

Kölner Kriminalwissenschaftliche Schriften

---

Band 81

# Schutz virtualisierter räumlicher Privatsphäre

## Grenzen zulässiger Strafverfolgung im Smart Home

Von

Christine Untch



Duncker & Humblot · Berlin

CHRISTINE UNTCH

## Schutz virtualisierter räumlicher Privatsphäre

Kölner Kriminalwissenschaftliche Schriften

Herausgegeben von

Claus Kreß, Cornelius Nestler

Frank Neubacher, Anja Schiemann, Frauke Rostalski

Martin Waßmer, Thomas Weigend, Bettina Weißen

Professoren an der Universität zu Köln

Band 81

# Schutz virtualisierter räumlicher Privatsphäre

Grenzen zulässiger Strafverfolgung  
im Smart Home

Von

Christine Untch



Duncker & Humblot · Berlin

Die Rechtswissenschaftliche Fakultät der Universität zu Köln  
hat diese Arbeit im Jahr 2024 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  
© 2025 Duncker & Humblot GmbH, Berlin  
Satz: 3w+p GmbH, Rimpau  
Druck: CPI books GmbH, Leck  
Printed in Germany

ISSN 0936-2711  
ISBN 978-3-428-19488-9 (Print)  
ISBN 978-3-428-59488-7 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier  
entsprechend ISO 9706 ☺

Verlagsanschrift: Duncker & Humblot GmbH, Carl-Heinrich-Becker-Weg 9,  
12165 Berlin, Germany | E-Mail: [info@duncker-humblot.de](mailto:info@duncker-humblot.de)  
Internet: <https://www.duncker-humblot.de>

*Meinen Eltern*



## **Vorwort**

Die vorliegende Arbeit wurde von der Rechtswissenschaftlichen Fakultät der Universität zu Köln im Sommersemester 2024 als Dissertation angenommen. Literatur wurde bis April 2024, Kommentarliteratur bis August 2024 berücksichtigt.

An erster Stelle danke ich ganz herzlich meiner akademischen Lehrerin und Doktormutter Frau Prof. Dr. Bettina Weißen nicht nur für die hervorragende Betreuung und die wertvollen Diskussionen und Anregungen im Zusammenhang mit dieser Arbeit, sondern auch für die darüber hinausgehende Unterstützung und Förderung. Frau Prof. Dr. Schiemann danke ich ganz herzlich für die zügige Erstellung des Zweitgutachtens.

Ihnen beiden und den anderen Herausgebern der „Kölner Kriminalwissenschaftliche Schriften“ danke ich für die Aufnahme meiner Dissertation in die Schriftenreihe.

Für die großzügige Förderung während der Promotionszeit danke ich sehr herzlich der Studienstiftung des deutschen Volkes. Dem Verein zur Förderung der Kriminalwissenschaften an der Universität zu Köln danke ich vielmals für die Gewährung eines großzügigen Druckkostenzuschusses.

Zudem danke ich der Zentral- und Ansprechstelle Cybercrime NRW, allen voran Herrn Leitenden Oberstaatsanwalt Markus Hartmann und Herrn Oberstaatsanwalt Andreas Brück, für den wertvollen Austausch, zahlreiche Anregungen und die Ermöglichung, einen Teil der höchstinteressanten Gespräche in dieser Arbeit veröffentlichen zu dürfen.

Dem Team des Instituts für ausländisches und internationales Strafrecht danke ich sehr – sowohl für zahlreiche lebhafte Diskussionen und Anregungen als auch für die sehr schöne gemeinsame Zeit, die mir immer in Erinnerung bleiben wird. Besonders hervorheben möchte ich in diesem Zusammenhang Jan Osten, der die Arbeit Korrektur gelesen hat, sowie Kirsten Kindler, Dr. Johannes Block, Jonathan Macziola, Max Wrobel, Alexander Oliveri, Elena Himmelmann und Yara Bröcker.

Mein tiefer Dank gilt zudem meinen Freunden Dr. Dennis Jennessen, Dr. Lava Gaff, Ebru Aydogan sowie Lisa und Olav Böseke für das Korrekturlesen, die vielen hilfreichen Gespräche und nicht zuletzt dafür, dass ihr immer für mich da seid.

David danke ich von ganzem Herzen für den tagtäglichen Beistand, die bedingungslose Unterstützung und Fürsorge, deine bemerkenswerte Geduld mit mir sowie den unendlichen Rückhalt.

Vom ganzen Herzen möchte ich schließlich auch meiner Familie, insbesondere meinen Eltern Nicole und Ortwin Untch, danken. Für eure uneingeschränkte Unterstützung und den felsenfesten Rückhalt werde ich euch auf Ewig dankbar sein. Euch ist diese Arbeit gewidmet.

Köln, im Januar 2025

*Christine Untch*

# **Inhaltsverzeichnis**

<i>1. Teil</i>	
<b>Einleitung</b>	23
A. Erkenntnisziel .....	25
B. Gang der Untersuchung .....	27
<i>2. Teil</i>	
<b>Strafverfolgungsbehördliche Zugriffe auf das Smart Home</b>	30
A. Das Phänomen des Smart Home .....	30
I. Begriff und Ausprägungen des Smart Home .....	31
1. Begriff des Smart Home .....	31
2. Ausprägungen von Smart Home-Systemen .....	34
II. Wesentliche Funktionsweise von Smart Home-Systemen .....	36
1. Smart Home-Komponenten .....	37
a) Smart Home-Zentrale .....	37
b) Sensorik und Aktorik .....	38
c) Eingabegeräte und digitale Sprachassistenten .....	39
2. Realisierung der Vernetzung und Kontextantizipation .....	42
a) Umfassende Vernetzung .....	42
aa) Lokale Vernetzung innerhalb des Smart Home-Systems .....	43
bb) Vernetzung mit Stellen des Internets .....	44
b) Kontextualisierung .....	45
3. (Verschlüsselte) Kommunikation auf mehreren zeitlichen und funktionalen Ebenen .....	47
a) Zeitliche Anknüpfungspunkte: Daten in der Phase der Datenübertragung .....	48
aa) TCP/IP-Referenzmodell .....	50
bb) Beginn und Ende der Datenübertragung beim Smart Home-Nutzer .....	51
cc) Akteure im Smart Home .....	52
(1) Netzbetreiber und Internetzugangsanbieter (Network Provider und Internet Access Provider) .....	53
(2) Anbieter von Ressourcen und Anwendungen (Host Provider) .....	54
(3) Inhalteanbieter (Content Provider) .....	54

