

Kurzinhaltverzeichnis

Inhaltsverzeichnis.....	XIII
Abkürzungsverzeichnis	XXXV
Literaturverzeichnis.....	XXXIX
Kapitel 1 Einleitung.....	1
A. Einführung in die Thematik	1
B. Ziel der Untersuchung.....	2
C. Gang der Untersuchung.....	7
Kapitel 2 Informationstechnik als Gegenstand von Ermittlungsverfahren – Definitionen.....	11
A. Cloud-Computing	11
B. Informationstechnisches System	11
C. Keylogger (Hardware/Software)	12
D. Kritische Infrastruktur	12
E. Smart Car/Intelligentes KFZ.....	13
F. Spiegeln eines Datenträgers	13
G. Trojaner/Staatstrojaner/Bundestrojaner.....	13
H. Zero-Day-Exploit	13
Kapitel 3 Verfassungsrechtliche Grenzen verdeckter digitaler Ermittlungsmaßnahmen.....	15
A. Grenzen aus dem Grundgesetz.....	15
I. Menschenwürde (Art. 1 Abs. 1 GG).....	15
II. Fernmeldegeheimnis (Art. 10 Abs. 1 GG)	16
III. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG)	17
IV. Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG)	18
V. Bestimmtheitsgebot, Gebot der Normenklarheit.....	19

VII

VI.	Wesentlichkeitsgrundsatz	20
VII.	Zitiergebot (Art. 19 Abs. 1 Satz 2 GG).....	20
VIII.	Verhältnismäßigkeitsgrundsatz (Übermaßverbot)	21
IX.	Der staatliche Schutzauftrag für seine Bürger gemäß Art. 2 Abs. 2 Satz 1 GG i. V. m. Art. 1 Abs. 1 Satz 2 GG	22
B.	Exkurs: Grenzen aus der EMRK.....	22
I.	Recht auf Privatleben und Familienleben (Art. 8 Abs. 1 EMRK)	23
II.	Recht auf ein faires Verfahren (Art. 6 EMRK).....	24
Kapitel 4	Darstellung verschiedener Infiltrationsmethoden unter Berücksichtigung ihrer ermittlungstaktischen Vor- und Nachteile und rechtlichen Grenzen.....	25
A.	Physischer Zugriff	26
I.	Möglichkeiten des physischen Zugriffs	26
II.	Eigene Stellungnahme.....	27
B.	Infiltration mithilfe einer Täuschung des Nutzers	33
I.	Möglichkeiten der Infiltration mithilfe einer Täuschung des Nutzers.....	33
II.	Tatsächliche Vor- und Nachteile einer Infiltration mittels Täuschung	35
III.	Rechtliche Grenzen einer Infiltration mittels Täuschung	36
C.	Infiltration ohne wissentliche Mitwirkung des Betroffenen.....	41
D.	Verwendung von Sicherheitslücken für staatliche Akteure („Bundes-Backdoor“).....	43
E.	Ergebnis.....	45
Kapitel 5	Darstellung ausgewählter Gefahren infolge der Schädigung der allgemeinen IT-Sicherheit durch staatliches Handeln zur Vorbereitung von verdeckten digitalen Ermittlungsmaßnahmen nach § 100a und § 100b StPO.....	47
A.	Bedeutung der allgemeinen IT-Sicherheit.....	47
B.	Probleme für die allgemeine IT-Sicherheit.....	48
I.	Durchführung mittels <i>Zero-Day-Exploits</i>	48
II.	Interessenkonflikt bei der Nutzung von <i>Zero-Day-Exploits</i>	48
C.	Entstehung von <i>Zero-Day-Exploits</i>	49

D. Interessenkonflikt bei der Nutzung von Zero-Day-Exploits	50
I. Bedarf an Schwachstellen	51
II. Gefährdung der allgemeinen IT-Sicherheit durch Zero-Day-Exploits	51
E. Schädigung der allgemeinen IT-Sicherheit durch staatliches Handeln zur Vorbereitung von Ermittlungsmaßnahmen	52
I. Schädigung durch die Schaffung einer Nachfrage	53
II. Schädigung durch Interesse an Geheimhaltung.....	54
F. Darstellung ausgewählte Nachteile durch die staatliche Schädigung der allgemeinen IT-Sicherheit.....	54
I. Gefährdung kritischer Infrastrukturen	55
II. Gefährdung durch die Erleichterung von Wirtschaftsspionage mittels Cyberangriffen	55
III. Gefährdung staatlicher Einrichtung und Funktionen.....	56
IV. Gefährdung durch die Erleichterung von terroristischen Angriffen	56
G. Das Computervirus „WannaCry“	57
H. Staatliche Schutzwpflicht für die allgemeine IT-Sicherheit?	59
I. Entscheidung des BVerfG zu § 54 BWPolG.....	62
II. Stellungnahme durch Pötl.....	63
III. Eigene Stellungnahme.....	63
J. Lösungsmöglichkeiten.....	64
I. Nutzung nur bekannter Sicherheitslücken	64
II. Rechtlicher Rahmen zur Nutzung von Sicherheitslücken.....	67
K. Ergebnis.....	69
Kapitel 6 Gesetzgebungsverfahren des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens	71
A. Ablauf des Gesetzgebungsverfahrens	71
B. Mängel im Gesetzgebungsverfahren	72
I. Einfügen durch Änderungsantrag	72
II. Mangelhafte Beteiligung der damaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	75
C. Verbesserungsvorschlag für ein zukünftiges Gesetzgebungsverfahren.....	75

