agierenden Online-Händlern, Airlines, Hotelketten oder Social-Media-Plattformen betroffen sind, bilden grenzüberschreitende Sachverhalte den Regelfall. Dann drängt sich die international-privatrechtliche Frage auf, welches nationale Recht in solchen grenzüberschreitenden Konstellationen anzuwenden ist. Schließlich bleibt selbst der unionsrechtlich-autonome Tatbestand des Art. 82 DSGVO lückenhaft und bedarf hinsichtlich so zentraler Fragen wie Verschuldensmaßstab, Mitverschulden, Verjährung und Schadensbemessung der Ergänzung durch das nationale Privatrecht. Welches nationale Zivilrecht in Sachverhalten mit Auslandsbezügen anwendbar ist, muss anhand des Kollisionsrechts ermittelt werden. Dabei ist umstritten, ob die Rom II-VO auf Ansprüche infolge von Datenschutzverletzungen anwendbar ist. Die besseren historisch-teleologischen ebenso wie auch systematischen Argumente sprechen hier für eine restriktive Auslegung der Bereichsausnahme in Art. 1 Abs. 2 lit. g Rom II-VO, so dass es keines Rückgriffs auf nationale Kollisionsnormen, wie Art. 40 ff. EGBGB, bedarf. Die nicht in Art. 82 DSGVO geregelten und damit der Ergänzung durch nationales Recht bedürftigen Rechtsfragen können damit nach der Rom II-VO angeknüpft werden. Nach der hier vertretenen Ansicht sollte der Erfolgsort bei DSGVO-Verstößen infolge von Cyber-Incidents dann in Anlehnung an die zuständigkeitsrechtlichen Erwägungen des EuGH in der Rechtssache *eDate und Martinez* konzentriert werden können: Eine solche Schwerpunktbetrachtung ermöglicht Art. 4 Abs. 3 Rom II-VO im Fall einer offensichtlich engeren

Verbindung zum Recht des Staates, an dem der Geschädigte den „Mittelpunkt seiner Interessen“ hat. Der infolge einer Cyber-Attacke Betroffene sollte seinen gesamten Schaden nach dem Erfolgsortrecht des EU-Mitgliedstaates geltend machen können, in dem ebendieser „Mittelpunkt seiner Interessen“ liegt.[388] Dieser Interessenschwerpunkt wird bei der Haftung für Datenschutzverstöße regelmäßig am gewöhnlichen Aufenthalt des Betroffenen zu lokalisieren und somit das dortige Recht anwendbar sein, was angesichts des Aufenthaltsgerichtsstandes in Art. 79 Abs. 2 S. 2 DSGVO einen Gleichlauf von *forum und ius* ermöglicht.

Bei der grenzüberschreitenden Haftung infolge von Cyber-Vorfällen, die durch die Nichteinhaltung von IT-Sicherheitsstandards verursacht werden, kann es zu einem „Rechtsmix“ kommen, weil gemäß Art. 17 Rom II-VO die „Sicherheits- und Verhaltensregeln“ am Handlungsort des Schädigers auch ungeachtet der nach den allgemeinen Kollisionsnormen ermittelten *lex causae* „berücksichtigt“ werden können. Darüber hinaus mögen in vertraglichen Schuldverhältnissen sowie bei der Frage eines etwaigen Mitverschuldens des Geschädigten die jeweiligen lokalen Cyber-Sicherheitsstandards grundsätzlich ebenfalls (analog Art. 17 Rom II-VO) als *local data* herangezogen werden. Der Anwendungsbereich des Art. 17 Rom II-VO wird indes vor allem durch unionsrechtliche Vorgaben und insbesondere durch den in Art. 3 DSGVO und in Art. 2 Abs. 1 NIS-2-RL abgesteckten räumlich-territorialen Anwendungsbereich der EU-Cyber-Sicherheitsstandards begrenzt. Dies steht einer „Berücksichtigung“ drittstaatlicher Standards an einem Handlungsort außerhalb der EU über Art. 17 Rom II-VO entgegen. Darüber hinaus dürften viele mitgliedstaatliche Cyber-Sicherheitsstandards auch Eingriffsnormcharakter haben. Zumindest grundsätzlich bleibt ein ergänzender Rückgriff auf Art. 17 Rom II-VO in Intra-EU-Konstellationen möglich, soweit hier jedenfalls die Einhaltung des unionsrechtlich vorgegebenen (Mindest)Cyber-Sicherheitsniveaus unter der NIS-2-

[388] Vgl. erneut oben III 1 c) bb). Vgl. EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 52 ff. sowie sodann auch EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 30 ff.; EuGH 17.6.2021 – Rs. C-800/19 (*Mittelbayerischer Verlag*) ECLI:EU:C:2021:489 Rn. 24 ff.; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv/DR*) ECLI:EU:C:2021:1036 Rn. 31 und 39.

RL bzw. der DSGVO gewährleistet ist. Infolge der Teilharmonisierung in diesem Bereich durch die DSGVO bzw. die NIS-2-RL haben sich die mitgliedstaatlichen Cyber-Sicherheitsstandards zumindest stark angenähert. Impulse liefert hier die Rechtsprechungslinie des EuGH in den Rechtssachen *Unamar* und *HUK COBURG II*, obschon der Gerichtshof es einem EU-Mitgliedstaat nicht prinzipiell verwehrt, sein EU-Richtlinien- bzw. EU-Verordnungsvorgaben übertreffendes Recht gegenüber den großzügigeren Standards anderer EU-Mitgliedstaaten durchzusetzen.

Angesichts des – insbesondere im Kontext des Art. 82 DSGVO und des Art. 17 Rom II-VO – stets möglichen „law mix“ auf der Haftpflichtseite werden zugleich die Schwächen des in Ziff. A1-11 AVB Cyber 2024 für die Deckungsseite gewählten Ansatzes deutlich: Wird der Versicherungsschutz für potentiell weltumspannende Cyber-Risiken von der Gerichtszuständigkeit und dem anwendbaren Recht in EWR-Staaten abhängig gemacht, so stellt dies die Rechtsanwender vor große praktische und international-privatrechtliche Herausforderungen.

D. Versicherbarkeit von Geldbußen wegen Verstößen gegen Cybersicherheits- und Datenschutzbestimmungen

Auch im Cyber-Space wird die Normbefolgung zunehmend durch Geldbußentatbestände flankiert: So sehen im Bereich des Datenschutzrechts in der EU insbesondere Art. 83 DSGVO,[389] Art. 40 Abs. 4 Data Act[390] sowie in den USA zahlreiche bundesstaatliche Gesetze, wie der California Consumer Privacy Act (CCPA),[391] empfindliche Geldbußenzahlungen bei Datenschutzverstößen vor.[392] Hinzu treten in jüngerer Zeit weitere geldbußenbewehrte Tatbestände, etwa im Bereich der Cyber-Sicherheit und der Regulierung Künstlicher Intelligenz (KI): Hier sieht zunächst Art. 34 NIS-2-RL[393] bei Unterschreiten des Cyber-Sicherheitsniveaus empfindliche Geldbußen für Unternehmen vor, die als „wesentliche" oder „wichtige Einrichtungen" zu qualifizieren sind.[394] Ebenso können bestimmte Verstöße gegen die KI-VO[395] beim „Hochrisiko-KI-Einsatz" nach Art. 99 Abs. 3 KI-VO mit Geldbußen von bis zu 35 Millionen Euro bzw. von bis zu 7% des weltweiten Jahresumsatzes eines Unter-

389 Zu jüngeren Tendenzen z.B. *Brams*, ZD 2023, 484 ff.

390 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828, ABl. L, 2023/2854 v. 22.12.2023.

391 Titel 1.81.5. *California Consumer Privacy Act of 2018*, sec. 1798.100 bis 1798.199.100 *California Civil Code*.

392 Auf Bundesebene kommt in den USA nun auch der Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) hinzu, der insbesondere bei Verletzung von Reporting-Anforderungen ebenfalls hoheitliche Durchsetzungsinstrumente vorsieht, vgl. zu den am 4.4.2024 vorgeschlagenen Enforcement-Mechanismen nur *Department of Homeland Security: Cybersecurity and Infrastructure Security Agency,* 6 CFR Part 226 [Docket No. CISA-2022-0010] RIN 1670-AA04, abrufbar unter: https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements (zuletzt abgerufen am 1.5.2025).

393 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. EU 2022 L 333/80.

394 Nach Art. 34 Abs. 4 NIS2-RL sind dabei – je nach Klassifikation der Einrichtung – Geldbußen von bis zu 2% des weltweiten Jahresumsatzes möglich.

395 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828, ABl. L, 2024/1689 v. 12.7.2024.

nehmens geahndet werden.[396] Teilweise entfernen sich gerade die unionsrechtlichen Vorgaben zu Sanktionen in der DSGVO auch von den restriktiven Voraussetzungen des deutschen Rechts, etwa mit Blick auf das „Rechtsträgerprinzip" des § 30 OWiG.[397] Ein ganz ähnliches Bild zeigt sich – neben den US-Bundesstaaten – etwa auch im UK, wo der Information Commissioner empfindliche Geldbußen verhängen kann, so dass man insgesamt von einem geldbußenträchtigen „complex array of global regulations and compliance governing cyber security" sprechen kann.[398]

Doch nicht nur die Zahl der Tatbestände, sondern gerade auch die Höhe der Geldbußen wächst rasant: So ist die Summe der in der EU wegen Datenschutzverstößen verhängten Geldbußen bis März 2024 auf 4,48 Milliarden Euro gestiegen und hat sich damit binnen zwei Jahren mehr als verdoppelt.[399] Angesichts des auf bis zu 4% des weltweiten Jahresumsatzes zielenden Sanktionsrahmens der DSGVO konnten einzelne Geldbußen dabei schon bis zu 1,2 Milliarden Euro erreichen.[400] Mit der Ausweitung des Geldbußenrahmens der KI-VO auf bis zu 7% des weltweiten Jahresumsatzes eines Unternehmens[401] steigen auch die Risiken für Unternehmen, zumal in diesem Kontext – anders als bei gleichzeitigen Verstößen gegen Cyber-Risikomanagementmaßnahmen nach dem NIS-2-Re-

396 Vgl. zu dieser Sanktion sog. verbotener Praktiken i.S.d. Art. 5 i.V.m. Art. 99 Abs. 3 KI-VO.

397 Vgl. GA *Campos Sánchez-Bordona* Schlussanträge v. 27.4.2023 – Rs. C-807/21 (*Deutsche Wohnen SE/Staatsanwaltschaft Berlin*) ECLI:EU:C:2023:360; GA *Emiliou* Schlussanträge v. 4.5.2023 – Rs. C-683/21 (*Nacionalinis visuomenės sveikatos centras*) ECLI:EU:C:2023:376. Dazu z.B. *Wybitul/Hager*, MMR 2023, 321 f.; *Wybitul/Klaas*, ZD 2023, 498 ff. Siehe auch schon BeckOK DatenschutzR/*Holländer*, 49. Ed. 1.8.2024, Art. 83 DSGVO Rn. 8 ff. m.w.N. sowie die Kontroverse der deutschen Instanzgerichte und namentlich des LG Bonn MMR 2021, 173 ff. einerseits und des LG Berlin ZD 2021, 270 f. sowie des sodann ein Vorabentscheidungsverfahren beim EuGH veranlassenden KG Berlin ZD 2022, 156 ff. andererseits.

398 *Croft*, Cyber threats put pressure on in-house legal chiefs, Financial Times v. 11.9.2024, abrufbar unter: https://www.ft.com/content/5ce0a155-ddc2-43e4-a383-c6e78f51f836 (zuletzt abgerufen am 1.5.2025).

399 Vgl. nur GDPR Enforcement Tracker Report N°5, abrufbar unter: https://cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures (zuletzt abgerufen am 1.5.2025).

400 Vgl. zur Geldbuße gegen „Meta Platforms Ireland Limited" v. 12.5.2023 wiederum GDPR Enforcement Tracker Report N°5, abrufbar unter: https://cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures (zuletzt abgerufen am 1.5.2025).

401 Vgl. Art. 99 Abs. 3 KI-VO.

gime einerseits und der DSGVO andererseits – keine Deckelung der Geldbußen vorgesehen ist.[402]

Angesichts solcher neuer Rekordwerte ist der Wunsch nach Versicherungsschutz für Geldbußenzahlungen im Rahmen von Cyber-Policen nur allzu verständlich. Dies gilt umso mehr, als sich gerade international agierende Unternehmen angesichts des extraterritorialen Anwendungsbereichs von geldbußenbewehrten Gesetzen wie der DSGVO in der EU, des CCPA und vergleichbarer bundesstaatlicher Normen in den USA sowie z.B. des chinesischen Personal Information Protection Law (PIPL)[403] selbst bei einem punktuellen „Datenleck" potentiell gleich weltweit Geldbußen wegen Datenschutzverstößen ausgesetzt sehen. Besonders exponiert sind in dieser Hinsicht Unternehmen mit einem internationalen Kundenstamm, wie Fluglinien und Hotelketten, da hier jede – vermeintlich nur lokale – Datenpanne leicht internationale Tragweite erlangen kann.

Die Cyber-Bedingungswerke reagieren hierauf oftmals mit Deckungsbausteinen für Bußgelder und versprechen im Rahmen dieser besonderen Form der Vermögenschadenversicherung sodann grundsätzlich weltweiten Versicherungsschutz.[404] Auf den ersten Blick legen manche AVB-Klauseln dabei nahe, dass Deckung für Geldbußen gewährt werden kann, wenn nur die Versicherbarkeit in dem Staat gegeben ist, der die Geldbuße erlässt.[405] Manche Bedingungswerke stellen dagegen auf das Recht ab, dem der Cyber-Versicherungsvertrag untersteht, sowie zudem auf die Rechtsordnung, in der die Versicherungsleistung zu erbringen ist.[406] In noch weitaus größerem Maße als bei der Deckung des Verbandsgeld-

---

402 Vgl. Art. 35 NIS-2-RL.

403 In englischsprachiger Fassung abrufbar unter: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (zuletzt besucht am: 1.5.2025).

404 Während kraft hoheitlicher Anordnung gegen den Versicherten verhängte Bußgelder nicht bereits als „Schadenersatzansprüche aufgrund gesetzlicher Haftpflichtbestimmungen" schon vom Haftpflichtbaustein erfasst werden, sind Geldbußen-Deckungen sowohl in der Cyber-Versicherung als auch z.B. im D&O-Bereich verbreitet, vgl. auch *Armbrüster/Schilbach*, r+s 2016, 109, 110; *Pott*, ZfV 2023, 357 ff.; Dickmann/*Schilbach*, Cyberversicherung, Ziff. A1-17.11 AVB-Cyber Rn. 1 ff.

405 Vgl. etwa Ziff. 2.11. *Hiscox* CyberClear Bedingungen 10/2020 („Bußgelder und Entschädigungen mit Strafcharakter im Ausland").

406 Vgl. Ziff. I.3.4.b. *Allianz* Cyber Protect Premium („Geldbußen").

bußenregresses in der D&O-Versicherung[407] dürften sich deshalb bei Geldbußenbausteinen in der Cyber-Versicherung Fallstricke verbergen: Ausweislich jüngerer Stellungnahmen aus der Makler-Praxis lehnen nämlich D&O-Versicherer schon unter Verweis auf das deutsche Recht die Regulierung ab.[408] Angesichts des üblicherweise „weltweiten" Deckungsversprechens im Rahmen von Cyber-Versicherungen könnten in den praktisch häufigen grenzüberschreitenden Sachverhalten dann gleich mehrere Rechtsordnungen für die Frage der Versicherbarkeit von Geldbußen relevant werden.

Vor diesem Hintergrund soll zunächst rechtsvergleichend die Haltung einiger Rechtsordnungen zur Versicherbarkeit beispielhaft in den Blick genommen werden (dazu unter I). Dabei wird in deutschen Cyber-Versicherungsverträgen in aller Regel deutsches Recht gewählt und ein Gerichtsstand in Deutschland vereinbart.[409] Entsprechend wird in einem Deckungsstreit zumindest auch das auf den Vertrag anwendbare Recht für die Versicherbarkeit relevant. Aus der Perspektive eines deutschen Gerichts und unter Anwendung des Internationalen Privatrechts kommen angesichts des üblicherweise „weltweiten" Deckungsversprechens in Cyber-Versicherungsverträgen noch weitere potentiell zu berücksichtigende nationale Rechte hinzu (hierzu unter II). Schließlich gewinnt die Frage der Versicherbarkeit auch eine unionsrechtliche Dimension, wann immer die Geldbuße zur Sanktionierung von Verstößen gegen Normen EU-rechtlicher Provenienz verhängt wird (dazu unter III). Mit Blick auf den „sanktionenrechtlichen Effektivitätsgrundsatz" im EU-Recht sind auch Deckungskonzepte kritisch zu hinterfragen, welche die Versicherbarkeit durch Rechtswahl und forum-shopping oder Gestaltungen wie „fine-wraps" gewährleisten sollen (dazu unter IV).

---

407 Zur kontrovers diskutieren Zulässigkeit und Ausgestaltung des Regresses und der D&O-Deckung für Unternehmensgeldbußen *Lüttringhaus,* FS Juristische Fakultät Hannover, 2025, 207 ff.

408 Vgl. mit der Wiedergabe des Wortlautes gängiger Ablehnungsschreiben *Pott*, ZfV 2023, 357 ff. Siehe allgemein auch Bruck/Möller/*Gädtke*, 10. Aufl. 2022, Ziff. A-7 AVB-D&O Rn. 104 ff.

409 Vgl. nur die – zumindest insoweit die Marktpraxis durchaus abbildenden – Ziff. B4-5.3 und Ziff. B4-6 AVB-Cyber 2024.

I. Rechtsvergleichende Umschau: Kaum explizite Versicherungsverbote – viel Rechtsunsicherheit

Die Versicherbarkeit von Geldstrafen und Geldbußen wird seit langer Zeit kontrovers diskutiert.[410] Während solche Deckungskonzepte vielfach *per se* für unzulässig gehalten werden, differenzieren manche entlang der Begehungsweise und/oder halten bestimmte Verschuldensgrade für versicherbar.[411] Im Zentrum steht dabei jeweils die Frage, ob eine Beeinträchtigung der intendierten Sanktions- und Präventionsfunktion droht und, ob solche straf- bzw. ordnungswidrigkeitenrechtliche Wertungen sodann auf die gesellschaftsrechtliche Binnenhaftung[412] und ggf. auch auf das Privatversicherungsrecht durchschlagen.[413]

Die nachfolgenden Betrachtungen legen den Fokus auf die als Eigenschadendeckung konzipierten Deckungsbausteine in Cyber-Versicherungsverträgen, in denen die Erstattung von behördlichen Geldbußen versprochen wird, wenn solche Geldbußen infolge eines Cyber-Incidents, z.B. wegen Verstoßes gegen Datenschutz- oder Cyber-Sicherheitsbestimmungen, verhängt werden. Soweit – wie im Regelfall – gesetzliche Regelungen zur Versicherbarkeit von Geldbußen fehlen, werden auch angrenzende Materien, wie das Straf- und Ordnungswidrigkeitenrecht, das allgemeine Zivilrecht sowie andere Deckungskonzepte, z.B. in der D&O-Versicherung in den Blick genommen. Die Aufmerksamkeit gilt dabei, neben der Rechtslage in Deutschland (**dazu unter 1**), Italien (**hierzu unter 2**) und Frankreich (**dazu unter 3**) England und Wales (**hierzu unter 4**) und einigen ausgewählten Bundesstaaten der USA (**dazu unter 5**).

---

410 Vgl. nur *Rehbinder*, ZHR 148 (1984), 555 ff.; *Kapp*, NJW 1992, 2796, 2797 ff.

411 Einen Überblick über das Meinungsspektrum bieten z.B. *Armbrüster/Schilbach*, r+s 2016, 109 ff.; *Lüttringhaus,* FS Juristische Fakultät Hannover, 2025, 207, 209 ff.

412 Dafür im Kontext der D&O-Versicherung etwa OLG Düsseldorf r+s 2023, 827 Rn. 152 ff.; LG Saarbrücken NZKart 2021, 64 Rn. 122 f. dagegen etwa LG Dortmund VersR 2023, 1313; LG Dortmund VersR 2023, 1314 ff. Siehe vornehmlich im Kontext des Binnenregreseses gegen Geschäftsleiter und der D&O-Versicherung auch *Dreher*, FS Konzen, 2006, 85, 103 ff.; *Fleischer*, BB 2008, 1070, 1073.

413 Siehe zu Geldbußen-Deckungsbausteinen i.R.d. D&O-Versicherung LG Frankfurt 20.1.2023 – 2-08 O 313/20 (juris) Rn. 49 ff. gegenüber OLG Düsseldorf r+s 2023, 827 Rn. 167. Offen gelassen durch OLG Frankfurt 21.11.2023 – 18 U 17/23 (unveröffentlicht, unter II 4 g der Gründe).

1. Deutschland

Ein explizites Verbot, behördliche Geldbußen zu versichern, enthält das deutsche (Versicherungs)Recht nicht. Gleiches gilt im Ausgangspunkt auch für in Strafverfahren verhängte Geldstrafen. Allerdings können auch Strafgesetze zu den Verbotsgesetzen i.S.d. § 134 BGB zählen, soweit ihr Tatbestand verwirklicht und sodann durch den Versicherungsschutz der mit dieser Norm verfolgte Strafzweck vereitelt wird (**dazu unter a**). Zudem finden Deckungskonzepte für Bußgelder eine Schranke in § 138 Abs. 1 BGB (**hierzu unter b**).

a) § 134 BGB i.V.m. Straftatbeständen des StGB

Der BGH hatte sich im Kontext der Strafvereitlung nach § 258 Abs. 2 StGB mit der Frage zu beschäftigen, ob die Zahlung einer gegen den Täter verhängten Geldstrafe den Tatbestand der Straf(vollstreckungs)vereitlung erfüllt.[414] Dies verneinte der BGH mit dem Argument, dass § 258 Abs. 2 StGB nur die Verhinderung der Durchsetzung des Strafanspruchs – und damit die Vollstreckung der Strafe – pönalisiere, was bei der Zahlung oder Erstattung des Geldbetrages indes nicht der Fall sei, weil der Verurteilte unverändert der Strafvollstreckung ausgesetzt bleibt.[415] Eine etwaige Schmälerung der (Individual)Prävention sei dagegen i.R.d. § 258 Abs. 2 StGB schon nicht tatbestandsmäßig, weil die Norm die Straf*zweck*vereitlung nicht erfasse.[416] Nur ausnahmsweise dürfte eine strafrechtliche Verantwortlichkeit in Betracht kommen, die zugleich die privatrechtliche Nichtigkeit nach § 134 BGB zu begründen vermag, wenn die auf Seiten des Versicherers handelnde Person zu ihr – etwa im Rahmen einer langen Geschäftsbeziehung – bekannten rechtswidrigen Haupttaten eines Versicherten (psychische) Beihilfe nach § 27 StGB leistet oder sich i.S.d. § 14 OWiG beteiligt, indem vorab

414 BGH NJW 1991, 990, 992 f.
415 BGH NJW 1991, 990, 992. Vgl. zur Begünstigung zuvor schon RGZ 169, 267; BGH NJW 1957, 586.
416 BGH NJW 1991, 990, 992 f.

Deckung für Geldstrafen oder Geldbußen versprochen wird.[417] Zumeist wird es indes im relevanten Zeitpunkt des Deckungsversprechens schon an einer hinreichenden Konkretisierung der Haupttat fehlen.[418]

Im absoluten Regelfall wird durch die Gewährung von Versicherungsschutz kein Straf- oder Ordnungswidrigkeitentatbestand erfüllt, noch liegt Beihilfe nach § 27 StGB oder Beteiligung gemäß § 14 OWiG vor, so dass auch gegen kein Verbotsgesetz i.S.d. § 134 BGB verstoßen wird. Begreift man das Straf- und Ordnungswidrigkeitenrecht einerseits und das Privatrecht andererseits jeweils als eigenständige und voneinander unabhängige Regelungsebenen,[419] so folgt aus der fehlenden Strafbarkeit freilich noch lange nicht die privatrechtliche Zulässigkeit eines bestimmten Verhaltens.[420] Dreh- und Angelpunkt der Debatte um die rechtliche Zulässigkeit von Deckungskonzepten für behördliche Geldbußen ist vor diesem Hintergrund § 138 Abs. 1 BGB.[421]

b) § 138 Abs. 1 BGB und (in- und ausländische) Geldbußen

Nach ständiger Rechtsprechung ist sittenwidrig i.S.d. § 138 Abs. 1 BGB, was dem „Anstandsgefühl aller billig und gerecht Denkenden" zuwiderläuft.[422] Ob ein Rechtsgeschäft i.d.S. gegen die guten Sitten verstößt, mithin von den ethischen Grundlagen der Rechtsgemeinschaft abweicht, deshalb für sie unerträglich ist und verhindert werden muss, ist durch eine Gesamtwürdigung zu ermitteln, in die stets auch Inhalt, Beweggrund und Zweck des Geschäfts einzubeziehen sind.[423] Diese Formel legt den normativen, durch die Rechtspre-

---

417 *Armbrüster/Schilbach*, r+s 2016, 109, 110; Bruck/Möller/*Gädtke*, 10. Aufl. 2022, Ziff. A-7 AVB-D&O Rn. 108.

418 Eingehend *Ruttmann*, Die Versicherbarkeit von Geldstrafen, Geldbußen, Strafschadensersatz und Regressansprüchen in der D&O-Versicherung, 2014, S. 80 ff.; Bruck/Möller/*Gädtke*, 10. Aufl. 2022, Ziff. A-7 AVB-D&O Rn. 108. Vgl. auch schon *Rehbinder*, ZHR 148 (1984), 555, 564 f.

419 Vgl. aus jüngerer Zeit nur LG Dortmund VersR 2023, 1313; LG Dortmund VersR 2023, 1314 ff. Siehe auch schon *Fleischer*, BB 2008, 1070, 1073.

420 Vgl. BGH WM 1961, 530; BGH NJW 1970, 1179 f. Siehe auch *Armbrüster/Schilbach*, r+s 2016, 109, 112.

421 *Armbrüster/Schilbach*, r+s 2016, 109, 110 f.

422 Z.B. BGH NJW 2014, 1380 Rn. 8 m.w.N.

423 Vgl. nur OLG Köln NJW 2016, 649 Rn. 16.

chung einzelfallbezogen mit Inhalt zu füllenden Maßstab offen.[424] Einen ersten, etwas konkreteren Ansatzpunkt zur Begründung der Sittenwidrigkeit von Bußgelddeckungen liefert womöglich das Urteil des BAG vom 25.1.2001: Nach dieser Entscheidung soll die Zusage eines Arbeitgebers gegenüber seinen als LKW-Fahrer tätigen Arbeitnehmern, etwaig gegen diese Arbeitnehmer wegen Überschreitung von Lenkzeiten im Güterverkehr verhängte Geldbußen zu erstatten, i.S.d. § 138 Abs. 1 BGB sittenwidrig und damit nichtig sein.[425] Obschon dieses Urteil auch und gerade von Seiten mancher Versicherer herangezogen wird,[426] ersetzt der Verweis auf ein – zumal vor arbeitsrechtlichem Hintergrund ergangenes – Judikat für sich genommen kaum die Subsumtion unter § 138 Abs. 1 BGB im versicherungsvertraglichen Kontext. Die zentrale Begründung des BAG für das Verdikt der Sittenwidrigkeit gibt indes auch für die hiesige Fragestellung wichtige Impulse: Laut BAG liefe die arbeitgeberseitige Zusage der Übernahme eines Bußgeldes nicht nur dem Sanktionsziel, sondern auch dem (general- wie individual-)präventiven Zweck der Straf- und Bußgeldvorschriften zuwider und setze insbesondere die Hemmschwelle der Arbeitnehmer herab, Ordnungswidrigkeiten oder gar Straftaten zu begehen.[427] Solche über die Repression hinausgehenden Präventionsziele sind in der Tat im Rahmen der nach § 138 Abs. 1 BGB gebotenen Gesamtwürdigung

---

424 Statt vieler BeckOGK BGB/*Jakl*, 1.8.2024, § 138 BGB Rn. 24 ff.; MünchKommBGB/*Armbrüster*, 10. Aufl. 2025, § 138 BGB Rn. 21 ff.

425 BAG NJW 2001, 1962, 1963. Vgl. auch FG Köln DStRE 2006, 203, 207; BFH DStRE 2009, 374 ff.

426 Mit Blick auf Bußgelddeckungsbausteine in der D&O-Versicherung paraphrasiert *Pott*, ZfV 2023, 357 ff., den Wortlaut gängiger Ablehnungsschreiben wie folgt: „In Deutschland ist ein solches Versicherungsverbot, welches in Ziffer 1.2 benannt ist, die Sittenwidrigkeit nach § 138 Abs.1 BGB. Nach seinem Urteil vom 25.01.2001 hat das Bundesarbeitsgericht unter Verweis auf den Sanktionszweck der Geldbuße entschieden, dass Zusagen eines Arbeitgebers über die Erstattung von etwaigen Geldbußen für Verstöße des Arbeitnehmers sittenwidrig und daher nach § 138 Abs. 1 BGB unwirksam sind. Da es im Ergebnis keinen Unterschied macht, ob der Strafzweck des Bußgeldes durch eine direkte Erstattungszusage des Arbeitgebers vereitelt wird oder ob dies durch den Abschluss einer entsprechenden Versicherung geschieht, liegt in der Versicherung persönlicher Bußgelder nach deutschen Recht eine Sittenwidrigkeit vor.“.

427 BAG NJW 2001, 1962, 1963. Gleichsinnig sodann FG Köln DStRE 2006, 203, 207 sowie zuvor LAG Hamm NJW 1991, 861.

zu berücksichtigen.[428] Allerdings ist das Verhalten eines Arbeitgebers, der seine Mitarbeiter durch Zusagen von Erstattungen mehr oder minder offenkundig zur Missachtung von Rechtsnormen auffordert, kaum mit Versicherungslösungen für Geldbußen oder auch Geldstrafen gleichzusetzen.

Die Sittenwidrigkeit eines Deckungsversprechens für Geldbußen oder Geldstrafen liegt – ebenso wie im erwähnten BAG-Fall – nur nahe, soweit hierdurch ordnungswidriges oder sogar strafbewehrtes Verhalten gefördert wird: Dann läuft die Versicherungslösung der Einhaltung von – der Sicherheit des Rechtsverkehrs und damit aller Bürgerinnen und Bürger dienenden – Normen zuwider und verdient infolgedessen keine rechtliche Anerkennung.[429] Dies dürfte zu bejahen sein, wenn durch den Versicherungsschutz jegliche (individual- und general)präventive Wirkung bzw. bei Geldstrafen auch die Vergeltungsfunktion aufgehoben und die Sanktion – zugespitzt formuliert – insgesamt zahnlos würde.[430] In dieser Konstellation greift das Zivilrecht in die Sphäre des Straf- bzw. Ordnungswidrigkeitenrechts über und beeinträchtigt dessen Funktionen. Jenseits solcher „Überwirkungen“ und Rückkopplungen dürfte die zivilrechtliche Wirksamkeit von Vertragsgestaltung dagegen nicht ohne Weiteres durch das Straf- und Ordnungsrecht präjudiziert werden.[431] Das gilt in besonderem Maße, wenn nach ausländischem Sanktionenrecht verhäng-

---

428 *Armbrüster/Schilbach*, r+s 2016, 109, 110 verweisen zu Recht auf die durch das Bundesaufsichtsamt für das Versicherungswesen, GB BAV 1972, 63, 64, ebenfalls mit Präventionszielen begründete Sittenwidrigkeit einer Versicherung gegen die (finanziellen) Folgen einer im Straf- oder Ordnungswidrigkeitenverfahren verhängten Entziehung der Fahrerlaubnis. Dies deckt sich i.Ü. mit der Rechtslage in Frankreich, wo das *Ministère de l'économie et des finances* 1992 neben dem Ausgleich der finanziellen Folgen explizit auch das Stellen eines Fahrers untersagt hat, vgl. *Haut Comité Juridique de la Place Financière de Paris*, Rapport sur l'assurabilité des risques cyber v. 28.1.2022, S. 11 m.w.N.

429 Vgl. BAG NJW 2001, 1962, 1963 und deutlich auch zuvor LAG Hamm NJW 1991, 861. Vgl. z.B. zu ordnungswidrigkeitenrechtlichen Normen der StVO nur BGH NJW 2005, 1490 ff.; BGH NJW 2010, 610 ff.

430 Vgl. *Armbrüster/Schilbach*, r+s 2016, 109, 111.

431 Vgl. BeckOGK AktG/*Fleischer*, 1.2.2024, § 93 AktG Rn. 260. Indes verfängt das u.a. von *Kapp*, NJW 1992, 2796, 2798 und *Rehbinder*, ZHR 148 (1984), 555, 565 f. vorgebrachte Argument nicht, dass es der Einheit der Rechtsordnung widerspreche, ein strafrechtlich i.R.d. § 258 Abs. 2 StGB tatbestandsloses Verhalten sodann zivilrechtlich durch die Nichtigkeitssanktion nach § 138 Abs. 1 BGB zu ahnden: Die Fehlende Pönalisierung und damit auch die Unanwendbarkeit des § 134 BGB sagen noch nichts über die mögliche Sittenwidrigkeit i.S.d. § 138 Abs. 1 BGB aus, treffend Bruck/Möller/*Gädtke*, 10. Aufl. 2022, Ziff. A-7 AVB-D&O Rn. 110; *Armbrüster/Schilbach*, r+s 2016, 109, 111.

te Geldbußen vom Deckungsversprechen eines dem deutschen Recht unterliegenden Cyber-Versicherungsvertrags umfasst werden.[432]

aa) Impulse aus der Rechtsprechung zur (Steuer)Beraterhaftung

In der deutschen Rechtsprechungspraxis sowie insbesondere im Schrifttum werden indes unterschiedliche Ansatzpunkte gewählt, die nicht immer anhand der vorstehend herausgearbeiteten Kriterien erklärbar erscheinen: Während ein Teil des Schrifttums Versicherungsschutz für Geld*strafen* immer mit dem Verdikt der Sittenwidrigkeit belegen will, sprechen sich andere für die generelle Unversicherbarkeit von Geldbußen und Geldstrafen aus.[433] Wiederum andere wollen – teils nach Straf- oder Ordnungswidrigkeitenrecht differenzierend – zwischen der Versicherung fahrlässiger und vorsätzlicher Begehungsweisen unterscheiden.[434] Abgesehen davon, dass aus versicherungsrechtlicher Sicht eine vorsätzliche Tatbegehung ohnehin als vorsätzliche Herbeiführung des Versicherungsfalls bzw. als „wissentliche Pflichtverletzung" aus dem Deckungsumfang fallen kann,[435] zeigt der BGH in seiner Judikatur durchaus eine Tendenz, die Erstattung bei lediglich fahrlässiger Begehungsweise rechtlich zu billigen: Namentlich lässt der BGH die Erstattung von strafrechtlichen Geldstrafen und – *argumentum a majore ad minus* – ordnungswidrigkeitenrechtlicher Geldbußen grundsätzlich zu, wenn und soweit privatrechtlich ein solcher Anspruch besteht

---

[432] Dazu sogleich noch näher unter II.

[433] Z.B. OLG Düsseldorf r+s 2023, 827 Rn. 168 ff. im Anschluss an *Thomas*, NZG 2015, 1409, 1416 (zur Eigenschadendeckung).

[434] Allgemein z.B. *Kapp*, NJW 1992, 2796, 2798. Siehe zur D&O-Versicherung nur den Überblick bei Bruck/Möller/*Gädtke*, 10. Aufl. 2022, Ziff. A-7 AVB-D&O Rn. 109 ff.; *Ruttmann*, Die Versicherbarkeit von Geldstrafen, Geldbußen, Strafschadensersatz und Regressansprüchen in der D&O-Versicherung, 2014, S. 99 ff.

[435] Je nach Konstellation ist gerade bei Versicherungen für fremde Rechnung und einem Ausschluss nur von „wissentlichen Pflichtverletzungen" durchaus eine vorsätzliche Begehung der Ordnungswidrigkeit bzw. Straftat möglich, ohne dass der versicherungsvertragliche Risikoausschluss greift: Denn während letzterer dann direkten Vorsatz (*dolus directus* 2. Grades) voraussetzt, mag bei vielen Straf- und Ordnungswidrigkeitentatbeständen schon bedingter Vorsatz (*dolus eventualis*) ausreichen. Ob dies allein allerdings die Annahme von *Armbrüster/Schilbach*, r+s 2016, 109, 112 trägt, dass in der Deckungszusage für Bußgelder dann notwendigerweise eine „Unterstützung des Willens zu erblicken (sei), einen Straf- oder Ordnungswidrigkeitentatbestand zu verwirklichen", erscheint fraglich und dürfte eher von der konkreten Ausprägung der Deckung und der jeweiligen Personenkonstellation abhängen.

und sieht sodann einen solchen Anspruch auch „nicht dadurch ausgeschlossen, daß er inhaltlich auf die Abwälzung der … auferlegten Strafe gerichtet ist".[436] Dies soll jedenfalls insoweit gelten, als die Person, gegen die die Geldbuße verhängt worden ist, ihrerseits *nicht vorsätzlich*, sondern nur *fahrlässig* – bzw. i.S.d. § 378 AO „leichtfertig" – gegen die Ordnungswidrigkeitentatbestände verstoßen hat.[437] Der BGH hat die Abwälzung der finanziellen Folgen einer Ordnungswidrigkeit zwar ausdrücklich nur mit Blick auf Ansprüche für möglich gehalten, die sich „aus den allgemeinen Regeln des bürgerlichen Rechts" ergeben.[438] Angesprochen sind damit insbesondere Schadensersatzansprüche wegen Verletzung von Beratungs- und Schutzpflichten im Rahmen von Steuerberater- bzw. Kontokorrentverträgen.[439] Dieser Entscheidung lässt sich indes die allgemeine Wertung entnehmen, dass aus der Warte des BGH privatrechtliche Erstattung von Geldbußenzahlungen nicht ohne Weiteres die intendierte Präventionswirkung vereitelt: Denn der sanktionsrechtlich verpflichtete Adressat der Geldbuße ist und bleibt die bebußte Person, gleichviel, ob Grundlage der Sanktion nun – wie in der BGH-Entscheidung – § 378 Abs. 1 AO oder – wie bei IT-Sicherheits- und Datenschutzverstößen infolge eines Cyber-Incidents – nun z.B. Art. 83 DSGVO ist. Man mag allenfalls einwenden, dass bei den bislang durch den BGH entschiedenen Konstellationen das Verhalten des sodann im Wege privatrechtlicher Schadensersatzansprüche Ersatzpflichtigen zur Verhängung des Bußgeldes beigetragen hat: In der bisherigen BGH-Judikatur ging es um die Verletzung von vertraglichen (Beratungs- und/oder Schutz)Pflichten, die sodann nach § 280 Abs. 1 BGB zum Ersatz des hieraus folgenden Vermögensschadens verpflichtete.[440] Aus der Perspektive des Ord-

---

436 BGH NJW 1957, 586. Gleichsinnig sodann BGH NJW 1997, 518, 519; BGH 15.4.2010 – IX ZR 189/09, BeckRS 2010, 11952 Rn. 8.

437 BGH 15.4.2010 – IX ZR 189/09, BeckRS 2010, 11952 Rn. 9 f. setzt dabei allerdings auf Tatbestandsebene der Ersatzpflicht und namentlich der Schutzpflicht des Steuerberaters an: „Begeht der Mandant … eine vorsätzliche Steuerhinterziehung, so kann er die sein Vermögen treffenden steuerstrafrechtlichen Folgen also nicht auf seinen Berater abwälzen" Der BGH nahm indes eine nur leichtfertige Steuerverkürzung nach § 378 Abs. 1 AO an.

438 BGH NJW 1957, 586; BGH NJW 1997, 518, 519.

439 Vgl. wiederum BGH NJW 1957, 586; BGH NJW 1997, 518, 519. Nach heutigem Recht geht es somit um Schadensersatzansprüche nach § 280 Abs. 1 i.V.m. § 241 Abs. 1 bzw. Abs. 2 BGB.

440 BGH 15.4.2010 – IX ZR 189/09, BeckRS 2010, 11952 Rn. 8 ff. Vgl. erneut BGH NJW 1957, 586; BGH NJW 1997, 518, 519.

nungswidrigkeitenrechts ist die Mitverursachung durch den privatrechtlich zum Ersatz Verpflichteten zumindest mit Blick auf die intendierte Präventionswirkung aber völlig gleichgültig: Denn sanktioniert werden soll auch in diesem Fall einzig und allein der – fehlerhaft beratene – Adressat der Geldbuße, nicht aber der Berater als Mitverursacher.

bb) Geldbußendeckung und Präventionswirkung

Vor diesem Hintergrund erscheinen die Aussagen des BGH zur (Schadens)Ersatzfähigkeit von Geldbußen durchaus verallgemeinerungsfähig und damit auch für die Geldbußen-Deckungszusage durch einen Versicherer relevant. Zunächst handelt es sich nämlich in beiden Fällen um Ansprüche, die „aus den allgemeinen Regeln des bürgerlichen Rechts“ folgen:[441] Während bei der Schutzpflichtverletzung §§ 280 Abs. 1, 241 Abs. 2, 249 BGB einschlägig sind, handelt es sich beim Deckungsversprechen für Geldbußen – ungeachtet der spezialgesetzlichen Normierung bestimmter Aspekte des Versicherungsvertragsrechts im VVG – um einen privatautonom nach § 311 Abs. 1 und § 241 Abs. 1 BGB vereinbarten Anspruch, der genuin privatrechtlicher Natur ist. Vor allem lassen sich die Überlegungen, die der BGH mit Blick auf leichtfertige Verstöße gegen das Steuerrecht (§ 378 Abs. 1 AO) anstellt, zumindest auf fahrlässige und – erst recht – auf ohne jede Vorwerfbarkeit[442] begangene Verstöße, z.B. gegen Datenschutzbestimmungen und die zur Sanktion nach Art. 83, 84 DSGVO verhängten Geldbußen, übertragen: Denn hier wie dort ist die Materie

441 Vgl. BGH NJW 1957, 586; BGH NJW 1997, 518, 519.

442 Vgl. im Anschluss an EuGH Urt. v. 5.12.2023 – C-807/21, ECLI:EU:C:2023:950 – *Deutsche Wohnen*, zuletzt KG Berlin GRUR-RS 2024, 2154: „Nach der Rechtsprechung des EuGH … erfordert eine Verbandshaftung weder das Verschulden eines Repräsentanten (§ 30 OWiG) noch eine Aufsichtspflichtverletzung (§ 130 OWiG). Vielmehr sind Unternehmen im Deliktsbereich der DSGVO per se schuldfähig … Die vom EuGH für den Bereich der DSGVO entwickelten sachlichrechtlichen Grundzüge der Verbandsgeldbuße überformen, prägen und gestalten auch das diesbezügliche nationale Verfahrensrecht“.

„vielfach kompliziert und … (es) … ist oft nur schwer erkennbar, was noch gesetzmäßig ist und was den Rahmen der … Legalität sprengt".[443]

Ob der Rahmen des nach der DSGVO – aber z.B. auch i.R.d. NIS-2-Regelungssystems – gesetzlich Zulässigen immer hinreichend klar umrissen und für die rechtsunterworfenen Unternehmen auch erkennbar ist, muss man zum einen deshalb hinterfragen, weil im unionalen Datenschutzrecht und im novellierten Cyber-Sicherheitsrecht zahlreiche konkretisierungsbedürftige Tatbestände existieren, die – wie noch zu zeigen sein wird – längst nicht umfassend und eindeutig durch Gesetzgebung, Behörden und/oder Rechtsprechung mit Inhalt gefüllt worden sind. Hinzu kommt zum anderen die im Ordnungswidrigkeitenrecht allgemein übliche Verwendung von Blanketttatbeständen: Die objektiven und subjektiven Tatbestandsmerkmale ergeben sich demnach gar nicht aus dem mit einer Geldbuße bewehrten Ordnungswidrigkeitentatbestand selbst, sondern erst aus der Verweisung auf eine Vielzahl spezieller Einzelnormen.[444] Ebendiese Blankett-Technik findet gerade auch bei Unionsrechtsakten, wie der DSGVO und der NIS-2-RL, Anwendung. Infolgedessen sind selbst solche Cyber-Sicherheits- und Datenschutztatbestände potentiell sanktionsbewehrt, die aus Sicht der Rechtsanwender noch gar nicht abschließend klar konturiert sind.

Im Kontext der Ersatzfähigkeit von Geldbußen i.R.d. (Steuer)Beraterhaftung stellt der BGH entscheidend auf die Erkennbarkeit der Gesetzeswidrigkeit ab.[445] Das verdient Zustimmung, weil eine mit Geldbußen nach Ordnungswidrigkeitenrecht bezweckte „eindringlichen Pflichtenmahnung" dort angezeigt ist, wo der Handelnde, der seine Rechtspflichten kennt oder bei gehöriger Anstrengung kennen müsste, sich dennoch gegen seine Pflichten stellt. Hier bedarf es der Prävention, d.h. einer– individuell und generell wirkenden – eindringlichen und nachhaltigen Mahnung zur Einhaltung der vorgegebenen Rechtspflichten. Zugleich mag die Erstattung von Geldbußen

443 Vgl. BGH NJW 1997, 518, 519.

444 Statt vieler BeckOK-OWiG/*Gerhold*, 44. Ed. 1.10.2024, Einl. OWiG Rn. 59; KK-OWiG/Rogall, 5. Aufl. 2018, Vorbemerkungen Rn. 15.

445 Vgl. erneut BGH NJW 1997, 518, 519.

in solchen Konstellationen auch geeignet sein, besonders nachlässiges oder sogar doloses Verhalten zu fördern.[446] Deutlich anders liegt der Fall aber, wenn in vergleichsweise neuen Regelungsmaterien die zu beachtenden Pflichtenmaßstäbe noch gar nicht hinreichend klar umrissen sind: So können die Normadressaten womöglich in bestimmten Regelungsbereichen der DSGVO, der NIS-2-RL oder auch der KI-VO mangels Konkretisierung durch die Judikatur des EuGH und mangels einer einheitlichen Linie von Behörden und Schrifttum weder ihre konkreten gesetzlichen Verhaltenspflichten noch infolgedessen überhaupt „den Rahmen der … Legalität“[447] abschließend und eindeutig beurteilen. Hier trägt das Argument der Präventionswirkung nicht: Denn zu welcher Sorgfalt soll der Geldbußenadressat bereits durch drohende ordnungswidrigkeitenrechtliche Sanktionen angehalten werden? Soweit aber keine hinreichend umrissenen Präventionsziele in Gestalt konkret erwünschter Verhaltenspflichten bestehen, können diese schwerlich auf Ebene des Privatrechts durch Ersatz- bzw. Erstattungsansprüche vereitelt werden.

cc) Geldbußendeckung bei noch nicht hinreichend konkretisierten Regelungsbereichen in neuen (EU-)Rechtsakten

Die Rechtsprechungslinie des BGH zur (Steuer)Beraterhaftung lässt sich deshalb dahingehend verstehen, dass jedenfalls in „rechtlichen Graubereichen“ zumindest bei (leicht) fahrlässigem Handeln – oder gänzlich fehlender Vorwerfbarkeit – die Erstattung von Geldbußen zulässig sein kann. Ähnliches dürfte nun auch für Geldbußen-Deckungsversprechen in Cyber-Versicherungsverträgen gelten. Als möglicher Anwendungsfall kommt im Cyber-Kontext vor allem die stetig anwachsende unionsrechtliche und nationale Regulierung im Bereich des Datenschutzes, der Cybersicherheit und der KI in Betracht: Denn hier finden sich z.B. in der NIS-2-RL[448] zahlreiche mit Geldbußen bewehrte Tatbestände, ohne dass die (Sorgfalts)Pflich-

[446] Vgl. zu diesem Motiv nur OLG Düsseldorf r+s 2023, 827 Rn. 168 ff. sowie z.B. *Thomas*, NZG 2015, 1409, 1416.

[447] Vgl. BGH NJW 1997, 518, 519.

[448] Richtlinie des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie), ABl. 2022 L333/80.

ten den Normadressaten schon ab Inkrafttreten oder auch nur ab der Richtlinien-Umsetzung stets hinreichend klar erkennbar wären.[449] Im Fall von Geldbußen, die wegen Verstößen in solchen – erst in der behördlichen und gerichtlichen Anwendungspraxis überhaupt konkretisierten – „rechtlichen Graubereichen" verhängt werden, erscheint mangels effektiver Präventionswirkung dann ein als Eigenschadendeckung konzipierter Geldbußenbaustein in Cyber-Versicherungsverträgen kaum *per se* als mit den „guten Sitten" i.S.d. § 138 Abs. 1 BGB unvereinbar.

Als Beispiel lassen sich zunächst Geldbußen gegen Verantwortliche nach Art. 83 DSGVO anführen, wenn der DSGVO-Verstoß durch einen – in der Praxis häufig eingeschalteten – Auftragsverarbeiter erfolgt:[450] Hier kann der bebußte Verantwortliche nämlich durchaus *ohne* jede Fahrlässigkeit handeln und wird – sanktionenrechtlich – trotzdem nur dann aus der Verantwortung entlassen, wenn sein Auftragsverarbeiter „Daten auf eine Weise verarbeitet hat, die nicht mit dem Rahmen oder den Modalitäten der Verarbeitung, wie sie vom Verantwortlichen festgelegt wurden, vereinbar ist oder auf eine Weise, bei der vernünftigerweise nicht davon ausgegangen werden kann, dass der Verantwortliche ihr zugestimmt hätte".[451] Wann das der Fall ist, und was hier den Maßstab bildet, bleibt beim gegenwärtigen Stand vielfach noch unklar. Gleiches gilt im Übrigen für die allgemeine Frage, wann ein Unternehmen als Verantwortlicher bei DSGVO-Verstößen überhaupt fahrlässig handelt: Der EuGH stellt dazu nur heraus, „dass ein Verantwortlicher für ein Verhalten, das in den Anwendungsbereich der DSGVO fällt, sanktioniert werden kann, wenn er sich über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte, gleichviel, ob ihm dabei bewusst war, dass es gegen die Vorschriften der DSGVO verstößt".[452] Auch diese

[449] Vgl. Art. 41 und Art. 45 NIS-2-RL und siehe zu Art. 21 Abs. 5 NIS-2-RL sowie § 30 Abs. 3 bis Abs. 5 BSIG-E sogleich ausführlich unten.

[450] EuGH 5.12.2023 – Rs. C-683/21(*Nacionalinis visuomenės sveikatos centras*) ECLI:EU:C:2023:949 Rn. 84.

[451] Vgl. zu Art. 28 Abs. 10 DSGVO EuGH 5.12.2023 – Rs. C-683/21 (*Nacionalinis visuomenės sveikatos centras*) ECLI:EU:C:2023:949 Rn. 85.

[452] Vgl. EuGH 5.12.2023 – Rs. C-807/21 (*Deutsche Wohnen SE/Staatsanwaltschaft Berlin*) ECLI:EU:C:2023:950 Rn. 76; EuGH 5.12.2023 – Rs. C-683/21 (*Nacionalinis visuomenės sveikatos centras*) ECLI:EU:C:2023:949 Rn. 81.

– aus dem EU-Kartellrecht stammende –[453] Formel schafft für sich genommen keine klaren Sorgfalts- und Verhaltensmaßstäbe für das Datenschutzrecht.[454]

Als weiteres Beispiel lässt sich das NIS-2-Regime zur Cybersicherheit anführen, welches seit dem 18. Oktober 2024 in allen EU-Mitgliedstaaten umzusetzen und anzuwenden ist.[455] Im Gegensatz zur DSGVO hat der Unionsgesetzgeber bei den Vorgaben zur Cybersicherheit auf Übergangsfristen verzichtet. Hinzu kommt in Deutschland eine ganz erhebliche Verzögerung bei der Umsetzung der NIS-2-Richtlinienvorgaben in das nationale Recht.[456] Just vor diesem Hintergrund mögen nun wiederum „Graubereiche" entstehen, in denen zwar einerseits hinreichend klare Verhaltensanforderungen fehlen, andererseits aber dem Normwortlaut nach empfindliche Geldbußen im Fall von – durch die jeweiligen Behörden als solche qualifizierten – Zuwiderhandlungen gegen das NIS-2-Regime vorgesehen sind. Die Wurzel des Problems liegt bei den Vorgaben zu branchen- bzw. tätigkeitsspezifischen Cybersicherheitsstandards: Hier konnte zum einen die EU-Kommission „bis 17. Oktober 2024" – und damit nur einen einzigen Tag vor Ablauf der Frist zur Umsetzung der NIS-2-RL – diverse sektorspezifische Normen zur Festlegung der im NIS-2-Regelungssystem zentralen „Risikomanagementmaßnahmen im Bereich der Cybersicherheit" erlassen.[457] Soweit keine unionalen Regelungen durch solche Durchführungs-

---

453 Vgl. nur aus dem kartellrechtlichen Kontext EuGH 18.6.2013 – Rs. C-681/11 (*Schenker & Co. u.a.*) ECLI:EU:C:2013:404 Rn. 37; EuGH 25.3.2021 – Rs. C-591/16 P (*Lundbeck/Kommission*) ECLI:EU:C:2021:243 Rn. 156; EuGH 25.3.2021 – Rs. C-601/16 P (*Arrow Group und Arrow Generics/Kommission*) ECLI:EU:C:2021:244, Rn. 97.

454 Im EU-Kartellrecht soll sich ein Unternehmen über die Rechtswidrigkeit einer Praktik dann nicht im Unklaren sein können, wenn es von einer veröffentlichten aufsichtsbehördlichen Auffassung abweicht, vgl. nur *Roßnagel/Rost*, ZD 2024, 183, 188. Vgl. statt vieler Immenga/Mestmäcker/*Biermann*, 7. Aufl. 2025, Vorb. Art. 23 VO 1/2003 Rn. 188 ff.

455 Vgl. Art. 41 NIS-2-RL.

456 Vgl. zur Umsetzungsverpflichtung bis zum 18.10.2024 einerseits nur Art. 41 NIS-2-RL sowie zur gepanten Umsetzung in Deutschland andererseits Referentenentwurf des BMI, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (Stand: 26.5.2025).

457 Vgl. den durch § 30 Abs. 3 und Abs. 4 BSIG-E in Bezug genommenen Art. 21 Abs. 5 und dort insbesondere UAbs. 2 NIS-2-RL, wonach die Kommission Durchführungsrechtsakte erlassen kann, „in denen die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen in Bezug auf andere als die in Unterabsatz 1 des vorliegenden Absatzes genannten wesentlichen und wichtigen Einrichtungen festgelegt werden".

rechtsakte der EU-Kommission getroffen werden, haben die nationalen Gesetzgeber zum anderen die Möglichkeit, eigene Vorgaben zu machen, was in Deutschland dem BMI als Verordnungsgeber in § 30 Abs. 5 BSIG-E überlassen wird.[458] Sodann stellt auch die i.R.d. NIS-2-Regimes geforderte Cyber-Sicherheitszertifizierung eine große Herausforderung dar, weil – in Ermangelung flächendeckend klarer Standards und potentieller Abweichungen durch untergesetzliche unionale wie nationale Regelungen – weder „one-size-fits-all"-Ableitungen aus bestehenden Zertifizierungsstandards, wie etwa ISO 270001, noch überhaupt alle sektorspezifischen Standards bis zum Ablauf der Umsetzungsfrist der NIS-2-RL rechtssicher zu gestalten und vollumfänglich zu zertifizieren sind.[459] Ob hier – trotz der in rechtlicher wie in tatsächlicher Hinsicht – zuweilen diffusen Vorgaben bereits Geldbußen verhängt werden, dürfte damit entscheidend von der jeweiligen Aufsichtspraxis in den Mitgliedstaaten abhängen.

Auch im Ordnungswidrigkeiten- und Sanktionenrecht erscheinen Geldbußen und andere Sanktionen, die „*sine lege certa*"[460] verhängt werden, zwar prinzipiell fragwürdig.[461] Soweit es nicht um unmittelbar pönale Sanktionen geht, lässt sich eine laxere Handhabung des „*lege certa*"-Erfordernisses durch in- und ausländische Datenschutz- oder Cyber-Sicherheitsbehörden freilich nicht ausschließen. Sollten in den soeben skizzierten DSGVO- oder NIS-2-Szenarien dennoch Geldbußen verhängt werden, so spricht viel für die Zulässigkeit von Geldbußendeckungen i.R.v. Cyber-Versicherungsverträgen: Denn sind schon die einzuhaltenden Sorgfaltsmaßstäbe (noch) nicht hinreichend klar umrissen, kann der Geldbußenadres-

---

458 § 30 Abs. 5 BSIG-E lautet auszugsweise: „Sofern die Durchführungsrechtsakte der Europäischen Kommission nach Artikel 21 Absatz 5 der NIS-2-Richtlinie keine abschließenden Bestimmungen über die technischen und methodischen Anforderungen sowie erforderlichenfalls über die sektoralen Anforderungen … enthalten, können diese Bestimmungen vom Bundesministerium des Innern und Heimat … präzisiert und erweitert werden.".

459 Vgl. zur Umsetzungsfrist erneut Art. 41 NIS-2-RL sowie zu den Durchführungsrechtsakten wiederum Art. 21 Abs. 5 NIS-2-RL und § 30 Abs. 3 bis Abs. 5 BSIG-E.

460 Der Grundsatz „*nullum crimen, nulla poena sine lege*" umfasst insbesondere auch das Verbot der Sanktion „*sine lege certa*" (Bestimmheitsgebot) sowie „*sine lege scripta*" (Gesetzesvorbehalt), „*sine lege praevia*" (Rückwirkungsverbot) und „*sine lege stricta*" (Analogieverbot).

461 Vgl. zum Ordnungswidrigkeitenrecht statt vieler KK-OWiG/*Mitsch*, 5. Aufl. 2018, Einleitung Rn. 122; BeckOK-OWiG/*Gerhold*, 44. Ed. 1.10.2024, § 3 OWiG Rn. 22 und insbesodnere Rn. 24 ff.

sat durch die drohende (regelmäßig ordnungswidrigkeitenrechtliche) Sanktion kaum zur lückenlosen und detailgetreuen Einhaltung eines – wie auch immer gearteten – Cyber-Security-Niveaus angehalten werden. Wenn einer Geldbuße in solchen – im Datenschutz- und Cyber-Sicherheitsrecht durchaus nicht seltenen – „Graubereichen" kaum Präventionsfunktion zukommt, so kann diese Präventionswirkung auch nicht durch Geldbußendeckungen in Cyber-Versicherungsverträgen vereitelt werden.

c) Zwischenergebnis: Unionale und nationale Präventionsrichtung als Maßstab

Nach der hier vertretenen Ansicht bleibt gerade im Kontext von Cyber-Risiken Raum für Deckungsbausteine, welche die Erstattung von Geldbußen vorsehen, die für (leicht) fahrlässige Verstöße, insbesondere in noch unzureichend geklärten „Graubereichen" z.B. des unionalen und nationalen Datenschutz- und Cyber-Sicherheitsrechts vorgesehen sind. Es gibt bei der Flut neuer Rechtsakte im Datenschutz-, IT-, Cybersicherheits- und KI-Bereich durchaus eine Reihe geldbußenbewehrter Tatbestände, in denen die (Verhaltens) Pflichten der Normadressaten noch nicht klar umrissen werden. Hier kann eine Geldbußendeckung für die betroffenen Unternehmen einerseits praktisch Sinn ergeben, ohne dass andererseits die mit solchen Geldbußen intendierten Ziele kompromittiert werden: Denn wo schon der einzuhaltende (Sorgfalts)Maßstab noch nicht hinreichend konkretisiert ist, kann auch diesbezüglich keine Individual- oder Generalprävention stattfinden. Ein Verstoß gegen die guten Sitten i.S.d. § 138 Abs. 1 BGB lässt sich hier jedenfalls kaum mit der Vereitlung von Präventionszielen begründen. Der Umstand allein, dass der Gesetzgeber die Verhängung einer Geldbuße auch insoweit für erforderlich gehalten hat, führt mangels einer mit dieser Geldbuße verbundenen effektiven Präventionswirkung ebenfalls nicht weiter.[462]

[462] Vgl. aber auch *Armbrüster/Schilbach*, r+s 2016, 109, 111 f.; Dickmann/*Schilbach*, Cyberversicherung, Ziff. A1-17.11 AVB-Cyber Rn. 3.

Allerdings – und das sei zugestanden – ist die rechtliche Zulässigkeit der Geldbußendeckung in solchen „Graubereichen“ sachlich-zeitlichen Schranken unterworfen: Werden Rechtsfragen geklärt und eindeutige Verhaltenspflichten – z.B. durch die Rechtsprechung des EuGH zur DSGVO oder zur NIS-2-RL – hinreichend klar definiert, mag sich das auch auf die Beurteilung i.R.d. § 138 Abs. 1 BGB und damit auf die Versicherbarkeit von Geldbußen infolge von Verstößen gegen ebendiese Verhaltenspflichten auswirken. Hier ist dann allerdings zu fragen, ob tatsächlich die Präventionsziele durch eine Geldbußen-Eigenschadendeckung i.R.v. Cyber-Versicherungsverträgen gänzlich vereitelt werden: Das kann ohne detaillierte Analyse der konkret intendierten Präventionsrichtung kaum pauschal beantwortet werden. Denn viele der im hiesigen Kontext relevanten Rechtsakte – insbesondere die DSGVO und die NIS-2-RL – sind zum einen gerade hinsichtlich der Sanktionswirkung unionsrechtlich determiniert, und zum anderen lässt sich die – aus der Sicht des EU-Rechts bezweckte und geforderte – Prävention womöglich auch ungeachtet einer Eigenschadendeckung für Geldbußen erreichen. Hierauf wird im Kontext des Unionsrechts noch gesondert und vertiefend einzugehen sein.[463] Festzuhalten bleibt, dass sich eine holzschnittartige Anwendung des § 138 Abs. 1 BGB gegenüber Geldbußendeckungen verbietet. Vielmehr erscheint eine Einzelfallbetrachtung unausweichlich, wie sie im Übrigen auch für die Versicherung von nach ausländischem Recht verhängten Geldbußen anzulegen ist.[464]

2. Italien: Allgemeines Verbot

Das italienische Recht wird zwar mit Blick auf die rechtliche Zulässigkeit von Lösegeldzahlungen nach Ransomware-Attacken oft als Paradebeispiel für ein Verbot sowohl von Lösegeldzahlungen als auch von Versicherungsleistungen für solche Zahlungen genannt.[465] Während diese Einordnung schon aufgrund des Wortlauts berech-

[463] Dazu ausführlich unter III.
[464] Dazu sogleich näher unter II.
[465] Vgl. etwa *Pache*, Kompass Cyberversicherungen, 2. Aufl. 2023, S. 205 m.w.N.

tigten Zweifeln begegnet und – soweit ersichtlich – auch nicht der dortigen Marktpraxis entspricht,[466] normiert Art. 12(1) *Codice delle Assicurazione Private* hingegen ausdrücklich ein allgemeines Verbot der Versicherung von Geldbußen. Die Norm lautet auszugsweise:

> *„Sono vietate le … assicurazioni che hanno per oggetto il trasferimento del rischio di pagamento delle sanzioni amministrative ... In caso di violazione del divieto il contratto è nullo…".*
>
> *Zu deutsch:*
>
> *„Versicherungen, welche die Übernahme des Risikos der Zahlung von verwaltungsrechtlichen Sanktionen … zum Gegenstand haben, …sind verboten… Ein Verstoß führt zur Nichtigkeit des Vertrags…".*

Eine weitere Präzisierung liefert Art. 4 Abs. 3 des Regolamento n°29 v. 16.3.2009 der italienischen Versicherungsaufsichtsbehörde IVASS:

> *„Non è assicurabile il rischio relativo al pagamento di una sanzione amministrativa anche nel caso di accollo da parte di un Ente della somma corrispondente alla sanzione comminata all'autore dell'illecito, quando l'Ente rinuncia alla rivalsa nei confronti del responsabile stesso."*
>
> *Zu deutsch:*
>
> *„Nicht versicherbar ist das Risiko der Zahlung von verwaltungsrechtlichen Sanktionen auch in Fällen, in denen ein Unternehmen die finanzielle Verpflichtung in Höhe der gegen den für den Verstoß Verantwortlichen verhängten Geldbuße übernimmt, wenn das Unternehmen auf den Regressanspruch gegen den Verantwortlichen verzichtet".*[467]

---

466 Dazu sogleich näher unter E II 1 a).

467 Die offizielle englische Fassung von Art. 4 Abs. 3 Regolamento n°29 v. 16.3.2009 lautet: „The risk relating to the payment of an administrative sanction may not be insured, also in case the entity assumes financial liability for the amount of the sanction imposed against the infringer, when the entity renounces its right of recourse against the infringer.".