(4) Nutzer .....	54
(5) Zusammenfassung .....	55
dd) Beginn und Ende der Datenübertragung beim Provider .....	55
b) Zeitliche Anknüpfungspunkte: Daten in der Phase der Datenspeicherung .....	56
aa) Datenübertragung innerhalb des Smart Home-Systems als Datenspeicherungsphase? .....	56
bb) Datenspeicherung bei beteiligten Providern .....	57
c) Funktionelle Anknüpfungspunkte: Von Mensch-Mensch- zu Mensch-Maschine- bis hin zu Maschine-Maschine-Kommunikation .....	58
aa) Technisch vermittelte Mensch-Mensch-Kommunikation .....	58
bb) Mensch-Maschine-Kommunikation .....	59
cc) Maschine-Maschine-Kommunikation .....	61
(1) Systemkonfiguration .....	62
(2) Lernende Systeme .....	62
dd) Fehlende Trennschärfe .....	64
d) Fernsteuerung .....	66
e) Verschlüsselung .....	67
III. Zwischenergebnis .....	69
B. Faktische und IT-forensische Zugriffsmöglichkeiten auf das Smart Home .....	70
I. Zugriffsobjekt Smart Home .....	70
1. Erlangung der Kenntnis von der Existenz eines Smart Home-Systems .....	72
2. Einzelfallbezogener Zugriff mangels verbreiteter Standards .....	72
3. Smart Home-Systeme als vernetzte Systeme .....	74
4. Mehrere Zugriffspunkte und -arten durch Einbindung unterschiedlicher Diensteanbieter .....	74
5. Andere Datenqualität und -quantität: (Re-)Konstruktion des physischen Wohnraumgeschehens .....	76
6. Ergebnis: Berücksichtigung bei Smart Home-Zugriffen .....	77
II. IT-Forensische Grundlagen für Zugriffe auf informationstechnische Systeme .....	78
1. Vorbereitung: Suche, Identifikation und Zugriffsplan .....	80
2. Sicherung .....	81
a) Post-Mortem-Sicherung .....	82
aa) Vorteile der Post-Mortem-Sicherung .....	84
bb) Hürden bei der Post-Mortem-Sicherung .....	84
cc) Bedeutung der Post-Mortem-Analyse für Smart Home-Zugriffe .....	86
b) Live-Sicherung .....	86
aa) Nutzung systemeigener Programme und Funktionen .....	87
bb) Einsatz von Software der Ermittler .....	88

cc) Online-Durchsuchung .....	88
(1) Infiltrationsmöglichkeiten .....	89
(a) Ausnutzen von Sicherheitslücken .....	90
(b) Einschleusen von Sicherheitslücken durch die Mitwirkung des Systemnutzers .....	91
(c) Physische Infiltration .....	92
(2) Spähsoftware .....	93
(3) Online-Durchsicht und Online-Überwachung .....	94
(4) De-Infiltration des Systems .....	95
(5) Quellen-Telekommunikationsüberwachung .....	95
(6) Sonderfall: Erstellen von Snapshots .....	97
dd) Vorteile der Live-Sicherung .....	98
ee) Hürden bei der Live-Sicherung .....	98
ff) Bedeutung der Live-Sicherung für Smart Home-Zugriffe .....	99
c) Zwischenergebnis .....	100
3. Entschlüsselungsmöglichkeiten .....	100
4. Analyse und Präsentation .....	102
III. Zwischenergebnis: Faktische Zugriffsmöglichkeiten auf das Smart Home .....	103
1. Zugriffe auf Daten in der Übertragungsphase .....	103
2. Zugriffe auf gespeicherte Daten .....	104
3. Zugriffe auf das physische Geschehen in der Wohnung .....	104

*3. Teil*

<b>Grundrechtseingriffe durch Datenzugriffe auf das Smart Home</b>	105
A. Zugriffe auf das Smart Home als Eingriffe in das Wohnungsgrundrecht nach Art. 13 Abs. 1 GG .....	106
I. Schutzzweck des Art. 13 Abs. 1 GG .....	107
II. Schutz der „Wohnung“ .....	107
III. Schutz vor Zugriffen auf informationstechnische Systeme wie das Smart Home? .....	108
1. Durchsuchung, lokale Datenzugriffe und der klassische Lauschangriff .....	109
2. Fernzugriff auf das Smart Home als Eingriff in Art. 13 Abs. 1 GG? .....	111
a) Keine Vergleichbarkeit zu von außen ohne technische Hilfsmittel hörbare Vorgänge in der Wohnung .....	111
b) Systemstandort als untaugliches Kriterium .....	113
c) Vergleichbare Erwartung der Vertraulichkeit informationstechnischer Systeme auch außerhalb der Wohnung .....	116
d) Keine Schutzlosigkeit außerhalb der Wohnung befindlicher informationstechnischer Systeme .....	118

