

# Inhaltsübersicht

Inhaltsverzeichnis	13
Einleitung	51
Abschnitt 1: Problemstellung	51
Abschnitt 2: Ziel der Arbeit	56
Abschnitt 3: Vorgehensweise	57
Teil 1: Smarte Systeme im Internet der Dinge	59
Abschnitt 1: Begriffserläuterungen und technische Grundlagen	59
Abschnitt 2: Einsatzbereiche smarter Systeme und Beteiligte	78
Abschnitt 3: Smart Home als Anwendungsbeispiel für privat genutzte Systeme	81
Abschnitt 4: Das automatisierte bzw. autonome Fahren als Anwendungsbeispiel	87
Abschnitt 5: Chancen und Risiken smarter Systeme des Internets der Dinge	91
Zusammenfassung zu Teil 1 und Fazit	102
Teil 2: Tauglichkeit und Anpassungsbedürftigkeit des Produktstrafrechts zum Schutz privater Nutzer smarter Systeme vor Bedrohungen von „innen“ durch Produktgefahren	105
Abschnitt 1: Gegenstand und Gang der Untersuchung des Produktstrafrechts	105

Abschnitt 2: Überblick über begriffliche, historische sowie funktionelle Grundlagen des Produktstrafrechts	107
Abschnitt 3: Strafrechtliche Produktverantwortung für durch Fehler smarter Produkte hervorgerufene Verletzungen	123
Abschnitt 4: Strafrechtlicher Schutz der Rechtsgüter des Nutzers durch das Produktstrafrecht bei vorab einprogrammierten Dilemma-Entscheidungen autonomer Systeme	307
Abschnitt 5: Strafbarkeit eines künstlich intelligenten Systems selbst?	329
Ergebnisse und Zusammenfassung zu Teil 2	346
Teil 3: Tauglichkeit und Anpassungsbedürftigkeit des Computer- und des Datenschutzstrafrechts zum Schutz privater Nutzer smarter Systeme vor Bedrohungen durch Angriffe von „außen“	351
Abschnitt 1: Hintergrund der Bedrohungslage für private Nutzer und Ablauf der Untersuchung des Computer- und des Datenschutzstrafrechts	351
Abschnitt 2: Historische, grund- und menschenrechtliche sowie funktionelle Grundlagen des Computer- und des Datenschutzstrafrechts	356
Abschnitt 3: Anwendbarkeit der untersuchten Tatbestände bei Angriffen auf privat genutzte smarte Systeme bzw. ihre Daten – Strafanwendungsrecht	408
Abschnitt 4: Strafrechtliche Verantwortlichkeit nach Computerstrafrecht beim Angriff auf ein smartes System bzw. dessen Daten – Untersuchung der §§ 202a – 202c StGB und §§ 303a, 303b StGB	437
Abschnitt 5: Strafbarkeit nach Datenschutzstrafrecht durch Anschlussdaten nach dem Eindringen in ein privat genutztes smartes System – Untersuchung der §§ 201, 201a, 202d StGB sowie § 42 BDSG und § 33 KUG	610
Ergebnisse und Zusammenfassung zu Teil 3	702

Teil 4: Berührungspunkte und Wechselwirkungen von Produkt-, Computer- und Datenschutzstrafrecht beim Schutz privater Nutzer	709
Abschnitt 1: Hackingangriff auf ein smartes Produkt durch Ausnutzung von IT-Sicherheitslücken	709
Abschnitt 2: Cyberangriff auf den Hersteller mit Auswirkungen auf private Nutzer	724
Abschnitt 3: „Innenangriff“ auf smarte Systeme durch Mitarbeiter des Herstellers	730
Abschnitt 4: Präventive Wirkung der Produktverantwortlichkeit hin zur Vermeidung von Computer- und Datenkriminalität	737
Ergebnisse und Zusammenfassung zu Teil 4	739
Schlussbetrachtung	743
Abschnitt 1: Zusammenfassung	743
Abschnitt 2: Abschließendes Fazit	763
Literaturverzeichnis	767
Anhang	809

# Inhaltsverzeichnis

Abkürzungsverzeichnis	41
Einleitung	51
Abschnitt 1: Problemstellung	51
A. Hohe Präsenz smarter Systeme in der privaten Alltagswelt aktuell und in der Zukunft	51
B. Rechtliche Herausforderungen im Zusammenhang mit smarten Systemen	53
Abschnitt 2: Ziel der Arbeit	56
Abschnitt 3: Vorgehensweise	57
Teil 1: Smarte Systeme im Internet der Dinge	59
Abschnitt 1: Begriffserläuterungen und technische Grundlagen	59
A. Der Begriff „Internet der Dinge“ und verwandte Bezeichnungen	59
B. Smarte Systeme	62
I. Begriffserläuterung von „System“	63
II. Begriffserläuterung von „smart“	65
III. Zentrale Eigenschaften smarter Systeme	66
1. Vernetzung	66
2. Künstliche Intelligenz und Lernfähigkeit	69
3. Autonomie und Automatisierung	72
C. Weitere technische Grundlagen, Trends und Treiber im Hinblick auf smarte Systeme im Internet der Dinge	74
I. Lokalisierungstechnologien	75
II. Sensorik und Aktorik	75
III. Mensch-Computer-Schnittstellen	76
IV. Miniaturisierung	77
Abschnitt 2: Einsatzbereiche smarter Systeme und Beteiligte	78
A. Kurzer Überblick über verschiedene Segmente smarter Systeme	78
B. Beteiligte Akteure im Internet der Dinge	80
Abschnitt 3: Smart Home als Anwendungsbeispiel für privat genutzte Systeme	81
A. Definition des Begriffs „Smart Home“	81

B. Vorstellung einzelner Teilbereiche und Beispiele smarter Systeme im Smart Home	82
C. Zusammenspiel und Vernetzung von smarten Systemen im Smart Home	85
Abschnitt 4: Das automatisierte bzw. autonome Fahren als Anwendungsbeispiel	87
A. Begriffserläuterungen	87
B. Verschiedene Autonomie- bzw. Automatisierungsstufen	87
C. Umwelterfassung und Vernetzung	89
D. Aktuelle rechtliche Zulässigkeit und Verbreitung des automatisierten bzw. autonomen Fahrens	90
Abschnitt 5: Chancen und Risiken smarter Systeme des Internets der Dinge	91
A. Chancen und Nutzen smarter Systeme des Internets der Dinge	92
B. Gefahren für Rechtsgüter und Interessen der Nutzer smarter Systeme	95
I. Bedrohung „von innen“ durch produktimmanente Fehler	95
II. Bedrohung „von außen“ durch Spionage- und Hackingangriffe auf das smarte System oder einzelne Komponenten	96
III. Weitere Nachteile für die Interessen der Nutzer	101
Zusammenfassung zu Teil 1 und Fazit	102
Teil 2: Tauglichkeit und Anpassungsbedürftigkeit des Produktstrafrechts zum Schutz privater Nutzer smarter Systeme vor Bedrohungen von „innen“ durch Produktgefahren	105
Abschnitt 1: Gegenstand und Gang der Untersuchung des Produktstrafrechts	105
Abschnitt 2: Überblick über begriffliche, historische sowie funktionelle Grundlagen des Produktstrafrechts	107
A. Begriffliche Festlegungen	107
B. Entstehungshintergrund des Produktstrafrechts	110
I. Ausgangspunkt: Zivilrechtliche Produkthaftung	110
1. Haftung des Herstellers nach § 823 Abs. 1 BGB	111
a) Wesentliche Voraussetzungen	111
b) Beweislastverteilung	112

