Inhaltsverzeichnis

Vorwort V

Einleitung 1

A. Einführung 1
I. Die konkreten Fragestellungen dieser Arbeit 1
1. Übergeordnete Fragestellungen 1
2. Einzelfragen im Überblick 2
3. Nicht beantwortete Fragen / Grenzen der Untersuchung 3
II. Methodik der Untersuchung 4

B. Staatlicher Zugriff auf elektronisch gespeicherte Daten vor dem Hintergrund zweier Grundsatzurteile des BVerfG 5

C. § 110 Abs. 3 StPO als Reaktion auf neue Formen der EDV 8
I. Offenheit und Heimlichkeit der Durchsuchung 12
II. Gesetzesbegründung der Bundesregierung zu § 110 Abs. 3 StPO (a. F.) 16
III. Änderungsbegründung des Rechtsausschusses zu § 110 Abs. 3 StPO 20
IV. Weitere Verheimlichung durch Zurückstellung der Benachrichtigung des Beschuldigten gem. § 110 Abs. 4 i. V. m. § 95a StPO 24
V. Zusammenfassung / Problemaufriss 26

D. Begriffe 30
I. Online-Durchsuchung in Abgrenzung zur Netzwerkdurchsicht 31
1. Exkurs: Gesetzgebungsgeschichte des § 100b StPO 32
2. Vielgestaltigkeit der „Online-Durchsuchung“ 35
3. Abgrenzung des § 110 Abs. 3 S. 2 StPO zu anderen Formen der „Online-Durchsuchung“ 37
4. § 110 Abs. 3 S. 2 StPO: Die „Netzwerkdurchsicht“ 40
II. Heimliche Maßnahmen, Verdeckte Maßnahmen / Offene Maßnahmen 42
III. Begriffe aus der Informationstechnik und Informationstechnologie 46

Bibliografische Informationen
http://d-nb.info/1251140203

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

1. EDV und IT 47
2. Daten und Informationen 47
a) Der Unterschied zwischen Daten und Informationen ... 47
b) Personenbezogene Daten 50
c) Bestandsdaten; Verkehrsdaten; Inhaltsdaten; Metadaten 52
3. Speichermedium; Computersystem; Informationstechnisches System 55

E. Weiterer Gang der Untersuchung 58

F. Zitierweise der Normen (§ 110 Abs. 1 und Abs. 3 S. 1, 2 StPO) 60

Kapitel 1: Einordnung des § 110 Abs. 3 S. 2 StPO im Gefüge zwischen physischem und virtuellem Raum 61

Kapitel 2: Die Durchsicht lokaler informationstechnischer Systeme gemäß § 110 Abs. 3 S. 1 StPO 67

A. Durchsuchung als Ausgangspunkt für die Durchsicht informationstechnischer Systeme 68
I. Erscheinungsformen der Durchsuchung 68
II. Abgrenzung zwischen § 102 StPO und § 103 StPO 70
1. Gewahrsam und Mitgewahrsam 72
2. Überwiegende Ansicht: Mitgewahrsam Verdächtiger als „Schlüssel" zu § 102 StPO 73
3. Gegenansicht: Mitgewahrsam Unverdächtiger als Sperre des § 102 StPO 75
4. Folgerungen mit Blick auf die Durchsicht informationstechnischer Systeme 80

B. Durchsicht eines lokalen informationstechnischen Systems gemäß § 110 Abs. 3 S. 1 StPO 81
I. Allgemeines zur Durchsicht gemäß § 110 Abs. 1 StPO 82
II. Mitnahme zur Durchsicht 85
1. „Vorläufige Sicherstellung" 87
2. Anfertigung von Datenkopien bei der Mitnahme zur Durchsicht 88
a) Ausmaß und Umfang der Datenkopien 89
b) Komplettsicherung der Daten zur Erhaltung des Beweiswerts 95
c) Rückgriff auf den Datenträger oder das gesamte informationstechnische System 99
d) Zwischenergebnis und Ausblick zur Problematik von (vollständigen) Datenkopien 101