Kapitel 7 § 100a und § 100b StPO als wichtige verdeckte digitale Ermittlungsmaßnahmen.....	77
A. Konventionelle Telekommunikationsüberwachung im Sinne des § 100a Abs. 1 Satz 1 StPO.....	78
I. Begriff der Telekommunikationsüberwachung des § 100a StPO	79
II. Eingriffsintensität einer Maßnahme nach § 100a Abs. 1 Satz 1 StPO	81
III. Anordnungsvoraussetzungen des § 100a Abs. 1 Satz 1StPO	82
IV. Kernbereichsschutz einer Maßnahme nach § 100a Abs. 1 Satz 1 StPO	113
V. Schutz von zeugnisverweigerungsberechtigten Personen	126
VI. Grundrechtsprüfung	128
B. Die Quellen-Telekommunikationsüberwachung im Sinne des § 100a Abs. 1 Satz 2 StPO.....	132
I. Begriff der Quellen-Telekommunikationsüberwachung	132
II. Rechtliche Lage vor in Kraft treten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens	134
III. Eingriffsintensität des § 100a Abs. 1 Satz 2 StPO.....	135
IV. Anordnungsvoraussetzungen	146
V. Grundrechtsprüfung	152
VI. Überlegungen de lege ferenda	175
C. Die sogenannte kleine Online-Durchsuchung im Sinne des § 100a Abs. 1 Satz 3 StPO	186
I. Begriff und Abgrenzung der kleinen Online-Durchsuch im Sinne des § 100a Abs. 1 Satz 3 StPO zur Online-Durchsuchung im Sinne des § 100b StPO.....	186
II. Eingriffsintensität.....	188
III. Anordnungsvoraussetzungen	194
IV. Grundrechtsprüfung	196
V. Überlegungen de lege ferenda	208
D. Die Anforderungen an die Durchführung der Maßnahme nach § 100a Abs. 5 StPO	213
I. Die einzelnen Pflichten des § 100a Abs. 5 StPO.....	213
II. Rechtsfolgen eines Verstoßes gegen die technischen Anforderungen des § 100a Abs. 5 StPO	223
III. Kritik an § 100a Abs. 5 StPO, insbesondere den fehlenden Vorgaben zur Beschaffung der einzusetzenden Software.....	226
IV. Normvorschlag	231

E. Die Protokollierungspflichten des § 100a Abs. 6 StPO.....	231
I. Darstellung der Rechtslage und Ratio der Protokollierungspflicht.....	231
II. Offenlegung des Quellcodes	233
III. Verstoß gegen die Voraussetzungen des § 100a Abs. 6 StPO.....	235
IV. Kritik an § 100a Abs. 6 StPO	235
V. Normvorschlag	237
F. Die Online-Durchsuchung im Sinne des § 100b StPO	237
I. Rechtslage vor der Reform	237
II. Zugriff auf ein informationstechnisches System mit technischen Mitteln	239
III. Ermittlungstaktische Möglichkeiten einer Online-Durchsuchung.....	242
IV. Eingriffsintensität.....	254
V. Anordnungsvoraussetzungen des § 100b StPO.....	265
VI. Richtervorbehalt.....	291
VII. Kernbereichsschutz	297
VIII. Schutz von Zeugnisverweigerungsberechtigten	304
IX. Grundrechtsprüfung	308
X. Weitere ausgewählte Kritikpunkte	325
XI. Überlegungen de lege ferenda	334
XII. Voraussetzungen des § 100a Abs. 5 und Abs. 6 StPO im Rahmen des § 100b StPO	338
Kapitel 8 Möglichkeiten der Überwachung von Cloud-Computing und smarten Geräten mittels § 100a und § 100b StPO	339
A. Die Überwachung von Cloud-Computing gemäß § 100a Abs. 1 Satz 1, 2, 3 StPO, § 100b StPO.....	339
I. Begriff, Arten und Verbreitung von Cloud-Computing	339
II. Ermittlungstaktischer Nutzen	340
III. Anwendbarkeit von § 100a und § 100b StPO auf Cloud-Computing	341
IV. Überlegungen de lege ferenda	349
B. Die Überwachung smarter Geräte mittels § 100a Abs. 1 Satz 1, 2, 3 und § 100b StPO.....	350
I. Intelligente KFZ – „Smart Cars“	350
II. Alexa und andere virtuelle Assistenten am Beispiel von smarten Lautsprechern	359

III.	Smarte medizinische Geräte.....	374
Kapitel 9 Zusammenfassung der Ergebnisse und Normvorschläge		381
A.	Zusammenfassung der Ergebnisse	381
I.	Infiltration von informationstechnischen Systemen.....	381
II.	Bedeutung von Gefahren für die allgemeine IT-Sicherheit durch verdeckte digitale Ermittlungsmaßnahmen.....	383
III.	Gesetzgebungsverfahren des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens	384
IV.	§ 100a und § 100b StPO als wichtige verdeckte digitale Ermittlungsmaßnahmen.....	385
V.	Möglichkeiten der Überwachung von Cloud-Computing und smartten Geräten mittels § 100a und § 100b StPO.....	400
B.	Übersicht über alle Normvorschläge	404

Inhaltsverzeichnis

Abkürzungsverzeichnis	XXXV
Literaturverzeichnis.....	XXXIX
Kapitel 1 Einleitung.....	1
A. Einführung in die Thematik	1
B. Ziel der Untersuchung.....	2
C. Gang der Untersuchung.....	7
Kapitel 2 Informationstechnik als Gegenstand von Ermittlungsverfahren – Definitionen.....	11
A. Cloud-Computing	11
B. Informationstechnisches System	11
C. Keylogger (Hardware/Software)	12
D. Kritische Infrastruktur	12
E. Smart Car/Intelligentes KFZ.....	13
F. Spiegeln eines Datenträgers	13
G. Trojaner/Staatstrojaner/Bundestrojaner.....	13
H. Zero-Day-Exploit	13
Kapitel 3 Verfassungsrechtliche Grenzen verdeckter digitaler Ermittlungsmaßnahmen.....	15
A. Grenzen aus dem Grundgesetz.....	15
I. Menschenwürde (Art. 1 Abs. 1 GG).....	15
II. Fernmeldegeheimnis (Art. 10 Abs. 1 GG)	16
III. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG)	17
IV. Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG)	18
V. Bestimmtheitsgebot, Gebot der Normenklarheit.....	19
VI. Wesentlichkeitsgrundsatz	20
VII. Zitiergebot (Art. 19 Abs. 1 Satz 2 GG).....	20