2. Haftung des Herstellers nach dem ProdHaftG	114
II. Anfänge und bedeutsame Fälle bei der Entwicklung des Produktstrafrechts	115
C. Funktionen des Produktstrafrechts und Unterschiede zum Zivilrecht	118
I. Unrechtssanktionierung und Rechtsgüterschutz durch das Produktstrafrecht	118
II. Funktionelle und strukturelle Abgrenzung zum Zivilrecht	120
Abschnitt 3: Strafrechtliche Produktverantwortung für durch Fehler smarter Produkte hervorgerufene Verletzungen	123
A. Täterkreis, typische Tatbestände und Begehungsformen	123
I. Kreis möglicher strafrechtlich Verantwortlicher	123
1. Allgemeines zum Täterkreis im Produktstrafrecht	123
2. Kreis der Verantwortlichen und Besonderheiten bei Fehlern smarter Produkte	127
3. Zwischenergebnis	129
II. Wesentliche Tatbestände des Produktstrafrechts	130
III. Tun und Unterlassen des Herstellers smarter Produkte	131
1. In Betracht kommende Verhaltensweisen des Herstellers	131
2. Abgrenzung von Tun und Unterlassen	132
IV. Garantenstellung des Herstellers smarter Produkte	133
1. Dogmatische Uneinigkeit bei der Begründung der Garantenstellung des Herstellers im Produktstrafrecht allgemein	134
a) Begründung der Garantenstellung aus Ingerenz durch den BGH	134
b) Kritik und Begründungsversuche der Garantenstellung im Schrifttum	135
c) Fazit und Bewertung	138
2. Anwendung dieser Dogmatik zur Garantenstellung auf Hersteller smarter Produkte	139
3. Zwischenergebnis	140
V. Vorsätzliche oder fahrlässige Begehungsweise?	141
1. Wenig Praxisrelevanz von Vorsatzdelikten (auch) bei der Herstellerhaftung für smarte Produkte	141
2. Große praktische Bedeutung von Fahrlässigkeitsdelikten	143

3. Zwischenergebnis	144
VI. Zusammenfassung und Ergebnis	145
B. Untersuchung der Kausalität	145
I. Zunahme von Fällen der Multikausalität im Zusammenhang mit smarten Produkten	146
II. Generelle Kausalität: Nachweis der Schadensursächlichkeit smarter Produkte	148
1. Notwendigkeit eines exakten naturwissenschaftlichen Ursachennachweises?	148
a) „Ausschlussverfahren“ des BGH	148
b) Kritik aus der Literatur und Bewertung	149
c) Anwendbarkeit und Beurteilung in Bezug auf smarte Produkte im Internet der Dinge	150
2. Zwischenergebnis	153
III. Ursachenzusammenhang zwischen unterlassenem Rückruf und Verletzung	153
1. Problemaufriss	153
2. Lösungen in Literatur und Rechtsprechung	154
3. Eigene Bewertung	156
4. Zwischenergebnis	159
IV. Ursächlichkeit einer unterlassenen Instruktion oder Warnung	159
1. Problemaufriss	160
2. Auffassungen in Literatur und Rechtsprechung – ähnliches Bild wie beim unterlassenen Rückruf	160
3. Eigene Bewertung unter Einbeziehung der Parallelproblematik beim Rückruf	161
4. Zwischenergebnis	163
V. Einführung von abstrakten Gefährdungsdelikten im Produktstrafrecht als Lösungsalternative für die bislang aufgezeigten Kausalitätsprobleme?	164
1. Etablierung eines allgemeinen abstrakten Gefährdungsdelikts im Produktstrafrecht	164
a) Im Hinblick auf das Herstellen und Inverkehrbringen	164
b) Bezüglich des Unterlassens gefahrabwendender Maßnahmen	165
c) Bewertung und Kritik	165

2. Abstraktes Gefährdungsdelikt spezifisch für das Inverkehrbringen künstlich intelligenter Produkte?	168
a) Bisherige Überlegungen zur Ausgestaltung eines KI-spezifischen Gefährdungsdelikts	168
b) Kritische Würdigung	169
3. Zwischenergebnis	172
VI. Kollegialentscheidungen	173
1. Pflichtgemäßes Handeln des Abstimmenden oder Rückruf trotz pflichtwidrigen Votums	173
2. Pflichtwidriges Votum ausschlaggebend für die Entscheidung gegen den Rückruf	174
3. Pflichtwidriges Votum nicht ausschlaggebend für die Entscheidung gegen den Rückruf	174
a) Lösungsansatz des BGH	175
b) Reaktionen und Ansätze in der Literatur	176
c) Stellungnahme	177
4. Zwischenergebnis und Fazit	179
VII. Ergebnis und Zusammenfassung	179
C. Untersuchung der objektiven Fahrlässigkeit im Besonderen	181
I. Bestimmung der objektiven Sorgfaltsanforderungen an Hersteller smarter Produkte	182
1. Allgemeine Kriterien und Faktoren zur Begründung und Bestimmung der strafrechtlichen Sorgfaltsanforderungen	183
a) Gesetzliche und nichtgesetzliche Sonderregelungen und Standards	183
aa) Das Produktsicherheitsgesetz und darauf gestützte Rechtsverordnungen	185
(1) Allgemeine Inhalte und Vorgaben	185
(2) Anwendbarkeit des ProdSG auch auf smarte Produkte?	186
bb) EU-Rechtsakte zur Produktsicherheit und technische Normen	187
cc) Neue gesetzliche Regelungen zum automatisierten Fahren	191
dd) Medizinprodukteverordnung – VO (EU) 2017/745	193