e) Kein umfassender Schutz virtualisierter Privatsphäre durch räumliche Privatsphäre .....	120
f) Ausnahme: Sensorische Wohnraumüberwachung mittels des Smart Home-Systems .....	123
aa) Zugriffe auf das virtuelle Abbild des vergangenen physischen Wohngeschehens .....	124
bb) Zugriffe auf das virtuelle Abbild des aktuellen physischen Wohngeschehens .....	126
cc) Zwischenergebnis .....	127
dd) Wertungswiderspruch im Hinblick auf Smart Home-Datenzugriffe .....	127
3. Zielrichtung des Smart Home-Zugriffs für Schutz durch das Wohnungsgrundrecht entscheidend .....	128
a) Offener Zugriff auf Smart Home-Systeme und -Daten (in der Übertragungs- und Speicherphase) .....	129
b) Fernzugriff auf Smart Home-Systeme (in der Wohnung) .....	129
aa) Ausnahme: physische Infiltration .....	130
bb) Ausnahme: Überwachung des physischen Wohnraumgeschehens mittels des Smart Home-Systems .....	130
B. Schutz vor Smart Home-Zugriffen durch das Fernmeldegeheimnis, Art. 10 Abs. 1 Var. 3 GG .....	131
I. Schutzzweck des Art. 10 Abs. 1 Var. 3 GG .....	132
II. Umfassender Schutz individueller Telekommunikation .....	133
1. Kein Personenbezug erforderlich .....	135
2. Schutzwürdiges Vertrauen in die Begrenzung des Empfängerkreises? .....	137
a) Abgrenzungsschwierigkeiten durch Kommunikationsdienste des Internets .....	138
b) Abgrenzungsvorschläge in der Literatur .....	139
c) Kritik .....	140
d) Interesse an und Vertrauen in die Begrenzung des Teilnehmerkreises entscheidend .....	141
III. Kommunikationsebenen des Smart Home als Telekommunikation im Sinne des Art. 10 Abs. 1 Var. 3 GG? .....	141
1. Begrifflichkeiten: Mensch-Mensch-, Mensch-Maschine- und Maschine-Maschine-Kommunikation .....	142
a) Mensch-Maschine-Kommunikation .....	143
aa) Funktionale Abgrenzung zur Mensch-Mensch-Kommunikation .....	143
bb) Smart Home- und Cloud-Diensteanbieter als Kommunikationsmittler, nicht menschlicher Kommunikationspartner .....	145
b) Abgrenzung Mensch-Maschine- und Maschine-Maschine-Kommunikation .....	146
c) Zwischenergebnis .....	147
2. Telekommunikationsbegriff: Zwischenmenschliche Kommunikation als zwingende Voraussetzung? .....	147
a) Keine klare Konturierung durch das Bundesverfassungsgericht .....	147

b) Zwischenmenschliche Kommunikation als zwingende Voraussetzung . . . . .	151
c) Mangelnde Trennschärfe in technischer und rechtlicher Hinsicht . . . . .	152
d) Zweifelslösung . . . . .	154
e) Zwischenmenschliche Kommunikation keine zwingende Voraussetzung . . . . .	154
aa) Kommunikationswandel . . . . .	155
bb) Entwicklungsoffenheit . . . . .	155
cc) Kein entgegenstehender Wortlaut . . . . .	156
dd) Keine entgegenstehende Systematik . . . . .	156
ee) Funktionale Vergleichbarkeit mit zwischenmenschlicher Kommunikation . . . . .	157
ff) Kongruentes Telos . . . . .	158
gg) Zwischenergebnis . . . . .	160
3. Maschine-Maschine-Kommunikation als Telekommunikation? . . . . .	160
a) Kein Schutz menschlich nicht veranlasster Kommunikation . . . . .	161
b) Schutz auch der Maschine-Maschine-Kommunikation . . . . .	161
c) Zwischenergebnis . . . . .	164
IV. „Laufende“ Telekommunikation im Smart Home? . . . . .	165
1. Laufende Telekommunikation im Sinne des Art. 10 Abs. 1 Var. 3 GG . . . . .	166
2. Abgrenzung nach Herrschaftsbereichen . . . . .	166
3. Alleiniger Herrschaftsbereich im Smart Home? . . . . .	167
a) Daten auf Endgeräten . . . . .	167
b) Lokale Datenübertragungen im Smart Home . . . . .	168
c) Externe Smart Home-Datenübertragung und providerseitig gespeicherte Daten . . . . .	170
d) Sonderfall: Zugriff mittels Quellen-Telekommunikationsüberwachung . . . . .	171
4. Ergebnis . . . . .	175
C. Ausprägungen des Allgemeinen Persönlichkeitsrechts, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG . . . . .	176
I. Schutz vor Smart Home-Zugriffen durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) . . . . .	176
1. Smart Home als eigenes informationstechnisches System im Sinne des IT-Grundrechts . . . . .	177
a) Informationstechnische Systeme im Sinne des IT-Grundrechts . . . . .	177
b) Nutzung als eigenes System . . . . .	180
aa) Eigennutzung fremdbeherrschter informationstechnischer Systeme? . . . . .	181
bb) Einheitliches informationstechnisches System? . . . . .	182
cc) Ergebnis . . . . .	184
2. Vertraulichkeits- und Integritätsschutz . . . . .	184
a) Schutz der Vertraulichkeit . . . . .	185
b) Schutz der Integrität . . . . .	185
3. Ergebnis: Eingriffe in das IT-Grundrecht durch Datenzugriffe im Smart Home	187

II. Eingriffe in das Recht auf informationelle Selbstbestimmung .....	187
D. Verhältnis betroffener Grundrechte .....	189
I. Verhältnis von Art. 10 Abs. 1 Var. 3 GG zum Allgemeinen Persönlichkeitsrecht	189
II. Verhältnis des IT-Grundrechts zum Recht auf informationelle Selbstbestimmung	191
E. Ergebnis .....	193
I. Grundrechtseingriffe bei Zugriffen auf Daten in der Übertragungsphase .....	193
II. Grundrechtseingriffe bei Zugriffen auf gespeicherte Daten .....	194
III. Grundrechtseingriffe bei Zugriffen auf das physische Wohngeschehen .....	194
IV. Konsequenzen für die weitere Untersuchung .....	195