Der Normwortlaut sieht dabei keine Einschränkung in sachlicher Hinsicht vor, so dass dieses Versicherungsverbot im Ausgangspunkt jede Form von behördlichen Sanktionen, einschließlich der durch Datenschutz- oder IT-Sicherheitsbehörden verhängten Bußgelder, erfasst.[468] Gleiches gilt für das – weitergehende – Verbot in Art. 4 Abs. 3 des Regolamento n°29 v. 16.3.2009. Teile des italienischen Schrifttums erstrecken dieses Versicherungsverbot nicht nur auf behördliche Bußgelder, sondern erwägen im Zuge der Anerkennung ausländischer *punitive damages awards* durch die Corto di Cassazione[469] grundsätzlich, z.B. Deckungskonzepte für die Verhaltenssteuerung und der Prävention dienende *punitive damages* an Art. 12(1) *Codice delle Assicurazione Private* sowie an Art. 4 Abs. 3 des Regolamento n°29 v. 16.3.2009 zu messen.[470]

3. Frankreich: Rechtsunsicherheit

Französische Instanzgerichte haben in der Vergangenheit die Versicherbarkeit von behördlichen Geldbußen verneint:[471] Die Versicherung solcher von Behörden ausgehenden Geldbußen verstoße – ebenso wie Deckungsschutz für durch Gerichte in Strafverfahren verhängte Geldstrafen[472] – gegen den *ordre public* gemäß Art. 6 Code civil.[473] Zur Begründung führt die Cour d'appel de Paris mit Blick auf „sanctions financières" der *Autorité des Marchés Finan-*

---

468 So im Ergebnis wohl auch *Pache*, Kompass Cyberversicherungen, 2. Aufl. 2023, S. 205.

469 Corte di Cassazione, Sezioni Unite, 5.7.2017, no.16601/2017 (englische Übersetzung veröffentlicht von *Quarta*, Italian Law Journal 3 (2017), 278 ff.).

470 So – allerdings mit einer differenzierten Lösung – *Cerini*, The polyfunctional role of punitive damages and the conundrum of their insurability: an Italian perspective, in: Bernitz/Mahmoudi/Bakardjieva Engelbrekt (eds.), Scandinavian Studies in Law 2018, S. 57, 70 f.

471 Siehe mit Blick auf „sanctions financières" der *Autorité des Marchés Financiers* nach Art. L621-15 *Code Monétaire et Financier* grundlegend Cour d'appel de Paris, 14.2.2012 n° 09/06711, JurisData: 2012-001924, vorausgehend: Tribunal de Grande Instance de Paris 8.1.2009 — RG n° 07/10204.

472 Grundlegend zu strafrechtlichen Sanktionen Cass. com. 21.6.1960, Bull. civ. IV n° 246; RGAT 1961, 53.

473 Art. 6 Code civil lautet auszugsweise: « ne peut déroger par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes moeurs ». Siehe auch Art. 1102 Code civil, der auszugsweise lautet: « La liberté contractuelle ne permet pas de déroger aux règles qui intéressent l'ordre public ». Siehe ferner Art. 1162 Code civil, der ebenfalls bestimmt, dass der « contrat ne peut déroger à l'ordre public ni par ses stipulations, ni par son but, que ce dernier ait été connu ou non par toutes les parties ».

ciers nach Art. L621-15 *Code Monétaire et Financier* aus, dass solche Geldbußen mit strafrechtlichen Sanktionen vergleichbar seien, da sie ebenfalls sowohl repressiven wie präventiven Zwecken dienten („double aspect répressif et dissuasif").[474] Die Cour d'appel de Paris bejaht damit den „quasi-pönalen" und sogar „neben-strafrechtlichen" Charakter („caractère para-pénal") solcher Verwaltungssanktionen.[475] Diese – aus Sicht der Cour d'appel für die Unversicherbarkeit solcher Geldbußen zentrale – Gleichsetzung begegnet indes durchaus dogmatischen Bedenken und findet in dieser Pointiertheit auch nicht durchweg eine Stütze in der Rechtsprechung der Cour de cassation, des Conseil d'état und des Conseil constitutionnel.[476]

Die Cour de cassation hat zur Frage der Versicherbarkeit von behördlichen Geldbußen bislang selbst nicht ausdrücklich Stellung bezogen: Zwar war sie bereits mit einer Konstellation befasst, in der ein Geschäftsleiter unter der D&O-Police Deckungsschutz für ein behördliches Bußgeld verlangte.[477] Die Cour de cassation konnte in diesem Deckungsstreit jedoch angesichts des vorsätzlichen Verhaltens den Versicherungsschutz ablehnen und musste sich dementsprechend nicht mit der Frage der Versicherbarkeit der Geldbuße auseinandersetzen.[478] Denn ebenso wie nach § 103 VVG im deutschen Versicherungsrecht besteht gemäß Art. L. 113-1 *Code des assurances* auch nach französischem Recht kein Versicherungsschutz bei der vorsätzlichen Herbeiführung des Versicherungsfalls („*faute intentionelle ou dolosive*"). In einem ähnlichen Verfahren konnte die Cour de cassation den Deckungsschutz angesichts der Kenntnis des Versicherungsnehmers der D&O-Versicherung vom Eintritt des Versicherungsfalls bei Vertragsschluss ablehnen: Eben-

474 Cour d'appel de Paris, 14.2.2012 n° 09/06711, JurisData: 2012-001924.

475 Die Cour d'appel de Paris, 14.2.2012 n° 09/06711, JurisData: 2012-001924.

476 Zurückhaltender unter Verweis auf die obergerichtliche Rechtsprechung deshalb z.B. *Bouvier*, Revue de jurisprudence commerciale – Les Cahiers du Chiffre et du Droit 5/2013, 1, 2 ff. dort m.w.N. In der Tat spricht die Cour de cassation nur von einer „condamnation administrative" und verzichtet auf solche Gleichsetzung der behördlichen Bußgelder der *Autorité des Marchés Financiers* mit strafrechtlichen Sanktionen, vgl. nur Cass. civ. 2ème 14.6.2012, n° 11-17.367, ECLI:FR:CCASS:2012:C201023 (*Frydman c/ Sté Chartis Europe*).

477 Cass. civ. 2ème 14.6.2012, n° 11-17.367, ECLI:FR:CCASS:2012:C201023 (*Frydman c/ Sté Chartis Europe*).

478 Cass. civ. 2ème 14.6.2012, n° 11-17.367, ECLI:FR:CCASS:2012:C201023 (*Frydman c/ Sté Chartis Europe*).

so wie § 2 VVG sieht Art. L. 124-5 al. 4 *Code des assurances* hier die Leistungsfreiheit des Versicherers vor.[479] Erneut musste sich die Cour de cassation damit nicht mit der Frage der Versicherbarkeit von behördlichen Bußgeldern auseinandersetzen und hat jedenfalls nicht explizit deren Versicherbarkeit verneint.[480] Nicht zuletzt vor diesem Hintergrund gehen Teile des französischen Schrifttums von der grundsätzlichen Versicherbarkeit behördlicher Bußgelder aus, soweit das Bußgeld nicht der Sanktion vorsätzlichen Verhaltens diene und damit schon nach Art. L. 113-1 *Code des assurances* aus der Deckung falle.[481]

Die *Groupe d'études Assurances* der französischen *Assemblée Nationale* unter der Leitung von *Valéria Faure-Muntian* hat sich dieser Auffassung angeschlossen und bejaht insbesondere die Versicherbarkeit von Bußgeldern, die durch die französische Datenschutzbehörde[482] bei DSGVO-Verstößen verhängt werden.[483] Zur Begründung verweist diese – rechtlich unverbindliche – Stellungnahme u.a. auf Art. L. 121-2 *Code des assurances*, demgemäß Versicherer frei seien, jedwede Schädigung ungeachtet des Verschuldensgrades zu versichern.[484] Auch regt die Stellungnahme einen verbindlichen Selbstbehalt zur Effektivierung der repressiven und präventiven Wirkung von Bußgeldern an.[485] Dem ist die Expertengruppe des *Haut Comité Juridique de la Place Financière de Paris* in einer – wiederum rechtlich nicht bindenden – Stellungnahme entgegengetreten, die von der grundsätzlichen Unversicherbarkeit von behördlichen Geldbußen – einschließlich der nach Art. 83, 84 DSGVO verhängten Bußgelder wegen Datenschutzverstößen –[486] ausgeht.[487]

---

479 Siehe zu dieser – speziell auf das Versicherungsfallprinzip bezogenen – Norm Cass. civ. 2ème 13.5.2019, n° 17-26.171, ECLI:FR:CCASS:2019:C200824 (*Société Avenir finance investment manager c/ Société Ace european group Limited*).

480 Cass. civ. 2ème 13.5.2019, n° 17-26.171, ECLI:FR:CCASS:2019:C200824 (*Société Avenir finance investment manager c/ Société Ace european group Limited*).

481 Z.B. *Kullmann*, JCP Entreprises 10/2009, 1226 ff.

482 Commission nationale de l'informatique et des libertés (CNIL).

483 *Groupe d'études Assurances*, Rapport La cyber-assurance, 2021, S. 14 ff.

484 *Groupe d'études Assurances*, Rapport La cyber-assurance, 2021, S. 15.

485 *Groupe d'études Assurances*, Rapport La cyber-assurance, 2021, S. 15.

486 Nach französischem Recht können die nach Art. 83 DSGVO zu verhängenden Bußgelder zum einen „amendes administratives" i.S.d. Art. 20 al. 3 n° 7 und zum anderen „astreintes" i.S.d. Art. 20 al. 3 n° 2 und Art. 21 al. 1 n° 6 *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* umfassen.

Dagegen sollen nach Auffassung der Expertengruppe des *Haut Comité Juridique de la Place Financière de Paris* aber dem Versicherungsnehmer entstehende Schäden versicherbar sein, soweit diese durch die Ausübung datenschutzbehördlicher „Abhilfebefugnisse" nach Art. 58 Abs. 2 DSGVO (mit Ausnahme von Bußgeldern nach Art. 58 Abs. 2 lit. i i.V.m. Art. 83 DSGVO) entstehen: Denn anders als bei Bußgeldern, die nach Art. 83 Abs. 1 DSGVO u.a. stets „abschreckend" sein müssen, gehe es hier nicht um Prävention.[488]

Während die Frage der Versicherbarkeit von behördlichen Geldbußen im französischen Recht damit weder durch den Gesetzgeber noch durch die Rechtsprechung abschließend geklärt ist, sprechen in der Zusammenschau wohl gewichtige Argumente gegen die Versicherbarkeit solcher Geldbußen: Neben der – wenn auch in dieser Deutlichkeit vereinzelt gebliebenen – Entscheidung der Cour d'appel de Paris[489] streitet die weitgehende Gleichsetzung der Repressions- und Präventionswirkung von strafrechtlichen Geldstrafen einerseits mit jenen Funktionen behördlicher Geldbußen andererseits gegen die rechtliche Zulässigkeit von Bußgelddeckungen.[490]

4. England und Wales

Das Recht von England und Wales kennt durchaus spezifische Versicherungsverbote für Geldbußendeckungen. So sieht im Bereich der durch die *Financial Conduct Authority (FCA)* verantworteten Finanzmarktaufsicht die Regelung in GEN 6.1.5 *FCA Handbook* folgendes vor:

> *„No firm may enter into, arrange, claim on or make a payment under a contract of insurance that is intended to have, or has or*

---

487 *Haut Comité Juridique de la Place Financière de Paris*, Rapport sur l'assurabilité des risques cyber v. 28.1.2022, S. 11 ff.

488 *Haut Comité Juridique de la Place Financière de Paris*, Rapport sur l'assurabilité des risques cyber v. 28.1.2022, S. 15 ff. Anders im Ergebnis wohl *Eggen*, Die Cyberversicherung, 2023, S. 213 ff.

489 Cour d'appel de Paris, 14.2.2012 n° 09/06711, JurisData: 2012-001924.

490 Zu diesem Ergebnis gelangt auch *Haut Comité Juridique de la Place Financière de Paris*, Rapport sur l'assurabilité des risques cyber v. 28.1.2022, S. 11 ff. m.w.N. aus der französischen Rechtsprechung.

> *would have, the effect of indemnifying any person against all or part of a financial penalty.“*[491]

Eine vergleichbare Regelung hat das *Information Commissioner's Office (ICO)* für den bei Cyber-Vorfällen relevanten Bereich des Datenschutzrechts noch nicht erlassen. Auch in sec. 155 bis sec. 159 Data Protection Act 2018[492] finden sich beim derzeitigen Stand keine ausdrücklichen Verbote von Geldbußendeckungen.

Die Frage der rechtlichen Zulässigkeit der Versicherung von Geldbußen i.R.v. Cyber-Versicherungsverträgen hängt nach dem englischen *common law* von dem auch als „*illegality defence*“ bekannten sog. *ex turpi causa*-Grundsatz ab: Im engeren Sinne besagt dieser Grundsatz, dass

> *„compensation was not recoverable for damage that flowed from … a fine or other punishment lawfully imposed as a consequence of one's own unlawful act.“*[493]

Die Rechtsprechung beurteilt danach die rechtliche Zulässigkeit der Durchsetzung eines solchen Ersatzanspruchs, der einen Bezug zu vorausgegangenem „illegalen“ Verhalten des Anspruchsstellers aufweist, im Wesentlichen anhand von drei Faktoren: *Erstens* ist zu fragen, ob durch die Anspruchsdurchsetzung – hier also die Erfüllung des Geldbußendeckungsversprechens – die mit der Geldbuße intendierte Prävention von Zuwiderhandlungen gegen die verletzte Verbotsnorm vereitelt würde; *zweitens*, ob im umgekehrten Fall der Nicht-Durchsetzung des Anspruchs andere gegenläufige öffentliche Interessen vereitelt oder beeinträchtigt würden und schließlich, *drittens*, der Grundsatz der Verhältnismäßigkeit.[494]

So hatte beispielsweise mit Blick auf die (Binnen)Regressfähigkeit von Unternehmensgeldbußen der Court of Appeal in *Safeway Stores Ltd v Twigger* den Regress eines durch die Kartellbehörde

---

491 Eingeführt durch General Provisions (Prohibition of insurance against fines) Instrument 2003, FSA 2003/92.

492 2018 c. 12.

493 *Gray v Thames Trains Ltd* [2009] AC 1339 Rn. 32 ff. (Lord Hoffmann).

494 Gefestigt durch *Patel v Mirza* [2016] UKSC 42 Rn. 101 (Lord Toulson).

bebußten Unternehmens gegen seinen Geschäftsleiter abgelehnt: Aus der Anwendung des *ex turpi causa*-Grundsatz folge, dass

> *„(i)t would be inconsistent for a claimant to be criminally and personally liable (or liable to pay penalties to a regulator such as the OFT) but for the same claimant to say to a civil court that he is not personally answerable for that conduct".*[495]

Demgegenüber hatte zuvor der High Court die Anwendbarkeit des *ex turpi causa*-Grundsatzes verneint und einen Regress gegen den Geschäftsleiter mit dem Argument zugelassen, dass das Unternehmen durch die Buße gerade nicht für (höchst)persönliches Fehlverhalten sanktioniert werde; mangels einer „*personally liability*" sei entsprechend die Erstattungsfähigkeit im Regresswege gegeben.[496] Gegen die soeben skizzierte Position des Court of Appeal in *Safeway Stores Ltd v Twigger* haben sich sodann Lord *Toulson* und Lord *Hodge* in einem *obiter dictum* in *Jetivia SA & Anor v Bilta (UK) Ltd & Ors* gewendet: Aus Sicht der Richter am UK Supreme Court könnten allenfalls *public policy*-Gründe gegen die Erstattung im Wege des Binnenregresses angeführt werden, wobei sie ausdrücklich keine Position dazu beziehen, ob solche Einwände bei (Kartell) Geldbußen durchgreifen.[497]

Aus dieser Entscheidungslinie ist zu ersehen, dass es jedenfalls der strafrechtlichen oder zumindest kartell- bzw. ordnungswidrigkeitenrechtlichen Vorwerfbarkeit und Verwerflichkeit („*moral turpitude*")[498] des mit einer Geldbuße oder -strafe sanktionierten Verhaltens bedarf, um sodann die „*illegality defence"* gegenüber der Erstattungsfähigkeit der Geldbuße auf Ebene des Zivilrechts zu tragen.[499] Daraus ist gefolgert worden, dass die „*illegality defence*" bei nicht schuldhaften Verstößen ausscheidet,[500] wobei diese mit Blick auf

---

495 *Safeway Stores Ltd v Twigger* [2010] EWCA Civ 1472 Rn. 16 (Longmore LJ).

496 *Safeway Stores Ltd v Twigger* [2010] EWHC 11 (Comm) (Flaux J).

497 *Jetivia SA & Anor v Bilta (UK) Ltd & Ors* [2015] UKSC 23 (Lord Toulson/Lord Hodge).

498 Zur Definition vgl. nur Les Laboratoires Servier & Anor v Apotex Inc & Ors [2014] UKSC 55 Rn. 23 ff. (Lord Sumption).

499 Vgl. erneut *Safeway Stores Ltd v Twigger* [2010] EWCA Civ 1472 Rn. 16 (Longmore LJ); *Les Laboratoires Servier & Anor v Apotex Inc & Ors* [2014] UKSC 55 Rn. 25 (Lord Sumption).

500 Vgl. *Sainsbury's Supermarkets Ltd v MasterCard Inc and Others* [2016] CAT v. 14.7. 2016 Rn. 290 ff. Vgl. auch *Sainsbury's Supermarkets Ltd v Mastercard Incorporated & Ors* [2018] EWCA Civ 1536 Rn. 37 ff.

Kartellrechtsverstöße getroffene Aussage ohne Weiteres auch auf geldbußenbewehrte Verstöße gegen andere Normen, z.B. des Datenschutz- oder des IT-Sicherheitsrechts, übertragbar erscheint. Während demnach zur Sanktion vorsätzlicher Verstöße dienende Geldbußen nicht versicherbar sind, kann die Erstattung von Geldbußen, die wegen schuldloser Zuwiderhandlungen verhängt werden, grundsätzlich wirksam in das Deckungsversprechen einer Cyber-Versicherung einbezogen werden.[501] Bei Geldbußen zur Sanktion fahrlässigen Verhaltens dürfte hingegen nach *Safeway Stores Ltd v Twigger* die Ersatzfähigkeit und damit die Versicherbarkeit eher zu verneinen sein, wobei im Einzelfall – nämlich bei geringem Verschulden und fehlender Verwerflichkeit („*moral turpitude*“) – durchaus auch eine andere Sichtweise der englischen Rechtsprechung denkbar erscheint.[502] Eine noch liberalere Haltung gegenüber der Versicherbarkeit von finanziellen Sanktionen legt indes die Rechtsprechung zu *punitive* bzw. *exemplary damages* nahe. Denn in *Lancashire County Council v. Municipal Mutual Insurance Limited* stellt der High Court heraus:

> *„There is no present authority in English law which establishes that it is contrary to public policy for an insured to recover under a contract of insurance in respect of an award of exemplary damages whether imposed in relation to his own conduct or in relation to conduct for which he is merely vicariously liable.“*[503]

Während es nach dieser Entscheidung also nicht zwingend auf den Grad (eigenen) Verschuldens ankommen soll, dürften auch hier „*public policy*“-Überlegungen eine Grenze dort ziehen, wo das Verhalten des Versicherten als „*criminal act*“[504] oder sonstiges „*especially outrageous misconduct*“, wie z.B. „*malice*“, zu qualifizieren ist.[505]

---

501 Dies gilt freilich nur, soweit nicht ein spezialgesetzliches Versicherungsverbot, z.B. nach GEN 6.1.5 *FCA Handbook* entgegen steht.

502 Vgl. einerseits *Safeway Stores Ltd v Twigger* [2010] EWCA Civ 1472 (Longmore LJ) und andererseits *Sainsbury's Supermarkets Ltd v Mastercard Incorporated & Ors* [2018] EWCA Civ 1536 Rn. 37 ff.

503 *Lancashire County Council v. Municipal Mutual Insurance Limited* [1996] 3 WLR 493 ff.

504 Vgl. *Askey v Golden Wine Co Ltd*, [1948] 2 All ER 35, 38 (Denning J); *Gray v Barr* (1971) 2 QB 554.

505 *Lancashire County Council v. Municipal Mutual Insurance Limited* [1996] 3 WLR 493 ff. Vgl. *UK Law Commission*, Aggravated, Exemplary and Restitutionary Damages (Law Com No 247, 1997), 90 ff., 167 und 170 ff.

Sollten diese Überlegungen auch auf Geldbußen übertragbar sein, so wäre der Kreis versicherbarer Szenarien deutlich weiter zu ziehen.[506]

5. USA

Geldbußen und Zivilstrafen (*fines and civil penalties*) sind in vielen Bundesstaaten der USA nicht versicherbar. So enthält beispielsweise sec. 533.5 *California Insurance Code* – auszugsweise – folgende Regelung:

> *„No policy of insurance shall provide, or be construed to provide, any coverage or indemnity for the payment of any fine, penalty, or restitution in any criminal action or proceeding or in any action or proceeding brought … by the Attorney General, any district attorney, any city prosecutor, or any county counsel … Any provision in a policy of insurance which is in violation … is contrary to public policy and void.“*

Dieses Verbot dürfte sich damit auch auf *administrative fines*[507] bzw. etwaige *civil penalties* erstrecken, die bei Datenschutzverstößen nach dem kalifornischen *California Consumer Privacy Act (CCPA)*[508] verhängt werden.[509]

Ein ähnliches Bild zeigt sich grundsätzlich auch im Bundesstaat New York, dessen *public policy* nach gefestigter Rechtsprechung die Versicherung von *fines* und *civil penalties* ebenfalls untersagt: Der „Stachel“ der Sanktion soll den Sanktionsadressaten selbst treffen und abschrecken, und die Bürde der Geldbuße soll nicht durch das Versichertenkollektiv getragen werden, zumal der Versicherer

---

506 Vgl. zu einer solchen liberalen Haltung zur Versicherbarkeit finanzieller Sanktionen erneut auch *UK Law Commission*, Aggravated, Exemplary and Restitutionary Damages (Law Com No 247, 1997), 90 ff., 167 und 170 ff.

507 Vgl. sec. 1798.155 *California Civil Code*.

508 Titel 1.81.5. *California Consumer Privacy Act of 2018*, sec. 1798.100 bis 1798.199.100 *California Civil Code*.

509 Vgl. zur Unversicherbarkeit von *civil penalities* nach sec. 533.5 *California Insurance Code* nur *Bulluck v. Maryland Casualty Company*, 85 Cal. App. 4th 1435 (Cal. Ct. App. 2001); *Allen v. Steadfast Insurance Company*, 2014 U.S. Dist. LEXIS 1994, (C.D. Cal. 22.8.2014). Vgl. ferner nur *Carter v. EnterCom Sacramento, LLC,* 219 Cal. App.4th 337 (Cal. Ct. App. 2013).

dann die Prämien für alle Versicherungsnehmer erhöhen könnte.[510] Darüber hinaus verbietet New York in sec. 27.11 Regulation 41[511] den der dortigen Aufsicht unterworfenen Versicherungs-Brokern, Versicherungsschutz im *excess line market* für all jene Risiken zu vermitteln, deren Deckung im Bundesstaat New York entweder gesetzlich verboten oder aber durch eine Entscheidung der Appellate Division des State Supreme Court or des Court of Appeals für mit der public policy unvereinbar erklärt worden ist.[512] Allerdings lässt die Rechtsprechung dann die Versicherung von „*statutory damages"* zu, wenn diese sowohl punitive als auch kompensatorische Elemente enthalten.[513] Dieser Ansatz ist in jüngerer Zeit verallgemeinernd auf Sanktionen erstreckt worden, die nicht allein strafende oder präventive Zwecke verfolgen.[514]

Demgegenüber untersagt die *public policy* von Delaware weder die Versicherung von *fines* und *civil penalties* noch von *punitive damages*.[515] Die Gerichte in diesem Bundesstaat dürften deshalb auch Deckungskonzepten für Geldbußen in Cyber-Versicherungsverträgen grundsätzlich offen gegenüberstehen: Die ständige Rechtsprechungspraxis betont explizit den besonderen Stellenwert der Vertragsfreiheit und

---

510 Vgl. nur *Silverman Neu, LLP v. Admiral Insurance Company*, 933 F. Supp. 2d 463 (E.D.N.Y. 2013); *J.P. Morgan Sec. Inc. v. Vigilant Ins. Co.*, 21 NY.3d 324, 334 (2013); *Zurich Ins. Co. v. Shearson Lehman Hutton, Inc.*, (N.Y. 1994); *Drexel Burnham Lambert Group, Inc. v. Vigilant Insurance Company*, 157 Misc. 2d 198, 595 N.Y.S.2d 999, 1010 (N.Y. Sup. Ct. 1993); *Padavan v. Clemente*, 43 A.D.2d 729, 730, 350 N.Y.S.2d 694 (2d Dep't 1973); *Public Serv. Mut. Ins. Co. v. Goldfarb*, 77 A.D.2d 521 (N.Y. App. Div. 1980).

511 11 CRR-NY 27.11.

512 *Office of General Counsel*, Opinion No. 08-08-09 v. 27.8.2008: Placement of Punitive Damages Insurance Coverage in the Excess Line Market, abrufbar unter: https://www.dfs.ny.gov/insurance/ogco2008/rg080809.htm (zuletzt abgerufen am 1.5.2025).

513 Vgl. *Navigators Ins. Co. v. Sterling Infosystems, Inc.,*145 A.D.3d 630 (N.Y. Sup. Ct., 2016).

514 Vgl. *J.P. Morgan Sec. Inc. v. Vigilant Ins. Co.*, No. 61 (N.Y. 23.11.2021) legt den Versicherungsvertrag aus Sicht eines verständigen Versicherungsnehmers so aus, dass eine im Vertrag als „*penalty*" bezeichnete Zahlung nicht zutrifft „*where a sanction has both compensatory and punitive components*". Vgl. auch *Call One Inc. v. Berkley Insurance Co.*, No. 21-CV-00466, 2022 WL 580802 (N.D. Ill. 25.2.2022).

515 Vgl. nur *Wilson v. Chem-Solv, Inc.*, No. 85CMY-1, 1988 Del. Super. LEXIS 372 (Super Ct. 14.10.1988); *U.S. Bank N.A. v. Indian Harbor Insurance Company*, 2014 U.S. Dist. LEXIS 91335, (D. Minn. 3.7.2014). Siehe ferner *Arch Insurance Co. v. Murdock*, 2018 WL 1129110, at 12 (Del. 1.3.2018); *Whalen v. On-Deck, Inc.*, 514 A.2d 1072, 1074 (Del. 1986): „(p)ublic policy in this State does not prohibit the issuance of an insurance contract that covers punitive damages."

„the right of sophisticated parties to enter into insurance contracts as they deem fit in the absence of clear indicia that … [a countervailing public] policy exists".[516]

Demnach ist das Bild der Versicherbarkeit von Geldbußen auch und gerade in den Bundesstaaten der USA sehr unterschiedlich. Dies führt zur Frage, wie in grenzüberschreitenden Konstellationen mit Versicherungsverboten umzugehen ist.[517]

II. International-privatrechtliche Herausforderungen von Geldbußendeckungen in marktüblichen Klauseln

Angesichts immer neuer Sanktionsinstrumente – etwa i.R.d. NIS-2-RL und der KI-VO –[518] und Rekordsummen fragen insbesondere global agierende Unternehmen Deckungskonzepte für Geldbußen nach. Der weit gefasste und zuweilen gar extraterritoriale Anwendungsbereich, z.B. von DSGVO, CCPA und PIPL, führt dazu, dass sich gerade solche Unternehmen potentiell weltweit Bußgeldern wegen Datenschutz- und/oder Cyber-Sicherheits-Verstößen ausgesetzt sehen.[519] Die Cyber-Bedingungswerke reagieren hierauf mit grundsätzlich weltweitem Versicherungsschutz,[520] wobei in der folgenden Darstellung die allgemeine *Non-admitted/Not-allowed*-Problematik ausgeklammert bleiben soll.[521] Marktgängige AVB legen zuweilen nahe, dass die Geldbußendeckung sodann nur von der rechtlichen Versicherbarkeit in einem einzigen (ausländischen) Staat abhängt – etwa dem Staat, dessen Behörde die Geldbuße er-

---

516 *RSUI Indemnity Company v. Murdock*, 2021 BL 76083 (Del. 3.3.2021); *Whalen v. On-Deck, Inc.*, 514 A.2d 1072, 1074 (Del. 1986).

517 Vgl. auch *RSUI Indemnity Company v. Murdock*, 2021 BL 76083 (Del. 3.3.2021), wo ein in Delaware inkorporiertes, aber in Kalifornien ansässiges Unternehmen Deckung begehrte, die nach kalifornischem Recht grundsätzlich ausgeschlossen erscheint.

518 Vgl. Art. 34 NIS-2-RL sowie Art. 99 Abs. 3 KI-VO.

519 Vgl. nur Art. 3 DSGVO sowie sec. 1798.140(a)(1) *California Civil Code*. Auch nach dem PIPL sind Geldbußen von bis zu 5 Prozent des Vorjahresumsatzes möglich.

520 Vgl. nur Ziff. A1-11 AVB Cyber 2024.

521 Dazu statt vieler *Armbrüster*, r+s 2023, 97, 98 ff.; *Ganzer,* Internationale Versicherungsprogramme, 2012, S. 194 ff.

lässt.[522] Allerdings wird in den in Deutschland marktgängigen Cyber-Versicherungsverträgen i.d.R. deutsches Recht gewählt und ein Gerichtsstand in Deutschland vereinbart.[523] Schon deshalb lautet bei einem Deckungsstreit die alles entscheidende Frage, welches in- und/oder ausländische Recht deutsche Gerichte insoweit heranziehen, um die Versicherbarkeit von Geldbußen zu bestimmen. Die zuweilen mit Blick auf das Kollisionsrecht geäußerte Annahme, dass die Versicherung von Geldbußen *per se* einen Verstoß gegen den *ordre public* (nach Art. 6 EGBGB bzw. Art. 21 Rom I-VO) darstelle,[524] erscheint demgegenüber allzu holzschnittartig und lässt vorrangige kollisionsrechtliche Mechanismen außer Acht.

Das lässt sich am nachfolgenden – fiktiven – Beispielfall illustrieren:[525] Protagonisten sind eine deutsche Gesellschaft als Cyber-Versicherungsnehmerin, die u.a. auch die weltweiten Aktivitäten ihrer finnischen Tochtergesellschaft in den Cyber-Versicherungsschutz einbezogen hat. Der Cyber-Versicherungsvertrag sieht eine Deckung für behördliche Geldbußen vor, und der Vertrag unterliegt kraft Rechtswahl deutschem Recht und erklärt in einer Gerichtsstandsklausel deutsche Gerichte für international zuständig. Die finnische Tochtergesellschaft bietet ihre (digitalen) Dienstleistungen u.a. auch einer Vielzahl von Kunden im US-Bundesstaat Kalifornien an. Die zuständige kalifornische Behörde sieht den territorialen Anwendungsbereich des CCPA[526] aufgrund dieses „doing business in the State of California“ als eröffnet an[527] und verhängt gegen die finnische Tochtergesellschaft eine Geldbuße in Form einer *administrative fine* wegen Verstößen gegen das Datenschutzniveau des CCPA.[528] Welches Recht entscheidet nun über die Versicherbarkeit der Geldbuße: Kommt es allein auf das Recht des die Geldbuße

522 Vgl. nur Ziff. 2.11. *Hiscox* CyberClear Bedingungen 10/2020.

523 Vgl. nur Ziff. B4-5.3 und Ziff. B4-6 AVB-Cyber 2024. Für die Zwecke der nachfolgenden Überlegungen wird die Wirksamkeit der Gerichtsstandswahl (vgl. Art. 15, 16 Brüssel Ia) ebenso wie der Rechtswahl im Fall von Großrisiken (vgl. Art. 7 Abs. 1 und Abs. 2 Rom I-VO) jeweils unterstellt.

524 In diesem Sinne wohl Prölss/Dreher/*Präve*, VAG, 13. Aufl. 2018, § 11 VAG Rn. 20 a.E.

525 Der Beispielfall geht zurück auf den Vortrag des Autors „Grenzüberschreitende Cyber-Risiken und anwendbares Recht“ an der Freien Universität Berlin am 27.9.2021. Das Beispiel sowie die Darstellung hat nun auch *Eggen*, Die Cyberversicherung, 2023, S. 218 ff., aufgegriffen.

526 Titel 1.81.5. *California Consumer Privacy Act of 2018*, sec. 1798.100 bis 1798.199.100 *California Civil Code*.

527 Vgl. sec. 1798.140(a)(1) *California Civil Code*.

528 Vgl. sec. 1798.155 *California Civil Code*.

verhängenden Staates – im Beispielfall also auf das kalifornische Recht – an? Oder auf das auf den Versicherungsvertrag anwendbare deutsche Recht?[529] Ist das Recht des Ortes maßgeblich, an dem die Versicherungsleistung zu erbringen ist – hier also potentiell finnisches Recht am Sitz der Tochtergesellschaft?[530] Oder sind womöglich alle Rechte relevant? Schon hier zeigt sich: Grenzüberschreitende Deckung für Geldbußen ist in Cyber-Versicherungsverträgen weitaus leichter versprochen als gewährt.

Allenfalls auf den ersten Blick halten marktübliche Klauseln eine eindeutige Antwort auf die Frage bereit, welches Recht darüber entscheidet, ob Geldbußen – z.B. wegen Datenschutzverstößen infolge von Cyber-Attacken – versicherbar sind: Manche AVB-Klauseln stellen ausschließlich darauf ab, ob das Recht des die Geldbuße verhängenden Staates insoweit ein Versicherungsverbot enthält (**dazu unter 1**). Schließlich finden sich auch kombinierte Ansätze, die noch weitere Rechtsordnungen hinzuziehen, etwa das Recht am Erfüllungsort der Versicherungsleistung sowie das auf den Cyber-Versicherungsvertrag anwendbare Recht (**dazu unter 2**). Die mit diesen Ansätzen in der praktischen Rechtsanwendung verbundenen international-privatrechtlichen Herausforderungen sollen im Folgenden anhand dieser Klauselvarianten illustriert werden. Dabei sind jeweils zwei Ebenen klar zu unterscheiden: Auf der einen Seite die sachlich-inhaltliche Reichweite des vertraglichen Deckungsversprechens für Geldbußen im jeweiligen Cyber-Versicherungsvertrag und auf der anderen Seite die Frage, ob dieses vertragliche Deckungsversprechen im Streitfall auch vor den kraft Gerichtsstandsklausel international zuständigen deutschen Gerichten mit Erfolg durchsetzbar wäre.

[529] Vgl. Art. 3 Rom I-VO.
[530] Vgl. Art. 9 Abs. 3 Rom I-VO.

1. Klauselvariante Nr. 1: Verbote in der das Bußgeld verhängenden Rechtsordnung

In der ersten Klauselvariante sagt der Cyber-Versicherer Deckung für Geldbußen zu, sofern kein Verbot in der das Bußgeld verhängenden Rechtsordnung besteht:

> *„Der Versicherer ersetzt – soweit dies in der ausländischen Rechtsordnung, nach der das Bußgeld verhängt wird, rechtlich zulässig sein sollte – Bußgelder".*

Im hiesigen Beispielfall wäre somit auf das kalifornische Recht abzustellen, wenn wegen CCPA-Verstößen die mitversicherte finnische Tochtergesellschaft der deutschen Cyber-Versicherungsnehmerin bebußt wird. Das kalifornische Recht steht der Versicherung von Geldbußen, die zur Ahndung von Gesetzesverstößen verhängt werden, ausweislich des sec. 533.5 *California Insurance Code* entgegen:

> *„No policy of insurance shall provide, or be construed to provide, any coverage or indemnity for the payment of any fine … is contrary to public policy and void."*

Dieses Verbot dürfte sich damit auch auf *administrative fines*[531] bzw. etwaige *civil penalties* erstrecken, die bei Datenschutzverstößen nach dem kalifornischen *California Consumer Privacy Act (CCPA)*[532] verhängt werden.[533] Bemerkenswert ist nun, dass nach der soeben zitierten Ziff. 2.11. der Klausel die Geldbußendeckung nur durch ausländische Verbote eingeschränkt werden soll, wohingegen das auf den Versicherungsvertrag anwendbare deutsche Recht ebenso wie etwaig beteiligte weitere Rechtsordnungen – zumindest prima facie – unbeachtlich bleiben. Allerdings dient Ziff. 2.11. der Klausel nur der sachlich-inhaltlichen Eingrenzung des

---

531 Vgl. sec. 1798.155 *California Civil Code*.

532 Titel 1.81.5. *California Consumer Privacy Act of 2018*, sec. 1798.100 bis 1798.199.100 *California Civil Code*.

533 Vgl. zur Unversicherbarkeit von *civil penalities* nach sec. 533.5 *California Insurance Code* erneut nur *Bulluck v. Maryland Casualty Company*, 85 Cal. App. 4th 1435 (Cal. Ct. App. 2001); *Allen v. Steadfast Insurance Company*, 2014 U.S. Dist. LEXIS 1994, (C.D. Cal. 22.8.2014). Vgl. ferner nur *Carter v. EnterCom Sacramento, LLC,* 219 Cal.App.4th 337 (Cal. Ct. App. 2013).

Deckungsversprechens.[534] Denn die Parteien können nicht einfach eine Teilrechtswahl zugunsten ausländischer Verbotsgesetze treffen und dadurch zugleich etwaige deutsche und/oder unionsrechtlich zwingende Normen abwählen. Das folgt im unionalen internationalen Schuldvertragsrecht bereits aus Art. 3 Abs. 3 und Abs. 4 sowie aus Art. 9 Rom I-VO. Sobald also der sachliche Deckungsumfang eröffnet ist, weil die verhängende Rechtsordnung – wie etwa das Recht von Delaware –[535] kein Versicherungsverbot vorsieht, lautet die zentrale Frage deshalb, welche weiteren Rechte und Rechtsnormen deutsche Gerichte bei einem Deckungsstreit heranziehen könnten.

Zu denken ist zunächst an das Recht am Erfüllungsort der Versicherungsleistung: Nach Art. 9 Abs. 3 Rom I-VO kann das Gericht „Eingriffsnormen des Staates, in dem die durch den Vertrag begründeten Verpflichtungen erfüllt werden sollen," anwenden.[536] Der Erfüllungsort ist hier Finnland. Dort existiert in der Tat ein aufsichtsrechtliches Verbot der Versicherung von Geldbußen durch finnische Versicherer, weil dies ein Verstoß gegen die „*good insurance practice*" wäre:

> *„According to the interpretation of the Financial Supervisory Authority (FIN-FSA), provision of insurance against administrative fines and penalty payments is contrary to good insurance practice and is therefore not permitted. The FIN-FSA's interpretation pertains equally to criminal fines as well as administrative fines and penalty payments, irrespective of whether they are imposed on the basis of a deliberate act, omission or negligence.*

---

534 Vgl. zu dieser Differenzierung zwischen versicherungsvertraglichem Deckungsversprechen einerseits und den Einwirkung – ausländischer bzw. unionaler – Verbotstatbestände aus der Perspektive des Rechts von England und Wales auch *Mamancochet Mining Ltd v Aegis Managing Agency Ltd & Ors* [2018] EWHC 2643 (Comm) (12.10.2018, *Teare* J Rn. 82). Vgl. ferner *Lamesa Investments Ltd v Cynergy Bank Ltd* [2020] EWCA Civ 821 (30.6. 2020, *Vos* C Rn. 39 ff.).

535 Vgl. erneut nur *Wilson v. Chem-Solv, Inc.*, No. 85CMY-1, 1988 Del. Super. LEXIS 372 (Super Ct. 14.10.1988); *U.S. Bank N.A. v. Indian Harbor Insurance Company*, 2014 U.S. Dist. LEXIS 91335, (D. Minn. 3.7.2014); *Arch Insurance Co. v. Murdock*, 2018 WL 1129110, at 12 (Del. 1.3.2018). Vgl. ferner *Whalen v. On-Deck, Inc.*, 514 A.2d 1072, 1074 (Del. 1986).

536 Siehe dazu bereits oben B II 3.

It is also of no consequence whether they are imposed on a legal or natural person."[537]

Während dieses Verbot noch mit aufsichtsrechtlichen Normen begründet wird und damit als auf die der finnischen Aufsicht als „*home regulator*" unterworfenen Versicherer begrenzt zu verstehen sein mag,[538] wird darüber hinaus womöglich ein allgemeineres Verbot auf die Verletzung von „*generally accepted social values*" gestützt: Es sei inakzeptabel, dass die Präventionswirkung von Geldbußen durch Versicherungsschutz beeinträchtigt werde.[539] Dieses Verbot ist nicht explizit auf inländische – d.h. von finnischen Behörden erlassene – Geldbußen sachlich beschränkt.[540] Ein solch allgemeines Verbot mag deshalb selbst der Versicherung drittstaatlicher Geldbußen durch ausländische Versicherer am Erfüllungsort Finnland entgegenstehen und als Eingriffsnorm des Erfüllungsortrechts nach Art. 9 Abs. 3 Rom I-VO von deutschen Gerichten zu beachten sein. Diese Frage ist – soweit ersichtlich – allerdings bislang noch nicht in der Gerichtspraxis aufgeworfen worden und damit ungeklärt.

Doch damit ist der Kreis potentiell tangierter Rechtsordnungen noch nicht geschlossen: Schließlich wird ein international zuständiges deutsches Gericht selbstverständlich auch die rechtlichen Schranken beachten, die das von den Parteien nach Art. 3 Rom I-VO als Versicherungsvertragsstatut gewählte deutsche Recht aufstellt. Darüber hinaus sind ungeachtet des Vertragsstatuts stets die Eingriffsnormen des Gerichtsstaates (*lex fori*) nach Art. 9 Abs. 1, Abs. 2

---

537 Vgl. *Financial Supervisory Authority (FIN-FSA)*, Interpretation 16.10.2018 – 2/2018: Insurability of administrative fines and penalty payments, FIVA 3/01.02/2018.

538 Vgl. auch *Financial Supervisory Authority (FIN-FSA)*, Interpretation 16.10.2018 – 2/2018: Insurability of administrative fines and penalty payments, FIVA 3/01.02/2018: „According to chapter 25, section 1, subsection 1 of the Insurance Companies Act, the FIN-FSA is responsible for supervising that insurance companies comply with insurance legislation and good insurance practice. 'Good insurance practice' is a concept from the Insurance Companies Act and an established principle in the insurance business. Insurance activity must not only be formally legal, but also ethically sound, fair and just, i.e. in line with good insurance practice".

539 *Financial Supervisory Authority (FIN-FSA)*, Interpretation 16.10.2018 – 2/2018: Insurability of administrative fines and penalty payments, FIVA 3/01.02/2018: „The FIN-FSA's view is that it is contrary to good insurance practice to provide insurance against a risk where the insurance might encourage actors' indifference to regulatory compliance and compromise actors' obligation to comply with the respective regulations. *Provision of insurance against such a risk is in conflict with generally accepted social values*." (Herv. d. Verf.).

540 Vgl. *Financial Supervisory Authority (FIN-FSA)*, Interpretation 16.10.2018 – 2/2018.

Rom I-VO anwendbar. Ein explizites und unmittelbar anwendbares Verbotsgesetz nach § 134 BGB existiert in Bezug auf Geldbußen freilich weder in der deutschen noch in der unionalen Rechtsordnung.[541] Jedoch ist hier stets nach der Berücksichtigungsfähigkeit ausländischer Verbotsnormen i.R.d. Sittenwidrigkeit gemäß § 138 Abs. 1 BGB zu fragen: Nach zutreffender und auch durch den EuGH in der *Nikiforidis*-Entscheidung gestützten Auffassung, steht Art. 9 Abs. 3 Rom I-VO keineswegs der gängigen Praxis deutscher Gerichte[542] entgegen, ausländische Verbotstatbestände zumindest als Faktum auf Ebene des materiellen Rechts zu berücksichtigen.[543] Dieser Punkt wird in der Zusammenschau weiterer Klauselvarianten sogleich noch zu vertiefen sein.[544] Festzuhalten bleibt indes bereits an dieser Stelle: Anders als Ziff. 2.11. der vorgenannten Klausel suggeriert, sind im Fall eines Deckungsstreits weit mehr Rechtsordnungen durch das Gericht zu konsultieren und damit zugleich potentielle Verbotstatbestände zu beachten, die das Deckungsversprechen entwerten können, als nur die Rechtsordnung, nach der das Bußgeld verhängt wurde.

2. Klauselvariante Nr. 2: Verbote des Vertragsstatuts und des Rechts am Erfüllungsort

Eine zweite der Cyber-Versicherungs-Praxis entnommene Klausel wählt einen anderen Ansatz als die erste Klausel:

> *„Der Versicherer bietet Versicherungsschutz für Geldbußen, die eine Datenschutzbehörde oder ein Gericht wegen einer Datenschutzverletzung gegen einen Versicherten … verhängt, sofern … einer solchen Versicherung nach dem Recht, dem dieser Versicherungsvertrag unterliegt und dem Recht des Landes, in dem die Versicherungsleistung zu erbringen ist, kein gesetzli-*

541 Siehe dazu erneut oben I.

542 Vgl. nur BGHZ 59, 82, 85 f.; BGHZ 94, 268, 271; BGH NJW-RR 2021, 1244 Rn. 31; OLG Frankfurt a. M. NJW 2018, 3591 Rn. 31 ff. und insbesondere Rn. 43; OLG München BeckRS 2020, 15428 Rn. 31 ff.; OLG Frankfurt IPRax 2025, 184 Rn. 69 ff.

543 EuGH 18.10.2016 – Rs. C-135/15 (*Nikiforidis*) ECLI:EU:C:2016:774 Rn. 40 ff. und 55. Enger indes z.B. Grüneberg/*Thorn* 84. Aufl. 2025, Art. 9 Rom I-VO Rn. 14.

544 Siehe unten 2.

ches Versicherungsverbot oder „ordre public“ entgegensteht und … insoweit kein behördliches Versicherungsverbot ergeht … .“[545]

Bei dieser Klauselgestaltung wird bereits das Deckungsversprechen selbst durch solche Verbotstatbestände begrenzt, die das auf den Versicherungsvertrag anwendbare deutsche Recht vorsieht. Ohnehin wird das international zuständige deutsche Gericht die Eingriffsnormen des deutschen Rechts – wenn auch nicht als Teil des Vertragsstatuts, so doch als Eingriffsnormen der *lex fori* i.S.d. Art. 9 Abs. 2 Rom I-VO – anwenden.[546] Zugleich wird auch auf etwaige Verbote an dem Ort abgestellt, an dem die Versicherungsleistung erbracht werden soll – hier also am Sitz der Auslandstochter in Finnland. Im Gegensatz zum ersten Klausel-Beispiel schweigt dieses Wording jedoch zum möglichen Einfluss des Rechts des Staates, dessen Behörden oder Gerichte das Bußgeld verhängen – im hier gebildeten Beispielfall wäre dies demnach das Recht des US-Bundesstaates Kalifornien. Anders ausgedrückt, verspricht der Cyber-Versicherer also auch Deckung von Geldbußen, ungeachtet etwaiger Versicherungsverbote im Erlassstaat. Hier drängt sich nun die Frage auf, ob ein deutsches Gericht im Falle eines Deckungsstreits die Eintrittspflicht des Cyber-Versicherers dennoch auch an etwaigen Versicherungsverboten im kalifornischen Recht messen würde. Dabei handelt es sich jedoch nicht um einen Fall des Art. 9 Abs. 3 Rom I-VO, weil der Erfüllungsort der Versicherungsleistung gerade nicht im Erlassstaat (d.h. in Kalifornien), sondern vielmehr am Sitz der Tochtergesellschaft der Versicherungsnehmerin (d.h. in Finnland) liegt. Bei dem Versicherungsverbot in sec. 533.5 *Califor-*

---

545 Die vollständige Klausel lautet: „Der Versicherer bietet Versicherungsschutz für Geldbußen, die eine Datenschutzbehörde oder ein Gericht wegen einer Datenschutzverletzung gegen einen Versicherten zum Abschluss eines behördlichen Verfahrens gemäß Ziffer I.3.1. (Behördliche Verfahren) dieses Vertrages verhängt, sofern
a) es sich nicht um eine Geldbuße strafrechtlichen Charakters handelt und
b) einer solchen Versicherung nach dem Recht, dem dieser Versicherungsvertrag unterliegt und dem Recht des Landes, in dem die Versicherungsleistung zu erbringen ist, kein gesetzliches Versicherungsverbot oder „ordre public“ entgegensteht und
c) insoweit kein behördliches Versicherungsverbot ergeht und
d) die Datenschutzverletzung nicht vorsätzlich begangen wurde.“

546 Art. 9 Abs. 2 Rom I-VO lautet: „Diese Verordnung berührt nicht die Anwendung der Eingriffsnormen des Rechts des angerufenen Gerichts“. Zur Frage der Anwendung von Eingriffsnormen im Wege einer Sonderanknüpfung statt aller BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 9 Rom I-VO Rn. 87 ff.

nia Insurance Code[547] handelt es sich aus der Perspektive eines deutschen Gerichts somit um Eingriffsnormen eines sonstigen Drittstaats, die von Art. 9 Rom I-VO nicht unmittelbar erfasst werden.

Allerdings entspricht es der gefestigten Rechtsprechungspraxis deutscher Gerichte, dass – jenseits der Eingriffsnormen der *lex fori* und des Erfüllungsortes – auch weitere ausländische Verbotsnormen i.R.d. § 138 Abs. 1 BGB unter bestimmten Voraussetzungen herangezogen werden können: Dabei geht es indes nicht um die unmittelbare Anwendung, sondern vielmehr um die materiell-rechtliche „Berücksichtigung" der Normen als ein Faktum, welches ggf. das Verdikt der Sittenwidrigkeit gemäß § 138 Abs. 1 BGB zu begründen vermag.[548] Seit der „nigerianischen Masken"-Entscheidung des BGH ist anerkannt, dass ausländische Eingriffsnormen materiell-rechtlich insbesondere über § 138 Abs. 1 BGB berücksichtigt werden können, wenn diese Normen entweder (mittelbar) deutsche Interessen schützen oder aber diesen Regelungen legitime und anerkennenswerte öffentliche Interessen zugrunde liegen, die ein „allgemein zu achtendes Interesse aller Völker" darstellen und sich daher weitgehend mit den inländischen Interessen decken.[549] Zumindest mit Blick auf den Kulturgüterschutz hat der BGH eine solche Interessenkonvergenz frühzeitig bejaht und einer nigerianischen Norm des Kulturgüterschutzes über § 138 Abs. 1 BGB ein Versicherungsverbot entnommen.[550] Der EuGH hat in der Rechtssache *Nikiforidis* die materiell-rechtliche Berücksichtigung ausländischer Normen ausdrücklich gebilligt und in Art. 9 Abs. 3 Rom I-VO insoweit keine Hürde gesehen.[551]

---

547 Die Norm lautet auszugsweise: „No policy of insurance shall provide, or be construed to provide, any coverage or indemnity for the payment of any fine … is contrary to public policy and void."

548 Vgl. aus der Rechtsprechungspraxis nur BGHZ 59, 82, 85 f.; OLG Frankfurt NJW 2018, 3591 Rn. 31 ff. und insbesondere Rn. 43 ff.; OLG München BeckRS 2020, 15428 Rn. 31 ff.; OLG Frankfurt IPRax 2025, 184 Rn. 69 ff.

549 Vgl. nur BGHZ 59, 82, 85 f. Deutlich zuletzt etwa BGH NJW-RR 2021, 1244 Rn. 31: „Der Verstoß gegen ausländisches Recht kann zwar nach § 138 Abs. 1 BGB die Nichtigkeit der Vereinbarung zur Folge haben. Das ist aber nur anzunehmen, wenn die verletzten ausländischen Bestimmungen mittelbar auch deutsche Interessen schützen oder ihre Umgehung allgemein zu achtenden Interessen aller Völker widerspricht."

550 BGHZ 59, 82, 85 f.

551 EuGH 18.10.2016 – Rs. C-135/15 (*Nikiforidis*) ECLI:EU:C:2016:774 Rn. 40 ff. und 55. Enger und differenzierend m.w.N. BeckOGK/*Maultzsch*, 1.3.2025, Art. 9 Rom I-VO Rn. 153 ff.

Betrachtet man die hier interessierende Fallgestaltung der Geldbußen-Deckung durch Cyber-Versicherer nun vor dem Hintergrund der BGH-Judikatur, so lautet die – bislang ungeklärte – Frage, ob die potentielle Vereitelung der Präventionswirkung von drittstaatlichen Geldbußen, die der Sanktion von Datenschutzverstößen dienen, nun ebenfalls einen Verstoß gegen die deutschen guten Sitten gemäß § 138 Abs. 1 BGB begründen kann.[552] Obschon sich die jeweiligen regulatorischen Instrumente ebenso wie die Regelungsdichte durchaus unterscheiden, wird der Datenschutz als Regelungsziel und als öffentliches Interesse weltweit in der Tat zunehmend anerkannt: In der auf mehr als 1250 Seiten angelegten rechtsvergleichenden Studie „*Data Protection Laws of the World*" wird schon im Jahre 2022 rund der Hälfte der Staaten ein zumindest „robustes" und nahezu 90% der Staaten ein zumindest „begrenztes" Regulierungs- und Durchsetzungsniveau im Bereich des Datenschutzes attestiert.[553] Vor diesem Hintergrund lässt sich nun durchaus argumentieren, dass die effektive Durchsetzung eines (Mindest)Datenschutzniveaus mittlerweile ein „allgemein zu achtendes Interesse aller Völker" darstellt.[554] Die öffentlichen Interessen von ausländischen (Dritt)Staaten erscheinen nach der Lesart des BGH jedenfalls insoweit i.R.d. Auslegung und Anwendung von Generalklauseln anerkennenswert, als sich diese Interessen mit denen der überwiegenden Vielzahl von Staaten – einschließlich des Inlands – decken.[555] Damit nähert sich der BGH dem Grundsatz des entgegenkommenden völkerrechtsfreundlichen Verhaltens staatlicher Stellen i.S.d. *comitas gentium* durchaus an.[556]

Mit diesem Begründungsansatz ließe sich prinzipiell auch einer etwaigen Beeinträchtigung der Präventionswirkung von Geldbußen

---

552 Vgl. zur grundsätzlichen Orientierung am Inland und zur Problematik ausländischer Wertungen nur MünchKommBGB/*Armbrüster*, 10. Aufl. 2025, § 138 BGB Rn. 28 ff. m.w.N.

553 Vgl. *DLA Piper*, Data Protection Laws of the World (2025) sowie die begleitende Übersichtskarte, abrufbar unter: https://www.dlapiperdataprotection.com/ (zuletzt abgerufen am 1.5.2025).

554 Vgl. zum Kulturgüterschutz BGHZ 59, 82, 85 f.

555 Vgl. erneut BGHZ 59, 82, 85 f. Siehe statt vieler MünchKommBGB/*Armbrüster*, 10. Aufl. 2025, § 138 BGB Rn. 29 f.

556 Siehe nur *Armbrüster*, VersR 2016, 1, 4; *Eggen*, Die Cyberversicherung, 2023, S. 233 m.w.N. Die *comitas gentium* ist freilich vom Grundsatz der Völkerrechtsfreundlichkeit zu unterscheiden, weil bei der Berücksichtigung einzelstaatlicher Verbote gerade keine bindenden völkerrechtlichen Normen in Rede stehen, vgl. mit Blick auf die Bindung von Staatsorganen nur BVerfGE 112, 1, 24. Vgl. auch BVerfGE 58, 1, 34; BVerfGE 59, 63, 89.

begegnen: Wird das Ziel des Datenschutzes ebenso wie die effektive Ahndung von Verstößen als legitimes und anerkennenswertes öffentliches Interesse sowohl des Erlassstaates als auch Deutschlands anerkannt, so könnte über § 138 Abs. 1 BGB womöglich ein ausländisches Versicherungsverbot materiell-rechtlich berücksichtigt und die Deckung einer von ausländischen Behörden zu Sanktion von Datenschutzverstößen verhängten Geldbuße verhindert werden.[557] In der zum Kulturgüterschutz ergangenen Leitentscheidung stellte der BGH zumindest in Bezug auf mit einem ausländischen Exportverbot belegte „nigerianische Masken" heraus, dass ein deutschem Recht unterliegender Transportversicherungsvertrag insoweit eine „Beeinträchtigung (darstelle, der) kein bürgerlichrechtlicher Schutz zuteilwerden kann".[558] Überträgt man diese Argumentation z.B. auf Datenschutz- und womöglich auch auf Cyber-Sicherheitsvorschriften, so liegt es keineswegs fern, die zur Gewährleistung einer effektiven Präventionswirkung von drittstaatlichen Bußgeldern erlassenen ausländischen Versicherungsverbote – z.B. nach dem kalifornischen CCPA – über § 138 Abs. 1 BGB zu berücksichtigen.

Auch wenn man sich dieser Sichtweise anschließen möchte,[559] wird man die Interessenkonvergenz und damit eine materiell-rechtliche Berücksichtigung ausländischer Versicherungsverbote über § 138 Abs. 1 BGB zutreffenderweise immer nur insoweit befürworten können, als es um Geldbußen geht, die auch im Inland rechtlich missbilligte Handlungen – wie etwa Datenschutz- und/oder Cyber-Sicherheitsverstöße – sanktionieren. Das wird man immer dann verneinen müssen, wenn ausländische Behörden mit den Geldbußen sachfremde (wirtschafts)politische Fernziele verfolgen oder die Sanktionen völlig willkürlich und außerhalb jedweden rechtsstaatlichen Verfahrens verhängen. In solchen Fallgestaltungen fehlt schon die für die Berücksichtigung ausländischer Verbotsgesetze erforderliche Konvergenz der in- und ausländischen (Präventions)Interes-

[557] Vgl. erneut BGHZ 59, 82, 85 f.
[558] BGHZ 59, 82, 85 f.
[559] Dafür z.B. *Eggen*, Die Cyberversicherung, 2023, S. 233 f.

sen.[560] Das muss erst recht in Bereichen gelten, in denen der nationale oder unionale Gesetzgeber seine Missbilligung der jeweiligen ausländischen (Sanktions)Praxis durch entsprechende Rechtsakte klar zum Ausdruck gebracht hat.[561] Hier wie dort stehen gerade keine „allgemein zu achtende(n) Interesse(n) aller Völker" im Raum, die eine materiell-rechtliche Berücksichtigung ausländischer Versicherungsverbote über § 138 Abs. 1 BGB erst ermöglichen.[562]

3. Zwischenergebnis: Verbote aus multiplen Rechtsordnungen – auch jenseits der „ordre public"-Klausel

Zusammenfassend bleibt mit Blick auf die beiden vorgenannten Beispiel-Klauseln festzuhalten, dass in einem Deckungsstreit vor deutschen Gerichten jeweils mehr Rechtsordnungen – und damit auch potentielle Versicherungsverbote – zu berücksichtigen sind, als die AVB-Klauseln zunächst vermuten lassen.

Anders als manche der am Markt für Cyber-Versicherung gängigen AVB auf den ersten Blick suggerieren mögen, kann die Durchsetzbarkeit des Geldbußen-Deckungsversprechens gerade in Sachverhalten mit diversen Auslandsbezügen an Versicherungsverboten aus unterschiedlichen Rechtsordnungen scheitern: Neben dem gemäß Art. 3 Rom I-VO als Vertragsstatut gewählten Recht sind die Eingriffsnormen des Gerichtsstaates nach Art. 9 Abs. 1, Abs. 2 Rom I-VO stets anwendbar. Ist die Versicherungsleistung in einem anderen Staat – etwa am Sitz eines mitversicherten Tochterunternehmens – zu erbringen, kann das Gericht auch die dortigen Versicherungsverbote mit Eingriffsnormcharakter nach Art. 9 Abs. 3 Rom I-VO berücksichtigen. Im Gefolge der „Nigerianische Masken"-Entscheidung des BGH und der Rechtssache „Nikiforidis" des EuGH bleibt zudem eine materiell-rechtliche Berücksichtigung ausländi-

---

560 OLG Frankfurt IPRax 2025, 184 Rn. 77. So schon *Eggen*, Die Cyberversicherung, 2023, S. 234. Siehe auch MünchKommBGB/*Armbrüster*, 10. Aufl. 2025, § 138 BGB Rn. 29.

561 Vgl. mit Blick auf die EU-Blocking-VO und den Iran-Sanktionen der USA etwa EuGH 21.12.2021 – Rs. C-124/20 (*Bank Melli Iran/Telekom Deutschland*), ECLI:EU:C:2021:1035 Rn. 69 ff.; OLG Frankfurt IPRax 2025, 184 Rn. 77.

562 Vgl. zum Kulturgüterschutz wiederum BGHZ 59, 82, 85 f.

scher Versicherungsverbote über die bürgerlich-rechtlichen Generalklauseln möglich. Damit kann auch ein Versicherungsverbot des die Geldbuße verhängenden Staates über § 138 Abs. 1 BGB grundsätzlich durch deutsche Gerichte berücksichtigt werden.

Dabei bedarf es – bei der hier vorausgesetzten internationalen Zuständigkeit eines deutschen Gerichts und der Wahl deutschen Rechts – im Deckungsstreit keines Rückgriffs auf den kollisionsrechtlichen *ordre-public*-Vorbehalt nach Art. 21 Rom I-VO.[563] Folgt man den hiesigen Erwägungen zum deutschen Sachrecht im Kontext des § 138 Abs. 1 BGB[564] und analysiert man sodann die unionsrechtlichen Vorgaben zur effektiven Präventionswirkung,[565] so dürfte darüber hinaus auch eine Deckung von Geldbußen unter fremdem Recht keineswegs dem deutschen bzw. unionalen *ordre public* i.S.d. Art. 21 Rom I-VO oder gar dem anerkennungsrechtlichen *ordre public* nach Art. 45 Brüssel Ia-VO automatisch „offensichtlich" widersprechen.[566] Bei ausländischen Versicherungsverboten bedarf es hier jeweils eines hinreichend festen Bandes zu den grundlegenden inländischen Gerechtigkeitsvorstellungen. Dass nun deutsche öffentliche Interessen[567] durch die Versicherbarkeit von im Ausland verhängten Geldbußen in einer Weise beeinträchtigt wer-

563 Nach Art. 21 Rom I-VO kann die Anwendung einer durch die Kollisionsnormen der Rom I-VO zur Anwendung berufenen Rechtsnorm „nur versagt werden, wenn ihre Anwendung mit der öffentlichen Ordnung („ordre public") des Staates des angerufenen Gerichts offensichtlich unvereinbar ist."

564 Siehe dazu erneut oben I 1.

565 Siehe dazu gleich noch ausführlich unten III.

566 Zumindest die Grenzen, innerhalb deren ein mitgliedstaatliches Gericht den – kollisions- und anerkennungsrechtlichen – *ordre public* in Stellung bringen kann, überwacht dabei der EuGH, deutlich zuletzt EuGH 7.9.2023 – Rs. C-590/21 (*Charles Taylor Adjusting Ltd*) ECLI:EU:C:2023:633 Rn. 33 f.: „Zwar können die Mitgliedstaaten aufgrund des Vorbehalts in dieser Bestimmung grundsätzlich selbst festlegen, welche Anforderungen sich nach ihren innerstaatlichen Anschauungen aus ihrer öffentlichen Ordnung ergeben, jedoch gehört die Abgrenzung dieses Begriffs zur Auslegung dieser Verordnung … . Auch wenn es demnach nicht Sache des Gerichtshofs ist, den Inhalt der öffentlichen Ordnung eines Mitgliedstaats zu definieren, hat er doch über die Grenzen zu wachen, innerhalb deren sich das Gericht eines Mitgliedstaats auf diesen Begriff stützen darf, um der Entscheidung eines Gerichts eines anderen Mitgliedstaats die Anerkennung zu versagen." Gleichsinnig zum anerkennungsrechtlichen ordre public schon EuGH 28.3.2000 – Rs. C-7/98 (*Krombach*) ECLI:EU:C:2000:164 Rn. 22; EuGH 7.4.2022 – Rs. C-568/20 (*H Limited*) ECLI:EU:C:2022:264 Rn. 42. Vgl. zu Inhalt und Handhabung des nationalen und unionalen *ordre public* nur BeckOK BGB/*Spickhoff*, 73. Ed. 1.8.2024, Art. 21 Rom I-VO Rn. 1 ff.; MüchKomm BGB/*von Hein*, 9. Aufl. 2024, Art. 6 EGBGB Rn. 168 ff. und Rn. 141 ff. A.A. wohl Prölss/Dreher/*Präve*, VAG, 13. Aufl. 2018, § 11 VAG Rn. 20 a.E. Zurückhaltender *Armbrüster/Schilbach*, r+s 2016, 109, 112.

