

Inhaltsverzeichnis

A. Einleitung	21
I. Die Überwachung von Telekommunikationsinhalten	21
II. Gegenstand und Gang der Untersuchung	23
B. Grundlagen	26
I. Die historische Entwicklung und Technik des Internets und der E-Mail-Kommunikation	26
1. Die historische Entwicklung von Internet und E-Mail	26
2. Technische Grundlagen der Datenübertragung im Internet	35
3. Technische Grundlagen des E-Mail-Verkehrs	47
4. Sicherheit des Mailverkehrs und Zugriffsmöglichkeiten der Ermitt- lungsbehörden	54
II. Entwicklung und Bedeutung der Regelungen zur Telekommunikations- überwachung	55
III. Inhaltsdaten als Gegenstand der Überwachung	59
1. Abgrenzung zu weiteren Telekommunikationsdaten	59
2. Inhaltsdatenbegriff	61
IV. Die vier Phasen der E-Mail-Kommunikation und die mit ihnen verbun- denen, rechtlichen Folgen	62
1. Das klassische Drei-Phasen-Modell	64
2. Erweiterung um eine vierte Phase	65
C. Der verfassungsrechtliche Schutz der Inhaltsdaten während der ver- schie- denen Phasen der E-Mail-Kommunikation	68
I. Schutz im Vorfeld der Übertragung?	68
II. Der verfassungsrechtliche Schutz der Inhaltsdaten der E-Mail während der Übertragung in den Phasen 1 und 3	71
1. Der verfassungsrechtliche Schutz durch Art. 10 Abs. 1 GG	71
a) Gemeinsamer Schutzzweck der Grundrechte des Art. 10 Abs. 1 GG	72
b) Besondere Nähe zum allgemeinen Persönlichkeitsrecht und zur Meinungsfreiheit	72
c) Gewährleistung einer Privatheit auf Distanz	73
d) Verbot von Kommunikationsformen	74
2. Zuordnung der E-Mail-Kommunikation zu den Schutzgewährleistun- gen des Art. 10 Abs. 1 GG	75
a) Verhältnis der Grundrechte des Art. 10 Abs. 1 GG	75
b) Anwendbarkeit des Briefgeheimnisses	77

3. Anwendbarkeit des Fernmeldegeheimnisses	79
a) Terminologie	79
b) Schutzbereich des Fernmeldegeheimnisses	80
c) Zeitliche Reichweite des Schutzes des Fernmeldegeheimnisses bei der E-Mail-Kommunikation in den Phasen 1 und 3	85
4. Sonderprobleme des verfassungsrechtlichen Schutzes der E-Mail-Kommunikation durch das Fernmeldegeheimnis	87
a) Mangelnde Schutzfähigkeit aufgrund technischer Anfälligkeit?	87
b) Versendung an eine Vielzahl von Empfängern	90
c) Entwicklungsoffenes Auffanggrundrecht	92
5. Grundrechtsträger und -adressaten	92
6. Eingriffe in den Schutzbereich	94
7. Rechtfertigung von Eingriffen in den Schutzbereich	95
8. Paralleler Schutz der E-Mail-Kommunikation in den Phasen 1 und 3 durch weitere Grundrechte?	98
a) Anwendbarkeit des Postgeheimnisses	99
b) Schutz durch das Recht auf Unverletzlichkeit der Wohnung des Art. 13 Abs. 1 GG	102
c) Schutz durch das allgemeine Persönlichkeitsrecht in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung und als Recht auf Gewährleistung der Vertraulichkeit und Integ- rität informationstechnischer Systeme nach Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG	105
III. Der verfassungsrechtliche Schutz der Inhaltsdaten der E-Mail während der Zwischenspeicherung (Phase 2)	106
1. Definition der Zwischenspeicherung	107
2. Der verfassungsrechtliche Schutz gemäß Art. 10 Abs. 1 GG	108
a) Anwendbarkeit des Fernmeldegeheimnisses	108
aa) Beendigung des Schutzes durch das Fernmeldegeheimnis während der Zwischenspeicherung?	108
bb) Die Entwicklung in Rechtsprechung und Literatur	109
(1) Die Mailboxentscheidung des BGH vom 31. Juli 1995	110
(2) Ablehnung eines Schutzes durch das Fernmeldegeheim- nis in Rechtsprechung und Literatur	113
(a) Die Drei-Phasen-Theorie aus verfassungsrechtlichem Blickwinkel	113
(b) Anwendbarkeit des Briefgeheimnisses?	116
(3) Einheitlichkeit des Übermittlungsvorgangs (Einheitlich- keits- bzw. Homogenitätstheorie)	117
(4) Die Entwicklung der Rechtsprechung des Bundesverfas- sungsgerichtes	119
(5) Die Entscheidung des Bundesverfassungsgerichtes vom 16. Juni 2009	122
(a) Sachverhalt	122
(b) Entscheidungsinhalt	125

