

Strafrechtliche Abhandlungen

Neue Folge · Band 321

Das Internet der Dinge und das Strafrecht

**Herausforderungen vernetzter Geräte für
das materielle Strafrecht und das Strafprozessrecht**

Von

Florian Nicolai



Duncker & Humblot · Berlin

FLORIAN NICOLAI

Das Internet der Dinge und das Strafrecht

Strafrechtliche Abhandlungen · Neue Folge

Begründet von Dr. Eberhard Schmidhäuser (†)

em. ord. Prof. der Rechte an der Universität Hamburg

Herausgegeben von

Dr. Dres. h. c. Friedrich-Christian Schroeder (†)

em. ord. Prof. der Rechte an der Universität Regensburg

und

Dr. Andreas Hoyer

ord. Prof. der Rechte an der Universität Kiel

in Zusammenarbeit mit den Strafrechtslehrern der deutschen Universitäten

Band 321

Das Internet der Dinge und das Strafrecht

Herausforderungen vernetzter Geräte für
das materielle Strafrecht und das Strafprozessrecht

Von

Florian Nicolai



Duncker & Humblot · Berlin

Gedruckt mit Unterstützung der Deutschen Forschungsgemeinschaft (DFG)

Zur Aufnahme in die Reihe empfohlen von
Professor Dr. Hans Kudlich, Erlangen

Der Fachbereich Rechtswissenschaft
der Friedrich-Alexander-Universität Erlangen-Nürnberg hat
diese Arbeit im Jahre 2023 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
© 2024 Duncker & Humblot GmbH, Berlin
Satz: 3w+p GmbH, Rimpf
Druck: CPI Books GmbH, Leck
Printed in Germany

ISSN 0720-7271
ISBN 978-3-428-19056-0 (Print)
ISBN 978-3-428-59056-8 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☼

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

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde vom Fachbereich Rechtswissenschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg im Sommer 2023 als Dissertation angenommen. Literatur und Rechtsprechung konnten bis Dezember 2023 berücksichtigt werden. Die Arbeit entstand im Rahmen des DFG-Graduiertenkollegs 2475 „Cyberkriminalität und Forensische Informatik“. Für den großzügigen Druckkostenzuschuss danke ich der Deutschen Forschungsgemeinschaft (DFG). Für die Aufnahme in die Schriftenreihe „Strafrechtliche Abhandlungen – Neue Folge“ danke ich den Herausgebern, den Verantwortlichen des Verlages Duncker & Humblot, namentlich Frau Anke Geidel, für die freundliche Betreuung bei der Publikation.

Die Anfertigung einer Dissertation ist, wie alles im Leben, nur möglich (jedenfalls aber leichter), wenn man das Glück hat von unterstützenden Menschen umgeben zu sein. Einigen von ihnen möchte ich im Folgenden meinen Dank aussprechen.

Mein tiefer Dank gilt meinem Doktorvater Herrn Prof. Dr. Hans Kudlich, der mir stets mit wertvollem Rat zur Seite stand und steht – sowohl wissenschaftlich als auch bei anderen Fragen des Lebens. Für die Gewährung größtmöglicher wissenschaftlicher Freiheit bei zugleich bestmöglicher Betreuung bin ich außerordentlich dankbar. Die familiäre, vertrauensvolle Atmosphäre an seinem Lehrstuhl ist von unschätzbarem Wert. Herzlich danken möchte ich zudem Frau Prof. Dr. Gabriele Kett-Straub nicht nur für die zügige Erstellung des Zweitgutachtens, sondern auch dafür, dass auch sie stets ein offenes Ohr hatte – und nicht zuletzt dafür, dass Sie bereits zu Beginn meines Studiums meine Freude am Strafrecht geweckt hat. Außerdem danke ich Herrn Prof. Dr. Christian Jäger, an dessen Lehrstuhl ich als studentische Hilfskraft meine ersten Erfahrungen in der wissenschaftlichen Welt sammeln durfte.

Die Arbeit im Graduiertenkolleg war v. a. aufgrund des steten Austauschs mit den anderen Mitgliedern sehr bereichernd. Aus den Reihen des Graduiertenkollegs danke ich daher besonders: Herrn Prof. Dr.-Ing. Jürgen Teich für die freundliche Unterstützung bei Fragen zu technischen Einzelheiten smarterer Geräte, Herrn Prof. Dr. Christoph Safferling für seine kritischen Anregungen und unsere Diskussionen sowie Herrn Prof. Dr.-Ing. Felix Freiling, der mit seiner herzlichen und unkomplizierten Art die Arbeit im Graduiertenkolleg zu einer wahren Freude gemacht hat. Die „AG StPO und IT-Forensik“ ermöglichte regelmäßige interdisziplinäre Diskussionen, für die ich allen Mitgliedern – namentlich dem Initiator der AG, Herrn Prof. Dr. Christian Rückert – sehr dankbar bin. Ebenso denke ich sehr gerne an die GRK-Workshops mit Herrn Dr. Dominic Deuber, Frau Dr. Janine Schneider und Herrn Dr. Jens Trautmann zurück.

Herrn Moritz Gärber und Herrn Mathis Ohlig danke ich vielmals für die tatkräftige redaktionelle Unterstützung, ebenso danke ich Frau Muriel Brixner, Herrn Ali Demir, Herrn Luis Reinwald, Herrn Philipp Schnapp und Herrn Bill Yan, die mir bei der Endkontrolle vor der Drucklegung der Arbeit engagiert zur Seite standen.

