

Daniel Wittig

# Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten



**Nomos**

**Schriften zum Medien- und Informationsrecht**

herausgegeben von  
Prof. Dr. Boris P. Paal, M.Jur.

**Band 50**

Daniel Wittig

# Die produzentenrechtlichen Verkehrssicherungspflichten von Softwareproduzenten



**Nomos**



Onlineversion  
Nomos eLibrary

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

Zugl.: Münster, Univ., Diss., 2020

ISBN 978-3-8487-7042-7 (Print)

ISBN 978-3-7489-1091-6 (ePDF)

**D 6**

1. Auflage 2021

© Nomos Verlagsgesellschaft, Baden-Baden 2021. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

## Vorwort

Die vorliegende Arbeit wurde im August 2020 von der rechtswissenschaftlichen Fakultät der Westfälischen Wilhelms-Universität Münster (WWU) als Dissertation angenommen. Sie entstand neben meiner beruflichen Tätigkeit als Rechtsanwalt in einer mittelständischen Wirtschaftskanzlei in Paderborn und unter Betreuung durch meinen Doktorvater Herrn Prof. Dr. Hoeren, dem Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) an der WWU. Ihm Danke ich u. a. für seine teils harsche Kritik, die zur Fokussierung der Arbeit auf das Wesentliche führte und so maßgeblich zum Gelingen dieser beitrug. Ebenfalls danke ich Herrn Prof. Dr. Fabian Gieseke vom Lehrstuhl Maschinelles Lernen und Data Engineering für die rasche Erstellung des Zweitgutachtens. Mein Dank gilt auch meinen Arbeitskollegen, die Rücksicht auf meine nebenberufliche Promotion nahmen und mich nach Möglichkeit unterstützen.

Während meiner Zeit im Referendariat wurde ich von einem meiner Mentoren auf die Problematik der Haftung von Softwareproduzenten aufmerksam gemacht. Ich musste feststellen, dass wir die für die Haftung wesentlichen Verkehrssicherungspflichten kaum bestimmen konnten. Ab diesem Zeitpunkt stand für mich fest, dass ich einen wissenschaftlichen Beitrag zu diesem Thema leisten wollte, um an der Lösung des Problems mitzuwirken.

Mein ganz besonderer Dank geht an meine Eltern, Petra und Werner Tanger, sowie an meine Ehefrau Katarina. Meine Eltern unterstützten stets vorbehaltlos meinen Lebensweg und die Entscheidungen, die ich auf diesem getroffen habe. Sie ermöglichten mir meine Ausbildung, welche die Basis für meine persönliche und berufliche Entwicklung geworden ist. Nur durch Sie konnte ich mich immer auf meine Ziele konzentrieren, ohne mir Sorgen machen zu müssen. Meine Frau Katarina, welche seit dem Jahr 2016 an meiner Seite ist, gibt mir darüber hinaus in jeder Lebenslage ein unglaubliches Maß an Unterstützung, Rückhalt und Liebe. Ohne ihren Zuspruch und ihr Durchhaltevermögen hätte ich diese Arbeit wohl nicht vollenden können. All dies hat im wesentlichen Maße zum Gelingen dieser Arbeit beigetragen.

Paderborn, im November 2020

Daniel Wittig



# Inhaltsverzeichnis

A. Einleitung	19
I. Die steigende Bedeutung von Software für Wirtschaft und Gesellschaft	20
II. Sicherheit von Software als gesamtgesellschaftliches deliktsrechtliches Problem	21
III. Die Herstellung fehlerfreier Software unter ökonomischen Gesichtspunkten	23
IV. Verkehrssicherungspflichten – Kernstück der Produzentenhaftung	26
B. Begriffsdefinitionen	28
I. Software und Softwareproduzent	28
II. Daten	29
III. IT-Sicherheit und Datensicherheit	30
1. Der Begriff der IT-Sicherheit	30
a) Schutzgüter der IT-Sicherheit	32
aa) Verfügbarkeit	32
bb) Vertraulichkeit	32
cc) Integrität	33
dd) Authentizität	33
ee) Interdependenz der Schutzgüter	33
b) Bedeutung der IT-Sicherheit	34
c) Abgrenzung der IT-Sicherheit von der Produktsicherheit	34
2. Ableitung des Begriffs der Datensicherheit	35
3. Abgrenzung der Datensicherheit vom Datenschutz	35
IV. Schwachstelle	36
C. Deliktische Haftungsrisiken und die Produzentenhaftung	39
I. Deliktisches Haftungsrisiko für Softwareproduzenten	39
1. Zweiseitige Inanspruchnahme möglich	39
2. Steigerung der Angriffsfläche durch IT und Vernetzung	41
3. Bisherige Tätigkeit des Gesetzgebers	41