567 Vgl. Erwägungsgrund 37 S. 1 Rom I-VO.

den, dass das Rechtsanwendungsergebnis mit der hiesigen öffentlichen Ordnung „offensichtlich unvereinbar" ist, bedarf – gerade angesichts der aufgezeigten Rechtsprechungslinie des BGH und mancher Instanzgerichte –[568] vielmehr einer ausführlichen Begründung. Zu fragen ist also nicht allein, ob der Zweck der jeweiligen Sanktion des ausländischen Staates vereitelt zu werden droht, sondern notwendigerweise, inwieweit dieses Ergebnis zusätzlich auch mit der inländischen öffentlichen Ordnung schlechthin unvereinbar ist.[569]

Festzuhalten bleibt, dass sich die kollisions- und sachrechtliche Durchsetzung von Versicherungsverboten im Deckungsstreit kaum allein an den – teils überaus liberal anmutenden – AVB-Gestaltungen orientiert. Versicherungsnehmer, die sich auf derartige vertragliche Konstruktionen verlassen, sehen sich damit erheblichen Unwägbarkeiten bei der Durchsetzung ihrer Geldbußendeckung gegenüber.

III. Unionale Dimension der Versicherbarkeit: sanktionenrechtlicher Effektivitätsgrundsatz

Bei Geldbußen, die innerhalb der EU durch die Behörden anderer EU-Mitgliedstaaten verhängt werden, wird ein ganz zentraler Punkt in der bisherigen Debatte oft übergangen. Als Illustration einer solchen Fallgestaltung mag der bereits oben gebildete Beispielfall dienen,[570] in dem nun aber nicht eine Behörde des US-Bundesstaates Kalifornien, sondern vielmehr eine französische Behörde das unter einer deutschem Recht unterliegenden Cyber-Police mitversicherte finnische Tochterunternehmen z.B. nach der DSGVO bebußt. Hier

[568] Vgl. zur BGH Rechtsprechung erneut oben I 1 und vgl. aus dem D&O-Kontext erneut LG Frankfurt 20.1.2023 – 2-08 O 313/20 (juris) Rn. 49 ff., das sich überzeugend gegen den Einwand des D&O-Versicherers wendet, dass das Deckungsversprechen gegen § 138 Abs. 1 BGB verstoße und nichtig sei. Das OLG Frankfurt 21.11.2023 – 18 U 17/23 (unveröffentlicht) konnte diese Frage offenlassen (dort unter II 4 g der Gründe).

[569] Vgl. BeckOGK BGB/*Lüttringhaus*, 1.12.2023, Art. 7 Rom I-VO Rn. 193 („soweit"). Vgl. auch *Armbrüster/Schilbach*, r+s 2016, 109, 112; Staudinger/*Armbrüster*, 2021, Anh zu Art 7 Rom I-VO Rn. 81.

[570] Vgl. oben II.

suggerieren rechtsvergleichende Studien großer Anwaltskanzleien und auch der OECD, dass es für die Frage der Versicherbarkeit solcher Geldbußen zuvörderst auf das jeweilige nationale Recht – hier also auf französisches, deutsches und finnisches Recht ankäme.[571] Das ist aber nur die halbe Wahrheit: Denn die Präventionswirkung einer etwa durch die DSGVO oder auch die NIS-2-RL geforderten Geldbuße ist gerade durch die EU-Rechtsakte und damit unionsrechtlich vorgegeben. Der EuGH hat in diesem Kontext einen besonderen „sanktionsrechtlichen Effektivitätsgrundsatz" entwickelt, wonach stets eine „verhältnismäßige, wirksame und abschreckende Sanktion" von Verstößen gegen die jeweilige unionale Norm geboten ist.[572] Allgemein halten der Effektivitäts- und der Äquivalenzgrundsatz die Mitgliedstaaten an, das Unionsrecht effektiv sowie in gleicher Weise und nach den gleichen Modalitäten wie das nationale Recht durchzusetzen.[573] Die sanktionenrechtliche Ausprägung dieser Grundsätze wirkt in jene Regelungsbereiche hinein, in denen das EU-Sekundärrecht zwar einerseits effektive, verhältnismäßige und abschreckende Sanktionen als Ziel vorgibt, aber andererseits die konkrete Gewährleistung dem mitgliedstaatlichen Recht überantwortet. Hier beeinflusst der Effektivitäts- und Äquivalenzgrundsatz ggf. nicht-harmonisierte Regelungsfelder – wie z.B. das Ordnungswidrigkeitenrecht – und stellt sicher, dass sich die mitgliedstaatlichen Sanktionsinstrumente stets in dem unionsrechtlich gebotenen Rahmen bewegen.[574]

Deshalb steht bei Geldbußen, die – im Falle einer Verordnung unmittelbar und bei Richtlinien zumindest mittelbar – auf unionsrechtlichem Fundament ruhen, stets die Frage nach der Einhaltung ebendieses sanktionenrechtlichen Effektivitätsgrundsatzes im Raum.

---

571 Vgl. *OECD*, Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation, 2020, S. 14 ff.; *DLA Piper/Aon*, The price of data security: A guide to the insurability of GDPR fines across Europe, 3rd ed. 2020, S. 11 ff.; *Marsh*, GDPR Fines and Penalties: Insurability will Vary by Location, Policy Details, and More, September 2018, S. 1 ff.

572 *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, S. 20 ff.

573 Grundlegend EuGH 16.12.1976 – Rs. 33/76 (*Rewe*) Slg. 1976, 1989 Rn. 5; EuGH 16.12.1976 – Rs. 45/76 (*Comet*) Slg. 1976, 2043 Rn. 12. Besonders deutlich auch z.B. EuGH 22.1.2015 – Rs. C-463/13 (*Stanley*) ECLI:EU:C:2015:25 Rn. 37.

574 Vgl. EuGH 5.12.2023 – Rs. C-807/21 (*Deutsche Wohnen SE/Staatsanwaltschaft Berlin*) ECLI:EU:C:2023:950 Rn. 51 ff.; EuGH 14.12.2023 – Rs. C-340/21 (*Natsionalna agentsia za prihodite*) ECLI:EU:C:2023:986 Rn. 22 ff.

Konkret auf die hier interessierende Versicherbarkeit von Geldbußen bezogen, ist demnach zu untersuchen, ob der Deckungsschutz für unionsrechtlich geforderte Geldbußen das unionale Sanktionsziel in einer Weise beeinträchtigt, die mit dem Effektivitätsgrundsatz unvereinbar erscheint. Während ein jüngeres EuGH-Vorabentscheidungsersuchen zum Verbandsgeldbußenregress bei Kartellbußen künftig Aufschluss geben mag, ist beim gegenwärtigen Stand die unionale Rechtslage und Rechtsprechungsentwicklung keineswegs eindeutig (**dazu unter 1**).

1. Ausgangslage: EU-Effektivitätsgrundsatz und Geldbußen

Auf einer der Versicherbarkeit noch vorgelagerten Ebene hat nun auch der BGH diese Frage zum Gegenstand seines Vorabentscheidungsverfahrens zum EuGH gemacht: Beeinträchtigt der Verbandsgeldbußeninnenregress nach § 43 Abs. 2 GmbHG bzw. § 93 Abs. 2 AktG die Effektivität der gegen den Verband durch das deutsche BKartA verhängten Kartellbußen?[575] Obschon der BGH – anders als die Vorinstanz –[576] das Bestehen von D&O-Deckung für den Innenregressanspruch mit überzeugenden Argumenten für wenig relevant hält, so berührt das Vorabentscheidungsverfahren doch das ganz grundsätzliche Problem, inwieweit der sanktionenrechtliche EU-Effektivitätsgrundsatz eine privatrechtliche Verteilung von unionsrechtlich gebotenen Geldbußen gestattet.[577]

Mit Blick auf die Frage der (Binnen)Regressfähigkeit und Versicherbarkeit von Kartellgeldbußen wird zuweilen vorgebracht, dass hier die abschreckende Wirkung, die öffentlich-rechtliche Kartellverfolgung durch die EU-Kommission und damit die Effektivität der

[575] BGH 11.2.2025 – KZR 74/23, Vorabentscheidungsersuchen Rs. C-347/25 (*Zapp*).
[576] OLG Düsseldorf r+s 2023, 827 Rn. 165 ff. und andererseits LG Dortmund VersR 2023, 1313 f.; LG Dortmund VersR 2023, 1314 ff.; LG Frankfurt 20.1.2023 – 2-08 O 313/20 (juris) Rn. 30 ff. (obiter).
[577] Vgl. BGH 11.2.2025 – KZR 74/23, Vorabentscheidungsersuchen Rs. C-347/25 (*Zapp*).

Art. 101, 105 AEUV beeinträchtigt würden.[578] In der Tat hat die EU-Kommission – und *obiter* auch der EuGH –[579] im Fall kartellrechtlicher Geldbußen bereits den Effektivitätsgrundsatz ins Feld geführt: Dabei ging es jedoch jeweils um die steuerliche Abzugsfähigkeit von Geldbußen nach nationalem Steuerrecht, die sowohl der Effektivität der unionsrechtlich vorgesehenen Sanktionen als auch dem EU-Wettbewerbsrecht insgesamt zuwider läuft.[580] Denn wenn ein EU-Mitgliedstaat den in ihrem Hoheitsgebiet steueransässigen Unternehmen die von der EU-Kommission oder einer nationalen Behörde auf unionsrechtlicher Grundlage verhängten Kartellgeldbußen über den Umweg der steuerlichen Abzugsfähigkeit „erstattet", so führt dies im Ergebnis zu einer von der EU-Wettbewerbsordnung missbilligten „*staatlichen de facto-Subventionierung*" solcher Unternehmen.[581] Damit ist allerdings noch nichts darüber ausgesagt, ob das Unionsrecht in gleicher Weise einer privatrechtlichen (Innen) Haftung, z.B. nach § 43 Abs. 2 GmbHG oder § 93 Abs. 2 AktG, und/oder Deckungsbausteinen für Verbandsgeldbußen, z.B. i.R.d. D&O- oder Cyber-Versicherung, entgegensteht. Denn zumindest soweit der unionsrechtliche Sanktionsanspruch bereits durch die Zahlung der Geldbuße erfüllt worden ist, lässt das Unionsrecht in seiner Auslegung durch den EuGH sehr wohl eine anschließende privatrechtliche Weiterverteilung und Übernahme von Geldbußen nach den jeweiligen nationalen Vorschriften des mitgliedstaatlichen Privatrechts zu.[582] Hierin mag man durchaus eine grundsätzlich andere Wertung und Tendenz erkennen: Anders als bei der steuerlichen Abzugsfähigkeit von Geldbußen privilegiert hier kein EU-Mitgliedstaat ein bei ihm steueransässiges Unternehmen, sondern die privatrechtliche Verteilung der Geldbuße erfolgt nach deren vollständiger Bezahlung allein unter privaten Akteuren.

---

578 So meint etwa das LG Saarbrücken NZKart 2021, 64 Rn. 122 f, es läge schon bei Zulassung eines Innenregresses bei kartellrechtlichen Bußen ein Verstoß gegen das Gebot des „effet utile" vor. Vgl. auch *Dreher*, FS Konzen, 2006, 88 f.; *Strasser*, VersR 2017, 65 ff.

579 Vgl. – nur *obiter* – EuGH 11.6.2009 – Rs. C-429/07 (*Inspecteur van de Belastingdienst*) ECLI:EU:C:2009:359 Rn. 39.

580 Vgl. die *amicus curiae* Eingaben der EU-Kommission v. 8.3.2012 *Tessenderlo Chemie v Belgische Staat*, sj.e(2012)227414 Rn. 25 und 29.

581 Eingehend dazu *Lüttringhaus*, VersR 2025, 843, 848 ff.

582 Siehe zum Innenregress unter Mitkartellanten nur EuGH 10.4.2014 – Rs. C-231/11 P u.a. (*Siemens Österreich*) ECLI:EU:C:2014:256 Rn. 60 ff.; EuGH 10.4.2014 – Rs. C-247/11 P u.a. (*Areva*), ECLI:EU:C:2014:257 Rn. 149 ff. Dazu ausführlich *Lüttringhaus*, VersR 2025, 843, 848 f.

2. Sanktionenrechtliche Effektivität und Versicherungsschutz für Geldbußen

In einer jüngeren Entscheidung zur D&O-Versicherung hat das LG Frankfurt zumindest die Versicherbarkeit des Innenregresses von Verbandsgeldbußen gegen den Geschäftsleiter ohne Weiteres bejaht.[583] Ob diese Erwägungen auch auf eine Cyber-Eigenschadendeckung des – im Regelfall als DSGVO-Geldbußenadressat auftretenden – Unternehmens zutreffen, bedarf näherer Betrachtungen. Dabei ist vorauszuschicken, dass weder für die vorsätzliche Herbeiführung des Versicherungsfalls noch im Regelfall für wissentliche Pflichtverletzungen Versicherungsschutz besteht.[584] Damit wird eine Eigenschadendeckung für Geldbußen ohnehin zuvörderst bei fahrlässigem Handeln relevant. Hier lautet die entscheidende Frage, ob ein solcher Deckungsbaustein dann den Versicherungsnehmer und die versicherten Personen zu einem nachlässigeren bzw. risikoreicheren Verhalten motiviert und auf diese Weise die mit der Geldbuße *unionsrechtlich* intendierte Prävention konterkariert.[585] Das wird teilweise mit dem Argument bejaht, dass der (EU-)Gesetzgeber gerade eine Geldbuße für erforderlich gehalten habe, um das Präventionsziel zu erreichen.[586] Allerdings ist damit noch nichts darüber ausgesagt, ob die Prävention im Fall einer Geldbußen-*Eigenschaden*deckung immer vollständig entfällt und solche Bausteine deshalb per se unionsrechtswidrig sind oder, ob – ganz im Gegenteil – womöglich erst hierdurch die Prävention gegenüber den tatsächlich verantwortlichen Personen sichergestellt werden kann.

Bei den nachfolgenden Erwägungen wird davon ausgegangen, dass ein als Verband organisiertes Unternehmen als Cyber-Versicherungsnehmer auftritt und eine Geldbußen-Eigenschadende-

---

583 LG Frankfurt 20.1.2023 – 2-08 O 313/20 (juris) Rn. 49 ff. wendet sich u.a. unter Verweis auf *Armbrüster/Schilbach*, r+s 2016, 109, 113 überzeugend gegen den Einwand des D&O-Versicherers, dass das Deckungsversprechen gegen § 138 Abs. 1 BGB verstoße und nichtig sei. Für OLG Frankfurt 21.11.2023 – 18 U 17/23 (unveröffentlicht) war diese Frage hingegen nicht entscheidungserheblich (dort unter II 4 g der Gründe).

584 Vgl. nur Ziff. A1-17.9 AVB-Cyber 2024 sowie § 81 Abs. 1, § 103 VVG.

585 *Armbrüster/Schilbach*, r+s 2016, 109, 111 ff.

586 Vgl. in diese Richtung *Armbrüster/Schilbach*, r+s 2016, 109, 111 f.; Dickmann/*Schilbach*, Cyberversicherung, Ziff. A1-17.11 AVB-Cyber Rn. 3.

ckung anstrebt. Solche Verbände können denknotwendig nur durch ihre Organe handeln und es obliegt ihren Geschäftsleitern, die Einhaltung von (Legalitäts)Pflichten – etwa im Bereich des Datenschutzes und der Cyber-Sicherheit – zu organisieren und zu überwachen. Besonders effektive Prävention ist deshalb dadurch zu erzielen, dass diese Geschäftsleiter – zumindest auch – selbst für Verstöße einstehen müssen. Dies stellt nach deutschem Gesellschaftsrecht der Binnenregress nach § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG sicher. Obschon dieser Regress gerade bei Verbandsgeldbußen hoch umstritten ist,[587] räumen selbst dessen Gegner ein, dass das ebenso scharfe wie ständig präsente Damoklesschwert des Regresses exakt bei dem Personenkreis ansetzt, der die Einhaltung der Legalitätspflichten im Verband sicherzustellen hat. Die Anreiz- und Präventionswirkung des Binnenregresses von (Verbands)Geldbußen ist damit besonders zielgenau und wirkmächtig: Denn durch die potentiell existenzgefährdende Haftung nach § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG werden Geschäftsleiter dazu angehalten, besonders genau auf die Einhaltung, Organisation und Überwachung der jeweiligen mit Geldbußen bewährten Legalitätspflichten zu achten. Gerade unter Anreizgesichtspunkten dürfte der Binnenregress also die sanktionenrechtlich – auch und gerade durch den Unionsgesetzgeber, z.B. mit Art. 83 DSGVO – intendierte Präventionswirkung stärken.[588] Folgt man dieser Überlegung, so wird aus unionsrechtlicher Perspektive also durch die Geldbußen-Eigenschadendeckung des Unternehmens noch nicht zwingend die Präventionswirkung vereitelt: Entscheidend ist vielmehr, ob die unionsrechtlich vorgegebene Abschreckungs- und Präventionsfunktion sich auf einer nachgelagerten Ebene dadurch entfalten kann, dass ein Regress gegen den handelnden Geschäftsleiter möglich und auch

---

587 Vgl. einerseits LArbG Düsseldorf NZKart 2015, 277, 278 f.; LG Saarbrücken NZKart 2021, 64 Rn. 122 f.; OLG Düsseldorf r+s 2023, 827 Rn. 152 ff. und andererseits LG Dortmund VersR 2023, 1313 f.; LG Dortmund VersR 2023, 1314 ff.; LG Frankfurt 20.1.2023 – 2-08 O 313/20 (juris) Rn. 30 ff. (obiter). Vgl. aus dem ausländischen Diskurs nur einerseits *Safeway Stores Ltd v Twigger* 21.12.2010 [2010] EWCA Civ 1472 Rn. 16 (Longmore LJ) und andererseits Rechtbank Noord-Nederland 23.9.2020, ECLI:NL:RBNNE:2020:329. Vgl. ferner nur *Jetivia SA & Anor v Bilta (UK) Ltd & Ors* [2015] UKSC 23 (Lord Toulson/Lord Hodge).

588 Das gilt umso mehr, als der *ex post*-Regress aus gesellschaftsrechtlicher Sicht – in Ermangelung von *ex ante*-wirkenden Instrumenten – zugleich die einzig praktikable Sanktionsmaßnahme ist, *Fleischer* DB 2014, 345, 347. Das LG Dortmund VersR 2023, 1313 hält die Anerkennung des Binnenregress deshalb für „zwingend".

praktisch wahrscheinlich ist. Hier setzt nun ein zentrales Argument für die Versicherbarkeit an: Denn während Unternehmen bei der Durchsetzung von Binnenregressansprüchen wegen Verbandsgeldbußen – z.B. aus Rücksichtnahme auf die Geschäftsleiter – auch ungeachtet der *ARAG/Garmenbeck*-Rechtsprechungslinie[589] des BGH Zurückhaltung üben mögen, wird dies ein Cyber-Versicherer kaum tun, wenn dieser das Geldbußendeckungsversprechen gegenüber dem Unternehmen erfüllt und sodann im Wege der Legalzession den Regressanspruch des Unternehmens gegen den Geschäftsleiter nach § 86 VVG i.V.m. § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG erwirbt. Von dieser Warte aus besehen, verleiht also der Regress durch den Versicherer der Prävention erst richtige Durchschlagskraft. Just diesen Ansatz hat auch der Unionsgesetzgeber gewählt: Art. 20 Abs. 1 NIS-2-RL gebietet eine Binnenhaftung des Geschäftsleitungsorgans bei Verletzung ihrer Pflichten zur Organisation („Billigung") und Überwachung von Cyber-Risikomanagementmaßnahmen.[590] Damit fordert das – in Deutschland künftig in § 38 Abs. 1 und Abs. 2 i.V.m. § 30 BSIG-E umgesetzte – NIS-2-Regime gerade explizit eine Inregressnahme der Geschäftsleiter zur Verwirklichung der Präventionsziele. Richtigerweise fallen dabei auch Geldbußen unter den mithilfe der Differenzhypothese auszufüllenden Schadensbegriff nach § 249 Abs. 1 BGB. Dies hat die Begründung des Referentenentwurfs des BMI zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz v. 3.7.2023 wie folgt explizit hervorgehoben:

> *„Vom Schadensbegriff sind … auch Bußgeldforderungen umfasst."*[591]

Für diese Lesart spricht, dass auf diese Weise die Präventionswirkung gerade bei den handelnden Akteuren eintritt und nicht nur die

---

589 BGH NJW 1997, 1926, 1927 f.

590 Siehe zur Umsetzung in § 38 Abs. 1, Abs. 2 i.V.m. § 30 BSIG-E i.d.F. des Entwurfs eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) BR-Drucks 380/24 v. 16.8.2024, S. 163 f.

591 Vgl. die Vorläuferfassung in Gestalt des Referentenentwurfs des Bundesministeriums des Innern und für Heimat v. 3.7.2023, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG), S. 118.

– im Regelfall an dem jeweiligen Verstoß nicht in vorwerfbarer Weise beteiligten – Aktionäre oder sonstigen Anteilseigner des Unternehmens finanziell trifft. Nach der hier vertretenen Auffassung lässt sich den speziellen unionsrechtlichen Regelungen der NIS-2-RL im Bereich der Cybersicherheit durchaus ein allgemeines Leitbild für effektive und zielgenaue Sanktion und Prävention entnehmen. Denn hier gibt der Unionsgesetzgeber bei Verstößen gegen an Verbände adressierte Verhaltensregeln wie den NIS-2-Cybersicherheitsvorgaben gerade ohne jede Einschränkung – und damit potentiell auch mit Blick auf Geldbußen –[592] die Inregressnahme von Geschäftsleitern vor.[593] Vor diesem Hintergrund erscheint es begründungsbedürftig, weshalb ausgerechnet ein solcher Regress nun in anderen unionsrechtlich normierten Materien – wie dem Datenschutzrecht – dann vermeintlich der Präventionswirkung abträglich sein sollte.[594] Dies gilt umso mehr, als der Unionsgesetzgeber die Sanktionsregimes der NIS-2-RL einerseits und der DSGVO andererseits gerade eng aufeinander abstimmt.[595] Es erscheint vielmehr so, dass beim Ausschluss des Binnenregresses nicht nur im unionalen Kartell-

592 Vgl. wiederum auch die Vorläuferfassung in Gestalt des Referentenentwurfs des Bundesministeriums des Innern und für Heimat v. 3.7.2023, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG), S. 118.

593 Art. 20 Abs. 1 UAbs. 1 NIS-2-RL lautet: „Die Mitgliedstaaten stellen sicher, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können". Aus Art. 20 Abs. 1 UAbs. 2 und aus Erwägungsgrund Nr. 128 NIS-2-RL folgt sodann, dass es um die zivilrechtliche Binnenhaftung geht, die – anders als bei Amtsträgern – durch nationales Recht grundsätzlich nicht weiter begrenzt werden kann. Ein ähnliches Bild ergibt sich auch für wesentliche (und besonders wichtige) Einrichtungen, vgl. Art. 32 Abs. 6 (i.V.m. Art. 33 Abs. 5) NIS-2-RL: „Die Mitgliedstaaten stellen sicher, dass jede natürliche Person, die für eine wesentliche Einrichtung verantwortlich ist oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreterin der wesentlichen Einrichtung handelt, befugt ist zu gewährleisten, dass die Einrichtung diese Richtlinie erfüllt. Die Mitgliedstaaten stellen sicher, dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung dieser Richtlinie haftbar gemacht werden können."

594 So aber zum EU-Kartellrecht LG Saarbrücken NZKart 2021, 64 Rn. 122 f.

595 Vgl. insbesondere Art. 35 Abs. 2 NIS-2-RL, wonach die für die Aufsicht über die NIS-2-Cybersicherheit zuständigen Behörden dann keine Geldbuße verhängen dürfen, wenn schon die Datenschutzbehörden einen DSGVO-Verstoß mit einer Geldbuße sanktioniert haben und sich dieser „Verstoß … aus demselben Verhalten ergibt wie" der Verstoß gegen die NIS-2-Vorgaben.

recht,[596] sondern z.B. auch bei der Sanktion von DSGVO-Verstößen unweigerlich ein erhebliches Präventionsdefizit („*prevention gap*“) entstehen dürfte, weil die Geschäftsleiter als die einzig handelnden und letztverantwortlichen Akteure kaum jemals individuelle Sanktionen zu fürchten hätten.[597]

Akzeptiert man diese Prämisse, so hängt dann die sanktionenrechtliche Effektivität der – unionsrechtlich vorgegebenen – Prävention weitaus weniger von der Frage ab, ob z.B. eine Cyber-Eigenschadendeckung des Verbandes für Geldbußen besteht, sondern vielmehr davon, ob ein effektiver (Binnen)Regress gegen die tatsächlich handelnden Akteure möglich bleibt. Nach dem Vorabentscheidungsersuchen des BGH hält nun der EuGH das Heft des Handelns in den Händen: Lässt der EuGH den Regress gegen verantwortliche Leitungspersonen zu, dann kann allein durch das Bestehen dieser empfindlichen Haftungsdrohung schon eine überaus effektive Prä-

596 Im unionalen Kartellrecht ist der EU-Kommission die Inanspruchnahme von natürlichen Personen und damit selbst von solchen Geschäftsleitern verwehrt, die ganz gezielt Kartellabsprachen treffen, vgl. nur Art. 101, 102 AEUV sowie statt aller *Biermann* in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Aufl. 2019, Vor Art. 23 VO 1/2003 Rn. 74.

597 So für das Kartellrecht schon überzeugend *J-U Franck/Seyer,* Management Liability for Companies' Antitrust Fines, Discussion Paper Series - CRC TR 224 (Discussion Paper No. 429 Project B 05), November 2023, 20 ff. Weitergehend zu DSGVO und NIS-2-Regime *Lüttringhaus*, FS Juristische Fakultät Hannover, 2025, 207, 221 ff.: Nach der Konzeption von Art. 83 und Art. 58 Abs. 2 DSGVO sind nur das Daten verarbeitende Unternehmen als „Verantwortlicher“ sowie ggf. dessen „Auftragsverarbeiter“ Adressaten von Geldbußen. Aus dem Geldbußenrahmen des Art. 83 Abs. 5 DSGVO für natürliche Personen und für Unternehmen lässt sich schon deshalb kein Argument gegen die privatrechtliche Regressfähigkeit einer Verbandsgeldbuße herleiten, weil unter der DSGVO gerade keine doppelte Inanspruchnahme droht: Die individuelle Bebußung von Geschäftsleitern ist keineswegs unionsrechtlich vorgezeichnet. Ob und inwieweit mitgliedstaatliche (Datenschutz)Behörden auf Grundlage (weitergehender) Regelungen des nationalen Rechts i.S.d. Art. 84 DSGVO auch handelnde Leitungspersonen mit Geldbußen belegen (können), wäre im Wege einer rechtsvergleichenden und rechtstatsächlichen Untersuchung zu klären, die den Rahmen dieses Beitrags sprengt. Ein kurzer Seitenblick auf die jüngere mitgliedstaatliche Geldbußenpraxis in besonders prominenten Fällen spricht indes dafür, dass Adressaten dieser Bußgelder prima facie allein die Unternehmen als „Verantwortliche“ i.S.d. DSGVO waren: Soweit ersichtlich, ist z.B. bei den zur Sanktion von DSGVO-Verstößen verhängten Geldbußen gegen Meta, Google, TikTok, Amazon, Vonovia, Facebook und H&M jeweils keine Rede von weiteren individuellen Geldbußen gegen Geschäftsleiter, vgl. nur die Übersicht der jeweiligen Sanktionsadressaten bei *CMS.Law*, GDPR Enforcement Tracker (2024), abrufbar unter: https://www.enforcementtracker.com/?insights (zuletzt abgerufen am 1.5.2025).

vention erzielt werden – wenn auch vermittelt über die privatrechtliche Regressierbarkeit der sanktionenrechtlichen Geldbuße.[598]

Auf der nächsten Ebene wäre freilich zu untersuchen, ob der D&O-Versicherer des handelnden Geschäftsleiters sodann Deckung für die Ansprüche aus § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG bieten kann.[599] Nach der hier vertretenen und auch durch das LG Frankfurt[600] gestützten Auffassung ist dies grundsätzlich zu bejahen, weil schon durch die Ausschlüsse vorsätzlicher und wissentlicher Pflichtverletzungen ebenso wie durch den Selbstbehalt sowie durch die begrenzte Deckungssumme und vergleichsweise niedrige Sublimitierungen ein jeder handelnder Geschäftsleiter immer in erheblichem Maße seine persönliche Haftung fürchten muss und schon durch dieses „*skin in the game*“ eine ausreichende Verhaltenssteuerung gewährleistet werden dürfte.[601]

Festzuhalten bleibt zunächst, dass eine Eigenschadendeckung für Geldbußen i.R.d. Cyber-Versicherungsvertrags angesichts des Ausschlusses der vorsätzlichen Herbeiführung des Versicherungsfalls und des Ausschlusses von wissentlichen Pflichtverletzungen nur in Szenarien relevant wird, in denen fahrlässige Verstöße – z.B. gegen die DSGVO – im Raum stehen. Es spricht sodann aus der Perspektive des EU-Rechts viel dafür, dass eine Eigenschadendeckung auch für unionsrechtlich vorgezeichnete Geldbußen keineswegs *per se* dem sanktionenrechtlichen Effektivitätsgrundsatzes zuwiderläuft und unwirksam ist. Jüngere Regelungsansätze in der NIS-2-RL legen vielmehr nahe, dass Prävention gegenüber Verbänden gerade auch zielgerichtet gegenüber den Geschäftsleitern wirken soll. Diese in Art. 20 Abs. 1 NIS-2-RL anklingende Präventionswirkung ließe sich womöglich auch dann noch zur Geltung bringen, wenn ein Cyber-Versicherer die gegen einen Verband verhängte Geldbuße zu-

---

598 Vgl. zum Vorlagefrage betreffend die Vereinbarkeit des Verbandsgeldbußenregresses nach § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG mit dem sanktionenrechtlichen EU-Effektivitätsgrundsatz BGH 11.2.2025 – KZR 74/23, Vorabentscheidungsersuchen Rs. C-347/25 (*Zapp*).

599 Dagegen OLG Düsseldorf r+s 2023, 827 Rn. 167.

600 LG Frankfurt 20.1.2023 – 2-08 O 313/20 (juris) Rn. 49 ff. Das OLG Frankfurt 21.11.2023 — 18 U 17/23 (unveröffentlicht) konnte die Frage der Versicherbarkeit offenlassen (dort unter II 4 g der Gründe).

601 Eingehend *Lüttringhaus*, FS Juristische Fakultät Hannover, 2025, 207, 224 ff.; *Lüttringhaus*, VersR 2025, 843, 852 ff.

nächst i.R.d. Eigenschadenbausteins deckt und anschließend den Geschäftsleiter, der für den jeweiligen Rechtsverstoß verantwortlich ist, nach § 86 VVG i.V.m. § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG in Regress nimmt. In der Cyber-Versicherung dürfte schon Ziff. A3-7.2 AVB Cyber 2024 der (Mit)Versicherung des Haftpflichtinteresses der Organperson entgegenstehen[602] und ohne weitere Anhaltspunkte lässt sich kaum ein pauschaler stillschweigender Regressverzicht zu Gunsten des Geschäftsleiters begründen.[603] Dies gilt umso mehr, als sich die im deutschen Markt verwendeten Cyber-Bedingungswerke zuweilen explizit die Möglichkeit der Inregressnahme von versicherten Personen – einschließlich der Geschäftsleiter – offen halten.[604]

Abgesehen davon bleibt nach der hier vertretenen Ansicht ohnehin Raum für Deckungsbausteine, welche die Erstattung von Geldbußen vorsehen, die zur Sanktion von fahrlässigen Verstößen insbesondere in noch unzureichend geklärten „Graubereichen" z.B. des unionalen Datenschutz- und Cyber-Sicherheitsrechts verhängt werden. Soweit beispielsweise im Kontext der NIS-2-RL die (Verhaltens)Pflichten der Normadressaten noch nicht hinreichend klar – sei es durch Durchführungsrechtsakte, sei es durch die Judikatur des EuGH – definiert worden sind, kann eine Geldbußendeckung für die betroffenen Unternehmen einerseits praktisch Sinn ergeben, ohne dass andererseits die mit solchen Geldbußen intendierten Ziele kompromittiert werden. Sofern nämlich schon der einzuhaltende (Sorgfalts)Maßstab noch nicht konkretisiert ist, kann auch diesbe-

602 Treffend *Schilbach/Becker*, r+s 2023, 289, 290. Vgl. aus der Marktpraxis z.B. auch Ziff. 9.3 HDI Versicherungsbedingungen zur Cyberversicherung für Firmen und Freie Berufe (Juni 2022).

603 Vgl. zur Diskussion um den Regress von Cyber-Versicherern gegen Organmitglieder der Versicherungsnehmerin *Schilbach/Becker*, r+s 2023, 289 ff.; *Hoffmann/Schürger*, r+s 2024, 789 ff., die unter bestimmten Voraussetzungen einen stillschweigenden Regressverzicht befürworten.

604 Vgl. deutlich etwa Ziff. 3.5 („Regressansprüche gegen versicherte Personen werden nur in Abstimmung mit der Versicherungsnehmerin geltend gemacht.") einerseits sowie Ziff. 14.39 eines marktgängigen Bedingungswerks („Versicherte Personen sind …Mitglieder des Vorstands, Aufsichtsrats, Beirats, Board of Directors, Geschäftsführer und alle Mitglieder sonstiger vergleichbarer geschäftsführender, beratender und/oder beaufsichtigender satzungsgemäßer Organe nach dem für die Gesellschaft jeweils gültigen Recht") anderseits. Vgl. auch Ziff. IV.11 bis Ziff. IV.12 der AVB eines anderen Cyber-Versicherers, wonach ein Regressverzicht nur gegenüber mitversicherten natürlichen Personen vereinbart wird, wozu ausdrücklich u.a. nicht „Mitglieder des Vorstandes" und „Geschäftsführer" zählen.

züglich keine effektive Individual- oder Generalprävention stattfinden.

Allerdings sind die durch die jeweiligen EU-Rechtsakte vorgegebene Präventionswirkung ebenso wie die Reichweite und die Einhaltung des sanktionenrechtlichen Effektivitätsgrundsatzes genuin unionsrechtliche Fragen. Das letzte Wort hat hier der EuGH, der nun durch den BGH mit Blick auf die Binnenregressfähigkeit von Verbandsgeldbußen um Vorabentscheidung ersucht worden ist.[605]

IV. Versicherbarkeit von Geldbußen durch „fine-wraps" und „most favorable jurisdiction/venue"?

Im Kontext der Versicherbarkeit von Geldbußen wegen Verstößen gegen Datenschutz- und Cyber-Sicherheitsbestimmungen werden häufig Parallelen zur Deckung von „*punitive damages*" gezogen: Hier wie dort lasse sich nach dem Vorbild der US-Marktpraxis womöglich die Versicherbarkeit trotz (bundes)staatlicher Versicherungsverbote erreichen, indem gezielt ein anwendbares Recht und ein für etwaige Deckungsstreitigkeiten zuständiges (Schieds)Gericht bestimmt wird, das jeweils einer Geldbußendeckung zur Wirksamkeit verhilft. Als zentrales Instrument, das „Versicherbarkeit durch Vertragsgestaltung" zu gewährleisten sucht, dient hierbei eine Kombination aus Rechts- und (Schieds)Gerichtswahl: Dies trifft sowohl auf die „*Punitive Damages Wrap*"- bzw. „*Fine Wrap*"-Policy (**dazu unter 1**) als auch auf den „*most favorable jurisdiction/venue*"-Ansatz (**dazu unter 2**) zu.

1. Von der „Puni-" zur „Fine-Wrap-Policy"?

Bei einer „*Punitive Damages Wrap*"-Policy sollen *punitive damages awards* in solchen US-Bundesstaaten gedeckt werden, die eigentlich die Versicherung solcher Sanktionsinstrumente untersagen. Diese auch als sog. „Puni Wraps" bezeichneten „*offshore"*-Versiche-

[605] Vgl. erneut BGH 11.2.2025 – KZR 74/23, Vorabentscheidungsersuchen Rs. C-347/25 (*Zapp*).

rungsverträge werden zusätzlich zu einer durch einen im jeweiligen US-Bundesstaat zur Erbringung von Versicherungsdienstleistungen zugelassenen „*onshore“*-Versicherer ausgestellten (Haftpflichtversicherungs-)Police abgeschlossenen. Dabei setzt die „*Puni Wrap“*-Policy grundsätzlich auf den Bedingungen des „*onshore“*-Hauptversicherungsvertrags auf und ergänzt diese nur bezüglich der Deckung von in dem fraglichen US-Bundesstaat nicht versicherbaren *punitive damages*. Die „*Puni Wrap“*-Policies werden deshalb als „*offshore“* charakterisiert, weil sie mit einem in Bermuda niedergelassenen Versicherer geschlossen werden. Die „*Puni Wrap“*-Policy wird kraft Rechtswahl dem Recht von Bermuda unterstellt, und durch eine Schiedsvereinbarung – meist mit Schiedsort Bermuda oder London – wird zusätzlich sichergestellt, dass die *punitive damages*-Deckung im Fall eines Deckungsstreits ungeachtet etwaiger „*onshore“*-Versicherungsverbote durchgesetzt werden kann. Dieser Ansatz ließe sich nun grundsätzlich auch auf die Deckung von Geldbußen wegen Verstößen gegen die DSGVO oder das NIS-2-Regime übertragen: Im Zentrum dieses „*Fine Wrap*“-Konzepts steht wiederum die Kombination aus einer Rechtswahl zugunsten eines insoweit permissiven Rechts (z.B. Bermuda) einerseits und einer Schiedsklausel andererseits.[606]

Doch in der Praxis dürften sich mit dieser Gestaltung längst nicht alle Schwierigkeiten umschiffen lassen: Zunächst haben (Versicherungsaufsichts)Behörden bereits auf „*Punitive Damages Wrap*“-Policies reagiert und untersagen – beispielsweise im US-Bundesstaat New York – dortigen Brokern ausdrücklich

[606] Vgl. schon frühzeitg *Kerr*, Do You Even Know What a Puni-Wrap Is? Hint — It Could Protect You From GDPR Fines, Risk & Insurance v. 22.4.2019, abrufbar unter: https://riskandinsurance.com/gdpr-fines-are-knocking-will-your-insurance-respond/ (zuletzt abgerufen am 1.5.2025): „One existing option is a twist on a punitive damages wrap (puni-wrap). A carrier will write a domestic cyber policy, and an offshore affiliate will pair it with a punitive wraparound policy. Such wraparounds have been in use for at least two decades for other liability risks including EPL, D&O and E&O. Puni-wraps are typically used to insure against punitive damages awards in states where such awards are not payable with insurance. Some of these are now in play to cover GDPR fines.“

> *„(to) place insurance coverage … (or to) hire a third party to place insurance coverage in the excess line market on risks located in New York State that would cover punitive damages.“*[607]

Durch sec. 27.11 Regulation 41[608] wird den Brokern allgemein untersagt, Deckung von nicht zugelassenen (ausländischen) *Excess-Line*-Versicherern für Risiken zu organisieren, deren Versicherbarkeit entweder gesetzlich verboten ist oder

> *„determined by any Appellate Division of the New York State Supreme Court or the New York State Court of Appeals to be against public policy in this State“.*[609]

Deshalb dürften auch und gerade die hier diskutierten „*fine-wraps*“ im Cyber-Versicherungsbereich aller Voraussicht nach unter dieses Verbot fallen, zumal zur Deckung von *fines* und *civil penalties* bereits eine gefestigte Rechtsprechungslinie der nach sec. 27.11 Regulation 41 relevanten Obergerichte im Bundesstaat New York existiert:

> *„There is no basis for a finding that a fidelity insurer must indemnify an insured which has incurred criminal fines and civil penalties. … The sting of criminal penalties is not to be soothed by permitting its payment out of an insurance pool rather than directly by the wrongdoer.“*[610]

Darüber hinaus birgt die Kombination aus Rechtswahlklauseln zugunsten einer liberalen Rechtsordnung (wie etwa Bermuda) einerseits und einer Schiedsklausel (i.d.R. einer *Bermuda arbitration provision*) andererseits ebenfalls Risiken. Denn ein nicht eintrittswilliger Cyber-Versicherer mag durchaus vor staatliche Gerichte ziehen, um

---

607 *Office of General Counsel*, Opinion No. 08-08-09 v. 27.8.2008: Placement of Punitive Damages Insurance Coverage in the Excess Line Market, abrufbar unter: https://www.dfs.ny.gov/insurance/ogco2008/rg080809.htm (zuletzt abgerufen am 1..2025).

608 11 CRR-NY 27.11.

609 Vgl. zu sec. 27.11 Regulation 41 (11 CRR-NY 27.11) wiederum *Office of General Counsel*, Opinion No. 08-08-09 of 27 August 2008: Placement of Punitive Damages Insurance Coverage in the Excess Line Market, abrufbar unter: https://www.dfs.ny.gov/insurance/ogco2008/rg080809.htm (zuletzt abgerufen am 1.5.2025).

610 *Drexel Burnham Lambert Group, Inc. v. Vigilant Insurance Company*, 157 Misc. 2d 198, 213 (N.Y. Sup. Ct. 1993). Vgl. auch *Hartford Acc. Indem. Co. v Village of Hempstead*, 48 N.Y.2d 218, 226 f.; *Silverman Neu, LLP v. Admiral Insurance Company*, 933 F. Supp. 2d 463 (E.D.N.Y. 2013).

die Unversicherbarkeit von Geldbußen feststellen zu lassen, in den US-Bundesstaaten etwa durch eine *declaratory relief action*.[611] In diesem Fall muss der Versicherungsnehmer den Schiedseinwand erheben, wobei in die Beurteilung der Wirksamkeit der Schiedsklausel sodann einfließen mag, ob diese Klausel ausschließlich dazu dient, zum *ordre public* bzw. zur *public policy* oder zu den Eingriffsnormen zählende Versicherungsverbote zu umgehen. Spätestens im Aufhebungs- oder Vollstreckbarerklärungsverfahren kommen derartige auf den *ordre public* gestützte Angriffe in Betracht: Jedenfalls soweit ein Staat – wie z.B.: Italien in Art. 12(1) *Codice delle Assicurazione Private* –[612] explizit die Versicherbarkeit von Geldbußen untersagt, dürfte in einer Geldbußendeckung dann eine verbotsgesetzwidrige Verpflichtung liegen, zu der sich der Versicherer nicht wirksam verpflichten kann und die entsprechend am jeweiligen Pendant zu Art. V(2) New Yorker Übereinkommen[613] bzw. § 1059 ZPO zu messen wäre.[614] Obschon zu Verbandsgeldbußen bereits dargetan worden ist, dass eine Geldbußendeckung hier keineswegs automatisch mit dem sanktionenrechtlichen Effektivitätsgrundsatz kollidiert,[615] so mag im Einzelfall zumindest bei unionsrechtlich vorgezeichneten (individuellen) Geldbußen die Effektivität durch Versicherungslösungen bedroht sein. Diese unionsrechtliche Dimension wäre sodann durch deutsche Gerichte ebenso wie durch die Gerichte anderer EU-Mitgliedstaaten zu berücksichtigen, da nach ständiger Rechtsprechung des EuGH jedenfalls „die grundlegenden Bestimmungen des Unionsrechts im Rahmen dieser Kontrolle geprüft werden … und gegebenenfalls Gegenstand einer Vorlage zur Vor-

611 Vgl. in anderem Kontext zu einer solchen prozesstaktischen Vorgehensweise *Chubb Custom Insurance Company v. The Prudential Insurance Company of America*, 195 N.J. 231, 245 (N.J. 2008): „(I)f an insurer is permitted to file first it will choose a forum that is hostile to the insurance of punitive damages".

612 Siehe dazu erneut oben I 2.

613 New Yorker Übereinkommen vom 10. Juni 1958 über die Anerkennung und Vollstreckung ausländischer Schiedssprüche.

614 Vgl. zu § 1059 ZPO nur Musielak/Voit/*Voit*, ZPO, 22. Aufl. 2025, § 1059 ZPO Rn. 31 m.w.N.: „Aufzuheben ist ein Schiedsspruch, der zu einer Leistung verpflichtet, deren Erbringung gegen ein Verbotsgesetz verstößt".

615 Vgl. zum sanktionenrechtlichen Effektivitätsgrundsatz bei Verbandsgeldbußen erneut oben III.

abentscheidung an den Gerichtshof sein“ sollen.[616] Gelangt das jeweils angerufene staatliche Gericht – etwa im i.R.d. *declaratory relief action* – direkt zur Unwirksamkeit der Schiedsklausel oder versagt es nachträglich im Vollstreckbarerklärungs- bzw. Aufhebungsverfahren dem Schiedsspruch die Wirksamkeit, so fällt damit das gesamte „*Fine-Wrap*“-Konzept in sich zusammen.

Ganz ähnliche Bedenken wird man gegenüber vergleichbaren Gestaltungen äußern müssen, z.B. wenn in einem Exzedenten-Turm in einem höheren Layer gezielt eine vom Primary- bzw. Grundversicherungsvertrag abweichende Rechtswahl (etwa zugunsten des Rechts von Bermuda) und eine abweichende Schiedsklausel (z.B. wiederum *Bermuda arbitration provision*) vorgesehen wird, wobei sodann eine DIC- (*difference in conditions*) mit einer „Drop Down“-Klausel dergestalt kombiniert wird, dass dieser höhere xs-Layer ungeachtet der Erschöpfung der unteren Layer für den Fall leistungspflichtig sein soll, dass die unteren Layer aufgrund eines Versicherungsverbots (hier: hinsichtlich Geldbußendeckungen) aus rechtlichen Gründen nicht eintrittspflichtig sind.[617]

2. Keine „most favorable jurisdiction/venue“ bei Geldbußendeckungen

Ein ähnliches Bild zeigt sich auch bei den – in Anlehnung an die aus den US für die Deckung von „*punitive damages*“ bekannten – „*most favorable venue*“- bzw. „*most favorable jurisdiction*“-Klauseln: Solche Klauseln versprechen die Versicherbarkeit von

---

[616] Vgl. zur unionsrechtlichen Einwirkung auf das Aufhebungsverfahren EuGH 1.6.1999 – Rs. C-126/97 (*Eco Swiss*) ECLI:EU:C:1999:269 Rn. 35 ff.; EuGH 26.10.2006 – Rs. C-168/05 (*Mostaza Claro*) ECLI:EU:C:2006:675 Rn. 34 ff.; EuGH 6.3.2018 – Rs. C-284/16 (*Achmea*) ECLI:EU:C:2018:158 Rn. 54. Siehe ferner nur *Schütze/Thümmel*, Schiedsgericht und Schiedsverfahren, 7. Aufl. 2021, S. 144 und 204 f.; Musielak/Voit/*Voit*, ZPO, 22. Aufl. 2025, § 1059 ZPO Rn. 31 jeweils m.w.N.

[617] Vgl. *Kerr*, Do You Even Know What a Puni-Wrap Is? Hint — It Could Protect You From GDPR Fines, Risk & Insurance v. 22.4.2019, abrufbar unter: https://riskandinsurance.com/gdpr-fines-are-knocking-will-your-insurance-respond/ (zuletzt abgerufen am 1.5.2025): „They have … to sit on the tower as a regular excess player and they will issue a DIC endorsement that will drop down [and provide affirmative coverage] in the event that the primary is unable to pay it due to insurability reasons.“

„reimbursement of fines and penalties where insurable under the laws of an applicable jurisdiction most favourable to the insured".[618]

Anders ausgedrückt, verfolgen die „*most favorable venue*"- bzw. „*most favorable jurisdiction*"-Klauseln also einen „Meistbegünstigungs-Ansatz": Die Parteien des Versicherungsvertrags vereinbaren sowohl die Zuständigkeit desjenigen Gerichts als auch die Anwendbarkeit desjenigen Rechts, welches jeweils die Versicherbarkeit von Geldbußen anerkennen und den Deckungsanspruch durchsetzen wird.[619] Bei diesem aus der US-amerikanischen Vertragspraxis stammenden Ansatz bedarf es indes einer gewissen Verbindung der Parteien zur gewählten Jurisdiktion. In der Regel wird die alternative „*most favorable*"-Wahl für das Deckungsverhältnis deshalb auf den für das Haftpflichtverhältnis maßgeblichen Handlungs- bzw. Erfolgsort, den Sitz des Versicherten oder auf das für den Versicherungsvertrag maßgebliche Recht zielen:

„the law of the jurisdiction most favorable to the insurability of those damages shall control for the purpose of resolving any dispute between the Company and the Insured regarding whether the damages specified . . . above are insurable . . . provided that such jurisdiction: is where those damages were awarded or imposed; is where any Wrongful Act occurred for which such damages were awarded or imposed; is where any Insured Organization is incorporated or has its principal place of business; or is where the Company is incorporated or has its principal place of business."[620]

---

618 Vgl. zu diesem Klauselbeispiel nur *OECD*, Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation, 2020, S. 19. *Oehninger, S. and P. Moura* (2019), Equifax's Hefty $700M Bill is a Powerful Reminder to Close Cyber Coverage Gaps, Hunton Insurance Recovery Blog, abrufbar unter: https://www.huntonak.com/hunton-insurance-recovery-blog/equifaxs-hefty-700m-bill-is-a-powerful-reminder-to-close-cyber-do-coverage-gaps „Companies and organizations that hold personal data can strategically structure their cyber insurance coverages to avoid tricky sublimits and to employ a governing law that will maximize the insurability of regulatory fines" (zuletzt abgerufen am 1.5.2025).

619 Vgl. erneut nur *OECD*, Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation, 2020, S. 19.

620 Vgl. *Chubb Custom Insurance Company v. The Prudential Insurance Company of America*, 195 N.J. 231, 244 ff. (N.J. 2008), wo diese Klausel indes allein als eine Rechtswahlklausel und nicht – wie wohl intendiert – auch als eine Gerichtsstandsklausel ausgelegt worden ist.

Allerdings dürfte eine Übertragung dieser „Meistbegünstigungs-Klauseln“ zumindest im System des internationalen Zuständigkeits- und Privatrechts der EU kaum den gewünschten Erfolg erzielen: Zum einen stehen solche „asymmetrischen“ Gerichtsstandsklauseln potentiell quer zu den Anforderungen des Art. 25 Brüssel Ia-VO, der eine eindeutige – und grundsätzlich ausschließliche – Gerichtsstandswahl zugunsten der Gerichte *eines EU-Mitgliedstaates* fordert.[621] Nicht ohne Grund sind „asymmetrische“ Gerichtsstandsklauseln – wenn auch in etwas anderer Ausprägung – derzeit Gegenstand eines Vorabentscheidungsverfahrens zum EuGH.[622] Zum anderen ist eine Teilrechtswahl stets an den Schranken der Rom I-VO sowie – im Fall der Zuständigkeit deutscher Gerichte – des § 138 Abs. 1 BGB zu messen.[623] Schon Art. 3 Abs. 1 Rom I-VO fordert, dass sich die Rechtswahl „eindeutig aus den Bestimmungen des Vertrags“ ergibt. Diesem auf Rechtssicherheit und Vorhersehbarkeit zielenden Erfordernis ist bei einer alternativen Rechtswahl nicht genügt, wenn die Parteien mehrere Rechtsordnungen potentiell zur Anwendung berufen. Fehlt es – wie in den „*most favorable venue*“- bzw. „*most favorable jurisdiction*“-Klauseln – an der Konkretisierung des anwendbaren Rechts, so liegt keine wirksame Rechtswahl vor.[624] Versicherungsnehmer, die sich auf derartige vertragliche Konstruktionen verlassen, sehen sich damit erheblichen Unwägbarkeiten bei der Durchsetzung ihrer Geldbußendeckung gegenüber.

---

621 Vgl. Art. 25 Brüssel Ia-VO: „ein Gericht oder die Gerichte eines Mitgliedstaats“. Vgl. aber auch EuGH 9.11.1978 – Rs. 23/78 (*Meeth*) ECLI:EU:C:1978:198, wobei hier die Gerichtsstandswahl aus Sicht jeder Partei eindeutig zugunsten des jeweiligen Wohnsitz-Mitgliedstaates getroffen wurde. Vgl. noch weitergehend bei einem einseitigen Wahlrecht des Klägers OLG Hamm IPRax 2007, 125, 126. Zu solchen „unilateral optional“ und „non-uniquely exclusive agreements“ eingehend und kritisch dagegen *Keyes/Marshall*, 11 Journal of Private International Law (2015), 345 ff.; *Marshall*, Asymmetric Jurisdicion Clauses, 2023. Siehe ferner *Freitag*, FS Magnus, 2014, 419 ff. Vgl. schließlich auch die Entscheidung der französischen Cour de cassation 1ère civ., 26.9.2012 – 11-26.022, ECLI:FR:CCASS:2012:C100983.

622 Vgl. die Vorlagefragen der französischen Cour de cassation v. 22.8.2023 – Rs. C-537/23 (*Societa Italiana Lastre SpA (SIL)/Agora SARL*) ABl. EU C/2023/956.

623 Vgl. neben Art. 3 Abs. 1, Abs. 3 und Abs. 4 Rom I-VO auch zu Art. 9 Abs. 3 Rom I-VO sowie zu § 138 Abs. 1 BGB und der materiell-rechtlichen Berücksichtigung ausländischer Verbotsnormen erneut oben II 1 und 2.

624 Zutreffend statt vieler BeckOGK BGB/*Wendland*, 1.9.2022, Art. 3 Rom I-VO Rn. 123; Staudinger/*Magnus*, 2021, Art. 3 Rom I-VO Rn. 63; *Wilhelmi*, RIW 2016, 253, 254.

V. Ergebnis

Im internationalen Vergleich wird die Frage der Versicherbarkeit von Geldbußen durchaus unterschiedlich beantwortet. Die rechtsvergleichende Umschau offenbart, dass nur wenige Rechtsordnungen explizite Versicherungsverbote aufstellen – wie z.B. Italien in Form des Art. 12(1) *Codice delle Assicurazione Private* –, zahlreiche Jurisdiktionen aber allgemeine Grundsätze – wie die *illegality defence* (*ex turpi causa*) – oder auch *ordre-public*- bzw. *public-policy*-Erwägungen gegenüber Geldbußendeckungen in Stellung bringen. Das Bild ist hier gerade in den US-Bundesstaaten jedoch keineswegs einheitlich und auch der Blick auf einzelne EU-Mitgliedstaaten offenbart häufig erhebliche Rechtsunsicherheit. Dies führt zur Frage, wie in grenzüberschreitenden Konstellationen mit potentiellen Verboten von Geldbußendeckungen umzugehen ist.[625]

Anders als manche Geldbußen-Klauseln in Cyber-Versicherungsverträgen suggerieren, lässt sich die Frage der Durchsetzung solcher Deckungsversprechen keineswegs vertraglich auf bestimmte Rechtsordnungen beschränken: Im Deckungsstreit wird ein international zuständiges deutsches Gericht vielmehr alle kollisions- und sachrechtlich relevanten Versicherungsverbote berücksichtigen. Dazu zählen neben dem gemäß Art. 3 Rom I-VO als Vertragsstatut gewählten Recht stets die Eingriffsnormen des Gerichtsstaates (*lex fori*) nach Art. 9 Abs. 1, Abs. 2 Rom I-VO. Soll die Versicherungsleistung in einem anderen Staat – etwa am Sitz eines mitversicherten Tochterunternehmens – erbracht werden, kann das Gericht unter bestimmten Voraussetzungen auch die dort geltenden Versicherungsverbote als Eingriffsnorm i.S.d. Art. 9 Abs. 3 Rom I-VO berücksichtigen. Auf Ebene des materiellen deutschen Sachrechts – und namentlich insbesondere i.R.d. § 138 Abs. 1 BGB – können deutsche Gerichte schließlich etwaige Versicherungsverbote derjenigen Rechtsordnung berücksichtigen, deren Behörden die Geldbuße verhängt haben.

---

[625] Vgl. auch *RSUI Indemnity Company v. Murdock*, 2021 BL 76083 (Del. 3.3.2021), wo ein in Delaware inkorporiertes, aber in Kalifornien ansässiges Unternehmen Deckung begehrte, die nach kalifornischem Recht grundsätzlich ausgeschlossen erscheint.

Aus der Perspektive des EU-Rechts spricht viel dafür, dass eine Eigenschadendeckung auch für unionsrechtlich vorgezeichnete Geldbußen – etwa im Bereich der DSGVO – nicht automatisch dem sanktionenrechtlichen Effektivitätsgrundsatzes zuwiderläuft. Jüngere Regelungsansätze in der NIS-2-RL legen vielmehr nahe, dass Prävention gegenüber Verbänden gerade auch zielgerichtet gegenüber den Geschäftsleitern wirken soll. Diese – in Art. 20 Abs. 1 NIS-2-RL anklingende – Präventionswirkung könnte sich selbst dann noch entfalten, wenn ein Cyber-Versicherer die gegen einen Verband verhängte Geldbuße zunächst i.R.d. Eigenschadenbausteins deckt und sodann den Geschäftsleiter, der für den jeweiligen Rechtsverstoß verantwortlich ist, nach § 86 VVG i.V.m. § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG in Regress nimmt. Denn diese Vorgehensweise macht eine effektive Prävention gegenüber dem tatsächlich verantwortlichen Akteur – nämlich dem Geschäftsleiter – zum einen wahrscheinlicher und verhindert zugleich ein „underenforcement", das angesichts der fehlenden direkten Sanktionierung individueller Geschäftsleiter (z.B. nach der DSGVO) droht. Freilich sind die durch die jeweiligen EU-Rechtsakte, wie die DSGVO oder die NIS-2-RL, vorgegebene Präventionswirkung ebenso wie die Einhaltung des sanktionenrechtlichen Effektivitätsgrundsatzes unionsrechtliche Fragen, die letztverbindlich nur durch den EuGH im Wege eines Vorabentscheidungsverfahrens geklärt werden können.

In Anlehnung an die aus den USA als „*Punitive Damages Wrap*" bekannten Deckungskonzepte für Strafschadensersatz könnte auch eine Geldbußendeckung für Verstöße gegen die DSGVO oder das NIS-2-Regime gestaltet werden: Im Zentrum eines solchen „*Fine Wrap*"-Konzepts steht die Wahl eines liberalen Rechts (z.B. Bermuda), wobei diese Rechtswahl sodann durch eine Schiedsklausel zugunsten permissiver Schiedsorte und -ordnungen (z.B. *Bermuda arbitration provision*) abgesichert wird. Soweit hierdurch die Umgehung von Versicherungsverboten bezweckt wird, könnten jedoch spätestens im Vollstreckbarerklärungs- bzw. Aufhebungsverfahren *ordre public*-Einwände gegen die Wirksamkeit des Schiedsspruches erhoben werden. Ähnlichen Bedenken begegnen durch korrespondierende Schieds- und Rechtswahlvereinaberungen flankierte „*Drop-Down*"- und „*DIC*"-Klauseln in (höheren) Layern von Exzeden-

ten-Türmen. Auch die aus der anglo-amerikanischen Vertragspraxis bekannten sog. „*most favorable jurisdiction/venue*“-Klauseln dürften im System des europäischen internationalen Zuständigkeits- und Kollisionsrechts kaum Erfolg versprechen. Das birgt erhebliche Unwägbarkeiten für die Cyber-Versicherungsnehmer, die sich kaum auf die Durchsetzbarkeit des Leistungsversprechens unter dem Geldbußendeckungsbaustein verlassen können.

Allerdings erscheint selbst die gängige Formulierung in Geldbußenbausteinen, wonach Cyber-Versicherungsschutz nur „soweit rechtlich zulässig“ gewährt werden soll, keineswegs unangreifbar: Auch bei einem gewerblich tätigen Cyber-Versicherungsnehmer mag man nämlich hinterfragen, ob dieser in Sachverhalten mit Bezügen zu mehreren Rechtsordnungen womöglich

> *„(m)it der Einschränkung „soweit rechtlich zulässig“ … überfordert (ist), da ihm die für die anzustellenden rechtlichen Erwägungen notwendigen dezidierten Rechtskenntnisse, insbesondere dazu, welche gesetzlichen Vorschriften … abdingbar sind…, in der Regel schlicht fehlen werden.“*[626]

Festzuhalten bleibt, dass man auch und gerade bei der Versicherbarkeit von Geldbußen über Staatsgrenzen hinweg an vielen rechtlichen Klippen Schiffbruch erleiden kann.

[626] Vgl. – freilich im Kontext des Lauterkeits- und Verbrauchsgüterkaufsrechts – LG Berlin 28.11.2014 – 15 O 601/12, BeckRS 2015, 2687.

E. Versicherbarkeit und Erstattungsfähigkeit von „Lösegeldern“ bei Ransomware-Attacken

Wenige Rechtsfragen sind ebenso ausgiebig analysiert und diskutiert worden und doch zugleich ohne klare Antwort geblieben wie die rechtliche Zulässigkeit und Versicherbarkeit von Lösegeldzahlungen nach Cyber- und insbesondere Ransomware-Attacken.[627] Insbesondere die oftmals grenzüberschreitende Komponente von Cyber-Delikten und Cyber-Deckungskonzepten trägt zur Komplexität und Ungewissheit bei.[628]

Vor diesem Hintergrund machen manche Cyber-Versicherer die Erstattung von Lösegeldern, die zwecks Beendigung einer Ransomware-Attacke durch den Versicherungsnehmer, einen Versicherten oder durch einen hiermit beauftragten Dritten gezahlt werden, ausdrücklich davon abhängig, „dass die Zahlung gesetzlich zulässig und versicherbar ist“. Hierin liegt eine zweifache Einschränkung: Weder darf die vom Versicherten veranlasste Lösegeldzahlung als solche ungesetzlich sein, noch darf insoweit ein Versicherungsverbot bestehen. Bei den im Regelfall grenzüberschreitend ausgeführten Ransomware-Attacken und Lösegeldzahlungen kommen hier viele Rechtsordnungen in Betracht, was den Umfang des Deckungsversprechens nicht unerheblich schmälern, in jedem Fall

627 Verbote nehmen einerseits z.B. *Pache*, K ompass Cyberversicherungen, 2. Aufl. 2023, S. 205 (mit Blick auf Italien) sowie *Steimer*, Einführung in die Cyberversicherung, 2023, S. 105 (mit Blick auf Frankreich) an und andererseits findet sich bisweilen die apodiktische Aussage zugunsten einer generellen EU-weiten Zulässigkeit der Zahlung und Versicherung von Lösegeldern nach Ransomware-Attacken, so etwa bei *France Assureurs*, Livre blanc: Bâtir une économie de la donnée, 2022, S. 25: „Aucun texte national ou européen n’interdit le paiement d’une rançon par une entreprise ni le remboursement des rançons par un assureur, à l’exception des cas particuliers de financement du terrorisme et de blanchiment de capitaux.“ Aus der internationalen Debatte die Versicherbarkeit befürwortend statt vieler *Baker/Shortland*, Insurance and enterprise: cyber insurance for ransomware, The Geneva Papers on Risk and Insurance 48 (2023), 275 ff.; *Sieg/Schilbach*, VersR 2023, 745 ff. und ablehnend z.B. *Offener Brief*, Lösegeldzahlungen bei Ransomware-Angriffen: ein geostrategisches Risiko, 2022, abrufbar unter: https://ransomletter.github.io (zuletzt abgerufen am 1.5.2025); *Logue/Shniderman*, The Case for Banning (and Mandating) Ransomware Insurance, 28 Connecticut Insurance Law Journal (2021), 247 ff. Siehe zur Debatte in den USA z.B. *Abraham/Schwarcz*, The Limits of Regulation by Insurance, 98 Indiana Law Journal (2023), 215, 264; *Simpson*, P/C Insurers Defend Ransomware Reimbursements in New Cyber Principles, Insurance Journal v. 2.7. 2021, abrufbar unter: https://www.insurancejournal.com/news/national/2021/07/02/621178.htm (zuletzt abgerufen am 1.5.2025).