Eine große Freude war mein Aufenthalt als Gastwissenschaftler am *Institutet för Rättsinformatik* der Universität Stockholm im Sommer 2022, bei dem eine fortwährende Zusammenarbeit entstand. Ich danke insbesondere Prof. Peter Wahlgren, LL.D. und Prof. Liane Colonna, LL.D. für die herzliche Aufnahme am Institut. Frau Marie Hessel danke ich dafür, dass sie mit ihrer offenen, zugewandten Art der Motor dafür war, Stockholm zu einem zweiten zu Hause für mich werden zu lassen. Tack så jättemycket!

Herzlich danken möchte ich zudem Frau Jana Kuhlmann, Frau Dr. Anna-Lena Nix, Frau Anna Sperber und Herrn Johannes Weichselbaum, die allesamt für eine juristische Sekunde „nur“ meine Kollegen waren, doch sofort zu engen Freunden und lieben Begleitern durch Studium, Referendariat, Promotion und das Leben außerhalb des Juridicums wurden. Gleiches gilt für Prof. Dr. Mustafa Temmuz Oğlacioğlu, dem ich für unsere vielen inspirierenden und motivierenden Gespräche danken möchte. Ebenso danke ich Herrn Simon Kreiner, der nicht müde wurde, mich nach langen Tagen am Schreibtisch zum Sport zu motivieren.

Besonders danken möchte ich Herrn Bernhard Gahr, Herrn Stefan Gebhard und Frau Susanne Moseev. Unsere schon über Jahrzehnte währende Freundschaft hat mich immer beflügelt und ist mir eine fortwährende Energie- und Glücksquelle, für die ich unermesslich dankbar bin.

Der größte Dank gilt meinen Eltern und meinen Großeltern. Ihnen ist diese Arbeit gewidmet. Sie haben mir schon immer die Freiheit gewährt, mich frei zu entfalten und meine eigenen Ziele zu verfolgen. Ohne ihre Liebe und ihren Rückhalt wäre die Anfertigung dieser Arbeit nicht möglich gewesen. Die Dankbarkeit, die ich dafür empfinde, lässt sich nicht in Worte fassen.

Nürnberg, im Februar 2024

Florian Nicolai

Inhaltsübersicht

Einleitung: Smarte Geräte – Smartes Strafrecht?	23
--	----

Kapitel 1

Rechtstatsächliche Grundlagen	25
A. Das Internet der Dinge (IoT)	25
B. Der Bezug zum Strafrecht – Das Strafrecht der Dinge	48

Kapitel 2

Das Internet der Dinge und das materielle Strafrecht	67
A. Materiellrechtliche Herausforderungen	67
B. Aktuelle Reformbestrebungen des Gesetzgebers	179
C. Fazit der materiellrechtlichen Betrachtungen	181

Kapitel 3

Das Internet der Dinge und das Strafprozessrecht	182
A. Das Internet der Dinge als digitale Ermittlungsperson	182
B. Grundrechtsschutz von IoT-Daten und Systemen	183
C. Strafprozessuale Eingriffsnormen für den Zugriff auf Daten, Geräte und Systeme des IoT	213
D. Strafprozessuale Grundsätze und Grenzen im Zusammenhang mit dem IoT	289
E. Fazit der strafprozessualen Betrachtungen	368

Schlussbemerkungen	369
---------------------------------	-----

Literatur	371
------------------------	-----

Sachwortverzeichnis	407
----------------------------------	-----

Inhaltsverzeichnis

Einleitung: Smarte Geräte – Smartes Strafrecht?	23
--	----

Kapitel 1

Rechtstatsächliche Grundlagen	25
A. Das Internet der Dinge (IoT)	25
I. Hinführung	25
II. Ausgewählte Anwendungsbereiche	26
1. SmartHome	28
a) Utopie und Dystopie des SmartHome	28
b) Allgemeines	28
c) Aufbau und Funktionsweise	30
d) Vorteile der Nutzung	32
2. SmartCar	33
a) Utopie und Dystopie des SmartCar	33
b) Allgemeines	33
c) Aufbau und Funktionsweise	34
d) Vorteile der Nutzung	37
3. IoT im Gesundheitswesen/Medical IoT (MIoT)	39
a) Utopie und Dystopie des Medical IoT	39
b) Allgemeines	40
c) Aufbau und Funktionsweise	41
d) Vorteile der Nutzung	43
III. Fazit – Die Vernetzung des Alltags	47
B. Der Bezug zum Strafrecht – Das Strafrecht der Dinge	48
I. Bezug zum materiellen Strafrecht	48
1. SmartHome	51
2. SmartCar	54
3. IoT im Gesundheitswesen/Medical IoT (MIoT)	57
II. Bezug zum Strafprozessrecht	60
1. SmartHome	62
2. SmartCar	63
3. IoT im Gesundheitswesen/Medical IoT (MIoT)	64