#### *4. Teil*

##### **Strafprozessuale Ermächtigungsgrundlagen für Smart Home-Zugriffe**      197

A. Anforderungen an die Verfassungsmäßigkeit von strafprozessualen Eingriffsbefugnissen .....	198
I. Gemeinsame Anforderungen .....	199
1. Gebot der Normenklarheit und -bestimmtheit .....	199
2. Schutz des Kernbereichs privater Lebensgestaltung .....	201
3. Verbot der Rundumüberwachung und von Persönlichkeitsprofilen .....	202
4. Grundsatz der Verhältnismäßigkeit .....	202
II. Grundrechtsspezifische Anforderungen .....	204
1. Rechtfertigungsanforderungen des Art. 13 GG .....	204
a) Anforderungen an Durchsuchungen nach Art. 13 Abs. 2 GG .....	205
b) Anforderungen an die Rechtfertigung von Wohnraumüberwachungen, Art. 13 Abs. 3 GG .....	206
aa) Unzulässigkeit sensorischer, nicht bloß akustischer Wohnraumüberwachungen .....	206
bb) Zulässigkeit akustischer Wohnraumüberwachungen nach Art. 13 Abs. 3 GG .....	206
2. Rechtfertigungsanforderungen an Eingriffe in Art. 10 Abs. 1 Var. 3 GG .....	208
3. Anforderungen an Ermächtigungsgrundlagen zur Einschränkung des IT-Grundrechts .....	208
B. Zulässigkeit von sensorischen Wohnraumüberwachungen mittels des Smart Home-Systems? .....	209
I. Legitimation durch § 100c StPO? .....	210
1. Wohnung im Sinne des § 100c StPO .....	210
2. Nichtöffentliche gesprochenes Wort von in der Wohnung befindlichen Personen	210
3. Technische Mittel im Sinne des § 100c StPO .....	211
a) Smart Home-Sensoren als technische Mittel im Sinne des § 100c StPO? ..	211
aa) Kein entgegenstehender Wortlaut .....	212

bb) Unklarer Gesetzgeberwille .....	213
cc) Systematische Erwägungen .....	216
(1) Vergleich zur Begriffsverwendung in §§ 100a Abs. 1 S. 2, 100b Abs. 1 StPO .....	217
(2) Vergleich zur Begriffsverwendung in § 100i Abs. 1 StPO .....	219
(3) Vergleich zu § 100f StPO .....	221
(4) Entgegenstehende Systematik .....	222
dd) Eigenständiger Eingriff in das IT-Grundrecht .....	222
(1) Keine vergleichbaren Eingriffswirkungen für den Betroffenen .....	222
(2) Eigenständige Bedeutung der Integritätsverletzung .....	223
(3) Keine vergleichbare Eingriffsintensität bei heimlichem Betreten der Wohnung .....	226
(4) Vergleichbare Eingriffsintensität wie bei der Online-Durchsuchung .....	227
(5) Keine Subsidiarität des IT-Grundrechts .....	227
(6) Kein anderes Ergebnis beim Abhören über einen einzelnen Smart Speaker .....	228
b) De lege lata keine akustische Wohnraumüberwachung durch ermittlerseitige Umfunktionierung von nutzereigenen Sensoren über § 100c StPO .....	229
II. § 100b StPO als hinreichende Eingriffsermächtigung für sensorische Wohnraum- überwachungen mittels des Smart Home-Systems? .....	229
1. Datenerhebung „daraus“ nicht <i>mittels</i> .....	230
2. Durchsuchung vs. Überwachung .....	231
3. § 100c StPO als abschließende Sonderregelung? .....	232
4. Keine Berücksichtigung der Vorgaben des Art. 13 Abs. 3 GG .....	233
5. Mangelnde technische Unterscheidbarkeit zulässiger und unzulässiger Daten- kreationen .....	234
6. Der Begriff der technischen Mittel in §§ 100b und 100c StPO: Unterschiedliche Zielrichtung der Maßnahmen .....	235
7. Keine Generalermächtigung unzulässiger Rundumüberwachung .....	237
8. Entwurf eines Gesetzes zur Begrenzung der Eingriffsbefugnisse im Rahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung .....	239
9. Auch keine Wohnraumüberwachung durch den Einsatz kriminalistischer List .....	240
III. Kombination von § 100c und § 100b StPO? .....	240
IV. Ergebnis .....	243
C. Zugriffe auf das Smart Home-System .....	243
I. Zugriffe auf Smart Home-Kommunikation nach § 100a StPO .....	244
1. Smart Home-Daten als Telekommunikation im Sinne des § 100a Abs. 1 StPO? .....	245
a) Bestimmung der richtigen Auslegungshoheit .....	246
aa) Weiter technischer Telekommunikationsbegriff .....	246
(1) Formal-technischer Telekommunikationsbegriff .....	247
(2) Kommunikationsbezogene technikorientierte Auslegung .....	247