b) Stellungnahme	127
c) Anwendbarkeit des Briefgeheimnisses	131
3. Verfassungsrechtlicher Schutz der zwischengespeicherten Nachricht durch weitere Grundrechte?	131
IV. Der verfassungsrechtliche Schutz der Inhaltsdaten der E-Mail während der Endspeicherung (Phase 4)	133
1. Definition der Endspeicherung	133
2. Besondere Gefahren der dauerhaften Speicherung von E-Mails in E-Mail-Postfächern	137
3. Verfassungsrechtlicher Schutz endgespeicherter E-Mails durch das Fernmeldegeheimnis des Art. 10 Abs. 1 GG?	140
a) Speicherung auf dem heimischen Computer	141
aa) Die Kammerentscheidung des Bundesverfassungsgerichtes aus dem Jahr 2005	141
bb) Die „Bargatzky-Entscheidung“ des Zweiten Senats aus dem Jahr 2006	143
cc) Stellungnahme	146
b) Speicherung in einem Online-Postfach beim Provider oder bei einem sonstigen Dritten	149
aa) Die Entwicklung in Rechtsprechung und Literatur	150
bb) Entwicklung in der Literatur	150
(1) Enger, technisch orientierter Ansatz	150
(2) Differenzierende Ansätze	151
(3) Weite Auslegung des Schutzbereichs	155
cc) Entwicklung in der Rechtsprechung	158
(1) Entwicklung der Rechtsprechung des BGH und der Instanzgerichte bis 2009	158
(2) Der Beschluss des Hessischen Verwaltungsgerichtshofs vom 15. Mai 2009	162
(3) Die Entscheidung des Bundesverfassungsgerichtes vom 16. Juni 2009	167
c) Stellungnahme	169
aa) Das Fernmeldegeheimnis als Speicherschutzrecht?	171
bb) Notwendigkeit eines Schutzes durch das Fernmeldegeheimnis?	176
cc) Abgrenzungskriterien der Endspeicherung	178
d) Anwendbarkeit des Briefgeheimnisses	180
4. Schutz durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG	180
a) Entstehung und Herleitung des Computergrundrechtes durch das Bundesverfassungsgericht	181
b) Reaktionen in der Literatur	185

c) Bewertung	187
d) Schutzbereich des Computergrundrechtes	189
aa) Das informationstechnische System als Schutzgegenstand des Computergrundrechtes	189
(1) Definition des Bundesverfassungsgerichtes	190
(2) Komplexität des elektronischen Systems	191
(a) Anforderungen an die Datenverarbeitungsfähigkeit	191
(b) Vernetzung	192
(c) Notwendigkeit einer eigenständigen Funktionalität des Systems?	192
(d) Nutzung als eigenes System	193
(e) Schwierigkeit des Zugriffs	194
bb) Eingriffe in die Vertraulichkeit und Integrität des informa- tionstechnischen Systems	194
(1) Vertraulichkeit des informationstechnischen Systems ...	195
(2) Integrität des informationstechnischen Systems	195
(3) Vertraulichkeit und die Integrität des informationstech- nischen Systems als eigenständige Schutzgewährleistun- gen	196
(4) Schutz von Vertraulichkeits- und Integritätserwartungen	198
e) Grundrechtsträger und -adressaten	198
f) Rechtfertigung von Eingriffen in den Schutzbereich	200
aa) Allgemeine Anforderungen an ein das Computergrundrecht beschränkendes Gesetz	201
(1) Normenbestimmtheit und Normenklarheit	201
(2) Verhältnismäßigkeit der Beschränkungen	202
(a) Beschränkung auf überragend wichtige Rechtsgüter des Einzelnen und der Allgemeinheit	202
(b) Konkretisierungsansätze	203
(c) Hinreichende Tatsachenbasis und Eintrittswahr- scheinlichkeit der Gefährdung	205
bb) Formale Anforderungen an die Anordnung von Eingriffen ..	207
cc) Schutz des Kernbereiches privater Lebensgestaltung	208
(1) Gefahr der Erhebung kernbereichsbezogener Daten	208
(2) Schutzkonzept des Bundesverfassungsgerichtes	209
(a) Zweistufiges System der Erhebung und Auswertung	209
(b) Probleme der Datenerhebung aus informationstech- nischen Systemen	210
(c) Auswertung der Daten	211
(d) Bewertung	213
g) Das E-Mail-Postfach als geschütztes informationstechnisches System?	214