III. Fazit der rechtstatsächlichen Erwägungen	65
---	----

Kapitel 2

Das Internet der Dinge und das materielle Strafrecht	67
A. Materiellrechtliche Herausforderungen	67
I. Der strafrechtliche Schutz der Daten des IoT	68
1. Ausspähen von Daten, § 202a StGB	70
a) Rechtsgut/Allgemeines	70
b) Tatobjekt	70
aa) Datenbegriff, Einschränkung nach Abs. 2	70
(1) Speicherung	70
(a) Rechtstatsächliches	71
(b) Speicherung der Daten im Arbeitsspeicher	72
(aa) Speicherung im Arbeitsspeicher nicht ausreichend	73
(bb) Speicherung im Arbeitsspeicher ausreichend	74
(c) Ergebnis	75
(2) Übermittlung	76
(a) Rechtstatsächliches	77
(b) Zugriff auf Daten in Sensorgeräten und Geräte-zu-Geräte-Übermittlungen	78
(aa) Geräte-zu-Geräte-Kommunikation als übermittelte Daten i. S. d. § 202a Abs. 2 StGB	78
(bb) Zugriff am Sensorgerät	80
(3) Fazit: IoT und der Datenbegriff nach § 202a Abs. 2 StGB	82
bb) Nicht für den Täter bestimmt	82
cc) Gegen unberechtigten Zugang besonders gesichert	86
(1) Sicherungsmechanismen	87
(2) Verschlüsselung als Zugangssicherung	87
c) Tathandlung	90
d) Zusammenfassung und Übertragung auf IoT-Sachverhalte	91
2. Abfangen von Daten, § 202b StGB	93
a) Daten aus einer nichtöffentlichen Datenübermittlung	93
aa) Datenübermittlung	93
bb) Nichtöffentlich	94
b) Daten aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage	96
c) Tathandlung	97
d) Zusammenfassung und Übertragung auf IoT-Sachverhalte	98
3. Vorbereiten des Ausspähens und Abfangens von Daten, § 202c StGB	98

4. Datenhehlerei, § 202d StGB	100
5. Weitere Delikte des 15. Abschnitts des StGB	102
6. Verletzung von Geschäftsgeheimnissen, § 23 GeschGehG	102
7. Strafvorschriften des BDSG, § 42 BDSG (n.F.)	104
a) § 42 Abs. 1 BDSG	104
aa) Personenbezogene Daten	105
bb) Nicht allgemein zugänglich	108
cc) Personenbezogene Daten einer großen Zahl von Personen	108
dd) Übermittlung/Zugänglichmachen	110
ee) Ohne Berechtigung	110
(1) Informationsgrundlage	111
(2) Freiwilligkeit der Einwilligung	112
(3) Einwilligung bei IoT-Sachverhalten	113
ff) Subjektiver Tatbestand: Gewerbsmäßiges Handeln	115
b) § 42 Abs. 2 BDSG	115
aa) Nicht allgemein zugängliche personenbezogene Daten	115
bb) Tathandlungen im Einzelnen	116
cc) Gegen Entgelt oder mit Bereicherungs-/Schädigungsabsicht	116
c) Fazit: Das IoT und der strafrechtliche Schutz durch das BDSG	117
8. Fazit: Der strafrechtliche Schutz der Daten des IoT	118
II. Der strafrechtliche Schutz der (Integrität der) Systeme und Geräte des IoT	119
1. Datenveränderung, § 303a StGB	120
a) Schutzgut	120
b) Tatobjekt	121
aa) Einschränkung des Tatobjekts	121
bb) Eigentümerähnliche Verfügungsbefugnis	121
cc) Dogmatische Anknüpfung	123
c) Tathandlungen	124
d) Subjektiver Tatbestand	126
e) Übertragung auf Konstellationen des IoT	126
2. Computersabotage, § 303b StGB	127
a) Allgemeines	128
b) Tatobjekt: Datenverarbeitung	129
c) Wesentliche Bedeutung der Datenverarbeitung	129
aa) Die Problematik des unbestimmten Rechtsbegriffs	131
bb) Definitions-/Konkretisierungsansätze	132
cc) Auslegungshilfe: Die Gesetzesbegründung/Beschlussempfehlung	134
(1) Betriebe, Behörden und Unternehmen	134
(2) Private	135
(3) Fazit	135

dd) Auslegungshilfe: Die Ratio	135
(1) Europarechtliche Vorgaben	136
(2) Die Filterfunktion	137
(3) Allgemeine Bagatellgrenze	138
(4) „Wesentlichkeit“ als höhere Schwelle unbestimmt	140
ee) Kasuistik und richterliche Rechtsfortbildung	141
(1) Kasuistik der Strafgerichtsbarkeit	142
(a) LG Ulm, Urteil v. 1.12.1988 – 1 Ns 229/88-01	142
(b) OLG Frankfurt/M., Beschluss v. 22.5.2006 – 1 Ss 319/05	142
(c) LG Düsseldorf, Urteil v. 22.3.2011 – 3 KLS 1/11	143
(d) AG Wiesbaden, Beschluss v. 2.5.2012 – 71 Gs 393/12	143
(e) BGH, Beschluss v. 11.1.2017 – 5 StR 164/16/LG Leipzig, Urteil v. 4.2.2016 – 11 KLS 390 Js 9/15	143
(f) BGH, Beschluss v. 8.4.2021 – 1 StR 78/21	144
(2) Kasuistik anderer Gerichtsbarkeiten	144
(3) Fazit	145
ff) Kasuistische Konkretisierungsversuche in der strafrechtlichen Literatur	146
(1) Betriebe, Unternehmen, Behörden	146
(2) Private	147
(3) Fazit zu den Konkretisierungsversuchen in der Literatur	149
gg) Herausarbeitung abstrakter Kriterien	152
(1) Betriebe, Unternehmen und Behörden	152
(2) Private	157
(a) Maßstab	157
(aa) Rein objektiver Maßstab	158
(bb) Einfluss subjektiver Aspekte	158
(cc) Stellungnahme/Lösung: Gemischt objektiv-subjektiver (in- dividueller) Ansatz	160
(b) Mögliche Abgrenzungskriterien bei Privaten	163
(aa) Rein wirtschaftliche Abgrenzung	163
(a) Keine „geltungserhaltende Reduktion“ auf wirtschaftli- che Gesichtspunkte	164
(β) Scheinargument Affektionsinteresse	165
(γ) Stellungnahme: Wirtschaftlicher Bezug kein pauschales Abgrenzungskriterium	165
(bb) Primär der Datenverarbeitung dienend	167
(cc) Konkretisierung anhand anderer Merkmale nicht möglich	168
d) Fazit: Unbestimmtheit des § 303b Abs. 1 StGB	169
e) Bei Anwendung trotz hier angenommener Unbestimmtheit: Restriktive Einzelfallentscheidungen	170

