

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 Technikeuphorie 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 Techniksouveränität	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 1

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 Fahrtschreibern 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 Datenträger	172
g) Zwischenergebnis: Deliktischer Schutz vor unberechtigter Löschung	172
4. Zwischenergebnis: Rechtspflicht zur Datensicherung als ein „Verbot der Datenlöschung“	173
IV. Rechtspflicht zur Herausgabe oder Vorlage der gespeicherten beweisereheblichen 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 beweisereheblichen 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 Erschweris 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

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