bb) Grundrechtsanaloger Telekommunikationsbegriff .....	249
cc) Strafprozessualer Telekommunikationsbegriff .....	249
dd) Stellungnahme .....	250
(1) Bewertung der technischen Auslegungen .....	251
(2) Bewertung der grundrechtsanalogen Auslegung .....	254
ee) Zwischenergebnis: genuin strafprozessuale Auslegung erforderlich ..	256
b) Strafprozessualer Telekommunikationsbegriff .....	257
aa) Wortlaut .....	257
bb) Gesetzeshistorie und Zweck der Telekommunikationsüberwachung nach § 100a StPO .....	259
cc) Systematische Erwägungen .....	261
dd) Keine entgegenstehende verfassunggerichtliche Rechtsprechung ..	263
(1) Beschluss des Bundesverfassungsgerichts zur Überwachung der In- ternetnutzung nach § 100a StPO .....	263
(2) Bewertung .....	265
ee) Teleologische Erwägungen: Wesensverschiedenheit selbstbezogener Internetkommunikation .....	268
(1) Wesensverschiedener Maßnahmencharakter .....	269
(2) Selbstbezogenheit und Kernbereichsnähe der einseitigen Internet- nutzung .....	270
(a) Virtuelle Manifestation und Aufbewahrung im Netz als Kernbe- reichshindernis? .....	272
(b) Quantität bedingt Qualität .....	274
(c) Zwischenergebnis .....	276
(3) Eingriffsintensität vergleichbar der Online-Durchsuchung .....	277
(4) Zwischenergebnis .....	278
ff) Keine Änderung des Maßnahmencharakters durch technikoffene Aus- legung .....	279
gg) Ergebnis .....	279
2. Zugriff auf providerseitig gespeicherte Daten nach § 100a StPO? .....	280
3. Ergebnis .....	281
II. Heimliche Zugriffe nach § 100b StPO .....	282
1. Vom Betroffenen genutztes informationstechnisches System .....	282
a) Informationstechnisches System im Sinne des § 100b StPO .....	282
aa) Verfassungsrechtlicher Begriff .....	283
bb) Technischer Begriff .....	283
cc) Strafprozessualer Begriff .....	283
dd) Zwischenergebnis .....	285
b) Keine Nutzung als eigenes erforderlich .....	285
c) Kein einheitliches informationstechnisches System im Falle vernetzter Sys- teme .....	286

d) Zwischenergebnis .....	287
2. Eingriff mit technischen Mitteln .....	287
a) Keine Beschränkung auf „Online“-Zugriffe .....	287
b) Technische Mittel .....	288
aa) Infiltration des informationstechnischen Systems als zulässiger Begleiteingriff? .....	289
(1) Physische Infiltration .....	290
(a) Heimliches Betreten der Wohnung als unzulässiger Begleiteingriff .....	290
(aa) Entgegenstehender Wille des Gesetzgebers .....	291
(bb) Kein notwendiger oder typischer Begleiteingriff .....	292
(cc) Eigenständiger Eingriff in Art. 13 Abs. 1 GG .....	292
(b) Keine Legitimation im Wege anderer Eingriffsbefugnisse .....	294
(c) Unzulässigkeit der physischen Infiltration unter Eindringen in die räumliche Privatsphäre .....	294
(2) Unbewusste Mitwirkung des Nutzers durch den Einsatz kriminalistischer List .....	295
(a) (Un-)Zulässigkeit kriminalistischer List .....	295
(b) Grenzen des Einsatzes kriminalistischer List zur Infiltration informationstechnischer Systeme .....	300
(c) Ergebnis: Grundsätzliche Zulässigkeit täuschungsbedingter Infiltration .....	301
(3) Offthalten und Ausnutzen von (unbekannten) Sicherheitslücken .....	302
(a) Unzulässige Gefahr für die IT-Sicherheit in ihrer Gesamtheit ..	303
(b) Unzuständigkeit der Strafverfolgungsbehörden? .....	303
(c) Gefahrenabwehrrechtliche Abwägungslösung des Bundesverfassungsgerichts .....	304
(d) Unzuständigkeiterklärung nicht sachgemäß .....	305
(e) Übertragbarkeit gefahrenabwehrrechtlicher verfassungsgerichtlicher Rechtsprechung auf das Strafprozessrecht .....	306
(f) Zulässigkeit abhängig von simultaner Meldung .....	309
(4) Zwischenergebnis .....	309
bb) Unzureichende Regelung zugelassener Spähsoftware .....	310
(1) Kommerzielle Hacking-Tools als zulässige Alternative? .....	311
(2) Intransparenz und mangelnde Integrität von Spähsoftware .....	315
(3) Manipulationsanfälligkeit und Beweiswert .....	316
c) Zwischenergebnis .....	317
3. Zulässiger Umfang von nach § 100b StPO erfassten Smart Home-Zugriffen .....	318
a) Grundsätzliche Reichweite der Datenerhebung nach § 100b StPO .....	319

b) (Kein) Schutz virtualisierter räumlicher Privatsphäre? .....	320
aa) Virtuelle sensorische Wohnraumüberwachung: Legitimation von Zugriffen auf vom Nutzer initiierte Sensordaten des Smart Home? .....	321
(1) Wertungswiderspruch: Das informationstechnische Ende der räumlichen Privatsphäre? .....	321
(2) Keine geringere Schutzwürdigkeit des Smart Home-Nutzers durch freiwillige Aufgabe der räumlichen Privatsphäre .....	323
(3) (Enge) Reichweite des Schutzes virtualisierter räumlicher Privatsphäre .....	325
bb) Teleologische Reduktion auf akustische Sensorüberwachungen in Echtzeit .....	326
cc) Beschränkung der Sensordaten-basierten Rekonstruktion des vergangenen physischen Wohngeschehens auf akustische Wahrnehmungen .....	327
c) Zwischenergebnis: keine virtuelle Wohnraum-Komplettüberwachung durch die Hintertür der Online-Durchsuchung .....	327
4. Verfassungsmäßigkeit des § 100b StPO mit Blick auf Smart Home-Zugriffe .....	328
a) Unzureichender Schutz virtualisierter räumlicher Privatsphäre .....	328
b) Unzureichende Subsidiaritätsklausel: Gesetzgeberische Verkenntnung der Eingriffsintensität des § 100b StPO? .....	331
aa) Weitreichendere Einblicke in die Persönlichkeit durch Online-Durchsuchungen .....	331
bb) Kein pauschal geringeres Schutzbedürfnis des privaten virtuellen Raums .....	333
cc) § 100b StPO als Generalermächtigung zur Rundumüberwachung des virtuellen Raums? .....	334
dd) Bestätigender Referentenentwurf .....	335
c) Inkonsistenter Straftatenkatalog .....	336
aa) Übertragbarkeit verfassungsgerichtlicher Vorgaben zur Gefahrenabwehr .....	336
bb) Keine Beschränkung auf überragend wichtige Rechtgüter schützende Straftaten .....	338
cc) Keine verfassungskonforme Auslegung nach dem jeweiligen informationstechnischen System .....	340
d) Unzureichender Kernbereichsschutz .....	341
aa) Verfassungsrechtliche Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung .....	341
(1) Inhalt und Bedeutung .....	341
(2) Unumgängliche Unschärfe des Kernbereichs und Risiken pauschaler Kriterien .....	345
(3) Schutzkonzept des Bundesverfassungsgerichts .....	347
(4) Kritik am verfassungsgerichtlichen Kernbereichsschutzkonzept ..	349