ee) Normierungsbestrebungen in Bezug auf künstliche Intelligenz	195
(1) Entwicklung von technischen Normen für künstliche Intelligenz	195
(2) Europäische Vorhaben – insbesondere Entwurf einer Verordnung zur Regulierung und Nutzung von künstlicher Intelligenz	196
ff) Zusammenfassung und Bewertung	197
b) Aktueller Stand der Wissenschaft und Technik	200
c) Der Maßstab eines besonnenen, gewissenhaften Verkehrsteilnehmers	201
d) Sonderwissen und besondere Fähigkeiten	202
e) Interessenabwägung	204
f) Grad der vom Hersteller smarter Produkte einzuhaltenden Sorgfalt	205
aa) Allgemeine Kriterien	205
bb) Spezifische Anwendung auf den Bereich smarter Produkte	206
(1) Verletzungspotential eines smarten Produkts als Ausgangspunkt	206
(2) Denkbare Faktoren zur Bestimmung des Verletzungspotentials smarter Produkte im Internet der Dinge	206
(3) Ableitbare Tendenzen für den Grad der objektiven Sorgfaltsanforderungen	211
(4) Anwendungsbeispiele vor allem im Smart Home- und Automobilbereich	212
cc) Zwischenfazit	214
g) Zusammenfassung und Fazit	215
2. Konflikt der objektiven Fahrlässigkeit mit Art. 103 Abs. 2 GG?	217
3. Weitere Konkretisierung der strafrechtlichen Sorgfaltsanforderungen an Hersteller smarter Produkte durch die Übertragung zivilrechtlicher Verkehrspflichten ins Strafrecht?	220
a) Planungs- bzw. Konstruktionspflichten bei der Herstellung smarter Produkte	221

b) Fabrikationspflichten bei der Herstellung smarter Produkte	223
c) Instruktionspflichten bei smarten Produkten	224
d) Bedeutungszuwachs von Produktbeobachtungspflichten bei smarten Produkten	225
aa) Pflicht zur aktiven Informationsbeschaffung	227
bb) Sicherungsmaßnahmen nach Auffinden eines Fehlers bei smarten Produkten	228
cc) Zwischenergebnis	232
4. Problem des Umfangs und der Reichweite der Übertragbarkeit zivilrechtlicher Sorgfaltspflichten ins Strafrecht	232
a) Ultima-ratio-Funktion des Strafrechts als Ausgangspunkt	233
b) Meinungsstand zur Anwendung zivilrechtlicher Sorgfaltspflichten im Strafrecht	234
aa) Ganzheitliche Übertragung nach der Einheitlichkeits- und Präjudizienthese	234
bb) Einwände gegen die Einheitlichkeits- und Präjudizienthese	235
cc) Teilweise weitgehende Orientierung an den zivilrechtlichen Sorgfaltspflichten in der Praxis	236
dd) Eigene Würdigung und Zwischenfazit	237
c) Blick auf die den Sorgfaltsmaßstäben allgemein zugrundeliegenden teleologischen Interessenabwägungen im Zivil- und Strafrecht	240
d) Folgerung: Plädoyer für eine differenzierte Übertragung zivilrechtlicher Maßstäbe in Abhängigkeit vom Verletzungspotential	242
e) Fazit	244
5. Zwischenergebnis	245
6. Einschränkung der Sorgfaltsanforderungen an Hersteller smarter Produkte	246
a) Anwendung des Gedankens des Vertrauensgrundsatzes	247
aa) Allgemeines zum Vertrauensgrundsatz	247

bb) Beschränkung der Sorgfaltsanforderungen speziell im Verhältnis zum (privaten) Nutzer smarter Produkte	249
cc) Exkurs: Beschränkung der Sorgfaltsanforderungen gegenüber Dritten	250
dd) Zwischenergebnis	251
b) Unzumutbarkeit pflichtgemäßen Verhaltens	251
c) Implementierung einer Wesentlichkeitsschwelle zur Abschwächung der Sorgfaltspflichten?	253
d) Alleinige Berücksichtigung von gesetzlich festgeschriebenen Sorgfaltspflichten im Strafrecht?	254
e) Anhebung des für die strafrechtliche Haftung erforderlichen Fahrlässigkeitsgrades?	256
f) Begrenzung mithilfe der Rechtsfigur des erlaubten Risikos	257
aa) Allgemeines und rechtsdogmatische Einordnung des erlaubten Risikos	257
bb) Differenzierung zwischen erlaubtem und unerlaubtem Risiko	261
(1) Gesetzliche Vorgaben, Standards und behördliche Zulassungen	261
(2) Unterscheidung hinsichtlich risikosenkender und -steigernder Innovationen	262
cc) Bisherige Handhabung der Einschränkung im Bereich des automatisierten bzw. autonomen Fahrens	263
(1) Hintergrund des Einsatzes der Rechtsfigur des erlaubten Risikos im Bereich des automatisierten bzw. autonomen Fahrens	264
(2) Differenzierung zwischen erlaubtem und unerlaubtem Risiko beim automatisierten bzw. autonomen Fahren	265
(3) Zwischenfazit	267
dd) Anwendbarkeit dieser Grundsätze auf andere Bereiche smarter Produkte im Internet der Dinge	268
ee) Zwischenergebnis	271

g) Fazit	272
II. Objektive Vorhersehbarkeit des Erfolgs bei smarten Produkten	273
1. Allgemeines zur objektiven Vorhersehbarkeit	273
2. Objektive Vorhersehbarkeit des Erfolgs beim Einsatz smarter, insbesondere autonomer und selbstlernender Systeme	274
a) Problemaufriss	274
b) Anforderungen an das Merkmal der objektiven Vorhersehbarkeit bei lernfähigen und autonom agierenden Produkten	276
c) Eigene Bewertung	278
d) Zwischenergebnis	280
III. Zusammenfassung und Ergebnis	281
D. Weitere Einschränkungsmöglichkeiten der (Fahrlässigkeits-)Strafbarkeit von Herstellern smarter Produkte	287
I. Haftungsbegrenzung auf Ebene der objektiven Zurechnung	287
1. Ausschluss der Zurechnung zum Hersteller aufgrund der Fallgruppe des rechtmäßigen Alternativverhaltens	288
a) Vermeidbarkeitstheorie der h.M.	288
b) Risikoerhöhungslehre	289
c) Stellungnahme	289
2. Ausschluss der Zurechnung aufgrund atypischen Kausalverlaufs	291
3. Ausschluss der objektiven Zurechnung aufgrund mangelnder Beherrschbarkeit des Kausalverlaufs bei (voll-)autonomen und selbstlernenden Systemen?	292
4. Ausschluss der objektiven Zurechnung aufgrund von Risikoverringerung?	294
5. Einschränkung durch das Verantwortungsprinzip – Eigenverantwortliche Selbstgefährdung des Nutzers	295
a) Freiverantwortlichkeit des Nutzers smarter Produkte	296
b) Selbstschädigendes Verhalten des Nutzers smarter Produkte	298
aa) Tatherrschaft – Abgrenzung zur einverständlichen Fremdgefährdung	298