3. Anwesenheitsrecht und drohende Heimlichkeit der Maßnahme bei der Mitnahme zur Durchsicht 104
4. Rechtsgrundlage der Mitnahme zur Durchsicht 107
a) Bedeutung des § 110 Abs. 2 S. 2 StPO 109
b) Bedeutung des § 110 Abs. 3 S. 3 StPO 110
c) Bedeutung des § 110 Abs. 4 StPO 111
d) Bedeutung der §§ 94 ff. StPO 112
e) Annexkompetenz zu § 110 Abs. 1 StPO und Abs. 3 S. 1 StPO als Grundlage für Grundrechtseingriffe? 114
III. Betroffene Grundrechte bei der Durchsicht informationstechnischer Systeme 119
1. Unverletzlichkeit der Wohnung 119
a) Art. 13 GG als spezielles Datenschutzrecht 120
b) Art. 13 GG – Kein ausschließlicher Maßstab für Datenerhebungen innerhalb der Wohnung 122
2. IT-Grundrecht 127
a) Allgemeines 129
b) Vertraulichkeit und Integrität informationstechnischer Systeme 131
aa) Informationstechnisches System 131
bb) Vertraulichkeit und Integrität 140
cc) Zwischenergebnis 144
c) Einsatz von Spionagesoftware im Gegensatz zu einfachen Zugriffen auf das System 145
aa) Ausgangspunkt des Urteils zur Online-Durchsuchung 146
bb) Persönlichkeitsschutz als Leitlinie des IT-Grundrechts 148
cc) Einschub: Integritätsverletzung als Intensivierung des Eingriffs 153
dd) Kein Eingriff in den Schutzbereich bei Datenerhebungen „auf dem technisch dafür vorgesehenen Weg“? 155
ee) Zusätzliches Argument aus dem E-Mail-Beschluss des BVerfG (BVerfGE 124, 43)? 160
ff) Zwischenergebnis 162
d) Heimliche Zugriffe im Gegensatz zu offenen Zugriffen auf das System 163
aa) Ausgangspunkt beim Urteil zur Online-Durchsuchung 164
bb) Die Formulierung „insbesondere“ als Argument für die Annahme eines Eingriffs in das IT-Grundrecht auch bei offenen Zugriffen auf informationstechnische Systeme 165

cc) Grundrechtsdogmatik: Schutz durch IT-Grundrecht unabhängig von Eingriffsmodalität 168
dd) Nochmal: Der E-Mail-Beschluss des BVerfG (BVerfGE 124, 43) 170
ee) Zwischenergebnis 171
e) Längerfristige Überwachung im Gegensatz zu einmaligem Zugriff auf das System 171
f) Präventives Staatshandeln im Unterschied zu repressivem Staatshandeln 173
g) Spätere Rechtsprechung des BVerfG: Keine Anwendung des IT-Grundrechts? 178
h) Zwischenergebnis & Folgerungen aus der Anwendbarkeit des IT-Grundrechts 182
3. Das Recht auf informationelle Selbstbestimmung im Verhältnis zum IT-Grundrecht 183
4. Fernmeldegeheimnis 190
5. Eigentum 194
6. Pressefreiheit und Rundfunkfreiheit 197
7. Berufsfreiheit 199
8. Wissenschaftsfreiheit 202
9. Religionsfreiheit 204
10. Schutz von Ehe und Familie 205
11. Zusammenfassend: Anwendbare Grundrechte und Konkurrenzen 205
12. Zwischenergebnis 207
IV. Kriterien zur Bestimmung der Verhältnismäßigkeit und der Eingriffsintensität von Durchsichten informationstechnischer Systeme 207
1. Legitimer Zweck von Durchsichten informationstechnischer Systeme 208
2. Geeignetheit von Durchsichten informationstechnischer Systeme 210
3. Erforderlichkeit von Durchsichten informationstechnischer Systeme 212
a) Mitnahme / Umfang der mitgenommenen und gesichteten Daten 212
b) Dauer der Durchsicht 213
c) Erforderlichkeit der Durchsicht informationstechnischer Systeme im Einzelfall 214
4. Angemessenheit / Verhältnismäßigkeit im engeren Sinne von Durchsichten informationstechnischer Systeme 214
a) Datenmenge 216

