

Inhaltsübersicht

Inhaltsverzeichnis	XV
Abkürzungsverzeichnis	XXVII
Einleitung	1
1. Kapitel: Problemstellung und Erkenntnisinteresse	5
A. Problemstellung	5
B. Gang der Untersuchung und Erkenntnisinteresse	9
2. Kapitel: Die Cyberversicherung und die Grenzen der Versicherbarkeit	13
A. Grundlagen der Cyberversicherung	13
B. Grenzen der Versicherbarkeit von Löse- und Bußgeldern	34
3. Kapitel: Die Versicherbarkeit von Lösegeldzahlungen bei Ransomware	39
A. Grundlegendes zu Ransomware	39
B. Lösegeldzahlungen in der Cyberversicherung	51
C. Rechtliche Zulässigkeit von Lösegelddeckungen in der Cyberversicherung	74
D. Zusammenfassung der wesentlichen Ergebnisse zur Versicherung von Lösegeldern bei Ransomware.....	156
4. Kapitel: Die Versicherbarkeit von Bußgeldern bei Datenschutzverstößen	159
A. Grundlagen und Problemdarstellung.....	159
B. Bußgelder in der Cyberversicherung.....	171
C. Rechtliche Zulässigkeit von Bußgelddeckungen in der Cyberversicherung	185
5. Kapitel: Schlussbetrachtung	239
A. Abschließende Stellungnahme	239
B. Ausblick.....	245
C. Zusammenfassung der wesentlichen Ergebnisse in Thesen ..	246
Quellenverzeichnis	251

XIII

Inhaltsverzeichnis

Inhaltsübersicht	XIII
Abkürzungsverzeichnis	XXVII
Einleitung	1
1. Kapitel: Problemstellung und Erkenntnisinteresse	5
A. Problemstellung	5
I. Zur Versicherbarkeit von Lösegeldzahlungen bei Ransomware	6
II. Zur Versicherbarkeit von Bußgeldern bei Datenschutzverstößen	8
B. Gang der Untersuchung und Erkenntnisinteresse	9
2. Kapitel: Die Cyberversicherung und die Grenzen der Versicherbarkeit	13
A. Grundlagen der Cyberversicherung	13
I. Begriff der Cyberversicherung	13
II. Dynamische Marktsituation	14
III. Versicherte Gefahren im Überblick.....	16
1. Neuartige Angriffsmodelle	18
2. Hohes Schadenspotenzial	19
3. Unternehmen als Ziele von Angriffen	19
IV. Die Cyberversicherung am Beispiel marktüblicher Policen	21
1. Überblick zu verschiedenen Deckungskonzepten	21
2. Der versicherte Gegenstand am Beispiel der AVB-Cyber.....	22
a. Vermögensschaden	22
b. Eintritt einer Informationssicherheitsverletzung	23

c.	Versicherte Ereignisse	24
aa.	Angriff auf elektronische Daten und informationsverarbeitende Systeme (Spiegelstrich 1)	25
bb.	Unberechtigter Zugriff auf elektronische Daten (Spiegelstrich 2)	25
cc.	Eingriffe in informationsverarbeitende Systeme (Spiegelstrich 3)	26
dd.	Verletzung datenschutzrechtlicher Vorschriften (Spiegelstrich 4)	26
ee.	Schadprogramme, die auf Daten oder Systeme wirken (Spiegelstrich 5)	27
3.	Versicherter Gegenstand in anderen marküblichen Policen	27
4.	Eintritt des Versicherungsfalls	29
5.	Obliegenheiten	31
6.	Typische Risikoausschlüsse: Krieg, Terror, Lösegelder und Bußgelder	32
V.	Versicherungsrechtliche Einordnung der Cyberversicherung	33
B.	Grenzen der Versicherbarkeit von Löse- und Bußgeldern	34
I.	Ökonomische Grenzen der Versicherbarkeit	34
1.	Zweifelsfreie Risikodefinition	35
2.	Zufälliger Eintritt des Schadensereignisses	35
3.	Kalkulierbarkeit des Schadens	36
II.	Rechtliche Grenzen der Versicherbarkeit	37
3.	Kapitel: Die Versicherbarkeit von Lösegeldzahlungen bei Ransomware.....	39
A.	Grundlegendes zu Ransomware	39
I.	Zum Begriff Ransomware	39
II.	Kursorischer Entwicklungsüberblick	40

