

Internetrecht und Digitale Gesellschaft

Band 16

**IT- und Rechtssicherheit
automatisierter und vernetzter
cyber-physischer Systeme**

**Event Data Recording und integrierte Produktbeobachtung
als Maßnahmen der IT-Risikominimierung am Beispiel
automatisierter und vernetzter Luft- und Straßenfahrzeuge**

Von

Alexander Schmid



Duncker & Humblot · Berlin

ALEXANDER SCHMID

IT- und Rechtssicherheit automatisierter und
vernetzter cyber-physischer Systeme

Internetrecht und Digitale Gesellschaft

Herausgegeben von
Dirk Heckmann

Band 16

IT- und Rechtssicherheit automatisierter und vernetzter cyber-physischer Systeme

Event Data Recording und integrierte Produktbeobachtung
als Maßnahmen der IT-Risikominimierung am Beispiel
automatisierter und vernetzter Luft- und Straßenfahrzeuge

Von

Alexander Schmid



Duncker & Humblot · Berlin

Die Juristische Fakultät der Universität Passau
hat diese Arbeit im Jahre 2018 als Dissertation angenommen.

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.

Alle Rechte vorbehalten
© 2019 Duncker & Humblot GmbH, Berlin
Satz: TextFormA(r)t, Daniela Weiland, Göttingen
Druck: CPI buchbücher.de gmbh, Birkach
Printed in Germany

ISSN 2363-5479
ISBN 978-3-428-15633-7 (Print)
ISBN 978-3-428-55633-5 (E-Book)
ISBN 978-3-428-85633-6 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

„1 –

A robot may not injure a human being, or, through inaction, allow a human being to come to harm.

2 –

A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

3 –

A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.“

Isaac Asimov, 1920–1992

I, Robot, vor Introduction

Vorwort

In Zeiten, in denen Algorithmen eigenständig Musik komponieren oder Bilder malen, in denen jeder Alltagsgegenstand vernetzt zu werden scheint und cyber-physische Systeme wie selbstfahrende Straßenfahrzeuge oder selbstfliegende Drohnen allmählich unsere Straßen und unseren Himmel bevölkern, steht es mehr denn je in der Verantwortung des Rechts, mit diesen Entwicklungen Schritt zu halten und den sich hieraus ergebenden Gefahren effektiv entgegenzuwirken.

Zwei mögliche Instrumente der Risikominimierung stellen in diesem Kontext das Event Data Recording und die Produktbeobachtung dar, für die sich im Anwendungsbereich automatisierter und vernetzter Systeme zukünftig völlig neuartige Möglichkeiten ergeben werden. Während die Produktbeobachtung dabei dem präventiven Gefahrenschutz dient, bezweckt das Event Data Recording die Aufrechterhaltung der Rechtssicherheit, sollte es dennoch zu einem Unfall kommen.

Ausgehend von der Erkenntnis, dass Technik und Recht untrennbar miteinander verzahnt sind, versucht diese Arbeit, neue technische Ansätze für das Event Data Recording und die Produktbeobachtung in der „smartifizierten“ Welt von morgen auszuloten und rechtlich einzuordnen. Dabei soll insbesondere das derzeit geltende Recht betrachtet, ergänzend aber auch Anforderungen an zukünftige Rechtsreformen aufgezeigt werden. Zur Veranschaulichung dienen hierfür in erster Linie automatisierte und vernetzte Straßen- und Luftfahrzeuge. Gleichwohl wird der Blick auch stets auf „das große Ganze“, also auf automatisierte und vernetzte Systeme im übergeordneten Kontext, geweitet.

Die Arbeit wurde im April 2018 fertiggestellt und von der Juristischen Fakultät der Universität Passau im August 2018 als Dissertation angenommen. Neuere Gesetzgebung und Literatur wurden im Wesentlichen bis Oktober 2018 berücksichtigt.

Mein besonderer Dank gilt meinem Doktorvater Herrn Professor Dr. Dirk Heckmann für seine kontinuierliche Förderung und Unterstützung während meiner Zeit an seinem Lehrstuhl als studentische Hilfskraft, wissenschaftlicher Mitarbeiter und Doktorand sowie für seine wertvollen Ratschläge und inspirierenden Anregungen.

Herrn Professor Dr. Michael Beurskens danke ich für die rekordverdächtig schnelle Erstellung des Zweitgutachtens sowie für die äußerst hilfreichen Anmerkungen und Hinweise.

Ebenso danke ich meinen ehemaligen Arbeitskollegen des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht sowie allen Studienkollegen und Freunden, die meine Studienzeit in Passau unvergesslich gemacht haben.

Allen voran danke ich von Herzen aber meiner Familie sowie meiner lieben Freundin Mina und ihrer Familie, die mich in der Verwirklichung meiner Ziele in jeglicher Hinsicht uneingeschränkt unterstützt haben und unterstützen. Ohne deren stete Motivation wäre diese Arbeit sicherlich nicht in dieser Form möglich gewesen.