bb) Arten und „Qualität“ des selbstschädigenden Verhaltens	300
c) Bewertung im Hinblick auf private Nutzer smarter Produkte	303
6. Fazit	304
II. Subjektive Sorgfaltspflichtverletzung sowie subjektive Vorhersehbarkeit und Vermeidbarkeit des Erfolges	304
III. Strafrechtliche Verantwortlichkeit nur für explizit geregelte Vorsatz- und Fahrlässigkeitstatbestände?	305
IV. Zusammenfassung und Ergebnis	306
Abschnitt 4: Strafrechtlicher Schutz der Rechtsgüter des Nutzers durch das Produktstrafrecht bei vorab einprogrammierten Dilemma-Entscheidungen autonomer Systeme	307
A. Verantwortlichkeit des Herstellers in Dilemma-Situationen am Beispiel des autonomen Fahrens	308
I. Konkretes Beispiel einer Dilemma-Situation	308
II. Rechtliche Überlegungen zur Strafbarkeit des Herstellers	309
1. Denkbare Tatbestände und Begehungsformen	309
a) Tun oder Unterlassen sowie Kausalität	310
b) Einschlägigkeit von Vorsatz- oder Fahrlässigkeitsdelikten?	310
c) Zwischenergebnis	312
2. Objektive Sorgfaltspflichtverletzung	312
a) Dilemma-Entscheidungen als erlaubte Risikoschaffung?	313
aa) Gesetzliche Zulassungsvorschriften in Bezug auf Dilemma-Entscheidungen	313
bb) Aspekte einer Interessensabwägung und eines ethischen Diskurses sowie Ausblick	314
b) Zwischenergebnis	317
3. Objektive Vorhersehbarkeit	318
4. Objektive Zurechnung	318
5. Rechtfertigung	319
a) Rechtfertigender Notstand, § 34 S. 1 2. Alt. StGB	319

b) Anwendung der rechtfertigenden Pflichtenkollision?	321
aa) Allgemeines und klassischer Anwendungsbereich der rechtfertigenden Pflichtenkollision	321
bb) Übertragbarkeit auf Dilemma-Situationen im Zusammenhang mit autonomen Systemen?	322
c) Zwischenergebnis	323
6. Entschuldigungsgründe	324
a) Entschuldigender Notstand, § 35 StGB	324
b) Übergesetzlicher entschuldigender Notstand	324
aa) Allgemeines und Anwendungsbereich	325
bb) Anwendung auf Dilemma-Fälle beim Einsatz autonomer bzw. hochautomatisierter Fahrzeuge	326
c) Zwischenergebnis	326
B. Übertragbarkeit und Relevanz für andere Segmente smarter Produkte?	327
C. Bewertung und Zusammenfassung	327
Abschnitt 5: Strafbarkeit eines künstlich intelligenten Systems selbst?	329
A. Handlungs- und Schuldfähigkeit eines künstlich intelligenten Systems	331
I. Handlungsfähigkeit eines künstlich intelligenten Systems?	331
1. Früher: Kausale Handlungslehre	332
2. Finale Handlungslehre	333
3. Soziale Handlungslehre	335
4. Personale Handlungslehre	335
5. Stellungnahme und Bewertung	335
6. Zwischenergebnis	336
II. Schuldfähigkeit von autonomen, selbstlernenden Systemen?	336
III. Zwischenergebnis	339
B. Überlegungen zur Umgehung dieser dogmatischen Schwierigkeiten	339
I. Auswahl von Vorschlägen in der Literatur	339
II. Zusammenfassende Bewertung und Ausblick	340
C. Sanktionsmöglichkeiten	342
D. Zusammenfassung und Ergebnis	345

Ergebnisse und Zusammenfassung zu Teil 2	346
Teil 3: Tauglichkeit und Anpassungsbedürftigkeit des Computer- und des Datenschutzstrafrechts zum Schutz privater Nutzer smarter Systeme vor Bedrohungen durch Angriffe von „außen“	351
Abschnitt 1: Hintergrund der Bedrohungslage für private Nutzer und Ablauf der Untersuchung des Computer- und des Datenschutzstrafrechts	351
A. Gefahr von Hackingangriffen durch die Ausbreitung des Internets der Dinge in den privaten Alltag	351
B. Gegenstand und Gang der Untersuchung des Computer- und des Datenschutzstrafrechts	353
I. Begriffliche Festlegungen	353
II. Ablauf der Untersuchung und Eingrenzung des Untersuchungsgegenstands	354
Abschnitt 2: Historische, grund- und menschenrechtliche sowie funktionelle Grundlagen des Computer- und des Datenschutzstrafrechts	356
A. Die historische Entwicklung des Computer- und des Datenschutzstrafrechts unter europäischen Einflüssen und Vorgaben bis zum Jahr 2010	356
I. Frühe Vorläufer des Datenschutzstrafrechts	357
II. Bedeutungszuwachs des Datenschutzes in den 1960er und 1970er Jahren und erste Datenschutzgesetze	357
III. Konvention Nr. 108 des Europarats im Jahr 1981	359
IV. Einführung erster computerstrafrechtlicher Tatbestände im Jahr 1986	359
V. Zweites BDSG von 1991	361
VI. Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und ihre Umsetzung	362
VII. Europäische Harmonisierungen auf dem Gebiet des Computer- und des Datenschutzstrafrechts von 2001 bis 2008	364
1. Cybercrime-Konvention im Jahr 2001	364
2. Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme	366

3. Sonstige Harmonisierungen	367
VIII. Einführung des § 201a StGB im Jahr 2004	368
IX. Ausweitung der §§ 202a ff. StGB und §§ 303a f. StGB im Jahr 2007	368
B. Neue Entwicklungen im Bereich des Computer- und des Datenschutzstrafrechts in Deutschland und Europa seit 2010	370
I. Richtlinie 2013/40/EU über Angriffe auf Informationssysteme und ihre Umsetzung	371
II. VO (EU) 2016/679 (Datenschutzgrundverordnung) von 2016	373
1. Allgemeines und Anwendungsbereich	373
2. Grundsätze der Datenverarbeitung und Erlaubnistatbestände	375
3. Bußgeldtatbestände (Art. 83 DSGVO)	376
4. Strafrechtliche Vorgaben (Art. 84 DSGVO)	376
5. Die Umsetzung der strafrechtlichen Vorgaben der DSGVO in Deutschland	377
III. Weitere Harmonisierungen auf Unionsebene	378
IV. Punktuelle gesetzgeberische Aktivitäten – u.a. Einführung des § 184k StGB und des § 126a StGB im Jahr 2021	379
V. Gesetzesantrag zur Einführung des Tatbestands eines digitalen Hausfriedensbruchs	380
1. Hintergrund und Überblick über die inhaltliche Ausgestaltung	382
2. Überblick über einige Kritikpunkte aus der Literatur	383
3. Ausblick	385
C. Grund- und menschenrechtlicher Schutz des Privatlebens und von Daten	386
I. Schutz der Privats- und Intimsphäre, von Daten und informationstechnischen Systemen im Grundgesetz	386
II. Schutz des Privatlebens durch Art. 8 EMRK	388
III. Datenschutz in der GRC	390
1. Achtung des Privat- und Familienlebens nach Art. 7 GRC	390
2. Schutz personenbezogener Daten in Art. 8 GRC	390



