

Inhaltsverzeichnis

Einleitung	15
<i>1. Kapitel</i>	
Der Begriff des Persönlichkeitsprofils	19
A. Bisherige Erkenntnisse über das Persönlichkeitsprofil	19
I. Übersicht über die Rechtsprechung	20
II. Erkenntnisse der Persönlichkeitsspsychologie	22
B. Eine Definition des Persönlichkeitsprofils	23
<i>2. Kapitel</i>	
Entwicklung eines Rechtsmaßstabs für die Gefahr der Bildung von Persönlichkeitsprofilen	25
A. Der Schutz des Kernbereichs der privaten Lebensgestaltung als verfassungsrechtlicher Maßstab	25
I. Die Gefahr der Bildung von Persönlichkeitsprofilen als Teil des Kernbereichs privater Lebensgestaltung	26
1. Einordnung der Rechtsprechung	26
2. Gesamtschau der Daten	27
3. Persönlichkeitsprofilbildung als Ergebnis einer Rundumüberwachung	30
4. Abgrenzung zum Verhältnismäßigkeitsgrundsatz	33
5. Zwischenergebnis	33
II. Entwicklung des Kernbereichs privater Lebensgestaltung in der Rechtsprechung	34
1. Das Elfes-Urteil	34
2. Die (zweite) Tagebuch-Entscheidung	34
3. Verfassungsbeschwerde zur Wohnraumüberwachung	38
4. Urteil zum IT-Grundrecht	42
5. Urteil zum BKAG	44
III. Analyse der Rechtsprechung im Hinblick auf die Gefahr der Bildung von Persönlichkeitsprofilen	46
IV. Weitreichender Maßstab über Art. 1 Abs. 1 GG als das zweistufige Schutzkonzept des Bundesverfassungsgerichts	47
V. Gefahrenbegriff	49

B.	Unionsrechtlicher Maßstab	50
I.	Möglichkeiten zur Einbeziehung des Unionsrechts	51
II.	Verstoß gegen Unionsrecht: Die Gefahr der Bildung von Persönlichkeitsprofilen bei der Online-Durchsuchung	53
1.	Art. 8, 7 Grundrechte Charta	54
2.	Richtlinie (EU) 2016/680 [DSRL-JI]	57
a)	Verstoß gegen allgemeine Verarbeitungsgrundsätze	58
b)	Verstoß gegen das Verbot des Profilings	60
3.	E-privacy Richtlinie 2002/58	61
III.	Gleichrangiges Schutzniveau von grundgesetzlichen Grundrechten und der Grundrechtecharta	62
 <i>3. Kapitel</i>		
Die Online-Durchsuchung		66
A.	Historische Entwicklung	67
I.	Erste Überlegungen auf Bundesebene	67
1.	Online-Durchsuchung auf einer Mailbox	67
2.	Erste Erwähnung einer Online-Durchsuchung	69
3.	Online-Durchsuchung als klassische Durchsuchung?	70
4.	Kehrtwende am Bundesgerichtshof	71
5.	Das „Programm zur Stärkung der Inneren Sicherheit“	72
6.	Zusammenfassung	73
II.	Entwicklung in der Literatur	74
1.	Besteht eine Ermächtigungsgrundlage für die Online-Durchsuchung?	74
2.	Online-Durchsuchung als Eingriff in Art. 13 GG?	75
3.	Zusammenfassung	76
III.	Verfassungsschutzgesetz Nordrhein-Westfalen	77
1.	Gesetzgebungsverfahren	78
a)	Kontroversen um den Gesetzesentwurf	78
b)	Unklarheiten bei der Begriffsbestimmung	80
2.	Entscheidung des Bundesverfassungsgerichts	81
a)	Der „Zugriff auf informationstechnische Systeme“	82
b)	Das IT-Grundrecht	84
c)	Kritik in der Literatur	87
d)	Zwischenresümee zur ersten Normierung der Online-Durchsuchung	88
IV.	Bundeskriminalamtsgesetz	89
1.	Erstes Gesetzgebungsverfahren	90
2.	Entscheidung des Bundesverfassungsgerichts	93
3.	Das neue BKAG	96
V.	Einführung der Online-Durchsuchung in die Strafprozessordnung	99