III. Technische Katalogisierung	43
IV. Aktuelle Bedrohungslage durch Ransomware	44
1. Neuartige Angriffsmethoden	46
a. Phishing	47
b. Drive-by-Exploits.....	47
c. Back-ups und Sicherheitskopien als Angriffsziel.....	48
2. Unterschiedliche Erpressungsmethoden	49
3. Zunehmender Wettbewerb durch Ransomware- as-a-Service	50
V. Zwischenergebnis	51
B. Lösegeldzahlungen in der Cyberversicherung	51
I. Zur Auslegung von Versicherungsbedingungen.....	52
II. Lösegelder als versichertes Risiko	53
1. Definition des Lösegeldbegriffs.....	53
2. Lösegeldzahlungen im Kontext marktüblicher Deckungskonzepte	54
a. Versicherungsfall nach den AVB-Cyber.....	54
aa. Ransomware als Informationssicherheitsverletzung.....	55
bb. Lösegeldzahlungen als Vermögensschaden.....	56
cc. Ransomware als versichertes Ereignis	56
b. Ransomware als definierte Tathandlung.....	58
c. Ransomware als Netzwerksicherheitsverletzung.....	58
3. Bestimmung des Versicherungsfalls.....	59
a. Zur Beweislastverteilung bei vorvertraglichen Ransomwareattacken	60
b. Anwendung des Schadensereignisprinzips	60
c. Anwendung des Manifestationsprinzips.....	61

4. Einschränkungen der Leistungspflicht bei Lösegeldern	62
a. Ransomware als Kriegs- und Terrorwaffe.....	62
aa. Reichweite üblicher Ausschlussklauseln für Krieg und Terror	63
(1) Auslegung des Kriegsbegriffs.....	63
(2) Auslegung des Terrorbegriffs	67
bb. Der Fall Merck ./ Ace American.....	68
cc. Der Fall Mondelez ./ Zurich Versicherungen	70
dd. Zwischenergebnis	72
b. Ausschluss bei Verstößen gegen Sanktionen und Embargobestimmungen	74
C. Rechtliche Zulässigkeit von Lösegelddeckungen in der Cyberversicherung	74
I. Versicherungsaufsichtsrechtliche Perspektive	75
1. Erlaubnis zum Geschäftsbetrieb gem. 8 ff. VAG	76
a. Anspruch auf Zulassung gem. 8 Abs. 1 VAG.....	76
b. Eingriff eines Versagungsgrundes	76
aa. Keine dauernde Erfüllbarkeit der Verpflichtungen gem. § 11 Abs. 1 Nr. 1 VAG	77
bb. Gefährdung der Belange der Versicherten gem. § 11 Abs. 1 Nr. 4 lit. a VAG	77
cc. Umfang der aufsichtsbehördlichen Prüfpflicht	78
2. Missstandsaufsicht gem. § 294 Abs. 2 VAG	79
3. Aufsichtsrechtliche Entwicklung von Lösegeldbausteinen in der Cyberversicherung.....	80
a. Aufhebung des Bündelungsverbotese	81
b. Fortgeltung übriger Rahmenvorgaben des BAV aus dem Jahr 1998	82

c. Kritische Betrachtung der aufsichtsbehördlichen Rahmenvorgaben	83
4. Ergebnis zur versicherungsaufsichtsrechtlichen Zulässigkeit.....	85
II. Privatrechtliche Perspektive	85
1. Verstoß gegen ein gesetzliches Verbot	
i. S. v. § 134 BGB	86
a. Verstoß gegen strafrechtliche Verbotsgesetze	86
aa. Unterstützung krimineller Vereinigungen gem. § 129 Abs. 1 S. 2 Var. 1 StGB	87
(1) Tatbestandsmäßigkeit der Lösegeld- zahlung.....	88
(i) Hacker als kriminelle Vereinigung i. S. d. § 129 Abs. 1 StGB	89
(α) Anonymität der Hacker.....	90
(β) Keine Bestimmung organisa- torischer Verbundenheit	92
(ii) Lösegeld als Unterstützungshandlung ..	93
(iii) Anwendbarkeit des Tatbestands bei Zahlungen an ausländische Vereinigungen	94
(iv) Subjektiver Tatbestand.....	95
(2) Rechtswidrigkeit: die Lösegeldzahlung als gerechtfertigte Handlung	97
(i) Rechtfertigung nach § 34 StGB.....	97
(α) Lösegeldzahlung als erforder- liches Mittel der Gefahrenabwehr....	98
(β) Abwägung der widerstreitenden Interessen im Nötigungsnotstand ..	100
(γ) Stellungnahme: Notwendigkeit eines vermittelnden Recht- fertigungsansatzes	102