f) Tathandlung	171
aa) Abs. 1 Nr. 1 – Datenveränderung nach § 303a Abs. 1 StGB	171
bb) Abs. 1 Nr. 2 – Eingabe oder Übermittlung von Daten (§ 202a Abs. 2 StGB) in Nachteilszufügungsabsicht	171
cc) Abs. 1 Nr. 3 – Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern (Sabotagehandlungen) einer Datenverarbeitungsanlage oder eines Datenträgers	172
g) Tataufschlag: Erhebliche Störung der Datenverarbeitung	174
h) Regelbeispiele des Abs. 4	176
3. Fazit: Der strafrechtliche Schutz der (Integrität der) Systeme und Geräte des IoT	177
B. Aktuelle Reformbestrebungen des Gesetzgebers	179
C. Fazit der materiellrechtlichen Betrachtungen	181

Kapitel 3

Das Internet der Dinge und das Strafprozessrecht	182
A. Das Internet der Dinge als digitale Ermittlungsperson	182
B. Grundrechtsschutz von IoT-Daten und Systemen	183
I. Grundsätzliches	183
II. Das Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	184
III. Das Fernmeldegeheimnis (Telekommunikationsgeheimnis), Art. 10 Abs. 1 Var. 3 GG	184
1. Allgemeines	185
2. Das Telekommunikationsgeheimnis im Kontext des IoT	186
a) Menschliche Komponente/Geräte-zu-Geräte-Kommunikation	186
b) Notwendige Anzahl der Kommunikationsteilnehmer	188
aa) Mindestens zwei Teilnehmer	189
bb) Ein Teilnehmer ausreichend	189
cc) Stellungnahme	190
3. Schlussfolgerungen für IoT-Konstellationen	192
a) In Peripherie- und Steuergeräten gespeicherte Daten	192
b) Geräte-zu-Geräte-Übermittlung	193
c) Cloud-Übermittlung und Cloud-Speicherung	193
4. Fazit	195
IV. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht), Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	196
1. Allgemeines	196

2. Das IT-Grundrecht im Kontext des IoT	197
a) Komplexität und Persönlichkeitsrelevanz	197
b) Grenzen des Schutzbereichs – Grenzen des informationstechnischen Systems	198
3. Schlussfolgerungen für IoT-Konstellationen	200
4. Fazit	202
V. Art. 13 GG – Unverletzlichkeit der Wohnung	202
1. Allgemeines	202
2. Die Unverletzlichkeit der Wohnung im Kontext des IoT	203
a) Strafprozessualer Zugriff durch physisches Eindringen in die Wohnung	203
b) Strafprozessualer Zugriff ohne physisches Eindringen in die Wohnung	204
aa) Gerät außerhalb von Wohnraum	204
bb) Gerät innerhalb von Wohnraum	205
(1) Art. 13 Abs. 1 GG betroffen	205
(2) Art. 13 Abs. 1 GG nicht betroffen	206
(3) Stellungnahme und differenzierende Ansicht	206
(a) Stellungnahme	206
(b) Ausnahme: Notwendigkeit einer differenzierenden Betrachtung	209
3. Schlussfolgerungen für IoT-Konstellationen	211
4. Fazit	211
VI. Fazit Grundrechtlicher Schutz	213
C. Strafprozessuale Eingriffsnormen für den Zugriff auf Daten, Geräte und Systeme des IoT	213
I. Der strafprozessuale Zugriff auf gespeicherte Daten in den IoT-Systemen	214
1. Der Zugriff auf in Peripheriegeräten gespeicherte IoT-Daten	214
a) Daten in IoT-Geräten	215
b) Peripherie- und Steuergeräte	215
c) Grundrechtliche Implikationen	215
d) Strafprozessuale Ermittlungsmaßnahmen zum Zugriff auf in den Peripheriegeräten gespeicherte Daten	216
aa) § 94 StPO	216
(1) Daten als Gegenstand i. S. d. § 94 ff. StPO	217
(2) Sicherstellung und Beschlagnahme der Daten aus den IoT-Geräten gem. § 94 StPO	218
(a) Eingriffe in das IT-Grundrecht über § 94 StPO	219
(b) Eingriffe in das Telekommunikationsgeheimnis, Art. 10 Abs. 1 Var. 3 StPO, über § 94 StPO	219
(c) Eingriffe in das Wohnungsgrundrecht über § 94 StPO	220
(3) Maßnahmen im Zusammenhang mit der Durchsuchung beim Beschuldigten, §§ 102 StPO, § 110 Abs. 3 StPO	220
bb) § 100a StPO	222