628 Vgl. etwa die durch das schweizerische Bundesgericht 17.8.2023 – 4A_206/2023, entschiedene Fallgestaltung.

aber aus Sicht des Versicherungsnehmers weniger vorhersehbar machen kann. Zwar wird für die deutsche (Master-)Police üblicherweise deutsches Recht gewählt und für den Deckungsstreit eine Gerichtsstandswahl zugunsten deutscher Gerichte getroffen.[629] Allerdings umfasst der Versicherungsschutz in räumlich-territorialer Hinsicht die ganze Welt, soweit dies „nach den Vorschriften und gesetzlichen Bestimmungen zulässig" ist. Damit mögen nicht nur Verbote der Lösegeldzahlung nach deutschem Recht (**dazu unter I**), sondern potentiell auch etwaige Verbote in ausländischen Rechtsordnungen relevant werden (**dazu unter II**).[630] Gleiches gilt mit Blick auf Versicherungsverbote, die meist an der rechtlichen Missbilligung von Lösegeldzahlungen anknüpfen. Erschwerend kommt hinzu, dass die in- und ausländische Rechtslage nicht nur für Versicherungsnehmer, sondern auch für Versicherer und Makler häufig undurchsichtig ist und Rechtsansichten hier teils diametral auseinanderklaffen.[631] Denn nur selten findet man eine ausdrückliche – wenn auch an die Erfüllung bestimmter Bedingungen geknüpfte – gesetzgeberische Billigung von Lösegeldzahlungen nach Ransomware-Attacken: Hier ist Frankreich nun mit Art. L. 12-10-1 *Code des assurances*[632] mit vorbildlicher Klarheit vorangegangen, obschon dieser Regelung ein zunächst in sehr unterschiedliche Richtungen

---

629 Vgl. etwa die folgende marktübliche Klausel: „Diese Police unterliegt deutschem Recht. Ausschließlich zuständig für Streitigkeiten im Zusammenhang mit dieser Police sind die deutschen Gerichte.".

630 Dieses restriktive Verständnis ist zuweilen im Klauselwortlaut und in der Systematik der AVB angelegt, wenn dort nämlich explizit die etwaig „für die jeweiligen Vertragsparteien geltenden Handels- und Wirtschaftssanktionen" angesprochen werden, so deutlich etwa in den vorstehend zitierten AVB. Solche Sanktionen wirken teils extra-territorial und können sowohl nationalen, unionalen wie auch drittstaatlichen Ursprungs sein.

631 Vgl. für Frankreich einerseits Art. L. 12-10-1 Code des assurances und andererseits etwa *Steimer*, Einführung in die Cyberversicherung, 2023, S. 105, der meint in Frankreich sei „die Lösegeldzahlung gesetzlich verboten". Vgl. mit Blick auf Italien nur *Pache*, Kompass Cyberversicherungen, 2. Aufl. 2023, S. 205, der von einem Verbot ausgeht, das aber so im Markt nicht einheitlich als auf Lösegelder nach Ransomware-Attacken gemünzt interpretiert wird. Siehe hierzu sogleich noch eingehend unter II 1 a) und b).

632 Art. L. 12-10-1 Code des assurances ist durch Art. 5 LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur, JORF n°21 v. 25.1.2023, eingefügt worden und nach Art. 5 Abs. 2 dieses Gesetzes mit Wirkung zum 25.4.2023 in Kraft getreten. Die Norm lautet auszugsweise: « Art. L. 12-10-1.-Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime.».

weisendes Gesetzgebungsverfahren vorausgegangen ist.[633] Die Rechtslage in Deutschland ist weniger eindeutig, obschon die Bundesregierung wiederholt von einer Zahlung von Lösegeldern nach Cyber-Attacken explizit abgeraten hat.[634]

I. Verbotsgesetze i.S.d. § 134 BGB: Straftatbestände und Sanktions- und Embargobestimmungen

Mit Blick auf die Versicherbarkeit von Lösegeldern im Zusammenhang mit erpresserischem Menschenraub ging die deutsche Aufsichtsbehörde zunächst von der Unvereinbarkeit mit den guten Sitten aus, ohne das jedoch am Maßstab des § 138 Abs. 1 BGB detailliert zu begründen.[635] Erst mit einem Rundschreiben aus dem Jahr 1998 änderte die Aufsichtsbehörde ihre Sichtweise, wobei sie zugleich eine Reihe von restriktiven Voraussetzungen aufstellte: Hierzu zählt neben der Geheimhaltung des Versicherungsschutzes für Lösegeldzahlungen insbesondere das Verbot, die Lösegelddeckung mit anderen Versicherungsprodukten zu kombinieren.[636] Diese Einschränkungen hat die BaFin sodann 2017 für die Cyber-Versicherung konkretisiert und das Verbot der Bündelung der Lösegeldversicherung für den Cyber-Kontext aufgehoben: Seither können – zumindest aus der Warte der Aufsichtsbehörde – Versicherer einen

633 Für ein Verbot von Lösegeldzahlungen und -versicherungen bei Ransomware-Attacken plädierte zunächst einerseits die Groupe d'études Assurances der französischen Assemblée Nationale unter der Leitung von *Valéria Faure-Muntian*, siehe nur *Groupe d'études Assurances*, Rapport La cyber-assurance, 2021. Demgegenüber sprach sich sodann andererseits das Haut Comité Juridique de la Place Financière de Paris gegen ein solches Verbot der Lösegeldzahlung und -versicherung aus, siehe *Haut Comité Juridique de la Place Financière de Paris*, Rapport sur l'assurabilité des risques cyber v. 28.1.2022.

634 Vgl. nur Antwort der *Bundesregierung* v. 27.7.2022, Drucksache 20/2926, S. 3: „Zahlungsaufforderungen im Falle von Ransomware-Angriffen sollte nicht Folge geleistet werden. Das Zahlen von Lösegeld bei Ransomware-Angriffen unterstützt kriminelle Akteure und finanziert weitere Straftaten. Betroffenen ist zudem davon abzuraten zu zahlen, da sie andernfalls als zahlungsbereite und daher attraktive Ziele für weitere Angriffe erscheinen können.".

635 Vgl. BAV, Geschäftsbericht 1981, S. 31 Nr. 141.

636 Hinzu treten als weitere Vorgaben neben der Geheimhaltung des Versicherungsschutzes auch solche zur inhaltlichen Ausgestaltung des Versicherungsvertrages: So ist dem VN nicht zuletzt eine Obliegenheit zur Geheimhaltung des Versicherungsschutzes sowie zur unverzüglichen Anzeige der Tat bei der Polizei aufzuerlegen und die Vertragslaufzeit darf zudem ein Jahr nicht überschreiten, vgl. BaFin, Rundschreiben 3/1998 (VA) – Hinweise des BAV zum Betrieb von Lösegeldversicherungen, abrufbar unter: (https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_9803_va_loesegeldversicherung.html zuletzt abgerufen am 1.5.2025).

Lösegeldbaustein in ihre Cyber-Deckungskonzepte integrieren.[637] Nach einer im Vordringen befindlichen Ansicht im Schrifttum sollen Lösegelder bei Ransomware-Attacken zudem unter bestimmten Voraussetzungen als Rettungskosten nach § 83 VVG ersatzfähig sein.[638]

Sowohl bei den expliziten Lösegeldbausteinen als auch bei einer etwaigen Ersatzfähigkeit als Rettungskosten stellt sich indes gleichermaßen die Frage nach der rechtlichen Zulässigkeit der Erstattung von Lösegeldern, die der Versicherungsnehmer oder ein von diesem beauftragter Dritter an Cyber-Kriminelle zahlt. Denn die in einem BaFin-Rundschreiben geäußerte Einschätzung der Aufsichtsbehörde ist weder rechtlich bindend noch umfasst sie in sachlicher Hinsicht eine abschließende Bewertung der privat-, straf- und sanktionenrechtlichen Wirksamkeit von Lösegeldbausteinen in AVB oder etwaigen Lösegelderstattungen nach § 83 VVG. Ebenso wie alle anderen BaFin-Rundschreiben hat auch diese Stellungnahme lediglich norminterpretierenden Charakter und beschränkt sich inhaltlich auf aufsichtsbehördliche Zwecke. Das Rundschreiben vermag deshalb allenfalls die BaFin selbst, nicht aber z.B. Gerichte im Deckungsprozess zu binden.[639]

Aus der Perspektive des deutschen Rechts ist somit insbesondere zu fragen, ob Verbotsgesetze i.S.d. § 134 BGB einer Lösegeldzahlung und/oder der Erstattungsfähigkeit von einmal gezahltem Lösegeld entgegenstehen. Bei Lösegelddeckungen kann sich ein gegen die Wirksamkeit des vertraglichen Leistungsversprechens gerichte-

---

637 Vgl. BaFin Journal 09/2017, S. 4 f.

638 Rüffer/Halbach/Schimikowski/*Salm*, 4. Aufl. 2020, A1-17 AVB Cyber Rn. 15; Prölss/Martin/*Klimke*, 22. Aufl. 2024, A1-17 AVB-Cyber Rn. 26 ff.; *König* in: MAH Versicherungsrecht, 5. Aufl. 2022, § 36 Rn. 126; *Sieg/Schilbach*, VersR 2023, 745, 749 ff.; *dies.*, PHi 2023, 46, 53; *Ballo/Pieper/Schneider*, r+s 2023, 741, 742. Vgl. zur Erstattungsfähigkeit eines „Lösegelds" zur Wiederbeschafftung eines gestohlenen versicherten Kfz auch OLG Saarbrücken VersR 1998, 1499 f.: „Unter diese Aufwendungen fallen auch die Aussetzung einer Belohnung oder die Zahlung eines Lösegelds. Denn ein Versicherungsnehmer ist berechtigt, als Geschädigter alle Maßnahmen zu treffen, die geeignet sind, sich den Besitz an einem gestohlenen Fahrzeug wieder zu beschaffen. Dazu zählt auch die Aussetzung und Bezahlung einer Belohnung oder eines Lösegeldes an Personen, welche für die Rückschaffung der gestohlenen Sache sorgen". Vgl. ferner nur Langheid/Wandt/*Looschelders*, VVG, 3. Aufl. 2022, § 83 VVG Rn. 13.

639 Die Rundschreiben entbehren einer – etwa für Allgemeinverfügungen notwendigen – gesetzlichen Ermächtigung und stellen unverbindliches Verwaltungshandeln dar, näher Langheid/Wandt/*Langheid/Goergen*, VVG, 3 Auf. 2024, Versicherungsaufsichtsrecht Rn. 152.

tes Verbot zunächst aus Straftatbeständen wie § 129 Abs. 1 S. 2 Var. 1, § 27 StGB oder § 89c Abs. 1 Nr. 3, Abs. 3, § 27 StGB ergeben (**dazu unter 1**).[640] Weitere Verbotstatbestände mögen aus Wirtschaftssanktionen des nationalen und des unmittelbar in Deutschland anwendbaren unionalen Rechts – wie der Cyberangriffs-VO[641] und den dazugehörigen Durchführungs-VO[642] sowie aus länder- bzw. personenspezifischen Sanktions- und Embargo-Verordnungen[643] – erwachsen (**dazu unter 2**). Soweit nicht durch ein Verbotsgesetz i.S.d. § 134 BGB eine rechtliche Missbilligung zum Ausdruck kommt, dürfte aus der Warte des deutschen Rechts dagegen weder die Zahlung noch die Erstattung von Lösegeldern im Gefolge von Ransomware-Attacken gegen die guten Sitten nach § 138 Abs. 1 BGB verstoßen.[644] Allerdings mag § 138 Abs. 1 BGB durchaus als Einfallstor für ausländische Verbotstatbestände dienen, soweit diese nicht schon als Eingriffsnormen nach Art. 9 Abs. 2 Rom I-VO anwendbar oder gemäß Art. 9 Abs. 3 Rom I-VO berücksichtigungsfähig sind.[645]

---

640 Dagegen liegt psychische Beihilfe zu den Straftaten der Cyber-Angreifer nach der hier vertretenen Auffassung überaus fern, vgl. im Ergebnis auch *Sieg/Schilbach*, VersR 2023, 745, 747.

641 Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, ABl. EU 2019 L 129I/1. Art. 3 Abs. 2 der Cyberangriffs-VO lautet: „Den in Anhang I aufgeführten natürlichen oder juristischen Personen, Organisationen oder Einrichtungen dürfen weder unmittelbar noch mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung gestellt werden oder zugutekommen."

642 Vgl. nur Durchführungsverordnung (EU) 2024/1778 des Rates vom 24. Juni 2024 zur Durchführung der Verordnung (EU) 2019/796 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, ABl. EU 2024 L 2024/1778.

643 Vgl. z.B. Beschluss (GASP) 2022/661 des Rates vom 21. April 2022 zur Änderung des Beschlusses (GASP) 2016/849 über restriktive Maßnahmen gegen die Demokratische Volksrepublik Korea, ABl. EU 2022 L 120/14.

644 Anders noch BAV, Geschäftsbericht 1981, S. 31 Nr. 141. Eingehend zum Ganzen *Sieg/Schilbach*, VersR 2023, 745, 748 ff.; *Eggen*, Die Cyberversicherung, 2023, S. 115 ff., die jeweils zutreffend betonen, dass durch den Lösegeldbaustein bzw. eine Ersatzfähigkeit als Teil der Rettungskosten i.S.d. § 83 VVG weder ein Anreiz für kriminelles Handeln geschaffen noch der Strafanspruch des Staates unterminiert wird.

645 Dazu sogleich näher unter II.

1. Beihilfe zur Unterstützung krimineller Vereinigungen oder zur Terrorismusfinanzierung als strafrechtliche Verbotsgesetze

Die Unwirksamkeit des versicherungsvertraglichen Leistungsversprechens mag sich nach § 134 BGB aus einem Verstoß gegen den Straftatbestand des § 129 Abs. 1 S. 2 Var. 1, § 27 StGB (**dazu unter a**) oder des § 89c Abs. 1 Nr. 3, Abs. 3, § 27 StGB (**dazu unter b**) ergeben.

a) Unterstützung einer kriminellen Vereinigung: § 129 Abs. 1 S. 2 Var. 1, § 27 StGB als Verbotsgesetz

Dreh- und Angelpunkt ist im allgemeinen Strafrecht § 129 Abs. 1 S. 2 Var. 1 StGB: Bei Hackergruppen, die den Versicherungsnehmer mithilfe von Ransomware zur „Lösegeldzahlung" zwingen, kann es sich um eine kriminelle Vereinigung und entsprechend bei der Zahlung des Lösegelds um die Unterstützung einer solchen Vereinigung handeln. § 129b Abs. 1 StGB erstreckt die Strafbarkeit auch auf die Unterstützung ausländischer krimineller Vereinigungen. Bei der Frage, ob der Tatbestand im hier interessierenden Zusammenhang verwirklicht wird, ist stets die Ausgestaltung des Deckungskonzepts für Lösegeldzahlungen im Blick zu behalten: Laut AVB ersetzen Versicherer dem Versicherungsnehmer nur im Nachhinein den ausgezahlten Lösegeldbetrag.[646] Die Lösegeldzahlung selbst wird dagegen – meist in Form von Krypto-Währungen – im Regelfall durch einen eigens vom Versicherungsnehmer beauftragten Dritten vorgenommen. Der strafrechtliche Vorwurf der Unterstützung einer kriminellen Vereinigung nach § 129 Abs. 1 S. 2 Var. 1 StGB kann in dieser Fallgestaltung also zunächst nur den unmittelbar zahlenden Akteur treffen. Handelt es sich hierbei um einen vom Versicherungsnehmer beauftragten Dritten, so dürfte der Versicherungsnehmer regelmäßig Tatherrschaft haben und die Zahlung ebenso wie die Verwirklichung des gesamten Tatbestandes als eigene Tat

[646] Eine Formulierung in AVB lautet beispielsweise „Der Versicherer erstattet Erpressungsgelder, die unmittelbar aufgrund einer angedrohten Informationssicherheitsverletzung von einem Versicherten gezahlt werden".

wollen. Damit kann der Versicherungsnehmer (Mit)Täter i.S.d. § 25 StGB sein.[647] Zu dieser Tat des Versicherungsnehmers könnte der Versicherer entweder durch das ausdrückliche Deckungsversprechen oder womöglich auch durch den – bereits vor Zahlung in Aussicht gestellten – Ersatz des Lösegelds als Rettungskosten sodann (psychische) Beihilfe im Sinne des § 27 StGB leisten.[648] Hier liegt entsprechend der Anknüpfungspunkt für eine etwaige Nichtigkeitssanktion: Strafrechtliche Normen können Verbotsgesetze i.S.d. § 134 BGB sein, wenn sie sich gegen den Abschluss eines Vertrages richten, durch den Beihilfe zu einer Straftat geleistet wird.[649]

Eine Beihilfe zur Unterstützung einer kriminellen Vereinigung nach § 129 Abs. 1 S. 2 Var. 1, § 129b Abs. 1 StGB setzt auf der ersten Ebene voraus, dass der Versicherungsnehmer (ggf. auch i.S.d. § 25 StGB „durch einen anderen“ in Gestalt einer von ihm hierzu beauftragten Person) durch die Lösegeldzahlung vorsätzlich und rechtswidrig den Tatbestand des § 129 Abs. 1 S. 2 Var. 1 StGB verwirklicht. Zu dieser Tat müsste der Versicherer sodann auf der zweiten Ebene durch sein die Lösegeldzahlung umfassendes Deckungsversprechen vorsätzlich Hilfe im Sinne des § 27 StGB leisten.

Zunächst dürften Hackergruppen häufig die Anforderungen des § 129 Abs. 1 S. 2 Var. 1, Abs. 2 StGB an eine kriminelle Vereinigung erfüllen, wenn sie wiederholt Computer- und Vermögensdelikte – etwa nach §§ 202a, 202d, § 303b sowie § 253 StGB – begehen die jeweils im Höchstmaß mit Freiheitsstrafe von mindestens zwei Jahren bedroht sind.[650] Die durch den Versicherungsnehmer veranlasste Lösegeldzahlung wird der Tätigkeit einer solchen kriminellen Vereinigung auch stets vorteilhaft und damit eine Unterstützungshandlung i.S.d. Norm sein. Obschon damit der objektive Tatbestand

---

647 In Betracht kommt – je nach Fallgestaltung – freilich auch eine Teilnehmerstellung und insbesondere die Anstiftung i.S.d. § 26 StGB.

648 Näher zum Anknüpfungspunkt der Beihilfe *Sieg/Schilbach*, VersR 2023, 745, 746 ff.

649 Vgl. BGH NJW 1996, 1812, 1813; BGH 15.4.2020 und 10.6.2020 – 5 StR 435/19, BeckRS 2020, 15826 Rn. 26. Siehe auch MünchKommBGB/*Armbrüster*, 10. Aufl. 2025, § 134 BGB Rn. 67 ff. Andeutungsweise auch *Eggen,* Die Cyberversicherung, 2023, S. 86 ff.

650 Vgl. zur Ransomware nur BGH NJW 2021, 2301. Eine kriminelle Vereinigung ist nach der Legaldefinition des § 129 Abs. 2 StGB „ein auf längere Dauer angelegter, von einer Festlegung von Rollen der Mitglieder, der Kontinuität der Mitgliedschaft und der Ausprägung der Struktur unabhängiger organisierter Zusammenschluss von mehr als zwei Personen zur Verfolgung eines übergeordneten gemeinsamen Interesses.“.

des § 129 Abs. 1 S. 2 Var. 1 StGB erfüllt sein mag, dürfte in der Praxis eine sichere Bestimmung der konkret handelnden Hackergruppe zum Zeitpunkt der Lösegeldzahlung kaum verlässlich möglich sein. Es erscheint mehr als fraglich, ob dem die Zahlung veranlassenden Versicherungsnehmer in subjektiver Hinsicht bedingter Vorsatz (*dolus eventualis*) hinsichtlich aller objektiven Tatbestandsmerkmale nachzuweisen sein wird: So dürften gerade in Zeiten von „ransomware-as-a-service", die im „Darknet" als für jedermann handhabbarer Erpressungsmalware zu erwerben ist, auch viele Einzeltäter anzutreffen sein, die – mangels Zusammenschlusses von mindestens zwei Personen – nun einmal keine kriminelle „Vereinigung" darstellen können.[651] Von Ausnahmefällen abgesehen, wird dem Versicherungsnehmer schon deshalb in der Praxis kaum bedingter Vorsatz hinsichtlich der Unterstützung einer „Vereinigung" nachzuweisen sein. Das gilt insbesondere dann, wenn der angegriffene Versicherungsnehmer nur mit einem Ansprechpartner – etwa per Chat – kommuniziert.[652]

Selbst sofern der Versicherungsnehmer ausnahmsweise sowohl den objektiven als auch subjektiven Tatbestand des § 129 Abs. 1 S. 2 Var. 1 StGB nachweisbar verwirklichen sollte, kommt auf Ebene der Rechtswidrigkeit rechtfertigender Notstand nach § 34 StGB in Betracht: Hier kann die Lösegeldzahlung nach Abwägung der widerstreitenden Interessen durchaus durch ein wesentlich überwiegendes Interesse des Ransomware-Opfers gerechtfertigt sein,[653] wobei freilich zu beachten ist, dass das Allgemeininteresse mit Höhe des Unterstützungsbeitrags sowie der Gefährlichkeit der unterstützten Vereinigung steigt.[654] Neben den eigenen Interessen des betroffenen Versicherungsnehmers sind auch die Interessen seiner Kunden an der Vertraulichkeit von Daten und Geschäftsgeheimnissen sowie – etwa im Fall der jüngst von einer Ransomware-Attacke betroffenen Universitätsklinik Düsseldorf – selbstverständlich auch

---

651 Vgl. erneut § 129 Abs. 2 StGB.

652 Ähnlich *König*, NZWiSt 2023, 167, 168 f., die allerdings bei Einschaltung eines IT-Dienstleisters wohl pauschal eine Identifikation der Gruppierung für möglich hält. Strenger *Eggen,* Die Cyberversicherung, 2023, S. 95 f. unter Verweis auf *Salomon*, MMR 2016, 575, 576 und *Arzt*, JZ 2001, 1052, 1054.

653 Eingehend *König*, NZWiSt 2023, 167 ff.; *Eggen,* Die Cyberversicherung, 2023, S. 97 ff.

654 *Brodowski/Schmid/Scholzen/Zoller*, NStZ 2023, 385, 389 f.

Bedrohungen von Leib und Leben Dritter zu berücksichtigen.[655] Obschon in letzterer Konstellation gemäß § 35 StGB notstandsfähige Rechtsgüter betroffen sind, kann ein angegriffenes Unternehmen jedoch bereits nicht in dem erforderlichen Näheverhältnis zum bedrohten Rechtsgutträger stehen, so dass ein entschuldigender Notstand ausscheidet.[656]

Vor diesem Hintergrund dürfte bereits eine für den Versicherer gemäß § 27 StGB teilnahmefähige vorsätzlich begangene rechtswidrige Tat des Versicherungsnehmers nach § 129 Abs. 1 S. 2 Var. 1 StGB fehlen. Folglich wird in der Praxis weder ein ausdrücklich in den AVB vorgesehener Lösegeldbaustein noch eine bereits vor Zahlung des Lösegeldes durch den Versicherer in Aussicht gestellte Erstattung über § 83 VVG eine Strafbarkeit wegen Beihilfe zur Unterstützung einer kriminellen Vereinigung nach § 129 Abs. 1 S. 2 Var. 1, § 27 StGB begründen.[657]

b) Terrorismusfinanzierung: § 89c Abs. 1 Nr. 3, Abs. 3, § 27 StGB als Verbotsgesetz

Die Finanzierung von Terrorismus ist nach § 89c Abs. 1 Nr. 3, Abs. 3 StGB auch im Fall von – bei Cyber-Angreifern wohl den Regelfall bildenden – Auslandstaten strafbar.[658] Durch die Zahlung von Lösegeld stellt der Versicherte Vermögenswerte zu Verfügung, die zudem nach § 89c Abs. 1 Nr. 3 StGB für Computerstraftaten wie eine Computersabotage nach § 303b StGB genutzt werden können. Doch auch sofern es sich um terroristisch motivierte Taten mit objektiver Schadensneigung i.S.d. Norm handeln sollte, müsste der Versicherte zumindest sicher wissen (*dolus directus* 2. Grades), dass die von ihm veranlasste Lösegeldzahlung gerade für die Begehung einer der Katalogstraftaten nach § 89c Abs. 1 S. 1 StGB

---

655 Wie hier *König*, NZWiSt 2023, 167, 170. In dieser Konstellation verstarb eine 78-jährige Notfallpatientin, die infolge der Ransomware-Attacke nicht im Uniklinikum Düsseldorf behandelt werden konnte und verlegt werden musste, *Kerkmann/Nagel*, Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf, Handelsblatt v. 18.9.2020. Vgl. zur späteren Aufklärung *Burger*, Die Spur führt nach Russland, FAZ v. 6.3.2023.

656 *Eggen,* Die Cyberversicherung, 2023, S. 95 f.

657 Im Ergebnis ebenso *Eggen,* Die Cyberversicherung, 2023, S. 109 f.

658 MünchKommStGB/*Schäfer/Anstötz*, 4. Aufl. 2021, § 89c StGB Rn. 18.

verwendet wird.[659] *Dolus eventualis* reicht insoweit folglich nicht aus. Die Lösegeldzahlung durch einen Versicherten, der eine terroristische Verwendung i.S.d. Norm in der Praxis allenfalls für möglich hält und – um der raschen Wiederherstellung seiner Daten willen – sodann billigend in Kauf nimmt, erfüllt damit nicht den Straftatbestand des § 89c Abs. 1 S. 1 StGB.[660] Mangels vorsätzlicher rechtswidriger Haupttat scheidet auch eine psychische Beihilfe seitens des Versicherers von vornherein aus.

Insgesamt lässt sich die in jüngeren Veröffentlichungen gerne schlagworthaft in den Raum gestellte Frage „Zuerst erpresst, dann verfolgt?“[661] damit sowohl für Versicherte als auch für Versicherer im Regelfall verneinen.

2. Nationale und unionale Sanktions- und Embargobestimmungen

Finanzsanktionen der EU können sich insbesondere gegen natürliche und juristische Personen als sanktionierte Entitäten richten.[662] Demgegenüber zielen Embargobestimmungen – etwa durch Ein- und Ausfuhrbeschränkungen – vorrangig auf Staaten und staatliche Akteure, die bei Cyber-Erpressungen zuweilen ebenfalls eine Rolle

---

659 Statt aller MünchKommStGB/*Schäfer/Anstötz*, 4. Aufl. 2021, § 89c StGB Rn. 15 m.w.N.

660 *Meyer/Biermann*, MMR 2022, 940, 943.

661 *Brodowski/Schmid/Scholzen/Zoller*, NStZ 2023, 385. Siehe auch zuvor *Gelinsky*, Erst erpresst, dann angeklagt, FAZ v. 11.5.2022, S. 16.

662 Vgl. beispielsweise zu sanktionierten Personen, die – u.U. gerade auch durch Cyber-Attacken auf Krypto-Assets und Ransomware-Angriffe – zur Finanzierung des nordkoreanischen Atomprogramms beitragen nur Beschluss (GASP) 2016/849 des Rates vom 27. Mai 2016 über restriktive Maßnahmen gegen die Demokratische Volksrepublik Korea und zur Aufhebung des Beschlusses 2013/183/GASP, ABl. EU 2016 L 141/79 in der jeweils letzten Fassung, zuletzt Beschluss (GASP) 2022/661 des Rates vom 21. April 2022 zur Änderung des Beschlusses (GASP) 2016/849 über restriktive Maßnahmen gegen die Demokratische Volksrepublik Korea, ABl. EU 2022 L 120/14. Vgl. für einen Überblick über die Russland-Sanktionen nur *P. Koch*, UKuR 2022, 400 ff.; *Lilie/Becker*, NZWiSt 2025, 133, 134.

spielen.[663] Dabei verschwimmen die Grenzen zwischen staatlichen und nicht-staatlichen Akteuren insbesondere bei Hacker-Gruppen.[664] Im Fall von Finanzsanktionen werden die sanktionierten Personen durch an die übrigen Wirtschaftsteilnehmer gerichtete Ge- und Verbote vom Wirtschaftsverkehr weitgehend ausgeschlossen.[665] Die Instrumente können neben Einschränkungen des Zahlungs- und Kapitalverkehrs und dem Einfrieren von Vermögenswerten in der Regel Bereitstellungsverbote umfassen, die im Kontext von Lösegeldzahlungen von besonderer Bedeutung sind: Denn durch ein Bereitstellungsverbot wird den übrigen Wirtschaftsakteuren untersagt, der sanktionierten Person und Entitäten Gelder oder sonstige wirtschaftliche Ressourcen zur Verfügung zu stellen.[666] Das Bereitstellungsverbot ist dabei weit gefasst: Der EuGH legt in seiner ständigen Rechtsprechung die Begriffe „Gelder" und „zur Verfügung stellen" extensiv aus und lässt es bereits ausreichen, dass die sanktionierte Person „tatsächlich die vollständige

---

663 Siehe mit Blick auf einen internen Beichte der Vereinten Nationen zu den Hacker-Aktivitäten Nordkoreas und insbesondere der staatlichen „Lazarus"-Gruppe *SRF*, Nordkoreas Hacker erbeuten Rekordsumme für Atomwaffenprogramm v. 7.2.2023: „In den vergangenen rund sechs Jahren sollen die staatlich eingesetzten Hacker online insgesamt etwa 1.2 Milliarden Dollar erbeutet haben.", abrufbar unter: https://www.srf.ch/news/international/uno-expertenbericht-nordkoreas-hacker-erbeuten-rekordsumme-fuer-atomwaffenprogramm (zuletzt abgerufen am 1.5.2025). Siehe auch Verordnung (EU) 2017/1509 des Rates vom 30. August 2017 über restriktive Maßnahmen gegen die Demokratische Volksrepublik Korea und zur Aufhebung der Verordnung (EG) Nr. 329/2007, ABl. EU 2017 L 224/1: Darin wurden die gegen Nordkorea verhängten Sanktionen aus Gründen der Übersichtlichkeit zusammengefasst. Hierdurch ergaben sich Änderungen der jeweiligen Artikelbezeichnungen. Inhaltliche Änderungen wurden nicht vorgenommen. Weiterhin bestehen gegen Nordkorea unterschiedlichste güter- und dienstleistungsbezogene Beschränkungen sowie Beschränkungen im Geld- und Kapitalverkehr. Daneben gelten auch die Finanzsanktionen fort. Die Gelder und wirtschaftlichen Ressourcen der Personen, Organisationen und Einrichtungen, die in den Anhängen XIII, XV, XVI und XVII dieser Verordnung genannt sind, werden eingefroren. Diesen Personen dürfen weder Gelder noch sonstige Wirtschaftsressourcen zur Verfügung gestellt werden (Bereitstellungsverbot).

664 Vgl. zur zumindest staatsnahen Gruppe „Storm-0558" aus der Volksrepublik China nur *Finsterbusch/Sachse*, Chinas Hacker rüsten auf, FAZ v. 29.7.2023, S. 24; vgl. zur nordkoreanischen „Lazarus"-Gruppe erneut nur *SRF*, Nordkoreas Hacker erbeuten Rekordsumme für Atomwaffenprogramm v. 7.2.2023.

665 Vgl. allgemein nur Europäische Union, Leitlinie zur Umsetzung und Evaluierung restriktiver Maßnahmen (Sanktionen) im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU v. 4.5.2018, 5664/18.

666 Vgl. zur SDN-Listung in den USA nur schweizerisches Bundesgericht 17.8.2023 – 4A_206/2023. Vgl. nur Art. 32 Verordnung (EU) 2017/1509. Siehe allgemein Europäische Union, Leitlinie zur Umsetzung und Evaluierung restriktiver Maßnahmen (Sanktionen) im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU v. 4.5.2018, 5664/18, Rn. 82.

Verfügungsbefugnis über die betreffenden Gelder, andere finanzielle Vermögenswerte oder wirtschaftliche Ressourcen erlangen kann".[667] Im Vordergrund steht hier damit weniger die Art der bereitgestellten Sache, als vielmehr ihre Eigenschaft als Vermögenswert und die Verschaffung der effektiven Verfügungsmöglichkeit über ebendiesen Wert. Vor diesem Hintergrund werden auch die bei Ransomware-Attacken üblicherweise geforderten Zahlungen mithilfe von digitalen Vermögenswerten – wie insbesondere Kryptowährungen – ohne Weiteres von den Bereitstellungsverboten des Unionsrechts erfasst.[668]

Speziell mit Blick auf Cyberattacken sieht die Cyberangriffs-VO[669] der EU eine Reihe von Finanzsanktionen gegenüber den an solchen Attacken beteiligten Personen vor.[670] Hierzu zählt nach Art. 3 Abs. 2 Cyberangriffs-VO insbesondere ein umfassendes Bereitstellungsverbot. Verstöße gegen dieses unionsrechtliche Bereitstellungsverbot sanktioniert das deutsche Außenwirtschaftsrecht bei vorsätzlicher Zuwiderhandlung sodann nach § 18 Abs. 1 Nr. 1 lit. a AWG mit einer Freiheitsstrafe von bis zu fünf Jahren. Ein (bedingt) vorsätzliches Handeln der Person, die ein Lösegeld nach einer Ransomware-Attacke entrichtet, kommt aber allenfalls dann in Betracht, wenn aus den individuellen Umständen des Einzelfalls ausnahmsweise die Identität der Cyber-Kriminellen bereits im Zeitpunkt der Lösegeldzahlung mit hinreichender Sicherheit erkennbar ist.[671] Das dürfte nur in Ausnahmefällen zutreffen, und dieses subjektive

---

667 Siehe nur EuGH 11.10.2007 – Rs. C-117/06 (*Möllendorf*) ECLI:EU:C:2007:596 Rn. 51; EuGH 29.6.2010 – Rs. C-550/09 (*E und F*) ECLI:EU:C:2010:38 Rn. 67.

668 Vgl. Europäische Union, Leitlinie zur Umsetzung und Evaluierung restriktiver Maßnahmen (Sanktionen) im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik der EU v. 4.5.2018, 5664/18, Rn. 60. Vgl. auch BGH NJW 2010, 2370 Rn. 19.

669 Verordnung (EU) 2019/796 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, ABl. 2019 L 129 I/1. Siehe auch Beschluss (GASP) 2019/797 des Rates vom 17. Mai 2019 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, ABl. 2019 L 129 I/13.

670 Allerdings adressiert die Cyberangriffs-VO weder Ransomware-Attacken noch Lösegeldzahlungen gesondert und sieht – anders als das mittlerweile aufgehobene EU-Sanktionsregime gegen den Iran – keine expliziten Versicherungsverbote vor, vgl. dagegen Art. 35 Abs. 1 Verordnung (EU) Nr. 267/2012 des Rates vom 23. März 2012 über restriktive Maßnahmen gegen Iran und zur Aufhebung der Verordnung (EU) Nr. 961/2010, ABl. 2012 L 88/1: „Es ist verboten, Versicherungen oder Rückversicherungen bereitzustellen oder die Bereitstellung von Versicherungen oder Rückversicherungen zu vermitteln …".

671 Vgl. zum Erfordernis (bedingten) Vorsatzes im Zeitpunkt der Vornahme der strafbewehrten Handlung nur § 8 S. 1, § 16 Abs. 1 S. 1 StGB.

Tatbestandsmerkmal wird selbst dann durch die Ermittlungsbehörden nur schwerlich beweisbar sein. Dennoch kann im Grundsatz ein Verbot von Lösegeldzahlungen aus sanktionen- und embargorechtlichen Normen nationalen und unionalen Ursprungs folgen.[672] Auf der nächsten Ebene könnte sich ein – an die Cyber-Versicherer gerichtetes – Verbot i.S.d. § 134 BGB daraus ergeben, dass der Versicherer mit der Erstattung des Lösegeldes (sei es auf Grundlage eines Lösegeldbausteins oder als vorab in Aussicht gestellter Ersatz von Rettungskosten nach § 83 VVG) psychische Beihilfe zur vorsätzlichen und rechtswidrigen Haupttat des entgegen der strafbewehrten Sanktions- und/oder Embargobestimmungen zahlenden Versicherungsnehmers leistet.[673] Denn ebenso wie inländische[674] Sanktionsinstrumente sind unmittelbar in Deutschland anwendbare EU-Sanktions- und Embargo-Verordnungen im Grundsatz Verbotsgesetze i.S.d. § 134 BGB: Sie richten sich nämlich stets gegen den wirtschaftlichen Erfolg des jeweiligen Rechtsgeschäfts oder der jeweiligen Transaktion.[675]

Diese Frage dürfte allerdings in der Praxis schon deshalb kaum relevant werden, weil die Cyber-Versicherer in ihren Bedingungswerken üblicherweise alle Zahlungen vom Deckungsversprechen ausnehmen, die gegen „für die jeweiligen Vertragsparteien geltenden Handels- und Wirtschaftssanktionen“ verstoßen. Nach dem ausdrücklichen Wortlaut der Klausel erstattet der Versicherer damit keine (Lösegeld)Zahlungen, durch die der ursprünglich zahlende Versicherte seinerseits gegen Sanktionen verstößt. Auf die Frage der strafrechtlichen Beurteilung sowie auf § 134 BGB kommt es ange-

672 Vgl. im Ergebnis auch *Salomon*, MMR 2016, 575; *Habbe/Gergen*, CCZ 2020, 281, 285 f.

673 Dagegen sind explizit an den Versicherer adressierte Verbote, dem Versicherten eine bereits geleistete Zahlung zu erstatten – wie Lösegeld nach einer Ransomware-Attacke –, selten. Eine Ausnahme findet sich im nationalen Recht des Vereinigten Königreichs mit Blick auf die Terrorismusfinanzierung. Sec. 17A(1) Terrorism Act 2000, 2000 c. 11, lautet auszugsweise: „The insurer under an insurance contract commits an offence if (a) the insurer makes a payment under the contract, or purportedly under it, (b) the payment is made in respect of any money … that has been … handed over in response to a demand made wholly or partly for the purposes of terrorism, and (c) the insurer or the person authorising the payment on the insurer's behalf knows or has reasonable cause to suspect that the money or other property has been … handed over in response to such a demand.“.

674 Zu diesen zählen freilich auch Instrumente, die der Umsetzung von Sanktionen des UN-Sicherheitsrats dienen, vgl. §§ 4, 5, 5a und 6 AWG.

675 Statt vieler *Wandt*, VersR 2013, 257, 262; *Armbrüster/Schilbach*, r+s 2016, 109, 114; *P. Koch*, UKuR 2022, 400 ff.

sichts dieser Begrenzung des vertraglichen Leistungsversprechens gar nicht mehr an. Die Inkorporation der Sanktionsbestimmungen zum Zweck der Definition des vertraglichen Leistungsspektrums trägt zum einen der potentiell extra-territorialen Wirkung solcher Instrumente Rechnung und soll zum anderen Versicherer ihrerseits vor eigener straf- und sanktionenrechtlicher Verantwortlichkeit wegen (psychischer) Beihilfe zu etwaigen Taten des Versicherten schützen.[676] Derartige anerkennenswerte Motive sind auch im Rahmen der Klauselkontrolle solcher Risikoausschlüsse in AVB zu berücksichtigen und dürften grundsätzlich für die Wirksamkeit der Klausel streiten.[677] Anders mag der Fall liegen, wenn die Ausschlussklausel die Beachtlichkeit ausländischer Sanktionen auch im Hinblick auf Vertragsdritte (etwa die Muttergesellschaft oder die Konzernobergesellschaft des Versicherers) vorgibt und so den Versicherungsschutz auszuhöhlen droht, obgleich der Cyber-Versicherer sich in dieser Konstellation keiner eigenen straf- oder sanktionsrechtlichen Verantwortlichkeit ausgesetzt sieht.[678]

II. Drittstaatliche Verbotstatbestände: Art. 9 Rom I-VO und § 138 Abs. 1 BGB als Einfallstore

Die Erstattung von Lösegeldern im Gefolge einer Ransomware-Attacke wird in manchen AVB davon abhängig gemacht, dass zum einen schon die Lösegeldzahlung „gesetzlich zulässig“ und zum an-

[676] Vgl. neben der bereits erörterten Beihilfe des Versicherers nach § 27 StGB zu einer Straftat des Versicherten nach § 18 Abs. 1 Nr. 1 lit. a AWG auch erneut die Pönalisierung des Versicherers in manchen Rechtsordnungen, z.B. im Vereinigten Königreich nach Sec. 17A(1) *Terrorism Act 2000* (2000 c. 11). Nicht zuletzt vor diesem Hintergrund stellt auch die „Lloyd’s Sanctions Guidance“ allgemein Folgendes heraus: „the insurer (and/or the broker) may not be able, directly *or indirectly*, to make payments to or for the benefit of, or receive payments from, the individual or entity designated under sanctions“, siehe dazu *Wragg,* Lloyd’s Sanctions Guidance – Sanctions Clauses 2015 (Market Bulletin Y4832), Lloyd’s of London, abrufbar unter: https://www.lloyds.com/~/media/files/the-market/communications/market- bulletins/2014/10/y4832.pdf (zuletzt abgerufen am 1.5.2025).

[677] Vgl. *Wandt*, VersR 2013, 257, 263 ff. Vgl. – implizit – auch LG Hamburg VersR 2015, 1024, 1025.

[678] Vgl. *Looschelders*, VersR 2015, 1025, 1026. Vgl. zur Frage der Zahlung an eine u.U. in den USA SDN-gelistete Gruppe nur schweizerisches Bundesgericht 17.8.2023 – 4A_206/2023.

deren diese Zahlung auch „versicherbar“ ist.[679] Wenn die Parteien deutsches Recht im Cyber-Versicherungsvertrag gewählt haben, bilden hier zunächst deutsche und unionale Verbotsnormen den Maßstab.[680] Dagegen führen Verbote aus ausländischen Rechtsordnungen grundsätzlich nicht schon als „Verbotsgesetze“ i.S.d. § 134 BGB i.V.m. Art. 2 EGBGB zur Unwirksamkeit eines Rechtsgeschäfts und stehen damit weder der Lösegeldzahlung durch den Versicherten noch der Versicherbarkeit und damit der nachträglichen Erstattung des Lösegelds entgegen.[681] Etwas anderes gilt zunächst, wenn die Parteien ihren (Versicherungs)Vertrag zwar durch Rechtswahl gezielt deutschem Recht unterstellt haben, alle anderen Sachverhaltselemente aber zum Recht eines anderen Staates weisen: Hier kann gemäß Art. 3 Abs. 3 Rom I-VO durch die parteiautonome Bestimmung des Vertragsstatuts nicht von den – intern wie international – zwingenden Normen dieses anderen Staates abgewichen werden,[682] so dass dessen zum *ius cogens* zählende Verbotsgesetze über § 134 BGB zur Nichtigkeit des Vertrages führen können.[683]

Aber auch jenseits dieser Konstellation können bei Cyber-Versicherungsverträgen mit grenzüberschreitenden Bezügen durchaus auch Verbote aus ausländischen Rechtsordnungen relevant werden: Allerdings ist der Kreis expliziter Verbote von Lösegeldzahlungen jenseits von Sanktions- und Embargobestimmungen[684] vergleichsweise eng gezogen, wie eine – keineswegs erschöpfende – rechtsvergleichende Umschau verdeutlicht (**dazu unter 1**). Solche ausländischen Verbotstatbestände können auch ungeachtet des

---

679 Vgl. etwa die folgende marktübliche Formulierung: „Cyber-Lösegeld ist Geld und Kryptowährungen, die von dem Versicherten zwecks Unterbindung oder Beendigung von Cyber-Erpressung gezahlt werden, vorausgesetzt, dass die Zahlung gesetzlich zulässig und versicherbar ist“.

680 Siehe dazu erneut oben F II.

681 Vgl. nur BGH NJW-RR 2021, 1244 Rn. 30. Vgl. auch BGH 23.10.2018 – 1 StR 234/17, BeckRS 2018, 37760 Rn. 45; BGH NJW 1977, 2356; BGH VersR 1972, 849, 850. Vgl. statt vieler auch *Armbrüster/Schilbach*, r+s 2016, 109, 114.

682 Art. 3 Abs. 4 Rom I-VO erstreckt diesen Ansatz bei einer Rechtswahl drittstaatlichen Rechts auch auf all jene Normen des Rechts der EU – gegebenenfalls in der von dem Mitgliedstaat des angerufenen Gerichts umgesetzten Form –, von denen nicht durch Vereinbarung abgewichen werden kann.

683 Vgl. nur Staudinger/*Fischinger/Hengstberger*, 2021, § 134 BGB Rn. 72 ff., 181 und 537; MünchKommBGB/*Armbrüste*r, 10. Aufl. 2025, § 134 BGB Rn. 57. Vgl. auch – unter umgekehrten Vorzeichen und inhaltlich verkürzend – BAG NZA 2021, 225 Rn. 57.

684 Zu diesen sogleich näher unter 1 und 2.

kraft Rechtswahl auf den Versicherungsvertrag anwendbaren Rechts als Eingriffsnormen gemäß Art. 9 Rom I-VO Anwendung finden (**dazu unter 2**). Darüber hinaus können solche Verbotsnormen auch bei der Wahl deutschen Rechts stets im Rahmen der Generalklauseln materiell-rechtlich berücksichtigt werden (**hierzu unter 3**).[685]

1. Vermeintliche und tatsächliche Verbote von Lösegeldzahlungen in ausländischen Rechtsordnungen

Im Schrifttum zur Cyber-Versicherung finden sich unterschiedliche Ansichten dazu, inwieweit bestimmte ausländische Rechtsordnungen die Zahlung und/oder die Versicherung von Lösegeldern im Gefolge von Ransomware-Attacken untersagen.[686] Während eine abschließende Analyse aller relevanten Rechtsordnungen schon aufgrund der Dynamik des Rechtsgebiets und der Komplexität nicht Gegenstand dieser Abhandlung sein kann, sollen im Folgenden doch im Rahmen einer exemplarischen rechtsvergleichenden Umschau einige Tendenzen und Entwicklungslinien aufgezeigt werden: Im Zentrum stehen dabei neben dem italienischen (**dazu unter a**) und französischen Recht (**hierzu unter b**) einige Rechtsordnungen ausgewählter US-Bundesstaaten (**dazu unter c**), in denen in jüngerer Zeit eine besonders intensive Gesetzgebungstätigkeit zu verzeichnen war.

a) Italien: Klare Unklarheit

Das italienische Recht wird in der Diskussion um die rechtliche Zulässigkeit von Lösegeldzahlungen nach Ransomware-Attacken häufig als Paradebeispiel für ein Verbot sowohl von Lösegeldzahlungen als auch von Versicherungsleistungen für solche Zahlungen ge-

685 Siehe BGHZ 59, 82, 85 f.; BGHZ 94, 268, 271; BGH NJW-RR 2021, 1244 Rn. 31; OLG Frankfurt a. M. NJW 2018, 3591 Rn. 31 ff. und insbesondere Rn. 43; OLG München BeckRS 2020, 15428 Rn. 31 ff. Siehe auch EuGH 18.10.2016 – Rs. C-135/15 (*Nikiforidis*) ECLI:EU:C:2016:774 Rn. 40 ff. und 55. A.A. und enger indes Grüneberg/*Thorn*, 84. Aufl. 2025, Art. 9 Rom I-VO Rn. 14.

686 Vgl. nur *Pache*, Kompass Cyberversicherungen, 2. Aufl. 2023, S. 205.

nannt.[687] Allerdings ist hier jeweils der Wortlaut und vor allem auch der – im historischen Kontext zu würdigende – Sinn und Zweck dieser Regelungen zu beachten. So lautet Art. 12(1) des italienischen Privatversicherungsgesetzes (*Codice delle Assicurazione Private*) auszugsweise:

> *„Sono vietate le … assicurazioni che hanno per oggetto il trasferimento del rischio di pagamento delle sanzioni amministrative e quelle che riguardano il prezzo del riscatto in caso di sequestro ... In caso di violazione del divieto il contratto è nullo…".*
>
> *Zu deutsch:*
>
> *„Versicherungen, welche die Übernahme des Risikos der Zahlung von verwaltungsrechtlichen Sanktionen oder von Lösegeldern im Fall von Entführungen zum Gegenstand haben, …sind verboten… Ein Verstoß führt zur Nichtigkeit des Vertrags…".*

Im Italienischen bezeichnet „sequestro" allerdings zuvörderst eine Entführung, die – noch präziser gefasst – als „sequestro di persona" die Entführung einer Person und als „sequestro di persona a scopo di estorsione" den erpresserischen Menschenraub benennt. Der Wortlaut des Art. 12(1) *Codice delle Assicurazione Private* ist damit jedenfalls nicht ausdrücklich auf Datenverschlüsselungen und die damit bei Ransomware-Attacken üblicherweise einhergehenden Lösegeldforderungen gemünzt. Vielmehr legt die verkürzte Formulierung „sequestro" eine physische Freiheitsberaubung („sequestro di persona") nahe, deren Opfer nur ein Mensch, nicht aber auch IT-Systeme sein können.

Diese am Wortlaut orientierte Auslegung von Art. 12(1) *Codice delle Assicurazione Private* findet eine Stütze in der historischen Entwicklung und Motivation der strafrechtlichen Bewehrung von Lösegeldzahlungen, die sich – soweit ersichtlich – in Italien ausschließlich auf den erpresserischen Menschenraub beschränkt: So wird die Zahlung von Lösegeld (u.a. durch Angehörige von Entführungsop-

[687] So exemplarisch von *Pache*, Kompass Cyberversicherungen, 2. Aufl. 2023, S. 205 m.w.N.

fern) mit einer Freiheitsstrafe von bis zu 5 Jahren bestraft.[688] Hinter dieser Pönalisierung von Lösegeldzahlungen stand das gesetzgeberische Anliegen, die Einnahmen sowohl der organisierten Kriminalität („Mafia“) als auch terroristischer Vereinigungen zu beschneiden und so dem bis dahin weit verbreiteten erpresserischen Menschenraub Einhalt zu gebieten.[689] Andere Rechtsordnungen – wie jüngst etwa Nigeria mit der *Terrorism (Prevention) Act 2013 (Amendment) Bill 2022* – sind dem italienischen Vorbild gefolgt und untersagen ebenfalls die Zahlung von Lösegeldern bei erpresserischem Menschenraub, um terroristischen und/oder kriminellen Organisationen wichtiger Einnahmequellen zu berauben.[690]

Vor diesem Hintergrund erscheint es mehr als fraglich, dass das im italienischen Recht in Art. 12(1) *Codice delle Assicurazione Private* niedergelegte Verbot von Lösegeldzahlungen auch auf Lösegeldbausteine im Rahmen von Cyber-Versicherungsverträgen anwendbar ist.[691] Zu dieser Lesart passt, dass dem Vernehmen nach durchaus manche im italienischen Markt aktive Cyber-Versicherer Deckung für Lösegeldzahlungen nach Ransomware-Attacken anbieten, obschon auch einige – vornehmlich ausländische – Versicherer spezifische Ausschlussklauseln für „Cyber-Extorsion“ mit Bezug zu Italien vorsehen.

b) Frankreich: Bedingte Zulässigkeit

Mit Blick auf die französische Rechtsordnung findet sich im deutschen Schrifttum die Aussage, dass in Frankreich „die Zahlung von Lösegeld gesetzlich verboten“ sei.[692] Diese Annahme gilt es im Folgenden kritisch zu überprüfen, zumal der – dem deutschen GDV entsprechende – Verband der französischen Versicherungswirtschaft, France Assureurs, in einer Publikation aus dem Jahr 2022

---

688 Vgl. mit Blick auf die Reform des italienischen Strafrechts im Jahre 1991 nur *v. Hippel*, ZRP 2002, 442, 443.

689 Vgl. zu den mit diesem Regelungsansatz erzielten Erfolgen bei der Kriminalitätsbekämpfung *v. Hippel*, ZPR 2002, 442, 443.

690 Vgl. zu nigerianischem Recht *Terrorism (Prevention) Act 2013 (Amendment) Bill 2022* nur https://placng.org/i/wp-content/uploads/2022/05/Senate-Report-on-Terrorism-Prevention-Act-2013-Amendment-Bill-2021.pdf (zuletzt 1.5.2025).

691 Anders *Pache*, Kompass Cyberversicherungen, 2. Aufl. 2023, S. 205.

692 *Steimer*, Einführung in die Cyberversicherung, 2023, S. 105.

apodiktisch meint, dass weder die Lösegeldzahlung nach Ransomware-Attacken noch die Erstattung solcher Lösegeldzahlungen durch Cyber-Versicherer durch irgendein nationales oder europäisches Gesetz untersagt würden.[693]

Die Debatte in Frankreich ist in der Tat kontrovers geführt worden: Für ein Verbot von Lösegeldzahlungen und -versicherungen bei Ransomware-Attacken plädierte zunächst die Groupe d'études Assurances der französischen *Assemblée Nationale* unter der Leitung von *Faure-Muntian*.[694] Demgegenüber sprach sich sodann andererseits das *Haut Comité Juridique de la Place Financière de Paris* gegen ein solches Verbot der Lösegeldzahlung und -versicherung aus und führte u.a. unionsrechtliche Argumente ins Feld.[695] Mit Blick auf die Versicherbarkeit von Lösegeldern hat der französische Gesetzgeber sodann die Vorschläge der zuletzt genannten Organisation aufgegriffen.[696] Nunmehr hat Frankreich als – soweit ersichtlich – erster EU-Mitgliedstaat eine – unter die Bedingung der Meldung des Cyber-Angriffs an die Behörde gestellte – gesetzgeberische Billigung auch der Erstattung von Lösegeldzahlungen nach Ransomware-Attacken erlassen. Art. L. 12-10-1 *Code des assurances*[697] lautet auszugsweise wie folgt:

> *« Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard*

693 *France Assureurs*, Livre blanc: Bâtir une économie de la donnée, 2022, S. 25: „Aucun texte national ou européen n'interdit le paiement d'une rançon par une entreprise ni le remboursement des rançons par un assureur, à l'exception des cas particuliers de financement du terrorisme et de blanchiment de capitaux.".

694 *Groupe d'études Assurances*, Rapport La cyber-assurance, 2021.

695 *Haut Comité Juridique de la Place Financière de Paris*, Rapport sur l'assurabilité des risques cyber v. 28.1.2022.

696 Vgl. Art. 4 Projet de Loi d'orientation et de programmation du ministère de l'intérieur v. 18.10.2022, n° 2 Sénat.

697 Art. L. 12-10-1 Code des assurances ist durch Art. 5 LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur, JORF n°21 v. 25.1.2023, eingefügt worden und nach Art. 5 Abs. 2 dieses Gesetzes mit Wirkung zum 25.4.2023 in Kraft getreten.

soixante-douze heures après la connaissance de l'atteinte par la victime. »

Zu deutsch:

Die Auszahlung einer Summe gemäß den Bestimmungen eines Versicherungsvertrags, der die Entschädigung des Versicherten für Einbußen infolge von Angriffen auf ein System zur automatisierten Datenverarbeitung im Sinne der Artikel 323-1 bis 323-3-1 des Strafgesetzbuches zum Gegenstand hat, steht unter der Bedingung, dass der Geschädigte bei den zuständigen Behörden spätestens 72 Stunden nach Kenntniserlangung von dem Angriff Anzeige erstattet.

Im Gesetzesentwurf des *Sénat* v. 18.10.2022 war zunächst nur von Lösegeldbausteinen die Rede, die eine Erstattung von Lösegeldern nach Ransomware-Attacken vorsahen: Allein die Erstattung von Lösegeldzahlungen unter dem Cyber-Versicherungsvertrag sollte von der rechtzeitigen Anzeigeerstattung durch den angegriffenen Versicherten gegenüber der zuständigen Behörde abhängig gemacht werden.[698] Der französische Gesetzgeber hat sodann jedoch die Einschränkung auf die Erstattung von Lösegeldern gestrichen und vielmehr alle Zahlungen unter dem Cyber-Versicherungsvertrag nach einer Cyber-Attacke von der Erstattung einer (Straf)Anzeige binnen 72 Stunden nach Kenntniserlangung durch den Versicherten vorgesehen.[699] Aus dem Gesetzgebungsverfahren und insbeson-

[698] Art. 4 des Gesetzentwurfs (Projet de Loi d'orientation et de programmation du ministère de l'intérieur v. 18.10.2022, n° 2 Sénat) lautet auszugsweise: « Le versement d'une somme en application d'une clause assurantielle *visant à couvrir le paiement d'une rançon par l'assuré dans le cadre d'une extorsion prévue à l'article 312-1 du code pénal*, lorsqu'elle est commise au moyen d'une atteinte à un système de traitement automatisé de données prévue aux articles 323-1 à 323-3-1 du même code, est subordonné à la justification du dépôt d'une pré-plainte de la victime auprès des autorités compétentes dans les 24 heures suivant l'attaque et avant tout paiement de cette rançon. » (Herv. d. Verf.).

[699] Die Ausweitung über die Erstattung von Lösegeldern hinaus auf alle Versicherungsleistungen nach einer Cyber-Attacke ist durch den Bericht und den sodann von der Assemblée Nationale am 22.11.2022 angenommenen Textvorschlag v. 4.11.2022 eingefügt worden, der ausdrücklich die Gestattung von Lösegelderstattung vorsieht und nur eine Erweiterung des Anzeigeerfordernisses beinhaltet, vgl. Art. 4 (dort insbesondere unter 3.) Rapport n° 436 (*Florent Boudié*) fait au nom de la commission des lois, déposé le 4 novembre 2022, Texte de la commission n° 436 déposé le 4 novembre 2022 sowie Texte n° 32 modifié par l'Assemblée nationale le 22 novembre 2022, jeweils abrufbar unter: https://www.senat.fr/dossier-legislatif/pjl21-876.html (zuletzt abgerufen am 1.5.2025).

dere aus den Kommissionsdokumenten der *Assemblée Nationale* und aus den Diskussionen sowie vor allem aus dem Gesetzeswortlaut selbst geht hervor, dass der französische Gesetzgeber unter der bereits erwähnten Bedingung der Anzeigeerstattung von der Ersatzfähigkeit von Lösegeldzahlungen im Rahmen von Lösegelddeckungen bei Cyber-Versicherungen ausgeht.[700] Aus Art. L. 12-10-1 *Code des assurances* geht damit hervor, dass Lösegeldzahlungen nach Ransomware-Attacken aus der Warte des französischen Gesetzgebers grundsätzlich rechtlich gestattet sind, sofern der Versicherte das Anzeigeerfordernis rechtzeitig erfüllt.[701]

Ebenso wie in anderen Rechtsordnungen drohen dem Versicherten, der eine Lösegeldzahlung veranlasst, indes auch in Frankreich strafrechtliche Konsequenzen, sofern die Zahlung z.B. eine terroristische Vereinigung i.S.d. Art. 421-2-2 *Code pénal* unterstützt. Hier mag sich dann die bereits mit Blick auf das deutsche Recht diskutierte Frage stellen,[702] ob der Versicherte den objektiven wie subjektiven Straftatbestand erfüllt und angesichts seiner Zwangslage auch nicht durch Art. 122-2 *Code pénal* von der strafrechtlichen Verantwortung befreit ist. Dies begegnet den gleichen Bedenken wie im deutschen Recht.[703] Entsprechend erübrigt sich im Regelfall die weitergehende Frage, ob der Cyber-Versicherer durch die Lösegelddeckung zum Teilnehmer einer etwaigen Haupttat des Versicherten werden kann.[704]

---

700 Siehe erneut Art. 4 (dort insbesondere unter 3.) des Rapport n° 436 (*Florent Boudié*) fait au nom de la commission des lois, déposé le 4 novembre 2022, Texte de la commission n° 436 déposé le 4 novembre 2022 sowie sodann den Texte n° 32 modifié par l'Assemblée nationale le 22 novembre 2022, jeweils nebst aller späteren Kommissionsdokumente und Mitschriften der Debatten abrufbar unter: https://www.senat.fr/dossier-legislatif/pjl21-876.html (zuletzt abgerufen am 1.5.2025).

701 So die – soweit ersichtlich – einhellige Ansicht im französischen Schrifttum, siehe statt vieler *Marly*, Recueil Dalloz 2023, 112; *Perrier*, RSC 2023, 381 f.; *Bigot/Cayol/Noguéro/Pierre*, Recueil Dalloz 2023, 1142 f.

702 Vgl. oben I 1.

703 Vgl. erneut oben I 1.

704 Vgl. erneut oben I 1.

c) US-Bundesstaaten: Beispiele für punktuelle Verbote und weitergehende Gesetzesentwürfe

In den USA haben beim derzeitigen Stand bereits mehrere Bundesstaaten Gesetzesentwürfe auf den Weg gebracht, durch welche die Zahlung von Lösegeld nach Ransomware-Attacken untersagt werden soll: Hierzu zählen neben dem Bundesstaat New York (Senate Bill S6806A[705] und Senate Bill S6154[706]) unter anderem Florida (House Bill 7055),[707] North Carolina (House Bill 813),[708] Pennsylvania (Senate Bill 726)[709] und Texas (House Bill 3892).[710] Während die Gesetzgebungsverfahren in Texas ebenso wie in North Carolina und Pennsylvania jeweils zunächst auf Ausschussebene gescheitert sind,[711] laufen die Gesetzgebungsvorhaben in New York sowie mittlerweile auch in Pennsylvania[712] fort. Zum Abschluss gekommen sind nur die Gesetzgebungsverfahren in North Carolina[713] und Florida,[714] wo jeweils ein ausschließlich an Hoheitsträger und öffentliche Einrichtungen adressiertes Verbot von Lösegeldzahlungen im Kontext von Ransomware-Attacken eingeführt worden ist.[715]

Dabei umfasst der in New York eingebrachte Entwurf – anders als in den anderen Bundesstaaten – nicht nur ein an öffentliche Stellen

---

705 NY Senate Bill S6806A An act to amend the state technology law, in relation to the payment of ransom in the event of a cyber incident or a cyber ransom or ransomware attack v. 18.5.2021.

706 NY Senate Bill S6154 An act to amend the executive law and the state finance law, in relation to cyber security enhancement funding; and to restrict the use of taxpayer moneys in paying ransoms v. 12.4.2021.

707 House Bill 7055 An act relating to cybersecurity v. 3.2.2022.

708 House Bill 813 Prohibit State Agencies Payment of Ransomware v. 13.5.2021.

709 Senate Bill 726 v. 28.5.2021 i.d.F. v. 18.1.2022, Printer's No, 1326.

710 Texas House Bill 3892 No. 3892 Relating to matters concerning governmental entities, including cybersecurity, governmental efficiencies, information resources, and emergency planning v. 11.3.2021.

711 Vgl. https://legiscan.com/TX/bill/HB3892/2021 sowie https://legiscan.com/NC/bill/H813/2021 und https://legiscan.com/PA/bill/SB726/2021 (jeweils zuletzt abgerufen am 1.5.2025).

712 Vgl. zur Disskussion in der zweiten Kammer nur Commenwealth of Pennsylvania, Legislative Journal Senate No. 3 v. 19.1.2022, S. 35.

713 Das Gesetz ist als Teil des Budgetgesetzes 2021-2022 (*budget appropriations*) des Bundesstaates (Ch. SL 2021-180) v. 18.11.2021 verabschiedet worden, siehe https://www.ncleg.gov/EnactedLegislation/SessionLaws/HTML/2021-2022/SL2021-180.html (zuletzt abgerufen am 1.5.2025).

714 House Bill 7055 An act relating to cybersecurity… prohibits certain entities from paying or otherwise complying with ransom demand ... v. 1.7.2022.

715 Vgl. zu Florida https://www.myfloridahouse.gov/Sections/Bills/billsdetail.aspx?BillId=76628 und zu North Carolina https://www.ncleg.gov/EnactedLegislation/SessionLaws/HTML/2021-2022/SL2021-180.html. Siehe zum Ganzen https://therecord.media/an-inside-look-into-states-efforts-to-ban-govt-ransomware-payments (jeweils zuletzt abgerufen am 1.5.2025).

und Hoheitsträger gerichtetes Verbot, Lösegelder nach Ransomware-Attacken aus Steuergeldern zu begleichen, sondern verbietet auch Lösegeldzahlungen durch private Akteure. Die geplante Regelung in sec. 1 NY Senate Bill S6806A zur Ergänzung des State Technology Law um sec. 401(2) lautet auszugsweise wie folgt:

> *„No … business entity or health care entity within the state shall pay or have another entity pay on their behalf, ransom in the event of a cyber incident or a cyber ransom or ransomware attack".*

Sollte der Gesetzesentwurf in dieser Form verabschiedet werden, bestünde im Bundesstaat New York mithin ein umfassendes Verbot von Lösegeldzahlungen für alle privaten Unternehmen und andere „business entities". Dem Entwurf ist allerdings nicht eindeutig zu entnehmen, ob für das Eingreifen des Verbotstatbestands bereits ausreicht, dass ein privater Akteur (auch) im Bundesstaat New York einen Sitz oder eine Niederlassung unterhält („business entity … within the state"), oder ob weitere Faktoren hinzutreten müssen und sich die Lösegeldzahlung z.B. auf innerhalb der Bundesstaatsgrenzen lokalisierte verschlüsselte IT-Systeme des Unternehmens bezieht oder zumindest die Auszahlungsentscheidung im Bundesstaat selbst veranlasst werden muss. Für die zuerst genannte, weite Lesart des Verbots mag sprechen, dass der Gesetzesentwurf eine „business entity" wie folgt definiert: „…any legal entity conducting business in the State of New York". Im Zweifelsfall dürfte der räumlich-territoriale Anwendungsbereich des Verbots anhand des Kollisionsrechts des Bundesstaates New York zu bestimmen sein.