München, Oktober 2018

Alexander Schmid

Inhaltsübersicht

1. Teil

Problemstellung und Gang der Untersuchung	25
--	----

2. Teil

Die Entwicklung und Klassifizierung der Automatisierung und Vernetzung von CPS	30
---	----

Kapitel 1

Entwicklung der Automatisierung und Vernetzung an den Beispielen Industrie, Straßenverkehr und unbemannter Luftverkehr	30
---	----

Kapitel 2

Klassifizierung der Automatisierung an den Beispielen Straßenverkehr und unbemannter Luftverkehr	45
---	----

3. Teil

Die Ambivalenz und Paradoxität der Automatisierung und Vernetzung von CPS	53
--	----

Kapitel 1

Technischer Fortschritt zwischen Techniqueuphorie und Technikfrustration	53
---	----

Kapitel 2

Ambivalenz der Automatisierung und Vernetzung am Beispiel des unbemannten Luftverkehrs	56
---	----

Kapitel 3

Automatisierung und Vernetzung als Verhinderer und Förderer von IT- und Rechtssicherheit: ein Paradoxon?	95
---	----

4. Teil

Rechtspflicht zum Event Data Recording und zur integrierten Produktbeobachtung bei CPS	105
---	-----

Kapitel 1

Event Data Recording als Rechtspflicht	105
---	-----

Kapitel 2

Integrierte Produktbeobachtung als Rechtspflicht	180
---	-----

Kapitel 3

Anforderungen an eine Gesetzesreform	244
---	-----

5. Teil

Zusammenfassung und Schlussbemerkung	250
---	-----

Kapitel 1

Zusammenfassung	250
------------------------	-----

Kapitel 2

Schlussbemerkung	257
-------------------------	-----

Begriffsbestimmungen	260
-----------------------------------	-----

Literaturverzeichnis	267
-----------------------------------	-----

Stichwortverzeichnis	289
-----------------------------------	-----

Inhaltsverzeichnis

1. Teil

Problemstellung und Gang der Untersuchung	25
--	----

2. Teil

Die Entwicklung und Klassifizierung der Automatisierung und Vernetzung von CPS	30
---	----

Kapitel 1

Entwicklung der Automatisierung und Vernetzung an den Beispielen Industrie, Straßenverkehr und unbemannter Luftverkehr	30
A. Exkurs: Vernetzung als Schlüssel- und Komplementärtechnologie; Schutz der M2M-Kommunikation nach dem Entwurf einer ePrivacyVO	30
B. Automatisierung und Vernetzung der Industrie	35
C. Automatisierung und Vernetzung des Straßenverkehrs	36
I. Automatisierung von Straßenfahrzeugen	37
II. Vernetzung und Integration in die Verkehrsinfrastruktur	39
D. Automatisierung und Vernetzung des unbemannten Luftverkehrs	42
I. Automatisierung von UAS	42
II. Vernetzung und Integration in den Luftraum	44

Kapitel 2

Klassifizierung der Automatisierung an den Beispielen Straßenverkehr und unbemannter Luftverkehr	45
A. Klassifizierung der Automatisierung des Straßenverkehrs	46
I. Assistenz	46
II. Teilautomatisierung	47
III. Hochautomatisierung	47
IV. Vollautomatisierung	48
V. Autonomie	48
VI. Souveränität	49
B. Entwicklung einer Klassifizierungslehre für den unbemannten Luftverkehr	50

3. Teil

Die Ambivalenz und Paradoxität der Automatisierung und Vernetzung von CPS	53
--	-----------

Kapitel 1

Technischer Fortschritt zwischen Techniqueuphorie und Technikfrustration	53
---	-----------

Kapitel 2

Ambivalenz der Automatisierung und Vernetzung am Beispiel des unbemannten Luftverkehrs	56
A. Chancen automatisierter und vernetzter UAS	57
I. Chancen im Transportwesen	58
1. Beispiel: DHL Paketkopter und UPS HorseFly	58
2. Beispiel: Amazon Prime Air	59
II. Chancen in der Industrie und Landwirtschaft	61
1. Einsatz im Rahmen der Industrie 4.0	61
a) Beispiel: Ball-Drohne von Fraunhofer IML	61
b) Beispiel: InventAIRy von Fraunhofer IML	62
2. Einsatz im Rahmen von Inspektion und Wartung	62
3. Einsatz in der Land- und Forstwirtschaft	63
a) Beispiel: Schutz und Rettung von Wildtieren	63
b) Beispiel: Überwachung der Ernte	64
c) Beispiel: Weitere Anwendungsszenarien in der Forstwirtschaft	65
III. Chancen im Polizei- und Sicherheitswesen	66
1. Vorteile von UAS-Pol gegenüber stationärer Videoüberwachung	67
2. UAS-Pol als Bestandteil eines Sicherheitsgesamtkonzepts	67
IV. Chancen durch Synergie- und Katalysatoreffekte	69
B. Gefahren automatisierter und vernetzter UAS	70
I. Mehrfache Unterscheidung notwendig	71
1. Unterscheidung: Gefahr und Risiko	71
2. Unterscheidung: Lufttransportsystem und Nutzlast	72
3. Unterscheidung: Inhärente und intendierte Gefahren	73
II. Gefahrenarten bei automatisierten und vernetzten UAS	74
1. Gefahr der Kollision und des Absturzes	74
a) Gefahr der Kollision	75
b) Gefahr des Absturzes	76
2. Gefahren für das Vertrauen in automatisierte Systeme	77

3. Gefahren für die Rechtssicherheit	78
a) Zahlreiche Haftungsadressaten und Anspruchsgrundlagen	78
b) Konsequenz: „Legal Causes of Trouble“	80
c) Exkurs: Einführung einer „ePerson“ zur Wiederherstellung der Rechtssicherheit?	82
4. Gefahren für Datenschutz- und Persönlichkeitsrechte	82
5. Gefahren für den Natur- und Lärmschutz	84
6. Technikethische Gefahren	84
III. Gefahrenquellen bei automatisierten und vernetzten UAS	86
1. Automatisierungsspezifische Gefahrenquellen	87
a) Technische Eigenheiten	87
b) Mehrfache Komplexität	88
aa) Komplexität automatisierter und vernetzter CPS	88
bb) Komplexität der Operationsumgebungen	88
cc) Konsequenz: „Unknown Causes of Trouble“	89
c) Abhängigkeit (von) der Technik	89
d) Nichtdeterminismus und Techniksoveränität	91
e) Menschliche Heuristiken	92
2. Vernetzungsspezifische Gefahrenquellen	93