cc) § 100b StPO	222
dd) Fazit	223
2. Der Zugriff auf IoT-Daten in einem Steuergerät	224
3. Der Zugriff auf gespeicherte IoT-Daten in der Cloud	225
a) Rechtstatsächliches – Daten in der Cloud	225
b) Grundrechtliche Implikationen	225
c) Zugriff auf die gespeicherten Daten	225
aa) §§ 94 ff. StPO (i. V. m. §§ 102, 110 Abs. 3 StPO)	226
bb) § 100a StPO	227
cc) § 100b StPO	227
d) Exkurs: Zugriff auf Cloud-Daten im Ausland	227
aa) Kein Zugriff über nationale Ermittlungsmaßnahmen der StPO	227
bb) Folge von Verstößen: Beweisverwertungsverbot	228
cc) Rückgriff auf Rechtshilfverfahren	229
dd) Zusammenfassung	229
e) Fazit	229
4. Daten auf dem Server des Herstellers/Diensteanbieters (ohne Cloud)	230
II. Der strafprozessuale Zugriff auf Übertragungsdaten in, von und zu IoT-Geräten	231
1. Überwachung von IoT-Kommunikation	231
a) Grundrechtliche Implikationen	231
b) §§ 94 ff. (ggf. i. V. m. § 110 Abs. 3) StPO	232
aa) Schutzbereich IT-Grundrecht	232
bb) Schutzbereich Telekommunikationsgeheimnis	232
c) § 100a StPO	232
aa) Rein technischer Telekommunikationsbegriff	233
bb) Technikorientierte Auslegung des BGH	234
cc) Grundrechtsanaloge Auslegung	234
dd) Genuin strafprozessualer Telekommunikationsbegriff	235
ee) Stellungnahme	236
(1) Ablehnung des rein technischen Telekommunikationsbegriffs	236
(2) Ablehnung der Definition des BGH	237
(3) Ablehnung der grundrechtsorientierten Auslegung	237
(4) Vorzugswürdigkeit eines genuin strafprozessualen Telekommunikationsbegriffs	238
ff) Subsumtion der IoT-Geräte-zu-Geräte-Kommunikation unter den genuin strafprozessualen Telekommunikationsbegriff	239
(1) Geräte-zu-Geräte-Kommunikation	239
(2) IoT-Cloud-Kommunikation	240
(3) Sonderfall: Sprachassistenten/SmartSpeaker	241
gg) Zwischenergebnis	242

d) § 100b	242
2. Fazit	243
III. Die Live-Überwachung und der gezielte Einsatz der IoT-Geräte durch die Ermittlungsbehörden	244
1. Akustische Wohnraumüberwachung mit Hilfe der IoT-Technik	245
a) § 100c StPO	246
aa) Wortlaut sowie Sinn und Zweck	247
bb) Grundrechtliche Erwägungen	247
(1) Verletzung des IT-Grundrechts, Art. 2 Abs. 1 i. V.m. Art. 1 Abs. 1 GG	247
(2) Die argumentative Räuberleiter der Entwicklungsoffenheit	248
cc) Systematik der Eingriffsbefugnisse	249
(1) Abschließende Regelungen zu Eingriffen in informationstechnische Systeme	249
(2) Technische Mittel vs. Informationstechnisches System	250
dd) Zwischenergebnis § 100c StPO	251
b) § 100b StPO	251
aa) Wortlaut	252
(1) Daraus vs. damit	252
(2) Durchsuchung	253
(3) Gebotenheit restriktiver Auslegung	254
(4) Sinn und Zweck	254
bb) Grundrechtsrelevanz	256
cc) Keine Ausnahme: Aktivierung durch den Betroffenen selbst	256
c) § 100a StPO	259
d) Kombination mehrerer Maßnahmen	260
aa) Parallele Anwendung verschiedener Ermittlungsmaßnahmen	260
bb) Kombination verschiedener Eingriffsbefugnisse für dieselbe Maßnahme	261
cc) Exkurs: Normenklarheit	262
dd) Fazit	264
e) Fazit akustische Wohnraumüberwachung	264
2. Akustische Überwachung außerhalb von Wohnraum mit Hilfe der IoT-Technik	264
a) § 100f StPO	264
b) § 100b StPO	266
aa) Ausnahme: Veranlassung durch den Betroffenen	266
bb) Rückausnahme: Einsatz kriminalistischer List	267
c) § 100a StPO	268
d) Kombination	270
3. Optische Wohnraumüberwachung mit Hilfe der IoT-Technik	270