Die geplante Regelung in sec. 1 NY Senate Bill S6806A schweigt darüber hinaus zur Frage der Versicherbarkeit von Lösegeldzahlungen nach Ransomware-Angriffen. Beim derzeitigen Stand können Versicherer in den USA grundsätzlich Deckungsschutz für Lösegeldzahlungen bieten, wie eine jüngere Entscheidung des Federal Court in Oregon im Verfahren *Yoshida Foods International, LLC v.*

Federal Insurance Company illustriert.[716] Tritt das für New York geplante umfassende Verbot von Lösegeldzahlungen durch private Unternehmen in Kraft, mag sich die Bewertung indes zumindest in diesem Bundesstaat ändern.[717]

2. Eingriffsnormen des Erfüllungsortes

Gemäß Art. 9 Abs. 1 Rom I-VO ist eine Eingriffsnorm „eine zwingende Vorschrift, deren Einhaltung von einem Staat als so entscheidend für die Wahrung seines öffentlichen Interesses, insbesondere seiner politischen, sozialen oder wirtschaftlichen Organisation, angesehen wird, dass sie ungeachtet des nach Maßgabe dieser Verordnung auf den Vertrag anzuwendenden Rechts auf alle Sachverhalte anzuwenden ist, die in ihren Anwendungsbereich fallen." Cyber-Versicherungsverträge, einschließlich von Master-Policen in internationalen Versicherungsprogrammen (IVP) für deutsche Unternehmen, treffen üblicherweise eine Rechtswahl zugunsten deutschen Rechts und flankieren dies durch die Wahl eines Gerichtsstandes in Deutschland.

---

716 *Yoshida Foods International, LLC v. Federal Insurance Company*, No. 3:2021cv01455 – Document 31 (D. Or. 6.12.2022). The policyholder suffered a ransomware attack demanding payment of $107,074.20 in cryptocurrency to recover encrypted data. Because Yoshida lacked access to cryptocurrency, one of its executives paid the ransom from his personal cryptocurrency account and was later reimbursed by the company. The policy did not explicitly provide coverage for extortion, ransomware, or encryption, but did cover a „direct loss" caused by „Computer Fraud," which included unlawful taking of money resulting from unauthorized entry into a computer system. Federal refused to cover the ransomware payment, arguing among other things that the payment was not a „direct loss" insured by the computer fraud coverage grant because the company's reimbursement to its executive was an indirect or consequential loss, and because the transfer of funds represented the company's conscious decision instead of direct theft by the criminals. Over Federal's objections, the district court found the policy language was broad enough to encompass the ransomware attack, obligating the insurer to indemnify Yoshida for its loss. The policyholder prevailed – but only after litigating the scope of the insurance policy that it purchased.

717 Auf Grundlage der allgemeinen *public policy* des Bundesstaates New York, keine verbotswidrigen und sanktionsbewehrten Zahlungen zu versicheren, könnte womöglich auch ein Versicherungsverbot hinsichtlich von Lösegeldern begründetet werden, die der Versicherte unter Zuwiderhandlung gegen sec. 1 NY Senate Bill S6806A gezahlt hat, vgl. – jeweils mit Blick auf die Versicherbarkeit von „punitive damages and damages for conduct intended to cause harm" – z.B. *Zurich Insurance Co. v. Shearson Lehman Hutton, Inc.*, (N.Y. Court of Appeals 1994, 84 N.Y.2d 309); *Public Serv. Mut. Ins. Co. v. Goldfarb*, (N.Y. Court of Appeals 1981, 53 N.Y.2d 392). Vgl. auch *Navigators Insurance Co. v. Sterling Infosystems, Inc.*, (N.Y. Supreme Court, 2015 NY Slip Op 31402(U)); *Navigators Insurance Co. v. Sterling Infosystems, Inc.* (Appellate Division 2016, NY Slip Op 08941 [145 AD3d 630]).

Im Fall eines Deckungsstreits wird das international zuständige deutsche Gericht entsprechend die Eingriffsnormen des deutschen Rechts als *lex fori* anwenden, wobei diese Normen richtigerweise nicht als Teil des Vertragsstatuts, sondern erst im Wege einer von den allgemeinen international-schuldvertraglichen Verweisungen unabhängigen Sonderanknüpfung über Art. 9 Abs. 2 Rom I-VO zur Anwendung gelangen.[718] Eingriffsnormen der *lex fori*, die eine Lösegeldzahlung oder eine Lösegelddeckung explizit verbieten, gibt es zumindest aus deutscher Sicht nicht.[719]

Darüber hinaus kann das Gericht jedoch gemäß Art. 9 Abs. 3 Rom I-VO auch den Eingriffsnormen des Staates „Wirkung verleihen", in dem der Erfüllungsort der durch den (Versicherungs)Vertrag begründeten Verpflichtungen liegt, soweit diese Eingriffsnormen „die Erfüllung des Vertrags unrechtmäßig werden lassen".[720] Dem Gericht gibt Art. 9 Abs. 3 Rom I-VO hier einen weiten Ermessensspielraum: Berücksichtigt werden sollen insbesondere Art und Zweck der Eingriffsnormen sowie die Folgen ihrer (Nicht)Anwendung.[721] Beispielsweise bei einem IVP unter einer deutschen Master-Police für ein deutsches Unternehmen und dessen Auslandstöchter sind Konstellationen denkbar, in denen das deutsche Recht als Versicherungsvertragsstatut keine Verbote von Lösegeldzahlungen und Lösegelddeckungen vorsieht, wohl aber das Recht am Sitz einer versicherten Auslandstochter.[722] Sollte nun eine Lösegeldzahlung nach einer Ransomware-Attacke dieser Auslandstochter ersetzt werden, stünde das Recht des Erfüllungsortes der Versicherungsleistung womöglich entgegen. Das im Deckungsprozess international zuständige deutsche Gericht müsste sich – trotz der Rechtswahl

---

718 Art. 9 Abs. 2 Rom I-VO lautet: „Diese Verordnung berührt nicht die Anwendung der Eingriffsnormen des Rechts des angerufenen Gerichts". Zur Frage der Anwendung von Eingriffsnormen über das Vertragsstatut oder im Wege einer Sonderanknüpfung statt aller BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 9 Rom I-VO Rn. 87 ff.

719 Vgl. erneut oben I.

720 Auch nach Auffassung des EuGH 18.10.2016 – Rs. C-135/15 (*Nikiforidis*) ECLI:EU:C:2016:774 Rn. 40 ff. und 55 soll Art. 9 Abs. 3 Rom I-VO damit die Anwendung der drittstaatlichen Norm ermöglichen. Wie hier z.B. BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 9 Rom I-VO Rn. 148 ff. m.w.N. A.A. und enger indes Grüneberg/*Thorn*, 84. Aufl. 2025, Rom I-VO Rn. 14.

721 BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 9 Rom I-VO Rn. 130 ff.

722 Vgl. etwa den Gesetzentwurf im Bundesstaat New York: NY Senate Bill S6806A An act to amend the state technology law, in relation to the payment of ransom in the event of a cyber incident or a cyber ransom or ransomware attack v. 18.5.2021. Siehe dazu oben 1 c).

zugunsten deutschen Rechts – sodann mit der Frage auseinandersetzen, ob es sich bei dem drittstaatlichen Verbot um eine Eingriffsnorm handelt, der über Art. 9 Abs. 3 Rom I-VO mit der Folge „Wirkung verliehen“ werden kann, dass die Vertragserfüllung insoweit ausgeschlossen ist.[723] Gerade bei IVP können damit zahlreiche Rechtsordnungen relevant werden – und dies selbst dann, wenn sowohl die das IVP koordinierende „Besondere Vereinbarung“ als auch vor allem die Master-Police nebst aller Deckungsbausteine (z.B. DIL, DIC, Step-Down)[724] kraft Rechtswahl deutschem Recht unterstehen: Denn nach Auffassung des OLG Frankfurt a.M. soll grundsätzlich auf jeden „tatsächlichen Erfüllungsort“ abzustellen sein,, „an dem eine faktische Leistungsbewegung stattgefunden hat oder vorgesehen ist“.[725] Dafür streitet in der Tat, dass der Staat des (faktischen) Erfüllungsorts es in der Hand hat, die Vertragserfüllung insoweit zu vereiteln.[726] Werden z.B. bei Ransomware-Attacken separate Lösegeldforderungen an diverse versicherte Auslandstöchter gestellt und zahlen diese Versicherten jeweils, so wären – freilich abhängig von der konkreten Ausgestaltung der Lösegelddeckung unter dem IVP – grundsätzlich Versicherungsleistungen am jeweiligen Sitz der betroffenen Auslandstochter und damit an mehreren Erfüllungsorten zu erbringen.[727] Das gilt gerade dann, wenn ergänzend zu Lokal-Policen eine DIL-, DIC- oder Step-Down-Klausel unter der deutschem Recht unterliegenden Master-Police greift und die Versicherungsleistung an die jeweilige versicherte Auslands-

---

723 Vgl. zur Wirkung drittstaatlicher Verbotsgesetzte (hier: betreffend die Luftbeförderung israelischer Passagiere durch eine kuweitische Fluggesellschaft) nur OLG Frankfurt NJW 2018, 3591 Rn. 31 ff.; OLG München BeckRS 2020, 15428 Rn. 31 ff. (jeweils auch im Kontext der Unmöglichkeit nach § 275 Abs. 1 BGB). Vgl. im Gefolge der Entscheidung des EuGH 18.10.2016 – Rs. C-135/15 (*Nikiforidis*) ECLI:EU:C:2016:774 Rn. 40 ff. zur Frage der Berücksichtigung griechischer Gesetze zur zwingenden Senkung des Arbeitsentgelts von Lehrkräften, deren Arbeitsverträge i.Ü. deutschem Arbeitsrecht unterliegen BAG IPRax 2018, 86 ff.; LAG Hamm 3.4.2014 – 17 Sa 999/13, BeckRS 2014, 68510.

724 Vgl. statt vieler *Armbrüster*, Privatversicherungsrecht, 2. Aufl. 2019, S. 688 ff.; *Lange*, D&O-Versicherung, 2. Aufl 2022, § 23 Rn. 29 ff.

725 Vgl. OLG Frankfurt NJW 2018, 3591 Rn. 31 ff. Siehe auch BeckOGK BGB/*Maultzsch,* 1.3.2025, Art. 9 Rom I-VO Rn. 107 ff. und insbesondere Rn. 114 ff.

726 OLG Frankfurt NJW 2018, 3591 Rn. 33 f. Siehe auch Staudinger/*Magnus*, 2021, Art. 9 Rom I-VO Rn. 108 ff.

727 Das gilt sowohl, wenn im Dienstleistungsverkehr Deckung innerhalb der EU bzw. des EWR grenzüberschreitend angeboten werden kann, als auch in Konstellationen, in denen koordinierte lokale Policen verwendet werden.

tochter ausgekehrt wird.[728] Unter den Voraussetzungen des Art. 9 Abs. 3 Rom I-VO sind dann die Eingriffsnormen aller – vertraglich vereinbarten oder auch rein tatsächlichen – Erfüllungsorte potentiell berücksichtigungsfähig.[729] Über Art. 9 Abs. 3 Rom I-VO kann das Gericht den Eingriffsnormen des jeweiligen Erfüllungsorts allerdings jeweils nur Wirkung verleihen, soweit hierdurch die Erfüllung des Vertrags unrechtmäßig wird. Soweit sich Eingriffsnormen nicht gegen die Erfüllung, sondern gegen andere Aspekte der vertraglichen Vereinbarung richten, ist Art. 9 Abs. 3 Rom I-VO unanwendbar.[730] Anders als bei der materiell-rechtlichen Berücksichtigung drittstaatlicher Eingriffsnormen über § 138 Abs. 1 BGB[731] setzt die Anwendung von Art. 9 Abs. 3 Rom I-VO nicht zwingend voraus, dass hinsichtlich der mit der Norm verfolgten Zwecke ein vollständiger Wertungsgleichlauf im Erlassstaat einerseits und im Forumstaat andererseits besteht.[732]

Allgemein mag die Berücksichtigung von statut- und forumsfremden Eingriffsnormen über Art. 9 Abs. 3 Rom I-VO näherliegen, wenn der Schuldner der Leistung im Fall einer verbotswidrigen Erfüllung im Erlassstaat zugleich einer strafrechtlichen Verantwortung ausgesetzt ist: In einer solchen Konstellation steht das Erfüllungsinteresse des Gläubigers nämlich dem – *prima facie* – bedeutenderen Interesse des Schuldners gegenüber, von strafrechtlichen Sanktionen

---

728 Obschon man im Anschluss an OLG Frankfurt NJW 2018, 3591 Rn. 31 ff. auch bei FINC-Klauseln kritisch hinterfragen mag, wo für die Zwecke des Art. 9 Abs. 3 Rom I-VO „eine faktische Leistungsbewegung stattgefunden hat oder vorgesehen ist“ und damit der „tatsächliche“ Erfüllungsort liegt, wird hier die geschuldete Versicherungsleistung rechtlich und tatsächlich zunächst allein an die Versicherungsnehmerin (regelmäßig das inländische Mutterunternehmen) erbracht. Für Art. 9 Abs. 3 Rom I-VO dürfte es sodann irrelevant sein, wenn die Versicherungsnehmerin ebendiese Valuta – z.B. zur Gewährleistung ausreichender Liquidität – sodann direkt an ihre Auslandstochter weiterleitet.

729 Vgl. erneut nur OLG Frankfurt NJW 2018, 3591 Rn. 33 f. und statt vieler Staudinger/*Magnus*, 2021, Art. 9 Rom I-VO Rn. 108 ff. Für sich genommen dürfte es indes kaum ausreichen, dass eine Zahlung in US-Dollar abgewickelt wird, obschon die Zahlung gegen eine US-amerikanische Sanktionsbestimmung verstößt, so aber wohl *Tehrani*, VersR 2016, 85, 93.

730 Zudem ist die bei „internen“ Sachverhalten geltenden Vermutung der Gesamtnichtigkeit nach §§ 134, 139 BGB im Fall des Art. 9 Abs. 3 Rom I-VO stets zu hinterfragen, vgl. statt vieler MünchKommBGB/*Martiny*, 9. Aufl. 2025, Art. 9 Rom I-VO Rn. 127 ff.; *Sonnentag*, VersR 2024, 201, 206 f.

731 Vgl. dazu sogleich unter 3.

732 Siehe nur *Max Planck Institute*, RabelsZ 68 (2004), 1, 76: Erforderlich und zugleich ausreichend soll vielmehr sein, dass der Forumstaat die Zielrichtung und das Schutzinteresse der Eingriffsnorm ebenfalls prinzipiell anerkennt, ohne die Wertung vollauf zu teilen oder gar korrespondierende eigene Normen vorzusehen.

verschont zu bleiben. Das Forum mag der strafbewehrten drittstaatlichen Eingriffsnorm deshalb selbst dann Wirkung verleihen, wenn die mit dieser Norm verfolgten Zwecke – wie etwa ein Embargo oder eine Sanktion – im Forumstaat nicht geteilt oder gar missbilligt werden.[733] Bei Lösegeldzahlungen nach Ransomware-Attacken dürften allerdings häufig Verbote der Terrorismusfinanzierung sowie Sanktions- und Embargo-Bestimmungen als drittstaatliche Eingriffsnormen relevant werden: Hier besteht vielfach ein weitgehender Gleichlauf der gesetzgeberischen Motive im deutschen Forumstaat einerseits sowie in Drittstaaten – wie z.B. den USA[734] oder dem UK[735] – andererseits. Allerdings fallen gerade die Verbote des US *Office of Foreign Assets Control (OFAC)* in ihrer sachlichen und territorialen Reichweite teils deutlich umfassender aus.[736] So existieren nicht zuletzt spezifische „*Cyber-Related Sanctions Regulations*" in 31 C.F.R. Part 578,[737] die extraterritorial wirken und bestimmte Transaktionen vollständig untersagen.[738] Hinzu kommen allgemeine Verbote aus dem „International Emergency Economic Powers Act (IEEPA)" und dem „Trading with the Enemy Act (TWEA)",[739] die nicht nur die Vornahme, sondern potentiell schon die Beihilfe zu solchen sanktions- oder embargowidrigen Transaktionen im Fall von Lösegeldzahlungen nach Ransomware-Angriffen sanktionieren können.[740] Dabei sind solche Verbots- und Sanktionstatbestände

---

733 Dafür plädiert mit Blick auf die Grundrechte des Schuldners BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 9 Rom I-VO Rn. 135.1. Deutlich zu streng ist demgegenüber *Tehrani*, VersR 2016, 85, 94, der stets „völkerrechtlich tradierte Rechtfertigungsgründe" für die Anwendung ausländischer Eingriffsnormen des Erfüllungsortes fordert.

734 Vgl. etwa das exterritorial wirkende Verbot in 18 U.S. Code § 2339B mit Blick auf terroristische Vereinigungen.

735 Vgl. zu der zwischen 2000 und 2019 verabschiedeten Reihe von Anti-Terrorismus-Gesetzen und insbesondere zum *Terrorism Act 2000* (2000 c. 11) sowie zu den Rechtsakten zur Geldwäschebekämpfung, wie vor allem den *Proceeds of Crime Act 2002* (2002 c. 29) näher *Eggen*, Die Cyberversicherung, 2023, S. 130 ff.

736 Vgl. nur OFAC's Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments v. 21.9.2021, abrufbar unter: https://ofac.treasury.gov/media/912981/download?inline (zuletzt abgerufen am 1.5.2025). Vgl. etwa schweizerisches Bundesgericht 17.8.2023 – 4A_206/2023.

737 Basierend auf 87 FR 54376 v. 6.9.2022. Siehe auch https://ofac.treasury.gov/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities (zuletzt abgerufen am 1.5.2025).

738 Vgl. zu „prohibited transactions" nur 31 C.F.R. Part 578 § 578.201.

739 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06.

740 Vgl. zum weit gefassten Tatbestand des „facilitating" nur OFAC's Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments v. 21.9.2021, S. 3 f.

nicht zuletzt im Lichte der durch das OFAC veröffentlichten Verlautbarungen und „FAQs“ auszulegen und anzuwenden.[741] Diese Verlautbarungen des OFAC dürften entsprechend auch bei der Bewertung der relevanten Interessen i.R.d. Art. 9 Abs. 3 Rom I-VO eine zentrale Rolle spielen.

3. Materiell-rechtliche Berücksichtigung ausländischer Verbotsnormen über § 138 Abs. 1 BGB

Wo die Anwendung ausländischer Verbotsnormen über Art. 9 Rom I-VO ausscheidet – etwa, weil der Erfüllungsort nicht im Erlassstaat der Sanktions- oder Embargobestimmung liegt –, können solche Verbotsgesetze womöglich über die Generalklausel des § 138 Abs. 1 BGB materiell-rechtlich durch das international zuständige deutsche Gericht berücksichtigt werden. Das mag auch bei Cyber-Versicherungsverträgen relevant werden, die kraft Rechtswahl deutschem Recht unterstehen. Zwar wird zuweilen im Schrifttum die Ansicht vertreten, dass die deutsche Rechtsordnung i.R.d. § 138 Abs. 1 BGB Lösegeldzahlungen infolge von Ransomware-Attacken selbst dann hinzunehmen habe, wenn durch diese Zahlungen im Ausland gegen Verbotsgesetze verstoßen wird.[742] Während § 134 BGB grundsätzlich nur Verstöße gegen deutsche Gesetze sanktioniert, gestattet § 138 Abs. 1 BGB jedoch die Einbeziehung ausländischer Verbotstatbestände als Leitlinien für die Konkretisierung der Sittenwidrigkeit.[743] Im Ausgangspunkt trifft es durchaus zu, dass inländische Standards maßgeblich für die Konkretisierung der „guten

741 Vgl. nur *Mamancochet Mining Ltd v. Aegis Managing Agency Ltd & Ors* [2018] EWHC 2643 (Comm): Die Sanktionsbestimmungen seien vor dem Hintergrund der durch das US Office of Foreign Assets Control veröffentlichten FAQs auszulegen, weshalb das Gericht hier schon keinen Verstoß gegen das Sanktionsregime sah und sich damit auch nicht mit einer Berücksichtigung der Verbotsnorm über Art. 9 Abs. 3 Rom I-VO in Bezug auf Versicherer und Versicherungsleistungen auseinandersetzen musste. In Rede stand dabei das gegen Iran gerichtete Sanktionenregime in US Iranian Transactions & Sanctions Regulations, 31 C.F.R. Part 560 § 560.204 der Sanktionsregelung untersagt die Erbringung aller Dienstleistungen, einschließlich von Versicherungsleistungen, wobei der persönliche Anwendungsbereich „US owned or controlled foreign entities“ umfasst.

742 Vgl. i.d.S. etwa *Sieg/Schilbach*, VersR 2023, 745, 746 ff.

743 BGH NJW-RR 2021, 1244 Rn. 30 f.

Sitten“ sind.[744] Allerdings hält der BGH eine Öffnung für Wertungen der unionalen[745] und auch ausländischer Rechtsordnungen stets für möglich.[746] Dabei bilden diese aber nicht den alleinigen Bewertungsmaßstab, sondern der BGH fordert zusätzlich, dass entweder „die verletzten ausländischen Bestimmungen mittelbar auch deutsche Interessen schützen“ (**dazu unter a**) oder aber „ihre Umgehung allgemein zu achtenden Interessen aller Völker widerspricht“ (**dazu unter b**).[747] Ist diese weitere Voraussetzung erfüllt, kann die Norm materiell-rechtlich im Rahmen des § 138 Abs. 1 BGB bei der Konturierung der innerstaatlichen „guten Sitten“ berücksichtigt werden. Diese materiell-rechtliche Berücksichtigung i.R.v. Generalklauseln des mitgliedsstaatlichen Privatrechts hat auch der EuGH in seiner *Nikiforidis*-Entscheidung grundsätzlich gebilligt und damit zugleich entschieden, dass Art. 9 Rom I-VO insoweit keine Sperrwirkung entfaltet.[748]

a) Reflexhafter Schutz (auch) deutscher Interessen

Einen – zumindest reflexhaften – Schutz auch deutscher Interessen hat der BGH etwa mit Blick auf bestimmte Embargo-Bestimmungen der USA bejaht.[749] Allerdings wird auch hier zum einen stets ein weitgehender Interessengleichlauf zu fordern sein.[750] Zum anderen

---

744 Statt vieler MünchKommBGB/*Armbrüster*, 10. Aufl. 2025, § 138 BGB Rn. 28 ff.

745 BGH NJW 1998, 2208, 2212 f.

746 Vgl. nur BGH NJW 1961, 822 f.; BGH NJW 1972, 1575, 1576 f.; BGH NJW 1977, 2356, 2357 f.; BGH NJW 1985, 2405, 2406; BGH NJW-RR 2021, 1244 Rn. 31.

747 BGH NJW-RR 2021, 1244 Rn. 31 m.w.N. aus der st. Rspr.

748 EuGH 18.10.2016 – Rs. C-135/15 (*Nikiforidis*) ECLI:EU:C:2016:774 Rn. 51 ff. Vgl. auch OLG Frankfurt a. M. NJW 2018, 3591 Rn. 31 ff.; OLG München BeckRS 2020, 15428 Rn. 31 ff. Wie hier z.B. BeckOGK BGB/*Maultzsch*, 1.3.2025, Art. 9 Rom I-VO Rn. 148 ff. m.W.n. Restriktiv dennoch Grüneberg/*Thorn*, 83. Aufl. 2024, Art. 9 Rom I-VO Rn. 14; *Staudinger* in: Ferrari/Kieninger/Mankowski u.a., Internationales Vertragsrecht, 3. Aufl. 2018, Art. 9 Rom I-VO Rn. 42 f., dort jeweils m.w.N. zur Gegenansicht. Deutlich zu restriktiv ist *Tehrani*, VersR 2016, 85, 94, soweit er per se verneint, dass „ausländische Eingriffsnormen außerhalb des Art. 9 Rom I-VO über zivilrechtliche Generalklauseln in die deutsche Rechtsordnung einbrechen können“ und dies „den Wortlaut des Art. 9 Rom I-VO und dem „Vereinheitlichungszweck“ der Rom I-VO entnehmen will.

749 BGH NJW 1961, 822, 823: die gegen Staaten des „Ostblocks“ gerichteten Embargo-Bestimmungen lägen „nicht nur im amerikanischen Interesse, sondern im Interesse des gesamten freiheitlichen Westens und damit auch im Interesse der Bundesrepublik Deutschland.“ Vgl. auch BGH NJW 1962, 1436, 1437. Vgl. zum Südafrika-Embargo nach thailändischem Recht im Kontext des § 826 BGB ferner BGH NJW 1991, 634, 635 f.; BGH NJW 1993, 194, 195.

750 Vgl. LG Hamburg VersR 2015, 1024 f.; OLG Frankfurt a.M. 9.5.2011 – 23 U 30/10, BeckRS 2011, 16032; *Looschelders*, VersR 2015, 1025, 1026 f.; *Wandt*, VersR 2013, 257, 265 f.

darf das betreffende ausländische Verbotsgesetz nicht mit inländischen oder unionalen Normen in Konflikt stehen. So liegt der Fall indes, wenn das Embargo oder eine Sanktionsbestimmung eines Drittstaates mit der sogenannten EU-Blocking-Verordnung[751] unvereinbar ist. Obschon die Verordnung gerade in der EU ansässige Wirtschaftsteilnehmer vor extraterritorial wirkenden drittstaatlichen Sanktionsregimes schützen soll,[752] birgt die Verordnung für grenzüberschreitend tätige Akteure – z.B. solche mit Konzerngesellschaften oder Niederlassungen (auch) im jeweiligen Erlassstaat – widersprüchliche Verhaltensanforderungen und damit Normkonfliktpotential.[753] Im Anwendungsbereich der Blocking-Verordnung kann ein deutsches Gericht sogar gehalten sein, ein nach ausländischen Sanktionsbestimmungen nichtiges Schuldverhältnis aufrechtzuerhalten und dem Vertragspartner des Sanktionierten etwaige Gestaltungsrechte zu verwehren.[754]

b) Schutz „allgemein zu achtender Interessen aller Völker“

Der Verstoß gegen eine ausländische Verbotsnorm kann auch bei einem deutschen Recht unterliegenden Cyber-Versicherungsvertragsstatut über § 138 Abs. 1 BGB zur Nichtigkeit der Vereinbarung führen, wenn die verletzte ausländische Norm „allgemein zu achtende Interessen aller Völker“ schützt und ihre Nichtberücksichtigung damit zugleich einen Verstoß (auch) gegen die im Inland maßgeblichen „guten Sitten“ bedeuten würde.[755] In der Diskussion um Verbote von Lösegeldzahlungen und Verbote von Lösegeld-Versicherungen für Ransomware-Attacken wird insbesondere die anreizmindernde Steuerungswirkung solcher Verbote betont: Cyber-

---

751 Verordnung (EU) Nr. 2271/96 des Rates vom 22.11.1996 zum Schutz vor den Auswirkungen der extraterritorialen Anwendung von einem Drittland erlassener Rechtsakte sowie von darauf beruhenden oder sich daraus ergebenden Maßnahmen, ABl. 2016 L 309/1.

752 Dazu statt vieler *Heinisch* in: Bürkle, Compliance in Versicherungsunternehmen, 3. Aufl. 2020, § 16 Rn. 47 ff.

753 Vgl. mit Blick auf EuGH 21.12.2021 – Rs. C-124/20 (*Bank Melli Iran/Telekom Deutschland*) ECLI:EU:C:2021:1035 statt vieler *Bälz*, EuZW 2020, 416 ff.; *Seibt/Denninger,* ZIP 2023, 81 ff.

754 Vgl. zur wegen Verstoßes gegen Art. 5 Abs. 1 EU-Blocking-Verordnung nach § 134 BGB nichtigen Kündigung eines Telekommunikationsvertrag nun OLG Hamburg IWRZ 2023, 87 Rn. 47 ff. (m. Anm. *Bälz*, 89 ff.) im Anschluss an EuGH 21.12.2021 – Rs. C-124/20 (*Bank Melli Iran/ Telekom Deutschland*) ECLI:EU:C:2021:1035.

755 Vgl. zuletzt BGH NJW-RR 2021, 1244 Rn. 31.

Kriminelle hätten zum einen kein finanzielles Motiv mehr für ihre Angriffe, weil sie angesichts des Verbotes von Lösegeldzahlungen keinerlei Geldmittel mehr erhielten. Zum anderen würde durch das Verbot von Lösegelddeckungen in Cyber-Versicherungsverträgen die Zahlungsbereitschaft der Ransomware-Opfer sinken, wohingegen sich Angreifer beim derzeitigen Stand gezielt Opfer mit Cyber-Versicherungen aussuchen und dann auf die Solvenz des den wirtschaftlichen Schaden tragenden Versicherers vertrauen könnten.

Die Verfechter solcher Verbote von Lösegeldzahlungen und/oder von Lösegelddeckungen im Cyber-Bereich konnten in vielen Rechtsordnungen bislang nicht mit ihren Argumenten durchdringen.[756] Sollten solche Verbote aber beispielsweise im für international tätige Unternehmen häufig relevanten US-Bundesstaat New York in Gesetzesform gegossen werden,[757] könnten auch deutsche Gerichte im Fall eines Deckungsstreits – z.B. im Rahmen von Internationalen Versicherungsprogrammen unter einer deutschen Master-Police – bald vor die Frage gestellt werden, ob die Bekämpfung und Prävention von Cyber-Kriminalität durch die Untersagung von Lösegeldzahlungen und -deckungen ein „allgemein zu achtendes Interesse aller Völker“ ist, „dessen Beeinträchtigung kein bürgerlich-rechtlicher Schutz zuteilwerden kann“.[758]

Eine materiell-rechtliche Berücksichtigung solcher ausländischer (Versicherungs)Verbotsnormen über § 138 Abs. 1 BGB setzt allerdings voraus, dass ein anerkennenswertes, auch von der inländischen Rechtsordnung geteiltes Interesse daran besteht, Lösegeldzahlungen ebenso wie auch deren Erstattung durch Cyber-Versicherer generell zu untersagen.[759] Zwar mag es auch aus Sicht der deutschen Rechtsordnung ein sinnvolles und anerkennenswertes Anliegen sein, den „Sumpf“ der Ransomware-Erpresser auszu-

[756] Siehe zur Rechtslage in Frankreich oben I 3 b); siehe zu zahlreichen US-Bundesstaaten oben I 3 c).
[757] Näher hierzu oben I 3 c).
[758] Vgl. erneut nur BGHZ 59, 82, 85 f. sowie zuletzt BGH NJW-RR 2021, 1244 Rn. 31.
[759] Vgl. wiederum BGHZ 59, 82, 85 f.; BGH NJW-RR 2021, 1244 Rn. 31.

trocknen.[760] Beim derzeitigen Stand der Rechtsentwicklung untersagt indes weder die deutsche Rechtsordnung Lösegeldzahlungen oder korrespondierende Versicherungslösungen, noch herrscht überhaupt auf internationaler Ebene Konsens hinsichtlich der Sinnhaftigkeit solcher Verbote. Von einem „allgemein zu achtende(n) Interesse aller Völker“ kann deshalb gegenwärtig kaum Rede sein.[761] Es erscheint damit äußerst unwahrscheinlich, dass ein deutsches Gericht in einem nach deutschem Recht geführten Deckungsstreit ausländische Versicherungsverbote über § 138 Abs. 1 BGB auf materiell-rechtlicher Ebene berücksichtigen würde.

III. Ergebnis

Das deutsche Recht untersagt Lösegeldzahlungen im Gefolge von Ransomware-Attacken nicht *per se*. Solche Ransom-Zahlungen können auf Grundlage eines speziellen Lösegeldbausteins in Cyber-Versicherungsverträgen ebenso wie als Rettungskosten nach § 83 VVG grundsätzlich erstattet werden.[762] Das Bild in ausländischen Rechtsordnungen ist deutlich heterogener: Während manche US-Bundesstaaten auch für private Unternehmen partielle Verbote erwägen,[763] hat sich der französische Gesetzgeber nach einer kontroversen politischen Debatte nun in Art. L. 12-10-1 *Code des assurances* für die ausdrückliche Gestattung von Lösegeld-Zahlungen und damit auch von Ransom-Versicherungen entschieden.[764] Dabei wird diese Gestattung jedoch – sinnvollerweise – unter den Vorbehalt gestellt, dass der Versicherte Anzeigepflichten gegenüber den (Strafverfolgungs)Behörden rechtzeitig erfüllt und hinreichend

[760] Vgl. in diesem Sinne *Bundesregierung* v. 27.7.2022, Drucksache 20/2926, S. 3. Vgl. auch die Petition von rund 100 IT-Sicherheitsexperten aus Bildung und Wirtschaft, die u.a. fordern, „Lösegeldzahlungen bei Ransomware-Angriffen effektiv (zu) unterbinden“ ebenso wie „Versicherungen, die diese Lösegeldzahlungen absichern“ zu verbieten, siehe Offener Brief, Lösegeldzahlungen bei Ransomware-Angriffen: ein geostrategisches Risiko, 2022, abrufbar unter: https://ransomletter.github.io (zuletzt abgerufen am 1.5.2025).

[761] Vgl. erneut nur BGHZ 59, 82, 85 f.

[762] Siehe erneut oben I.

[763] Siehe zum Gesetzgebungsprojekt im US-Bundesstaat New York erneut oben II 1 c).

[764] Siehe erneut oben II 1 b).

kooperiert.[765] Dagegen entpuppt sich die häufig als Paradebeispiel für ein Versicherungsverbot angeführte italienische Regelung in Art. 12(1) *Codice delle Assicurazioni Private* als wenig eindeutig: Ob sich die Norm nur auf Fälle von Personen-Entführungen beschränkt oder ob sie auch Cyber-Erpressungen erfasst und die Versicherung von Lösegeldzahlungen infolge von Ransomware-Angriffen untersagt, erscheint nicht abschließend geklärt. Aus rechtspolitischer Sicht sprechen gegen eine solche Ausdehnung schon die Erfahrungen, die Italien mit dem Verbot von Lösegeldzahlungen bei Kidnapping gemacht hat: Die Familienangehörigen von entführten Personen hörten mit Inkrafttreten des Verbots schlagartig auf, mit den Behörden zusammenzuarbeiten oder Entführungen auch nur zu melden.[766] Es erscheint im Kampf gegen Ransomware-Attacken wenig wünschenswert, nun der effektiven Erkennung und Verfolgung von Straftaten ähnlich abträgliche Mechanismen zu etablieren.

[765] So die – soweit ersichtlich – einhellige Ansicht im französischen Schrifttum, siehe statt vieler *Marly*, Recueil Dalloz 2023, 112; *Perrier*, RSC 2023, 381 f.; *Bigot/Cayol/Noguéro/Pierre*, Recueil Dalloz 2023, 1142 f.

[766] Vgl. nur *Geneva Association*, Ransomware: An insurance market perspective, 2022, S. 23.

F. Cyber-Versicherungen und Cumul-Risiken: Ausschluss von Krieg und Cyber-Operationen, Territorial-Ausschlüsse und „widespread events“

Lange Zeit beherrschte derjenige Staat die Welt, der die sieben Weltmeere befahren und von See aus Macht auf die Landmassen aller Kontinente projizieren konnte: „*Those who rule the waves, rule the world*“.[767] Der Chorus „*Britannia rule the waves*“ in der Hymne „*Rule, Britannia*!“ ist damit zugleich Aufforderung und Bekenntnis zur Vormachtstellung des Empire. Die zu beherrschenden Sphären erweiterten sich allerdings mit dem technologischen Fortschritt rasch über das Meer hinaus: Neben der See galt es nun auch den Luftraum und sodann den zugänglichen Teil des Weltraums zu beherrschen. Wer heutzutage macht-strategische oder gar militärische Erwägungen anstellt, würde angesichts der zunehmenden Digitalisierung und Vernetzung fraglos auch und gerade den Cyber-Space zu den zu dominierenden Sphären rechnen: „*Those* w*ho rule the Cyber-Space, rule the world*“. Doch gibt es neben dem Land-Krieg, dem See-Krieg, dem Luft-Krieg und dem – unter US-Präsident *Ronald Regan* in den 1980er Jahren im Rüstungswettlauf mit der UDSSR ausgerufenen – Weltraum-Krieg[768] nun eine weitere Ausweitung der Kampfzone durch einen veritablen Cyber-Krieg? Jenseits militärischer Überlegungen, wie sie bereits 2013 durch die „*International Group of Experts (The NATO Cooperative Cyber Defence Centre of Excellence)*“ im sog. „*Tallin Manual*“ angestellt worden sind,[769] soll hier der versicherungsrechtliche Zusammenhang betrachtet und die Gestaltung der Ausschlusstatbestände in Cyber-Versicherungen im Vordergrund stehen. Denn Kriege sind – dem Themenzuschnitt dieser Abhandlung entsprechend – zum einen

[767] Ebenso programmatisch wie plastisch beschrieben wird diese Machtprojektion etwa von *Schmitt*, Land und Meer (Erstaufl. 1942, 10. Aufl. 2020).

[768] Vgl. zur sog. Strategic Defense Initiative (SDI) nur *Podvig*, 25 Science & Global Security (2017), 2 ff.

[769] Vgl. dazu schon frühzeitig *Tallin Manual on the International Law Applicable Law to Cyber Warfare*, Cambridge 2013 und sodann *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge 2nd ed. 2017.

grundsätzlich zwischenstaatlich und damit „inter-national“.[770] Zum anderen bergen Kriege stets das Potential extrem hoher Schäden und Schadensfrequenzen und führen damit an die Grenze der Versicherbarkeit – und potentiell weit darüber hinaus.[771] Deshalb werden solche Cumul-Risiken üblicherweise durch einen versicherungsvertraglichen Ausschluss vom Deckungsversprechen ausgenommen.[772] Der breit gestreute kriegerische Einsatz von Schad-Code durch staatliche Akteure mit entsprechenden Ressourcen ist eines der wohl gravierendsten Cumul-Risiken in unserer digitalisierten Welt: Denn im Gegensatz zu einer lokal begrenzten Naturkatastrophe kann eine Cyber-Attacke zeitgleich Schäden an einer fast unbegrenzten Zahl von IT-Systemen weltweit hervorrufen, wenn sie eine weit verbreitete Schwachstelle ausnutzt.[773] Beredtes Zeugnis hiervon legt der – dem Russland-Ukraine-Konflikt zugeschriebene –[774] *NotPetya*-Schad-Code ab der allein im Fall des Pharmaproduzenten *Merck* wohl Schäden im Umfang von rund 1,4 Milliarden Dollar verursacht haben könnte. Hinzu kommt, dass staatliche Akteure in der Lage sind, IoT-und IIoT-Systeme – also etwa vernetzte Steuerungen von Industrieanlagen – zu treffen.[775] Das kann – beispielsweise durch gezielte Überlastung – zu Sachschäden führen: In – jeweils nicht verifizierbaren – Fällen sollen etwa die Steuerungseinheiten eines Stahl-Hochofens[776] sowie jüngst womöglich

---

770 Zur Zwischenstaatlichkeit klassischer Kriege und der Ausweitung der Definition in den Kriegs-Auschlussklauseln sogleich eingehend unter I.

771 Vgl. zur historischen Entwicklung des nunmehr gefestigten Konsenses in der Versicherungswirtschaft, kriegsbedingte Schäden grundsätzlich aus der (Rück)Versicherungsdeckung auszunehmen sogleich ausführlich unter 1.

772 Siehe nur *Schmidt/Gerathewohl*, ZVersWiss 1973, 281; *Hübner*, ZVersWiss 1981, 12 f.; *Makowsky*, VersR 2023, 1, 3 ff. Vgl. zur Definition von Cumul-Risiken nur *v. Fürstenwerth/Weiß/Consten/Präve*, VersicherungsAlphabet, 11. Aufl. 2019, S. 449 f. und 485 f.

773 *Cunningham/Talesh*, 28 Connecticut Insurance Law Journal (2020), 1, 51: „foreign government-sponsored cyberattacks … are the most likely to trigger a cyber insurance ecosystem-threatening catastrophe“.

774 Vgl. zur Anklage der mutmaßlich für die „NotPetya“-Attacke verantwortlichen Mitarbeiter des russischen GRU durch das US-amerikanische Department of Justice nur *US DOJ Justice News*, „Six Russian Officers Charged in Connection with Worldwide Deployment of Malware and Other Disruptive Actions in Cyberspace“ v. 19.10.2020, abrufbar unter: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (zuletzt abgerufen am 1.5.2025).

775 Siehe speziell zu Angriffen auf IIoT-Steuerungsanlagen nur *Lloyd's*, Cyber Risk: The Emerging Cyber Threat to Control Systems (2021), 6.

776 Z.B. *Lloyd's*, Cyber Risk: The Emerging Cyber Threat to Control Systems (2021), 20.

eines Flüssiggas-Terminals[777] betroffen gewesen sein.[778] Entstehen hier Sachschäden, ist der Ausschluss von „Cyber-Krieg" plötzlich nicht mehr nur ein Problem der Cyber-Versicherung, sondern – je nach Ausgestaltung des Deckungskonzepts – beispielsweise auch von industriellen Sach- und Betriebsunterbrechungsversicherungen. Die Gestaltung von Ausschlüssen für Cyber-Kriege ist damit eine besonders drängende und zugleich versicherungsrechtlich herausfordernde Frage. Historisch gesehen war die Reichweite von Kriegsausschlussklauseln bei jeder Fortentwicklung der Konfliktmittel und -modalitäten umstritten.[779] Jüngere Gerichtsentscheidungen legen nahe, dass der „Cyber-Krieg" hierbei keine Ausnahme bilden dürfte.[780] Vor diesem Hintergrund sind zunächst die konventionellen, historisch über längere Zeit gewachsenen und zunächst auch in Cyber-Policen verbreiteten Kriegsausschlussklauseln in den Blick zu nehmen (**dazu unter I**). Sodann bedürften die an LMA5564(a,b)-5567(a,b)[781] angelehnten Ausschlussklauseln für Cyber-Attacken außerhalb „klassischer" kriegerischer Auseinandersetzungen der kritischen Überprüfung – auch und gerade aufgrund der internationalen Dimension von Cyber-Risiken (**dazu unter II**). Besonderes Augenmerk gilt dabei dem neuen Ausschluss in den GDV-Muster-

---

777 Vgl. *Bloomberg*, Hackers Targeted U.S. LNG Producers in Run-Up to Ukraine War, abrufbar unter: https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine (zuletzt abgerufen am 1.5.2025).

778 *Lloyd's*, Shifting Powers: Physical Cyber Risk in a Changing Geopolitical Landscape (2022), 4 ff.

779 Vgl. zum US-Bürgerkrieg etwa *The Brig Army Warwick (The Prize Cases)*, 67 U.S. (2 Black) 635 (1863); *Welts v. Connecticut Mutual Life Insurance Co.*, 48 N.Y. 34 (1871). Vgl. zum ersten Weltkrieg nur *Britain S.S. Co. v. The King* [1919] 1 K.B. 575; *Queen Ins. Co. v. Globe & Rutgers Fire Ins. Co.*, 282 F. 976 (2d Cir. 1922); *Vanderbilt v. Travelers' Ins. Co.*, 184 N.Y.S. 54, 56 (Sup. Ct. 1920), aff'd, 194 N.Y.S. 986 (App. Div. 1922), aff'd, 235 N.Y. 514 (1923). Vgl. Zu Pearl Harbour nur *Rosenau v. Idaho Mut. Benefit Ass'n*, 145 P.2d 227 (Idaho 1944). Vgl. zu PLO-Attacken *Pan Amer. World Airways. v. Aetna*, 505 F.2d 989 (2d Cir. 1974).

780 Vgl. nur *Merck & Co., Inc. v. Ace Am. Ins. Co.*, No. UNN-L-002682-18 (N.J. Super. Ct. Law Div. 6.12.2021); *Merck & Co., Inc. v. Ace Am. Ins. Co.*, No. A-1879-21 / A-1882-21 (N.J. Super. Ct. Appelate Div. 1.5.2023). Dieser Deckungsstreit hat sich nunmehr durch einen Vergleich der Parteien vom 3.1.2024 erledigt, vgl. zu *Merck Co., Inc. v. ACE Am. Ins. Co., N.J.*, No. A-62/63-22, nur *Ebert*, Merck $1.4 Billion Cyberhack Settlement Ends 'Warlike' Act Claim, Bloomberg Law v. 4.1.2024, abrufbar unter: https://news.bloomberglaw.com/litigation/merck-1-4-billion-cyberhack-settlement-ends-warlike-act-claim (zuletzt abgerufen am 1.5.2025). Durch Vergleich beigelegt worden ist auch der erste in diesem Kontext geführte Rechtsstreit *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co.*, No. 2018-L-011008 (Ill. Cir. Ct.), vgl. dazu nur *Adriano*, Zurich, Mondelez settle longstanding lawsuit over $100 million claim, abrufbar unter: https://www.insurancebusinessmag.com/us/news/cyber/zurich-mondelez-settle-longstanding-lawsuit-over-100-million-claim-426741.aspx (zuletzt abgerufen am 1.5.2025).

781 LMA 5564(a,b) bis LMA 5567(a,b) v. 18.1.2023 (War and Cyber Operation Exclusion Clauses).

bedingungen in Ziff. A1-17-2 AVB-Cyber: Hier drängt sich die Frage nach der Vereinbarkeit dieser Klausel mit den Anforderungen der §§ 305 ff. BGB auf (**hierzu unter III**).

I. Cyber-Krieg und konventionelle Kriegsausschlussklauseln: History (not) repeating?

In nahezu sämtlichen jüngeren Konflikten sind Cyber-Angriffe durch staatliche, halb- oder auch nicht-staatliche Akteure zum integralen Bestandteil einer hybriden Kriegsführung geworden. Ebenso wie der Landkrieg durch die Entwicklung von See- und sodann Luft- und Raumfahrt beständig weitere Dimensionen erhielt, wird die Kampfzone nun womöglich auf den Cyber-Space ausgeweitet und damit – nach See-, Luft- und Weltraumkrieg[782] – um einen „Cyber-Krieg" ergänzt. Entsprechend mag man sich dem Thema des „Cyber-Krieges" mit der nüchternen Feststellung nähern, dass neue Erscheinungsformen des Krieges auch aus versicherungsvertraglicher Perspektive keineswegs ungewöhnlich sind:

> *„Modern manifestations (of war) have (always) had to be considered in the context of traditional war risk insurance wordings."*[783]

Dieser Befund ist ebenso wie die historische Entwicklung für das Verständnis der Ausschluss-Problematik bei staatlich motivierten und womöglich in „kriegerischer" Absicht ausgeführten Cyber-Angriffen hilfreich (**dazu unter 1**). Vor diesem Hintergrund erschließt sich zum einen, weshalb die bis heute spartenübergreifend weltweit vorherrschenden Wordings, die auf die rund 85 Jahre alte „NMA 464"-Klausel zurückgehen, für die Erfassung von „Cyber-Krieg" womöglich ungeeignet sind (**hierzu unter 2**). Zum anderen ist die

---

782 Vgl. zum Einsatz von Anti-Satelliten-Raketen durch Russland nur *Flage*, Wenn der Krieg den Weltraum erreicht, tagesschau.de v. 2.5.2022, abrufbar unter: https://www.tagesschau.de/ausland/amerika/krieg-satelliten-101.html (zuletzt abgerufen am 1.5.2025).

783 *O'May/Hill*, Marine Insurance, 1993, S. 250 ff.

Fortschreibung durch Ausschlüsse für „Cyber-Operationen“ im Gefolge von LMA5564(a,b)-5567(a,b)[784] entsprechend geboten.

1. Historische Entwicklung der Kriegsausschlüsse: Lehren aus statischen Wordings und der Siegeszug von NMA 464

Über die Zeitachse lässt sich durchaus eine gewisse Trägheit hinsichtlich bestehender Wordings feststellen. Skizziert man den Weg der Kriegsausschlüsse, so lassen sich seit den Anfangstagen in *Edward Lloyd's Coffee House* 1680 zumindest im maritimen Bereich des „*S.G. Form* (*Ships, Goods*)“ noch keine solchen Ausschlüsse konstatieren: Das Kriegsrisiko war als eine der Seegefahren mitgedeckt.[785] Doch spätestens die Kriege des 18. und 19. Jahrhunderts und insbesondere der US-Unabhängigkeitskampf zu Lande und zur See sowie die (See)Schlachten Napoleons änderten dies: Nachdem beispielsweise 1780 aus einem britischen Konvoi von 80 nur 8 Schiffe entkamen und die französische und die junge US-Flotte in der Folgezeit rund 10% des britischen Seehandels dezimierten und dadurch eine erhebliche Zahl von Lloyd's-Syndikaten ebenfalls Schlagseite bekamen, wurde die – freilich abdingbare – „*FC & S-Clause* (*Free of Capture and Seizure*)“ eingeführt.[786] Eine flächendeckende Übereinkunft der *Lloyd's*-Syndikate zum weitgehenden Ausschluss von „Kriegsrisiken“ gab es jedoch nicht vor 1898, wobei hier die noch heute bei maritimen Versicherungen anzutref-

[784] LMA 5564(a,b) bis LMA 5567(a,b) vom 18.1.2023 (War and Cyber Operation Exclusion Clauses).

[785] Z.B. *Marangos*, Historical overview of the insurance and exclusion of 'War Risks' and Associated Perils, in: ders. (ed.), War risks and terrorism, 2007, 15 f. m.w.N. Siehe zur Entwicklung in Deutschland m.w.N. auch *Makowsky*, VersR 2023, 1, 2, der u.a. auf die prägnante Aussage von *Beume*, ZVersWiss 1917, 297, 304 verweist: „Die Kriegsgefahr im weitesten Sinne ist vielleicht das älteste, jedenfalls aber das wesentliche Versicherungsrisiko des ursprünglichen Seeversicherungsvertrags und somit des ersten Versicherungsvertrags überhaupt.“.

[786] *O'May/Hill*, Marine Insurance, 1993, 3 und 250 ff.; *Marangos*, Historical overview of the insurance and exclusion of 'War Risks' and Associated Perils, in: ders. (ed.), War risks and terrorism, 2007, 15 f.; *Bateman*, War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions, Carnegie Endownment for International Peace, 2020, 1; *Chopra,* 82 Ohio State L.J. (2021), 121, 126 ff.

fende Differenzierung zwischen „marine risk“ und „(marine) war risk“ angelegt wurde.[787]

Doch die Erfahrungen im maritimen Bereich hinderten – trotz bereits existenter Kriegsausschlussklauseln – in den 1920er und 1930er Jahren die Underwriter insbesondere von UK- und US-Versicherern nicht daran, sogar ganz gezielt kriegsbedingte Risiken zu zeichnen: Namentlich bezogen nach den Erfahrungen des Ersten Weltkrieges viele Versicherer den ab 1914 durch breite Teile der Bevölkerung gefürchteten „bomb damage“ ebenso wie z.T. „civil commotion“ in den Deckungsumfang von Feuer-, Gebäude- und anderen Schadensversicherungen ein.[788] Diese sodann auch auf das kontinentale Europa ausgedehnte Zeichnungspraxis sollte nach Ausbruch des spanischen Bürgerkriegs und den verheerenden Zerstörungen durch neuartige Bomben manche *Lloyd's*-Syndikate an ihre Grenzen führen. Die Reaktion darauf war die Einführung der „NMA 464“-Klausel[789] zum 1.1.1938 durch *Lloyd's*: Dieser erste generelle und spartenübergreifende Ausschluss für „Krieg und Bürgerkrieg“ wurde rasch zum internationalen Marktstandard.[790] Als am 1.9.1939 der Zweite Weltkrieg ausbrach, fielen kriegsbedingte Schäden dann zumeist schon aus der Deckung heraus. Nicht zuletzt vor diesem Hintergrund hat die – aus Sicht der Versicherungswirtschaft überaus erfolgreiche – „NMA 464“-Klausel für nahezu sämtliche heutigen Wordings der Kriegsausschlüsse in allen Sparten Pate gestan-

787 *O'May/Hill*, Marine Insurance, 1993, 3 und 250 ff.; *Chopra,* 82 Ohio State L.J. (2021), 121, 126 ff. Zu eigenständigen Deckungskonzepten für Kriegsschäden im maritimen Kontext und im Luftfahrtbereich z.B. *Miller's*, Marine War Risks, 3rd ed. 2005, 8; *Nyampong*, Insuring the Air Transport Industry Against Aviation War and Terrorism Risks and Allied Perils, 2013, 75 ff.; *Makowsky*, VersR 2023, 1, 2.

788 Die Erfahrungen des Ersten Weltkriegs zeigten ein Prämienvolumen von fast 14 Millionen Pfund, dem eine Schadensbelastung von kaum 3 Millionen Pfund gegenüberstand: Denn Bombenschäden blieben – anders als z.B. Schäden durch Artillerie – im ersten Weltkrieg vergleichsweise gering. Hinzu kam ein staatliches Rückversicherungskonzept für ebendiese Schäden, vgl. *Carter/Falush*, The British Insurance Industry Since 1900, 2009, S. 22.

789 Vgl. NMA 464 (Non-Marine Association).

790 *O'May/Hill*, Marine Insurance, 1993, S. 296 f.; *Nyampong*, Insuring the Air Transport Industry Against Aviation War and Terrorism Risks and Allied Perils, 2013, 76 f.

den. Seit ihrer Einführung vor über 85 Jahren ist die Kriegsausschlussklausel jedoch nahezu unverändert geblieben.[791]

Erst am 25.11.2021 hat *Lloyd's* neue Definitionen von Krieg unter Erweiterung auf sog. „Cyber-Operations" veröffentlicht und insbesondere den Ausschluss von „state backed cyber-attacks" verbindlich vorgegeben.[792] Es hat sodann bekanntlich keine 20 Monate gedauert, bis ein Angriffskrieg in Europa losbrach, dessen „Cyber-Dimension" sich beständig weiter fortentwickelt.[793] Dieser kurze historische Abriss verdeutlicht zum einen die Gefahren statischer Wordings und illustriert zum anderen, welche Intention und welcher historischer Hintergrund den Klauseln der Generation „NMA 464" zugrunde liegt. Das führt unweigerlich zur Frage, ob denn ein „Cyber-Krieg" durch die überkommenen Kriegsausschlussklauseln erfasst wird.

2. Keine Erfassung des „reinen" Cyber-Krieges durch Ausschlussklauseln der „NMA 464"-Generation wie Ziff. A1-17.2 AVB-Cyber a.F. (2017)

In der Tat finden sich in den bislang marktgängigen Bedingungswerken der Cyber-Versicherung meistens an die „NMA 464"-Klausel von *Lloyd's* aus dem Jahre 1938 angelehnte Kriegsausschlüsse. So sollten laut Ziff. A1-17.2 AVB-Cyber a.F. (2017) vom Versicherungsschutz ausgeschlossen sein:

---

791 Vgl. zur zumeist nur graduellen Evolution der auf NMA 464 basierenden Klauseln nur *Young*, 52 Mich. L. Rev. (1956) 884; *Marangos*, Historical overview of the insurance and exclusion of 'War Risks' and Associated Perils, in: ders. (ed.), War risks and terrorism, 2007, 15 ff.

792 Vgl. LMA 5564 bis LMA 5567 („Cyber War and Cyber Operation Exclusion Clauses"), wobei nunmehr eine aktualisierte Fassung vom 18.1.2023 in Form der LMA 5564(a,b) bis LMA 5567(a,b) („War and Cyber Operation Exclusion Clauses") vorliegt. Diese Musterklauseln erfüllen die Anforderungen an den durch *Lloyd's* mit Wirkung zum 31. März 2023 (bzw. im Fall eines renewal) geforderten Ausschluss aller „state backed cyber-attacks", vgl. *Lloyd's Market Bulletin* Y5381 v. 16.8.2022, S. 2 f.

793 Dazu schon *Lüttringhaus*, VersR 2022, 1553.

„Versicherungsfälle oder Schäden aufgrund von Krieg. Krieg bedeutet: Krieg, Invasion, Bürgerkrieg, Aufstand, Revolution, Aufruhr, militärische oder andere Form der Machtergreifung."[794]

Erfasst diese an „NMA 464" angelehnte Definition nun auch einen „reinen", d.h. also ohne (Waffen)Gewalt und jenseits eines „klassischen" bewaffneten Konflikts ausgetragenen „Cyber-Krieg"? Teilweise wird im deutschsprachigen Schrifttum die Auffassung vertreten, dass heutzutage ein Cyber-Angriff gewissermaßen nur eine konsequente „Verlagerung der Kampfzone" vom physischen auf das digitale Schlachtfeld sei: Auch ein digitaler Krieg könne dann zum „Krieg" im versicherungsvertraglichen Sinne mutieren, wenn der Angriff und die dadurch hervorgerufenen – physischen – Schäden nur ein bestimmtes Maß überstiegen.[795]

Allerdings sind sekundäre Risikobeschreibungen stets restriktiv auszulegen[796] und Kriegsausschlussklauseln bilden dabei keine Ausnahme. „Krieg" ist kein feststehender Begriff der Rechtssprache und insbesondere existiert kein „versicherungsrechtlicher Kriegsbegriff"[797]: So hat der Gesetzgeber auch in § 84 VVG a.F. lediglich die AVB-Praxis der Kriegsausschlüsse übernommen, nicht aber eigene Begrifflichkeiten geprägt.[798] Selbst das Völkerrecht spricht allein von einem „bewaffneten Konflikt" bzw. von einer „Angriffshandlung", nicht aber von „Krieg", weshalb ein völkerrechtliches Begriffsverständnis im Versicherungsvertragsrecht kaum weiterhilft.[799]

---

[794] Ähnlich z.B. aus der Sachversicherung A. § 3 FBUB 2014 (Allgemeine Feuer-Betriebsunterbrechungs-Versicherungs-Bedingungen) und A. § 2 AFB 2010 (Allgemeine Bedingungen für die Feuerversicherung). Durchaus bemerkenswert ist, dass marktgängige Cyber-Policen – anders als die AVB-Cyber – zumeist keinen Ausschluss für „Cyberterrorismus" enthalten, vgl. nur *Woods/Weinkle*, Geneva Papers on Risk&Ins. 45 (2020), 639.

[795] *Günther*, r+s 2019, 190 f.: „Ein „Cyberkrieg" muss ein solches Ausmaß hinsichtlich seiner negativen Quantität und Qualität haben, dass er einem „klassischen" Krieg zwischen zwei Staaten gleichkommt." Gleichsinnig *ders.*, VW 4/2022, 68, 70 f. und im Grundsatz wohl auch *Makowsky*, VersR 2023, 1, 8 f. Kritisch hingegen *Lüttringhaus*, VersR 2022, 1553, 1558; *Rudkowski*, VersR 2024, 601, 607.

[796] Vgl. nur BGH VersR 2020, 692 Rz. 8.

[797] Vgl. aber *Dahlke*, VersR 2003, 25, 27 f.; *Naumann/Brinkmann*, r+s 2012, 469, 471; *Dallwig*, r+s 2022, 311, 314; Langheid/Wandt/*Dörner*, VVG, 3. Aufl. 2024, § 178 VVG Rn. 144.

[798] Vgl. *Motive und amtliche Begründung zum VVG*, 30.5.1908, Neudruck Berlin 1963, S. 156 f. Treffend *Makowsky*, VersR 2023, 1, 6.

[799] Vgl. schon RGZ 90, 378, 380. Wie hier z.B. *Perner/Artner*, Versicherungsrundschau 11/2022, 50, 55; *Makowsky*, VersR 2023, 1, 6. A.A. noch zu § 84 VVG a.F. dagegen Römer/Langheid/*Langheid*, 2. Aufl. 2003, § 84 VVG Rn. 3.

Vielmehr dürfte aus der maßgeblichen Perspektive des um Verständnis bemühten, geschäftserfahrenen und gewerblich tätigen Versicherungsnehmers zunächst der allgemeine Sprachgebrauch maßgeblich sein.[800] Der *Duden* definiert „Krieg" als einen „mit Waffengewalt ausgetragenen Konflikt zwischen Staaten".[801] Die Systematik und die durch den Versicherer mit der Kriegsausschlussklausel verfolgten Zwecke sind nach ständiger Rechtsprechung nur relevant, soweit sie für den Versicherungsnehmer bei Vertragsschluss hinreichend erkennbar sind.[802] Daran müssen sich auch die in Teilen des Schrifttums vertretenen Lesarten messen lassen, die auf konventionelle Gewaltmittel verzichten wollen, weil der Versicherungsnehmer ja erkennen müsse, dass zum einen sich Waffen und Kriegsführung fortentwickeln und zum anderen der Versicherer auch alle vergleichbaren Ereignisse ausschließen wolle, wenn der Cyber-Angriff nur

> *ein „solches Ausmaß hinsichtlich seiner negativen Quantität und Qualität (hat), dass er einem „klassischen" Krieg zwischen zwei Staaten gleichkommt";*[803]
>
> *oder sich*
>
> *„planmäßig in erheblichen Personen- und Sachschäden und damit in der physischen Welt (manifestiert)".*[804]

Das geht indes aus dem Wortlaut der Klauseln kaum hervor, und auch wenn der durchschnittliche Versicherungsnehmer den für ihn erkennbaren Sinnzusammenhang der Klausel betrachtet, wird er erkennen, dass zumindest die „klassische", auf „NMA 464" zurückgehende Ausschlussklausel den Kriegsbegriff an keiner Stelle anhand des Ausmaßes des Konflikts oder gar anhand von Art und Umfang der hierdurch hervorgerufenen Schäden definiert.[805] Anders verhält es sich hingegen mit den Konflikt*mitteln*: Die Kriegsdefinition setzt nach dem allgemeinen Sprachgebrauch nämlich immer den

---

800 Vgl. nur BGH NJW 2023, 684 Rn. 20.
801 https://www.duden.de/rechtschreibung/Krieg (zuletzt abgerufen am 1.5.2025).
802 Vgl. nur BGH NJW 2023, 684 Rn. 20.
803 *Günther*, r+s 2019, 190 f.
804 *Makowsky*, VersR 2023, 1, 8.
805 Vgl erneut nur Ziff. A1-17.2 AVB-Cyber a.F. (2017).

zwischenstaatlichen Einsatz physischer Gewalt voraus.[806] Vor allem definiert die Klausel „Krieg“ just in diesem Sinne zunächst einfach als „Krieg“ und verdeutlicht, dass der mit Waffengewalt zwischen Staaten ausgetragene „klassische Krieg“ als eine nicht weiter erläuterungsbedürftige Kategorie vorausgesetzt wird.[807] Ein um Verständnis bemühter Versicherungsnehmer wird sodann auch aus der Systematik der weiteren Aufzählung und namentlich der Erwähnung von „Invasion, Bürgerkrieg, Aufstand und Machtergreifung“ nur entnehmen können, dass „Krieg“ auch insoweit stets den Einsatz physischer Gewalt erfordert.[808] Ein Cyber-Angriff erfolgt hingegen grundsätzlich durch die Verbreitung von Schad-Code, was für sich genommen *nie* Gewaltausübung im Sinne physisch vermittelten Zwangs ist.[809]

Selbst wenn der Schad-Code-Einsatz bei besonders ausgefeilten und professionellen Attacken zu Sachschäden führen sollte, bleiben diese Schäden doch stets nur die mittelbare Folge des gewaltlosen, ohne physisch wirkenden Zwang vorgetragenen Angriffs.[810] Darüber kann auch die im Schrifttum teilweise vertretene „motiv- und wirkungsbezogene“ Interpretation der Kriegsklauseln nicht hinweghelfen: Selbst wenn die Vermeidung aller kriegsähnlichen Ausmaße an „negativer Quantität und Qualität“ – und damit von Cumul-Risiken – ein Motiv und Ziel des Versicherers sein mag,[811] ist das für den durchschnittlichen Versicherungsnehmer aus dem Bedingungswortlaut noch nicht einmal ansatzweise erkennbar und damit irrele-

---

806 Vgl. zum „mit Waffengewalt ausgetragener Konflikt zwischen Staaten“ erneut nur https://www.duden.de/rechtschreibung/Krieg (zuletzt abgerufen am 8.12.2024). Wie hier *Fortman*n, r+s 2019, 429, 433; *ders.*, FS Schimikowski, 2023, 93, 105; *Rudkowski*, VersR 2024, 601, 607.

807 *Lüttringhaus*, VersR 2022, 1550, 1558. In ebendiesem Sinne frühzeitig aus der US-Rechtsprechung etwa *The Brig Army Warwick (The Prize Cases)*, 67 U.S. (2 Black) 635, 666 (1863): „A war may exist where one of the belligerents, claims sovereign rights as against the other.“ Vgl. auch *Pan Amer. World Airways. v. Aetna*, 505 F.2d 989, 1005 (2d Cir. 1974): „[F]or there to be a ‚war‘ a sovereign or quasi-sovereign must engage in hostilities.“ Vgl. gleichsinnig aus der deutschen Rechtsprechung auch RGZ 90, 378, 380 f.