D. Funktion, Rechtsgüter und geschützter Personenkreis des Computer- und des Datenschutzstrafrechts	392
I. Computerstrafrecht (§§ 202a ff. StGB und §§ 303a f. StGB)	392
1. Rechtsgüterschutz	392
2. Geschützter Personenkreis von §§ 202a f. StGB und §§ 303a f. StGB im Kontext privat genutzter smarter Systeme	394
a) Vorstellung und Bewertung wesentlicher Ansatzpunkte zur Bestimmung des formell Verfügungsberechtigten	394
b) Anwendung auf die mithilfe von smarten Systemen generierten und gespeicherten Daten	398
3. Zwischenergebnis	400
II. Datenschutzstrafrechtliche Anschlussstaten (u.a. §§ 201 f., 202d StGB, § 42 BDSG und § 33 KUG)	401
III. Ergebnis	402
E. Überblick über einige verfassungsrechtliche und europäische Grenzen und Vorgaben bei der Normierung und Auslegung des materiellen Computer- und Datenschutzstrafrechts	403
I. Der Verhältnismäßigkeitsgrundsatz	403
1. Allgemeines	403
2. Bedeutung des Verhältnismäßigkeitsgrundsatzes für die strafrechtliche Gesetzgebung	404
II. Das Schuldprinzip	405
III. Der strafrechtliche Bestimmtheitsgrundsatz	406
IV. Wichtige europäische Grenzen und Vorgaben	407
Abschnitt 3: Anwendbarkeit der untersuchten Tatbestände bei Angriffen auf privat genutzte smarte Systeme bzw. ihre Daten – Strafanwendungsrecht	408
A. Maßgebliche Prinzipien des Strafanwendungsrechts	409
I. Territorialitäts- und Ubiquitätsprinzip (§§ 3, 9 StGB)	409
II. Aktives (§ 7 Abs. 2 Nr. 1 StGB) und passives (§ 7 Abs. 1 StGB) Personalitätsprinzip	410
III. Staatsschutzprinzip (§ 5 StGB)	411
B. Konstellationen bei Angriffen auf privat genutzte smarte Systeme bzw. deren Daten und ihre rechtliche Bewertung	411
I. Tatbegehung von Deutschland aus	412

II. Tatbegehung aus dem Ausland	412
1. Anwendbarkeit nach dem Territorialitätsprinzip i.V.m. dem Ubiquitätsprinzip	413
a) Handlungsort im Ausland	413
b) Erfolgsort i.S.d. § 9 Abs. 1 3. Var. StGB in Deutschland?	414
aa) Deliktstypen im untersuchten Computer- und Datenschutzstrafrecht	415
bb) Erfolgsorte von computer- und datenschutzstrafrechtlichen Erfolgsdelikten	418
(1) Beispielhafte Bestimmung einiger Erfolgsorte	418
(2) Sonderproblem: Verbreitung von Daten oder Aufnahmen	420
cc) Abstrakte Gefährdungsdelikte	425
(1) Ausweitung des Handlungsorts bei abstrakten Gefährdungsdelikten im Internet?	426
(2) Ausweitung des Erfolgsorts bei abstrakten Gefährdungsdelikten?	427
c) Zwischenfazit	433
2. Anwendbarkeit nach dem Personalitätsprinzip des § 7 StGB	434
C. Zusammenfassung und Fazit	435
Abschnitt 4: Strafrechtliche Verantwortlichkeit nach Computerstrafrecht beim Angriff auf ein smartes System bzw. dessen Daten – Untersuchung der §§ 202a – 202c StGB und §§ 303a, 303b StGB	437
A. Überblick über die für den Schutz privater Nutzer des Internets der Dinge besonders relevanten Tatbestände des Computerstrafrechts	437
I. Datenbegriff der §§ 202a – 202c StGB und §§ 303a f. StGB sowie Strafantrag	438
II. Ausspähen von Daten (§ 202a StGB)	438
III. Abfangen von Daten (§ 202b StGB)	440
IV. Vorbereiten des Ausspähens oder Abfangens von Daten (§ 202c StGB)	442
V. Datenveränderung (§ 303a StGB)	444

VI. Computersabotage (§ 303b StGB)	445
VII. Konkurrenzen	447
B. Blick auf das Unionsrecht: Aktuelle Vorgaben zur Harmonisierung des Computerstrafrechts in der EU und ihre Umsetzung in Deutschland	448
I. Ausgangspunkt: Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme	449
II. Die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme	449
III. Konformität des deutschen Computerstrafrechts mit der RL 2013/40/EU?	452
1. Rechtswidriger Zugang zu Informationssystemen (Art. 3 RL)	452
2. Rechtswidriger Systemeingriff (Art. 4 RL)	453
3. Rechtswidriger Eingriff in Daten (Art. 5 RL)	455
4. Rechtswidriges Abfangen von Daten (Art. 6 RL)	455
5. Tatwerkzeuge (Art. 7 RL), Versuch und Teilnahme (Art. 8 RL)	455
6. Strafen (Art. 9 RL), Verantwortlichkeit juristischer Personen (Art. 10 RL)	456
IV. Zusammenfassung und Fazit	460
C. Typische Szenarien beim Angriff auf ein privat genutztes smartes System bzw. dessen Daten und deren rechtliche Bewertung	462
I. Angriffe durch den Einsatz von Malware	463
1. Gängige Arten von Malware	464
2. Häufige Infektionswege mit Malware	466
3. Typische Angriffskategorien auf privat genutzte smarte Systeme bzw. die dort gespeicherten Daten unter Einsatz von Malware	469
4. Strafrechtliche Bewertung des Einsatzes von Malware	471
a) Zugangsverschaffung, Ausspähen und Abfangen von Daten privat genutzter smarter Systeme mithilfe von Malware	472
aa) Ausspähen der auf den smarten Systemen gespeicherten Daten	472
(1) Tatobjekt: nicht für den Täter bestimmte Daten des smarten Systems	473