b) Art und Vielfalt der Daten 217
c) Dauer der Ausforschung 219
d) Heimlichkeit des Zugriffs 220
e) Streubreite 222
f) Anzahl der beeinträchtigten Grundrechte 224
g) Einschüchterung & Gesamtgesellschaftliche Auswirkungen 226
5. Zwischenergebnis und Bewertung 229
V. Kernbereich privater Lebensgestaltung 230
1. Schutzgehalt des unantastbaren Kernbereichs privater Lebensgestaltung 230
2. Das zweistufige Schutzkonzept des BVerfG 234
a) Erste Stufe: Vermeidung von Kernbereichsberührungen in der Erhebungsphase 234
b) Zweite Stufe: Schutz in der Auswertungsphase durch Verfahrensvorschriften 235
c) Relevanz für die Durchsicht nach § 110 Abs. 3 S. 1 StPO 236
d) Ist eine Gefährdung des Kernbereichs privater Lebensgestaltung nur zum Schutz überragend wichtiger Rechtsgüter zulässig? 237
3. Bewertung des zweistufigen Schutzkonzepts 243
a) Unschärfe und Relativierung des Kernbereichs durch einzelfallabhängige Zuordnungnen von Inhalten als kernbereichsrelevant 243
b) Zweistufigkeit des Schutzes als Schwächung und Aufweichung des Kernbereichs privater Lebensgestaltung 246
4. Verstoß gegen die Pflicht zur gesetzlichen Regelung des Kernbereichsschutzes? 250
5. Analoge Anwendung des Kernbereichsschutzkonzepts aus § 100d Abs. 1 bis Abs. 3 StPO auf Durchsichten informationstechnischer Systeme 254
6. Zwischenergebnis 256
VI. Rundumüberwachung / Totalausforschung / Persönlichkeitsprofile 257
VII. Begleitmaßnahmen zur Durchsicht informationstechnischer Systeme 262
1. Inbetriebnahme des informationstechnischen Systems 262
2. Passwörter, Verschlüsselungen und staatliches Hacking 264
a) Herausgabeverlangen und Zeugnispflicht bezüglich Passwörter 265
b) Knacken des Passworts; Hacking; Aufspielen von Software 268

VIII. Zufallsfunde gemäß § 108 Abs. 1 StPO und das Problem der systematischen Suche nach Zufallsfunden (fishing expeditions) 272
IX. Eingriffe in Rechte Dritter bei der Durchsicht lokaler informationstechnischer Systeme 274
X. Reformvorschläge zur Durchsicht lokaler informationstechnischer Systeme gemäß § 110 Abs. 3 S. 1 StPO 276
1. Grundrechtssensitivität: Zusammenfassung der Probleme ... 276
2. Einordnung des § 110 Abs. 3 S. 1 StPO als echte Eingriffsgrundlage 278
3. Reformvorschläge zu tatbestandlichen Eingriffsschwellen und Schutzvorschriften 279
a) Schaffung eines Anlasstatenkatalogs 280
b) Übertragung der Schwellen des § 103 Abs. 1 S. 1 StPO ... 286
c) Einfügen einer Subsidiaritätsklausel 286
d) Ausdrückliche Regelung der Mitnahme zur Durchsicht 291
4. Gesetzliche Regelung des Kernbereichsschutzes 292
5. Ausdrückliche Regelung des Anwesenheitsrechts bei Mitnahme zur Durchsicht? 295
6. Ermächtigung zur Installation forensischer Software bzw. zur Überwindung von Verschlüsselungen 296
7. Spezielle gesetzliche Regelung zur Löschung nicht mehr benötigter Daten 296
8. Einschränkung des § 108 Abs. 1 S. 1 StPO? 300
XI. Zusammenfassung der wichtigsten Ergebnisse zu § 110 Abs. 3 S. 1 StPO 301

Kapitel 3: Die Durchsicht externer informationstechnischer Systeme gemäß § 110 Abs. 3 S. 2 StPO 305

A. Anwendungsbereich des § 110 Abs. 3 S. 2 StPO 306
I. Ausgangspunkte und Zielobjekte der Durchsicht: „Speichermedien" / „Computersysteme" / Informationstechnische Systeme 307
1. Webspace, Filehosting, Server: Der Grundfall von Speicherplatz im Netz 311
2. Cloud Computing 318
a) Definition 319
b) Erscheinungsformen 320
c) Private Clouds und Public Clouds 321
d) Virtualisierung: Verstreutheit der Daten 323
e) Synchronisierung der Cloud-Inhalte mit dem lokalen informationstechnischen System 324