Kapitel 3

Automatisierung und Vernetzung als Verhinderer und Förderer von IT- und Rechtssicherheit: ein Paradoxon?	95
A. Verhinderer von IT- und Rechtssicherheit: Legal Causes of Trouble und Unknown Causes of Trouble	95
B. Förderer von IT- und Rechtssicherheit: Event Data Recording und integrierte Produktbeobachtung	96
I. Event Data Recording als Gegenspieler zu Legal Causes of Trouble	97
1. Black Box als bisherige Form des Event Data Recordings	97
2. Neue Möglichkeiten aufgrund von Automatisierung und Vernetzung	98
a) Automatisiertes Event Data Recording	98
b) Vernetztes Event Data Recording	99
aa) Externe Speicherung bei dem Hersteller des Systems	100
bb) Externe Speicherung bei einer öffentlichen Stelle	100
cc) Externe Speicherung bei einem Dienstleister („Tracing-as-a-Service“)	101
3. Zwischenergebnis: Automatisiertes und vernetztes Event Data Recording ...	101
II. Integrierte Produktbeobachtung als Gegenspieler zu Unknown Causes of Trouble	102
C. Auflösung des Paradoxons: Automatisierung und Vernetzung als Problem und Problemlösung zugleich	104

4. Teil

Rechtspflicht zum Event Data Recording und zur integrierten Produktbeobachtung bei CPS 105

Kapitel I

Event Data Recording als Rechtspflicht 105

A. Spezialgesetzliche Rechtspflicht zum Event Data Recording	106
I. Verpflichtung zum Event Data Recording in der bemannten Luftfahrt	106
1. Flugdatenschreiber („Flight Data Recorder“/„FDR“)	107
2. Tonaufzeichnungsanlage für das Cockpit („Cockpit Voice Recorder“/„CVR“)	108
3. Flugwegverfolgungssystem (Aircraft Tracking System)	110
4. Zwischenergebnis: Event Data Recording in der bemannten Luftfahrt	111
II. Verpflichtung zum Event Data Recording im automatisierten Straßenverkehr ...	111
1. Aufzeichnungspflichten (§ 63a Abs. 1 StVG)	111
2. Datenübermittlung an und Datenverarbeitung durch Behörden (§ 63a Abs. 2 StVG)	114
3. Datenübermittlung an Dritte (§ 63a Abs. 3 StVG)	115
4. Datenlöschung und Datenaufbewahrung (§ 63a Abs. 4 StVG)	116
5. Anonymisierte Datenübermittlung zur Unfallforschung (§ 63a Abs. 5 StVG)	117
6. Verordnungsermächtigungen (§ 63b StVG)	118
7. Zwischenergebnis: Event Data Recording im automatisierten Straßenverkehr	118
III. Verpflichtung zum Einsatz von Fahrtsschreibern und Kontrollgeräten sowie der elektronischen Fahrtenregistrierung	118
IV. Ergebnis: Begrenzte spezialgesetzliche Rechtspflicht zum Event Data Recording	119
B. „Event Data Recording Basisschutz“ als ein „Verbot der Datenlöschung“	119
I. Datenbeschaffung und Datensicherung als Bestandteile des Event Data Recordings	119
1. Datenbeschaffung	120
2. Datensicherung	120
II. Erforderlichkeit einer Rechtspflicht zur Datenbeschaffung und zur Datensicherung	121
1. Regelungsbedürftigkeit der Datenbeschaffungsphase	122
2. Regelungsbedürftigkeit der Datensicherungsphase	123
3. Zwischenergebnis: Rechtspflicht nur für Datensicherungsphase erforderlich	124
III. Rechtspflicht zur Datensicherung als ein „Verbot der Datenlöschung“	124
1. Datenschutzrechtlicher und urheberrechtlicher Schutz vor unberechtigter Datenlöschung	125
a) Datenschutzrechtlicher Schutz vor unberechtigter Datenlöschung	125
aa) Rechtslage nach dem BDSG a.F.	126

bb) Rechtslage nach der DSGVO	126
(1) Personenbezogene Daten als Anwendungsvoraussetzung	127
(2) Datenschutzrechtlich Verantwortlicher als Adressat der Vorschrift	128
(a) Hersteller als alleiniger datenschutzrechtlich Verantwortlicher	129
(b) Gemeinsame Verantwortlichkeit (Joint Controllershship) des Herstellers und des Betreibers nach Art. 26 DSGVO	130
cc) Zwischenergebnis: Beschränkter datenschutzrechtlicher Schutz vor unberechtigter Datenlöschung	131
b) Urheberrechtlicher Schutz vor unberechtigter Datenlöschung	131
2. Strafrechtlicher Schutz vor unberechtigter Datenlöschung	132
a) Datenveränderung (§ 303a Abs. 1 StGB)	132
aa) Löschen, Unterdrücken, Unbrauchbarmachen, Verändern durch positives Tun	132
bb) Daten	133
cc) Fremdheit der Daten als notwendiges Korrektiv	134
(1) Zuordnung nach dem Eigentum am verkörpernden Datenträger	135
(2) Zuordnung nach bestehenden Datenschutzrechten oder Betriebs- bzw. Geschäftsgeheimnissen	136
(3) Zuordnung nach dem sog. „Skripturakt“	136
(a) Unmittelbarkeit der Datengenerierung als ausschließliches Zuordnungskriterium	137
(b) Exkurs: Abgrenzung nach der Wesentlichkeit des Beeinflussungsmoments bei automatischer Skriptur und Vielzahl an Beteiligten?	138
(4) Zuordnung nach der wirtschaftlichen Berechtigung	139
(5) Exkurs: Abgrenzung der Datenträger-, Daten- und Inhaltsebene	140
(a) Übersicht über die Ebenen	141
(aa) Datenträgerebene (physical layer oder strukturelle Information)	141
(bb) Datenebene (code layer oder syntaktische Information)	142
(cc) Inhaltsebene (content layer oder semantische Information)	143
(b) Grundsätze des Ebenenmodells	145
(aa) Grundsatz der getrennten Ebenenzuordnung	145
(bb) Grundsatz der kumulativen Verarbeitungsvoraussetzung	145
(cc) Grundsatz des Vorrangs gesetzlich angeordneter Datenverarbeitung	145
(6) Zwischenergebnis: Keine (ausschließliche) eigentümerähnliche Verfügungsbefugnis des Herstellers	146
dd) Mindestqualität der Daten	146
ee) Tatbestandsausschließendes Einverständnis	147