(ii) Zwischenergebnis	107
(3) Entschuldigender Notstand	108
(4) Verbotsirrtum.....	109
(5) Ergebnis zur Strafbarkeit nach § 129 Abs. 1 S. 2 Var. 1 StGB.....	109
bb. Unterstützung einer terroristischen Vereinigung gem. § 129a Abs. 5 StGB	110
cc. Geldwäsche gem. § 261 StGB.....	110
dd. Zwischenergebnis	111
b. Verstoß gegen unionsrechtliche Sanktions- und Embargobestimmungen.....	111
aa. EU-Namenslisten	112
(1) EU-Cyber-Verordnung Nr. 796/2019.....	112
(2) EU-Terror-Verordnung Nr. 2580/2001.....	113
bb. Ergebnislosigkeit des Listenabgleichs.....	114
2. Verstoß gegen die guten Sitten i. S. v. § 138 Abs. 1 BGB.....	115
a. Voraussetzungen eines sittenwidrigen Versicherungsvertrages	116
b. Vereinbarkeit der Lösegeldversicherung mit einer effektiven Generalprävention	117
3. Auswirkungen von Verstößen gegen ausländische Rechtsnormen	119
a. Rechtsvergleichende Umschau: Lösegeld- zahlungsverbote bei Ransomware in den USA und England.....	121
aa. US-amerikanische Sanktionsvorschriften.....	121
(1) US Secondary Sanctions	122
(i) Extraterritorialität von US Secondary Sanctions	123

(ii) Specially Designated Nationals and Blocked Persons List.....	124
(2) Antiterrorism and Effective Death Penalty Act	127
(3) Zwischenergebnis	127
bb. Lösegeldverbote auf dem englischen Markt.....	128
(1) Terrorism Act 2000.....	130
(2) Proceeds of Crime Act 2002.....	132
(3) Zwischenergebnis	132
b. Anwendung ausländischer Verbotsgesetze durch deutsche Gerichte.....	132
aa. Lösegeldzahlungsverbote als Eingriffsnormen i. S. v. Art. 9 Rom I-VO.....	133
(1) Voraussetzungen des Art. 9 Abs. 1 Rom I-VO	134
(i) Zwingende Vorschrift mit internationalem Geltungsanspruch	134
(ii) Überindividueller Normzweck.....	137
(2) Voraussetzungen des Art. 9 Abs. 3 Rom I-VO	138
(i) Geltung der Verbotsvorschriften am Erfüllungsort	138
(ii) Übereinstimmung zwischen deutscher Rechtsordnung und Wertungen der Verbotsvorschriften	141
bb. Zwischenergebnis	143
c. Anwendung des Art. 9 Abs. 3 Rom I-VO für Verbotsvorschriften ohne Geltungsanspruch am Erfüllungsort.....	144
aa. Sperrwirkung des Art 9 Abs. 3 Rom I-VO.....	145

bb.	Zulässigkeit der materiellrechtlichen Berücksichtigung.....	146
d.	Materiellrechtliche Berücksichtigung ausländischer Verbotsnormen	147
aa.	Anwendbarkeit des § 138 Abs. 1 BGB.....	148
bb.	Ausländische Verbotsvorschriften als tatsächliche Grundlage der Sittenwidrigkeit von Lösegelddeckungen	150
(1)	Zur Sittenwidrigkeit im Kontext der Rechtsprechung des BGH.....	151
(2)	Mittelbarer Schutz deutscher Interessen ...	151
(3)	Verbotsvorschrift dient der internationalen Staatengemeinschaft	154
4.	Ergebnis zur bürgerlich-rechtlichen Untersuchung	156
D.	Zusammenfassung der wesentlichen Ergebnisse zur Versicherung von Lösegeldern bei Ransomware.....	156
4.	Kapitel: Die Versicherbarkeit von Bußgeldern bei Datenschutzverstößen.....	159
A.	Grundlagen und Problemdarstellung.....	159
I.	Ausgangslage.....	162
1.	Zunehmende Datenschutzverstöße.....	162
2.	Konsequente Sanktionierung: Wettlauf der Bußgeldhöhen	163
3.	Cyberangriffe und Datenschutzverstöße	165
II.	Überblick über bestehende Datenschutzgesetze	166
1.	Die Datenschutzgrundverordnung	166
2.	Ergänzende Vorgaben des BDSG	167
3.	Einfluss der europäischen Rechtsprechung: Das „Schrems-II-Verfahren“.....	167
4.	Drittstaatliche Datenschutzvorschriften	168

III.	Bußgeldrisiken und ihre gesetzlichen Grundlagen	169
	1. Art. 83 DSGVO	169
	2. § 43 BDSG	170
	3. Drittstaatliche Bußgeldvorschriften	171
B.	Bußgelder in der Cyberversicherung.....	171
I.	Bußgelder als versicherter Gegenstand in marktüblichen Cyberdeckungskonzepten.....	172
	1. Bußgelder als Vermögensschaden.....	172
	2. Bußgeldzahlungen als versichertes Ereignis nach den AVB-Cyber.....	173
	3. Bußgelder als Versicherungsfall in anderen marktüblichen Bedingungswerken.....	174
	a. Datenschutzverletzung	175
	b. Vertraulichkeitsverletzung.....	175
	c. Netzwerksicherheitsverletzung	176
II.	Internationale Dimension des Versicherungsschutzes	177
	1. California Consumer Privacy Act.....	177
	2. Personal Information Protection Law of the People's Republic of China	179
	3. UK Data Protection Act 2018.....	180
III.	Sekundäre Risikobeschreibung des Versicherungsschutzes	181
	1. Datenschutzverletzung „nicht vorsätzlich oder nicht durch den VN begangen“.....	181
	2. Datenschutzverletzung „erstmalig während der Vertragslaufzeit“	183
	3. Versicherungsschutz im Rahmen der „rechtlichen Zulässigkeit“	183