II. Die Entwicklung der Produzentenhaftung	42
1. Die Schaffung der Produzentenhaftung	42
2. Verletzung einer Verkehrssicherungspflicht	44
3. Entwicklung von Beweiserleichterungen	45
III. Weiterhin offene Fragestellungen im Deliktsrecht	45
1. Entscheidungen autonomer Systeme	46
2. Daten als Rechtsgutverletzung	47
3. Kausalitätsprobleme	47
4. Verschuldensnachweis	48
5. Bestimmung von Verkehrssicherungspflichten	49
IV. Versicherbarkeit der Haftungsrisikos	50
V. Geltung der Produzentenhaftung für die Softwareerstellung	50
D. Die geltenden Verkehrssicherungspflichten	52
I. Konstruktionspflichten	55
1. Sicherheitserwartungen des Verkehrs	56
2. Erkennbarkeit des Fehlers bei einem Inverkehrbringen	57
3. Abgrenzung zum Entwicklungsfehler	57
II. Fabrikationspflichten	58
III. Instruktionspflichten	59
1. Erkennbarkeit der Gefahr bei einem Inverkehrbringen	60
2. Inhalt und Ausgestaltung der Instruktionspflichten	60
3. Umfang der Instruktionspflichten	61
IV. Produktbeobachtungspflichten	62
1. Haftungsgrund der Produktbeobachtungspflichten	64
2. Umfang der Produktbeobachtungspflicht	64
3. Zeitraum statt Zeitpunkt der Pflichterfüllung	65
4. Ende der Produktbeobachtungspflichten	65
5. Handlungspflicht bei Entdeckung eines Fehlers	66
a) Warnpflicht	67
b) Gefahrverdacht	67
c) Konstruktionsänderung	68
d) Rückrufverpflichtung	69
aa) Äquivalenz- vs. Integritätsinteresse	69
bb) Cheapest Cost Avoider	70
cc) Neben Rücknahme auch Reparatur	72
dd) Bestimmung im Einzelfall notwendig	73



ee) Kein subjektiver Anspruch des Nutzers	74
E. Die Ausgestaltung der Verkehrssicherungspflichten für Softwareproduzenten	75
I. Keine Entlastung bei Eingriffen durch Hacker	75
II. Maßstab für die Ermittlung der Verkehrssicherungspflichten	77
1. Einflussfaktor der Verkehrserwartung an Software	78
a) Einzelfallentscheidung – Kriterium des Absatzmarktes	79
b) Einzelfallentscheidung – Kriterium des Nutzerkreises	80
2. Einflussfaktor „aktueller Stand von Wissenschaft und Technik“	80
a) Abgrenzung vom Stand der Technik	80
aa) Verwendung unbestimmter Rechtsbegriffe	81
bb) Inhaltliche Unterscheidung	82
b) Heranziehung des Standes von Wissenschaft und Technik	83
c) Konkretisierung des Standes von Wissenschaft und Technik	85
d) Bildung des Standes von Wissenschaft und Technik in der IT-Branche	85
aa) Schwerpunkt Ausland	86
bb) Beeinflussung durch Marktführer	86
cc) Erweiterung der Einflussfaktoren	87
e) Einfluss technischer Standards und Zertifizierungen auf den aktuellen Stand von Wissenschaft und Technik	88
aa) Technische Standards	89
bb) Technische Standards sind keine verbindlichen Rechtsnormen	89
cc) Problem der Bestimmtheit eines technischen Standards	90
dd) Praktische Bedeutung von technischen Standards	91
(1) Keine Entlastung durch Einhaltung technischer Standards	91
(2) Technische Standards als Ansatzpunkt der Konkretisierung unbestimmter Rechtsbegriffe	92
f) Änderung des Standes von Wissenschaft und Technik nach einem Inverkehrbringen	93
g) Einhaltung des Standes von Wissenschaft und Technik durch Zertifizierung	93
aa) Begriff der Zertifizierung	94