(2) Besondere Sicherung dieser Daten gegen unberechtigten Zugang	474
(3) Zugangsverschaffung durch Überwinden der Zugangssicherung	476
bb) Abfangen von zwischen smarten Systemen übermittelten Daten	478
cc) Zwischenergebnis	478
b) Beeinträchtigung der Integrität durch Löschen, Beschädigen, Verändern oder Unterdrücken von Daten smarter Systeme	479
aa) Datenveränderung (§ 303a StGB)	479
bb) Zwischenergebnis	481
c) Störung von Datenverarbeitungen in privat genutzten smarten Systemen	482
aa) Denkbare Konstellationen der Computersabotage (§ 303b StGB)	482
bb) Tatobjekt: wesentliche Datenverarbeitung für einen anderen	482
cc) Erhebliche Störung der Datenverarbeitung	485
dd) Zwischenergebnis	485
d) Vorfeld des Angriffs auf smarte Systeme bzw. deren Daten	485
aa) Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB) – Denkbare Tatbestandsvarianten	486
bb) Zweckerfordernis des § 202c Abs. 1 Nr. 2 StGB	486
cc) Versuchsstrafbarkeiten	489
dd) Zwischenergebnis	489
e) Fazit und Zusammenfassung	489
II. (Distributed) Denial of Service-Angriffe	491
1. Allgemeines zur Vorgehensweise	492
2. Denkbare Szenarien im Internet der Dinge	493
3. Strafrechtliche Bewertung	495
a) Kapern privat genutzter smarter Systeme für ein Botnetz zur Begehung eines DDoS-Angriffs	495
aa) Infektion der privat genutzten smarten Systeme zum Aufbau des Botnetzes	495
bb) Vorbereitungshandlungen	497

b) Privat genutzte smarte Systeme bzw. deren Datenverarbeitungen als Ziel eines (D)DoS-Angriffs	497
aa) Datenveränderung (§ 303a Abs. 1 StGB)	498
bb) Computersabotage (§ 303b Abs. 1 StGB)	498
cc) Vorfeldhandlungen	500
4. Fazit	500
III. Erlangung von Passwörtern mithilfe von Phishing und Einsatz dieser zum Zugriff auf Daten privat genutzter smarter Systeme	502
1. Vorgehensweise	502
2. Strafrechtliche Bewertung	503
a) § 202a Abs. 1 StGB bei Einsatz des durch Phishing erlangten Passworts	503
b) Vorfeld: § 202c StGB durch Erlangung des Passworts mithilfe von Phishing	504
c) § 42 Abs. 2 Nr. 2 BDSG	505
3. Zwischenergebnis	506
IV. Brute-Force-Methoden zum Herausfinden von Login-Daten	506
1. Vorgehensweise	507
2. Strafrechtliche Bewertung	507
a) Einsatz des mithilfe einer Brute-Force-Methode erlangten Passworts	507
b) Vorfeld: Erlangung des Passworts unter Anwendung von Brute-Force-Methoden	508
3. Zwischenergebnis	509
V. IP-Spoofing	509
1. Vorgehensweise beim IP-Spoofing	510
2. Rechtliche Bewertung des IP-Spoofing	510
3. Zwischenergebnis	511
VI. Sniffing	511
1. Vorgehensweise beim Sniffing	512
2. Strafrechtliche Bewertung des Sniffings	513
a) Ausspähen und Abfangen von Daten (§§ 202a und 202b StGB)	513
b) Vorfeldstrafbarkeit	514
c) Zwischenergebnis	514

VII. Begehung von Cyberangriffen in gewerbsmäßiger oder in organisierter Form durch Banden	515
1. Aktuelle Lage und Entwicklung	515
2. Bisherige Erfassung bandenmäßiger und gewerbsmäßiger Begehungsformen im Bereich des untersuchten Computerstrafrechts	517
3. Fazit	518
VIII. Ergebnis und Zusammenfassung der Untersuchung des Computerstrafrechts	519
D. Vorschlag und Diskussion punktueller Anpassungen im materiellen Computerstrafrecht im Hinblick auf den Schutz privater Nutzer smarter Systeme	522
I. Reichweite und Anforderungen der Zugangssicherung bei § 202a Abs. 1 StGB	523
1. Viktimologischer Hintergrund und Intention des Gesetzgebers	524
2. Gesetzeswortlaut	525
3. Systematik	526
4. Aktuelle Anforderungen in der Literatur und der Rechtsprechung	528
5. Völlige Abkehr vom Erfordernis der Zugangssicherung durch den Gesetzesentwurf zum digitalen Hausfriedensbruch	530
a) Kein Sicherungserfordernis im Rahmen des § 202e Abs. 1 Nr. 1 StGB-E	530
b) Bewertung des Entwurfs mit Blick auf das dort fehlende Erfordernis der Zugangssicherung	531
6. Stellungnahme und Plädoyer für eine nutzerfreundliche Auslegung des Merkmals der Zugangssicherung und auch ihrer Überwindung in § 202a Abs. 1 StGB	534
7. Zwischenergebnis	541
II. Erfassung auch des „Zugangs zum System“ bei § 202a Abs. 1 StGB	541
III. Datenveränderung nach § 303a Abs. 1 StGB durch reines Hinzufügen einer Schadsoftware?	542
1. Ausgangslage	542

2. Einbeziehung von Binärcodes in den Datenbegriff des § 202a Abs. 2 StGB	544
3. Zwischenergebnis	545
IV. Erfassung vorübergehender Datenentziehungen durch § 303a Abs. 1 StGB	546
1. Rechtliche Ausgangslage bei Angriffen auf privat genutzte, smarte Systeme	546
2. Stellungnahme	547
3. Zwischenergebnis	549
V. Stärkere Einbeziehung der Datenverarbeitungen privat genutzer smarter Systeme in § 303b Abs. 1 StGB	550
1. Gesetzesbegründung und bislang h.M. in der Literatur	550
2. Weitere, eher restriktivere Auslegungsansätze in der Literatur	551
3. Gesetzesentwurf zum digitalen Hausfriedensbruch, § 202e StGB-E	553
a) Inhalt der entsprechenden Regelung des § 202e Abs. 1 Nr. 3 StGB-E	553
b) Bewertung	554
4. Plädoyer für eine vermehrte Einbeziehung von Datenverarbeitungen privat genutzter Systeme in § 303b Abs. 1 StGB	556
a) Veränderter Maßstab der „Wesentlichkeit“ aufgrund der technischen Entwicklung seit Einführung des § 303b Abs. 1 StGB	557
b) Der Ansatz von Kochheim – weite Auslegung des Merkmals der „wesentlichen Bedeutung“	558
c) Vorschlag zur Bestimmung der „wesentlichen Bedeutung“ im Privatbereich in Anknüpfung an Kochheim und den Gesetzesentwurf zum digitalen Hausfriedensbruch	560
aa) Entwicklung von Kriterien	560
bb) Kein Entgegenstehen der Wortlautgrenze und der ursprünglichen Gesetzesbegründung	562
cc) Verhältnismäßigkeit einer stärkeren Einbeziehung privat genutzter smarter Systeme in den § 303b Abs. 1 StGB	563
dd) Kein Entgegenstehen europäischer Vorgaben	566