1. Gesetzgebungsverfahren	99
a) Anhörung der Sachverständigen	100
b) Inkrafttreten der Maßnahme	102
2. Verfassungsbeschwerden	103
VI. Zwischenresümee	104
B. Rechtsrahmen der Online-Durchsuchung	106
I. Ermächtigungsgrundlage	107
1. Das informationstechnische System	107
a) Der Ursprung des Begriffs des IT-Systems	108
b) Der Begriff des IT-Systems des Bundesverfassungsgerichts	109
c) Der strafprozessuale Begriff des IT-Systems	109
2. Daten	112
a) Arten der zu gewinnenden Daten	112
aa) Daten als Äquivalent zur „klassischen“ Durchsuchung	112
bb) Profiling-Daten	113
b) Datengewinnung mittels Peripheriegeräten	116
aa) Aktivierung der Peripheriegeräte durch die Ermittlungsbehörden	116
bb) Die passive Kenntnisnahme durch Peripheriegeräte	117
cc) Aktivierung des Peripheriegeräts durch das Gerät selbst	119
c) Daten aus spezielleren Ermittlungsmaßnahmen	119
aa) Quellen-TKÜ	120
bb) Wohnraumüberwachung	121
(1) Optische Wohnraumüberwachung	121
(a) Möglichkeit des Eingriffs in Art. 13 GG	122
(b) Eingriff durch Kenntnisnahme von Videotelefonie .	124
(c) Eingriff durch die Erhebung von gespeicherten Videos	124
(aa) Videoaufnahmen während des Anordnungszeitraums	125
(bb) Gespeicherte Videos	125
(d) Zusammenfassung	126
(2) Akustische Wohnraumüberwachung	126
(a) Das Verhältnis zwischen akustischer Wohnraumüberwachung und Online-Durchsuchung	127
(b) Notwendigkeit der Anordnung einer akustischen Wohnraumüberwachung bei passiver Kenntnisnahme der Mikrofone?	127
(c) Verletzung des Zitiergebots	129
(cc) Beschlagnahme des IT-Geräts	131
(dd) Weitere Ermittlungsmaßnahmen	134
d) Zwischenergebnis	135
3. Verdachtsgrad	135

4. Katalogtat	137
a) Die Funktionsfähigkeit der Strafrechtspflege als Rechtsgut von Verfassungsrang	139
b) Besondere Schwere der Straftat	141
aa) Überragend wichtige Rechtsgüter im Strafprozessrecht	142
(1) Betreiben krimineller Handelsplattformen	142
(2) Bildung einer kriminellen Vereinigung	143
(3) Geld- und Wertzeichenfälschung	144
(4) Verbreitung, Erwerb und Besitz von kinderpornografischen Inhalten	144
(5) Bandendiebstahl und schwerer Bandendiebstahl	145
(6) Raub und räuberische Erpressung	145
(7) Gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei	146
(8) Besonders schwerer Fall der Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte	147
(9) Computerbetrug	147
(10) Besonders schwerer Fall der Bestechlichkeit	148
(11) Straftatbestände aus dem Asyl- und Aufenthaltsgesetz	148
(12) Straftatbestände aus dem Betäubungsmittelgesetz	149
(13) Straftatbestände aus dem Gesetz über die Kontrolle von Kriegswaffen	149
(14) Straftatbestände aus dem Waffengesetz	150
bb) Weitere Straftaten	150
c) Zwischenergebnis	150
5. Schwere der Tat auch im Einzelfall	153
6. Subsidiaritätsklausel	154
a) Das Verhältnis zur akustischen Wohnraumüberwachung	155
b) Verfassungskonforme Auslegung der Subsidiaritätsklausel	156
c) Zwischenergebnis	157
7. Verhältnismäßigkeit	158
II. § 100b Abs. 3 StPO – Betroffene*r einer Maßnahme	158
III. § 100b Abs. 4 i. V. m. § 100a Abs. 5, 6 StPO – technische Anforderungen	159
1. Das Tatbestandsmerkmal der technischen Umsetzbarkeit	160
2. Schutz gegen unbefugte Dritte	161
3. Schutz der kopierten Daten	161
4. Zwischenfazit	162
IV. § 100e StPO – Verfahren im Vergleich zur akustischen Wohnraumüberwachung	162
V. Weitere Verfahrensregelungen	163
C. Zwischenergebnis	164

*4. Kapitel***Kernbereichsschutz bei der Online-Durchsuchung de lege lata** 167

A. Erhebungsebene	169
I. § 100d Abs. 1 StPO – Erhebungsebene: keine Erhebung von allein kernbereichsrelevanten Daten	169
II. § 100d Abs. 3 S. 1 StPO – Vermeidung der Erhebung von kernbereichsrelevanten Daten	170
1. Durch Live-Überwachung	170
2. Durch die Verwendung von Suchbegriffen	171
3. Durch Verbot der Nutzung von Peripheriegeräten	172
III. Zwischenergebnis	172
B. Verwertungsebene	174
I. § 100d Abs. 2 StPO – Verfahrensvorschriften	174
II. § 100d Abs. 2 S. 1 StPO – Absolutes Verwertungsverbot	174
III. § 100d Abs. 3 S. 2, 3 StPO – Entscheidung durch eine unabhängige Stelle	175
1. Bindungswirkung und Gewaltenteilung	175
2. Umfang der Bindungswirkung	177
C. Zwischenresümee	177

*5. Kapitel***Fazit: Unzureichende Regelungen zur Begrenzung der Datenmenge** 179

A. Additiver Grundrechtseingriff	180
B. Ebene des Kernbereichsschutzes	182
I. Verfassungs- und unionsrechtskonforme Auslegung des § 100d Abs. 1 StPO	183
II. § 47 Nr. 3 BDSG	186
III. Unterbrechung der Maßnahme	186
IV. Exkurs: Verwendung intelligenter Systeme in der Zukunft? Ergebnis und Ausblick	187
V. Die Rolle des § 100e Abs. 3 S. 2 Nrn. 3, 4 StPO	188
VI. Erweiterung der Vorschriften	189
1. Ergänzung des § 100d Abs. 1 StPO	190
2. Normierung der Unterbrechung der Maßnahme	190
Ergebnis und Ausblick	192

Literaturverzeichnis	194
-----------------------------------	-----

Stichwortverzeichnis	201
-----------------------------------	-----