aa) Vorliegen eines geschützten informationstechnischen Systems	214
bb) Eingriff in die Vertraulichkeit des Systems	217
5. Schutz durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V.m. 1 Abs. 1 GG oder das Recht auf Unverletzlichkeit der Wohnung nach Art. 13 Abs. 1 GG	219
6. Erstreckung des Schutzes des Computergrundrechtes auch auf die auf dem heimischen Computer endgespeicherten E-Mails	219
7. Erstreckung des Schutzes des Computergrundrechts auf alle in einem E-Mail-Client enthaltenen Ordner?	222
V. Zusammenfassung der Ergebnisse der verfassungsrechtlichen Erwägungen	224
D. Verfassungskonforme strafprozessuale Eingriffsgrundlagen während der verschiedenen Phasen	228
I. Verfassungsrechtliche Mindestanforderungen an die Eingriffsermächtigungen	228
II. Verfassungskonforme Eingriffsermächtigungen in den Übertragungsphasen (Phasen 1 und 3)	230
1. Einhaltung der formalen Anforderungen an ein allgemeines Gesetz ..	231
2. Materielle Anforderungen des Fernmeldegeheimnisses an die Verfassungsmäßigkeit des § 100a StPO	231
a) Normenbestimmtheit und Normenklarheit des § 100a StPO	232
b) Verhältnismäßigkeitserwägungen	234
aa) Straftatenkatalog des § 100a Abs. 2 StPO	234
bb) Verdachtsgrad und Streubreite des Eingriffes	239
c) Schutz des Kernbereiches privater Lebensgestaltung	241
aa) Genereller Ausschluss von Eingriffen?	242
bb) Notwendigkeit einer Echtzeitüberwachung/unverzöglichen Auswertung?	243
cc) Verlagerung des Kernbereichsschutzes in die Auswertungsphase	246
(1) Beschränkungsmöglichkeiten in der Praxis	247
(2) Entscheidung der Staatsanwaltschaft über die Löschungspflicht	247
d) Regelung der verfassungsrechtlich gebotenen Verfahrensanforderungen	248
III. Verfassungskonforme Eingriffsermächtigungen während der Zwischenspeicherung (Phase 2)	251
1. Der strafprozessuale Lösungsansatz des Bundesverfassungsgerichtes	252
2. Sicherstellung und Beschlagnahme nach §§ 94 ff. StPO	259
a) Formale Anforderungen an ein allgemeines Gesetz	259
b) Materielle Anforderungen an ein allgemeines Gesetz	260
aa) Generelle Eignung der § 94 ff. StPO als Eingriffsgrundlage ..	260

(1) Durch das Bundesverfassungsgericht aufgeführte Literaturstimmen	260
(2) Systematische Argumente	262
(3) Historie der Normen	263
bb) Normenbestimmtheit und Normenklarheit der §§ 94 ff. StPO	265
(1) Beschlagnahme von Daten	266
(2) Überwachung laufender Telekommunikation durch §§ 94 ff. StPO	270
cc) Verhältnismäßigkeit der Einschränkungen des Fernmeldegeheimnisses	272
(1) Schwere der zu verfolgenden Straftat	272
(2) Überwiegen des Strafverfolgungsinteresses aufgrund von Besonderheiten der E-Mail-Kommunikation?	276
(a) Überwiegen des Strafverfolgungsinteresses?	276
(b) Abgeschlossenheit des Kommunikationsvorgangs?	278
(c) Verhältnismäßigkeit aufgrund Offenheit der Maßnahme?	280
(d) Verhältnismäßigkeit aufgrund Punktualität der Maßnahme?	283
(e) Begrenzung durch den Ermittlungszweck	284
(3) Verdachtsgrad und Streubreite des Eingriffes	285
dd) Schutz des Kernbereiches privater Lebensgestaltung	286
ee) Regelung der verfassungsrechtlich gebotenen Verfahrensanforderungen	290
ff) Benachrichtigung nach § 35 StPO und Zurückstellung der Benachrichtigung des Beschuldigten nach § 95a StPO	291
(1) Gesetzgebungsverfahren	292
(2) Materielle Verfassungsmäßigkeit der Neuregelung des § 95a StPO?	293
gg) Durchsicht von elektronischen Speichermedien gemäß § 110 Abs. 3 StPO	297
3. Die Postbeschlagnahme nach § 99 Abs. 1 StPO	298
a) Die Argumentation der Rechtsprechung	298
b) Materielle Anforderungen an ein allgemeines Gesetz	300
aa) Historie und Systematik der Norm	300
bb) Normenbestimmtheit und Normenklarheit des § 99 Abs. 1 StPO	301
cc) Verhältnismäßigkeit der Einschränkungen des Fernmeldegeheimnisses	305
(1) Schwere der zu verfolgenden Straftat	306
(2) Unverhältnismäßigkeit als heimliche Überwachungsmaßnahme?	306
dd) Schutz des Kernbereiches privater Lebensgestaltung	308
c) Die Rechtsprechung des BGH im Nachgang zur Bundesverfassungsgerichtsentscheidung vom Juni 2009	309