(1) Dispositionsbefugnis	147
(2) Innere Zustimmung	147
(3) Informiertheit	148
(4) Freiwilligkeit	148
(5) Zwischenergebnis: Tatbestandsausschließendes Einverständnis nur hinsichtlich nicht-beweiserheblicher Daten möglich	149
ff) Vorsatz	149
(1) Zeitpunkt der Tat	149
(2) Vorliegen von Vorsatz zum Zeitpunkt der Tat	150
(a) Absicht	150
(b) Direkter Vorsatz	151
(c) Bedingter Vorsatz	151
gg) Zwischenergebnis: Datenveränderung	152
b) Urkundenunterdrückung (§ 274 Abs. 1 Nr. 1, Nr. 2 StGB)	152
c) Zwischenergebnis: Strafrechtlicher Schutz vor unberechtigter Datenlöschung	152
3. Deliktischer Schutz vor unberechtigter Datenlöschung	152
a) Dateneigentum (§§ 823 Abs. 1, 903 Satz 1 BGB)	154
aa) Sinnliche Wahrnehmbarkeit von Daten	155
bb) Räumliche Abgrenzbarkeit von Daten	155
cc) Zwischenergebnis: Keine Existenz eines Dateneigentums	155
b) Dateneigentum in analoger Anwendung (§§ 823 Abs. 1, 903 Satz 1 BGB analog)	156
aa) Vereinbarkeit mit dem numerus clausus des Sachenrechts	156
bb) Planwidrige Regelungslücke und vergleichbare Interessenlage als Voraussetzungen der Analogie	156
(1) Planwidrige Regelungslücke	156
(2) Vergleichbare Interessenlage	157
cc) Zwischenergebnis: Kein Dateneigentum in analoger Anwendung	158
c) Recht am eigenen Datenbestand (§ 823 Abs. 1 BGB)	158
aa) Anerkennung eines Rechts am eigenen Datenbestand	158
(1) Zuordnungs- und Ausschlussfunktion	159
(2) Koexistenz des Rechts am eigenen Datenbestand und des Datenschutzrechts	159
(3) Regelungsbedürftigkeit	161
(4) Zwischenergebnis: Anerkennung eines Rechts am eigenen Datenbestand	162
bb) Verfügungsbefugnis	162
cc) Verletzungshandlung	163
dd) Rechtswidrigkeit	163

(1) Positive Feststellung nach der Lehre des Handlungsunrechts	163
(a) Verfassungsrechtlicher Schutz der Interessen des Betreibers .	164
(b) Verfassungsrechtlicher Schutz der Interessen des Herstellers	165
(c) Ergebnis der Interessenabwägung	166
(2) Rechtfertigende Einwilligung	167
ee) Verschulden	167
(1) Erkennbarkeit	167
(2) Vermeidbarkeit	168
(a) Eigenständige Erkennung von Störungen und Systemfehlern	168
(b) Eigenständige Erkennung von Unfallereignissen	168
(3) Zwischenergebnis: Fahrlässigkeit des Herstellers	169
ff) Zwischenergebnis: Recht am eigenen Datenbestand	169
d) § 303a Abs. 1 StGB als Schutzgesetz	169
e) Anspruch auf Unterlassen (§ 1004 Abs. 1 BGB analog i. V. m. § 823 Abs. 1 BGB)	170
f) Mittelbarer Schutz durch den verkörpernden Datenträger (§ 823 Abs. 1 BGB)	170
aa) Verkörpernder Datenträger als Eigentum	170
bb) Eingriff in das Eigentumsrecht durch Schreibzugriff	170
cc) Rechtswidrigkeit	172
dd) Verschulden	172
ee) Zwischenergebnis: Mittelbarer Schutz durch den verkörpernden Daten- träger	172
g) Zwischenergebnis: Deliktischer Schutz vor unberechtigter Löschung	172
4. Zwischenergebnis: Rechtspflicht zur Datensicherung als ein „Verbot der Da- tenlöschung“	173
IV. Rechtspflicht zur Herausgabe oder Vorlage der gespeicherten beweis- erheblichen Daten	173
1. Datenschutzrechtliche Ansprüche auf Auskunft und Datenübertragbarkeit . . .	173
2. Zivilrechtliche Herausgabeansprüche	174
a) Vertragliche Herausgabeansprüche	174
b) Außervertragliche Herausgabeansprüche	175
c) Zwischenergebnis: Zivilrechtliche Herausgabeansprüche	176
3. Prozessuale Vorlage- und Herausgabepflichten	176
a) Zivilprozessuale Vorlagepflichten	176
b) Strafprozessuale Herausgabepflichten	178
c) Zwischenergebnis: Prozessuale Vorlage- und Herausgabepflichten	179
4. Ergebnis: Rechtspflicht zur Herausgabe oder Vorlage der gespeicherten beweis- erheblichen Daten	179
V. Ergebnis: „Event Data Recording Basisschutz“ als ein „Verbot der Datenlöschung“	180