4. Optische Überwachung außerhalb von Wohnraum mit Hilfe der IoT-Technik	271
a) § 100h StPO	271
aa) Abs. 1 S. 1 Nr. 1	272
(1) Technisches Mittel	272
(2) Eingriff in informationstechnisches System	272
bb) Abs. 1 S. 1 Nr. 2	273
b) § 100b StPO	273
5. Live-Überwachung mittels anderer IoT-Sensoren	274
a) § 100b StPO	274
b) Weitere Daten außerhalb von Wohnraum, § 100h Abs. S. 2 StPO	275
IV. Erhebung von Nicht-Inhaltsdaten – Ein Überblick	276
1. § 100g StPO – Erhebung von Verkehrsdaten	276
2. § 100h StPO – GPS-Daten außerhalb von Wohnraum	277
3. § 100i StPO – Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten	277
4. § 100j StPO – Bestandsdatenauskunft	278
5. § 100k StPO – Erhebung von Nutzungsdaten von Telemediendiensten	279
V. Die Notwendigkeit spezieller strafprozessualer Ermittlungsmaßnahmen – Kein Rückgriff auf die Ermittlungsgeneralklausel möglich	280
1. § 161 StPO als Ermittlungsgeneralklausel	280
2. Bestimmung der maximalen Eingriffstiefe der Generalklauseln	281
a) Die leere Hülle der Schwellentheorie	281
b) Abgrenzungskriterien	282
aa) Binnensystematik: Vergleich mit <i>leges speciales</i>	283
bb) Zwang	284
cc) Heimlichkeit	285
dd) Privatsphäre-Eingriff/Höchstpersönlicher Lebensbereich	286
c) Folgen für IoT-Ermittlungen	286
VI. Fazit	288
D. Strafprozessuale Grundsätze und Grenzen im Zusammenhang mit dem IoT	289
I. Grenze der Totalüberwachung	289
1. Totalüberwachung	290
2. Keine gesetzliche Absicherung	292
3. Totalausforschung bei einzelner Maßnahme	292
4. Neue Dimensionen der Totalüberwachung aufgrund des IoT	293
5. Fazit – Totalüberwachung und das IoT	295
II. Der Kernbereichsschutz	296
1. Allgemeines	296
2. Die besonderen Kernbereichsregelungen des § 100d StPO	297
3. Inhalt des Kernbereichs höchstpersönlicher Lebensgestaltung	298
a) Grundsätze	298

b) Kriterien der Zuordnung zum Kernbereich	299
aa) Formal	300
bb) Inhaltlich	301
(1) Grundsatz: Höchstpersönlichkeit vs. Sozialbezug	301
(2) Sozialbezug durch Straftatbezug	302
(a) Rechtsprechung des BVerfG	302
(b) Kritik	303
4. Die Grundsätze des Kernbereichs im IoT	306
a) Formal	306
b) Inhaltlich	307
5. Fazit – Der Kernbereichsschutz und das IoT	309
III. Die Selbstbelastungsfreiheit	309
1. Allgemeines	310
2. Nemo Tenetur: Der Grundsatz	311
3. Einfachgesetzliche Ausprägungen des Grundsatzes	312
4. Inhalt und Reichweite	313
a) Aktives Handeln und passives Dulden	313
b) Extensive Ansätze	314
c) Eigenverantwortlichkeit der Entscheidung	315
d) Augenscheinobjekt vs. Wissensobjekt	316
e) Stellungnahme	317
5. Die Herleitung des Nemo-Tenetur-Grundsatzes – Auf der Suche der Veranke- rung eines Grundsatzes von Verfassungsrang	317
a) Menschenwürde, Art. 1 I GG	319
aa) Unzumutbarkeit: Selbsterhaltungstrieb	320
bb) Unzumutbarkeit: Ethische Überforderung	322
cc) Instrumentalisierung/Subjektstellung	324
b) Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG – Allgemeines Persönlichkeits- recht	325
aa) Nemo Tenetur als eigene Ausprägung des Allgemeinen Persönlich- keitsrechts	325
bb) Recht auf informationelle Selbstbestimmung	326
c) Eigenverantwortung (Ransiek)	327
d) Wissensschutz (Reiß)	328
e) Orientierung an Verfahrensgrundsätzen	328
aa) Allgemein	328
bb) Legitimation/Akzeptanz des Verfahrens (Lesch/Pawlik)	329
f) Ableitung aus der Unschuldsvermutung, Art. 6 EMRK	330
g) Stellungnahme – Eklektischer Ansatz	331

6. Die Selbstbelastungsfreiheit und das IoT	334
a) Die Freiheit von Selbstbelastung bei Nutzung des IoT – Eine zweigliedrige Frage	335
aa) Freiheit Stufe 1 – Benutzung der Geräte	335
(1) Sozialer „Zwang“	336
(2) „Zwang“ aus Sorge um die Gesundheit	338
(3) „Zwang“ des Marktes	338
(4) Wirtschaftlicher „Zwang“ durch Versicherungstarife	339
(a) KfZ-Haftpflicht-/Kasko-Versicherungen	340
(b) Hausratversicherungen etc.	342
(c) Lebens- und Krankenversicherung	342
(5) Staatlicher „Zwang“	344
(6) Fazit: Freiheit Stufe 1	346
bb) Freiheit Stufe 2 – Freiwillige Preisgabe mit Nutzung der Daten?	347
(1) Keine Konstruktion einer Einwilligung	347
(2) Kein Fall von Nemo-Tenetur?	348
(3) Fazit: Freiheit Stufe 2	350
b) Die Ratio der Selbstbelastungsfreiheit im Lichte von Ermittlungen mithilfe des IoT	350
aa) Menschenwürde – Ethische Überforderung und Selbsterhaltungstrieb	350
bb) Menschenwürde – Objektifizierung	351
cc) Allgemeines Persönlichkeitsrecht, Art. 1 I GG i. V.m. Art. 2 I GG	352
dd) Eigenverantwortung	354
ee) Wissensschutz	354
ff) Ausnahme von genereller Mitwirkungspflicht (Pawlik)	355
c) Inhalt und Reichweite der Selbstbelastungsfreiheit mit Blick auf das IoT	355
aa) Kein pauschales Zugriffsverbot	356
bb) Aktives Tun/passives Dulden – Keine Übertragung möglich	356
cc) „Tenetur“ – Neu-Evaluierung des Zwangskriteriums	357
(1) Staatlicher Zwang	358
(2) Nichtstaatlicher Zwang (wirtschaftlich, sozial etc.)	359
dd) „se ipsum accusare“ – Ausgleich des Minus des Zwangselements	359
ee) Einklang mit weiteren Aspekten der Ratio	361
(1) Eigenverantwortung zur Reichweitenbestimmung	361
(2) Wissensschutz	362
7. Folgen für die Selbstbelastungsfreiheit im Rahmen von Ermittlungen im und mithilfe des IoT	363
a) Die Einzelfallbetrachtung – „tenetur“ im Zusammenspiel mit „se ipsum accusare“	363
b) Vorzugswürdigkeit dieses graduellen Ansatzes	365