4. Die Regelung der Telekommunikationsüberwachung gemäß § 100a StPO	311
a) Normenbestimmtheit und Normenklarheit des §§ 100a StPO ...	312
aa) Vorliegen laufender Telekommunikation	312
bb) Generelle Eignung der Norm zur „Überwachung“ gespeicherter Inhalte laufender Telekommunikationsvorgänge	314
(1) „Überwachung“ laufender Telekommunikation	315
(2) Durchsetzbarkeit der Überwachungsanordnung	319
b) Verhältnismäßigkeitserwägungen	322
c) Regelung zum Schutz des Kernbereiches privater Lebensgestaltung und der verfassungsrechtlich gebotenen Verfahrensanforderungen	323
5. Die Online-Durchsuchung gemäß § 100b StPO	324
IV. Verfassungskonforme Eingriffsermächtigungen während der Endspeicherung (Phase 4)	324
1. Sicherstellung und Beschlagnahme nach §§ 94 ff. StPO	325
a) Vorbemerkung	326
b) Materielle Anforderungen an ein allgemeines Gesetz	327
aa) Normenbestimmtheit und Normenklarheit der §§ 94 ff. StPO	327
bb) Verhältnismäßigkeit der Einschränkungen des Computergrundrechts	327
cc) Schutz des Kernbereiches privater Lebensgestaltung	328
dd) Regelung der verfassungsrechtlich gebotenen Verfahrensanforderungen	329
ee) Durchsicht von elektronischen Speichermedien gemäß § 110 Abs. 3 StPO	329
2. Die Postbeschlagnahme nach § 99 Abs. 1 StPO	331
a) Ansicht der Rechtsprechung	331
b) Materielle Anforderungen an ein allgemeines Gesetz	332
aa) Historie und Systematik der Norm	332
bb) Normenbestimmtheit und Normenklarheit des § 99 Abs. 1 StPO	332
cc) Verhältnismäßigkeit der Einschränkungen des Computergrundrechtes und Kernbereichsschutz	333
3. Die Regelung der Telekommunikationsüberwachung gemäß § 100a StPO	334
a) Vorbemerkung	334
b) Normenbestimmtheit und Normenklarheit des § 100a StPO	336
aa) Vorliegen laufender Telekommunikation	336
bb) Eignung der Norm zur „Überwachung“ endgespeicherter Inhalte	339
c) Verhältnismäßigkeitserwägungen	341
d) Regelung zum Schutz des Kernbereiches privater Lebensgestaltung und der verfassungsrechtlich gebotenen Verfahrensanforderungen	343

4. Die Online-Durchsuchung gemäß § 100b StPO	343
a) Begriff der Online-Durchsuchung und Historie der Regelung ..	343
b) Eingriffstiefe der Online-Durchsuchung	346
c) Normenbestimmtheit und Normenklarheit des § 100b StPO	347
d) Verhältnismäßigkeit der Einschränkungen des Computergrund- rechts	347
aa) Eignung zur Ermittlung reversionssicherer Beweise	348
bb) Anlasstatenkatalog des § 100b Abs. 2 StPO	349
cc) Übermaßverbot	352
e) Regelung zum Schutz des Kernbereiches privater Lebensgestal- tung und der verfassungsrechtlich gebotenen Verfahrensanforde- rungen	352
5. Exkurs: Quellen-TKÜ	353
V. Zusammenfassung der Ergebnisse der strafprozessualen Erwägungen ..	355
E. Vorschlag für eine verfassungskonforme, strafprozessuale Rechtsgrund- lage für Zugriffe auf endgespeicherte Inhaltsdaten von E-Mails	361
I. Vorüberlegungen zur Neuregelung	361
1. Regelungsbedarf	362
2. Systematik und Ausgestaltung der vorgeschlagenen Regelung	366
a) Systematischer Standort	366
b) Aufbau der Norm	367
c) Allgemeine Voraussetzungen	367
d) Verhältnismäßigkeit des Anlasstatenkatalogs und Beschränkung des Anwendungsbereichs	368
aa) Ausgestaltung des Straftatenkataloges	368
(1) Verzicht auf eine konkrete Regelung der Anlasstaten ...	369
(2) Einzelheiten des Kataloges	370
bb) Beschränkungen des Anwendungsbereiches und Mitwir- kungspflichten	372
e) Kernbereichsschutz	372
f) Verfahrensvoraussetzungen	373
II. Gesetzentwurf	373
F. Fazit	396
Literaturverzeichnis	399
Stichwortverzeichnis	412