bb) Keine Entlastung durch eine Zertifizierung	94
(1) Statische Zertifikate	94
(2) Ausnahme: Öffentliches Recht	95
h) Einfluss von Zertifizierungen auf Verkehrssicherungspflichten	95
i) Besonderheiten im IT-Sektor	95
aa) Common Criteria – aktueller Einfluss und zukünftige Möglichkeiten	97
(1) Ausgestaltung der Common Criteria	98
(2) Common Criteria als Selbstverpflichtung	99
(3) Vorteile der Common Criteria für die Produzenten	99
(4) Hürden für die Produzenten	100
(5) Zukünftige Möglichkeiten der Common Criteria	100
bb) Protection Profiles	101
(1) Aufbau der Protection Profiles	102
(2) Anwendungsbereich einzelner Protection Profiles	102
(3) Zukünftige Möglichkeiten der Protection Profiles	103
cc) Security Design Principles	103
dd) Branchenspezifische Standards (Beispiel: PCI-DSS)	104
ee) Secure Coding Guidelines	104
ff) Einfluss von unbekanntem Zertifikaten auf die Verkehrssicherungspflichten von Softwareproduzenten	105
(1) Bestehen unbekannter Zertifikate	105
(2) Auswirkungen von im Verkehr unbekanntem Zertifikaten	106
3. Einflussfaktor Cybersecurity Act	107
a) Allgemeine Ziele	107
b) Sicherheitsziele	108
aa) Harmonisierung	109
bb) Fragmentierung	110
cc) Konkrete Sicherheitsziele	110
c) Ausgestaltung des Zertifizierungsverfahrens	111
aa) Keine Einführung operativer Zertifizierungssysteme	111
bb) Rückgriff auf technische Normen	111
cc) Unterschiedliche Ansätze und Sicherheitsstufen für die Schemata	112
dd) Freiwilligkeit der Zertifizierung	112
d) Rolle der Cybersicherheitsbehörde ENISA	113

e) Auswirkungen der Verordnung auf Softwareproduzenten – Erhöhung des Sicherheitsstandards	114
4. Einflussfaktor DS-GVO auf die Verkehrssicherungspflicht	115
a) Datenschutz ungleich Datensicherheit	116
b) Anwendungsbereich der DS-GVO	116
aa) Sachlicher Anwendungsbereich	117
bb) Räumlicher Anwendungsbereich	118
cc) Persönlicher Anwendungsbereich	118
(1) Verantwortlicher	119
(2) Auftragsverarbeiter	119
(3) Hersteller – Softwareproduzenten	120
(4) Mittelbare Anwendbarkeit der DS-GVO auf Softwareproduzenten	121
(a) Hersteller als Adressat des Art. 25 DS-GVO – Datenschutz durch Technikgestaltung	122
(b) Hersteller als Adressat des Art. 32 DS-GVO – Sicherheit der Verarbeitung	124
(c) Hersteller als Adressat des Art. 42 DS-GVO – Zertifizierungsmaßnahmen	124
c) Bindung der Produzenten an die Pflichten der DS-GVO	125
aa) Konkretisierung der Verkehrssicherungspflichten	125
(1) Stand von Wissenschaft und Technik	126
(a) Diskrepanz: „Stand der Technik“ und „Stand von Wissenschaft und Technik“	127
(b) Umsetzungserschweris aufgrund fehlender verbindlicher Leitlinien	129
(c) Rückgriff auf bereits bestehende Normen unzureichend	129
(2) Erwartungshaltung der Verantwortlichen	131
(a) Notwendigkeit der präzisen Abgrenzung bei der Verkehrserwartung	132
(b) Keine direkte Verpflichtung über Verkehrssicherungspflichten möglich	132
(c) Indirekte Verpflichtung	133
(3) Zumutbarkeit	134
(4) Zwischenfazit zu den Auswirkungen der DS-GVO	135
(a) Verschiebung der Nachfrage	135
(b) Keine Bußgelder, aber Schäden	136
bb) Erste Schritte mit und durch die DS-GVO	137
(1) Beispiel: Produktbeobachtungspflicht	137

