

Inhaltsverzeichnis

A. Einleitung	C 9
B. Bestandsaufnahme: Sicherstellung und Auswertung von IT-Geräten	C 13
I. Smartphones, Personal Computer, Laptops, Tablets und Co. als informationstechnische Systeme	C 13
II. Einfache und komplexe informationstechnische Systeme	C 13
III. Regelungen zum geheimen Zugriff auf IT-Geräte	C 16
IV. Sicherstellung und Beschlagnahme von IT-Geräten auf Grundlage der §§ 94 ff. StPO	C 18
1. Materielle Voraussetzungen der Sicherstellung nach § 94 StPO	C 19
a) Gegenstände als Beweismittel	C 19
b) Beweisrelevanz des Gegenstandes	C 21
c) Verhältnismäßigkeit der Sicherstellung	C 22
aa) Insbesondere: Erforderlichkeit	C 23
bb) Insbesondere: Angemessenheit	C 24
cc) Sicherstellungsverbote, insbesondere Kernbereichsschutz	C 26
2. Formelle Anforderungen an die Sicherstellung	C 28
3. Ausnahme: Zulässigkeit geheimer Beschlagnahmen, § 95a StPO	C 29
V. Einfache Durchsicht von Akten und elektronischen Speichermedien, § 110 StPO	C 31
1. Zweck und Anwendungsbereich der Durchsicht nach § 110 StPO	C 31
2. Durchführung der Sichtung	C 32
3. Dauer der Durchsicht	C 33
VI. Erweiterte Durchsicht, § 110 Abs. 3 S. 2 StPO	C 34
1. Hintergrund der Vorschrift	C 34
2. Charakter der Maßnahme, Voraussetzungen der Online-sichtung und betroffene Daten	C 35
VII. Zwischenergebnis	C 38
C. Grundrechtsdimension des offenen Zugriffs auf IT-Geräte: betroffene Grundrechte	C 40
I. Unterbeleuchtete Debatte über die verfassungsrechtliche Tragweite der Beschlagnahme von komplexen IT-Geräten ..	C 40
II. Von der Sicherstellung und der Auswertung betroffene Grundrechte	C 42
1. Eingriff in Art. 14 Abs. 1 GG, Eigentumsgarantie	C 42

2. Eingriff in Art. 13 GG, Unverletzlichkeit der Wohnung	C 43
3. Eingriff in Art. 10 GG, Fernmeldegeheimnis	C 44
4. Eingriff in die informationelle Selbstbestimmung, Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG	C 48
5. Beschlagnahme als Eingriff in das IT-Grundrecht, Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG	C 50
a) Grundsatzfrage	C 50
b) Neue Persönlichkeitsgefährdungen als Anlass für die Entwicklung des IT-Grundrechts	C 50
c) Schutzbereich	C 53
aa) Sachlicher und personeller Schutzbereich	C 53
bb) Keine Begrenzung auf präventive und heimliche Eingriffe (Infiltration)	C 55
(1) Keine Begrenzung des IT-Grundrechts auf präventiv ausgerichtete Maßnahmen	C 55
(2) Geltung des IT-Grundrechts auch für offene Zugriffe auf IT-Geräte	C 56
(3) Subsidiarität des IT-Grundrechts bei offenen Zugriffen	C 60
(4) Zwischenergebnis	C 63
D. Regelungs- und Schutzdefizite bei der Beschlagnahme von IT-Geräten	C 64
I. Einleitung	C 64
II. Notwendigkeit einer Sonderregelung für die Beschlagnahme von IT-Geräten	C 65
III. Keine Beschlagnahme von komplexen IT-Geräten zur Aufklärung leichter Straftaten	C 69
1. Bisher: Keine Beschränkung der Beschlagnahme von IT-Geräten auf bestimmte Delikte	C 69
2. Präventive Online-Durchsuchung nur bei konkreter Gefahr für überragend wichtige Rechtsgüter	C 70
3. Keine Übertragung der Vorgaben zur Online-Durchsuchung auf die Beschlagnahme von IT-Geräten	C 72
4. Keine Beschlagnahme von komplexen IT-Geräten zur Aufklärung von Straftaten unterhalb mittlerer Kriminalität	C 76
IV. Beschlagnahme nur bei qualifiziertem Verdacht einer Beweisrelevanz	C 80
V. Eigenständige Regelung zum Kernbereichsschutz	C 82
1. Zugriff auf kernbereichsrelevante Daten beim offenen Zugriff	C 82
2. Notwendigkeit einer positiv-rechtlichen Kernbereichsregelung für „verletzungsgeneigte“ Maßnahmen	C 84

VI. Richtervorbehalt und rechtsschutzbezogene Defizite	C 87
VII. Regelung zum Umgang mit Zufallsfunden	C 90
VIII. Subsidiarität der Gerätemitnahme gegenüber einer Daten- spiegelung	C 93
IX. Fristen für die Rückgabe des IT-Geräts und unverzügliche Aushändigung einer Datenkopie	C 96
X. Schutz der Integrität des IT-Geräts und der Daten vor Ver- änderungen sowie Dokumentation	C 98
E. Kurzfazit	C 100
F. Zusammenfassung der Thesen	C 101