bb) Unzureichende Umsetzung der verfassungsrechtlichen Anforderungen in § 100d StPO .....	351
(1) Einfachgesetzlicher Schutz in der Erhebungsphase: sachwidrige Schlechterstellung des Kernbereichsschutzes bei der Online-Überwachung .....	352
(2) § 100d Abs. 2 StPO: unzureichender Kernbereichsschutz auf Auswertungsebene .....	356
cc) Zwischenergebnis .....	357
5. Ergebnis .....	358
III. Erhebung von Smart Home-Daten nach §§ 94 ff. StPO? .....	359
1. Vorgelagerte Durchsuchung und Durchsicht .....	360
a) Gesetzgeberisch geschwächte Funktion der Durchsicht nach § 110 StPO ..	361
b) Datenträger und Daten als Gegenstand der Durchsicht .....	362
aa) Zulässigkeit der Anfertigung und Mitnahme von Datenkopien und informationstechnischen System-(bestandteil-)en .....	363
(1) Zulässigkeit der Anfertigung von Datenkopien .....	364
(2) (Un-)Zulässigkeit der Mitnahme von informationstechnischen System-(bestandteil-)en .....	369
(3) Geheimnischarakter der Datendurchsicht .....	372
(a) Anwesenheitsrecht bei der Durchsicht .....	373
(b) Zulässige private Datendurchsicht? .....	374
(aa) Outsourcing durch Sachverständigenbestellung? .....	375
(bb) Kooperation mit Privaten .....	377
(c) Gebotene gesetzliche Ausformung des Anwesenheitsrechts bei Datendurchsichten .....	378
bb) Durchsicht externer Speichermedien nach § 110 Abs. 3 S. 2 StPO: Grenzenlose Durchsicht? .....	379
(1) Erhöhte Eingriffsintensität .....	379
(2) (Kein) Zugriff auf Auslandsdaten nach § 110 Abs. 3 S. 2 StPO ..	380
(a) Begrenzte Reichweite nationaler Strafverfolgungskompetenzen ..	380
(b) Ausnahmen der Cybercrime Convention .....	381
(c) Verstoß auch bei Zugriff auf nur potenziell im Ausland befindliche Daten .....	382
(d) Grundsätzlich kein Beweisverwertungsverbot .....	384
(e) (Keine) Anwendbarkeit der E-Evidence-Verordnung .....	385
(f) Zwischenergebnis .....	387
c) Zwischenergebnis: Eigenständige Ermächtigungsgrundlage für die Durchsicht .....	387
2. Sachlicher Anwendungsbereich der §§ 94 ff. StPO: Daten(-träger) als Gegenstände? .....	388
a) Keine unmittelbare Erfassung unkörperlicher „Gegenstände“ .....	389

b) Mittelbare Beschlagnahmefähigkeit von Daten im Wege zulässiger Minusmaßnahmen .....	390
c) Bedeutung der Diskussion um den Gegenstandsbegriff .....	391
3. Verfassungswidrigkeit der §§ 94 ff. StPO hinsichtlich Datenzugriffen .....	392
a) Intensive Eingriffe in das IT-Grundrecht und Art. 10 Abs. 1 Var. 3 GG .....	392
aa) Grundrechtliche Einordnung der Datenzugriffe .....	392
bb) Erfordernis vergleichbarer Eingriffsschwellen .....	393
b) Keine Intensitätssenkung des Eingriffs durch vermeintlich offenen und punktuellen Zugriff .....	394
aa) Geringere Eingriffsschwellen durch Offenheit? .....	394
bb) Geringere Eingriffsschwellen für einmalige und punktuelle Zugriffe? .....	395
c) Keine normenklare Regelung durch generalklauselartige Ausgestaltung .....	397
4. Unzureichende Anpassung der §§ 94 ff., 110 StPO an die digitale Realität .....	399
D. Eckpfeiler einer Reform der Datenzugriffsermächtigungen .....	401
I. Strikte Trennung von „analogen“ und datenbezogenen Ermächtigungsgrundlagen .....	401
1. Unterschiede auf Erhebungsebene .....	402
2. Unterschiede auf Auswertungsebene .....	403
3. Notwendigkeit originär datenbezogener Ermächtigungsgrundlagen .....	403
II. Differenzierung nach zu erwartender Datenqualität .....	404
1. Scheinbar offene Maßnahmen .....	404
2. Gleichsetzung von einmaligen Datenzugriffen und Überwachungen .....	406
III. Konkrete Zugriffsbefugnisse statt Generalermächtigungen .....	407
1. System ausdifferenzierter Datenzugriffsermächtigungen .....	407
2. Sonderfall Online-Durchsuchung .....	408
IV. Gesetzlich angeleitete Verhältnismäßigkeitsprüfung .....	410
V. Schutz virtualisierter räumlicher Privatsphäre .....	411
1. Beweisverwertungsverbote für Zugriffe auf Sensordaten .....	411
2. Übertragung des Kernbereichsschutzes der räumlichen Privatsphäre .....	412
3. Unabhängige Stelle und mehr Kernbereichsschutz im Strafverfahren? .....	412
VI. Schluss .....	412
<i>5. Teil</i>	
<b>Zusammenfassung</b>	414
<b>Literaturverzeichnis</b> .....	422