c) Das Abwägungsverbot und der menschenrechtliche Kern der Selbstbelas- tungsfreiheit	366
8. Fazit	367
E. Fazit der strafprozessualen Betrachtungen	368
Schlussbemerkungen	369
Literatur	371
Sachwortverzeichnis	407

Einleitung: Smarte Geräte – Smartes Strafrecht?

Die Welt ist digitalisiert. Vorgänge, die unter dem Topos der *Digitalisierung* stattfinden, sind eine Perpetuierung und Vertiefung einer Ordnung, die in ihrem Kern bereits zu einem Ist-Zustand geworden ist: Das Leben ist digital geworden, viele Abläufe des Alltags sind ohne Internetanbindung nur schwer vorstellbar oder kaum möglich. Selbst in zunächst spärlich in diesen Zustand versetzten Bereichen des Lebens dringt das Digitale immer weiter vor. Damit werden nunmehr auch in Behörden, Gerichten, Schulen und Hochschulen die Umstände und Prozesse an die Bedürfnisse der digitalen Welt angepasst.

Das Recht hingegen ist nicht digitalisiert. Die digitale Progression des Rechts verläuft langsamer. Dies hat nicht nur mit der nötigen Dauer von Gesetzgebungsverfahren und möglicher Scheu vor Veränderung zu tun. Es hängt auch damit zusammen, dass die Veränderungsbedürfnisse des Rechts oftmals erst mit Kenntnis der rechtstatsächlichen Veränderungen und ihren Auswirkungen offenbar, jedenfalls aber erst richtig konturiert, werden können.

Der Grad der Vernetzung des Lebens als Teil der fortschreitenden Digitalisierung hat in den letzten Jahren stetig zugenommen. Dieser Trend setzt sich fort. Fahrzeuge, sog. SmartCars, senden unablässig Daten über Fahrer und Fahrzeug an den Hersteller, der Ofen des sog. SmartHome wird über das Smartphone vorgeheizt, Kinderspielzeug wird zum SmartToy und kann aufgrund einer Internetverbindung mit dem Kind und anderen verbindungs-fähigen Geräten kommunizieren, SmartWatches und smarte Gesundheitsgeräte haben ein Auge auf Gesundheit und Fitness des Trägers, Fabriken bestellen automatisch Bauteile für Fertigungsprozesse und in einer über allen Akteuren schwebenden Wolke – der Cloud – laufen sämtliche Informationen zusammen. Die Herausforderungen, die diese Entwicklung für das Recht im Allgemeinen sowie für das Strafrecht im Besonderen hervorbringt, sind vielseitig. Sie bestehen einerseits auf materieller Ebene, wenn die Gesellschaft sich fragen muss, ob diese Systeme sowie die produzierten und gespeicherten Daten strafrechtlich besonderen Schutz erfahren sollen – eine Diskussion, der v. a. die Frage vorauszugehen hat, wie es um den Schutz im materiellstrafrechtlichen *status quo* bestellt ist. Sie bestehen andererseits aber auch auf prozessualer Ebene. All das ließe sich zu einer pointierten Frage stilisieren: Haben wir für die Herausforderungen im Zusammenhang mit smarten Geräten ein smartes Strafrecht?

Schon vor mehreren Jahren wurden Begehrlichkeiten aus dem Bundesinnenministerium laut, denen zufolge Strafverfolgungsbehörden umfassenden Zugriff auf

Daten aus vernetzten Fahrzeugen gewährt werden soll.¹ Die Anpassung rechtlicher Rahmenbedingungen bedarf jedoch eines intensiven Blickes auf sowohl auf die rechtstatsächlichen Gegebenheiten als auch auf die Rechtslage. Chancen und Risiken müssen abgewogen werden, um beschreiben und bewerten zu können, inwieweit das Recht bereits jetzt universell auf neue rechtstatsächliche Entwicklungen angewendet werden kann. Dies gilt für das materielle Strafrecht einerseits, sowie das Strafprozessrecht andererseits.