VIII.	Verhältnismäßigkeitsgrundsatz (Übermaßverbot)	21
IX.	Der staatliche Schutzauftrag für seine Bürger gemäß Art. 2 Abs. 2 Satz 1 GG i. V. m. Art. 1 Abs. 1 Satz 2 GG	22
B.	Exkurs: Grenzen aus der EMRK.....	22
I.	Recht auf Privatleben und Familienleben (Art. 8 Abs. 1 EMRK)	23
II.	Recht auf ein faires Verfahren (Art. 6 EMRK).....	24
Kapitel 4	Darstellung verschiedener Infiltrationsmethoden unter Berücksichtigung ihrer ermittlungstaktischen Vor- und Nachteile und rechtlichen Grenzen.....	25
A.	Physischer Zugriff	26
I.	Möglichkeiten des physischen Zugriffs	26
II.	Eigene Stellungnahme	27
1)	Vorteile einer Infiltration mittels physischen Zugriffes	27
2)	Tatsächliche Schwierigkeiten einer Infiltration mittels physischen Zugriffes.....	27
3)	Rechtliche Grenzen einer Infiltration mittels physischen Zugriffes	28
a)	Verdecktes Betreten der Wohnung.....	28
aa)	Verstoß gegen das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG und Art. 13 Abs. 1 GG	28
bb)	Keine Rechtfertigung durch eine Kombination mit § 100c StPO	29
cc)	Keine Rechtfertigung durch eine Kombination mit § 102 StPO.....	31
b)	Betreten der Wohnung unter einer Legende	31
c)	Zwischenfazit	33
B.	Infiltration mithilfe einer Täuschung des Nutzers	33
I.	Möglichkeiten der Infiltration mithilfe einer Täuschung des Nutzers.....	33
II.	Tatsächliche Vor- und Nachteile einer Infiltration mittels Täuschung	35
1)	Vorteile einer Infiltration mittels Täuschung	35
2)	Nachteile einer Infiltration mittels Täuschung	35
III.	Rechtliche Grenzen einer Infiltration mittels Täuschung	36
1)	Vereinbarkeit mit § 136a StPO	37
2)	Vereinbarkeit mit der Selbstbelastungsfreiheit	37
3)	Pauschale Ablehnung eines Verstoßes	38

4) Eigene Stellungnahme	38
a) Unanwendbarkeit von § 136a StPO.....	38
b) Differenzierte Lösung	39
c) Unzulässigkeit der Nutzung staatlicher Identitäten	40
d) Beispiel für zulässige Täuschungen – CDs mit Spähsoftware	41
C. Infiltration ohne wissentliche Mitwirkung des Betroffenen.....	41
D. Verwendung von Sicherheitslücken für staatliche Akteure („Bundes-Backdoor“).....	43
E. Ergebnis.....	45
Kapitel 5 Darstellung ausgewählter Gefahren infolge der Schädigung der allgemeinen IT-Sicherheit durch staatliches Handeln zur Vorbereitung von verdeckten digitalen Ermittlungsmaßnahmen nach § 100a und § 100b StPO.....	47
A. Bedeutung der allgemeinen IT-Sicherheit.....	47
B. Probleme für die allgemeine IT-Sicherheit.....	48
I. Durchführung mittels Zero-Day-Exploits	48
II. Interessenkonflikt bei der Nutzung von Zero-Day-Exploits	48
C. Entstehung von Zero-Day-Exploits	49
D. Interessenkonflikt bei der Nutzung von Zero-Day-Exploits	50
I. Bedarf an Schwachstellen	51
II. Gefährdung der allgemeinen IT-Sicherheit durch Zero-Day-Exploits	51
E. Schädigung der allgemeinen IT-Sicherheit durch staatliches Handeln zur Vorbereitung von Ermittlungsmaßnahmen	52
I. Schädigung durch die Schaffung einer Nachfrage	53
II. Schädigung durch Interesse an Geheimhaltung.....	54
F. Darstellung ausgewählte Nachteile durch die staatliche Schädigung der allgemeinen IT-Sicherheit.....	54
I. Gefährdung kritischer Infrastrukturen	55
II. Gefährdung durch die Erleichterung von Wirtschaftsspionage mittels Cyberangriffen	55
III. Gefährdung staatlicher Einrichtung und Funktionen.....	56
IV. Gefährdung durch die Erleichterung von terroristischen Angriffen	56

G. Das Computervirus „WannaCry“	57
H. Staatliche Schutzwicht für die allgemeine IT-Sicherheit?	59
I. Entscheidung des BVerfG zu § 54 BWPolG	62
II. Stellungnahme durch Pötl.....	63
III. Eigene Stellungnahme.....	63
J. Lösungsmöglichkeiten.....	64
I. Nutzung nur bekannter Sicherheitslücken	64
II. Rechtlicher Rahmen zur Nutzung von Sicherheitslücken.....	67
1) Bereits bestehender rechtlicher Rahmen	67
2) Eigene Stellungnahme.....	68
K. Ergebnis.....	69
Kapitel 6 Gesetzgebungsverfahren des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens	71
A. Ablauf des Gesetzgebungsverfahrens	71
B. Mängel im Gesetzgebungsverfahren	72
I. Einfügen durch Änderungsantrag	72
1) Kritik während des Gesetzgebungsverfahren	72
2) Kritik in der Literatur und den Stellungnahmen der Experten	73
3) Eigene Stellungnahme.....	73
II. Mangelhafte Beteiligung der damaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	75
C. Verbesserungsvorschlag für ein zukünftiges Gesetzgebungsverfahren.....	75
Kapitel 7 § 100a und § 100b StPO als wichtige verdeckte digitale Ermittlungsmaßnahmen	77
A. Konventionelle Telekommunikationsüberwachung im Sinne des § 100a Abs. 1 Satz 1 StPO.....	78
I. Begriff der Telekommunikationsüberwachung des § 100a StPO	79
1) Telekommunikation.....	79
2) Technische Aspekte der Telekommunikationsüberwachung.....	81
II. Eingriffsintensität einer Maßnahme nach § 100a Abs. 1 Satz 1 StPO	81
III. Anordnungsvoraussetzungen des § 100a Abs. 1 Satz 1StPO	82

1)	Verdachtsgrad im Sinne des § 100a Abs. 1 Satz 1 Nummer 1 StPO	83
a)	Tatbestand	83
b)	Eigene Stellungnahme.....	84
2)	Katalog des § 100a Abs. 2 StPO	85
a)	Aktueller Katalog des § 100a Abs. 2 StPO	85
b)	Reaktionen der Literatur	87
aa)	Kritik am Katalog des § 100a Abs. 2 StPO	87
aaa)	Kritik an der Aufnahme von Delikten mit geringem Unrechtsgehalt und insbesondere von Alltagskriminalität	87
bbb)	Kritik an der Aufnahme von Qualifikationen und Regelbeispielen.....	88
ccc)	Kritik an der schleichenden Erweiterung des Katalogs....	90
bb)	Forderungen nach einer Erweiterung des Katalogs.....	90
c)	Eigene Stellungnahme.....	91
aa)	Eigene Stellungnahme zur Aufnahme von Delikten mit geringem Unrechtsgehalt und insbesondere von Alltagskriminalität	91
bb)	Eigene Stellungnahme zur Aufnahme von schwer aufklärbarer Kriminalität	94
dd)	Eigene Stellungnahme zur Aufnahme von Regelbeispielen.....	94
ee)	Eigene Stellungnahme zur schleichenden Erweiterung des Katalogs	95
ff)	Eigene Stellungnahme zu einer weiteren Erweiterung des Katalogs	95
d)	Änderungsvorschläge	96
aa)	Reduzierung des Kataloges auf Verbrechen im Sinne des § 12 Abs. 1 StGB.....	96
bb)	Reduzierung des Katalogs auf Verbrechen und Vergehen, bei welchen die Aussetzung zur Bewährung gemäß § 56 Abs. 2 Satz 1 StGB ausgeschlossen ist	97
cc)	Eigene Stellungnahme	98
3)	„Schwerwiegender im Einzelfall“ im Sinne des § 100a Abs. 1 Satz 1 Nr. 2 StPO	99
a)	Tatbestand § 100a Abs. 1 Satz 1 Nr. 2 StPO	99
b)	Eigene Stellungnahme.....	100
4)	Subsidiarität im Sinne des § 100a Abs. 1 Satz 1 Nr. 3 StPO	100
5)	Verhältnismäßigkeitsgrundsatz.....	103