Kapitel 2

Integrierte Produktbeobachtung als Rechtspflicht	180
A. Mehrfache Unterscheidung notwendig	182
I. Unterscheidung: Funktionssicherheit und Informationssicherheit	182
II. Unterscheidung: Produktentwicklungs- und Produktbeobachtungspflichten	184
III. Unterscheidung: Produktbeobachtungspflichten und Gefahrabwendungspflichten	184
IV. Ergebnis: Mehrfache Unterscheidung notwendig	185
B. Herstellerseitige Produktbeobachtungspflichten	186
I. Passive und aktive Produktbeobachtungspflichten	186
1. Bisherige Erscheinungsformen	186
a) Passive Produktbeobachtungspflichten	186
b) Aktive Produktbeobachtungspflichten	187
2. Rechtsgrundlagen	189
a) Produktbeobachtung als Verkehrssicherungspflicht des Haftungsrechts	189
aa) Verkehrssicherungspflichten zur Begründung von deliktischen Haftungsansprüchen	189
bb) Produktbeobachtungspflichten als Fallgruppe der Verkehrssicherungspflichten	191
cc) Erstreckung auf Softwarefehler und auf Schutz der Informationssicherheit	192
(1) Produktbeobachtung von Softwarefehlern	192
(2) Schutz der Informationssicherheit als Ziel der Produktbeobachtung	193
(3) Zwischenergebnis: Erstreckung auf Softwarefehler und auf Schutz der Informationssicherheit	195
b) Produktbeobachtungspflichten aus dem ProdHaftG	195
aa) Exkurs: Cyber-physische Systeme als „Produkt“	195
(1) Hardwarekomponente	196
(2) Softwarekomponente	196
(3) Vernetzungskomponente	197
bb) Inverkehrgabe als ausschließlich relevanter Zeitpunkt	197
cc) Sonderfall: Produktserien	198
dd) Zwischenergebnis: Begrenzte Produktbeobachtungspflichten aus dem ProdHaftG	199
c) Produktbeobachtung als öffentlich-rechtliche Verpflichtung	199
aa) Produktbeobachtungspflichten aus dem ProdSG	200
bb) Produktbeobachtungspflichten aus der DSGVO	202
(1) Dauerhafte Sicherstellung von Informationssicherheit sowie regelmäßige Überprüfung, Bewertung und Evaluierung	202

(2) Datenschutzrechtlich Verantwortlicher als Adressat der Vorschrift	203
(3) Zwischenergebnis: Begrenzte Produktbeobachtungspflichten aus der DSGVO	203
cc) Produktbeobachtungspflichten aus dem IT-Sicherheitsrecht	204
3. Zwischenergebnis: Passive und aktive Produktbeobachtungspflichten	205
II. Integrierte Produktbeobachtung bei automatisierten und vernetzten CPS	205
1. Defizite der passiven und aktiven Produktbeobachtung	206
2. Kompensation der Defizite durch integrierte Produktbeobachtung	207
3. Integrierte Produktbeobachtung als Verkehrssicherungspflicht des Haftungsrechts	207
a) Vereinbarkeit mit dem Charakter der Verkehrssicherungspflichten (Geeignetheit)	208
b) Vereinbarkeit mit dem rechtlich gebotenen Erfüllungsaufwand der Verkehrssicherungspflichten (Erforderlichkeit und Zumutbarkeit)	209
aa) Erforderlichkeit	210
(1) Bestimmung der Gefährlichkeit	210
(a) Schadenshöhe und Eintrittswahrscheinlichkeit als Faktoren der Gefährlichkeit	210
(b) Risikomatrizen als Hilfsmittel zur Bewertung der Gefährlichkeit	211
(c) Nichtexistenz von Unfallstatistiken als Erschwernis der Risikobewertung	213
(d) Beispielhafte Risikobewertung bei automatisierten und vernetzten UAS	213
(aa) Beurteilung der Schadenshöhe bei einer Kollision oder einem Absturz	214
(bb) Beurteilung der Eintrittswahrscheinlichkeit einer Kollision oder eines Absturzes	215
(cc) Beispielhafte Durchführung der Bewertung mittels Risikomatrix	216
(2) Objektive Erkennbarkeit nach dem Stand der Wissenschaft und Technik	217
(3) Erwartungshorizont der gefährdeten Verkehrsteilnehmer	218
(a) Vision Zero als Sicherheitsvorgabe im Luft- und Straßenverkehr	218
(b) Berücksichtigung des Erwartungshorizonts von unbeteiligten Passanten	219
(c) Zwischenergebnis: Erwartungshorizont der gefährdeten Verkehrsteilnehmer	221
(4) Zwischenergebnis: Erforderlichkeit	221
bb) Zumutbarkeit	221