5. Zwischenergebnis	566
VI. Zweckbestimmung des Computerprogramms bei § 202c Abs. 1 Nr. 2 StGB	566
1. Problemaufriss	567
2. Gesetzeswortlaut und dogmatische Einordnung des Merkmals	568
3. „Objektivierte Zweckbestimmung“ seitens des Gesetzgebers	569
4. Ansätze zur Bestimmung des Zwecks in Rechtsprechung und Schrifttum	570
5. Eigene Bewertung	572
6. Zwischenergebnis	575
VII. Einführung und Ausweitung von Regelbeispielen bzw. Qualifikationen?	575
1. Ausgangslage	575
2. Vorschläge in Gesetzgebung und Literatur	576
a) Gesetzesentwurf zum digitalen Hausfriedensbruch	576
b) Erster Referentenentwurf des BMI zum zweiten IT-Sicherheitsgesetz	577
c) Gesetzesantrag Bayerns zum Entwurf eines Gesetzes zur Verbesserung der Bekämpfung der Cyberkriminalität	579
d) Gesetzesantrag Nordrhein-Westfalens zum Entwurf eines Gesetzes zur effektiveren Verfolgung von Computerkriminalität	581
e) Auswahl von Vorschlägen in der Literatur	582
3. Allgemeine Bewertung sowie eigene Vorschläge im Hinblick auf privat genutzte smarte Systeme	583
a) Erweiterung der aktuellen Regelbeispiele des § 303b Abs. 4 StGB	584
aa) Ausweitung der Regelbeispiele auf den Privatbereich	584
bb) Anpassung an die RL 2013/40/EU?	586
cc) Erfolgsqualifikation bei Verursachung des Todes oder einer schweren Gesundheitsschädigung?	587
b) Einführung von Regelbeispielen bei §§ 202a, 202b und 202c StGB	588



c) Einführung von Regelbeispielen bei § 303a StGB	590
4. Zwischenergebnis	592
VIII. Einführung von Versuchsstrafbarkeiten bei §§ 202a, 202b StGB?	592
1. Haltung des Gesetzgebers	593
2. Kritik und Forderungen in der Literatur	594
3. Bewertung	595
4. Zwischenergebnis	598
E. Schwierige Verfolgbarkeit von Computerstraftaten – kein Ausreichen bloßer materieller Anpassungen	598
I. Probleme der Strafverfolgung in der Praxis	598
II. Notwendigkeit zusätzlicher strafprozessualer und praktischer Maßnahmen neben dem reinen materiellen Strafrecht	600
1. Bildung und Ausbau spezialisierter Stellen für Computerkriminalität sowie gegenseitige Kooperation	600
2. Strafprozessuale Zwangsmaßnahmen zur Bekämpfung des Computerstrafrechts	604
a) Überblick über aktuell verfügbares Instrumentarium	604
b) Ausweitung strafprozessualer Zwangsmaßnahmen als Mittel und gegebenenfalls als Alternative zu Verschärfungen im materiellen Recht?	605
F. Zusammenfassung der Ergebnisse des 4. Abschnitts	606
Abschnitt 5: Strafbarkeit nach Datenschutzstrafrecht durch Anschlussstaten nach dem Eindringen in ein privat genutztes smartes System – Untersuchung der §§ 201, 201a, 202d StGB sowie § 42 BDSG und § 33 KUG	610
A. Überblick über die untersuchten Normen des Datenschutzstrafrechts	611
I. Schutz der Vertraulichkeit des Wortes (§ 201 StGB)	611
II. Schutz der Vertraulichkeit des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen (§ 201a StGB)	613
III. Verbreiten und öffentliches Zurschaustellen von Bildnissen (§ 33 KUG)	615

IV. Straftatbestände des § 42 BDSG	615
1. Unberechtigte Verarbeitung oder Erschleichen gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht (Abs. 2)	616
2. Gewerbsmäßige Offenlegung einer großen Zahl personenbezogener Daten (Abs. 1)	618
V. Datenhehlerei (§ 202d StGB)	619
B. Denkbare Szenarien datenschutzrechtlicher Anschlussstaten nach dem Eindringen in ein privat genutztes smartes System	620
I. Unbefugtes Aufnehmen und Abhören des gesprochenen Wortes über smarte Systeme	621
1. Allgemeines zur Vorgehensweise	621
2. Strafrechtliche Bewertung	623
a) Unbefugte Aufnahme des nicht öffentlich gesprochenen Wortes (§ 201 Abs. 1 Nr. 1 StGB)	624
b) Unbefugtes Abhören des gesprochenen Wortes mithilfe eines Abhörgeräts (§ 201 Abs. 2 S. 1 Nr. 1 StGB)	625
II. Herstellen oder Übertragen von Bildaufnahmen privater Nutzer nach Übernahme der Steuerung des Geräts	626
1. Denkbare Szenarien	626
2. Strafrechtliche Bewertung	627
a) Bildaufnahmen oder -übertragungen von Personen in einer Wohnung oder einem anderen geschützten Raum (§ 201a Abs. 1 Nr. 1 StGB)	628
aa) Wohnung oder anderer geschützter Raum	628
bb) Reichweite der Verletzung des höchstpersönlichen Lebensbereichs	629
b) Zurschaustellen von Hilflosigkeit (§ 201a Abs. 1 Nr. 2 StGB) oder einer verstorbenen Person (§ 201a Abs. 1 Nr. 3 StGB)	630
c) Bildaufnahmen, die die Nacktheit einer anderen Person unter 18 Jahren zum Gegenstand haben (§ 201a Abs. 3 StGB)	631
d) Bildaufnahmen intimer Körperbereiche (§ 184k Abs. 1 Nr. 1 StGB)	632
3. Zwischenfazit	632

III. Gebrauch und Verbreitung der unbefugt mittels smarter Systeme erlangten Aufnahmen und Daten	632
1. Mögliche Szenarien	633
2. Strafrechtliche Bewertung	634
a) Sonderregelungen für Bild- und Tonaufnahmen im StGB	634
b) Strafvorschrift des § 33 KUG	636
c) Straftatbestände des § 42 BDSG	637
aa) Täterkreis des § 42 BDSG	637
bb) § 42 Abs. 2 Nr. 1 BDSG	640
cc) § 42 Abs. 1 BDSG	642
dd) Strafantrag und Vorfeldstrafbarkeit	644
3. Zwischenergebnis	644
IV. Hehlerei unbefugt erlangter Daten	645
1. Denkbare Szenarien	645
2. Strafrechtliche Bewertung	646
3. Zwischenergebnis	649
V. Zusammenfassung	649
C. Vorschlag und Diskussion punktueller Anpassungen im materiellen Datenschutzstrafrecht im Hinblick auf den Schutz privater Nutzer smarter Systeme	651
I. Smarte Systeme als Abhörgeräte i.S.d. § 201 Abs. 2 Nr. 1 StGB?	652
II. Ausdehnung der „Verletzung des höchstpersönlichen Lebensbereichs“ in § 201a StGB auf Konstellationen außerhalb der Intimsphäre?	653
III. Erfordernis der Einführung einer Versuchsstrafbarkeit bei § 201a StGB?	655
1. Vorschlag einer Versuchsstrafbarkeit im Zusammenhang mit Gesetzesänderungen zur Bekämpfung von sog. Gaffern	656
2. Stellungnahme	656
IV. § 42 BDSG als Jedermannsdelikt?	658
1. Ausgangslage und Problemaufriss	658
2. Stellungnahme	659
3. Plädoyer für die Einfügung des § 42 BDSG ins StGB	660
4. Zwischenergebnis	662