6)	Betroffene im Sinne des § 100a Abs. 3 StPO	103
a)	Anwendbarkeit auf den Beschuldigten.....	103
b)	Anwendbarkeit auf andere Betroffene	104
aa)	Anwendbarkeit auf Nachrichtenmittler	104
bb)	Anwendbarkeit auf Anschlussinhaber	105
7)	Überwachbarkeit Ausländische Kommunikation.....	106
8)	Dauer der Überwachung.....	106
9)	Anordnung §§ 100a Abs. 4, 100e StPO	107
a)	Grundfall: Richtervorbehalt	107
b)	Eilkompetenz der Staatsanwaltschaft.....	107
c)	Qualität des Richtervorbehalts.....	109
d)	Qualifizierter Richtervorbehalt des § 100e Abs. 2 StPO	111
10)	Zwischenergebnis	113
IV.	Kernbereichsschutz einer Maßnahme nach § 100a Abs. 1 Satz 1 StPO	113
1)	Definition des Kernbereichs	115
2)	Erhebungsverbot des § 100d Abs. 1 StPO	116
a)	Tatbestand des § 100d Abs. 1 StPO	116
b)	Reaktionen der Literatur zum Erhebungsverbot des § 100d Abs. 1 StPO	117
c)	Eigene Stellungnahme	118
3)	Ungeschriebene Unterbrechungspflicht.....	120
a)	Kritik an einer Pflicht zur Echtzeitüberwachung.....	120
b)	Alternative Lösungsmöglichkeiten	121
c)	Eigene Stellungnahme	122
4)	Verwertungsverbot § 100d Abs. 2 Satz 1 StPO.....	123
5)	Löschungs- und Dokumentationspflicht § 100d Abs. 2 Satz 2 und 3 StPO	123
6)	Notwendigkeit einer Kernbereichsprognose i. S. d. § 100d Abs. 4 Satz 1 StPO	124
7)	Ergebnis	126
V.	Schutz von zeugnisverweigerungsberechtigten Personen	126
VI.	Grundrechtsprüfung	128
1)	Legitimer Zweck der Maßnahme nach § 100a Abs. 1 Satz 1 StPO	128
2)	Geeignetheit der Maßnahme nach § 100a Abs. 1 Satz 1 StPO	129
3)	Erforderlichkeit	130
4)	Angemessenheit	131

5) Fazit	132
B. Die Quellen-Telekommunikationsüberwachung im Sinne des § 100a Abs. 1 Satz 2 StPO	132
I. Begriff der Quellen-Telekommunikationsüberwachung	132
II. Rechtliche Lage vor in Kraft treten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens	134
III. Eingriffsintensität des § 100a Abs. 1 Satz 2 StPO.....	135
1) Fernmeldegeheimnis (Art. 10 Abs. 1 GG)	136
2) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG)	136
a) Strömung Contra Anwendbarkeit des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG).....	137
b) Strömung Pro Anwendung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG).....	138
aa) Auffassung Hauck	139
bb) Auffassung Bode.....	140
c) Eigene Stellungnahme	141
aa) Parallelwertung in der Laiensphäre	141
bb) Begriff der Quellen-Telekommunikationsüberwachung	142
cc) Historische Einordnung von BVerfGE 120, 274.....	144
dd) Infiltration vor Telekommunikationsüberwachung	145
IV. Anordnungsvoraussetzungen	146
1) Subsidiarität gegenüber § 100a Abs. 1 Satz 1 StPO	146
a) Argumente für eine Subsidiarität gegenüber § 100a Abs. 1 Satz 1 StPO	147
b) Argumente gegen eine Subsidiarität gegenüber § 100a Abs. 1 Satz 1 StPO	147
c) Eigene Stellungnahme.....	148
2) Infiltration eines informationstechnischen Systems	149
a) Begriff des informationstechnischen Systems	149
b) Eigene Stellungnahme.....	150
3) Erfasste Kommunikationsarten	150
4) Zwischenergebnis	151
V. Grundrechtsprüfung	152

1) Legitimer Zweck	152
2) Geeignetheit.....	154
a) Geeignetheit der repressiven Quellen- Telekommunikationsüberwachung	154
b) Kritik an der Geeignetheit	155
c) Eigene Stellungnahme.....	156
3) Erforderlichkeit	156
a) Alternativen zur Quellen-Telekommunikationsüberwachung	156
aa) Man-in-the-middle-Angriff (Janusangriff)	156
bb) Deaktivierung der Verschlüsselung	157
cc) Auslesung des Schlüssels	158
dd) Erlangung der Daten beim Anbieter.....	159
ee) Auslesen von Instant Messaging via Desktop-Verknüpfung	161
b) Fazit	162
4) Angemessenheit	162
a) Argumente für eine Angemessenheit.....	163
aa) Technisches Funktionsäquivalent zur konventionellen Telekommunikationsüberwachung	163
bb) Höhere Eingriffsintensität bei Fehlen der Quellen- Telekommunikationsüberwachung	164
b) Argumente gegen eine Angemessenheit.....	164
aa) Kritik an der Übertragung der Anordnungsvoraussetzungen aus § 100a Abs. 1 Satz 1 StPO	165
bb) Fehlende Bestimmtheit der Norm des § 100a Abs. 1 Satz 2 StPO	165
c) Eigene Stellungnahme.....	165
aa) Abzuwägende Rechtsgüter	166
bb) Gleiche Anordnungsvoraussetzungen im Vergleich zur konventionellen Telekommunikationsüberwachung i. S. d. § 100a Abs. 1 Satz 1 StPO	167
aaa) Annahme geringerer Voraussetzung bei repressivem als bei präventivem Handeln.....	167
bbb) Erhöhte bzw. gleiche Anforderungsvoraussetzungen für repressives Handeln	168
ccc) Eigene Stellungnahme zum anzulegenden Maßstab	169
cc) Einhaltung dieser Anordnungsvoraussetzungen	170
aaa) Einhaltung der Anordnungsvoraussetzungen für Eingriffe in das Grundrecht auf Gewährleistung der	

Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG)	170
bbb) Einhaltung der Voraussetzungen für einen Eingriff in das Fernmeldegeheimnis des Art. 10 Abs. 1 GG	173
d) Fazit	174
5) Zusammenfassung	174
VI. Überlegungen de lege ferenda	175
1) Verdachtsgrad	175
2) Katalog	176
a) Orientierung an anderen Straftatenkatalogen.....	176
b) Einbeziehung von Internet und Kommunikationstechnik (IuK)-Kriminalität bzw. Cybercrime	177
c) Einbeziehung von Straftaten gegen die sexuelle Selbstbestimmung	178
d) Zusammenfassender Vorschlag für einen neuen Straftatenkatalog für die repressive Quellen-Telekommunikationsüberwachung	178
3) Schwerwiegender im Einzelfall	179
a) Vorschlag von Buermeyer.....	179
b) Lösungsvorschlag: zu verhängende Freiheitsstrafe von mindestens einem Jahr.....	180
4) Subsidiarität	181
5) Richtervorbehalt.....	181
a) Für die Anordnung zuständige Stelle.....	181
b) Eilkompetenz der Staatsanwaltschaft/des Vorsitzenden	183
6) Kernbereichsschutz	183
7) Normvorschlag	184
C. Die sogenannte kleine Online-Durchsuchung im Sinne des § 100a Abs. 1 Satz 3 StPO	186
I. Begriff und Abgrenzung der kleinen Online-Durchsuch im Sinne des § 100a Abs. 1 Satz 3 StPO zur Online-Durchsuchung im Sinne des § 100b StPO	186
1) Begriff.....	186
a) Einführung aufgrund eines ermittlungstaktischen Bedürfnisses	186
b) Reichweite der Maßnahme nach § 100a Abs. 1 Satz 3 StPO... ..	186
c) Bezeichnung als „kleine Online-Durchsuchung“	187
2) Abgrenzung zur Online-Durchsuchung im Sinne des § 100b StPO	188

II.	Eingriffsintensität.....	188
1)	Ansicht des Gesetzgebers	188
2)	Strömung Contra Anwendbarkeit des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG)	189
a)	Auffassung Krauß	189
b)	Auffassung Ruppert	190
3)	Strömung Pro Anwendbarkeit des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG)	190
a)	Auffassung Roggan	190
b)	Auffassung Großmann.....	191
c)	Auffassung Voßhoff und Blechschmitt.....	191
d)	Auffassung Buermeyer	192
4)	Eigene Stellungnahme.....	193
III.	Anordnungsvoraussetzungen	194
1)	Infiltration eines informationstechnischen Systems	195
2)	Zeitraum der Überwachung	195
3)	Subsidiarität	195
IV.	Grundrechtsprüfung	196
1)	Legitimer Zweck.....	196
2)	Geeignetheit.....	196
3)	Erforderlichkeit.....	196
4)	Angemessenheit	198
	a) Strömung Pro Angemessenheit.....	200
	aa) Auffassung Schlegel	200
	bb) Auffassung Niederhuber	200
	b) Vertreter Contra Angemessenheit	201
	aa) Auffassung Mansdörfer	201
	bb) Auffassung Voßhoff und Blechschmitt	202
	cc) Auffassung Keller/Braun	203
	dd) Auffassung Schniemann	203
	ee) Auffassung Burmeyer.....	204
	c) Eigene Stellungnahme	205
	aa) Technische Unmöglichkeit der Umsetzung.....	205

bb)	Gleiche Anordnungsvoraussetzungen trotz gesteigerter Eingriffsintensität.....	205
cc)	Beeinträchtigung von Grundrechten unbeteiligter Dritter.....	207
dd)	Existenz weniger eingriffsintensiver Alternativen.....	207
V.	Überlegungen de lege ferenda	208
1)	Verdachtsgrad.....	208
2)	Katalog	209
3)	Schwerwiegend im Einzelfall	209
4)	Subsidiarität	210
5)	Richtervorbehalt.....	210
6)	Kernbereichsschutz	211
7)	Normvorschlag	212
D.	Die Anforderungen an die Durchführung der Maßnahme nach § 100a Abs. 5 StPO	213
I.	Die einzelnen Pflichten des § 100a Abs. 5 StPO	213
1)	Umfang der Ausleitbaren Daten, § 100a Abs. 5 Satz 1 Nr. 1 StPO	213
a)	Beschränkung auf laufende Kommunikation, § 100a Abs. 5 Satz 1 Nr. 1 Buchstabe a StPO	214
b)	Vorgaben für die Maßnahme nach § 100a Abs. 1 Satz 3 StPO, § 100a Abs. 5 Satz 1 Nr. 1 Buchstabe b StPO	214
c)	Technische Umsetzbarkeit.....	215
aa)	Strömung, welche eine technische Umsetzbarkeit verneinen	215
bb)	Vertreter, welche von einer technischen Umsetzbarkeit ausgehen	216
cc)	Zwischenergebnis	216
d)	Rechtsfolgen einer fehlenden technischen Umsetzbarkeit.....	217
aa)	Verfassungswidrigkeit der Ermächtigungsgrundlage.....	217
bb)	Verfassungswidrigkeit der Ausführungshandlung.....	218
cc)	Eigene Stellungnahme	218
2)	Anforderungen des § 100a Abs. 5 Satz 1 Nr. 2 StPO	219
3)	Anforderungen des § 100a Abs. 5 Satz 1 Nr. 3 StPO	219
4)	Anforderungen des § 100a Abs. 5 Satz 2 StPO	221
5)	Anforderungen des § 100a Abs. 5 Satz 3 StPO	222
a)	(Zwischen-) Sicherung der Überwachungsinhalte auf physischen Datenträgern oder auf einem Gerichtsserver	222
b)	Hashwertanalyse	223