(1) Bestimmung der Gefährlichkeit	222
(2) Bestimmung des Sicherheitsaufwands	223
(a) Erforderlichkeit einer herstellerindividuellen Berücksichtigung von Ressourcen	223
(b) Beispielhafte und intuitive Bewertung des Sicherheitsaufwands bei automatisierten und vernetzten Luft- und Straßenfahrzeugen	223
(3) Zwischenergebnis: Zumutbarkeit	225
c) Zwischenergebnis: Integrierte Produktbeobachtung als Verkehrssicherungs- pflicht des Haftungsrechts	225
4. Verhältnis der integrierten Produktbeobachtung zur passiven und aktiven Pro- duktbeobachtung	225
5. Zwischenergebnis: Integrierte Produktbeobachtung bei automatisierten und vernetzten CPS	227
III. Ergebnis: Herstellerseitige Produktbeobachtungspflichten	227
C. Herstellerseitige Gefahrabwendungspflichten	227
I. Hinweis- und Warnpflichten	228
1. Rechtsgrundlagen	228
a) Hinweis- und Warnung als Verkehrssicherungspflicht des Haftungsrechts	228
b) Öffentlich-rechtliche Hinweis- und Warnpflichten aus dem ProdSG	229
c) Speziell: Datenschutzrechtliche Hinweis- und Warnpflichten aus der DSGVO	229
2. Formen bisheriger und vernetzter Hinweis- und Warnpflichten	230
3. Speziell: Pflicht zur Meldung sicherheitskritischer Ereignisse an Mitbewerber	231
a) Pflicht zur Meldung sicherheitskritischer Ereignisse an Mitbewerber aus dem ProdSG	231
b) Pflicht zur Meldung sicherheitskritischer Ereignisse an Mitbewerber als Verkehrssicherungspflicht	232
4. Zwischenergebnis: Hinweis- und Warnpflichten	232
II. Produktrückruf und weitere Pflichten	233
1. Öffentlich-rechtliche Rückrufpflichten aus dem ProdSG	233
2. Produktrückruf als Verkehrssicherungspflicht des Haftungsrechts	234
a) Vorgelagerte Pflichtverletzung als Voraussetzung	235
b) Geeignetheit	236
c) Erforderlichkeit	237
d) Zumutbarkeit	238
aa) Formen bisheriger und vernetzter Produktrückrufpflichten	238
bb) Speziell: Pflicht zur Bereitstellung von Sicherheitsupdates	240
cc) Speziell: Fernsperrung als Produktrückrufmaßnahme	242
3. Zwischenergebnis: Produktrückruf und weitere Pflichten	244
III. Ergebnis: Herstellerseitige Gefahrabwendungspflichten	244

Inhaltsverzeichnis	21
--------------------	----

Kapitel 3

Anforderungen an eine Gesetzesreform	244
A. Anforderungen an ein automatisiertes und vernetztes Event Data Recording	245
I. Geeigneter Regelungsort	245
II. Sicherstellung von Beweisverfügbarkeit	245
III. Sicherstellung von Beweiskräftigkeit	246
IV. Sicherstellung von Beweisverwertbarkeit	246
B. Anforderungen an eine automatisierte und vernetzte integrierte Produktbeobachtung	247
I. Zukünftige Pflicht zur Bereitstellung von Sicherheitsupdates	247
II. Zukünftige Pflicht zur Meldung sicherheitskritischer Ereignisse an Mitbewerber	248

5. Teil

Zusammenfassung und Schlussbemerkung	250
---	-----

Kapitel 1

Zusammenfassung	250
A. Die Entwicklung und Klassifizierung der Automatisierung und Vernetzung von CPS	250
B. Die Ambivalenz und Paradoxität der Automatisierung und Vernetzung von CPS	251
C. Rechtspflicht zum Event Data Recording und zur integrierten Produktbeobachtung bei CPS	253

Kapitel 2

Schlussbemerkung	257
Begriffsbestimmungen	260
Literaturverzeichnis	267
Stichwortverzeichnis	289

Abkürzungsverzeichnis

ABS	Antiblockiersystem
ACPS	Automatisiertes cyber-physisches System
AI	Artifizielle Intelligenz
ATS	Air Traffic Service
BASt	Bundesanstalt für Straßenwesen
BAuA	Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMW	Bayerische Motoren Werke (Kfz-Hersteller)
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVCP	Bundesverband Copterpiloten
C2C	Car-to-Car (Kommunikation)
C2I	Car-to-Infrastructure (Kommunikation)
CAT	Commercial Air Transport Operation
CD	Compact Disc
CEFIC	Conseil Européen de l'Industrie Chimique (Verband der Europäischen chemischen Industrie)
CPS	Cyber-physisches System
CVR	Cockpit Voice Recorder
DFS	Deutsche Flugsicherung GmbH
DJI	Dà-Jiāng Innovations (UAS-Hersteller)
DLR	Deutsches Zentrum für Luft- und Raumfahrt
DrohnenVO	Verordnung zur Regelung des Betriebs von unbemannten Fluggeräten
DVD	Digital Versatile Disc
EDR	Event Data Recorder
EDV	Elektronische Datenverarbeitung
EEPROM	Electrically Erasable Programmable Read-only Memory
ESP	Elektronisches Stabilitätsprogramm
EXE	Executable (Dateiformat)
FDR	Flight Data Recorder
FUEGO	Fire Urgency Estimator in Geosynchronous Orbit
GAU	Größter anzunehmender Unfall
GEN	General Requirements
GPS	Global Positioning System
GSG 9	Grenzschutzgruppe 9
GSM	Global System for Mobile Communications
HTML	Hypertext Markup Language
IBM	International Business Machines (EDV-Unternehmen)
ICAO	International Civil Aviation Organization
IDE	Instruments, Data, Equipment
IDS	Intrusion Detection System

ILS	Instrument Landing System
INDECT	Intelligent information system supporting observation, searching and detection for security of citizens in urban environment
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
KI	Künstliche Intelligenz
LTE	Long Term Evolution
M2I	Machine-to-Infrastructure (Kommunikation)
M2M	Machine-to-Machine (Kommunikation)
M2P	Machine-to-Pedestrian (Kommunikation)
M2V	Machine-to-Vehicle (Kommunikation)
MAC	Media Access Control
MCTOM	Maximum Certified Take-off Mass
MDP	Mobilitätsdienstplattform
MOPSC	Maximum Operational Passenger Seating Configuration
MPA	Motor Powered Aircraft
OBD	On-Board-Diagnose-System
PDF	Portable Document Format
PWC	PricewaterhouseCoopers International
RAM	Random-Access Memory
RFID	Radio-Frequency Identification
ROS	Robot Operating System
SAA	Sense-and-Avoid
SAE	Society of Automotive Engineers
SIM	Subscriber Identity Module
SLC	Single-Level-Cell
SORA	Specific Operations Risk Assessment
SSD	Solid State Drive
sUAS	Small Unmanned Aircraft System
UAS	Unmanned Aircraft System
UAS-Pol	Unmanned Aircraft System-Police
UAV	Unmanned Aerial Vehicles
UPS	United Parcel Service
USB	Universal Serial Bus
V2I	Vehicle-to-Infrastructure (Kommunikation)
V2N	Vehicle-to-Network (Kommunikation)
V2P	Vehicle-to-Pedestrians (Kommunikation)
V2V	Vehicle-to-Vehicle (Kommunikation)
VDA	Verband der deutschen Automobilindustrie
WHO	World Health Organization
WLAN	Wireless Local Area Network