<b>Anlage</b> .....	455
---------------------	-----

<b>Sachwortverzeichnis</b> .....	467
----------------------------------	-----



## *I. Teil*

### **Einleitung**

„Tod im Whirlpool: Alexa, wer ist der Mörder?“<sup>1</sup>, „Das Internet der Dinge vor Gericht“<sup>2</sup>, „Smarthouse wird für Straftäter zum Problem“<sup>3</sup>. Die Smart Home-Technologie scheint nicht nur die Aufmerksamkeit der Besitzer eigener vier Wände, sondern auch der Ermittler erregt zu haben. Durch Verlautbarungen wie „Innenminister wollen Zugriff auf Daten aus dem ‚Smart Home‘“<sup>4</sup> wird deutlich, dass das Interesse an Smart Home-Daten selbst in Regierungskreisen besteht. Doch woran liegt das? Ist das Smart Home tatsächlich eine so gute Beweisquelle oder sind solche Aufschreie nur viel Lärm um nichts – denn „welcher Verbrecher bestellt bei Alexa schon Sprengstoff?“<sup>5</sup>

Ganz so unwahrscheinlich scheint Letzteres indes nicht, wenn auch Google-Suchen nach Mordanleitungen und Entsorgungsmöglichkeiten für Leichen Realität sind.<sup>6</sup> Ob Smart Home-Daten für Ermittler interessant sind, hängt jedoch ohnehin nicht von Einzelfragen ab. Es ist eine logische Konsequenz des Einzugs der Informations- und Kommunikationstechnologie in den (auch häuslichen) Lebensalltag, dass Informationen über auch strafrechtlich relevante Verhaltensweisen in der digitalen Sphäre zu finden sind.

---

<sup>1</sup> *Stern*, v. 05.03.2017, abrufbar unter <https://tinyurl.com/pt585t9u> (zuletzt abgerufen am 26.04.2024).

<sup>2</sup> *Kühl*, Zeit Online, v. 09.05.2017, abrufbar unter <https://tinyurl.com/yn6sbm6f> (zuletzt abgerufen am 26.04.2024).

<sup>3</sup> *Klohn*, welt, v. 15.08.2018, abrufbar unter <https://tinyurl.com/5x5hjp53> (zuletzt abgerufen am 26.04.2024).

<sup>4</sup> *Rudl*, netzpolitik.org, v. 05.06.2019, abrufbar unter <https://tinyurl.com/2wpfas32> (zuletzt abgerufen am 26.04.2024).

<sup>5</sup> So ein Kommentar von *Tricarico* in der *taz*, Alexa, du Verräterin, v. 06.06.2019, abrufbar unter <https://tinyurl.com/266hep5h> (zuletzt abgerufen am 26.04.2024).

<sup>6</sup> S. hierzu nur *Orbach*, Deutschlandfunk Nova, Kriminelle aufspüren anhand ihrer Google-Suche, v. 21.05.2021, abrufbar unter <https://tinyurl.com/yrj96r8x>; *Al-Khanak*, Gießener Allgemeine, Prozess im Mordfall Ayleen: Angeklagter googelte „Wasserleiche“, v. 20.06.2023, abrufbar unter <https://tinyurl.com/bd63h3re>; s. auch *Levenson*, CNN, These are the Google searches Brian Walshe made before and after killing his wife Ana Walshe, according to prosecutors, v. 18.01.2023, abrufbar unter <https://tinyurl.com/2yep7yjz> (jeweils zuletzt abgerufen am 26.04.2024), wonach der Verdächtige Suchanfragen wie „10 ways to dispose of a dead body if you really need to“ schaltete.

Smart Home-Daten dürften für Ermittler besonders interessant sein.<sup>7</sup> Zum einen war der räumliche Bereich der Wohnung bisher strafprozessualen Ermittlungen ausschließlich im Rahmen offener Durchsuchungen oder heimlicher akustischer Wohnraumüberwachungen zugänglich. Die durch diese Maßnahmen gewonnenen Erkenntnisse beschränken sich dabei naturgemäß einerseits auf Einblicke in das physische Wohngeschehen in Echtzeit und andererseits auf das, was entweder im Rahmen einer Durchsuchung sinnlich wahrgenommen werden kann oder im Rahmen des Lauschangriffes gehört werden kann. Durch den Einzug von Smart Home-Systemen und -Geräten potenzieren sich die Überwachungsmöglichkeiten und damit auch die Möglichkeiten zur Straftataufklärung.<sup>8</sup> Denn die Smart Home-Technologie bedingt, dass das bisher flüchtige physische Wohnraumgeschehen digital manifestiert wird und damit auch rekonstruiert werden kann. Im Gegensatz zu Überwachungskameras oder für den Lauschangriff eingesetzten Wanzen haben Sensoren des Smart Home außerdem weitaus mehr Wahrnehmungsfähigkeiten, sodass diese Rekonstruktion des physischen Wohngeschehens auch in qualitativer und quantitativer Hinsicht weit über bisherige Einblicke in die räumliche Privatsphäre hinausgeht. Ein Blick in das Smart Home kann digitale Spuren, Indizien und Beweise ergeben zu Fragen wie etwa, ob der Verdächtige zu einem bestimmten Zeitpunkt tatsächlich Zuhause war, mit wem er sich zu Hause über Tatpläne ausgetauscht hat, wer der Einbrecher war, was zur Tatzeit am Tatort Wohnung geschah oder auch, ob der Nutzer mit der bestellten chemischen Substanz tatsächlich nur Hausarbeiten verrichtet hat. Zum anderen eröffnet die Smart Home-Technologie Ermittlern auch neue Wege zur Echtzeitüberwachung.<sup>9</sup> Abhörvorrichtungen hat der Nutzer bereits selbst installiert und mit dem Internet verbunden, sodass die Ermittler bei Überwindung technischer Schutzmechanismen unbemerkt am Geschehen in der Wohnung – je nach eingesetzter Sensorik – sogar besser, als wenn sie vor Ort wären, teilhaben können, da selbst mehrere Räume gleichzeitig überwacht werden können.