808 *Lüttringhaus*, VersR 2022, 1550, 1558. Ebenso im Ergebnis *Fortman*n, r+s 2019, 429, 433; *ders.*, FS Schimikowski, 2023, 93, 105. A.A. *Günther*, r+s 2019, 190 f.; *Makowsky*, VersR 2023, 1, 8 f.; *Perner/Artner*, Versicherungsrundschau 11/2022, 50, 58 ff.

809 *Lüttringhaus*, VersR 2022, 1550, 1558; *Rudkowski*, VersR 2024, 601, 607.

810 *Lüttringhaus*, VersR 2022, 1550, 1558. A.A. wiederum wohl *Günther*, r+s 2019, 190 f.; *Makowsky*, VersR 2023, 1, 8 f.; *Perner/Artner*, Versicherungsrundschau 11/2022, 50, 58 ff.

811 *Günther*, r+s 2019, 190 f. Ebenso *Perner/Artner*, Versicherungsrundschau 11/2022, 50, 58 ff., die sodann wohl eine interessengerechte Lösung über die Inhaltskontrolle der Kriegsausschlussklauseln anstreben.

vant.[812] Hinzu kommt, dass „Krieg“ in Ziff. A1-17.2 AVB-Cyber a.F. (2017) aus der Sicht eines durchschnittlichen Versicherungsnehmers einen Gewaltz*ustand*, nicht aber einen – wie auch immer gearteten – konkreten (Schadens)Erfolg voraussetzt und beschreibt: Spezifische Schäden sind allenfalls *Folge*n des Krieges, nicht aber notwendiger Bestandteil seiner Definition. Anders ausgedrückt, kann also längst ein „Krieg“ i.S.d. Ausschlussklausel herrschen, ohne dass bereits irgendwelche für die individuelle Cyber-Police relevante Schäden aufgetreten sind. Das erschließt sich dem um Verständnis bemühten Versicherungsnehmer im Fall von Ziff. A1-17.2 AVB-Cyber a.F. (2017) und anderer bisher marktüblicher Kriegsausschlussklauseln eindeutig aus dem Wortlaut und der erkennbaren Systematik: Denn die Klausel schließt alle „*Versicherungsfälle* … aufgrund von Krieg*“* und entsprechend gerade nicht nur bereits eingetretene „*Schäden“* aus.

Auch im Übrigen sprechen die für den Versicherungsnehmer erkennbare Systematik und Zielsetzung der AVB-Cyber a.F. (2017) ebenso wie die anderer Cyber-Bedingungswerke entschieden gegen einen weiten, „wirkungsbezogenen“ Kriegs-Begriff, der bei isolierten Cyber-Attacken ab dem Erreichen erheblicher „kriegsgleicher“ physischer Schäden erfüllt sein soll:[813] Denn Cyber-Versicherungsverträge decken vorrangig *reine Vermögensschäden*, wie Ziff. A1-1 i.V.m. Ziff. A1-3 AVB-Cyber a.F. (2017) illustriert.[814] Deshalb erscheint es aus der Perspektive eines Versicherungsnehmers kaum erklärlich, weshalb ausgerechnet ein bestimmtes Ausmaß von *Sach-* und/oder *Personenschäden* nun für den Kriegsbegriff im Cyber-Kontext entscheidend sein sollte. Zugleich behält das hier für Ziff. A1-17.2 AVB-Cyber a.F. (2017) befürwortete Verständnis des klassischen „Kriegs“ aus Versicherungsnehmersicht aber durchaus seinen praktischen Anwendungsbereich, weil der Versicherungsfall – typischerweise also eine „Informationssicherheitsverletzung“ –

[812] Vgl. erneut nur nur BGH NJW 2023, 684 Rn. 20.

[813] *Günther*, r+s 2019, 190 f.; *Makowsky*, VersR 2023, 1, 8 f.; *Perner/Artner*, Versicherungsrundschau 11/2022, 50, 58 ff.

[814] Partiell existieren auch Deckungsbausteine für Sachschäden an der IT-Hardware.

häufig mithilfe der sog. „Computersabotage“ nach § 303b StGB definiert wird, die vorliegt, wenn der Cyber-Angreifer die

> *„…Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht...“.*[815]

Demnach verbleibt aus Sicht des die Systematik betrachtenden Versicherungsnehmers für die auf physischen Gewalteinsatz fokussierte Kriegsausschlussklausel also der Anwendungsfall, dass im Zuge eines mit militärischen Mitteln – wie Bomben, Artillerie oder Raketen – geführten konventionellen Krieges Datenträger und/oder Datenverarbeitungsanlagen zerstört werden.[816] Nach den vorstehenden Ausführungen wäre demgegenüber eine isolierte Cyber-Attacke nicht erfasst.

Doch selbst wenn man – entgegen der hier vertretenen Auffassung – zumindest bei erheblichen physischen Folgeschäden „Krieg“ trotz des *per se* gewaltlosen Schad-Code-Einsatzes bejahen wollte, wäre weiterhin nach der ebenfalls zum überkommenen Kriegsverständnis zählenden Voraussetzung der Zwischenstaatlichkeit zu fragen: Just dieses Kriterium erscheint in den bisher diskutierten Konstellationen von physischen Folgeschäden durch Cyber-Attacken fraglich, solange der Angriff nur privaten Akteuren – wie z.B. einem Stahlwerk[817] oder einem Flüssiggas-Terminal-Betreiber[818] – gilt.[819] Selbst wenn man mit Blick auf den Angegriffenen ausreichen lässt, dass er auf dem Territorium eines bestimmten Staates attackiert wird, so bleibt doch die Identität des Angreifers zu klären: Und hier steht der hinsichtlich aller Tatbestandsmerkmale des Risikoausschlusses dar-

---

815 Solche Definitionen der Informationssicherheitsverletzung anhand der Computersabotage finden sich sowohl in den AVB großer Cyber-Versicherer als auch in Makler-Wordings.

816 Vgl. i.d.S. auch *Rudkowski*, VersR 2024, 601, 607.

817 Z.B. *Lloyd's*, Cyber Risk: The Emerging Cyber Threat to Control Systems (2021), 20.

818 Vgl. *Bloomberg*, Hackers Targeted U.S. LNG Producers in Run-Up to Ukraine War, abrufbar unter: https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine (zuletzt abgerufen am 1.5.2025). Siehe auch *Lloyd's*, Shifting Powers: Physical Cyber Risk in a Changing Geopolitical Landscape (2022), 4 ff.

819 Zu Staaten als Adressaten und Urheber des „Cyber-Krieges“ treffend *Perner/Artner*, Versicherungsrundschau 11/2022, 50, 55; *Fortmann*, FS Schimikowski, 2023, 93, 105; a.A. aber Rüffer/Halbach/Schimikowski/*Salm*, 4. Aufl. 2020, A1-17 AVB Cyber Rn. 3: „Durch die Plattform Internet ist die klassische Sichtweise einer Auseinandersetzung nicht mehr nur auf Staaten o.Ä. beschränkt. Ein Cyberkrieg kann demnach auch zwischen Unternehmen und/oder einem Staat entstehen.“.

legungs- und beweisbelastete Versicherer vor erheblichen Schwierigkeiten, die staatliche Herkunft und damit die Zwischenstaatlichkeit eines Cyber-Angriffs zu belegen.[820]

Zusammenfassend bleibt festzuhalten, dass herkömmliche, an NMA 464 orientierte Kriegs-Ausschlussklauseln das hier skizzierte Szenario des reinen „Cyber-Krieges" schon mangels physischer Gewaltanwendung nicht erfassen. Dieser Befund deckt sich auch mit der eindeutigen Tendenz, die US-Gerichte in den ersten Verfahren zum „Cyber-Krieg" haben erkennen lassen: In den – mittlerweile jeweils durch Vergleich beigelegten – Verfahren *Mondelez gegen Zurich*[821] und *Merck gegen ACE*[822] haben der *Illinois Circuit Court* ebenso wie der *Superior Court of New Jersey* übereinstimmend herausgestellt, dass selbst geschäftserfahrene Versicherungsnehmer die Bezugnahme auf „Krieg" in den tradierten Ausschlussklauseln nicht als Ausschluss von „reinen" Cyber-Angriffen verstehen müssen.[823] Besonders deutlich wird dies nun auch in der Entscheidung des *Superior Court of New Jersey (Appellate Division)* vom 1.5.2023:

> *„Contrary to the Insurers' contentions, these cases demonstrate a long and common understanding that terms similar to „hostile or warlike action" by a sovereign power are intended to relate to actions clearly connected to war or, at least, to a military action or objective. Therefore, in addition to the plain language interpretation of the exclusion requiring the inapplicability of the exclusion, the context and history of this and similarly worded exclusions and the manner in which similar exclusions have been*

820 Vgl. zur sog. „attribution" noch eingehend unten 3 c).

821 *Mondelez Int'l, Inc. v. Zurich Am. Ins. Co.*, No. 2018-L-011008 (Ill. Cir. Ct.).

822 *Merck & Co., Inc. v. Ace Am. Ins. Co.*, No. UNN-L-002682-18 (N.J. Super. Ct. Law Div. 6.12.2021).

823 Eine grundsätzlich restriktive Lesart von Krieg („war") findet sich bei US-Gerichten bereits zuvor, vgl. nur *Bas v. Tingy*, 4 U.S. (4 Dall.) 37, 40 (1800); *Vanderbilt v. Travelers' Ins.*, 112 Misc. 248, 184 N.Y.S. 54 (1920); *Stankus v. New York Life*, 312 Mass. 366, 44 N.E. (2d) 687 (1942); *Rosenau v. Idaho Mut. Benefit Ass'n*, 145 P.2d 227 (Idaho 1944); *Stanbery v. Aetna*, 26 N.J. Super 498 (Law Div. 1953); *Pan Amer. World Airways. v. Aetna*, 505 F.2d 989 (2d Cir. 1974); *Universal Cable v. Atlantic Specialty Ins.*, 929 F.3d 1143 (9 Cir. 2019). Vgl. aus UK nur *British Steamship v. The King*, 1 A.C. 99 (1921); *Spinneys (1948) Ltd v. Royal Insurance Co Ltd* [1980] 1 Lloyd's LR 406, 437.

interpreted by courts all compel the conclusion that the exclusion was inapplicable to bar coverage for Merck's losses."[824]

Während die streitgegenständlichen Formulierungen in den Ausschlussklauseln freilich nicht nur von den in Deutschland marktgängigen Cyber-Policen abweichen, sondern auch andere Versicherungsprodukte betreffen, ist die gemeinsame Wurzel dieser Kriegsausschlussklauseln doch stets „NMA 464".[825] Das mag – zumindest im Grundsatz – eine Übertragbarkeit der Argumente nahelegen.

II. Internationale Aspekte der neuen Ausschlüsse von „Cyber-Operationen" im Gefolgen von LMA 5564(a,b) bis 5567(a,b)

Angesichts der Unzulänglichkeiten der konventionellen Kriegsausschlussklauseln der „NMA 464"-Generation hat *Lloyd's* diverse Musterklauseln für Ausschlüsse für sog. „Cyber Operationen" erstellt, die – nicht zuletzt angesichts der seit 31. März 2023 für alle *Lloyd's*-Syndikate verbindlichen Vorgaben – in ähnlicher Form auch in deutsche Versicherungsverträge Eingang finden.[826] Nachdem die im November 2021 lancierten Wordings der LMA 5564 bis 5567 sogleich Kritik erfahren haben,[827] hat *Lloyd's* die Spannbreite der Kriegs- und „Cyber-Operations"-Ausschlüsse im Januar 2023 durch LMA 5564(a,b) bis 5567(a,b) deutlich erweitert. Die „a"- und „b"-Varianten der LMA 5564(a,b) bis 5567(a,b)-Klauseln unterscheiden sich insbesondere dadurch, dass nur in der jeweiligen „a"-Variante die Methode der „Attribution of a cyber operation to a state" näher

824 *Merck & Co. v. ACE Am. Ins. Co.* 475 N.J. Super. 420 (App. Div. 2023) 293 A.3d 535, 551.
825 Vgl. erneut oben unter 1.
826 Mit Wirkung zum 31. März 2023 (bzw. im Fall eines renewal) müssen alle „state backed cyber-attacks" ausgeschlossen werden, vgl. dazu *Lloyd's Market Bulletin* Y5381 v. 16.8.2022, S. 2 f.
827 Z.B. *Lüttringhaus*, VersR 2022, 1550, 1558 ff.

umrissen wird.[828] Im deutschen Markt wird der neue LMA-Ansatz zumeist aufgegriffen, so auch z.B. in Ziff. A1-17.2 a.E. AVB-Cyber 2024.[829] Allerdings nehmen die durch (Rück)Versicherer und Maklerhäuser in den Markt getragenen, teils sehr unterschiedlichen Klauselvarianten beständig zu, und eine detaillierte Bewertung aller bislang in der Übersicht bei *Lloyd's* erfassten Wordings würde den Rahmen dieser Abhandlung sprengen.[830]

Vor diesem Hintergrund werden im Folgenden die gängigsten und – soweit ersichtlich – im deutschen Markt in ähnlicher Form teilweise schon präsenten[831] Ansätze dargestellt (**dazu unter 1**) und sodann an den bei einer Rechtswahl zugunsten deutschen Rechts maßgeblichen Anforderungen des deutschen Versicherungsvertrags- und allgemeinen Zivilrechts gemessen (**hierzu unter 2**). Der praktisch bedeutsamen Frage der „Attribution", d.h. also der Zuschreibung einer Cyber-Attacke zu einem staatlichen bzw. staatsnahen Akteur, wird sodann im Kontext der AVB Cyber 2024 besonderes Augenmerk gewidmet.[832]

---

828 Der betreffende Abschnitt in den Klauseln lautet auszugsweise: „Notwithstanding the insurer's burden of proof, which shall remain unchanged by this clause, in determining attribution of a cyber operation to a state, the insured and insurer will consider such objectively reasonable evidence that is available to them. This may include formal or official attribution by the government of the state in which the computer system affected by the cyber operation is physically located to another state or those acting at its direction or under its control." Die vorausgehende Klauselgeneration aus dem November 2021 sah eine solche Unterscheidung nicht vor, vgl. Ziff. 3 LMA 5564, Ziff. 4 LMA 5565, Ziff. 3 LMA 5566 und Ziff. 4 LMA 5567.

829 Dieser Abschnitt in der Klausel lautet auszugsweise: „Zuschreibung von Informationssicherheitsverletzungen, die durch einen Staat, im Auftrag oder unter Kontrolle eines Staates verursacht worden sind: Bei der Feststellung der Zuschreibung an einen Staat trägt der Versicherer die Beweislast. Ungeachtet dessen können Versicherer und Versicherungsnehmer alle ihnen zur Verfügung stehenden objektiv angemessenen Beweismittel berücksichtigen. Unter allen rechtlich zulässigen Beweismitteln kann dies auch die offizielle Zuschreibung durch staatliche Stellen des Staates, dessen kritische Infrastrukturen durch die Informationssicherheitsverletzungen beeinträchtigt worden sind, an einen anderen Staat oder zu Gruppen oder Personen, die auf seine Anweisung oder unter seiner Kontrolle handeln, umfassen.".

830 Abrufbar unter: https://www.lmalloyds.com/LMA/Underwriting/Non-Marine/Cyber_Clauses/cyber_war_clauses.aspx (zuletzt abgerufen am 1.5.2025).

831 Vgl. z.B. auch das sog. MunichRe-Endorsement (June 2022) der LMA „War and Cyber Operation Exclusion".

832 Siehe eingehend unter III 3 und unter IV.

1. Übersicht über gängige Klauselvarianten

Ohne Anspruch auf Vollständigkeit und auf künftige Marktdurchdringung werden im Folgenden drei Regelungsansätze unterschieden: Der nicht weiter differenzierende Ausschluss der „Cyber-Operation“ nach LMA 5564(a,b) (**dazu unter a**), der an der Beeinträchtigung „kritischer Infrastruktur“ ansetzende Ausschluss gemäß LMA 5565(a,b) bis 5567(a,b), (**dazu unter b**) sowie schließlich ein folgenbezogener, die Anordnung von UN-Maßnahmen, Kriegs- oder Bündnisfall voraussetzender Ausschluss (**dazu unter c**). Diese Klauseln finden – im Fall der LMA-Klauseln teils unter Modifikationen, z.B. infolge unterschiedlicher „endorsements“ durch Erst- und Rückversicherer –[833] auch im deutschen Markt Verwendung. Ohnehin scheint für die auf die Beeinträchtigung kritischer Infrastruktur abstellenden Klauseln LMA 5565(a,b) bis 5567(a,b) das seit einigen Jahren auch in Deutschland anzutreffende Wording eines Versicherers aus UK Pate gestanden zu haben.[834] Diesen KRITIS-Ansatz machen sich im Ausgangspunkt auch die neugefassten AVB-Cyber 2024 des GDV zu eigen.[835]

a) Ausschluss von „Cyber-Operation“ nach LMA 5564(a,b)

Durch Staaten oder unter staatlicher Beteiligung ausgeführte Cyber-Attacken weisen potentiell ein besonders großes (Cumul-)Risiko auf, weil Staaten über Ressourcen für besonders effektive Malware und damit für verheerende Cyber-Angriffe verfügen. Dies illustrieren etwa die StuxNet- und NotPetya-Attacken, die vielfach staatlichen Akteuren zugeschrieben worden sind. Vor diesem Hintergrund besteht ein anerkennenswertes Interesse der Cyber-Versicherer, staatliche Cyber-Angriffe auch jenseits „klassischer“ bewaffneter Konflikte vom Versicherungsschutz auszunehmen. Dies gilt umso

---

833 Einen ständig aktualisierten Überblick über die im internationalen Markt verwendeten Klauseln bietet die Zusammenstellung des LMA Underwriting Team „Cyber war clauses“, abrufbar unter: https://www.lmalloyds.com/LMA/Underwriting/Non-Marine/Cyber_Clauses/cyber_war_clauses.aspx (zuletzt abgerufen am 1.5.2025).

834 Dazu schon *Lüttringhaus*, VersR 2022, 1550, 1558 ff.

835 Dazu sogleich noch gesondert und eingehend unter III.

mehr, als manche Staaten gerade sophistizierte *Ransomware*-Attacken in großem Umfang zur „Devisenbeschaffung“ nutzen.[836]

Deshalb stellt LMA 5564(a,b) neben den überkommenen Kriegsausschluss nunmehr den Ausschluss von Versicherungsfällen, die auf eine „Cyber Operation“ zurückgehen:

> *„1. Notwithstanding any provision to the contrary in this insurance, this insurance does not cover any loss, damage, liability, cost or expense of any kind:*
>
> *1.1. directly or indirectly arising from a war, and/or*
>
> *1.2. arising from a cyber operation. …*
>
> *4. Cyber operation means the use of a computer system by or on behalf of a state to:*
>
> *4.1. disrupt, deny access to or, degrade functionality of a computer system, and/or*
>
> *4.2. copy, remove, manipulate, deny access to or destroy information in a computer system.“*

b) LMA 5565(a,b) bis 5567(a,b): „KRITIS-Ansatz“

Demgegenüber wählt LMA 5565(a,b) bis 5567(a,b) einen enger gefassten „KRITIS-Ansatz“, der für den Ausschluss von durch „Cyber Operationen“ verursachten Versicherungsfällen neben der Beeinträchtigung der Sicherheit oder Verteidigungsfähigkeit („security or defence“) entscheidend auf die Beeinträchtigung kritischer Infrastruktur („essential services“) abstellt:

> *„… 1.2. arising from a cyber operation that is carried out as part of a war, or the immediate preparation for a war; and/or*

[836] Vgl. nur *Reuters*, UN experts investigate 58 cyberattacks worth $3 bln by North Korea v. 8.2.2024: „United Nations sanctions monitors are investigating dozens of suspected cyberattacks by North Korea that raked in $3 billion to help it further develop its nuclear weapons program.“, abrufbar unter: https://www.reuters.com/technology/cybersecurity/un-experts-investigate-58-cyber attacks-worth-3-bln-by-north-korea-2024-02-08/ (zuletzt abgerufen am 1.5.2025).

1.3. arising from a cyber operation that causes a state to become an impacted state.

Paragraph 1.3 shall not apply to the direct or indirect effect of a cyber operation on a computer system used by the insured or its third-party service providers that is not physically located in an impacted state but is affected by a cyber operation. …

5. Essential service, for the purposes of this exclusion, means a service that is essential for the maintenance of vital functions of a state including without limitation: financial institutions and associated financial market infrastructure, health services or utility services.

6. Impacted state means any state where a cyber operation has had a major detrimental impact on:

6.1. the functioning of that state due to disruption to the availability, integrity or delivery of an essential service in that state, and/or

6.2. the security or defence of that state."[837]

In deutschen Cyber-Wordings ist dieser Ansatz für Cyber-Attacken mit staatlichem Hintergrund, die außerhalb eines mit physischen Gewaltmitteln geführten „klassischen" Krieges ausgeübt werden, beispielsweise wie folgt ausgestaltet[838] worden:

„Kein Versicherungsschutz besteht wegen Schäden... im Zusammenhang mit ... dem unzulässigen Zugriff auf ein IT-System … durch oder im Namen eines Staates im Territorium eines anderen Staates (Cyber-Operation), wenn diese Cyber-Operation einem Staat zugeschrieben werden kann und:

– *im* Zuge *eines Krieges ausgeführt wird und/oder*

[837] Im Vergleich zu LMA 5565(a,b) sieht LMA 5566(a,b) zusätzliche Limits vor und LMA 5567(a,b) hingegen bezieht den Ausschluss nur auf „that part of any loss, damage, liability, cost or expense", der auf Krieg oder Cyber-Operationen entfällt.

[838] Wie bereits ausgeführt, dürfte das Bedingungswerk eines Versicherers aus dem UK Pate für die in LMA 5565(a,b) bis 5567(a,b) verwendeten Formulierungen gestanden haben.

– *direkt* oder *indirekt zu einer Störung der … kritischen Infrastruktur oder …. der Sicherheit oder Verteidigung eines anderen Staates führt.*

Eine Cyber-Operation kann insbesondere dann einem Staat zugeschrieben werden, wenn die Regierung oder eine Sicherheitsbehörde ... eines relevanten Staates dies öffentlich kommuniziert.

Ein relevanter Staat ist jeder Staat,

– *dessen … kritisch(e) Infrastruktur … durch die Cyber-Operation gestört wurde (betroffener Staat) oder*

– der Mitglied der EU oder

– der NATO ist.

Bei widersprüchlichen Zuschreibungen innerhalb eines relevanten Staates ist die von der Regierung des jeweiligen Staates im Rahmen der offiziellen Kommunikation vorgenommene Zuschreibung maßgeblich. Bei widersprüchlichen Zuschreibungen zwischen verschiedenen relevanten Staaten ist die Zuschreibung durch den betroffenen Staat maßgeblich. Hat der betroffene Staat keine Zuschreibung vorgenommen, genügt die Zuschreibung durch einen relevanten Staat, auch wenn ein oder mehrere andere relevante Staaten diese nicht teilen oder ihr widersprechen".

c) Reaktionsbezogener Ansatz im Markt

Demgegenüber wählen manche im Markt anzutreffende Cyber-Bedingungswerke einen primär folgenbezogenen Ansatz, der auf die Reaktionen des Angegriffenen auf die Cyber-Attacke abstellt:

„Der Versicherer leistet keinen Ersatz für Schäden im Falle von Ansprüchen, (4.11 Krieg) die auf Folgendem beruhen, hieraus entstanden oder hierauf zurückzuführen sind:

(a) jede mut- und böswillige Handlung gegen Computer und/oder unberechtigte Nutzung oder unbefugter Zugriff, die/der ganz oder teilweise von oder im Namen eines souveränen Staates oder eines staatlich unterstützten Akteurs begangen wurde und die dazu führt oder als Grund angeführt wird:

(i) dass ein Regierungschef der G7 …. oder ein Regierungsorgan eines anderen souveränen Staates Maßnahmen anordnet, die die Anwendung von Gewalt gegen einen souveränen Staat darstellen;

(ii) in einer Resolution oder einer anderen förmlichen Maßnahme des Sicherheitsrats der Vereinten Nationen, die die Anwendung von Gewalt oder Wirtschaftssanktionen gegen einen souveränen Staat genehmigt, oder die zur Anwendung von Gewalt durch die Nordatlantikvertrags-Organisation oder ein anderes gleichwertiges internationales zwischenstaatliches militärisches oder politisches Bündnis gegen einen souveränen Staat führt" (Herv. d. Verf.).

Allen vorgenannten Ansätzen ist gemein, dass sie Konfliktpotential mit dem deutschen Zivilrecht sowie insbesondere mit dem Recht der Klauselkontrolle aufweisen.

2. Grad staatlicher Involvierung und Transparenzkontrolle: „on behalf of", „im Auftrag" oder „unter Kontrolle eines Staates"

Bemerkenswert ist bei der in allen Spielarten eingeführten „Cyber-Operation"[839] nicht nur die Aufgabe des Erfordernisses der Anwendung physischer Gewalt, sondern gerade auch des zwischenstaatlichen Bezuges: Es reicht nunmehr aus, dass ein Computersystem in einem anderen Staat manipuliert wird, ohne dass der dadurch Betroffene selbst ein staatlicher Akteur sein müsste. Doch damit nicht

[839] Gleiches gilt für die „mut- und böswillige Handlung gegen Computer und/oder unberechtigte Nutzung oder unbefugter Zugriff" in einigen AVB.

genug: Je nachdem, wie man das Handeln „für einen Staat" („on behalf of") auslegt, verzichtet die Klausel potentiell sogar auf jedwede (quasi)staatliche Beteiligung auf Seiten des Angreifers und damit auf den für den herkömmlichen Kriegsbegriff lange prägenden staatlichen Bezug. Diese Klauselgestaltung betritt damit Neuland. Die Klauseln sind deshalb auf den Prüfstand des deutschen Zivilrechts zu stellen: Halten die Risikoausschlüsse der auch im unternehmerischen Verkehr – freilich in den Schranken des § 310 Abs. 1 BGB vorzunehmenden –[840] Klauselkontrolle stand? Hier sind Zweifel angebracht, zumal alle durch *Lloyd's* publizierten Cyber-Kriegsausschlussklauseln ähnliche Bruchstellen aufweisen. Die LMA-Wordings und ihre Übertragung in deutschsprachige Bedingungswerke werfen insbesondere mit Blick auf die Art und den Grad der erforderlichen staatlichen Involvierung Bedenken hinsichtlich der Transparenz i.S.d. § 307 Abs. 1 S. 2 BGB auf. Denn das Transparenzgebot umfasst zugleich ein Bestimmtheitsgebot, demzufolge alle Tatbestandsvoraussetzungen und Rechtsfolgen in der (Ausschluss) Klausel so genau beschrieben werden müssen, dass für den Versicherungsnehmer der Umfang des Versicherungsschutzes erkennbar ist und für den Versicherer als Verwender insoweit keine ungerechtfertigten Beurteilungsspielräume entstehen.[841]

Ebenso wie LMA 5564(a,b) bis LMA 5566(a,b) begegnen auch im Markt verbreiteten Formulierungen Transparenzbedenken, soweit der Ausschluss Cyber-Operationen erfasst, die „für einen Staat" oder „im Namen eines Staates" („*on behalf of a state*")[842] ausgeführt werden. Diese Gestaltung ist mehrdeutig: Soll hiervon nur ein – offi-

---

840 Siehe nur BGH NJW-RR 2018, 198 sowie statt vieler Grüneberg/*Grüneberg*, 84. Aufl. 2025, § 307 BGB Rn. 20. Keine Neuerung bringt für Cyber-Versicherungsverträge hingegen § 310 Abs. 1a BGB, weil es sich nicht um Geschäfte i.S.d. § 310 Abs. 1 S. 2 BGB handelt.

841 Vgl. BGH NJW 2024, 669 Rn. 23; BGH WM 2024, 1361 Rn 14 ff.; BGH BeckRS 2021, 30598 Rn. 56; BGH NJW 2016, 1308 Rn. 18; BGH NJW-RR 2016, 842 Rn. 26. Vgl. aus unionsrechtlicher und freilich auf Verbraucherverträge beschränkter Perspektive zu Ausschlussklauseln in Versicherungsverträgen auch EuGH 20.4.2023 – Rs. C-263/22 (*Ocidental – Companhia Portuguesa de Seguros de Vida SA/LP*) ECLI:EU:C:2023:311 Rn. 37 ff.

842 Die vorgenannte englische Formulierung in den LMA-Klauseln („*on behalf of*"), kann sowohl „im Auftrag" als auch „im Interesse", „für" oder „zu Gunsten" bedeuten, vgl. zum BE nur https://dictionary.cambridge.org/dictionary/english/on-behalf-of („done for another person's benefit or support, or because you are representing the interests of that person") sowie zum AE z.B. https://www.merriam-webster.com/dictionary/on%20behalf%20of (jeweils zuletzt abgerufen am 1.5.2025).

zieller und vertraglich verfasster – staatlicher Auftrag zur Durchführung einer Cyber-Operation erfasst sein oder kann schon das eigenmächtige Handeln von Einzeltätern im Interesse oder zu Gunsten eines Staates ausreichen?[843] Trifft also, zugespitzt formuliert, das folgende für das Völkerrecht formulierte dictum von *Hugo Grotius* auch i.R.d. Ausschlussklauseln für Cyber-Operationen zu:

„(T)he power to wage war privately resides in the individual"?[844]

Zwar sind Risikoausschlussklauseln grundsätzlich restriktiv auszulegen.[845] Hier stehen beide Auslegungsvarianten indes völlig gleichberechtigt nebeneinander: Gerade angesichts des vielfältigen „Hacktivismus" von Individualtätern bis hin zu nicht-staatlichen Gruppen (z.B. Anonymous) erscheint ein weitgehender Ausschluss des Handelns „für" oder „im Namen von" Staaten ebenso plausibel wie staatlich beauftragte Hackerattacken.[846] Auch die Unklarheitenregel des § 305c Abs. 2 BGB hilft hier kaum weiter: Sie dürfte allenfalls dazu führen, dass man ein Handeln nur „zu Gunsten" oder „im Interesse" eines Staates im Ergebnis ausscheiden und zumindest eine – wie auch immer geartete – „Billigung" durch den Staat zu verlangen hat.[847] Das wirft aber sogleich weitere Fragen auf: Welcher Art muss diese Billigung sein und kann sie ggf. auch erst konkludent und nachträglich erfolgen?[848]

---

843 Vgl. zur Problematik der Erfassung von Akten von Einzeltätern durch Kriegs- und Terrorausschlussklauseln nur differenzierend *Makowsky,* VersR 2023, 1, 7 f. und ablehnend für Attacken auf dem Territorium unbeteiligter Staaten *Fricke*, VersR 1991, 1098, 1101; *ders.*, VersR 2002, 6, 8; *Dahlke*, VersR 2003, 25, 28.

844 *Hugo Grotius*, De Iure Praedae Commentarius, Vol. I (*Williams/Zeydel*, A Translation of the Original Manuscript of 1604, London 1950), S. 62.

845 Z.B. BGH VersR 2012, 1253. Hierzu statt vieler *Wandt*, Versicherungsrecht, 6. Aufl. 2016, Rn. 228.

846 Das gilt nach der hier vertretenen Ansicht sowohl für die hier gewählte deutsche als auch für die englische Fassung („on behalf of a state").

847 Auch in der Variante LMA 5567(a,b) wird dieser erforderliche staatliche Einfluss nur wenig klarer zum Ausdruck gebracht: „Cyber operation means the use of a computer system by, at the direction of, or under the control of a state". Hier bleibt insbesondere fraglich, was „at the direction of" für Aufforderungen bzw. Anweisungen verlangt und ob z.B. ein allgemeiner Aufruf staatlicher Stellen diesen Anforderungen genügt, vgl. *Reuters*, Exclusive-Ukraine calls on hacker underground to defend against Russia (24.2.2022), abrufbar unter: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/ (zuletzt abgerufen am 1.5.2025).

848 Vgl. zu Terrorausschlüssen – allerdings allein unter Kausalitätsgesichtspunkten zurückhaltend – *Makowsky,* VersR 2023, 1, 7 f.

Kaum anders stellt sich nun das Bild bei den in jüngerer Zeit – etwa in Ziff. A1-17.2 AVB Cyber 2024 – verwendeten deutschen Formulierungen „im Auftrag oder unter Kontrolle eines Staates" dar: Denn auch damit ist nicht ausgesagt, welchen Verbindlichkeitsgrad „Auftrag" oder „Kontrolle" haben müssen. Ist eine (vertrags)rechtlich verfasste Grundlage bzw. eine faktische Steuerung erforderlich oder reicht ein rein moralisch bzw. patriotisch grundierter Appell oder eine bloße Anreizstruktur?[849] Hier existieren in der Praxis zahlreiche Grenzfälle, mit denen sich manche Parteien von Cyber-Versicherungsverträgen bereits haben auseinandersetzen müssen: Reicht etwa der allgemeine Aufruf ukrainischer Stellen an Hacker, Russland und damit potentiell alle dort tätigen Entitäten und Personen zu attackieren, um ein Handeln „für", „im Namen" oder gar „im Auftrag" oder „unter Kontrolle" der Ukraine zu begründen?[850] Wie liegt der Fall, wenn konkrete Ziele benannt und Handlungsanweisungen gegeben werden? Welche Rolle spielt sodann die z.B. durch das russische Strafrecht geschaffene Anreizstruktur, wenn die Strafgesetze *per se* Angriffe außerhalb Russlands auf nicht-russische Entitäten straffrei stellen: Ist das eine staatliche Billigung oder gar kontrollierte Lenkung von Cyber-Attacken und handeln die – zumindest auch kriminell und finanziell motivierten – Akteure wie z.B. die Gruppen „*DoppelSpider*", „*DoppelPaymer*" und „*Indrik Spider*" angesichts dieser Anreizstruktur somit schon „für" oder – z.B. i.S.d. Ziff. A1-17.2 AVB Cyber 2024 – gar „unter Kontrolle" von Russland?[851] Es bleibt somit unklar, welchen Grad an Deutlich- und Verbindlichkeit die staatliche Billigung, Incentivierung und/oder Steuerung erreichen muss, damit man i.S.d. hier diskutierten Ausschlussklauseln ein Handeln „für", „im Auftrag" oder „unter Kontrolle" bejahen kann. Denn obschon die bereits zu Eingang dieser Abhandlung aufgezeigten Parallelen zwischen Angriffen von Piraten auf Hoher See einer-

[849] Vgl. auch unten III.

[850] Vgl. erneut *Reuters*, Exclusive-Ukraine calls on hacker underground to defend against Russia (24.2.2022), abrufbar unter: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/ (zuletzt abgerufen am 1.5.2025).

[851] In diese Richtung angesichts der Kontakte zur „Wagner"-Söldnergruppe etwa NRW-Innenminister *Herbert Reul*: „Daher liegt die Vermutung nahe, dass die Attacken ‚mindestens staatlich geduldet' werden … . Gleichzeitig ist nicht auszuschließen, dass die abgeschöpften Daten und Gelder auch für staatliche Zwecke genutzt werden", siehe FAZ v. 6.3.2023, Die Spur führt nach Russland, abrufbar unter: https://www.faz.net/aktuell/gesellschaft/kriminalitaet/hacker-angriff-auf-uniklinik-duesseldorf-die-spur-fuehrt-nach-russland-18727405.html (zuletzt abgerufen am 1.5.2025).

seits zu den zahlreichen „Daten-Piraten“ und „Daten-Kaperfahrern“ im Cyber-Space andererseits existieren,[852] so manifestiert sich heutzutage die staatliche Billigung solcher Attacken jedenfalls nicht mehr explizit und formalisiert durch offizielle „Kaperbriefe“.[853] Insbesondere lassen sich Grad und Umfang der erforderlichen Billigung durch Staaten nicht verlässlich aus dem Wortlaut der Ausschlussklausel oder unter Zuhilfenahme des § 305c Abs. 2 BGB ermitteln.[854] Im Ergebnis wird man die hier diskutierten Klauselgestaltungen deshalb stets an § 307 Abs. 1 S. 2 BGB messen müssen.[855] Das Transparenzgebot zwingt den Verwender nach der ständigen Rechtsprechung des BGH dazu, die Rechte und Pflichten des Versicherungsnehmers möglichst klar und verständlich darzustellen, damit der Versicherungsnehmer von vornherein erkennen kann, in welchem Umfang er Versicherungsschutz erlangt und er auch später nicht von der Durchsetzung seiner Rechte abgehalten wird.[856] Die Intransparenz mag hier daraus folgen, dass ein durchschnittlicher Versicherungsnehmer aufgrund der Formulierung der Klausel selbst bei verständiger Würdigung, aufmerksamer Durchsicht und Berücksichtigung des erkennbaren Sinnzusammenhangs im Vorhinein zentrale Aspekte seines Versicherungsschutzes gar nicht vollständig zu übersehen vermag. Das lässt sich an folgendem Beispiel im Gefolge des Russland-Ukraine-Konflikts illustrieren: Wird etwa ein gewerblich tätiger deutscher Versicherungsnehmer, der sein Russlandgeschäft nicht eingestellt hat, gerade aus diesem Grund von einem pro-ukrainischen Hobby-Hackerkollektiv – nach

852 Siehe oben A.

853 Kaperbriefe berechtigten kraft hoheitlicher Verleihung durch einen Staat dazu, Schiffe feindlicher Nationen aufzubringen, vgl. grundlegend *Hugo Grotius*, De Iure Praedae Commentarius, Vol. I (*Williams/Zeydel*, A Translation of the Original Manuscript of 1604, London 1950).

854 Auch soweit bei den LMA 5564(a) bis 5567(a) jeweils der systematische Zusammenhang mit der „Attribution“-Klausel zu beachten und deshalb die Attacke als „at the direction of, or under the control of a state“ zu verstehen wäre, bleibt sodann fraglich, was „at the direction of“ für Aufforderungen bzw. Anweisungen verlangt und ob z.B. ein allgemeiner Aufruf staatlicher Stellen genügt, vgl. erneut das Beispiel der Ukraine bei *Reuters*, Exclusive-Ukraine calls on hacker underground to defend against Russia (24.2.2022), abrufbar unter: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/ (zuletzt abgerufen am 1.5.2025).

855 So schon zur ersten Generation der LMA 5565-5567 *Lüttringhaus*, VersR 2022, 1550, 1559. Für eine Auslegung – wohl auch dieser und anderer Kriegsausschlussklauseln – zugunsten des Versicherungsnehmers aber Prölss/Martin/*Armbrüster*, 32. Aufl. 2024, Einl. Rn. 159.

856 Z.B. BGH WM 2024, 1361 Rn 14 ff.; BGH VersR 2020, 692 Rn. 8; BGH VersR 2017, 1330 Rn. 13. Vgl. auch BGH NJW 2023, 1718 Rn. 30.

einem allgemeinen Aufruf der Ukraine, die eine Liste solcher Unternehmen veröffentlicht –[857] „im Namen der Ukraine“ angegriffen, so hätte der Versicherungsnehmer bei einem weiten Verständnis der Ausschlussklausel keinen Cyber-Versicherungsschutz, weil die Angreifer gerade „für“ die Ukraine („*on behalf of*“) und womöglich sogar i.S.d. Ziff. A1-17.2 AVB Cyber 2024 „im Auftrag“ dieses Staates handeln – wenn auch vorrangig aus eigenem Antrieb.[858] Eine solche gemischte Motivlage, zugleich „für“ oder auch „im Auftrag“ einen Staat zu handeln, lässt sich bei vielen – gerade mit Gewinnerzielungsabsicht tätigen – Hackern und Hackerkollektiven aus bestimmten Staaten grundsätzlich nie ausschließen.[859] Deshalb wäre zusätzlich zu den Transparenzbedenken zu fragen, ob eine solche weite Klauselgestaltung nicht den Versicherungsschutz i.S.d. § 307 Abs. 1 S. 1, Abs. 2 Nr. 2 VVG auszuhöhlen droht. Das gilt in ganz besonderem Maße für jene Klauseln, die eine staatliche Involvierung bereits bei einer Beteiligung von solchen Personen oder Gruppen postulieren, die (irgendwann) in der Vergangenheit schon einmal an „entsprechenden“ Aktionen eines Staates teilgenommen haben.[860]

3. „Attribution“ und Klauselkontrolle

Darüber hinaus erscheint auch die Regelung in den „Attribution“-Klauseln der LMA 5564(a) bis 5567(a)) mit Blick auf die Anforderungen des § 307 Abs. 1 S. 2 BGB fragwürdig, soweit darin die Zuschreibung der Cyber-Operation geregelt wird. Die Methode der „At-

[857] Vgl. für eine solche Liste nur https://www.coalitionforukraine.com/ (zuletzt abgerufen am 1.5.2025).

[858] Vgl. aber erneut auch den Aufruf ukrainischer staatlicher Stellen: *Reuters*, Exclusive-Ukraine calls on hacker underground to defend against Russia (24.2.2022), abrufbar unter: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/ (zuletzt abgerufen am 1.5.2025).

[859] Vgl. erneut die Einschätzung von NRW-Innenminister *Herbert Reul* bezüglich einer russischen Hackergruppe, wonach viele Angriffe der Gruppe dazu dienten, sich selbst zu bereichern und zugleich nicht auszuschließen sei, „dass die abgeschöpften Daten und Gelder auch für staatliche Zwecke genutzt werden“, FAZ v. 6.3.2023, Die Spur führt nach Russland, abrufbar unter: https://www.faz.net/aktuell/gesellschaft/kriminalitaet/hacker-angriff-auf-uniklinik-duesseldorf-die-spur-fuehrt-nach-russland-18727405.html (zuletzt abgerufen am 1.5.2025).

[860] Vgl. zu diesem Ansatz in Ziff. A1-17.2 AVB Cyber 2024 noch eingehend unter III.

tribution of a cyber operation to a state“ wird darin wie folgt konkretisiert:

> *„(I)n determining attribution of a cyber operation to a state, the insured and insurer will consider such objectively reasonable evidence that is available to them. This may include formal or official attribution by the government of the state in which the computer system affected by the cyber operation is physically located to another state or those acting at its direction or under its control.“*[861]

Transparenzbedenken bestehen schon hinsichtlich der für die „attribution“ in LMA 5564(a) bis 5567(a) als maßgeblich bezeichneten Stellen (**hierzu unter a**). Hinzu treten territoriale Abgrenzungsprobleme (**hierzu unter b**) die selbst die Reichweite des in einigen Klausel-Varianten anzutreffenden Wiedereinschlusses (**dazu unter c**) in Frage stellen.

a) Intransparenz der „Attribution“-Klausel in LMA 5564(a) bis 5567(a)

Das Transparenzgebot nach § 307 Abs. 1 S. 2 BGB verlangt, dass Rechte und Pflichten des Vertragspartners klar erkennbar und etwaige wirtschaftliche Nachteile einer Vertragsregelung hinreichend deutlich werden.[862] Insbesondere ist der Klausel-Verwender laut BGH damit verpflichtet,

> *„einerseits die tatbestandlichen Voraussetzungen und Rechtsfolgen so genau zu beschreiben, dass für ihn keine ungerechtfertigten Beurteilungsspielräume entstehen. Der Vertragspart-*

---

[861] Auch in marktgängigen deutschen Bedingungswerken finden sich vergleichbare Ansätze, wie das folgende Beispiel illustrieren soll: „Eine Cyber-Operation kann insbesondere dann einem Staat zugeschrieben werden, wenn die Regierung oder eine Sicherheitsbehörde (einschließlich Geheimdiensten und Verfassungsschutzbehörden) eines relevanten Staates dies öffentlich kommuniziert.“ Die vorgehende Klauselgeneration der LMA 5564 bis 5567 aus November 2021 formulierte die „attribution“ dabei noch – materiell-rechtlich – verbindlicher: „The primary but not exclusive factor in determining attribution of a cyber operation shall be whether the government of the state (including its intelligence and security services) in which the computer system affected by the cyber operation is physically located attributes the cyber operation to another state or those acting on ist behalf.“.

[862] Siehe nur BGH NJW 2020, 986 Rn. 25 m.w.N.

ner soll andererseits ohne fremde Hilfe möglichst klar und einfach seine Rechte feststellen können, damit er nicht von deren Durchsetzung abgehalten wird."[863]

Maßstab der Bewertung der Transparenz sind dabei „die Erwartungen und Erkenntnismöglichkeiten eines durchschnittlichen Vertragspartners des Verwenders zum Zeitpunkt des Vertragsschlusses", wobei auch auf die Eigenheiten des „Vertrages der geregelten Art" abzustellen ist.[864]

Legt man diesen Maßstab zugrunde, so ist aus dem Wortlaut der LMA 5564(a) bis 5567(a) bereits nicht ersichtlich – und auch nicht mithilfe der Unklarheitenregel in eine Richtung auflösbar –, welche konkrete Stelle diese „Attribution" vornehmen muss: Ist mit der „Regierung" das Regierungsoberhaupt gemeint? Reicht irgendeine (Landes)Ministerebene? Oder muss es ein zuständiger (Bundes- oder Landes)Minister sein? Und welche Hierarchiestufe der Leitungs- und/oder Fachebene soll bei den Nachrichten- und Sicherheitsdiensten erforderlich und ausreichend sein? Soll gar eine nicht näher spezifizierte Mutmaßung „aus Regierungs-, Geheimdienst- oder Sicherheitskreisen" ausreichen? Das führt zu einer weiteren zentralen Frage: Mit welchem Grad an Gewissheit muss die Feststellung erfolgen? Reicht bereits ein bloßer Verdacht?[865] Bedarf es „gerichtsfester" Beweise, der individuellen Benennung oder gar der rechtskräftigen Verurteilung der Verantwortlichen?[866] Für den Versicherungsnehmer sind jedenfalls die zentralen Elemente der Zuschreibung der Cyber-Operation zu einem Staat nicht klar und verständlich. Es bleibt aus seiner Sicht intransparent, unter welchen Voraussetzungen dieser Risikoausschluss den Versicherungsschutz beschneidet. Bereits an dieser Stelle sei angemerkt, dass

---

863 Deutlich etwa BGH NJW 2020, 986 Rn. 25.

864 Vgl. nur BGH NJW-RR 2011, 1144, 1145; BGH NJW 2020, 986 Rn. 25 a.E.

865 Vgl. zur „attribution" von NotPetya nur *Wolff*, 28 Conneticut Insurance Law Journal (2021), 85, 116: „The best you can get is high confidence".

866 Vgl. zur Anklage der mutmaßlich für die „NotPetya"-Attacke verantwortlichen Mitarbeiter des russischen GRU durch das US-amerikanische Department of Justice nur *US DOJ Justice News*, „Six Russian Officers Charged in Connection with Worldwide Deployment of Malware and Other Disruptive Actions in Cyberspace" v. 19.10.2020, abrufbar unter: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (zuletzt abgerufen am 1.5.2025).

sich der Ansatz in Ziff. A1-17.2 AVB Cyber 2024 insoweit ähnlicher Kritik ausgesetzt sieht.[867]

b) Intransparenz in internationalen Fallgestaltungen: Cloud-Dienste und „physische Belegenheit des IT-Systems“

Das Verdikt der Intransparenz dürfte die Klausel auch insoweit ereilen, als die Zuschreibung durch den Staat erfolgen soll, in dem sich das „betroffene IT-System physisch befindet“. Denn schon bei vermeintlich rein nationalen Sachverhalten drohen hier potentiell konfligierende Bestimmungen durch mehrere Staaten, wenn z.B. Daten in den – in der Praxis entweder durch Zusatzbausteine und teils auch standardmäßig mitversicherten – Cloud-Diensten betroffen sind. Die Cloud-Nutzung gehört mittlerweile zum Alltag für nahezu alle Unternehmen: Hier werden Daten fragmentiert und je nach verfügbarer Speicherkapazität beliebig zwischen Rechenzentren verschoben, die sich überall auf der Welt befinden können. Werden Daten oder Datenfragmente in der Cloud durch einen Cyber-Angriff kompromittiert, sind also die „betroffenen“ IT-Systeme physisch in unterschiedlichen Staaten belegen – nämlich dort, wo der jeweilige Server steht.[868] Die Formulierung der LMA-Klauseln lässt hier nun eine zentrale Frage unbeantwortet: Muss die Zuschreibung der Cyber-Attacke dann durch alle Staaten einstimmig erfolgen, damit der Ausschluss greift? Das würde immerhin dem Rechtsgedanken des § 317 Abs. 2 BGB bei der Bestimmung durch mehrere Dritte entsprechen. Oder reicht eine Zuschreibung durch einfache oder qualifizierte Mehrheit der Staaten? Ist – ganz im Gegenteil – vielleicht nur eine einzige Zuschreibung bereits ausreichend? Oder ist gar eine Mosaikbetrachtung gewollt, die nach individueller Serverbelegenheit differenziert? Kurzum: Auch die Anknüpfung an den physischen Standort des IT-Systems dürfte angesichts der weit verbreiteten Deckung für die Cloud-Nutzung zur Intransparenz der Klausel führen. Die soeben skizzierten Transparenzbedenken dürften im

---

867 Dazu eingehend unter III 3 b).

868 Zum kollisionsrechtlichen Parallelproblem *Nordmeier*, MMR 2010, 151, 154 ff.; *Nägele/Jacobs*, ZUM 2010, 281, 283; *Schneidereit*, Haftung für Datenverlust im Cloud Computing, 2017, S. 71 f.; *Bach* in: Spindler/Schuster, Elektron. Medien, 4. Aufl. 2019, Art. 4 Rom II-VO Rn. 14. Siehe auch schon *Mankowski*, RabelsZ 63 (1999), 203, 272 f.

Übrigen z.B. auch bei der Master-Police in internationalen Versicherungsprogrammen und bei der Versicherung mehrerer Risiken in der EU im Wege des Dienstleistungsverkehrs verfangen: Denn hier stellt die Klausel weder hinreichend klar, auf welchen Staat es für die „*attribution*“ ankommt, noch wie weit eine etwaige Zuschreibung dann territorial reichen soll.

4. Belegenheit des Computersystems für den Wiedereinschluss nach Ziff. 1 UAbs. 2 LMA 5565(a,b) bis 5567(a,b)

Ein ähnliches Problem ergibt sich hinsichtlich der Transparenz des Wiedereinschlusses nach Ziff. 1 UAbs. 2 LMA 5565(a,b) bis 5567(a,b), der wie folgt lautet:

> *„Paragraph 1.3 shall not apply to the direct or indirect effect of a cyber operation on a computer system used by the insured or its third-party service providers that is not physically located in an impacted state but is affected by a cyber operation (Herv. d. Verf.).“*

In deutschsprachigen Cyber-Versicherungsbedingungen findet sich teilweise eine vergleichbare Regelung:

> *„Die vorstehende Ziffer III.2.2. findet keine Anwendung bei Schäden, die sich daraus ergeben, dass IT-Systeme eines Versicherten, die sich nicht auf dem Territorium eines von der Cyber-Operation betroffenen Staates befinden, von der Cyber-Operation betroffen sind“ (Herv. d. Verf.).*

Denn auch in dieser Konstellation wäre zu fragen, wie es um den Deckungsschutz bestellt ist, wenn Daten bzw. Datenfragmente in einer Cloud betroffen sind, die – zumindest auch – auf Servern eines „impacted state“ abgespeichert und von der Cyber-Attacke betroffen sind. Die physische Belegenheit von Servern des Cloud-Dienste-Providers und damit die Speicherorte erscheinen aus Sicht der Beteiligten des Cyber-Versicherungsvertrags kaum vorherseh-

bar und angesichts der rein an Speicherkapazitäten orientierten Datenallokation auch völlig zufällig und willkürlich. Das territoriale Kriterium der physischen Belegenheit („physically located“) dürfte damit auch in diesem Zusammenhang erheblichen Transparenzbedenken i.R.d. § 307 Abs. 1 S. 2 BGB begegnen.

5. Zwischenfazit

Eine wortlautgetreue Übersetzung der LMA-Musterklauseln dürfte für den deutschen Markt weder in der ursprünglichen (LMA 5564 bis 5567) noch in der überarbeiteten Fassung (LMA 5564(a,b) bis 5567(a,b)) dieser Kriegs-Ausschlussklauseln eine tragfähige Lösung bieten. Das lenkt den Blick auf den Ansatz, den der GDV in Deutschland nun mit dem Ausschluss von „Krieg und staatlichen Angriffen“ nach Ziff. A1-17.2 AVB-Cyber 2024 verfolgt.

III. GDV-Musterbedingungen: Ausschluss von „Krieg und staatlichen Angriffen“ nach Ziff. A1-17-2 AVB-Cyber 2024

Die GDV-Musterbedingungen orientieren sich beim Ausschluss von „Krieg und staatlichen Angriffen“ nach Ziff. A1-17.2 AVB-Cyber 2024 zwar einerseits erkennbar an dem in LMA 5565(a,b) bis 5567(a,b) verwendeten „KRITIS-Ansatz“.[869] Andererseits geht der Ausschlusstatbestand in Ziff. A1-17.2 AVB-Cyber 2024 auch deutlich darüber hinaus und wirft in jedem seiner Unterabsätze zahlreiche Fragen mit Blick auf die AGB-Klauselkontrolle auf. Vor diesem Hintergrund sind die Ausschlussvarianten für Cyber-Attacken i.R.v. „klassischen“ Kriegen nach Ziff. A1-17.2 lit. a) AVB-Cyber 2024 (**dazu unter 1**) sowie für staatlich veranlasste „reine“ Cyber-Angriffe nach Ziff. A1-17.2 lit. b) AVB-Cyber 2024 (**hierzu unter 2**) eingehend auf den Prüfstand der §§ 305 ff. BGB zu stellen. Besonderes Augenmerkt verdienen schließlich die klauselförmigen Erleichterun-

[869] Vgl. dazu erneut oben II b).

gen der „Zuschreibung“ und der Erfüllung der „Voraussetzungen“ nach Ziff. A1-17-2 AVB-Cyber 2024 (**dazu unter 3**).

1. Cyber als Instrument eines „klassischen“ Krieges: Ziff. A1-17-2 lit. a) AVB-Cyber 2024

In Anlehnung an den „klassischen“ Kriegsausschluss nimmt Ziff. A1-17.2 lit. a) AVB-Cyber 2024 zunächst Versicherungsfälle oder Schäden aufgrund von Krieg, kriegsähnlichen Ereignissen, Bürgerkrieg, Revolution, Rebellion oder Aufstand vom Deckungsumfang aus,[870]

> *„auch wenn diese Versicherungsfälle oder Schäden aufgrund einer Informationssicherheitsverletzung gem. A1-2.1 durch einen Staat, im Auftrag oder unter Kontrolle eines Staates im Verlauf eines Krieges entstanden sind“.*

Damit erfasst der Ausschluss zum einen ISV, die durch physisch vermittelte Gewalt – etwa einen Raketen- oder Bombeneinschlag – die informationsverarbeitenden Systeme des Versicherungsnehmers beeinträchtigen. Zum anderen werden auch Schäden oder Versicherungsfälle infolge „reiner“ Cyber-Attacken ausgeschlossen, soweit sie im Rahmen eines Krieges durchgeführt werden. Offen bleibt indes, wer nach Ziff. A1-17.2 lit. a) AVB-Cyber 2024 Urheber und wer Adressat der Cyber-Attacke sein muss, damit der Angriff einem „Krieg“ zugerechnet werden kann und der Ausschlusstatbestand greift. Wie gezeigt, umfasst das überkommene Kriegsverständnis grundsätzlich das Merkmal der Zwischenstaatlichkeit. Dieses Kriterium erscheint jedenfalls immer dann fraglich, wenn die Cyber-Attacke einerseits nur privaten Akteuren gilt[871] und andererseits von Privaten – wie einem Hacker-Kollektiv oder einer allenfalls „staatsnahen“ Vereinigung – ausgeführt wird. Insoweit greifen die

---

[870] Aufgegeben wird im Vergleich zur Vorgängerfassung aus dem Jahre 2017 jedoch die – ohnehin kritikwürdige – „Machtergreifrung“, vgl. dazu *Rudkowski*, VersR 2024, 601, 607; *dies.*, VersR 2023, 416, 418.

[871] Zu Staaten als Adressaten und Urheber des „Cyber-Krieges“ treffend *Perner/Artner*, Versicherungsrundschau 11/2022, 50, 55; *Fortmann*, FS Schimikowski, 2023, 93, 105; a.A. aber wiederum Rüffer/Halbach/Schimikowski/*Salm*, 4. Aufl. 2020, A1-17 AVB Cyber Rn. 3: „Ein Cyberkrieg kann demnach auch zwischen Unternehmen und/oder einem Staat entstehen.“.

gleichen (Transparenz)Bedenken, wie sie schon gegenüber den Lösungen in LMA 5564(a,b) bis 5567(a,b) geäußert worden sind.[872] Hinzu kommt, dass der Cyber-Versicherer auch unter Ziff. A1-17.2 lit. a) AVB-Cyber 2024 hinsichtlich aller Tatbestandsmerkmale des Risikoausschlusses darlegungs- und beweisbelastet ist, wobei die Wirksamkeit und Wirkung der klauselförmigen Regelungen betreffend die erleichterte „Zuschreibung" sowie die Erfüllung der „Voraussetzungen dieses Ausschlusses" in Ziff. A1-17.2 AVB-Cyber 2024 äußert fraglich erscheinen – wenn man sie denn überhaupt nach Struktur und Erscheinungsbild der Klausel auf lit. a) erstrecken möchte.[873]

Bemerkenswert ist an diesem Ausschlusstatbestand hingegen die klare Eingrenzung der zeitlichen Dimension: Erfasst werden nach dem ausdrücklichen Wortlaut nur Versicherungsfälle oder Schäden durch eine ISV, die „im Verlauf eines Krieges" entstehen. Hier lohnt ein vergleichender Blick auf die Entwicklung der Judikatur zu Bomben-Blindgängern, die erst nach Ende des 2. Weltkrieges zu Schäden führten. Während die deutsche Rechtsprechung bei zeitlich dicht am Kriegsende liegenden Versicherungsfällen den Ausschluss noch bejahte,[874] sah die Rechtsprechung jedoch mit zunehmendem Zeitablauf eine Auflösung des Konnexes zum „Krieg" und damit auch zum Tatbestand der Kriegsausschlussklausel: Hier finde „das Prinzip der adäquaten Verursachung seine zeitliche Grenze in der Stabilisierung der Verhältnisse und der Rückkehr zur staatlichen Sicherheit und Ordnung nach der Beendigung eines Kriegszustandes".[875] Mag dies in der Sache auch überzeugen,[876] so ist dieser

---

872 Vgl. erneut oben unter II 2.

873 Gegen eine Erstreckung der im Anschluss an lit. b) aufgestellten „Erleichterungen" auch auf lit. a) von Ziff. A1-17.2 AVB-Cyber 2024 *Rudkowski*, VersR 2024, 601, 608, wobei hier wohl zu fragen ist, ob ein durchschnittlicher Versicherungsnehmer die anschließenden Absätze nicht als allgemeine Regelungen versteht und entsprechend auf alle Varianten des Ausschlusstatbestandes erstreckt. Dazu eingehend unter 2.

874 Vgl. BGH VersR 1952, 52; OLG Gera VW 1947, 234; OLG Braunschweig VW 1948, 13; OLG Düsseldorf VW 1949, 282; OLG Hamm VersR 1953, 319. Eingehend zum Ganzen *Rapp*, VersR 2020, 136, 143 ff.; *Dallwig*, r+s 2022, 311 ff.

875 Vgl. *Red.* r+s 2012, 498 unter Verweis auf LG Düsseldorf VersR 1951, 50. Siehe auch LG Frankfurt/Oder r+s 2024, 806 ff. (Revision anhängig beim OLG Brandenburg Az. 11 U 147/24). Dem ist in der Literatur vereinzelt mit Blick auf unentdeckte Fliegerbomben und Sprengladungen widersprochen worden: Diese seien „als adäquate Kriegsfolgen stets ausgeschlossen", vgl. z.B. *Günther*, r+s 2019, 188, 189. Vgl. auch *Visser/Dalisdas*, PHi 1/2025, 38, 39 f. Dagegen z.B. mit Blick auf die AFB treffend Prölss/Martin/*Armbrüster*, 32. Aufl. 2024, AFB A. § 2 Rn. 5.

Ansatz bei rechtsvergleichender Betrachtung keineswegs überall konsensfähig: Beispielsweise sah sich im Vereinigte Königreich der *Court of Appeal* in *University of Exeter* v. *Allianz Insurance*[877] mit einer nicht nach Plan verlaufenen kontrollierten Detonation einer deutschen Weltkriegsbombe im Jahr 2021 konfrontiert, durch die ein Universitätsgebäude beschädigt wurde. Der *Court of Appeal* bejahte das Eingreifen des – auf NMA 464 zurückgehenden „klassischen" – Kriegsausschlusses mit der Begründung, dass die Kriegshandlung des Bombardements einerseits und die fehlgeschlagene Entschärfung andererseits zwei konkurrierende Ursachen von nahezu gleicher Bedeutung seien.[878] Für den *Court of Appeal* stand damit die Gleichwertigkeit der Ursachen im Fokus, der Einfluss des Zeitablaufs auf die Festigkeit und Relevanz der kausalen Verknüpfung blieb eine Randnotiz.[879]

Vor diesem Hintergrund international durchaus unterschiedlicher Ansätze erscheint die Regelung in Ziff. A1-17-2 lit. a) AVB Cyber 2024 sinnvoll, da diese nicht nur die ausgeschlossene Gefahr, sondern auch die zeitliche Reichweite der Kausalkette konkretisiert: In temporaler Hinsicht werden nur Schäden oder Versicherungsfälle infolge von ISV durch einen Staat, im Auftrag oder unter Kontrolle eines Staates erfasst, die „im Verlauf" und damit *während* eines Krieges entstehen.[880] Stellt man diese ausdrückliche Einschränkung den bisher zu „klassischen" Kriegsausschlüssen im Wege der Auslegung ermittelten zeitlichen Grenzen gegenüber, so führt die Lösung in Ziff. A1-17-2 lit. a) AVB Cyber 2024 zu einem deutlich engeren Anwendungsbereich des Ausschlusses: Schäden oder Versicherungsfälle durch staatlich veranlasste ISV nach Beendigung des Krieges fallen nicht unter Ziff. A1-17-2 lit. a) AVB Cyber 2024. Damit schafft diese Klausel für die Parteien des Versicherungsvertrags

876 Dazu eingehend *Lüttringhaus/Ettl*, VersR 2025, 649, 654 ff.
877 Court of Appeal, 14.12.2023, The University of Exeter v. Allianz Insurance Plc, EWCA Civ 1484.
878 Court of Appeal, 14.12.2023, The University of Exeter v. Allianz Insurance Plc, EWCA Civ 1484.
879 *The University of Exeter v. Allianz Insurance Plc*, EWCA Civ 1484 (14.12.2023). Vgl. auch die ältere deutsche Rechtsprechung zu während dem zweiten Weltkrieg in Gang gesetzten und sich zeitlich später realisierenden Ursachenketten: OLG Frankfurt NJW 1947/48, 183; LG Düsseldorf VersR 1951, 50; AG Hannover VersR 1951, 47.
880 *Rudkowski*, VersR 2024, 601, 607 f.

Gewissheit über die zeitliche Dimension des Ausschlusstatbestandes.