f) Zwischenergebnis 326
3. E-Mail-Konten 327
a) Anwendbarkeit des § 110 Abs. 3 S. 2 StPO vor dem Hintergrund der Rechtsprechung des BVerfG zu Eingriffen in das Fernmeldegeheimnis (BVerfGE 124, 43) 327
b) Grundrechtlicher Maßstab: IT-Grundrecht oder Fernmeldegeheimnis? 333
c) Eingriff in das IT-Grundrecht durch Zugriff auf Ausgangssystem des Beschuldigten 341
4. Profile auf Social-Media-Plattformen und ähnlichen Angeboten 342
5. Ergebnisse 347
II. Tatbestandsvoraussetzung: Faktische Möglichkeit des Zugriffs auf externe Systeme 348
1. Die (fehlende) Bedeutung der Zugriffsberechtigung des Durchsuchten 349
2. Möglichkeit des Zugriffs durch Vernetzung zweier Systeme 353
a) Herstellen der Netzwerkverbindung erst durch die Ermittler 354
b) Überwindung von Zugangssperren, Passwörtern und Verschlüsselungen / Brute Force 355
III. Tatbestandsvoraussetzung: Befürchtung des Verlustes der gesuchten Daten 359
IV. Zulässigkeit der Überwachung oder des mehrmaligen Zugriffs auf das externe System? 361
V. Transnationale Datenzugriffe (transborder searches) 366
1. § 110 Abs. 3 S. 2 StPO als Ermächtigung zu transnationalen Ermittlungen? 368
2. Zulässigkeit der Netzwerkdurchsicht bei Zweifeln über den Standort des Systems? 373
3. Ausblick: Erweiterung der Convention on Cybercrime? 375
4. Ausblick: e-evidence 377

B. Weitere Besonderheiten der Durchsicht externer informationstechnischer Systeme gemäß § 110 Abs. 3 S. 2 StPO 378
I. Kein physischer Zugriff auf die Hardware des externen Systems möglich 379
II. Verhältnismäßigkeit: Schwächerer Grundrechtsschutz für vernetzte Systeme? 380

C. Eingriffe in Rechte Dritter bei der Durchsicht externer informationstechnischer Systeme gemäß § 110 Abs. 3 S. 2 StPO 385
I. Betroffene Grundrechte des Dritten 390

1. Unverletzlichkeit der Wohnung 390
2. IT-Grundrecht 395
3. Fernmeldegeheimnis in Konkurrenz zum IT-Grundrecht 397
II. Netzwerkdurchsicht als Durchsuchung beim Dritten? 402
III. Heimlichkeit des Zugriffs gegenüber dem Dritten 408
IV. Zwischenergebnis 418

D. Reformvorschläge zur Durchsicht externer informationstechnischer Systeme gemäß § 110 Abs. 3 S. 2 StPO 419
I. Grundrechtssensitivität: Zusammenfassung der Probleme 420
II. § 110 Abs. 3 S. 2 StPO als Eingriffsgrundlage und Spezialfall des § 110 Abs. 3 S. 1 StPO 421
III. Anlasstatenkatalog: Übernahme des § 100b Abs. 2 StPO? 423
IV. Subsidiaritätsklausel: Möglichkeiten zur Übernahme des § 100b Abs. 3 S. 2 StPO per Gesetzesreform de lege ferenda und per verfassungskonformer Auslegung de lege lata 426
V. Einschränkung des § 108 Abs. 1 S. 1 StPO zum Schutz unbeteiligter Dritter 430
VI. Pflicht zur Regelung des Kernbereichsschutzes aufgrund heimlicher Durchsicht? 432

E. Zusammenfassung der wichtigsten Ergebnisse zu § 110 Abs. 3 S. 2 StPO 435

Kapitel 4: Ergebnis und Ausblick 439

A. Zusammenfassung der Ergebnisse 439

B. Ausblick: Offene Fragen und ungelöste Probleme 442
I. Die Frage nach dem „richtigen" Grundrecht 443
1. Anwendung des IT-Grundrechts auf offene Durchsichten ... 443
2. Verhältnis zwischen IT-Grundrecht und informationeller Selbstbestimmung 443
3. Verhältnis zwischen IT-Grundrecht und Fernmeldegeheimnis 444
II. Das Dilemma über den Umfang der Datensicherung und -auswertung 444
III. Die Revelanz des Standorts des externen Speichermediums 446
IV. Der Umgang mit elektronisch gespeicherten Daten allgemein ... 448
V. Individueller Grundrechtsschutz vs. Effektive Strafverfolgung 448

Literaturverzeichnis 451

Sachregister 473