

# 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 Anschlussstaten 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