2. Reine Cyber-Attacken mit KRITIS-Bezug: Ziff. A1-17-2 lit. b) AVB-Cyber 2024

Im Vergleich zur lit. a) geht der Ausschluss in Ziff. A1-17-2 lit. b) AVB Cyber 2024 deutlich weiter und erfasst

> *„Versicherungsfälle oder Schäden aufgrund von Informationssicherheitsverletzungen, die durch einen Staat, im Auftrag oder unter Kontrolle eines Staates verursacht worden sind, wenn dadurch auch kritische Infrastrukturen im Umfang der Regelungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) in diesem oder einem anderen Staat ausgefallen oder beeinträchtigt sind."*

Ziff. A1-17-2 lit. b) AVB Cyber 2024 schließt damit „Versicherungsfälle oder Schäden, *erstens*, aufgrund von Informationssicherheitsverletzungen, die durch einen Staat, im Auftrag oder unter Kontrolle eines Staates verursacht worden sind aus, wenn dadurch, *zweitens*, zumindest auch kritische Infrastrukturen im Umfang der Regelungen des BSIG in diesem oder einem anderen Staat ausgefallen oder „beeinträchtigt" sind. Das erste zentrale Tatbestandsmerkmal wirft im Wesentlichen dieselben Probleme auf, wie die der Ziff. A1-17-2 lit. b) AVB Cyber 2024 erkennbar zugrunde liegende Formulierung in LMA 5564(a,b) bis 5567(a,b), wo von „*on behalf of a state*" bzw. „*at the direction of, or under the control of a state*" die Rede ist.[881] Auch hinsichtlich der Transparenz- und Inhaltskontrolle kann deshalb auf die obigen Ausführungen zu den LMA 5564(a,b) bis 5567(a,b) verwiesen werden.[882]

Entsprechend dem auf die internationalen Aspekte von Cyber-Vorfällen fokussierten Erkenntnisinteresse gilt besondere Aufmerksamkeit der sachlich-kausalen und vor allem territorialen Verknüpfung

[881] Siehe dazu erneut oben II.
[882] Siehe dazu eingehend oben II 2.

zwischen dem staatlich grundierten Cyber-Angriff einerseits sowie den dadurch jeweils hervorgerufenen „Beeinträchtigungen" kritischer Infrastruktur und dem Eintritt von Versicherungsfällen bzw. Schäden andererseits (**dazu unter a**). Darüber hinaus erscheint auch die Bezugnahme auf „Beeinträchtigungen" kritischer Infrastruktur i.S.d. KRITIS-Definition des deutschen BSIG unter verschiedenen Gesichtspunkten in Sachverhalten mit Auslandsbezug unglücklich (**dazu unter b**).

a) Sachlich-territoriale Auswirkungen auf KRITIS-Infrastruktur

Zunächst dürften schon die in Ziff. A1-17-2 lit. b) AVB Cyber 2024 geforderten sachlich-territorialen Auswirkungen auf KRITIS-Infrastruktur große Probleme bereiten. Ein durchschnittlicher Versicherungsnehmer wird die Formulierung zunächst dahingehend verstehen, dass ein Ausfall „kritischer Infrastruktur" zuvörderst im für die Cyber-Operation selbst verantwortlichen *angreifenden* Staat notwendig ist: Denn „in diesem Staat" im letzten Satzteil kann sich – mangels anderer erkennbarer Bezugspunkte – gerade nur auf „durch einen Staat" beziehen. Diese Anknüpfung kann zu nachgerade widersinnigen Ergebnissen führen, wenn einzig und allein im Angreiferstaat selbst kritische Infrastruktur „beeinträchtigt" wird, in anderen Staaten aber cyberversicherte Privatunternehmen Informationssicherheitsverletzungen zu beklagen haben. Die LMA 5565(b) bis 5567(b) wirken dem durch den Wiedereinschluss von Schäden oder Versicherungsfällen entgegen, die in einem anderen Staat, als dem von einer Beeinträchtigung der KRITIS-Infrastruktur betroffenen Staat (sog. „*impacted state*"), eintreten. Manche im deutschen Markt anzutreffende Wordings definieren die „Cyber-Operation" auch von vornherein eindeutig als Angriff „durch oder im Namen eines Staates im Territorium eines *anderen* Staates".[883] Zwar mag auch der GDV bei der Erstellung Ziff. A1-17-2 lit. b) AVB Cyber 2024 ausweislich der begleitenden GDV-Presse-Meldung möglicherweise einen engeren Anwendungsbereich im Sinn gehabt und nur einen Ausschluss der – direkt und gezielt oder aber indirekt als Kollateralschäden – auch Private treffenden „Folge(n) eines erfolgrei-

[883] Vgl. oben II 1 c).

chen staatlichen Angriffs auf kritische Infrastrukturen“ intendiert haben.[884] Selbst in dieser erläuternden Meldung wird jedoch nicht vollends deutlich, ob nur Infrastrukturen in anderen Staaten als dem Angreiferstaat relevant sein sollen. Vor allem wird ein solches potentiell restriktiveres Verständnis weder im Wortlaut der Ziff. A1-17-2 lit. b) AVB Cyber 2024 noch in der Systematik des Bedingungswerks in irgendeiner Form auch nur angedeutet. Damit ist die etwaige abweichende Intention der Klauselverfasser auch für einen um Verständnis bemühten Versicherungsnehmer in keiner Weise erkennbar und damit irrelevant.[885]

Ebensowenig hilft hier der – gerade bei Kriegsausschlüssen nach wie vor aufscheinende –[886] Ansatz einer objektiv-schutzweckbezogenen Auslegung von Ausschlüssen: Hierbei handelt es sich um ein Relikt der überholten „gesetzesähnlichen“ Interpretation von AVB, das quer zur nunmehr nach ständiger Rechtsprechung maßgeblichen Auslegungsperspektive des durchschnittlichen Versicherungsnehmers steht.[887] Eine vom Horizont des Versicherungsnehmers entkoppelte, einschränkende objektiv-schutzzweckbezogene Auslegung erscheint damit dogmatisch kaum haltbar.

Festzuhalten bleibt: Die „Kunstfigur“ des durchschnittlichen Versicherungsnehmers dürfte angesichts des insoweit klaren Wortlauts und grammatikalischen Bezugspunkts Ziff. A1-17-2 lit. b) AVB Cyber 2024 als sehr weit gefassten Ausschluss verstehen, der die Beeinträchtigung von kritischer Infrastruktur irgendwo auf der Welt – und zwar sogar vorrangig allein im Angreiferstaat selbst – ausreichen lässt.[888] Abweichende Auslegungsmöglichkeiten lassen sich

---

884 *GDV*, Cybersicherheit Versicherungsschutz gegen Cyberangriffe – GDV veröffentlicht neue Musterbedingungen v. 19.2.2024, abrufbar unter: https://www.gdv.de/gdv/medien/medieninformationen/versicherungsschutz-gegen-cyberangriffe-gdv-veroeffentlicht-neue-musterbedingungen—168132 (zuletzt abgerufen am 1.5.2025).

885 Zu Recht kritisch auch *Schilbach*, r+s 2024, 581, 587.

886 Vgl. etwa LG Bielefeld 27.5.1993 – 6 O 35/93 (juris); *Dallwig*, r+s 2022, 311, 314 f.

887 *Lüttringhaus/Ettl*, VersR 2025, 649, 650 ff. Siehe auch schon allgemein *Armbrüster* in: Karlsruher Forum 2007, *Lorenz* (Hrsg.), 2008, S. 89, 92 f.; *Schreier*, Verhältnis zwischen Schadensrecht und Schadensversicherung, 2017, S. 260 f.

888 *Lüttringhaus/Ettl*, VersR 2025, 649, 658 f. So im Ergebnis auch *Rudkowski*, VersR 2024, 601, 608.

weder mit dem erkennbaren Zweck der Klausel noch mit der Systematik der AVB Cyber 2024 begründen.[889]

Die Folge dürfte sein, dass der Versicherungsschutz entwertet zu werden droht, wenn nicht nur jedwede „Beeinträchtigung" kritischer Infrastruktur *im Angreiferstaat* selbst, sondern in irgendeinem Staat auf der Welt ausreicht, um den Ausschlusstatbestand zu erfüllen: Das Verdikt der unangemessenen Benachteiligung wegen Aushöhlung des Leistungsversprechens nach § 307 Abs. 1 S. 1 i.V.m. Abs. 2 Nr. 2 BGB liegt hier schon deshalb nahe, weil sich beispielsweise gerade in Entwicklungsländern immer irgendeine unzureichend gegen Cyber-Risiken gesicherte „kritische Infrastruktur" i.S.d. § 2 Abs. 10 BSIG finden dürfte, die durch selbstverbreitenden Schad-Code infiltriert wurde. Jedenfalls wenn dem Versicherer obendrein der Nachweis staatlicher Involvierung in erheblichem Maße durch die Klauselgestaltung erleichtert wird, würde der Ausschluss nach Ziff. A1-17-2 lit. b) AVB Cyber 2024 im Regelfall eingreifen, so dass der Cyber-Deckungsschutz – als Gegenstand des Vertrages – der Sache nach leerliefe.[890] Das dürfte dann als Gefährdung des Vertragszwecks i.S.d. § 307 Abs. 1 S. 1 i.V.m. Abs. 2 Nr. 2 BGB zu werten sein.[891]

b) „Beeinträchtigungen" von KRITIS-Infrastruktur i.S.d. BSIG

Darüber hinaus bietet Ziff. A1-17-2 lit. b) AVB Cyber 2024 neben der – für sich genommen schon vagen – Umschreibung der staatlichen Beteiligung[892] weitere Angriffsfläche unter Transparenzgesichtspunkten: Das gilt sowohl für die Inbezugnahme des deutschen BSIG als auch für den Begriff der „Beeinträchtigung". Die Schwierigkeiten des Verweises auf „kritische Infrastrukturen im Umfang der Regelungen des … BSIG" beginnen dabei schon in territorialer Hin-

---

889 Im Gegenteil findet die hier befürwortete weite Auslegung entlang des klaren Wortlauts auch unter systematischen Gesichtspunkten eine Stütze in Ziff. A1-17-5 AVB Cyber 2024, wo „Versicherungsfälle oder Schäden aufgrund des Ausfalls von Infrastruktur" gesondert adressiert werden.

890 So im Ergebnis wiederum *Rudkowski*, VersR 2024, 601, 608.

891 *Lüttringhaus/Ettl*, VersR 2025, 649, 658 ff. Vgl. zu den Voraussetzungen nach § 307 Abs. 1 S. 1 i.V.m. Abs. 2 Nr. 2 BGB nur BGH NJW 2022, 872, 877; BGH VersR 2017, 1076 Rn. 15.

892 Vgl. zur Bedeutung von „durch einen Staat, im Auftrag oder unter Kontrolle eines Staates" eingehend oben II 2 und siehe auch *Rudkowski*, VersR 2024, 601, 608 f.

sicht: Das BSIG findet – kraft einseitiger Kollisionsnorm des internationalen Verwaltungsrechts – räumlich-territorial nur innerhalb des deutschen Bundesgebiets Anwendung. Demgegenüber besteht nach Ziff. A1-11 AVB Cyber 2024 aber Versicherungsschutz für Versicherungsfälle weltweit. Soweit nun kritische Infrastruktur im Ausland betroffen ist, zwingt Ziff. A1-17-2 lit. b) AVB Cyber 2024 den Versicherungsnehmer folglich dazu, zum Zweck der genauen Bestimmung seines Cyber-Versicherungsschutzes zu ermitteln, ob eine Infrastruktur-Einrichtung eines ausländischen Staates unter die Definitionen des deutschen BSIG fällt. Das kann zu Friktionen führen: Die Definition in § 2 Abs. 10 BSIG nennt als kritische Infrastrukturen – im Ausgangspunkt ganz unzweideutig – die „Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung“. Allerdings ist zugleich erforderlich, dass die jeweiligen Anlagen in den Sektoren „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“.[893] Letzteres Kriterium füllt sodann die BSI-KritisV mit Inhalt, die in ihren zahlreichen Anhängen mit teils komplexen Berechnungsformeln und Schwellenwerten operiert, die sich entsprechend des sachlich-territorialen Anwendungsbereichs des BSIG an der – rechtlichen wie faktischen – Situation in der Bundesrepublik Deutschland orientieren.[894] Das kann zu Friktionen führen, wenn diese Anforderungen für die Zwecke des Ausschlusstatbestandes in Ziff. A1-17-2 lit. b) AVB Cyber 2024 auf andere Staaten erstreckt werden. Um die Problemlage zu illustrieren, sei als anschauliches Beispiel der Sektor Gesundheit angeführt: Nach § 6 Abs. 1 Nr. 3 BSI-KritisV zählt zu den kritischen Dienstleistungen i.S.d. § 10 Abs. 1 S. 1 BSIG u.a. gerade Herstellung, Vertrieb und Abgabe von „verschreibungspflichtigen Arzneimitteln“. Wird nun eine Arzneimittel vertreibende, herstellende oder abgebende Einrichtung im Ausland durch einen staatlichen Cyber-Angriff getroffen,

[893] § 2 Abs. 10 BSIG.

[894] Vgl. z.B. zu den Anlagenkategorien und Schwellenwerten im Sektor Informationstechnik und Telekommunikation nur Anhang 4 Teil 2 Nr. 9 und Nr. 10 BSI-KritisV.

wäre zu fragen, ob es sich um eine KRITIS-Einrichtung i.S.d. BSIG handelt. Dafür ließe sich einerseits danach fragen, ob im betroffenen Staat überhaupt eine Verschreibungspflicht besteht – und bejahendenfalls, wie diese im Einzelnen ausgestaltet ist. Andererseits könnte aber auch auf die Verschreibungspflicht gemäß § 48 AMG i.V.m. AMVV nach deutschem Arzneimittelrecht abgestellt werden – die jedoch räumlich-territorial im betroffenen ausländischen Staat weder gilt, noch womöglich überhaupt für die dort verwendeten Arzneimittel inhaltlich Sinn ergibt. Welche „Verschreibungspflicht" hier maßgeblich sein soll, ist damit für einen um Verständnis bemühten Versicherungsnehmer kaum ersichtlich, und auch die Unklarheitsregelung in § 305c Abs. 2 BGB dürfte dazu keine klare Antwort liefern können. Die Liste ähnlich gelagerter Abgrenzungs- und Problemfälle ließe sich fortsetzen.

Festzuhalten bleibt bereits an dieser Stelle, dass die Inbezugnahme des deutschen BSIG in Ziff. A1-17-2 lit. b) AVB Cyber 2024 in vielen Fällen das Verdikt der Intransparenz nach § 307 Abs. 1 S. 2 BGB nach sich ziehen dürfte. Denn das Transparenzgebot zwingt den Versicherer, die Rechte und Pflichten des Versicherungsnehmers möglichst klar und verständlich darzustellen, damit der Versicherungsnehmer von vornherein erkennen kann, in welchem Umfang er Versicherungsschutz erlangt und er auch später nicht von der Durchsetzung seiner Rechte abgehalten wird.[895] Eine klare Darstellung ließe sich etwa durch eine eigene Definition der kritischen Infrastruktur – wie sie die LMA-Klauseln mit Blick auf Cyber-Operations vorsehen –[896] durchaus bewerkstelligen.

Darüber hinaus bietet Ziff. A1-17-2 lit. b) AVB-Cyber 2024 weitere im Rahmen der Klauselkontrolle angreifbare Formulierungen: So wird man aus der Warte eines durchschnittlichen, um Verständnis bemühten Versicherungsnehmers kritisch hinterfragen müssen, was sich hinter dem Begriff der „Beeinträchtigung" kritischer Infrastruktur verbirgt. Aus dem grammatikalischen, systematischen und sachlichen Zusammenhang mit einer Informationssicherheitsverletzung

[895] Z.B. BGH WM 2024, 1361 Rn 14 ff.; BGH VersR 2020, 692 Rn. 8; BGH VersR 2017, 1330 Rn. 13. Vgl. auch BGH NJW 2023, 1718 Rn. 30.

[896] Vgl. nur Abs. 5 LMA 5565(a,b) bis 5567(a,b).

dürfte der Versicherungsnehmer darauf schließen, dass eine „Beeinträchtigung“ i.S.d. Ziff. A1-17-2 lit. b) jedenfalls bei einer „Informationssicherheitsverletzung“ nach Ziff. A1-2.1 AVB Cyber 2024 vorliegt. Denn dort ist gerade von einer „Beeinträchtigung der Verfügbarkeit, Integrität, Vertraulichkeit“ die Rede. Ziff. A1-17-2 lit. b) AVB Cyber 2024 würde damit schon bei jedweder Verfügbarkeits-, Integritäts- oder Vertraulichkeitsbeeinträchtigung von Daten einer kritischen Einrichtung eingreifen, ohne dass es weiterer Folgen, wie z.B. einer Ausschaltung der Arbeitsfähigkeit der Einrichtung bedürfte. Für diese Lesart eines durchschnittlichen Versicherungsnehmers spricht auch unter systematischen Gesichtspunkten, dass Ziff. A1-17-2 lit. b) AVB-Cyber 2024 zugleich den „Ausfall“ der Infrastruktur erfasst und die „Beeinträchtigung“ erkennbar ein unterhalb dieser Schwelle des (Total)Ausfalls liegendes Phänomen beschreiben soll. Selbst wenn man – ohne eindeutige Anhaltspunkte im Wortlaut oder der Systematik – ein engeres Verständnis dergestalt für möglich hält, dass sich die „Beeinträchtigung“ jedenfalls einem drohenden „Ausfall“ annähern muss, dürfte die Unklarheitenregel nicht weiterhelfen: Nach zutreffender Auffassung ist § 305c Abs. 2 BGB nämlich gerade kein Instrument zur Erhaltung von i.S.d. § 307 BGB missbräuchlichen Klauseln, und es ist insofern die „kundenfeindlichste“, zur Unwirksamkeit führende Auslegungsalternative zugrunde zu legen.[897] So dürfte der Fall auch hier liegen: Denn setzt man die „Beeinträchtigung“ mit einer Informationssicherheitsverletzung nach Ziff. A1-2.1 AVB Cyber 2024 gleich, droht eine Aushöhlung des Cyber-Versicherungsschutzes i.S.d. § 307 Abs. 1 S. 1, Abs. 2 Nr. 2 BGB. Schließlich ist das Eindringen von weit ausgestreuter Schad-Software in KRITIS-Infrastrukturen *irgendwo auf der Welt* wohl kaum je auszuschließen.[898] Bei dieser Lesart könnte der Versicherer die Deckung bereits dann unter Verweis auf eine „Beeinträchtigung“ kritischer Infrastruktur in einem beliebigen Staat nach Ziff. A1-17-2 lit. b) verweigern, wenn dort nur die Vertraulichkeit von Daten Ziff. A1-2.1 AVB Cyber 2024 kompromittiert worden ist. Diese Bewertung dürfte gerade in der Zusammenschau mit den weiteren

[897] Vgl. nur BGH NJW 2017, 1596 Rn. 39; BGHZ 175, 76 Rn. 9; BGHZ 176, 244 Rn. 19 sowie statt vieler MünchKommBGB/*Fornasier*, 9. Aufl. 2022, § 305c BGB Rn. 52.

[898] Vgl. erneut Ziff. A1-17-2 lit. b) AVB-Cyber 2024: „in diesem oder einem anderen Staat“.

Regelungen in Ziff. A1-17-2 lit. b) AVB Cyber 2024 Bestand haben, weil dort die Darlegung der weiteren Voraussetzungen des Ausschlusses sowie insbesondere die Zuschreibung der Cyber-Attacke zu einem Staat erleichtert werden.

3. Erleichterungen von Darlegung und Beweis der Voraussetzungen des Ausschlusses nach Ziff. A1-17-2 AVB-Cyber 2024

Seinem Wortlaut nach weist Ziff. A1-17-2 AVB-Cyber 2024 die Darlegungs- und Beweislast uneingeschränkt dem Versicherer zu,[899] der ohnehin nach allgemeinen Grundsätzen die ihm günstigen, den Ausschlusstatbestand erfüllenden Tatsachen hinreichend substantiiert dartun und im Bestreitensfalle auch beweisen muss. Bei näherer Betrachtung geht der Ansatz in Ziff. A1-17-2 AVB-Cyber 2024 jedoch darüber hinaus und bezweckt eine Reihe praktischer Erleichterungen für den Cyber-Versicherer. Hinsichtlich der Tatbestandsvoraussetzungen des Ausschlusses nach lit. a) und b) regelt Ziff. A1-17-2 AVB-Cyber 2024 Folgendes:

> *„Die Voraussetzungen dieses Ausschlusses liegen insbesondere dann vor, wenn eine IT-forensische Untersuchung der informationsverarbeitenden Systeme des Versicherungsnehmers oder bei der Informationssicherheitsverletzung verwendeter Systeme oder Hilfsmittel objektive Hinweise auf die Beteiligung, Urheberschaft oder Steuerung der Informationssicherheitsverletzung durch einen Staat, im Auftrag oder unter Kontrolle eines Staates ergeben.*
>
> *Das ist unter anderem dann der Fall, wenn eine Beteiligung von Gruppen oder Personen nachgewiesen werden kann, die in der Vergangenheit bereits an entsprechenden Handlungen dieses Staates beteiligt waren.“*

[899] Vgl. Ziff. A1-17-2 AVB-Cyber 2024: „Bei der Feststellung der Zuschreibung an einen Staat trägt der Versicherer die Beweislast“.

Material-inhaltlich bezweckt diese klauselförmige Bestimmung damit zweierlei: Einerseits sollen schon die Darlegung „objektiver Hinweise“ auf die Einbindung eines Staates ausreichen, wofür zum anderen als Beleg bereits der Nachweis einer Beteiligung von „Gruppen oder Personen“ an der Cyber-Attacke ausreichen soll, die schon zuvor an „entsprechenden“ Akten des Staates beteiligt waren.[900] Während die Parteien die Darlegungs- und Beweislast schon angesichts der Dispositionsmaxime privatautonom untereinander verteilen können,[901] sind solche „Prozessverträge“ doch in bestimmte Leitplanken gefasst: Zunächst lässt sich Ziff. A1-17-2 AVB-Cyber 2024 womöglich als Beweis- bzw. Vermutungsvertrag oder auch als vertragliche Regelung der Beweiswürdigung und des Beweismaßes verstehen.[902] Derartige klauselförmige Gestaltungen in AVB unterliegen stets der AGB-Klauselkontrolle.[903] Hinzu kommt, dass selbst Individualvereinbarungen betreffend die Beweiswürdigung und das Beweismaß aufgrund des damit verbundenen Eingriffs in die gerichtliche Beurteilungssphäre unwirksam sind.[904]

Vor diesem Hintergrund mag man die Regelung als einen Vermutungs- bzw. Beweisvertrag verstehen: Danach wäre die Tatsache der staatlichen Urheberschaft/Involvierung gemäß Ziff. A1-17-2 AVB-Cyber 2024 dann als gegeben zu behandeln, sobald die Existenz „objektiver (IT-forensischer) Hinweise“ – und somit eine ganz andere, bloße Anknüpfungstatsache – dargelegt und ggf. bewiesen werden kann.[905] Diese Regelungstechnik lässt sich dabei treffend als „Anstaffelung“ beschreiben, weil nicht nur das prozessuale Beweisthema verschoben wird, sondern schon ein bloßer „Hinweis“ ausreichen soll, dass „eine Beteiligung von Gruppen oder Personen nachgewiesen werden kann, die in der Vergangenheit bereits an

900 Vgl. Ziff. A1-17-2 AVB-Cyber 2024.
901 Siehe nur *Wagner*, Prozessverträge, 1998, S. 89.
902 *Laumen* in: Baumgärtel/Prütting/Laumen, Handbuch der Beweislast, 5. Aufl. 2023, Bd. 1, Kap. 26 Rn. 30 ff. und Rn. 47 ff.
903 *Laumen* in: Baumgärtel/Prütting/Laumen, Handbuch der Beweislast, 5. Aufl. 2023, Bd. 1, Kap. 26 Rn. 26 ff.
904 Vgl. nur BGH NJW 1993, 1856, 1860 sowie m.w.N. *Laumen* in: Baumgärtel/Prütting/Laumen, Handbuch der Beweislast, 5. Aufl. 2023, Bd. 1, Kap. 26 Rn. 30.
905 Vgl. wiederum *Laumen* in: Baumgärtel/Prütting/Laumen, Handbuch der Beweislast, 5. Aufl. 2023, Bd. 1, Kap. 26 Rn. 47; *Wagner*, Prozessverträge, 1998, S. 649.

entsprechenden Handlungen dieses Staates beteiligt waren."[906] Die der Klausel zugrunde liegende „Mechanik" ist dabei dreischrittig: Kann im ersten Schritt die Tatsache der Beteiligung gewisser einschlägiger Personen oder Gruppen dargelegt und bewiesen werden, ist damit schon der zweiten Schritt gemacht und die Tatsache „objektiver Hinweis" belegt, was wiederum im dritten Schritt dazu führen soll, dass die Tatsache „staatliche Involvierung" i.S.d. Ziff. A1-17-2 AVB-Cyber 2024 als dargelegt und bewiesen zu gelten habe.[907] Das begegnet indes schon deshalb erheblichen Bedenken, weil diese Klausel noch nicht einmal den Beweis des Gegenteils vorsieht. Es wirkt indes befremdlich, wenn allein die Involvierung einer Person, die in der – womöglich lange zurückliegenden – Vergangenheit einmal in staatlichen Diensten stand und diese Kenntnisse nunmehr als „einfacher Cyber-Krimineller" einsetzt, fortan immer den Ausschlusstatbestand der Ziff. A1-17-2 AVB-Cyber 2024 erfüllen soll.[908] Bei dieser Gestaltung liegt schon angesichts der auch im unternehmerischen Verkehr i.R.d. § 307 BGB zu berücksichtigenden Wertung des § 309 Nr. 12 BGB das Verdikt einer unangemessenen Benachteiligung nach § 307 Abs. 1 S. 1, Abs. 2 Nr. 1 BGB besonders nahe.[909]

4. Darlegung und Beweis der staatlichen Provenienz der Cyber-Attacke: „Zuschreibung" und Klauselkontrolle

Nicht minder kritikwürdig erscheinen sodann die Regelungen zur Zuschreibung von ISV zu einem Staat nach Ziff. A1-17-2 AVB-Cyber 2024:

> *„Zuschreibung von Informationssicherheitsverletzungen, die durch einen Staat, im Auftrag oder unter Kontrolle eines Staates verursacht worden sind:*

---

906 *Lüttringhaus/Ettl*, VersR 2025, 649, 658 ff.
907 *Lüttringhaus/Ettl*, VersR 2025, 649, 659.
908 *Lüttringhaus/Ettl*, VersR 2025, 649, 659. Ähnlich auch *Rudkowski*, VersR 2024, 601, 609 unter Verweis auf das gängige Geschäftsmodell des „Cyber-Crime as a Service" (CaaS).
909 *Lüttringhaus/Ettl*, VersR 2025, 649, 659.

Bei der Feststellung der Zuschreibung an einen Staat trägt der Versicherer die Beweislast. Ungeachtet dessen können Versicherer und Versicherungsnehmer alle ihnen zur Verfügung stehenden objektiv angemessenen Beweismittel berücksichtigen. Unter allen rechtlich zulässigen Beweismitteln kann dies auch die offizielle Zuschreibung durch staatliche Stellen des Staates, dessen kritische Infrastrukturen durch die Informationssicherheitsverletzungen beeinträchtigt worden sind, an einen anderen Staat oder zu Gruppen oder Personen, die auf seine Anweisung oder unter seiner Kontrolle handeln, umfassen."

Vordergründig trägt die Darlegungs- und Beweislast zwar wiederum der Cyber-Versicherer. Dabei intendiert Ziff. A1-17-2 AVB-Cyber 2024 eine erhebliche Erleichterung der Darlegung – und im Bestreitensfall – auch des Beweises der staatlichen Urheberschaft einer Cyber-Attacke. Die Klausel setzt an der „Zuschreibung" an und stellt auf alle den Parteien „zur Verfügung stehende objektiv angemessene Beweismittel" ab. Soweit der Klauselersteller durch diese Formulierung zivilprozessuale Anforderungen durch einen Beweismittelvertrag zu modifizieren versucht, unterliegt eine solche AVB der Klauselkontrolle.[910] Angreifbar erscheint dann schon die Verengung auf die „*zur Verfügung stehenden*" Beweismittel, weil das sowohl als Erweiterung über den womöglich geltenden *Strengbeweis* hinaus als auch als eine Einschränkung der Beweismittel auf beiden Parteien („ihnen") gleichzeitig verfügbare Beweismittel verstanden werden könnte.[911]

Während hier noch der Rückgriff auf § 305c Abs. 2 BGB weiterhelfen mag, dürfte die klauselförmige Beschränkung auf „*objektiv angemessene* Beweismittel" der Klauselkontrolle zum Opfer fallen. Zunächst dürfte aus Sicht eines durchschnittlichen Versicherungsnehmers nicht erkennbar sein, dass es nach den AVB Cyber 2024 eine zivilprozessuale Kategorie von objektiv (un)angemessenen Beweismitteln i.R.d. Ziff. A1-17-2 AVB-Cyber 2024 gibt.[912] Offen

---

910 Vgl. statt vieler *Laumen* in: Baumgärtel/Prütting/Laumen, Handbuch der Beweislast, 5. Aufl. 2023, Bd. 1, Kap. 26 Rn. 27 ff. und insbesondere Rn. 29 und Rn. 18 ff.

911 *Lüttringhaus/Ettl*, VersR 2025, 649, 659 f.

912 Ebenso *Rudkowski*, VersR 2024, 601, 609.

bleibt damit insbesondere, wie sich „objektiv angemessene“ Beweismittel jeweils – je nach Art der (streitigen) Behauptung und des Verfahrens – zum zivilprozessualen Streng- oder Freibeweis verhalten sollen.[913] Die Verengung des Kreises der Beweismittel auf „*objektiv angemessene*“ ist schon deshalb intransparent und damit nach § 307 Abs. 1 S. 2 BGB unwirksam, weil der Versicherungsnehmer die Reichweite des Ausschlusses und folglich zugleich seinen Versicherungsschutz nicht überblicken kann.[914]

Transparenzbedenken begegnet auch die Regelung zur „Attribution“ in Ziff. A1-17-2 AVB-Cyber 2024, soweit es einer „offiziellen Zuschreibung durch staatliche Stellen“ bedarf: Als offizielle Stellen lassen sich – keineswegs abschließend – nämlich nicht nur Regierung, Militär, Nachrichtendienste und Ministerialebenen fassen, sondern potentiell alle Polizei- und Sicherheitskreise ungeachtet der jeweiligen Hierarchiestufe. Im Dunkeln bleibt zudem der erforderliche Grad an Gewissheit: Müssen die Aussagen klar belegt werden oder reichen bloße Mutmaßungen?[915] Hinzu kommt, dass Staaten womöglich eher dazu tendieren, eine Cyber-Attacke automatisch ihren jeweiligen (System)Gegnern zuzuschreiben und dabei die wahren Urheber aus diplomatischen und politischen Gründen verschweigen.[916] Angesichts der Vielzahl „offizieller“ Stellen eines Staates sind zudem auch innerhalb ein und desselben Staates widersprüchliche Zuschreibungen möglich. Die Wahrscheinlichkeit solcher Widersprüche steigt, wenn die kritische Infrastruktur *in mehreren Staaten* durch einen weit gestreuten Cyber-Angriff betroffen ist und die jeweiligen „offiziellen Stellen“ eine andere Auffassung vertreten. Während manche Klauseln darauf reagieren und einen bestimmten Staat priorisieren,[917] schweigen die AVB Cyber 2024 in

---

913 *Lüttringhaus/Ettl*, VersR 2025, 649, 659 f.

914 *Lüttringhaus/Ettl*, VersR 2025, 649, 660. Vgl. nur BGH VersR 2020, 692 Rn. 8; BGH VersR 2017, 1330 Rn. 13. Vgl. auch BGH NJW 2023, 1718 Rn. 30.

915 *Lüttringhaus*, VersR 2022, 1553, 1560.

916 *Lüttringhaus*, VersR 2022, 1553, 1560.

917 Vgl. dagegen die Lösung in den AVB eines Versicherers aus dem UK: „Bei widersprüchlichen Zuschreibungen innerhalb eines relevanten Staates ist die von der Regierung des jeweiligen Staates im Rahmen der offiziellen Kommunikation vorgenommene Zuschreibung maßgeblich. Bei widersprüchlichen Zuschreibungen zwischen verschiedenen relevanten Staaten ist die Zuschreibung durch den betroffenen Staat maßgeblich. Hat der betroffene Staat keine Zuschreibung vorgenommen, genügt die Zuschreibung durch einen relevanten Staat, auch wenn ein oder mehrere andere relevante Staaten diese nicht teilen oder ihr widersprechen“.

diesem Punkt. Viel spricht dafür, dass für einen durchschnittlichen Versicherungsnehmer insgesamt intransparent bleibt, wann eine „Zuschreibung" zu einem Staat i.S.d. Ziff. A1-17-2 AVB-Cyber 2024 erfolgen und damit der Risikoausschluss eingreifen kann. Das bedeutet zugleich, dass der Versicherungsnehmer den Umfang seines Cyber-Versicherungsschutzes gar nicht vollständig übersehen kann.[918] Davon abgesehen mag die sekundäre Risikobeschreibung in Ziff. A1-17-2 AVB-Cyber 2024 auch deshalb einer Inhaltskontrolle anheimfallen, weil sie auch willkürliche und wahrheitswidrige „Zuschreibungen" von Cyber-Attacken ohne Einschränkungen gelten lässt.[919] Das ist mit dem allgemeinen – und damit leitbildfähigen – Rechtsgedanken des § 317 Abs. 1 BGB bei der Bestimmungen durch Dritte kaum vereinbar, weil demnach auch eine Zuschreibung durch Dritte stets „nach billigem Ermessen" zu erfolgen hat. Nach der hier vertretenen Auffassung liegt deshalb eine unangemessene Benachteiligung i.S.d. § 307 Abs. 1 S. 1, Abs. 2 Nr. 2 BGB durch Ziff. A1-17-2 AVB-Cyber 2024 nahe.

5. Bedarf nach einer objektiven „Zuschreibung" bzw. „attribution"

Sowohl der in LMA 5564(a) bis 5567(a) gewählte und in Ziff. A1-17.2 a.E. AVB-Cyber 2024 rezipierte Ansatz zur „Zuschreibung" bzw. „*attribution*" von Cyber-Attacken zu einem Staat begegnet gerade im Lichte der AGB-Kontrolle Bedenken.[920] Staaten sind zwar dank ihrer Geheimdienste und Ermittlungsbehörden grundsätzlich gut informiert und damit in einer günstigen Ausgangsposition für die „*attribution*" einer Cyber-Attacke. Dennoch drohen hier diverse Unsicherheiten, wenn nicht gar offene Widersprüche, sofern – gerade bei breit gestreuten Angriffen – diverse Staaten für die „Zuschreibung" bzw. „*attribution*" in Frage kommen. Die Effektivität eines Risikoausschlusses sollte indes nicht von – potentiell willkürlichen,

---

[918] *Lüttringhaus*, VersR 2022, 1553, 1560; *Rudkowski*, VersR 2024, 601, 609 f.

[919] *Lüttringhaus/Ettl*, VersR 2025, 649, 660.

[920] Das gilt auch für den in der vorausgehenden Klauselgeneration aus dem November 2021 gewählten Ansatz in Ziff. 3 LMA 5564, Ziff. 4 LMA 5565, Ziff. 3 LMA 5566 und Ziff. 4 LMA 5567. Dazu eingehend *Lüttringhaus*, VersR 2022, 1553, 1560.

weil nicht an billiges Ermessen gebundenen – (Nicht)Zuschreibungen einer Cyber-Attacke abhängen: Denn legt man die „*attribution*“ in staatliche Hand, so können und werden immer politische und diplomatische Motive dazu führen, dass ein Staat entweder besonders aggressiv auf einen vermeintlichen Urheber einer Cyber-Attacke zeigt oder – ganz im Gegenteil – aus diplomatischen Erwägungen bei Zuschreibung äußerste Zurückhaltung übt.[921] Weder aus Sicht des Cyber-Versicherers noch aus der des Versicherungsnehmers erscheint es sinnvoll, das Bestehen des Deckungsschutzes von solchen außerhalb des Versicherungsverhältnisses stehenden Zufälligkeiten abhängig zu machen.

Die „Zuschreibung“ bzw. „*attribution*“ sollte vor diesem Hintergrund so weit wie möglich objektiviert werden: Eine rechtssichere Zuschreibung einer Cyber-Attacke könnte etwa durch die Schaffung einer objektiven nicht-staatlichen Stelle erreicht werden, die alle verfügbaren Informationen aggregiert und zeitnah eine Entscheidung nach „billigem Ermessen“ trifft.[922] Den meisten gegenüber der „Zuschreibungs“-Konzeption in LMA 5564(a) bis 5567(a) und in Ziff. A1-17.2 a.E. AVB-Cyber 2024 geäußerten Bedenken ließe sich dadurch begegnen, dass die Einschätzung dieser Stelle für maßgeblich erklärt wird. Ein solcher objektiver Ansatz liegt nicht zuletzt im Interesse des Cyber-Versicherers, der die Voraussetzungen des Risikoausschlusses im Streitfall darlegen und beweisen muss und dabei – wie gezeigt – nicht auf die in Ziff. A1-17.2 a.E. AVB-Cyber 2024 vorgesehenen klauselförmigen Erleichterungen wird bauen können.[923]

---

921 *Lüttringhaus*, VersR 2022, 1553, 1560.

922 *Lüttringhaus*, VersR 2022, 1553, 1560.

923 Vgl. erneut oben III 4 und III 5. Vgl. zum Problem des Beweises der Urheberschaft einer Cyber-Attacke nur schweizerisches Bundesgericht 17.8.2023 – 4A_206/2023.

IV. Weitere Ansätze zur Vermeidung von Cumul-Risiken im Cyber-Bereich: „Widespread Event“ und „Territorial Exclusions“

Cyber-Versicherer haben darüber hinaus weitere Instrumente entwickelt, um den mit der weltweiten Verbreitung von Schad-Code potentiell verbundenen Cumul-Risiken zu begegnen: Als Beispiele aus jüngerer Zeit lassen sich zum einen Klauseln zu „weiterverbreiteten Ereignissen (widespread event)“(**dazu unter 1**) sowie zum anderen territoriale Ausschlussklauseln nennen, die potentiell von (halb) staatlichen Cyber-Attacken besonders betroffene Konfliktregionen vom Deckungsschutz ausnehmen (**dazu unter 2**). Beide Gestaltungen begegnen indes jeweils Bedenken im Rahmen der AGB-Klauselkontrolle.

1. „Weiterverbreitetes Ereignis“ und die AGB-Klauselkontrolle

Vereinzelt suchen Cyber-Versicherer ihre Exposition gegenüber Cumul-Risiken dadurch zu begrenzen, dass der Umfang des Cyber-Versicherungsschutzes anhand der – sachlichen wie auch territorialen – Auswirkungen einer Cyber-Attacke eingeschränkt wird: Zu diesem Zweck wird jede Informationssicherheitsverletzung entweder als „Ereignis mit begrenzter Auswirkung“ oder als „weitverbreitetes Ereignis“ eingestuft. Handelt es sich um ein „weitverbreitete Ereignis“, so greifen besondere vertragliche Restriktionen, insbesondere in Form von Sublimits, Selbstbeteiligung und Selbstbehalt. Die Definitionen der jeweiligen Ereignisse lauten dabei im Ausgangspunkt wie folgt:

> *„Ein Ereignis mit begrenzter Auswirkung ist ein Cyber-Vorfall … und/oder eine Datenschutz- und Netzwerksicherheitsverletzung, die nicht auf einen weitverbreiteten Auslöser zurückzuführen ist.“*

„Weitverbreitetes Ereignis bezeichnet einen Cyber-Vorfall … und/oder eine Datenschutz- und Netzwerksicherheitsverletzung, die auf einen weitverbreiteten Auslöser zurückzuführen ist."

Der „weitverbreitete Auslöser" wird sodann im Wesentlichen als eine Informationssicherheitsverletzung definiert, die ihren Ursprung außerhalb des cyberversicherten Unternehmens hat und nicht nur dieses betrifft, sondern auch Akteure „außerhalb der Gruppe Betroffener eines Ereignisses mit begrenzter Auswirkung". Zu letzterer Gruppe zählen in erster Linie die unter dem Cyber-Versicherungsvertrag versicherten Unternehmen sowie alle juristischen und natürlichen Personen, die direkt oder indirekt mit den versicherten Unternehmen Geschäftsbeziehungen unterhalten und just aufgrund dieser Geschäftsbeziehung von einer Informationssicherheitsverletzung betroffen sind.

Im Ergebnis führt diese Charakterisierung des „weitverbreiteten Ereignisses" dazu, dass der Cyber-Versicherungsschutz nicht nur im Haftpflichtbaustein, sondern auch in den anderen Deckungsbausteinen nur – un(sub)limitiert und ohne weitere Restriktionen wie höhere Selbstbehalte – besteht, wenn der Kreis der von einer Informationssicherheitsverletzung Betroffenen sich auf (mittelbare) Geschäftskontakte der Versicherten beschränkt. Aus der Reihe der sowohl an der Unklarheitenregel des § 305c Abs. 2 BGB als auch am Transparenzgebot des § 307 Abs. 1 S. 2 BGB zu messenden Fragen seien an dieser Stelle nur die Natur und Aktualität der – im Bedingungswerk nicht weiter definierten – „direkten oder indirekten Geschäftsbeziehung" genannt: Muss diese bereits zu einem Vertragsschluss geführt haben oder reicht auch ein sonstiger Geschäftskontakt, der nur der Anbahnung dient? Sind mit Geschäftsbeziehung nur aktuell bestehende „aktive" oder auch schon Jahre zurückliegende „passive" Kontakte gemeint? Sofern Letzteres zutreffen sollte, wäre weiterhin zu fragen, wie lange eine solche „Geschäftsbeziehung" dann zurückliegen darf. Ähnliche Fragen wären auch mit Blick auf die Kausalbeziehung zu stellen: Wann entsteht eine Informationssicherheitsverletzung „ausschließlich aufgrund dieser Geschäftsbeziehung"? Muss es sich um gezielten Da-

ten- bzw. Informationsaustausch in Erfüllung von Verbindlichkeiten handeln oder reichen z.B. auch mit Schad-Code infizierte werbliche E-Mails o.Ä., die Jahre nach Abwicklung der letzten vertraglichen Beziehungen versandt werden? Vor diesem Hintergrund dürfte es für den um möglichst umfassenden und un(sub)limitierten Versicherungsschutz bemühten Versicherungsnehmer kaum im Vorhinein erkennbar sein, wann ungeschmälerter Cyber-Versicherungsschutz besteht. Obschon eine detaillierte Analyse des gesamten Klauselwerkes den Rahmen dieser Abhandlung sprengen würde, bleiben aus Sicht eines gewerblich tätigen und um Verständnis bemühten Cyber-Versicherungsnehmers doch derart viele Fragen, die sich weder aus dem AVB-Gefüge selbst noch unter Zuhilfenahme der Unklarheitenregel des § 305c Abs. 2 BGB aufklären lassen, dass hier die Intransparenz dieser Klauselgestaltung nach § 307 Abs. 1 S. 2 BGB naheliegt. Hinzu kommt, dass ein durchschnittlicher – auch gewerblich tätiger – Cyber-Versicherungsnehmer kaum damit rechnen dürfte, dass sein Versicherungsschutz für Eigen- und insbesondere Betriebsunterbrechungsschäden von Zufälligkeiten wie der Frage abhängen soll, ob der Schad-Code nun allein das eigene Unternehmen und dessen Geschäftskontakte trifft oder aber – wie wohl bei breit gestreuter (Ransom)-Malware üblich – auch außenstehende Dritte beeinträchtigt. Selbst wenn – wie in dem hier diskutierten Klauselwerk – nur Sublimitierungen und höhere Selbstbehalte im Raum stehen, so lässt sich doch eine inhaltliche Missbräuchlichkeit wegen einer ungerechtfertigten Benachteiligung entgegen Treu und Glauben i.S.d. § 307 Abs. 1 S. 1 i.V.m. Abs. 2 Nr. 2 BGB kaum ausschließen.

Dabei ist die Eingrenzung des Deckungsversprechens auf bestimmte Cyber-Angriffsszenarien womöglich nicht von vornherein aussichtslos: Beispielsweise hat der Unionsgesetzgeber selbst in Art. 6 Nr. 7 NIS-2-RL einen „Cybersicherheitsvorfall großen Ausmaßes“ definiert, der Informationssicherheitsverletzungen in einem solchen Ausmaß versursacht, dass dies „die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder … beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat“. Dies führt in die Nähe der KRITIS-Lösung, wie sie in manchen „Cyber-Operations“-Ausschlüssen der LMA und nun auch in den AVB Cyber 2024 zugrunde gelegt

wird.[924] Obwohl auch dieser KRITIS-Ansatz Bedenken ausgesetzt ist, könnte gerade die besonders schwere Beeinträchtigung kritischer Infrastruktur in (mehr als) einem EU-Mitgliedstaat womöglich ein tauglicheres, weil leichter objektivier- und beweisbares Anknüpfungskriterium bilden als die Kategorie des „weitverbreiteten Ereignisses".

2. Territoriale Ausschlüsse und internationale Cyber-Versicherung

Soweit territoriale Ausschlüsse schon bislang in Cyber-Versicherungsverträgen vorgesehen worden sind, bezogen sich diese zumeist auf den Haftpflichtbaustein und dort namentlich auf Haftpflichtansprüche, die infolge eines Cyber-Incidents vor den Gerichten und/oder nach dem Recht der USA bzw. der US-Bundesstaaten geltend gemacht werden.[925] Nunmehr werden nicht zuletzt infolge des Russland-Ukraine-Konflikts weitergehende „territorial exclusions" vorgesehen, wobei die nachfolgende Musterklausel der LMA vom 8.3.2023 (LMA5583B) als Beispiel dienen mag:

> *„(T)his Policy excludes any loss, damage, liability, cost or expense of whatsoever nature, directly or indirectly arising from or in respect of any:*
>
> *i. entity domiciled, resident, located, incorporated, registered or established in an Excluded Territory;*
>
> *ii. property or asset located in an Excluded Territory;*
>
> *iii. individual that is physically in an Excluded Territory;*

[924] Vgl. dazu erneut eingehend oben II und III.

[925] Hierauf zielt auch vornehmlich das – wie dargelegt nicht unproblematische – Wording in Ziff. A1-11 AVB Cyber 2024 ab: „Versicherungsschutz besteht für Versicherungsfälle weltweit. Dies gilt jedoch nur, soweit die Ansprüche in EWR-Staaten und nach deren Recht geltend gemacht werden.".

iv. claim, action, suit or enforcement proceeding brought or maintained in an Excluded Territory;

v. payment in an Excluded Territory …

For purposes of this exclusion, „Excluded Territory" means:

– *Belarus (Republic of Belarus); and*

– *Russian Federation; and*

– *Ukraine (including any disputed regions of Ukraine and including the Crimean Peninsula)."*[926]

Die unbesehene Übertragung dieses Ausschlusses in Cyber-Versicherungsverträge, die deutschem Recht unterliegen, dürfte wiederum erheblichen Bedenken sowohl im Rahmen der Transparenz- als auch der Inhaltskontrolle begegnen: Denn die Formulierung „direkt oder indirekt zurückzuführen auf oder bezogen auf jedwede (*directly or indirectly arising from or in respect of any*)" lässt zum einen bereits nicht erkennen, welcher Natur die Kausalbeziehung zu dem „ausgeschlossenen Gebiet (*excluded territory*)" sein muss, um den Tatbestand des Ausschlusses zu erfüllen. Dem Wortlaut nach dürfte es beispielsweise bereits ausreichen, dass eine mit dem Cyber-Versicherungsnehmer völlig unverbundene Entität aus einem solchen Gebiet Schad-Code weiterleitet oder derartiger Schad-Code zumindest auch über im „*excluded territory*" lokalisierte Server verbreitet wird. Das dürfte schon für sich genommen eine ungerechtfertigte Benachteiligung entgegen Treu und Glauben i.S.d. § 307 Abs. 1 S. 1 i.V.m. Abs. 2 Nr. 2 BGB darstellen: Denn angesichts der üblichen Ursprungsorte und Verbreitungswege von Malware liegt es nahe, dass im Fall des in LMA5583B vorgesehenen territorialen Ausschlusses von Russland, Belarus und Ukraine der Cyber-Versicherungsschutz insgesamt entwertet wird.

Wohl nicht zuletzt vor diesem Hintergrund haben manche Cyber-Versicherer ihre Territorial-Ausschluss-Klauseln um einen Zusatz

926 LMA5583B v. 8.3.2023.

ergänzt, der eine solche Aushöhlung des Deckungsversprechens zu vermeiden sucht. Danach gelten die territorialen Ausschlüsse

> *„nicht für Tätigkeiten in einem anderen Land als der Ukraine, Russland oder Weißrussland bei Datenmissbrauch oder Datenbeschädigung, die ihren Ursprung in der Ukraine, Russland oder Weißrussland haben."*

V. Ergebnis

Ebenso wie andere an NMA 464 orientierte Kriegs-Ausschlussklauseln erfasste die ursprüngliche Formulierung der Ziff. A1-17.2 AVB-Cyber a.F. (2017) das Szenario eines reinen „Cyber-Krieges" bereits mangels der begrifflich für einen „klassischen" Krieg erforderlichen physischen Gewaltanwendung nicht.

Eine wortlautgetreue Übersetzung der LMA-Musterklauseln dürfte für den deutschen Markt weder in der ursprünglichen (LMA 5564 bis 5567) noch in der überarbeiteten Fassung (LMA 5564(a,b) bis 5567(a,b)) dieser Kriegs-Ausschlussklauseln eine tragfähige Lösung bieten. Transparenzbedenken begegnet etwa die Formulierung des erforderlichen Grades staatlicher Involvierung, der Belegenheit des „Computersystems" sowie vor allem die Regelung zur „Attribution" von Cyber-Attacken, wobei letztere Klausel zudem kaum einer Inhaltskontrolle standhalten dürfte.

Unter dem Gesichtspunkt der AGB-Kontrolle begegnen nun auch viele Aspekte des Ausschlusses von „Krieg und staatlichen Angriffen" nach Ziff. A1-17.2 AVB-Cyber 2024 Bedenken: So könnte durch Ziff. A1-17-2 lit. b) AVB Cyber 2024 eine Aushöhlung des Cyber-Versicherungsschutzes i.S.d. § 307 Abs. 1 S. 1, Abs. 2 Nr. 2 BGB drohen, weil das Eindringen von weit ausgestreuter Schad-Software in KRITIS-Infrastrukturen *irgendwo auf der Welt* kaum je auszuschließen ist. Der Cyber-Versicherer könnte die Deckung womöglich unter Verweis auf eine „Beeinträchtigung" kritischer Infrastruktur in einem beliebigen Staat nach Ziff. A1-17-2 lit. b) verwei-

gern, wenn dort nur die Vertraulichkeit von Daten Ziff. A1-2.1 AVB Cyber 2024 kompromittiert worden ist.

Das Verdikt der Missbräuchlichkeit dieser Klauselgestaltung dürfte gerade in der Zusammenschau mit den weiteren Regelungen in Ziff. A1-17-2 AVB Cyber 2024 Bestand haben, weil dort die Darlegung der weiteren Voraussetzungen des Ausschlusses wie insbesondere die Zuschreibung der Cyber-Attacke zu einem Staat erleichtert wird. Ziff. A1-17-2 AVB-Cyber 2024 ist insoweit dreischrittig aufgebaut: Wird im ersten Schritt die Tatsache der Beteiligung gewisser einschlägiger Personen oder Gruppen dargelegt und bewiesen, soll automatisch im zweiten Schritt die Tatsache „Hinweis“ und damit zugleich auch im dritten Schritt die Tatsache „staatliche Involvierung“ i.S.d. Ziff. A1-17-2 AVB-Cyber 2024 als dargelegt und bewiesen gelten. In dieser Gestaltung dürfte – insbesondere wegen der fehlenden Möglichkeit eines Gegenbeweises – eine unangemessene Benachteiligung nach § 307 Abs. 1 S. 1, Abs. 2 Nr. 1 BGB wegen eines Abgehens von grundlegenden Prinzipien der Darlegungs- und Beweislast liegen. Dabei ist nicht zuletzt zu beachten, dass die grundsätzliche Wertung des § 309 Nr. 12 BGB auch im unternehmerischen Verkehr i.R.d. § 307 BGB zu berücksichtigen ist.

Zudem dürfte die allgemeine Einschränkung auf „objektiv angemessene Beweismittel“ gegen das Transparenzgebot nach § 307 Abs. 1 S. 2 BGB verstoßen, weil völlig im Dunkeln bleibt, wie sich derartige Beweismittel jeweils – je nach Art der (streitigen) Behauptung und des Verfahrens – zum zivilprozessualen Streng- oder Freibeweis verhalten sollen. Schließlich erscheint auch die Regelung zur Zuschreibung in Ziff. A1-17-2 AVB-Cyber 2024 unter Transparenzgesichtspunkten angreifbar: Bedenken begegnet bereits die Forderung einer „offiziellen Zuschreibung durch staatliche Stellen“, weil hierunter neben Regierung, Militär, Nachrichtendiensten sowie Ministerial- und Sicherheitsbeamten ganz unterschiedliche „offizielle“ Quellen auf sehr unterschiedlichen Hierarchiestufen in Betracht kommen.

Die „Zuschreibung“ bzw. „*attribution*“ sollte vor diesem Hintergrund so weit wie möglich objektiviert werden: Eine rechtssichere Zuschreibung einer Cyber-Attacke könnte etwa durch die Schaffung

einer objektiven nicht-staatlichen Stelle erreicht werden, die alle verfügbaren Informationen aggregiert und zeitnah eine Entscheidung nach „billigem Ermessen“ trifft.[927] Den meisten gegenüber der „Zuschreibungs“-Konzeption in LMA 5564(a) bis 5567(a) und in Ziff. A1-17.2 a.E. AVB-Cyber 2024 geäußerten Bedenken ließe sich dadurch begegnen, dass die Einschätzung dieser Stelle für maßgeblich erklärt wird. Ein solcher objektiver Ansatz liegt nicht zuletzt im Interesse des Cyber-Versicherers, der die Voraussetzungen des Risikoausschlusses im Streitfall darlegen und beweisen muss und dabei – wie gezeigt – nicht auf die in Ziff. A1-17.2 a.E. AVB-Cyber 2024 vorgesehenen klauselförmigen Erleichterungen wird bauen können.

Der Bedarf nach einer rechtssicheren Gestaltung des Ausschlusses für Cyber-Attacken im Rahmen eines „Krieges“ und sog. „Cyber-Operations“ besteht nicht zuletzt auch deshalb weiterhin, weil die in Praxis anzutreffenden alternativen Mechanismen zur Eindämmung von Cyber-Cumul-Risiken – wie die Kategorie des „weiterverbreiteten Ereignisses“ und territorialer Ausschlüsse – ebenfalls erheblichen Transparenzbedenken begegnen.

[927] *Lüttringhaus*, VersR 2022, 1553, 1560.

G. Zusammenfassung der Ergebnisse

I. Cyber-Versicherungsvertragsstatut und international-privatrechtliche Grundlagen

Auch bei Deckungsstreitigkeiten im Rahmen von Cyber-Versicherungsverhältnissen ist das international zuständige Gericht zuvörderst anhand der in marktgängigen Cyber-Bedingungswerken üblichen Gerichtsstandsklauseln zu bestimmen.[928] Nur wenn eine Gerichtsstandsvereinbarung fehlen oder den Anforderungen des Art. 25 Brüssel Ia-VO nicht genügen sollte, ist auf die allgemeinen Regelungen zur internationalen Gerichtszuständigkeit und damit insbesondere auf Art. 11 ff. Brüssel Ia-VO zurückzugreifen.[929]

Das auf einen Cyber-Versicherungsvertrag in Sachverhalten mit Auslandsbezug anwendbare Recht bestimmt ein international zuständiges deutsches Gericht nach den allgemeinen Kollisionsnormen der Rom I-VO: Während der Rahmen der Parteiautonomie bei Großrisiken weiter gesteckt ist, wird die übliche Rechtswahl im Fall von Massenrisiken nicht nur in die Grenzen von Art. 3 Abs. 3 und Abs. 4, sondern auch in jene des Art. 7 Abs. 3 Rom I-VO gefasst, was etwa bei cyber-versicherten KMU unterhalb der Großrisiko-Schwelle Bedeutung erlangt.[930]

Cyber-Versicherungsverträge, die Risiken in mehreren Staaten decken, können besondere praktische wie rechtliche Herausforderungen mit sich bringen, etwa wenn es um die als Obliegenheit formulierte Einhaltung von IT-Sicherheitsvorschriften geht: So mag es z.B. Transparenzbedenken begegnen, wenn der Versicherungsnehmer nach Ziff. A1-16.2 lit. a AVB-Cyber 2024 an „alle gesetzlichen, behördlichen sowie vertraglich vereinbarten Sicherheitsvorschriften“ gebunden wird, ohne dass der Kreis dieser nationalen Regelungen sachlich und vor allem auch räumlich-territorial präzisiert wird.[931] Das Versicherungsverhältnis kann darüber hinaus

928 Siehe oben B I 1.
929 Siehe oben B I 2.
930 Siehe oben B II.
931 Siehe oben B II 1 c).

auch durch besondere kollisions- und/oder sachrechtliche Vorgaben beeinflusst werden, etwa falls künftig eine Cyber-Versicherungspflicht erlassen würde.[932] Darüber hinaus mögen insbesondere in- und ausländische Eingriffsnormen Einfluss darauf nehmen, ob bestimmte Deckungszusagen – z.B. für Lösegelder oder Geldbußen – rechtlich zulässig und im Streitfall auch gerichtlich durchsetzbar sind.[933]

II. Internationale Cyber-Haftpflicht und Verbindungslinien zur Cyber-Haftpflichtdeckung

Wer sich im Cyberspace bewegt, läuft Gefahr, sich Dritten gegenüber haftpflichtig zu machen: Zu denken ist beispielsweise an Szenarien, in denen Angreifer ein Unternehmen mit Malware attackieren und das Unternehmen den Schad-Code sodann in haftungsrelevanter Weise an seine Zulieferer, Abnehmer oder auch an unbeteiligte Dritte weiterleitet und diese dadurch schädigt. Aus Sicht des unionalen ebenso wie des deutschen Rechts kommen als haftungsbegründende Normen neben (vor)vertraglichen und deliktischen auch eine Reihe spezialgesetzlicher Tatbestände, wie Art. 82 DSGVO und § 10 GeschGehG, in Betracht.[934] Viele Unternehmen haben ihre Wertschöpfungsketten grenzüberschreitend vernetzt, so dass auch die Haftungsverhältnisse dem Recht unterschiedlicher ausländischer Staaten unterliegen können. Welches Recht im Einzelfall anwendbar und welches Gericht für Haftpflichtstreitigkeiten international zuständig ist, bestimmt das internationale Privat- und Zuständigkeitsrecht. Besondere Herausforderungen ergeben sich hier jeweils daraus, dass bei Cyber-Attacken ebenso wie bei der (fahrlässigen) Weiterverbreitung von Schad-Code sog. Streuschäden in vielen verschiedenen Staaten eintreten können.

Auf Ebene der Gerichtszuständigkeit sollte i.R.d. Deliktsgerichtsstands nach Art. 7 Nr. 2 Brüssel Ia-VO bei Cyber-Incidents zu-

[932] Siehe oben B II 2.
[933] Siehe oben B II 3.
[934] Siehe oben C I.

nächst ein Erfolgsort am „Mittelpunkt der Interessen“ des Geschädigten anerkannt werden.[935] Während am Handlungsort des Schädigers stets der Gesamtschaden eingeklagt werden kann, soll laut EuGH bei Streuschäden am jeweiligen Erfolgsort grundsätzlich nur der dort eingetretene Teilschaden zu liquidieren sein.[936] Daraus folgt bei der Einschleusung und Weiterverbreitung von Malware in der IT-Infrastruktur internationaler Unternehmen ein potentiell riesiges „Mosaik“ aus einzelnen Erfolgsorten, an denen das betroffene Unternehmen seine jeweiligen Teilschäden sodann mit großem Aufwand einzeln gerichtlich durchsetzen müsste. Noch weitaus komplexer wird das Bild durch die mittlerweile üblichen Cloud-Lösungen: Hier werden einheitliche Datenbestände auf diverse und – je nach Anbieter – europa- oder weltweit verstreute Server je nach verfügbarer Speicherkapazität fragmentweise verteilt und gespeichert. Lokalisiert man hier nun den Erfolgsort am jeweils zur Datenspeicherung verwendeten Server, wo Datenfragmente durch den Cyber-Angriff konkret betroffen sind, würde die Zuständigkeit unnötig zersplittert, obwohl das Gericht am jeweiligen – aufgrund der Funktionsweise einer Cloud: arbiträren – Speicherort keine besondere Sach- oder Beweisnähe aufweist. Bei grenzüberschreitender Geltendmachung von Cyber-Haftpflichtansprüchen sollte deshalb i.R.d. Art. 7 Nr. 2 Brüssel Ia-VO ein Gerichtsstand am „Mittelpunkt des Interesses“ des geschädigten Unternehmens entsprechend der durch den EuGH in den Rechtssachen *eDate und Martinez* und *Svensk Handel* entwickelten Maßstäbe begründet werden. Dieser „Mittelpunkt des Interesses“ deckt sich in der Regel mit dem Ort der Hauptverwaltung.

Auch im internationalen Privatrecht der Cyber-Haftpflicht führt die Grundanknüpfung außervertraglicher Ansprüche an den Erfolgsort nach Art. 4 Abs. 1 Rom II-VO potentiell zu einer Multiplikation der anwendbaren Rechte: Gerade beim Einsatz von Cloud-Computing-Diensten sowie z.B. bei weltweit tätigen Vertriebs- und Außendienstmitarbeitern und der engen Vernetzung der IT entlang der Wertschöpfungskette kann ein einheitlicher Cyber-Vorfall zahlreiche

[935] Siehe oben C II.
[936] Grundlegend EuGH 7.3.1995 – Rs. C-68/93 (*Shevill*) ECLI:EU:C:1995:61 Rn. 33.

Primärschadensorte am Sitz der jeweiligen Geschäftskontakte begründen. Für das Kollisionsrecht der Cyber-Haftpflicht gegenüber Unternehmen erscheint hier eine Lösung in Parallele zur internationalen Zuständigkeit erstrebenswert: Nach den Grundsätzen der *Svensk Handel*-Entscheidung des EuGH sollte eine Konzentration auf das Recht am „Mittelpunkt des Interesses" des Geschädigten nach Art. 4 Abs. 3 Rom II-VO erfolgen, wobei dies bei betroffenen Unternehmen regelmäßig zu deren Hauptsitz führen dürfte.[937] Hierfür sprechen neben der Vorhersehbarkeit für den Schädiger auch die Sach- und Beweisnähe, weil am Hauptsitz angesichts des Erfordernisses einer unternehmensweiten IT-Sicherheitsstrategie und der Reporting-Wege üblicherweise alle Informationen zu einem Cyber-Incident zusammenlaufen. Darüber hinaus kann so ein weitgehender Gleichlauf von internationaler Zuständigkeit und anwendbarem Recht erreicht werden, was die Rechtsermittlungs- und Rechtsanwendungskosten reduziert und die Rechtsdurchsetzung insgesamt beschleunigen und vereinfachen dürfte.

Cyber-Incidents können auch zu Datenschutzverstößen und damit zu Ansprüchen einer Vielzahl von betroffenen natürlichen Personen führen. Gerade wenn die IT-Systeme von global agierenden Online-Händlern, Airlines, Hotelketten oder Social-Media-Plattformen betroffen sind, bilden grenzüberschreitende Sachverhalte den Regelfall. Dann drängt sich die international-privatrechtliche Frage auf, welches nationale Recht in solchen grenzüberschreitenden Konstellationen anzuwenden ist.[938] Schließlich bleibt selbst der unionsrechtlich-autonome Tatbestand des Art. 82 DSGVO lückenhaft und bedarf hinsichtlich so zentraler Fragen wie Verschuldensmaßstab, Mitverschulden, Verjährung und Schadensbemessung der Ergänzung durch das nationale Privatrecht. Welches nationale Zivilrecht in Sachverhalten mit Auslandsbezügen anwendbar ist, muss anhand des Kollisionsrechts ermittelt werden. Dabei ist umstritten, ob die Rom II-VO auf Ansprüche infolge von Datenschutzverletzungen anwendbar ist. Die besseren historisch-teleologischen ebenso wie auch systematischen Argumente sprechen hier für ei-

[937] Siehe oben C III 1 c).
[938] Siehe oben C III 2.

ne restriktive Auslegung der Bereichsausnahme in Art. 1 Abs. 2 lit. g Rom II-VO, so dass es keines Rückgriffs auf nationale Kollisionsnormen, wie Art. 40 ff. EGBGB, bedarf. Die nicht in Art. 82 DSGVO geregelten und damit der Ergänzung durch nationales Recht bedürftigen Rechtsfragen können damit nach der Rom II-VO angeknüpft werden.[939] Nach der hier vertretenen Ansicht sollte der Erfolgsort bei DSGVO-Verstößen infolge von Cyber-Incidents – wiederum in Anlehnung an die zuständigkeitsrechtlichen Erwägungen des EuGH in der Rechtssache *eDate und Martinez* –[940] konzentriert werden können: Eine solche Schwerpunktbetrachtung ermöglicht Art. 4 Abs. 3 Rom II-VO im Fall einer offensichtlich engeren Verbindung zum Recht des Staates, an dem der Geschädigte den „Mittelpunkt seiner Interessen" hat. Der infolge einer Cyber-Attacke Betroffene sollte seinen gesamten Schaden nach dem Erfolgsortrecht des EU-Mitgliedstaates geltend machen können, in dem ebendieser „Mittelpunkt seiner Interessen" liegt. Dieser Interessenschwerpunkt wird bei der Haftung für Datenschutzverstöße regelmäßig am gewöhnlichen Aufenthalt des Betroffenen zu lokalisieren und somit das dortige Recht anwendbar sein, was angesichts des Aufenthaltsgerichtsstandes in Art. 79 Abs. 2 S. 2 DSGVO einen Gleichlauf von *forum und ius* ermöglicht.