(2) Beispiel: Konstruktionspflichten	138
(3) Beispiel: Instruktionspflichten	138
cc) Möglichkeit der Einhaltung datenschutzrechtlicher Vorschriften	138
d) Die (mittelbaren) Pflichten der DS-GVO für Softwareproduzenten	139
aa) Grundsätze der Datenverarbeitung, Art. 5 DS-GVO	140
(1) Neuausrichtung der Grundsätze der Datenverarbeitung	140
(2) Bezugnahme auf die Sicherheit der Datenverarbeitung	141
bb) Datenschutz durch Technikgestaltung und Voreinstellung, Art. 25 DS-GVO	142
(1) Anforderungen der Norm	143
(a) Privacy by Design	143
(b) Privacy by Default	143
(c) Organisatorische Maßnahmen	144
(2) Umsetzung der Norm	144
(a) Frühe Berücksichtigung der Einzelmaßnahmen	145
(b) Die wirtschaftliche Komponente der Umsetzung	145
(c) Datenschutz durch Technikgestaltung	146
(d) Datenschutz durch Voreinstellung	148
cc) Sicherheit der Verarbeitung, Art. 32 DS-GVO	149
(1) Anforderungen der Norm	149
(2) Umsetzung der Norm	150
(a) Konkret benannte Maßnahmen	151
(b) Weitere – technisch unbenannte – Maßnahmen des Art. 32 DS-GVO	151
dd) Zertifizierungsmaßnahmen, Art. 42 DS-GVO	154
(1) Ziele der Zertifizierung	154
(2) Zertifikat für Produzenten	154
ee) Data Breach Notification, Art. 33 DS-GVO	156
5. Einflussfaktor „EU-Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte“	156
a) Anwendungsbereich	157
b) Updatepflicht – Mangelbegriff	158
c) Grenze der Unverhältnismäßigkeit	159

d) Gewährleistungsfrist	159
e) Mögliche Auswirkungen auf die Verkehrssicherungspflichten der Softwareproduzenten	160
III. Die Konstruktionspflichten der Softwareproduzenten	161
1. Schlüsselfrage: Sind Fehler bei einem Inverkehrbringen erkennbar?	164
a) Möglichkeit der fehlerfreien Erstellung von Software	164
aa) Falschaussage: Fehlerfreie Erstellung nicht möglich	165
bb) Gründe für die Fehlerhaftigkeit von Software	166
(1) Gestiegene Komplexität	167
(a) Mehr Code, mehr Fehlermöglichkeiten	167
(b) Erschwerung der Testbedingungen	168
(2) Kosten für Qualitätssicherung	168
(3) Missmanagement	169
(a) Qualitätssicherung als Geldverschwendung	169
(b) Fehlerhafte Zeit- und Kostenplanung	170
(c) Lückenhafte Dokumentation	171
(d) Wartungsverträge	171
(4) Marktgegebenheiten	171
(a) Nachgefragte Qualität	171
(b) Unklare Anforderungen an Software	173
(c) Verkürzte Produktzyklen	173
(d) Wettbewerbsnachteil Fehlerfreiheit	174
(5) Fehlende Cybersicherheitskenntnisse	174
(6) Agile Programmiermethoden	175
(7) Alterung der Software	176
b) Korrektur der These	177
2. Konstruktionspflichten der Softwareproduzenten	177
a) Keine Ausnahme von den Konstruktionspflichten	178
b) Abschwächung der Konstruktionspflichten durch Verkehrserwartung	179
c) Einzelne Konstruktionspflichten	180
aa) Konstruktive und analytische Qualitätssicherung	181
bb) Organisationspflichten im Arbeitsablauf – konstruktive Maßnahmen	182
(1) Organisation des Betriebs und des Arbeitsablaufs	182
(2) Einsatz eines Versionsverwaltungssystems	185
(3) Entwicklungs- und Testdokumentationen	185
(4) Absicherung der Entwicklungsumgebung	186
(5) Einzelfallentscheidung	186

cc) Analytische / Technische Prüfpflichten	187
(1) Automatisierte Prüfungstools (Debugging)	187
(a) Teilautomatisierte werkzeuggestützte Analyse	188
(b) Debugger	189
(c) Automatisierte Prüfungstools und Big Data	190
(d) Integrierte Entwicklungsumgebungen	191
(2) Softwaretests – Organisation und Grundsätze	191
(a) Testgrundsätze	192
(b) Testorganisation	193
(c) Testorganisation in verschiedenen Entwicklungsmodellen	195
(3) Softwaretests – Arten und Auswahl	197
(a) Statische und dynamische Testverfahren	198
(b) White- und Black-Box-Tests	198
(c) Überblick verschiedener Testarten	199
(d) Auswahl der Tests	201
(4) Manuelle Softwareprüfungen	203
(a) Formen der manuellen Softwareprüfungen	204
(b) Vorteile der manuellen Softwareprüfungen	205
(c) Manuelles Testen als Ergänzung, nicht als Alternative	206
(5) Nachweis der Fehlerfreiheit – Softwareverifizierung	207
dd) Weitere mögliche Konstruktionspflichten	207
(1) Programmierung redundanter Software	208
(2) Updatability by Design	208
(3) Behebung festgestellter Schwachstellen im Quellcode	210
(a) Anpassung in laufender Produktion	210
(b) Zeitrahmen zur Behebung der Schwachstelle	210
(4) Vorgaben an Zulieferer	212
3. Zusammenfassung der einzelnen Konstruktionspflichten	213
a) Organisatorische Pflichten	213
b) Technische / Analytische Pflichten	214
aa) Verpflichtende Testverfahren	215
bb) Testtechniken	216
c) Weitere Konstruktionspflichten	217
d) BSIMM-Studie	217
4. Besonderheit: OEM-Version	218