II.	Rechtsfolgen eines Verstoßes gegen die technischen Anforderungen des § 100a Abs. 5 StPO	223
1)	Verstoß gegen § 100a Abs. 5 Satz 1 Nr. 1 Buchstabe a und Nr. 1 Buchstabe b StPO.....	224
2)	Verstoß gegen § 100a Abs. 5 Satz 1 Nr. 2 StPO	224
3)	Verstoß gegen § 100a Abs. 5 Satz 1 Nr. 3 StPO	224
4)	Verstoß gegen §§ 100a Abs. 5 Satz 2 und Satz 3 StPO	225
5)	Zwischenergebnis	225
III.	Kritik an § 100a Abs. 5 StPO, insbesondere den fehlenden Vorgaben zur Beschaffung der einzusetzenden Software.....	226
1)	Einführung in die Problematik	226
2)	Beschaffungsmöglichkeiten	226
3)	Eigene Stellungnahme.....	227
a)	Kein Erwerb aus dem Darknet	228
b)	Beschaffung nicht-staatlicher Software.....	228
c)	Staatliche Entwicklung der Software.....	229
d)	Staatliche Zertifizierung der Software	229
e)	Keine private Zertifizierung der Software.....	230
IV.	Normvorschlag	231
E. Die Protokollierungspflichten des § 100a Abs. 6 StPO.....	231	
I.	Darstellung der Rechtslage und Ratio der Protokollierungspflicht.....	231
II.	Offenlegung des Quellcodes	233
1)	Negative Folgen eines Bekanntwerdens des Quellcodes	233
2)	Lösungsvorschlag	235
III.	Verstoß gegen die Voraussetzungen des § 100a Abs. 6 StPO.....	235
IV.	Kritik an § 100a Abs. 6 StPO	235
1)	Gefahr der Verfälschung.....	236
2)	Überlegung de lege ferenda	236
V.	Normvorschlag	237
F. Die Online-Durchsuchung im Sinne des § 100b StPO	237	
I.	Rechtslage vor der Reform	237
II.	Zugriff auf ein informationstechnisches System mit technischen Mitteln	239
1)	Informationstechnisches System im Sinne des § 100b StPO.....	239
a)	Abweichender Begriff zu § 100a Abs. 1 Satz 2 und Satz 3 StPO	239

b)	Anhaltspunkte für eine Begriffsbestimmung	239
c)	Grundrechtsbezogener Begriff des informationstechnischen Systems	241
2)	Technisches Mittel	241
III.	Ermittlungstaktische Möglichkeiten einer Online-Durchsuchung.....	242
1)	Eignung zur Datenerhebung und Nutzungsüberwachung	243
a)	Eignung zur Datenerhebung	243
b)	Eignung zur Nutzerüberwachung/-analyse	244
c)	Sonstige ermittlungstaktische Eignung	246
2)	Eignung zur akustischen und/oder optischen Überwachung	247
a)	Für die Möglichkeit einer akustischen/optischen Überwachung	247
b)	Gegen die Möglichkeit einer akustischen/optischen Überwachung	248
aa)	Grammatikalische Auslegung	248
bb)	Zitiergebot des Art. 19 Abs. 1 Satz 2 GG.....	250
cc)	Verstoß gegen Art. 13 Abs. 3 GG	251
dd)	Eingriffstiefe	251
ee)	Zwischenergebnis	252
ff)	Sonderfall: Nutzer aktiviert selbst Kamera und Mikrofon.....	253
IV.	Eingriffsintensität.....	254
1)	Unverletzlichkeit der Wohnung Art. 13 Abs. 1 GG.....	254
2)	Fernmeldegeheimnis Art. 10 Abs. 1 GG	255
3)	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG)	256
a)	Gefahren und Umfang eines Eingriffs mittels einer Online-Durchsuchung	256
b)	Eingriffsvoraussetzungen des BVerfG	258
4)	Menschenwürdegarantie (Art. 1 Abs. 1 GG).....	259
a)	Verletzung durch Eingriff in den Kernbereich der privaten Lebensgestaltung	259
b)	Verletzung durch Verhaltens-, Kommunikations- und Persönlichkeitsprofile	259
c)	Verletzung durch mögliche Total- oder Rundumüberwachung	260
5)	Vergleich mit der Eingriffstiefe von § 100c StPO und Einordnung der Online-Durchsuchung im Vergleich mit anderen verdeckten technischen Überwachungsmaßnahmen	261

a)	Eingriffstiefe einer Online-Durchsuchung (§ 100b StPO)	262
b)	Eingriffstiefe des § 100c StPO	263
c)	Vergleich des § 100b Abs. 1 StPO mit der Eingriffstiefe des § 100c Abs. 1 StPO	263
d)	Ergebnis	265
V.	Anordnungsvoraussetzungen des § 100b StPO.....	265
1)	Verdachtsgrad im Sinne des § 100b Abs. 1 Nr. 1 StPO	265
a)	Aktuelle Rechtslage	265
b)	Vertreter für eine Verschärfung des zur Anordnung notwendigen Verdachtsgrades	266
aa)	Hinreichender Tatverdacht im Sinne des § 203 StPO	267
bb)	Dringender Tatverdacht	267
c)	Kritik an einer Steigerung des Verdachtsgrades	267
2)	Vorliegen einer Katalogtat im Sinne des § 100b Abs. 2 StPO....	269
a)	Aktueller Katalog des § 100b Abs. 2 StPO	269
b)	Anforderungen für den Katalog des § 100b Abs. 2 StPO	270
aa)	Durch das BVerfG aufgestellte Schranken für eine Online-Durchsuchung im präventiven Bereich.....	270
bb)	Übertragbarkeit dieser Vorgaben auf repressive Ermächtigungsgrundlagen	271
c)	Reaktionen in der Literatur.....	271
aa)	Forderung nach einer Reduzierung des Kataloges	272
aaa)	Allgemeine Kritik	272
bbb)	Kritik an konkreten Delikten	273
bb)	Forderungen nach einer Erweiterung des Straftatenkatalogs	274
aaa)	Aufnahme von IuK-Delikten zur Bekämpfung von Cybercrime und Terrorismus.....	275
bbb)	Aufnahme von § 17 AWG	276
ccc)	Begehung der Tat mittels informationstechnischer Systeme	276
d)	Eigene Stellungnahme	277
aa)	Streichung von Delikten wegen Unverhältnismäßigkeit....	277
bb)	Streichung aus anderen Gründen	278
cc)	Notwendige Erweiterung des Katalogs	278
dd)	Begehung der Tat mittels eines informationstechnischen Systems	279
3)	Tat im Einzelfall besonders schwerwiegend (§ 100b Abs. 1 Nr. 2 StPO).....	279