Bei der grenzüberschreitenden Haftung infolge von Cyber-Vorfällen, die durch die Nichteinhaltung von IT-Sicherheitsstandards verursacht werden, kann es zu einem „Rechtsmix" kommen, weil gemäß Art. 17 Rom II-VO die „Sicherheits- und Verhaltensregeln" am Handlungsort des Schädigers auch ungeachtet der nach den allgemeinen Kollisionsnormen ermittelten *lex causae* „berücksichtigt" werden können.[941] Darüber hinaus mögen in vertraglichen Schuldverhältnissen sowie bei der Frage eines etwaigen Mitverschuldens des Geschädigten die jeweiligen lokalen Cyber-Sicherheitsstandards grundsätzlich ebenfalls (analog Art. 17 Rom II-VO) als *local data*

939 Siehe oben C III 2 b).

940 Vgl. EuGH 25.10.2011 – verb. Rs. C-509/09 und C-161/10 (*eDate Advertising und Martinez*) ECLI:EU:C:2011:685 Rn. 52 ff. sowie sodann auch EuGH 17.10.2017 – Rs. C-194/16 (*Svensk Handel*) ECLI:EU:C:2017:766 Rn. 30 ff.; EuGH 17.6.2021 – Rs. C-800/19 (*Mittelbayerischer Verlag*) ECLI:EU:C:2021:489 Rn. 24 ff.; EuGH 21.12.2021 – Rs. C-251/20 (*Gtflix Tv/DR*) ECLI:EU:C:2021:1036 Rn. 31 und 39.

941 Siehe oben C IV.

herangezogen werden. Der Anwendungsbereich des Art. 17 Rom II-VO wird indes vor allem durch unionsrechtliche Vorgaben und insbesondere durch den in Art. 3 DSGVO und in Art. 2 Abs. 1 NIS-2-RL abgesteckten räumlich-territorialen Anwendungsbereich der EU-Cyber-Sicherheitsstandards begrenzt. Dies steht einer „Berücksichtigung" drittstaatlicher Standards an einem Handlungsort außerhalb der EU über Art. 17 Rom II-VO entgegen. Darüber hinaus dürften viele mitgliedstaatliche Cyber-Sicherheitsstandards auch Eingriffsnormcharakter haben. Zumindest grundsätzlich bleibt ein ergänzender Rückgriff auf Art. 17 Rom II-VO in Intra-EU-Konstellationen möglich, soweit hier jedenfalls die Einhaltung des unionsrechtlich vorgegebenen (Mindest)Cyber-Sicherheitsniveaus unter der NIS-2-RL bzw. der DSGVO gewährleistet ist. Infolge der Teilharmonisierung in diesem Bereich durch die DSGVO bzw. die NIS-2-RL haben sich die mitgliedstaatlichen Cyber-Sicherheitsstandards zumindest stark angenähert. Impulse liefert hier die Rechtsprechungslinie des EuGH in den Rechtssachen *Unamar* und *HUK COBURG II*, obschon der Gerichtshof es einem EU-Mitgliedstaat nicht prinzipiell verwehrt, sein EU-Richtlinien- bzw. EU-Verordnungsvorgaben übertreffendes Recht gegenüber den großzügigeren Standards anderer EU-Mitgliedstaaten durchzusetzen.

Angesichts des – insbesondere im Kontext des Art. 82 DSGVO und des Art. 17 Rom II-VO – stets möglichen „law mix" auf der Haftpflichtseite werden zugleich die Schwächen des in Ziff. A1-11 AVB Cyber 2024 für die Deckungsseite gewählten Ansatzes deutlich: Wird der Versicherungsschutz für potentiell weltumspannende Cyber-Risiken von der Gerichtszuständigkeit und dem anwendbaren Recht in EWR-Staaten abhängig gemacht, so stellt dies die Rechtsanwender vor große praktische und international-privatrechtliche Herausforderungen.

III. Versicherbarkeit von Geldbußen wegen Verstößen gegen Cybersicherheits- und Datenschutzbestimmungen

Im internationalen Vergleich wird die Frage der Versicherbarkeit von Geldbußen durchaus unterschiedlich beantwortet. Die rechtsvergleichende Umschau offenbart, dass nur wenige Rechtsordnungen explizite Versicherungsverbote aufstellen – wie z.B. Italien in Form des Art. 12(1) *Codice delle Assicurazione Private* –, zahlreiche Jurisdiktionen aber allgemeine Grundsätze – wie die *illegality defence* (*ex turpi causa*) – oder auch *ordre-public*- bzw. *public-policy*-Erwägungen gegenüber Geldbußendeckungen in Stellung bringen.[942] Das Bild ist hier gerade in den US-Bundesstaaten jedoch keineswegs einheitlich,[943] und auch der Blick auf einzelne EU-Mitgliedstaaten offenbart häufig erhebliche Rechtsunsicherheit. Dies führt zur Frage, wie in grenzüberschreitenden Konstellationen mit potentiellen Verboten von Geldbußendeckungen umzugehen ist.

Anders als manche Geldbußen-Klauseln in Cyber-Versicherungsverträgen suggerieren, lässt sich die Frage der Durchsetzung solcher Deckungsversprechen keineswegs vertraglich auf bestimmte Rechtsordnungen beschränken: Im Deckungsstreit wird ein international zuständiges deutsches Gericht vielmehr alle kollisions- und sachrechtlich relevanten Versicherungsverbote berücksichtigen.[944] Dazu zählen neben dem gemäß Art. 3 Rom I-VO als Vertragsstatut gewählten Recht stets die Eingriffsnormen des Gerichtsstaates (*lex fori*) nach Art. 9 Abs. 1, Abs. 2 Rom I-VO. Soll die Versicherungsleistung in einem anderen Staat – etwa am Sitz eines mitversicherten Tochterunternehmens – erbracht werden, kann das Gericht unter bestimmten Voraussetzungen auch die dort geltenden Versicherungsverbote als Eingriffsnorm i.S.d. Art. 9 Abs. 3 Rom I-VO berücksichtigen. Auf Ebene des materiellen deutschen Sachrechts – und namentlich insbesondere i.R.d. § 138 Abs. 1 BGB – können

942 Siehe oben D I.

943 Vgl. auch *RSUI Indemnity Company v. Murdock*, 2021 BL 76083 (Del. 3.3.2021), wo ein in Delaware inkorporiertes, aber in Kalifornien ansässiges Unternehmen Deckung begehrte, die nach kalifornischem Recht grundsätzlich ausgeschlossen erscheint.

944 Siehe oben D II.

deutsche Gerichte schließlich etwaige Versicherungsverbote derjenigen Rechtsordnung berücksichtigen, deren Behörden die Geldbuße verhängt haben.

Aus der Perspektive des EU-Rechts spricht viel dafür, dass eine (Eigenschaden)Deckung auch für unionsrechtlich vorgezeichnete Geldbußen – etwa im Bereich der DSGVO – nicht automatisch dem sanktionenrechtlichen Effektivitätsgrundsatz zuwiderläuft.[945] Jüngere Regelungsansätze in der NIS-2-RL legen vielmehr nahe, dass Prävention gegenüber Verbänden gerade auch zielgerichtet gegenüber den Geschäftsleitern wirken soll. Diese – in Art. 20 Abs. 1 NIS-2-RL anklingende – Präventionswirkung ließe sich womöglich auch auf dem Regressweg entfalten, wenn ein Cyber-Versicherer die gegen einen Verband verhängte Geldbuße zunächst i.R.d. Eigenschadenbausteins deckt und sodann den Geschäftsleiter, der für den jeweiligen Rechtsverstoß verantwortlich ist, nach § 86 VVG i.V.m. § 93 Abs. 2 AktG bzw. § 43 Abs. 2 GmbHG in Regress nimmt. Denn diese Vorgehensweise macht eine effektive Prävention gegenüber dem tatsächlich verantwortlichen Akteur – nämlich dem Geschäftsleiter – zum einen wahrscheinlicher und verhindert zugleich ein „underenforcement“, das angesichts der fehlenden direkten Sanktionierung individueller Geschäftsleiter (z.B. nach der DSGVO) droht. Freilich sind die durch die jeweiligen EU-Rechtsakte, wie die DSGVO oder die NIS-2-RL, vorgegebene Präventionswirkung ebenso wie die Einhaltung des sanktionenrechtlichen Effektivitätsgrundsatzes unionsrechtliche Fragen, die letztverbindlich nur durch den EuGH im Wege eines Vorabentscheidungsverfahrens geklärt werden können.

In Anlehnung an die aus den USA als „*Punitive Damages Wrap*“ bekannten Deckungskonzepte für Strafschadensersatz könnte auch eine Geldbußendeckung für Verstöße gegen die DSGVO oder das NIS-2-Regime gestaltet werden: Im Zentrum eines solchen „*Fine Wrap*“-Konzepts steht die Wahl eines liberalen Rechts (z.B. Bermuda), wobei diese Rechtswahl sodann durch eine Schiedsklausel zugunsten permissiver Schiedsorte und -ordnungen (z.B. *Bermuda*

[945] Siehe oben D III.

arbitration provision) abgesichert wird.[946] Soweit hierdurch die Umgehung von Versicherungsverboten bezweckt wird, könnten jedoch spätestens im Vollstreckbarerklärungs- bzw. Aufhebungsverfahren *ordre public*-Einwände gegen die Wirksamkeit des Schiedsspruches erhoben werden. Ähnlichen Bedenken begegnen durch korrespondierende Schieds- und Rechtswahlvereinaberungen flankierte „*Drop-Down*"- und „*DIC*"-Klauseln in (höheren) Layern von Exzedenten-Türmen. Auch die aus der anglo-amerikanischen Vertragspraxis bekannten sog. „*most favorable jurisdiction/venue*"-Klauseln dürften im System des europäischen internationalen Zuständigkeits- und Kollisionsrechts kaum Erfolg versprechen. Versicherungsnehmer, die sich auf derartige Konstruktionen verlassen, sehen sich damit erheblichen Unwägbarkeiten gegenüber. Festzuhalten bleibt, dass man auch und gerade bei der Versicherbarkeit von Geldbußen über Staatsgrenzen hinweg an vielen rechtlichen Klippen Schiffbruch erleiden kann.

IV. Versicherbarkeit und Erstattungsfähigkeit von „Lösegeldern" bei Ransomware-Attacken

Das deutsche Recht untersagt Lösegeldzahlungen im Gefolge von Ransomware-Attacken nicht *per se*. Solche Ransom-Zahlungen können auf Grundlage eines speziellen Lösegeldbausteins in Cyber-Versicherungsverträgen ebenso wie als Rettungskosten nach § 83 VVG grundsätzlich erstattet werden.[947] Das Bild in ausländischen Rechtsordnungen ist deutlich heterogener: Während manche US-Bundesstaaten auch für private Unternehmen partielle Verbote erwägen,[948] hat sich der französische Gesetzgeber nach einer kontroversen politischen Debatte nun in Art. L. 12-10-1 *Code des assurances* für die ausdrückliche Gestattung von Lösegeld-Zahlungen und damit auch von Ransom-Versicherungen entschieden.[949] Dabei wird diese Gestattung jedoch – sinnvollerweise – unter den Vor-

[946] Siehe oben D IV.
[947] Siehe oben E I.
[948] Siehe zum Gesetzgebungsprojekt im US-Bundesstaat New York oben E II 1 c).
[949] Siehe oben E II 1 b).

behalt gestellt, dass der Versicherte Anzeigepflichten gegenüber den (Strafverfolgungs)Behörden rechtzeitig erfüllt und hinreichend kooperiert. Dagegen entpuppt sich die häufig als Paradebeispiel für ein Versicherungsverbot angeführte italienische Regelung in Art. 12(1) *Codice delle Assicurazioni Private* als wenig eindeutig: Ob sich die Norm nur auf Fälle von Personen-Entführungen beschränkt oder ob sie auch Cyber-Erpressungen erfasst und die Versicherung von Lösegeldzahlungen infolge von Ransomware-Angriffen untersagt, erscheint nicht abschließend geklärt. Aus rechtspolitischer Sicht sprechen gegen eine solche Ausdehnung schon die Erfahrungen, die Italien mit dem Verbot von Lösegeldzahlungen bei Kidnapping gemacht hat: Die Familienangehörigen von entführten Personen hörten mit Inkrafttreten des Verbots schlagartig auf, mit den Behörden zusammenzuarbeiten oder Entführungen auch nur zu melden.[950] Es erscheint im Kampf gegen Ransomware-Attacken wenig wünschenswert, Verbotsgesetze zu erlassen, die der effektiven Erkennung und Verfolgung von Cyber-Delikten in ähnlicher Weise abträglich sind.

V. Cyber-Versicherungen und Cumul-Risiken: Ausschluss von Krieg und Cyber-Operationen, Territorial-Ausschlüsse und „widespread events“

Ebenso wie andere an NMA 464 orientierte Kriegs-Ausschlussklauseln erfasste die ursprüngliche Formulierung der Ziff. A1-17.2 AVB-Cyber a.F. (2017) das Szenario eines reinen „Cyber-Krieges“ bereits mangels der begrifflich für einen „klassischen“ Krieg erforderlichen physischen Gewaltanwendung nicht.[951]

Eine wortlautgetreue Übersetzung der LMA-Musterklauseln dürfte für den deutschen Markt weder in der ursprünglichen (LMA 5564 bis 5567) noch in der überarbeiteten Fassung (LMA 5564(a,b) bis 5567(a,b)) dieser Kriegs-Ausschlussklauseln eine tragfähige Lö-

[950] Vgl. nur *Geneva Association*, Ransomware: An insurance market perspective, 2022, S. 23.
[951] Siehe oben F I.

sung bieten.[952] Transparenzbedenken begegnet etwa die Formulierung des erforderlichen Grades staatlicher Involvierung, der Belegenheit des „Computersystems“ sowie vor allem die Regelung zur „Attribution“ von Cyber-Attacken, wobei letztere Klausel zudem kaum einer Inhaltskontrolle standhalten dürfte.

Unter dem Gesichtspunkt der AGB-Kontrolle begegnen nun auch viele Aspekte des Ausschlusses von „Krieg und staatlichen Angriffen“ nach Ziff. A1-17.2 AVB-Cyber 2024 Bedenken.[953] So könnte durch Ziff. A1-17-2 lit. b) AVB Cyber 2024 eine Aushöhlung des Cyber-Versicherungsschutzes i.S.d. § 307 Abs. 1 S. 1, Abs. 2 Nr. 2 BGB drohen, weil das Eindringen von weit ausgestreuter Schad-Software in KRITIS-Infrastrukturen *irgendwo auf der Welt* kaum je auszuschließen ist. Der Cyber-Versicherer könnte die Deckung womöglich unter Verweis auf eine „Beeinträchtigung“ kritischer Infrastruktur in einem beliebigen Staat nach Ziff. A1-17-2 lit. b) verweigern, wenn dort nur die Vertraulichkeit von Daten gemäß Ziff. A1-2.1 AVB Cyber 2024 kompromittiert worden ist.[954]

Das Verdikt der Missbräuchlichkeit dieser Klauselgestaltung dürfte gerade in der Zusammenschau mit den weiteren Regelungen in Ziff. A1-17-2 AVB Cyber 2024 Bestand haben, weil dort die Darlegung der weiteren Voraussetzungen des Ausschlusses sowie insbesondere die Zuschreibung der Cyber-Attacke zu einem Staat erleichtert werden.[955] Ziff. A1-17-2 AVB-Cyber 2024 ist insoweit dreischrittig aufgebaut: Wird im ersten Schritt die Tatsache der Beteiligung gewisser einschlägiger Personen oder Gruppen dargelegt und bewiesen, soll automatisch im zweiten Schritt die Tatsache „Hinweis“ und damit zugleich auch im dritten Schritt die Tatsache „staatliche Involvierung“ i.S.d. Ziff. A1-17-2 AVB-Cyber 2024 als dargelegt und bewiesen gelten. In dieser Gestaltung dürfte – insbesondere wegen der fehlenden Möglichkeit eines Gegenbeweises – eine unangemessene Benachteiligung nach § 307 Abs. 1 S. 1, Abs. 2 Nr. 1 BGB wegen eines Abgehens von grundlegenden Prinzipien der Darle-

952 Siehe oben F II.
953 Siehe oben F III.
954 Siehe oben F III 2.
955 Siehe oben F III 3.

gungs- und Beweislast liegen. Dabei ist nicht zuletzt zu beachten, dass die grundsätzliche Wertung des § 309 Nr. 12 BGB auch im unternehmerischen Verkehr i.R.d. § 307 BGB zu berücksichtigen ist.

Zudem dürfte die allgemeine Einschränkung auf „objektiv angemessene Beweismittel" gegen das Transparenzgebot nach § 307 Abs. 1 S. 2 BGB verstoßen, weil völlig im Dunkeln bleibt, wie sich derartige Beweismittel jeweils – je nach Art der (streitigen) Behauptung und des Verfahrens – zum zivilprozessualen Streng- oder Freibeweis verhalten sollen.[956] Schließlich erscheint auch die Regelung zur Zuschreibung in Ziff. A1-17-2 AVB-Cyber 2024 unter Transparenzgesichtspunkten angreifbar: Bedenken begegnet bereits die Forderung einer „offiziellen Zuschreibung durch staatliche Stellen", weil hierunter neben Regierung, Militär, Nachrichtendiensten sowie Ministerial- und Sicherheitsbeamten ganz unterschiedliche „offizielle" Quellen auf sehr unterschiedlichen Hierarchiestufen in Betracht kommen.

Die „Zuschreibung" bzw. „*attribution*" sollte vor diesem Hintergrund so weit wie möglich objektiviert werden: Eine rechtssichere Zuschreibung einer Cyber-Attacke könnte etwa durch die Schaffung einer objektiven nicht-staatlichen Stelle erreicht werden, die alle verfügbaren Informationen aggregiert und zeitnah eine Entscheidung nach „billigem Ermessen" trifft.[957] Den meisten gegenüber der „Zuschreibungs"-Konzeption in LMA 5564(a) bis 5567(a) und in Ziff. A1-17.2 a.E. AVB-Cyber 2024 geäußerten Bedenken ließe sich dadurch begegnen, dass die Einschätzung dieser Stelle für maßgeblich erklärt wird. Ein solcher objektiver Ansatz liegt nicht zuletzt im Interesse des Cyber-Versicherers, der die Voraussetzungen des Risikoausschlusses im Streitfall darlegen und beweisen muss und dabei – wie gezeigt – nicht auf die in Ziff. A1-17.2 a.E. AVB-Cyber 2024 vorgesehenen klauselförmigen Erleichterungen wird bauen können.

Der Bedarf nach einer rechtssicheren Gestaltung des Ausschlusses für Cyber-Attacken im Rahmen eines „Krieges" oder sog. „Cyber-Operations" besteht nicht zuletzt deshalb weiterhin, weil die in Pra-

[956] Siehe oben F III 4.
[957] Siehe oben F III 5.

xis anzutreffenden alternativen Mechanismen zur Eindämmung von Cyber-Cumul-Risiken – wie die Kategorie des „weiterverbreiteten Ereignisses“ und territorialer Ausschlüsse – ebenfalls Transparenzbedenken begegnen.[958]

[958] Siehe oben F IV.

Literaturverzeichnis

Abraham, Kenneth S./Schwarcz, Daniel: The Limits of Regulation by Insurance, 98 Indiana Law Journal (2023), 215-274.

Anders, Monika/Gehle, Burkhard: Zivilprozessordnung, München 82. Aufl. 2024 (zit.: Anders/Gehle/*Bearbeiter*).

Armbrüster, Christian: Folgenzurechnung im Privatversicherungsrecht, in: Karlsruher Forum 2007, *Lorenz, Egon* (Hrsg.), Karlsruhe 2008, S. 89-112.

Armbrüster, Christian: Privatversicherungsrecht, Tübingen 2. Aufl. 2019.

Armbrüster, Christian/Schilbach, Dan: Nichtigkeit von VersVerträgen wegen Verbots- oder Sittenverstoßes, r+s 2016, 109-117.

Arzt, Gunther: Zur Strafbarkeit des Erpressungsopfers, JZ 2001, 1052-1057.

Baker, Tom/Shortland, Anja: Insurance and enterprise: cyber insurance for ransomware, The Geneva Papers on Risk and Insurance 48 (2023), 275-299.

Bälz, Kilian: Das „Befolgungsverbot" der Blocking-VO (EG) Nr. 2271/96, EuZW 2020, 416-420.

von Bar, Christian/Mankowski, Peter: Internationales Privatrecht (Band I: Allgemeine Lehren), München 2. Aufl. 2003.

Basedow, Jürgen/Rühl, Giesela/Ferrari, Franco/de Miguel Asensio, Pedro: Encyclopedia of Private International Law, Bd. II, Cheltenham 2017 (zit.: *Bearbeiter* in: Basedow/Rühl/Ferrari).

Basedow, Jürgen/Scherpe, Jens: Das internationale Versicherungsvertragsrecht und „Rom I", in: Lorenz, Stephan/Trunk, Alexander/Eidenmüler, Horst/Wendehorst, Christiane/Adolff, Johannes (Hrsg.), Festschrift für Andreas Heldrich zum 70. Geburtstag, München 2005, S. 511-526 (zit.: *Basedow/Scherpe*, FS Heldrich).

Basedow, Jürgen/Hopt, Klaus J./Zimmermann, Reinhard: Handwörterbuch des Europäischen Privatrechts, Band 1, Tübingen 2009 (zit.: *Bearbeiter* in: Basedow/Hopt/Zimmermann, EurPrivatR-HdWB I).

Bateman, John: War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions, Carnegie Endownment for International Peace Working Paper, Washington 10/2020.

Baumgärtel, Gottfried/Laumen, Hans-Willi/Prütting, Hanns: Handbuch der Beweislast: Band 1: Grundlagen, Hürth 5. Aufl. 2023 (zit.: *Bearbeiter* in Baumgärtel/Prütting/Laumen).

beck-online.GROSSKOMMENTAR zum Handels- und Gesellschaftsrecht, (Gesamt-Hrsg.: Henssler, Martin) München 2024.

BeckOGK AktG (zit. BeckOGK AktG/*Bearbeiter*).

beck-online.GROSSKOMMENTAR zum Zivilrecht (Gesamt-Hrsg.: Gsell, Beate/Krüger, Wolfgang/Lorenz, Stephan/Reymann, Christoph) München 2024.

BeckOGK Rom I-Verordnung (zit.: BeckOGK Rom I-Verordnung/*Bearbeiter*).

BeckOGK Rom II-Verordnung (zit.: BeckOGK Rom II-Verordnung/*Bearbeiter*).

BeckOGK EGBGB (zit.: BeckOGK EGBGB/*Bearbeiter*).

BeckOGK BGB (zit.: BeckOGK BGB/*Bearbeiter*).

Beck'scher Online-Kommentar BGB (Hrsg.: Hau, Wolfgang/Poseck, Roman), München 2024 (zit.: BeckOK BGB/*Bearbeiter*).

Beck'scher Online-Kommentar DatenschutzR (Hrsg.: Wolff, Heinrich Amadeus/Brink, Stefan/v. Ungern-Sternberg, Antje), München 2024 (zit.: BeckOK DatenschutzR/*Bearbeiter*).

Beck'scher Online-Kommentar StGB (Hrsg.: v. Heintschel-Heinegg, Bernd/Kudlich, Hans), München 2024 (zit.: BeckOK StGB/Bearbeiter).

Beck'scher Online-Kommentar ZPO (Hrsg.: Vorwerk, Volkert/Wolf, Christian), München 2024 (zit.: BeckOK ZPO/*Bearbeiter*).

Bigot, Rodolphe/Cayol, Amandine/Noguéro, David/Pierre, Philippe: Droit des assurances, Recueil Dalloz Nr. 22 2020, 1124-1153.

Borges, Georg/Meents, Jan Geert: Cloud Computing, München 2016 (zit.: *Bearbeiter* in: Borges/Meents: Cloud Computing, München 2016).

Brkan, Maja: Data protection and conflict-of-laws: a challenging relationship, European Data Protection Law Review (2016), 324-341.

Brodowski, Dominik/Schmid, David/Scholzen, Alexandra/Zoller, Christoph: Zuerst erpresst, dann verfolgt?, NStZ 2023, 385-391.

Bruck, Ernst/Möller, Hans: Großkommentar zum Versicherungsvertragsgesetz:
Band 4: §§ 100-124 VVG, Haftpflichtversicherung; D&O-Versicherung, Berlin 10. Aufl. 2022.
Band 5: AHB; Produkthaftpflicht; Umwelt; Cyberversicherung, Berlin, 10. Aufl. 2023.
(zit.: Bruck/Möller/*Bearbeiter*).

Bürkle, Jürgen: Compliance in Versicherungsunternehmen, München 3. Aufl. 2020 (zit.: *Heinisch* in: Bürkle).

Carter, Robert L./Falush, Peter: The British Insurance Industry Since 1900, London 2009.

Chopra, Angad: Cyberattack – Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims, 82 Ohio State L.J. (2021), 121-162.

Cunningham, Bryan/Talesh, *Shauhin*: Uncle Sam RE: Improving cyber hygiene and increasing confidence in the cyber insurance ecosystem via government backstopping, 28 Connecticut Insurance Law Journal (2021), 1-84.

Dahlke, Peter: Terror als Schadensursache, VersR 2003, 25-33.

Dallwig, Florian: Kriegsbedingte Versorgungslücken mit Gas in der Betriebsunterbrechungsversicherung, r+s 2022, 311-318.

de Freitas, Silva: The interplay of digital and legal frontiers: analyzing jurisdictional rules in GDPR collective actions and the Brussels I-bis Regulation, NIPR (2023), 227-242.

de Miguel Asensio, *Pedro Alberto*: Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea, REDI 69 (2017), 75-108.

Dethloff, Nina/Nolte, Georg/Reinisch, August (Hrsg.): Freiheit und Regulierung in der Cyberwelt, Heidelberg 2016 (zit.: *Heiderhoff* in: Dethloff/Nolte/Reinisch).

Dickmann, Roman A. (Hrsg.): Cyberversicherung, München 2025 (zit.: Dickmann/*Bearbeiter*, Cyberversicherung).

Dittrich, Tillmann/Heinelt, *Christian*: Der Europäische DORA – neue Sicherheitsvorgaben für den Finanzsektor, RDi 2023, 164-172.

DLA Piper, Data Protection Laws of the World (2022).

DLA Piper, GDPR fines and data breach survey (2023).

DLA Piper/Aon, The price of data security: A guide to the insurability of GDPR fines across Europe, 3rd ed. (2020).

Domej Tanja: Internationale Zuständigkeit für Abhilfeklagen nach der EU-Verbandsklagen-Richtlinie, in: Kubis, Sebastian/Peifer, Karl-Nikolaus/Raue, Benjamin/Stieper, Malte (Hrsg.), Ius Vivum: Kunst – Internationales – Persönlichkeit Festschrift für Haimo Schack zum 70. Geburtstag, Tübingen 2022, S. 564-573 (zit.: *Domej*, FS Schack).

Dreher, Meinrad: Die kartellrechtliche Bußgeldverantwortlichkeit von Vorstandsmitgliedern. Vorstandshandeln zwischen aktienrechtlichem Legalitätsprinzip und kartellrechtlicher Unsicherheit, in: Dauner-Lieb, Barbara/Hommelhoff, Peter/Jacobs, Matthias/Kaiser, Dagmar/Weber, Christoph (Hrsg.), Festschrift für Horst Konzen zum 70. Geburtstag, Tübingen 2006, S. 85-108 (zit.: *Dreher*, FS Konzen).

Dutta, Anatol: Anmerkung zum Lechouritou-Urteil des Gerichtshofs der Europäischen Gemeinschaften vom 15. 2. 2007 – Rs. C-292/05 [Zum Begriff der Zivil- und Handelssache], ZZPInt 11 (2006), 208-220.

Eggen, Jonathan: Die Cyberversicherung, *Karlsruhe* 2023.

EIOPA, Cyber Security and Cyber Risk: A universal Challenge, Keynote speech by Gabriel Bernardino at the 3rd Annual FinTech and Regulation Conference on „Taking innovation to the next level" on 26 February 2019 in Brussels.

Engel, Andreas: Anmerkung zu: Zivilprozessrecht: Zuständigkeit für Schadensersatzklagen bei Beleidigungen im Internet – Gtflix Tv/DR, EuZW 2022, 226-227.

European Commission, Comparative study on the situation in the 27 Member States as regards the law applicable to non-contractual obligations arising out of violations of privacy and rights relating to personality (Final Report), JLS/2007/C4/028 (2009).

European Network and Information Security Agency (ENISA) (Hrsg.), (Autoren: *Anderson, Ross/Böhme, Rainer/Clayton, Richard/Moore, Tyler*), Security Economics and the Internal Market (2008).

European Union, Study on the Rome II Regulation (EC) 864/2007 on the law applicable to non-contractual obligations (JUST/2019/JCOO_FW_CIVI_0167) (2021).

Fleischer, Holger: Kartellrechtsverstöße und Vorstandsrecht, BB 2008, 1070-1076.

Fleischer, Holger: Regresshaftung von Geschäftsleitern wegen Verbandsgeldbußen, DB 2014, 345-352.

Fortmann, Michael: Cyberversicherung: ein gutes Produkt mit noch einigen offenen Fragen, r+s 2019, 429-443.

Fortmann, Michael: Der Kriegsausschluss, in: Fortmann, Michael/Maier, Karl (Hrsg.), Versicherungsrecht – Vergangenheit und Zukunft Festschrift für Peter Schimikowski zum 70. Geburtstag, München 2023, S. 93-112 (zit.: *Fortmann*, FS Schimikowski).

France Assureurs, Livre blanc: Bâtir une économie de la donnée (2022).

Franck, Jens-Uwe/Seyer, Till: Management Liability for Companies' Antitrust Fines, Discussion Paper Series – CRC TR 224 (Discussion Paper No. 429 Project B 05), November 2023.

Freitag, Robert: Halbseitig ausschließliche Gerichtsstandsvereinbarungen unter der Brüssel I-VO, in: Mankowski, Peter/Wurmnest, Wolfgang (Hrsg.), Festschrift für Ulrich Magnus zum 70. Geburtstag, München 2014, S. 419-432 (zit.: Freitag, FS Magnus).

Freitag, Robert/Leible, Stefan: Das Bestimmungsrecht des Art. 40 Abs. 1 EGBGB im Gefüge der Parteiautonomie im Internationalen Deliktsrecht, ZVglRWiss 99 (2000), 101-142.

Fricke, Martin: Rechtliche Probleme des Ausschlusses von Kriegsrisiken in AVB, VersR 1991, 1098-1103.

Fricke, Martin: Rechtliche Probleme des Ausschlusses von Kriegsrisiken in AVB, VersR 2002, 6-11.

Freiherr Frank von Fürstenwerth, Jörg, Weiß, Alfons, Consten, Werner, Präve, Peter: VersicherungsAlphabet, Karlsruhe 11. Aufl. 2019. (zit.: Fürstenwerth/Weiß/Consten/Bearbeiter).

Ganzer, Felix: Internationale Versicherungsprogramme, Karlsruhe 2012.

Gebauer, Martin/Wiedmann, Thomas: Europäisches Zivilrecht, München 3. Aufl. 2021 (zit.: *Bearbeiter* in: Gebauer/Wiedmann).

Geimer, Reinhold/Schütze, Rolf: Europäisches Zivilverfahrensrecht, München 4. Aufl. 2020, (zit.: Geimer/Schütze/*Bearbeiter*, EuZivilVerfR).

Geneva Association, Ransomware: An insurance market perspective (2022).

Gola, Peter/Heckmann, Dirk: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, München 3. Aufl. 2022 (zit.: Gola/Heckmann/*Bearbeiter*).

Groupe d'études Assurances, Rapport La cyber-assurance (2021).

Grüneberg, Christian (Hrsg.): Bürgerliches Gesetzbuch, München 84. Aufl. 2025. (zit.: Grüneberg/*Bearbeiter*).

Günther, Dirk-Carsten: „Cyberwar" und Kriegsausschluss, r+s 2019, 188-190.

Günther, Dirk-Carsten: Hybride Kriegsführung und Ausschluss für Kriegsschäden am Beispiel des russisch-ukrainischen Konflikts, VW 4/2022, 68-71.

Habbe, Julia Sophia/Gergen, Philipp: Compliance vor und bei Cyberangriffen – Pflichten der Geschäftsleitung und deren konkrete Umsetzung in der Praxis, CCZ 2020, 281-285.

Haut Comité Juridique de la Place Financière de Paris, Rapport sur l'assurabilité des risques cyber (2022).

Heinze, Christian/Warmuth, Cara: Das Sonderprozessrecht der Datenschutz-Grundverordnung, ZZPInt 21 (2016), 175-198.

Hennemann, Moritz/Steinrötter, Björn: Der Data Act, NJW 2024, 1-8.

Hippel, *Eike von:* Bessere Bekämpfung des erpresserischen Menschenraubs, ZRP 2002, 442-443.

Hoffmann, Jochen: Die internationale Zuständigkeit für Verbandsklagen gegen drittstaatliche Unternehmen, IPRax 2024, 7-15.

Hoffmann, Markus/Schürger, *Dominik:* Regress von Sach- und Cyberversicherern gegen Organmitglieder der VN, r+s 2024, 789-797.

Huang, Jeanne, Personal Jurisdiction based on the Location of a Server: Chinese Territorialism in the Internet Era?, 36 Wisconsin International Law Journal (2018), 87-121.

Huang, Jeanne: Chinese Private International Law and Online Data Protection, 15 Journal of Private International Law (2019), 186-209.

Hübner, Ulrich: Rechtsprobleme der Deckung politischer Risiken, ZVersWiss 1981, 1-48.

Hugo Grotius, De Iure Praedae Commentarius, Vol. I (*Williams/Zeydel*, A Translation of the Original Manuscript of 1604, London 1950), (2009).

Immenga/Mestmäcker: Wettbewerbsrecht, Band 1, 7. Aufl. 2025 (zit.: Immenga/Mestmäcker/*Bearb.*).

Insurance Europe, Insurers' role in EU cyber resilience (2019).

Insurance Institute, Cyber Insurance Research Findings (2022).

Janal, Ruth: Die Umsetzung der Verbandsklagenrichtlinie, GRUR 2023, 985-995.

Julian, Lesser: Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken, Karlsruhe 2021.

Junker, Abbo: Zwei Schritte vor, einer zurück. Die Abgrenzung von Vertrags- und Deliktsgerichtsstand in der Rechtsprechung des Europäischen Gerichtshofs, in: Kubis, Sebastian/Peifer, Karl-Nikolaus/Raue, Benjamin/Stieper, Malte (Hrsg.), Ius Vivum: Kunst – Internationales – Persönlichkeit Festschrift für Haimo Schack zum 70. Geburtstag, Tübingen 2022, S. 653-665 (zit.: *Junker*, FS Schack).

juris PraxisKommentar BGB (Gesamt-Hrsg.: Herberger, Maximilian/Martinek, Michael/Rüßmann, Helmut/Weth, Stephan/Würdinger, Markus):
Band 6: Internationales Privatrecht und UN-Kaufrecht, Saarbrücken 8. Aufl. 2017 (zit.: jurisPK-BGB/*Bearbeiter*).

juris PraxisKommentar Internetrecht (Hrsg.: Heckmann, Dirk/Paschke, Anne) Saarbrücken 8. Aufl. 2024 (zit.: jurisPK-Internetrecht/*Bearbeiter).*

Kapp, Thomas: Dürfen Unternehmen ihren (geschäftsleitenden) Mitarbeitern Geldstrafen bzw. -bußen erstatten?, NJW 1992, 2796-2800.

Kegel, Gerhard/Schurig, Klaus: Internationales Privatrecht, München 9. Aufl. 2004.

Keyes, Mary/Marshall, Brooke: Jurisdiction agreements: exclusive, optional and asymmetrical, 11 Journal of Private International Law (2015), 345-378.

Koch, Frank: Updating von Sicherheitssoftware – Haftung und Beweislast Eine Problemskizze zur Verkehrssicherungspflicht zum Einsatz von Antivirenprogrammen, CR 2009, 485-491.

Koch, Philipp: Versicherungsverbote in dem Russland-Sanktionspaket der Versicherungsverbote in Russland--Sanktionspaket der Europäischen Union, UKuR 2022, 400-405.

Koch, Robert: Haftung des Versicherers für fehlerhafte Assistanceleistungen, VersR 2019, 449-456.

Koch, Robert: Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801-807.

Kohler, Christian: Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union, RDIPP 52 (2016), 653-675.

König, Pia Marie: Lösegeldzahlungen bei Angriffen mit Ransomware – Rettungsanker oder strafrechtliches Risiko?, NZWiSt 2023, 167-171.

Kullmann, Jérôme: Amendes pénales et amendes administratives infligées au dirigeant : pour une assurance raisonnée, JCP Entreprises 10/2009, 1226.

Lange, Oliver: D&O-Versicherung, München 2. Aufl 2022.

Langheid, Theo/Wandt, Manfred: Münchener Kommentar zum Versicherungsvertragsgesetz:
Band 2: §§ 100-216, München 3. Aufl. 2023.
Band 3: Nebengesetze, Systematische Darstellungen I, München 3. Auflage 2024.
Band 4: Nebengesetze und systematische Darstellungen II, München 3. Aufl. 2024.
(zit.: Langheid/Wandt/*Bearbeiter*).

Lemnitzer, Jan Martin: Why cybersecurity insurance should be regulated and compulsory, Journal of Cyber Policy 6(2) (2021), 118-136.

Lilie, Astrid/Becker, Cheyenne: AWG-Verstöße vor dem Hintergrund der Russland-Sanktionen, NZWiSt 2025, 133-141.

Logue, Kyle/Shniderman, Adam: The Case for Banning (and Mandating) Ransomware Insurance, 28 Connecticut Insurance Law Journal (2021), 247-316.

Looschelders, Dirk: Auswirkungen US-amerikanischer Embargobestimmungen auf einen Versicherungsvertrag, Anmerkung zum Urteil des LG Hamburg vom 3.12.2014 – 401 HKO 7/14, VersR 2015, 1025-1027.

Looschelders, Dirk/Pohlmann, Petra: VVG – Kommentar, Hürth 4. Aufl. 2023 (zit.: Looschelders/Pohlmann/*Bearbeiter*).

Lüttringhaus, Jan D.: EU-Effektivitätsgrundsatz und Verbandsgeldbußenregress nach § 43 Abs. 2 GmbHG, § 93 Abs. 2 AktG – Haftung und Versicherbarkeit als Gretchenfragen im EuGH-Vorabentscheidungsersuchen des BGH v. 11.2.2025 – KZR 74/23, VersR 2025, 843-855.

Lüttringhaus, Jan D.: Verbandsgeldbußenregress gegen Geschäftsleiter – Zum Innenregress und zur Versicherbarkeit von Kartell-, DSGVO-, KI-VO- und NIS-2-Geldbußen, in: Eichelberger, Jan/Schwarze, Roland (Hrsg.), Festschrift 50 Jahre Juristische Fakultät Hannover, Baden-Baden 2025, S. 207-230 (abrufbar unter: https://doi.org/10.5771/9783748949893-207).

Lüttringhaus, Jan D.: Das internationale Datenprivatrecht: Baustein des Wirtschaftskollisionsrechts des 21. Jahrhunderts, ZVglRWiss 117 (2018), 50-82.

Lüttringhaus, Jan D.: Privatversicherungsrecht in und für Krisenzeiten –Risikoausschlüsse für „Cyber-Krieg" und Krisenresilienz im Versicherungsverhältnis, VersR 2022, 1553-1563.

Lüttringhaus, Jan/Ettl, Robin: Ursachenzusammenhänge in AVB: Was bedeutet eigentlich „durch" Krieg, „durch" staatliche Cyber-Angriffe oder „durch" Sturmflut?, VersR 2025, 649-661.

Lutzi, Tobias: Anmerkung zum EuGH Urteil vom 21.12.2021 – C-251/20 (Gtflix Tv/DR) – Internationale Zuständigkeit bei Persönlichkeitsrechtsverletzungen im Internet, NJW 2022, 768-768.

Lutzi, Tobias: Einseitigkeit statt Allseitigkeit als Strukturprinzip des Digitalen Binnenmarkts?, IPRax 2024, 262-266.

Lutzi, Tobias: Private International Law Online, Oxford 2020.

Makowsky, *Mark:* Das Kriegsrisiko im Privatversicherungsrecht – grundlegende Fragen und aktuelle Entwicklungen, VersR 2023, 1-17.

Mankowski, Peter: Das Internet im Internationalen Vertrags- und Deliktsrecht, RabelsZ 63 (1999), 203-294.

Marangos, *Hermes L.:* Historical overview of the insurance and exclusion of 'War Risks' and Associated Perils, in: ders. (ed.), War risks and terrorism, London 2007.

Marly, Pierre-Grégoire: L'assurance des risques de cyberattaques, Recueil Dalloz 2023, 112.

Marsh: GDPR Fines and Penalties: Insurability will Vary by Location, Policy Details, and More (2018).

Marshall, *Brooke:* Asymmetric Jurisdiction Clauses, Oxford 2023.

Maultzsch, Felix: Das neue Verbraucherrechtedurchsetzungsgesetz – VDuG, ZZP 137 (2024), 119-150.

Maultzsch, Felix: Der Einfluss US-amerikanischer Iran-Sanktionsprogramme auf Verträge mit deutschem Vertragsstatut, IPRax 2025, 164-171.

Maultzsch, Felix: Forumsfremde Eingriffsnormen im Schuldvertragsrecht zwischen Macht- und Wertedenken, in: Christoph Benicke/Stefan Huber (Hrsg.), National, International, Transnational: Harmonischer Dreiklang im Recht, Festschrift für Herbert Kronke zum 70. Geburtstag, Bielefeld, 2020, S. 363-377.

Max Planck Institute: Comments on the European Commission's Green Paper on the conversion of the Rome Convention of 1980 on the law applicable to contractual obligations into a Community instrument and its modernization, RabelsZ 68 (2004), 1-118.

Mehrbrey, Kim L./Schreibauer, Marcus: Haftungsverhältnisse bei Cyber-Angriffen – Ansprüche und Haftungsrisiken von Unternehmen und Organen, MMR 2016, 75-82.

Meyer; Eric/Biermann, Sina: Ransomware-Angriff, MMR 2022, 940-946.

Michaels, Ralf: Die europäische IPR-Revolution, in: Baetge, Dietmar/von Hein, Jan/von Hinden, Michael (Hrsg.), Festschrift für Jan Kropholler zum 70. Geburtstag, Tübingen 2008, 151-175 (zit.:Michaels, FS Kropholler).

Miller, Michael D.: Marine War Risks, London 3rd ed. 2005.

Mitsch, Wolfgang: Karlsruher Kommentar zum OWiG, München 5. Aufl. 2018 (zit.: OWiG/*Bearbeiter*).

Müller-Berg, Michael: Die Auswirkungen der neuen Produkthaftungsrichtlinie auf die internationale Produkthaftung, IPRax 2025, 221-230.

Münchener Kommentar zum Bürgerlichen Gesetzbuch (Hrsg.: Säcker, Franz, Jürgen/Pixecker, Roland/ Oetker, Harmut/ Limperg, Bettina/ Schubert, Claudia):
Band 1: Allgemeiner Teil (§§ 1-240; AllgPersönlR; ProstG; AGG), München 9. Aufl. 2021.
Band 2: Schuldrecht – Allgemeiner Teil I (§§ 241-310), München 9. Aufl. 2022.
Band 7: Schuldrecht – Besonderer Teil IV (§§ 705-853 Partnerschaftsgesellschaftsgesetz; Produkthaftungsgesetz), München 9. Aufl. 2024.
Band 12: Internationales Privatrecht I, Europäisches Kollisionsrecht Einführungsgesetz zum Bürgerlichen Gesetzbuche (Art. 1-26), München 8. Aufl. 2020.
(zit.: MünchKommBGB/*Bearbeiter*).

Münchener Kommentar zum Lauterkeitsrecht (Hrsg.: Heermann, Peter W./ Schlingloff, Jochen):
Band 1: Grundlagen des Lauterkeitsrechts, Internationales Wettbewerbs- und Wettbewerbsverfahrensrecht, Unionsrechtlicher Rahmen, Vorabentscheidungsverfahren, München 3. Aufl. 2020.
(zit.: MünchKommLauterkeitsrecht/*Bearbeiter*).

Münchener Kommentar StGB (Hrsg.: Erp, Volker/Schäfer, Jürgen):
Band 3 §§ 80-184k, München 4. Aufl. 2021.
(zit.: MünchKommStGB/*Bearbeiter*).

Münchener Kommentar zur Zivilprozessordnung mit Gerichtsverfassungsgesetz und Nebengesetzen (Hrsg.: Krüger, Wolfgang/Rauscher, Thomas):
Band 1: §§ 1-354, München 6. Auflage 2020.
Band 3: §§ 946-1120 (EGZP; GVG; EGGVG; UKlaG; Internationales und Europäisches Zivilprozessrecht), 6. Aufl. 2022.
(zit.: MünchKommZPO/*Bearbeiter*).

Musielak, Hans-Joachim/Voit, Wolfgang: Zivilprozessordnung mit Gerichtsverfassungsgesetz, München 21. Aufl. 2024 (zit.: Musielak/Voit/*Beabeiter,* ZPO).

Nägele, Thomas/Jacobs, Sven: Rechtsfragen des Cloud Computing, ZUM 2010, 281-292.

Naumann, André/Brinkmann, Christian: Zur Auslegung des Kriegsausschlusses in der privaten Unfallversicherung, r+s 2012, 469-477.

Nordmeier, Carl F.: Cloud Computing und Internationales Privatrecht – Anwendbares Recht bei der Schädigung von in Datenwolken gespeicherten Daten, MMR 2010, 151-156.

Nyampong, Yaw O. M.: Insuring the Air Transport Industry Against Aviation War and Terrorism Risks and Allied Perils, Berlin/Heidelberg 2013.

O'May, Donald/Hill, Julian: Marine Insurance: Law and Policy, London (1993).

OECD: Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation (2020).

Ohly, Ansgar/Sosnitza, Olaf: Gesetz gegen den unlauteren Wettbewerb mit Geschäftsgeheimnisgesetz (Auszug) und Preisangabenverordnung, München 8. Aufl. 2023 (zit.: Ohly/Sosnitza/*Bearbeiter*).

Oster, Jan: Gefällt Facebook nicht: Die Zähmung eines Datenriesen durch Internationales Datenschutz-Privatrecht, IPRax 2023, 198-217.

Paal, Boris P./Kritzer, Ina: Geltendmachung von DS-GVO-Ansprüchen als Geschäftsmodell NJW 2022, 2433-2349.

Pache, Thomas: Kompass Cyberversicherungen, Karlsruhe 2. Aufl. 2023.

Perner, Stefan/Artner, Felix: Versicherung und Krieg, versicherungsrundschau 11/2022, 50-61.

Perrier, Jean-Baptiste: Les infractions et sanctions de la LOPMI, ou la répression de Potemkine, RSC Nr. 2 2023, 381-394.

Piltz, *Carlo:* Rechtswahlfreiheit im Datenschutzrecht?, K&R 2012, 640-645.

Pohle, Jan/Adelberg, Philipp: Datenschutzrechtlicher Schadensersatzanspruch nach Cyberangriffen, ZD 2024, 312-317.

Pott, Claudia: Versicherbarkeit von Geldbußen und Geldstrafen, ZfV 2023, 357-361.

Prölss, Erich R. (Begr.)/Dreher, Meinrad (Hrsg.): Versicherungsaufsichtsgesetz, München 13. Aufl. 2018 (zit.: Prölss/Dreher/*Bearbeiter)*.

Prölss, Erich R./Martin, Anton: Versicherungsvertragsgesetz, München 32. Aufl. 2024. (zit.: Prölss/Martin/*Bearbeiter*).

Rapp, Julian: Haftung und Versicherung bei Schäden durch Bombenfunde, VersR 2020, 136-145.

Rauscher, Thomas: Europäisches Zivilprozess- und Kollisionsrecht:
Band I: Zivilverfahren I. Brüssel Ia-VO, Lugano-Übk, Köln 5. Aufl. 2021
Band III: Internationales Schuldrecht. Rom I, Rom II, Köln 5. Aufl. 2023.
(zit.: Rauscher/*Bearbeiter*).

Rehbinder, Eckard: Rechtliche Schranken der Erstattung von Bußgeldern an Organmitglieder und Angestellte, ZHR 148 (1984), 555-578.

Riehm, Thomas: Rechte an Daten – Die Perspektive des Haftungsrechts, VersR 2019, 714-724.

Rieländer, Frederick: Zur Qualifikation außervertraglicher Ansprüche zwischen Vertragsparteien im europäischen IZVR und IPR, RIW 2021, 103-112.

Römer, Wolfgang/Langheid, Theo: Versicherungsvertragsgesetz VVG mit Pflichtversicherungsgesetz (PflVG) und Kraftfahrzeug-Pflichtversicherungsverordnung (KfzPfVV), München 2. Aufl. 2003 (zit.: Römer/Langheid/*Bearbeiter).*

Roßnagel, Alexander/Rost, Maria Christina: Geldbußen gegen juristische Personen; Klarstellungen durch zwei Entscheidungen des EuGH, ZD 2024, 183-189.

Rudkowski, Lena: Von Cyberkrieg bis zum Ausfall von Infrastrukturen – die Risikoausschlüsse nach den AVB Cyber, VersR 2023, 416-424.

Rudkowski, Lena: Die AVB Cyber 2024 – Ein erster Überblick, VersR 2024, 601-610.

Rüffer, Wilfried/Halbach, Dirk/Schimikowski/Peter (Hrsg.): Versicherungsvertragsgesetz, Baden-Baden 4. Aufl. 2020 (zit.: Rüffer/Halbach/Schimikowski/*Bearbeiter).*

Ruttmann, Peter: Die Versicherbarkeit von Geldstrafen, Geldbußen, Strafschadensersatz und Regressansprüchen in der D&O-Versicherung, Karlsruhe 2014.

Salomon, Tim R.: Cybercrime und Lösegeld – Strafbarkeit der Zahlung von Lösegeld als Reaktion auf Erpressungstrojaner, MMR 2016, 575-579.

Schilbach, Dan/Becker, Oliver: Der Regress des Cyberversicherers gegen Organe oder Mitarbeiter der Versicherungsnehmerin, r+s 2023, 289-297.

Schmidt, Reimer. / Gerathewohl Klaus: Die Versicherung bei Gewalttätigkeiten gegen eine Gemeinschaft, wobei Personen oder Sachschäden entstehen, ZVersWiss 1973, 277–317.

Schmitt, Carl: Land und Meer, Leipzig 1. Auflage 1942, Stuttgart 6. Aufl. 2008.

Schneidereit, Peter: Haftung für Datenverlust im Cloud Computing, Baden-Baden 2017.

Schreier, Vincent: Verhältnis zwischen Schadensrecht und Schadensversicherung, Berlin 2017.

Schütze, Rolf, A./Thümmel, Roderich C.: Schiedsgericht und Schiedsverfahren, München 7. Aufl. 2021.

Schwemmer Sophia: Internationale Zuständigkeit für Cum-Ex-Haftungsklagen gegen Drittstaatsgesellschaften: Divergenzen zwischen EuGVVO und autonomem Zuständigkeitsrecht?, IPRax 2024, 130-134.

Seibt, Christoph H./Denninger, Philip: Handlungsoptionen für Unternehmen in der geopolitischen Zwickmühle von US-Sanktionen und EU-Blocking-Verordnung, ZIP 2023, 1969-1974.

Sieg, Oliver/Schilbach, Dan: Versicherbarkeit von Lösegeldzahlungen in der Cyberversicherung unter Berücksichtigung privatrechtlicher Beschränkungen der Vertragsfreiheit, VersR 2023, 745-751.

Sonnenberger, Hans J.: Randbemerkungen zum Allgemeinen Teil eines europäisierten IPR in: Baetge, Dietmar/von Hein, Jan/von Hinden, Michael (Hrsg.), Festschrift für Jan Kropholler zum 70. Geburtstag, Tübingen 2008, S. 227-247 (zit.: *Sonnenberger*, FS Kropholler).

Sonnentag, Michael: Forumsfremde Eingriffsnormen im Europäischen Internationalen Vertragsrecht, VersR 2024, 201-209.

Spindler, Gerald/Schuster, Fabian: Recht der elektronischen Medien, München 4. Aufl. 2019 (zit.: *Bearbeiter* in: Spindler/Schuster, Elektron. Medien).

Spindler, Gerald: Anmerkung zu einer Entscheidung des BGH, Urteil vom 24.01.2013 (III ZR 98/12; NJW 2013, 1072) – Zum Schadensersatzpflicht beim Ausfall des Internetanschlusses, JZ 2013, 897-899.

Stadler, Astrid: Grenzüberschreitende Inkassotätigkeit nach dem Zessionsmodell in: Kubis, Sebastian/Peifer, Karl-Nikolaus/Raue, Benjamin/ Stieper,Malte, Festschrift für Haimo Schack zum 70. Geburtstag, Tübingen 2022, S. 499-515. (zit.: *Stadler,* FS Schack).

Stadler, Astrid: Die neue Verbands(abhilfe)klage – Umsetzung der Richtlinie 2020/1828, ZZP 136 (2023) 129-153.

Staudinger, Julius von (Begr.): Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen: EGBGB/IPR; Art 1-10 Rom I-VO (Internationales Vertragsrecht 1 – Internationales Devisenrecht) Berlin 2021.
Buch 1 Allgemeiner Teil §§ 134-138; ProstG (Gesetzliches Verbot; verfügungsverbot, Sittenwidrigkeit) Berlin 2021.
(zit.:Staudinger/*Bearbeiter*).

Steimer, Michael*:* Einführung in die Cyberversicherung, Karlsruhe 1. Auflage 2023.

Strasser, Philipp: Die Deckung von Schäden aus Kartellgeldbußen in der D&O-Versicherung, VersR 2017, 65-72.

Tehrani, Ramin: US Secondary Sanctions und ihre Bedeutung für die europäische Versicherungswirtschaft – das Ende der Neutralität?, VersR 2016, 85-95.

Thomas, Stefan: Bußgeldregress, Übelszufügung und D&O-Versicherung, NZG 2015, 1409-1419.

Thönissen, Stefan F.: Schadensersatz in der Verbandsabhilfeklage, r+s 2023, 749-758.

Trang, Minhquang N.: Compulsory Corporate Cyber-Liability Insurance: Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches, 18 Minnesota Journal of Law, Science & Technology, (2017), 389-425.

Visser, Marco/Dalisdas, Leonie: Blindgänger und Kriegsausschluss in der Haftpflichtversicherung, PHi 1/2025, 38-40.

Wagner, Gerhard: Prozeßverträge: Privatautonomie im Verfahrensrecht, Tübingen 1998.

Wagner, Rolf: Das Vermittlungsverfahren zur Rom II-VO, in: Baetge, Dietmar/von Hein, Jan/von Hinden, Michael (Hrsg.), Festschrift für Jan Kropholler zum 70. Geburtstag, Tübingen 2008, 715-735 (zit.: *R. Wagner*, FS Kropholler).

Wandt, Manfred: Internationale Produkthaftung, Heidelberg 1995.

Wandt, Manfred: Versicherungsrecht, München 6. Aufl. 2016.

Wandt, Manfred: Versicherungsverbote im Rahmen von Embargomaßnahmen, VersR 2013, 257–267.

Wandt, Manfred: Versicherungsverbote im Rahmen von Embargomaßnahmen, VersR 2013, 257-267.

Westermann, Harm Peter/Grunewald, Barbara/Maier-Reimer, Georg: Erman BGB, Band 3, Köln 2023 (zit.: Erman/*Bearbeiter*, BGB).

Wilhelmi, Rüdiger: Derivate und Internationales Privatrecht, RIW 2016, 253–260.

Wirth, Christian/Schreier, Vincent: Aktuelle Entwicklungen im Versicherungsaufsichts- und Versicherungsunternehmensrecht, r+s 2024, 49–57.

Wolff, Josephine: „Cyberwar by almost any definition": notpetya, the evolution of insurance war exclusions, and their application to cyberattacks, 28 Connecticut Insurance Law Journal (2021), 85-130.

Woods, Daniel W./Weinkle, Jessica: Insurance definitions of cyber war, The Geneva Papers on Risk and Insurance 45 (2020), 639-656.

Wurmnest, Wolfgang: Der Missbrauch einer marktbeherrschenden Stellung im europäischen Zuständigkeitsrecht (EuGH, S. 369), IPRax 2021, 340–345.

Wybitul, Tim/Hager, Timo: Keine „vom EU-Gesetzgeber gewollte Erleichterung" für die Verhängung von DS-GVO-Geldbußen?, MMR 2023, 321–322.

Wybitul, Tim/Klaas, Arne: Generalanwälte am EuGH zu DS-GVO-Bußgeldern, ZD 2023, 498–501.

Young, Richard W.: Insurance Meaning of War in Insurance Policies, 52 Michigan Law Review, (1956), 884-893.

Veröffentlichungen der Hamburger Gesellschaft zur Förderung des Versicherungswesens mbH

Bisher erschienen:

1 Prof. Dr. Norbert Horn
Die Allgemeinen Feuerversicherungsbedingungen (AFB) und das AGB-Gesetz
(vergriffen)

2 Der Versicherungsbedarf der deutschen Wirtschaft nach dem Jahr 2000
Dokumentation eines Symposiums
1985, 10,20 €

3 Dr. Ralf Johannsen
Haftpflichtversicherungsschutz gegen Umweltschäden durch Verunreinigung des Erdbodens und der Gewässer
(vergriffen)

4 Prof. Dr. Attila Fenyves
Die rechtliche Behandlung von Serienschäden in der Haftpflichtversicherung
1988, 10,20 €

5 Dr. Friedrich Hosse und Wolfgang Poppelbaum
Systemvergleich der privaten und der öffentlichen Gebäudeversicherung
(vergriffen)

6 Prof. Dr. Hans Hölemann
Der Brandbegriff im Versicherungswesen aus naturwissenschaftlicher und technischer Sicht
(vergriffen)

7 Dr. Werner Pfennigstorf
Regulierung und Deregulierung im Versicherungswesen der Vereinigten Staaten
1989, 10,20 €

8 Prof. Dr. Ulrich Hübner
Rechtsprobleme des Abrechnungsverkehrs in der Erstversicherung bei Einschaltung von Versicherungsmaklern
1991, 10,20 €

9 Dr. Jürgen Kagelmacher
Die Schadenfallkündigung im Versicherungsvertragsrecht
1992, 10,20 €

10 Die Betriebsschadenklausel in der Feuerversicherung
Dokumentation eines Symposiums
1990 *(vergriffen)*

11 Prof. Dr. Siegfried Schulze
Die Entwicklung des Versicherungswesens und des Versicherungsrechts in der Sowjetischen Besatzungszone und in der Deutschen Demokratischen Republik
1992, 10,20 €

12 Versicherung des Kriegsrisikos
Dokumentation eines Symposiums
1992, 10,20 €

13 Beiträge über den Versicherungsmakler
Ewald Lahno gewidmet
1993, 10,20 €

14 Dr. Renate Köcher
Wandel des gesellschaftlichen Umfelds der Versicherungswirtschaft
1993, 10,50 €

15 Prof. Dr. Peter Albrecht
Ansätze eines finanzwirtschaftlichen Portefeuille-Managements und ihre Bedeutung für Kapitalanlage- und Risikopolitik von Versicherungsunternehmen
(vergriffen)

16 Prof. Dr. Helmut Bujard
Zum Einfluß des gesamtwirtschaftlichen Strukturwandels auf die Schadenversicherung der Produktionsbereiche
1997, 14,30 €, 978-3-88487-600-8

17 Die künftigen Risiken der Industrie: Ursachen und Ansätze zu ihrer Bewältigung
Dokumentation eines Symposiums
1997, 17,90 €, 978-3-88487-627-5

18 Prof. Dr. Ulrich Hübner et al.
Berufsregelung für Versicherungsvermittler in Deutschland
1997, 18,50 €, 978-3-88487-642-8

19 Dr. Thomas Holzheu
Die Belastung von Versicherungsdienstleistungen mit Verkehrssteuern
1998, 17,80 €, 978-3-88487-676-3

20 Andrea Heß
Financial Reinsurance
1998, 18,– €, 978-3-88487-670-1

21 Dr. Erwin Eszler
Versicherbarkeit und ihre Grenzen
1999, 40,– €, 978-3-88487-795-1

22 Stefan Häusele
„Standort Deutschland" für Versicherungen
Eine vergleichende Analyse ausgewählter europäischer Länder
1999, 46,– €, 978-3-88487-799-9

23 Dr. Thomas Holzheu
Die Einbeziehung der Schaden-/Unfallversicherung in das Umsatzsteuersystem
2000, 18,50 €, 978-3-88487-824-8

24 Prof. Dr. Manfred Wandt
Änderungsklauseln in Versicherungsverträgen
2000, 29,80 €, 978-3-88487-893-4

25 Robert von Winter
Risikomanagement und Interne Kontrollen beim Sachversicherer
2001, 37,– €, 978-3-88487-920-7

26 Der Umgang mit den Risiken im Grenzbereich der Versicherbarkeit
Dokumentation eines Symposiums
2002, 16,– €, 978-3-89952-012-5

27 Prof. Dr. Thomas Hoeren,
Prof. Dr. Gerald Spindler
Versicherungen im Internet –
Rechtliche Rahmenbedingungen
2002, 44,– €, 978-3-89952-014-9

28 Dr. Gerd Umhau
Vergütungssysteme der Versicherungsvermittlung im Wandel
2003, 31,– €, 978-3-89952-029-3

29 Prof. Dr. Christian Armbrüster
Das Alles-oder-nichts-Prinzip im Privatversicherungsrecht
Zugleich ein Beitrag zur Reform des VVG
2003, 22,90 €, 978-3-89952-084-2

30 Pflichtversicherung
– Segnung oder Sündenfall –
Dokumentation eines Symposiums
2005, 32,– €, 978-3-89952-230-3

31 Dr. Andreas Horsch
Rating in der Versicherungswirtschaft
Eine ökonomische Analyse
2006, 32,– €, 978-3-89952-262-4

32 Prof. Dr. Peter Reiff
Versicherungsvermittlerrecht im Umbruch
2006, 32,– €, 978-3-89952-283-9

33 Dr. Christian Thomann
Terrorversicherung, Risikomanagement und Regulierung
2007, 37,– €, 978-3-89952-359-1

34 Ethik in der Assekuranz
Dokumentation eines Symposiums
2008, 29,– €, 978-3-89952-388-1

35 Harald Krauß
Die Vergütung des Versicherungsmaklers im Rahmen internationaler Entwicklungen
2009, 29,– €, 978-3-89952-518-234

36 Fluch und Segen der Kapitalmärkte für die Versicherungswirtschaft
Dokumentation eines Symposiums
2010, 27,– €, 978-3-89952-545-8

37 Die Mehrfachaufsicht von Versicherungsunternehmen durch Aufsichts rat, BaFin und Wirtschaftsprüfer –
Duplizierung oder Ergänzung?
Dokumentation eines Symposiums
2011, 35,– €, 978-3-89952-465-9

38 Prof. Dr. Andreas Horsch,
Tanja Rathman
Kreditrisikotransfer durch
Kreditversicherung
Eine ökonomische Analyse der Prozesse, Strukturen und Regeln der Märkte für Kreditversicherungen
2012, 42,– €, 978-3-89952-665-3

39 Lena Rudkowski
Geschäftsgeheimnisse
des Versicherers
2012, 35,– €, 978-3-89952-701-8

40 Dr. Henning Schaloske
Folgerungen aus der Dornbracht-Entscheidung für die Praxis der offenen Mitversicherung
2013, 35,– €, 978-3-89952-757-5

41 Dr. Dominik Klimke
Information der Versicherten über vorvertragliche Anzeigepflichten und die Folgen ihrer Verletzung
2019, 37,– €, 978-3-96329-2699

Bestellungen sind zu richten an:
vertrieb@vvw.de
www.vvw.de

Hamburger Gesellschaft zur Förderung des Versicherungswesens mbH, Hamburg

Die HGFV wurde 1982 mit einer Kapitalausstattung von 1.000.000 DM von Jauch & Hübener – heute Aon – errichtet.

Gegenstand der Gesellschaft ist die Förderung von Untersuchungen und wissenschaftlichen Arbeiten im Bereich des Versicherungswesens und des Risikomanagements.

Neben der Organisation und Durchführung von Symposien mit prominenten Vertretern aus Wissenschaft und Wirtschaft dienen dazu auch das Unterstützen und Herausgeben von Publikationen zu Themen mit Bezug zum Versicherungswesen.

Bei ihrer Arbeit wird die Gesellschaft durch einen Beirat unterstützt, dem namhafte Vertreter aus Versicherungswirtschaft, Dienstleistung, Industrie und Wissenschaft angehören. Der Beirat lenkt und überwacht die Vergabe der nicht interessengebundenen Aufträge.

9 783963 295614 (D) 06480
vvw.de