Ansonsten werden die üblichen Abkürzungen gebraucht, vgl. *Kirchner*, Abkürzungsverzeichnis der Rechtssprache, 8. Aufl. 2015

1. Teil

Problemstellung und Gang der Untersuchung

„Suche nicht nach Fehlern, suche nach Lösungen.“

Henry Ford, 1863–1947

Gründer der Ford Motor Company

„Zum Greifen nah ist die Gemütlichkeit des griechischen Bürgers, die durch unsere mechanischen Diener ermöglicht wird, die seine zwölf bis fünfzehn pro freiem Mann bei Weitem übertreffen. Diese mechanischen Diener springen uns zu Hilfe. Beim Betreten eines Raumes erhellen uns auf Knopfdruck ein Dutzend Lichtquellen den Weg. Ein anderer Diener sitzt vierundzwanzig Stunden am Tag an unserem Thermostat und reguliert die Wärme in unserem Haus. Ein anderer sitzt Tag und Nacht an unserem automatischen Kühlschrank. Sie starten unser Auto, treiben unsere Motoren an, putzen unsere Schuhe und kultivieren unsere Haare.“¹
(Nash, Jay B.: Spectatoritis, New York 1932, S. 265)

Nash hat Recht behalten: Automatisierung und Vernetzung halten heute zunehmend Einzug in alle Lebensbereiche, von der *„Kaffeemaschine am Morgen und dem Funkwecker am Abend“*² („Smart Home“) über die intelligente Bekleidung („Smart Wearables“) und die vernetzte Verkehrsinfrastruktur („Smart Road Infrastructure“) bis hin zur vollständigen Automatisierung und Vernetzung der Industrie („Smart Factory“), unserer Stromversorgung („Smart Grids“) oder sogar ganzer Städte („Smart Cities“).³ Selbst die Art und Weise, wie wir zukünftig Verträge abschließen und durchführen („Smart Contracts“)⁴, wird von dieser allgegenwärtigen und alleserfassenden „Smartifizierung“⁵, die keinen Stein auf dem anderen zu lassen scheint, nicht verschont bleiben.

Angeführt wird diese disruptive digitale Transformation insbesondere durch automatisierte und vernetzte „cyber-physische Systeme“ („CPS“). Unter einem

¹ Frei übersetzt ins Deutsche von: „Within our grasp is the leisure of the Greek citizen, made possible by our mechanical slaves, which far outnumber his twelve to fifteen per free man. These mechanical slaves jump to our aid. As we step into a room, at the touch of a button a dozen light our way. Another slave sits twenty-four hours a day at our thermostat, regulating the heat of our home. Another sits night and day at our automatic refrigerator. They start our car; run our motors; shine our shoes, and cult our hair.“, Nash, Spectatoritis, S. 265.

² VK Baden-Württemberg, Beschl. v. 16.08.2017 – 1 VK 24/17, ZfBR 2018, 102.

³ Vgl. zu dieser umfassenden Smartifizierung bereits Heckmann/Schmid, vbw Studie Datenschutz, IT-Sicherheit und Haftung bei automatisierten Systemen, S. 12.

⁴ Vgl. hierzu Heckmann, vbw Studie Blockchain und Smart Contracts, S. 13 ff.

⁵ Hierzu bereits Heckmann/Schmid, vbw Studie Datenschutz, IT-Sicherheit und Haftung bei automatisierten Systemen, S. 12; Heckmann/Schmid, Informatik-Spektrum 2017, 430, 431.

cyber-physischen System ist dabei eine digitalisierte Maschine zu verstehen, also eine informationstechnische Einheit, die sowohl aus einer mechanischen Komponente als auch aus Software zusammengesetzt und somit fähig ist, in physischer Form auf ihre Umwelt einzuwirken und mit dieser in Interaktion zu treten.⁶ Neben der Automatisierung stellt dabei auch die Vernetzung eine wesentliche Eigenschaft cyber-physischer Systeme dar, die zusammen mit anderen IT-Systemen das sog. „Internet der Dinge“ („Internet of Things“/„IoT“) bilden.⁷ Aufgrund dieser Vernetzung kann das cyber-physische System mit anderen CPS, sonstigen IT-Systemen oder Menschen Informationen austauschen oder Befehle von diesen entgegennehmen. Neben den bereits aufgezählten Beispielen fallen unter den Begriff des CPS etwa Roboter aller Art, zudem aber bspw. auch Staudämme, Atom- oder Windkraftwerke, Herzschrittmacher oder vernetztes Spielzeug. Trotz dieser schier unendlichen Palette an denkbaren Arten und Formen cyber-physischer Systeme existiert derzeit aber wohl keine CPS-Gattung, über die in der Gesellschaft und Politik dermaßen leidenschaftlich diskutiert wird wie automatisierte und vernetzte Straßen- und Luftfahrzeuge.