a)	Reformvorschlag von Buermeyer	280
b)	Reformvorschlag von Stelzer.....	281
c)	Eigene Stellungnahme.....	281
4)	Subsidiarität (§ 100b Abs. 1 Nr. 3 StPO).....	283
5)	Verhältnismäßigkeitsgrundsatz.....	285
6)	Tauglicher Maßnahmegergner (§ 100b Abs. 3 StPO)	286
a)	Beschuldigter	286
b)	Nichtbeschuldigter	286
aa)	Kritik an § 100b Abs. 3 Satz 2 und Satz 3 StPO.....	288
bb)	Eigene Stellungnahme	289
aaa)	Kritik an der Unbestimmtheit des Begriffs „Benutzung“	289
bbb)	Betroffenheit anderer Personen (§ 100b Abs. 3 Satz 3 StPO).....	290
7)	Wahrscheinlichkeit, dass relevante Beweisdaten gefunden werden (analog zu § 100c Abs. 1 Nr. 3 StPO).....	290
a)	Tatbestand	290
b)	Eigene Stellungnahme	291
VI.	Richtervorbehalt.....	291
1)	Anordnungsvoraussetzungen	291
2)	Kritik am bestehenden qualifizierten Richtervorbehalt.....	293
3)	Eigene Stellungnahme.....	293
4)	Dauer der Maßnahme.....	294
a)	Forderungen nach Erweiterung der Anordnungsdauer	295
b)	Eigene Stellungnahme	295
aa)	Stellungnahme zur vorgeschlagenen Erweiterung der Erstanordnungsdauer.....	295
bb)	Stellungnahme zur Möglichkeit einer unbegrenzten Dauer der Maßnahme.....	296
VII.	Kernbereichsschutz	297
1)	Spezieller Kernbereichsschutz der Online-Durchsuchung, § 100d Abs. 3 StPO	297
2)	Kritik am Kernbereichsschutz des § 100d Abs. 3 StPO.....	298
a)	Allgemeine Kritik an § 100d Abs. 3 StPO	298
b)	Kritik an § 100d Abs. 3 Satz 2 StPO	299
c)	Forderung eines erhöhten Kernbereichsschutzes im Sinne des § 100d Abs. 4 StPO	299
d)	Ablehnung eines erhöhten Kernbereichsschutzes	300

3) Eigene Stellungnahme	300
a) Technische Umsetzbarkeit.....	301
b) Übernahme einer negativen Kernbereichsprognose (§ 100d Abs. 4 StPO).....	302
c) Wortlaut des § 100d Abs. 3 Satz 2 StPO.....	303
VIII. Schutz von Zeugnisverweigerungsberechtigten	304
1) Berufsgeheimnisträger im Sinne des § 53 StPO	304
2) Angehörige im Sinne des § 52 StPO und Berufshelfer gemäß § 53a StPO	304
3) Kritik	305
a) Reduzierung des Schutzniveaus	305
b) Erweiterung des Schutzniveaus.....	306
4) Eigene Stellungnahme	307
IX. Grundrechtsprüfung	308
1) Legitimer Zweck.....	308
2) Geeignetheit.....	308
a) Zweifel an Geeignetheit	309
b) Eigene Stellungnahme.....	310
aa) Fehlende Geeignetheit aufgrund der Anforderungen an repressive Maßnahmen	310
bb) Fehlende Geeignetheit aufgrund der Nutzung durch verschiedene Nutzer	311
cc) Fehlende Geeignetheit aufgrund von Abwehrmaßnahmen.....	311
3) Erforderlichkeit	312
a) Vorteile offener Maßnahmen	312
aa) Umfang offener Ermittlungsmaßnahmen	312
bb) Abwehrmaßnahmen des Einzelnen gegen offene Maßnahmen	313
b) Nachteile von offenen Maßnahmen	313
aa) Gefahr des Beweisverlustes	314
bb) Erforderlichkeit eines zusätzlichen Beschlusses für eine verdeckte Ermittlungsmaßnahme	314
c) Zwischenergebnis	315
d) Alternative verdeckte Ermächtigungsgrundlagen	315
aa) „Online-Durchsicht“	316
bb) Optische Wohnraumüberwachung.....	316
cc) Schaffung einer Generalermächtigungsgrundlage	316

e) Trennung einzelner Ermächtigungsgrundlagen	317
aa) Allgemeine Vorteile verschiedener Ermächtigungsgrundlagen	317
bb) Überwachung des Surfverhaltens	318
cc) Verhinderung von Festplattenverschlüsselung	319
dd) Infiltration eines informationstechnischen Systems Ermittlung des Aufenthaltsortes und der IP-Adresse eines Beschuldigten	319
ee) Straftatenkatalog bei separaten Ermächtigungsgrundlagen	319
f) Zwischenergebnis	320
4) Angemessenheit	320
a) Eingriffsintensität der Maßnahme	320
b) Unverhältnismäßigkeit der Anordnungsvoraussetzungen	322
aa) Katalog	323
bb) Tat im Einzelfall schwerwiegend (§ 100b Abs. 1 Nr. 2 StPO)	323
cc) Richtervorbehalt und Dauer der Maßnahme	324
dd) Kernbereichsschutz	324
ee) Schutz von Berufsgeheimnisträgern	324
ff) Ergebnis	325
X. Weitere ausgewählte Kritikpunkte	325
1) Kritik am Namen	326
a) Begriff der Durchsuchung	326
b) Vergleich des Namens mit der in § 100b StPO geregelten Ermittlungsmaßnahme	327
c) Folgen der Fehlklassifizierung	328
d) Namensvorschläge in der Literatur	328
e) Eigene Stellungnahme	328
2) Umgehung durch präventive Vorschriften	329
a) Argumente gegen eine Umgehung von § 100b StPO	329
b) Umgehung aufgrund eines schwächeren Richtervorbehalts	330
aa) Richtervorbehalt bei einer Maßnahme nach § 49 BKAG	331
bb) Anordnungsbefugnis bei einer Maßnahme nach Art. 45 BayPAG	331
3) Geringer tatsächlicher Einsatz der Online-Durchsuchung	332
a) Anzahl der Anordnung und Durchführungen einer Maßnahme nach § 100b StPO	332

b) Einordnung und Bewertung der geringen Anzahl	332
4) Regeln zur statistischen Erfassung	334
XI. Überlegungen de lege ferenda	334
1) Katalog im Sinne des § 100b Abs. 2 StPO	334
2) Tat im Einzelfall besonders schwerwiegend (§ 100b Abs. 1 Nr. 2 StPO).....	335
3) Kernbereichsschutz	335
4) Schutz von Berufsgeheimnisträgern.....	335
5) Normvorschläge.....	335
XII. Voraussetzungen des § 100a Abs. 5 und Abs. 6 StPO im Rahmen des § 100b StPO	338