V. Ausfüllung des Merkmals der „großen Anzahl von Personen“ in § 42 Abs. 1 BDSG	663
1. Ansätze in der Literatur	663
2. Stellungnahme	664
VI. Erfassung auch von Fällen unterhalb der Schwelle von Schädigungsabsicht durch § 42 Abs. 2 BDSG?	666
VII. Schwierige Strafverfolgung und Erforderlichkeit praktischer Maßnahmen auch in Bezug auf datenschutzstrafrechtliche Anschlussstaten	667
D. Blick auf das Unionsrecht – Aktuelle Vorgaben im Bereich des materiellen Datenschutzstrafrechts und deren „Umsetzung“	668
I. Öffnungsklausel in Art. 84 DSGVO	669
II. Inhaltliche Vorgaben der Öffnungsklausel des Art. 84 DSGVO	670
III. Rein strafrechtliche „Umsetzung“ des Art. 84 DSGVO in Deutschland	673
IV. Inhomogene „Umsetzung“ des Art. 84 DSGVO in anderen Ländern der EU	674
V. Kurzer Blick auf allgemeine Vorteile und Funktionen materiell-strafrechtlich harmonisierter Regelungen in der Union	677
VI. Zusammenfassung und Fazit	678
E. Vereinheitlichung der Sanktionierung von Datenschutzverstößen in besonders schweren Fällen durch eine strafrechtliche Richtlinie?	681
I. Kurzer Überblick über vorstellbare Regelungsinhalte einer strafrechtlichen Richtlinie auf dem Gebiet des Datenschutzes	681
1. Erfassung schwerer Verstöße gegen Datenschutzvorgaben	682
a) Denkbare Tatobjekte	682
b) Denkbare Tathandlungen	683
c) Schädigungs- oder Bereicherungsabsicht	684
2. Strafen und Begriffsdefinitionen	685
II. Gesetzgebungskompetenz der EU zur Harmonisierung datenschutzstrafrechtlicher Vorschriften?	685
1. Keine originäre, allgemeine Strafrechtssetzungskompetenz	685

2. Harmonisierung nach Art. 82 AEUV oder Art. 83 AEUV	687
a) Art. 82 Abs. 2 AEUV	687
b) Art. 83 Abs. 1 AEUV	688
c) Annexkompetenz des Art. 83 Abs. 2 AEUV	690
aa) Gebiet der Unionspolitik, auf dem Harmonisierungsmaßnahmen erfolgt sind	691
bb) Unerlässlichkeit der strafrechtlichen Harmonisierung?	693
(1) Ausgangspunkt: restriktive Auslegung des Merkmals der Unerlässlichkeit in Art. 83 Abs. 2 AEUV	693
(2) Erschwerte Zusammenarbeit und Gefahr von Forum Shopping angesichts inhomogener Rechtslage	696
(3) Bereits existierendes unionsweites Sanktionsregime auf Bußgeldebene	698
(4) Fazit und Ausblick	700
III. Zwischenergebnis	702
Ergebnisse und Zusammenfassung zu Teil 3	702
Teil 4: Berührungspunkte und Wechselwirkungen von Produkt-, Computer- und Datenschutzstrafrecht beim Schutz privater Nutzer	709
Abschnitt 1: Hackingangriff auf ein smartes Produkt durch Ausnutzung von IT-Sicherheitslücken	709
A. Strafrechtliche Verantwortlichkeit des Hackers	710
I. Computer- und Datenschutzstrafrecht	710
II. Körperverletzungs- und Tötungsdelikte	711
B. Strafrechtliche Verantwortlichkeit des Herstellers smarter Systeme für Verletzungsfolgen aufgrund von Hackingangriffen	712
I. Strafbarkeit des Herstellers nach §§ 229 und 222 StGB	712
1. Objektive Sorgfaltspflichtverletzung des Herstellers smarter Systeme	712
2. Objektive Vorhersehbarkeit des Erfolges	714
3. Ausschluss der objektiven Zurechnung?	715
a) Schutzzweck der Norm	715
b) Atypischer Kausalverlauf	717

c) Dazwischentreten eines Dritten durch den vorsätzlichen Cyberangriff	717
aa) Regressverbotslehre	718
bb) Aktuell herrschende Meinung	719
cc) Lehre von der Tatgeneigtheit	719
dd) Stellungnahme und Vorschlag zur Einschränkung der Herstellerhaftung	720
4. Zwischenergebnis	723
II. Strafbarkeit nach §§ 201 f., 202a ff., 303a f. StGB oder § 42 BDSG	723
Abschnitt 2: Cyberangriff auf den Hersteller mit Auswirkungen auf private Nutzer	724
A. Denkbare Konstellationen	724
B. Strafrechtliche Bewertung	725
I. Strafrechtliche Verantwortlichkeit des Hackers	725
1. Cyberangriff auf die Produktion des Herstellers	725
2. Cyberangriff auf Hersteller-Clouds	726
II. Strafrechtliche Verantwortlichkeit des Herstellers	728
1. Objektive Fahrlässigkeit	728
2. Objektive Zurechnung – Dazwischentreten eines Dritten	729
Abschnitt 3: „Innenangriff“ auf smarte Systeme durch Mitarbeiter des Herstellers	730
A. Mögliche Szenarien	730
B. Strafrechtliche Bewertung	731
I. „Veruntreuen“ anvertrauter Daten durch unbefugte Verschaffung oder Weitergabe	731
II. Unbefugte Zugangsverschaffung zu Daten über eine heimlich in die Produktsoftware integrierte Backdoor	732
III. Beeinträchtigung von Daten- oder Datenverarbeitungen	733
IV. Weitere datenschutzrechtliche Anschlussdelikte	734
V. Zwischenfazit und Zusammenfassung	734
C. Vorschläge in der Literatur zur Schließung von Lücken	735
D. Eigene Würdigung	736
Abschnitt 4: Präventive Wirkung der Produktverantwortlichkeit hin zur Vermeidung von Computer- und Datenkriminalität	737
A. Ausgangslage	737

B. Einfluss des Produktstrafrechts auf die IT-Sicherheit	738
Ergebnisse und Zusammenfassung zu Teil 4	739
Schlussbetrachtung	743
Abschnitt 1: Zusammenfassung	743
A. Schutz privater Nutzer vor Produktbedrohungen von „innen“	743
B. Schutz privater Nutzer vor Produktbedrohungen von „außen“	750
I. Schutz vor Hackingangriffen durch das Computerstrafrecht	751
II. Schutz vor datenschutzstrafrechtlichen Anschlussstaten von außen durch das Datenschutzstrafrecht	757
C. Berührungspunkte beim Schutz privater Nutzer	761
Abschnitt 2: Abschließendes Fazit	763
Literaturverzeichnis	767
Anhang	809