Während Straßenfahrzeuge dabei gefühlt seit jeher tief mit unserem Alltag verzahnt sind und die Automatisierung des Straßenverkehrs (nach der Einführung etwa des ABS, des ESP, des Tempomaten, des Abstandswarners und des Parklenkassistenten) den denklogisch nächsten Schritt darstellt, sind es vielmehr unbemannte Luftfahrzeuge („Unmanned Aircraft Systems“/„UAS“), die als technische Newcomer in den letzten Jahren ganze Industrie- und Technikzweige beflügelt haben. Egal ob im Transportwesen, in der Industrie, im Rahmen von Inspektion und Wartung, in der Land- und Forstwirtschaft oder im Polizei- und Sicherheitswesen – für zahlreiche Einsatzgebiete werden UAS derzeit entwickelt und getestet oder befinden sich bereits im Praxiseinsatz. Laut einer Studie von PricewaterhouseCoopers International („pwc“) stellen UAS, neben dem Internet der Dinge, der Augmented und Virtual Reality, der Blockchain-Technologie, der artifiziellen Intelligenz, dem 3D-Druck und der Robotertechnik im Allgemeinen, gar eine der acht „*[t]ech breakthroughs megatrends*“ der kommenden Jahre dar,⁸ die „*Geschäftsmodelle und Geschäfte rund um den Globus umwälzen*“ werden, worauf „*Unternehmen aller Größen und Branchen [...] vorbereitet sein [sollten]*“.⁹ Hält man sich vor Augen, dass bei automatisierten und vernetzten UAS sogar mehrere dieser Technologien gebündelt werden, wird die besondere Bedeutung und Brisanz dieser Technologie nochmals unterstrichen.

Neben den zahlreichen Chancen und Potentialen können sich als Schattenseite der Automatisierung und Vernetzung hieraus jedoch auch gesteigerte oder neuartige

⁶ Vgl. Bendel, 300 Keywords Informationsethik, S. 208.

⁷ Vgl. Bendel, 300 Keywords Informationsethik, S. 208.

⁸ Eckert/Curran/Bhardwaj: pwc-Studie, Tech breakthroughs megatrend: how to prepare for its impact, S. 5.

⁹ Sieger, pwc-Beitrag, Die gewaltigen Acht.

Risiken ergeben, da die Automatisierung stets mit Verselbstständigung und Kontrollverlust und die Vernetzung mit einer Öffnung des Systems für unberechtigte Dritte einhergeht. Insbesondere die letztgenannte Gefahr des Internets der Dinge wurde in den vergangenen Jahren bereits im Rahmen zahlreicher Sicherheitsvorfälle bei vernetzten Industrieanlagen (bspw. „Stuxnet“¹⁰), staatlichen Einrichtungen (bspw. „WannaCry“¹¹) oder privaten „Smart Devices“ (bspw. „My Friend Cayla“¹²) anschaulich verdeutlicht.¹³ Besondere Brisanz haben vor diesem Hintergrund aber erneut cyber-physische Systeme, die aufgrund ihrer mechanischen Komponente nicht nur eine Gefahr für die Informationssicherheit, sondern auch für die Funktionssicherheit darstellen können. Der sog. „Jeep Cherokee Hack“ aus dem Jahr 2014, bei dem auch sicherheitskritische Fahrfunktionen von Angreifern aus der Ferne übernommen werden konnten,¹⁴ stellt nur eines von vielen Beispielen hierfür dar.

Dabei ist zunächst zu befürchten, dass die Komplexität und der mehrschichtige Aufbau von automatisierten und vernetzten CPS (einerseits aufgrund des multilateralen Zusammenwirkens unterschiedlicher Hersteller von Teilkomponenten bei der Entwicklung, andererseits aufgrund der Einbettung von CPS in das Internet der Dinge) sowie die Komplexität der Operationsumgebungen, in denen CPS betrieben werden sollen, eine abgeschlossene und sichere Produktentwicklung in der Herstellersphäre, also sozusagen „am Reißbrett“¹⁵, immer weniger zulässt. Als Konsequenz könnte sich hieraus ergeben, dass automatisierte und vernetzte CPS künftig auch nach der Markteinführung und Inverkehrgabe noch unter zahlreichen, bislang unbekannten Produktfehlern leiden (im Rahmen dieser Arbeit daher als „Unknown Causes of Trouble“ bezeichnet), die nicht unter Laborbedingungen simulierbar sind, sondern erst im späteren Praxiseinsatz, also beim Kunden, zu Tage treten.¹⁶ Auch das Europäische Parlament betont aus diesem Grund mittlerweile, „dass die Prüfung von Robotern in lebensnahen Szenarien für die Ermittlung und Bewertung der Risiken, die mit ihnen verbunden sein können sowie für ihre technologische Entwicklung, die über eine reine Versuchsphase im Labor hinausgeht, von entscheidender Bedeutung ist“¹⁷.

¹⁰ Rieger, FAZ-Beitrag v. 22.09.2010, Der digitale Ersts Schlag ist erfolgt.

¹¹ Spiegel Online-Beitrag v. 13.05.2017, „WannaCry“-Angriff – Fakten zum globalen Cyberangriff.

¹² Kühl, Zeit Online-Beitrag v. 17.02.2017, Vernichten Sie diese Puppe.

¹³ Vgl. hierzu auch Helmbrecht, Redebeitrag Security and Liability in the Internet of Things, S. 2 ff.

¹⁴ Siehe 3. Teil, Kapitel 2, B., III., 2.

¹⁵ Heckmann/Schmid, Informatik-Spektrum 2017, 430, 432 f.; Schmid/Wessels, NZV 2017, 357, 359.

¹⁶ Vgl. hierzu bereits Heckmann/Schmid, Informatik-Spektrum 2017, 430, 433; Schmid/Wessels, NZV 2017, 357, 359; Jänich/Schrader/Reck, NZV 2015, 313, 318; Förster, in: Bamberger/Roth/Hau/Poseck, BeckOK BGB, § 823 BGB Rn. 734.

¹⁷ 2015/2103(INL), S. 9.