**Kapitel 8 Möglichkeiten der Überwachung von Cloud-Computing
und smarten Geräten mittels § 100a und § 100b StPO 339**

A. Die Überwachung von Cloud-Computing gemäß § 100a Abs. 1 Satz 1, 2, 3 StPO, § 100b StPO.....	339
I. Begriff, Arten und Verbreitung von Cloud-Computing	339
II. Ermittlungstaktischer Nutzen	340
III. Anwendbarkeit von § 100a und § 100b StPO auf Cloud-Computing	341
1) Unanwendbarkeit von § 100a Abs. 1 Satz 1 StPO	341
2) Überwachung gemäß § 100a Abs. 1 Satz 2 StPO	342
a) Überwachung der Synchronisation zwischen Gerät und Cloud-Server.....	342
aa) Gegen die Notwendigkeit einer Beteiligung von Menschen am Übertragungsvorgang.....	343
bb) Notwendigkeit der Beteiligung von mindestens einer Person am Übertragungsvorgang.....	343
cc) Für die Notwendigkeit einer Interaktion von mindestens zwei Personen am Übertragungsvorgang.....	344
dd) Eigene Stellungnahme.....	344
aaa) Übertragung sensiblerer Daten	345
bbb) Scheinbar grundrechtsfreundliche Auslegung	345
b) Direkter Zugriff auf Cloud-Speicher	346
3) Überwachung gemäß § 100a Abs. 1 Satz 3 StPO	346
a) Nutzung des Cloud-Speichers zur Sicherung von Kommunikationsdaten	347
b) Nutzung des Cloud-Speichers zur Individualkommunikation	347
4) Überwachung gemäß § 100b StPO	348

5) Zwischenergebnis	349
IV. Überlegungen de lege ferenda	349
B. Die Überwachung smarter Geräte mittels § 100a Abs. 1 Satz 1, 2, 3 und § 100b StPO.....	350
I. Intelligente KFZ – „Smart Cars“	350
1) Definition und Beispiele	350
2) Ermittlungstaktischer Nutzen	351
a) Bestehende gesetzliche Verpflichtungen zur Datenerhebung	351
b) Verwendungsmöglichkeiten der ausgeleiteten Daten.....	352
3) Eingriffsintensität einer verdeckten Infiltration	353
4) Überwachung gemäß § 100a Abs. 1 StPO.....	354
a) Überwachung der Synchronisation des Fahrzeugs mit dem Herstellerverserver.....	355
b) Überwachung der Kommunikation mittels eines Fahrzeugs....	355
c) Kritik an einer Infiltration eines intelligenten KFZ.....	356
aa) Gefahren einer Infiltration	356
bb) Verletzung von Art. 2 Abs. 2 Satz 2 und Art. 1 Abs. 1 GG	356
cc) Verstoß gegen den Wesentlichkeitsgrundsatz.....	357
5) Überwachung gemäß § 100b StPO	358
6) Überlegungen de lege ferenda	358
II. Alexa und andere virtuelle Assistenten am Beispiel von smarten Lautsprechern	359
1) Definition und Beispiele	359
2) Ermittlungstaktischer Nutzen	359
3) Eingriffsintensität einer verdeckten Infiltration und Überwachung	360
4) Überwachung gemäß § 100a Abs. 1 StPO.....	362
a) Überwachung der Synchronisation zwischen Betreiber-Server und smartem Lautsprecher	362
b) Überwachung von Servern und Cloud-Speichern bei der Nutzung von smarten Lautsprechern zur Kommunikation.....	362
5) Überwachung gemäß § 100b StPO	363
a) Anwendbarkeit auf die Benutzerhardware des virtuellen Assistenten	363
b) Anwendbarkeit auf Anbieter-Server.....	364

c) Verbot einer akustischen oder optischen Wohnraumüberwachung	364
6) Exkurs: Rechtfertigung einer akustischen Wohnraumüberwachung mittels smarter Lautsprecher auf Basis des § 100c StPO	365
a) Erforderlichkeit einer Nutzung smarter Lautsprecher für die Wohnraumüberwachung	365
b) Vorteile und Argumente für eine Nutzung von smarten Lautsprechern zur Durchführung einer Maßnahme nach § 100c StPO	365
c) Kritik an einer solchen Vorgehensweise	366
aa) Grammatikalische Auslegung des Begriffs „technisches Mittel“	366
bb) Historische Auslegung	366
d) Eigene Stellungnahme	367
aa) Systematische Auslegung	367
bb) Historische Auslegung	368
cc) Fehlende Aufnahme von § 100a Abs. 5 und Abs. 6 StPO entsprechenden Vorschriften	368
7) Zwischenergebnis	369
8) Kombination verschiedener Ermächtigungsgrundlagen zur akustischen Überwachung mittels smarter Lautsprecher	369
a) Mögliche Kombinationen	369
b) Eigene Stellungnahme	370
9) Überlegungen der lege ferenda	371
a) Keine freiwillige Aufgabe von Privatheit	372
b) Anordnungsvoraussetzungen einer neuen Regelung	372
10) Übertragbarkeit der Ergebnisse bezüglich der Überwachung von und mittels smarter Lautsprecher auf andere smarte Haushaltsgeräte	373
III. Smarte medizinische Geräte	374
1) Definition und Beispiele	374
2) Ermittlungstaktischer Nutzen	375
3) Eingriffsintensität	376
a) Vergleichbarkeit mit dem Einsatz eines Polygraphen	376
b) Eingriff in den Kernbereich der privaten Lebensführung	377
c) Parallelie Wertung des Gesetzgebers an anderer Stelle	377
d) Sonstige problematische Aspekte	377
4) Ergebnis	378

Kapitel 9 Zusammenfassung der Ergebnisse und Normvorschläge	381
A. Zusammenfassung der Ergebnisse	381
I. Infiltration von informationstechnischen Systemen.....	381
II. Bedeutung von Gefahren für die allgemeine IT-Sicherheit durch verdeckte digitale Ermittlungsmaßnahmen.....	383
III. Gesetzgebungsverfahren des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens	384
IV. § 100a und § 100b StPO als wichtige verdeckte digitale Ermittlungsmaßnahmen.....	385
V. Möglichkeiten der Überwachung von Cloud-Computing und smarten Geräten mittels § 100a und § 100b StPO	400
B. Übersicht über alle Normvorschläge	404