C. Rechtliche Zulässigkeit von Bußgelddeckungen in der Cyberversicherung	185
I. Versicherbarkeit von in Deutschland verhängten Bußgeldern.....	186
1. Zulässigkeit des Bußgeldregresses	186
2. Unternehmen als Bußgeldadressaten	189
a. LG Bonn: Datenschutzrechtliche Verbandshaftung von Unternehmen	189
b. LG Berlin: Erfordernis der persönlichen Verantwortlichkeit.....	191
c. Stellungnahme	192
3. Versicherungsaufsichtsrechtliche Perspektive.....	193
4. Privatrechtliche Perspektive	194
a. Verstoß gegen ein gesetzliches Verbot i. S. v. § 134 BGB	194
aa. Straf- und Vollstreckungsvereitelung gemäß § 258 Abs. 1, 2 StGB	195
bb. Begünstigung gemäß § 257 StGB.....	196
cc. Untreue gemäß § 266 StGB.....	197
dd. Beteiligungshandlung gemäß § 27 StGB und § 14 OWiG	198
ee. Gewohnheitsrechtlich anerkannte Verbotsgesetze	198
b. Verstoß gegen die guten Sitten i. S. v. § 138 Abs. 1 BGB	199
aa. Meinungsstand zur Sittenwidrigkeit der Deckung von Bußgeldern.....	199
bb. Sittenwidrigkeit der Deckung von DSGVO-Bußgeldern	201
(1) Beeinträchtigung des Sanktions- und Präventionszwecks.....	201

(i)	Sanktionsgrundlagen.....	202
(α)	Bußgelder nach Art. 83 Abs. 4 DSGVO	203
(β)	Bußgelder nach Art. 83 Abs. 5 DSGVO	204
(γ)	Bußgelder nach Art. 83 Abs. 6 DSGVO	205
(ii)	Zweck und Leitfunktionen von DSGVO-Bußgeldern.....	205
(iii)	Beeinträchtigung der Abschreckungswirkung	206
(2)	Verringerte Hemmschwelle bei fahr- lässigen Datenschutzverletzungen.....	211
c.	Zwischenergebnis.....	216
II.	Versicherung von im Ausland verhängten Bußgeldern	216
1.	Anwendbares Recht im Kontext der rechtlichen Zulässigkeit.....	217
2.	Vertragliche Reichweite des Versicherungsschutzes ..	218
a.	Rechtliche Zulässigkeit nach der bußgeldverhängenden Rechtsordnung.....	219
b.	Zulässigkeit im Kontext mehrerer Rechts- ordnungen.....	221
3.	Materiellrechtliche Berücksichtigung ausländischer Verbotsnormen	223
a.	Versicherbarkeit von Bußgeldern im Ausland	224
aa.	Versicherbarkeit von Bußgeldern im europäischen Ausland.....	224
bb.	Versicherbarkeit von Bußgeldern in den USA..	227
(1)	Verhängung von civil penalties nach US-amerikanischen Recht.....	227

(2) Versicherbarkeit von civil penalties nach US-amerikanischem Recht.....	228
(i) Versicherbarkeit in Delaware	228
(ii) Versicherbarkeit in Kalifornien.....	229
(iii) Zwischenergebnis	231
b. Widerspruch zur deutschen Rechtsordnung	231
aa. Ausländische DSGVO-Bußgelder	232
bb. Drittstaatliche Bußgelder	232
cc. Sonderfall: Willkürlich verhängte Bußgelder aus Drittstaaten	235
4. Zwischenergebnis.....	235
III. Rechtsfolge.....	236
D. Stellungnahme: Versicherungsschutz für Bußgelder als Potemkinsches Dorf	236
5. Kapitel: Schlussbetrachtung	239
A. Abschließende Stellungnahme	239
I. Zur Versicherung von Lösegeldern bei Ransomware.....	239
II. Zur Versicherung von Bußgeldern bei Datenschutz- verstößen	243
B. Ausblick.....	245
C. Zusammenfassung der wesentlichen Ergebnisse in Thesen ..	246
Quellenverzeichnis	251
A. Literatur.....	251
B. Sonstige Quellen.....	267