Unter der rechtstatsächlichen Klammer des „Internets der Dinge“ oder „Internet of Things“ werden diese Aspekte in der vorliegenden Arbeit untersucht. In einem ersten Kapitel werden die rechtstatsächlichen Grundlagen des Internets der Dinge dargestellt und anhand der Darstellung dreier Anwendungsbereiche der Weg für die rechtliche Diskussion geebnet. Im zweiten Kapitel der Arbeit, wird der materiell-rechtliche Zusammenhang zwischen dem Internet der Dinge und dem Strafrecht beleuchtet, wobei die Systeme und Geräte mitsamt den verarbeiteten Daten des Internets der Dinge in ihrer Eigenschaft als potenzielle Angriffsobjekte von Straftaten sowie die strafrechtlichen Ahndungsmöglichkeiten hierzu im Vordergrund stehen. Im dritten Kapitel steht das Internet der Dinge als Erkenntnisquelle der Ermittlungsbehörden im Fokus. Es wird betrachtet, inwieweit Strafverfolgungsbehörden nach der jetzigen Rechtslage Zugriff auf Daten und Systeme gewährt werden kann. Dies wird zudem in einen Kontext strafprozessualer Grundsätze – Verbot der Totalausforschung, Kernbereich höchstpersönlicher Lebensführung, Selbstbelastungsfreiheit – gestellt.

Im Rahmen der rechtlichen Diskussionen soll nicht nur deutlich gemacht werden, dass eine gesellschaftliche Auseinandersetzung mit diesen Fragen notwendig ist, sondern v. a. aufgezeigt werden, dass die rechtstatsächlichen Änderungen durch die Vernetzung des alltäglichen Lebens Auswirkungen auf die Vorschriften des Strafrechts haben und auch auf deren Lesart haben müssen, um die Grundgedanken der Vorschriften nicht auszuhöhlen und sie den Veränderungen der „echten Welt“ gerecht werdend anzuwenden. Die z. T. bereits in anderen Kontexten geführten rechtlichen Auseinandersetzungen mit bestimmten Auslegungs- und Anwendungsproblemen werden damit einerseits konkreter, öffnen andererseits jedoch auch neue Pforten zur Bewertung von Sachverhalten in einer smarten Welt.

¹ Der Spiegel, „Staatlicher Zugriff auf schlichtweg alles, jedes und jeden“, abrufbar unter: <https://www.spiegel.de/netzwelt/netzpolitik/thomas-de-maiziere-will-umfassenden-zugriff-auf-digitale-sicherungssysteme-a-1181209.html> (zuletzt abgerufen am 28. 12. 2023).

Kapitel 1

Rechtstatsächliche Grundlagen

A. Das Internet der Dinge (IoT)

I. Hinführung

Das Internet der Dinge (IoT, von Englisch: Internet of Things) bezeichnet – diverse Definitionsansätze zusammenfassend – ein Netzwerk verschiedener Gegenstände, die eine eigene IP-Adresse haben, miteinander kommunizieren und deren Kommunikationsprozesse nicht ausschließlich menschlich veranlasst sein müssen.¹ Die Geräte weisen dabei verschiedene Sensoren, Steuerungsfunktionen und ggf. Speicher-, jedenfalls aber Übertragungsmöglichkeiten auf. Auf diese Weise können jegliche Gegenstände und Geräte Umweltinformationen, aus der physischen, aber auch aus der virtuellen Welt, aufnehmen, verarbeiten und weiter übermitteln.² IoT-Systeme zeichnen sich zudem dadurch aus, dass sie nach Set-Up und Aktivierung weitestgehend ohne menschliches Eingreifen oder Mensch-zu-Maschine-Kommunikation auskommen.³ Zur Kommunikation untereinander müssen die Geräte miteinander verbunden sein, entweder direkt oder über einen Hub oder ein Endgerät, bspw. ein Smartphone, wobei die Verbindungen entweder kabelgebunden, meistens jedoch kabellos (bspw. über Bluetooth, WiFi, ZigBee, 5G) erfolgen.⁴ Die massenhafte Erhebung und Verarbeitung von Daten, die durch zum Teil zahlreiche IoT-Geräte in den jeweiligen Systemen stattfindet, verwandelt „konventionelle“ in smarte Infrastruktur.⁵ Auf diese Weise können sodann auch solche Geräte und Maschinen miteinander kommunizieren, deren originäre Aufgabe nicht per se die Kommunikation ist. Der Daten- und Informationsaustausch lässt neue Möglichkeiten der Automatisierung zu und kann in sämtlichen Anwendungsbereichen zu Verbesserungen von Sicherheit, Komfort, wirtschaftlichen Aspekten und Nachhaltigkeit

¹ Vgl. zum Begriff auch *Schmidt/Prufß*, in: Auer-Reinsdorf/Conrad, § 3 Rn. 431 ff.; IERC, Internet of Things, abrufbar unter: http://www.internet-of-things-research.eu/about_iot.htm (zuletzt abgerufen am 28. 12. 2023).

² *Onthoni/Sahoo/Neelakantam*, in: IoT Applications for Healthcare Systems, 33; BSI, Die Lage der IT-Sicherheit in Deutschland 2022, 108, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6 (zuletzt abgerufen am 28. 12. 2023).

³ *Gleißner/Dotzler/Hartig/Aßmuth/Buliitta/Hamm*, in: Cloud Computing 2021, 1 (2).

⁴ *Gleißner/Dotzler/Hartig/Aßmuth/Buliitta/Hamm*, in: Cloud Computing 2021, 1 (2).

⁵ *Onthoni/Sahoo/Neelakantam*, in: IoT Applications for Healthcare Systems, 33.