IV. Die Produktbeobachtungspflichten der Softwareproduzenten	218
1. Verschärfung der Produktbeobachtungspflicht bei (bewusst) fehlerhafter Software	219
2. Beobachtung der eigenen Software	220
3. Beobachtung von Fremdsoftware	220
4. Integrierte Produktbeobachtung	222
a) Vorteile der integrierten Produktbeobachtung	222
b) Integrierte Produktbeobachtung – Keine rein zukünftige Pflicht	223
c) Anwendbarkeit neben passiver und aktiver Produktbeobachtung	224
5. Handlungspflichten bei Entdeckung einer Gefahr	224
a) Warnung vor Schwachstellen	225
aa) Nutzerspezifische Warnung	226
(1) Art der Verbreitung der Warnung	227
(2) Mitteilungsquote	227
(3) Verständlichkeit der Warnung	228
bb) Unzulänglichkeit einer Warnung	228
cc) Warnung als Gefahrerhöhung	229
dd) Mitteilungspflicht von Sicherheitsstörungen beim BSI	230
b) Keine Herausgabe des Quellcodes	231
c) Softwarestilllegung mittels „Kill Switch“	231
aa) Stilllegung effektiver als Update?	232
bb) Grenzen der Stilllegung	232
(1) Beschränkung auf internetbasierte Software	233
(2) Mögliche Eigentumsverletzung durch Stilllegung	233
(3) Zwangsupdate als gleich effektives Mittel	233
(4) Bedrohung des Nutzers allein	234
cc) Kombination aus Kill Switch und Update	234
d) Erweiterte Rückruf- und Updatepflichten	234
aa) Ausgestaltung des Rückrufs bei Software	236
bb) Verschiebung der Zumutbarkeitserwägung	236
(1) Geringe Kosten für Update / Patch	237
(2) Dekompilierungsverbot	239
(a) Keine Umgehung des Dekompilierungsverbotes durch Reverse-Engineering	240
(b) Angewiesenheit auf den Produzenten	241
cc) Keine generelle Rückruf-/Updatepflicht	241
(1) Einklang mit dem Effizienzprinzip	243

(2) Nachhaltige Behebung	244
dd) Ende des Software-Supports	244
ee) Kein subjektiver Anspruch auf Updates	245
V. Weitere Verkehrssicherungspflichten für Softwareproduzenten	245
1. Fabrikationspflichten	246
2. Instruktionspflichten	247
a) Allgemeine Instruktionspflicht	247
b) Erneute Instruktionspflicht nach einem Update	248
F. Notwendigkeit zur Schaffung eines IT-Produktsicherheitsrechts oder von IT-Sicherheitsstandards	249
I. Schaffung einer IT-Sicherheit-Grundverordnung	251
1. Ausgestaltung und Bestandteile einer IT-Sicherheit- Grundverordnung	252
a) Einführung als Schutzgesetz i. S. d. § 823 Abs. 2 BGB	252
b) Einführung einer Meldepflicht	253
c) Sanktionierung unsicherer IT-Produkte	253
d) Updatepflicht	254
e) Prüfstelle für IT-Produkte	255
2. Notwendigkeit einer neuen Gesetzgebung	255
II. Schaffung von technischen Standards	256
1. Vorteile gegenüber Recht de lege ferenda	258
2. Ausgestaltung und Inhalt technischer Standards	259
a) Normungsorganisationen	260
b) Abstufung der Pflichten	261
c) Security by Design und Security by Default	262
d) Kontinuierliche Weiterentwicklung	264
e) Updatepflicht und Länge des Software-Supports	265
f) Mehrstufige Zertifizierungen	266
g) (Re-)Zertifizierungspflichten	266
h) Schwachstellen veröffentlichen	267
3. Schaffung von Standards allein genügt nicht	269
III. Initiative der Wirtschaft – Charter of Trust	270
1. Gründe für die Erstellung der Charter of Trust	271
2. Kernziele der Charter of Trust	271
3. Weitere Ziele und Maßnahmen der Charter of Trust	271
4. Fazit bezüglich der Charter of Trust	272



G. Fazit	274
Literaturverzeichnis	285