Neben diesem besonderen Bezug zur räumlichen Privatsphäre können Zugriffe auf das Smart Home für Ermittler auch deshalb von besonderem Interesse sein, da das Smart Home als mit dem Internet verbundenes informationstechnisches System auch andere, nicht wohnungsspezifische Technologien in sich vereint. So wird das Smart Home mit mobilen Geräten wie Smartphones, Tablets, Smartwatches etc. ebenso verbunden sein wie mit externen Anwendungen wie etwa dem Cloud-Computing oder E-Mail-Programmen. Auch kann mit Hilfe des Smart Home im Internet gesurft, eingekauft und mit anderen kommuniziert werden. Mit einem einzigen Zugriff auf ein Smart Home-System kann daher nicht selten die gesamte digitale und physische Welt des Betroffenen eingesehen werden.

---

<sup>7</sup> S. hierzu die Antworten auf die Fragen 1. und 2., Gespräch mit der ZAC NRW, Anhang.

<sup>8</sup> S. auch Antwort auf Frage 2., Gespräch mit der ZAC NRW, Anhang.

<sup>9</sup> S. auch Antwort auf Frage 2., Gespräch mit der ZAC NRW, Anhang.

## A. Erkenntnisziel

Auch außerhalb des Smart Home verlieren gegenstandsbezogene Ermittlungen aufgrund der zunehmenden Digitalisierung nahezu aller denkbaren Informationen an Bedeutung, während die Erhebung und Verwertung von Daten immer bedeutsamer wird<sup>10</sup> und der unaufhaltsame technische Fortschritt beständig zu neuen elektronischen Ermittlungsmöglichkeiten führt.<sup>11</sup> Dennoch finden sich in der deutschen Strafprozessordnung (StPO) nur vereinzelt Vorschriften dazu, wie mit diesen „neuen“ Beweismodalitäten und -findungsmöglichkeiten umzugehen ist.<sup>12</sup> So müssen Daten auch nach nunmehr Jahrzehnten immer noch nach den §§ 94 ff. StPO „beschlagnahmt“ werden und unter „Gegenstände“ subsumiert werden.<sup>13</sup> Technikbezogene Ermächtigungen wie etwa die Online-Durchsuchung nach § 100b StPO haben nicht nur einen zu weiten Anwendungsbereich, sondern hinterlassen mehr Fragen als Antworten.<sup>14</sup> Mit welcher Ermächtigung auf welches Datum von welchem Ort aus zugegriffen werden darf, ist nicht selten unklar. Gründe dafür liegen nicht nur in der Komplexität der Materie, sondern insbesondere an einem technikavers amutenden Gesetzgeber, der vom digitalen Wandel beinahe überrollt scheint. So haben sich Änderungen im System der strafprozessualen Ermächtigungen auf punktuelle „Ergänzungen“ oder „nachgeschobene“ Ermächtigungsgrundlagen beschränkt, was nicht zuletzt die inflationäre Verwendung von Buchstaben im Achten Abschnitt erahnen lässt. Mit Blick auf Datenzugriffe lässt sich vergeblich nach Kohärenz im strafprozessualen „System“ der Ermächtigungen suchen. Neben der technikignoranten Haltung des Gesetzgebers wurzeln viele Unklarheiten dabei schon auf der Ebene des Verfassungsrechts. So besteht in weiten Teilen Uneinigkeit darüber, welche Daten von welchen Grundrechten geschützt werden und welche Zugriffe in welches Grundrecht eingreifen, geschweige denn, wie die Intensität von Datenzugriffen als Grundrechtseingriffe zu bemessen ist.<sup>15</sup> Dabei gedeiht die Digitalisierung und Technologisierung bereits seit Jahrzehnten, das deutsche Strafverfahrensrecht hingegen scheint den Anschluss verpasst zu haben. Um dem Anspruch, als angewandtes Verfassungsrecht rechtstatsächlich Wirkung zu entfalten, auch im digitalen Zeitalter gerecht zu werden,<sup>16</sup> muss das Strafprozessrecht seinen Anker aus der analogen Welt lösen<sup>17</sup> und Raum für eine grundlegende Neuausrichtung im Umgang mit der digitalen Welt schaffen, die einen tiefgreifenden Wandel

---

<sup>10</sup> Warken, NZWiSt 2017, 289.

<sup>11</sup> Singenstein, NSZ 2012, 593.

<sup>12</sup> Genaue Auflistung bestehender StPO-Vorschriften mit Bezug zu elektronischen Beweismitteln bei Warken, NZWiSt 2017, 329 (333 ff.).

<sup>13</sup> S. hierzu noch 4. Teil C. III.

<sup>14</sup> S. hierzu noch 4. Teil C. II.

<sup>15</sup> Vgl. hierzu auch Antwort auf Frage 4., Gespräch mit der ZAC NRW, Anhang. S. noch ausführlich 3. Teil.

<sup>16</sup> Löffelmann, StV 2018, 536 (543).

<sup>17</sup> Gless, StV 2018, 671 (674).