

Inhaltsüberblick

Vorwort	V
Abkürzungsverzeichnis	XIX
Einleitung	1
Teil 1: Grundlagen	6
I. Begriffe	6
II. Wirtschaftliche Bedeutung	31
III. Technische Grundlagen zur Anonymisierung	46
IV. Folgerungen für die nachfolgende Untersuchung	69
Teil 2: Kriminalistische Analyse	72
I. Überwachung und Identifizierung von Nutzern	73
II. Anonymität gegenüber Host-Providern und Nutzern	84
III. Anonymität gegenüber Access-Providern	159
IV. Anonymität auf Rechner-Ebene	167
Teil 3: Rechtliche Analyse	195
I. Verankerung des Rechts auf Anonymität	195
II. Aufhebung und Einschränkung von Anonymität	407
III. Fazit	514
Literaturverzeichnis	529
Stichwortverzeichnis	597

Inhaltsverzeichnis

Vorwort	V
Abkürzungsverzeichnis	XIX
Einleitung	1
Teil I: Grundlagen	6
I. Begriffe	6
A. Anonymität	6
1. Anonymität als soziales Phänomen	9
a) Individuelle Anonymität	11
b) Anonymität von Beziehungen	14
c) Aufhebung von Anonymität	14
2. Bestimmung von Anonymität	17
a) Identitätsfaktoren	18
b) Anonymitätssets	23
c) Grad der Anonymität	24
B. Pseudonymität	27
C. Vertraulichkeit	31
II. Wirtschaftliche Bedeutung	31
A. Wirtschaftliche Bedeutung personenbezogener Daten	32
B. Anonymität als Dienstleistung	35
1. Zielgruppen für Anonymitätsdienstleistungen	35
2. Kommerzielle Anbieter	38
a) Technische Zuverlässigkeit und Vertrauenswürdigkeit	38
b) Nutzergruppen	39
c) Finanzierungskonzepte	40
3. Nicht-kommerzielle Anbieter	42
a) Anbieter	42
b) Nutzergruppen	43
c) Finanzierung und Missbrauchsregulierung	45
III. Technische Grundlagen zur Anonymisierung	46
A. Begriffe	46
B. Netzverbindungen	48
1. Schichtenmodell	48
2. Adressierung	51

C.	Anwendungsprotokolle und Dienste	53
1.	HTTP, WWW-Dokumente und URL	54
a)	Serverseitig anfallende Daten	54
b)	Nutzerseitig anfallende Daten	58
(1)	Cookies	58
(2)	Browser-Cache	60
(3)	Sonstige Nutzerdaten	61
2.	E-Mail	63
3.	Echtzeitsysteme	65
4.	Peer-to-Peer-Systeme	68
IV.	Folgerungen für die nachfolgende Untersuchung	69
A.	Problemstellung	69
B.	Umfang der Untersuchung	70
Teil 2:	Kriminalistische Analyse	72
I.	Überwachung und Identifizierung von Nutzern	73
A.	Identifizierungsmöglichkeiten mit Wissen des Nutzers	74
B.	Identifizierungsmöglichkeiten ohne Wissen des Nutzers	77
C.	Identifizierungsmöglichkeiten ohne Wissen von Anbieter oder Nutzer	80
D.	Identifizierungsmöglichkeiten durch Zweckentfremdung	81
E.	Schlussfolgerungen	83
II.	Anonymität gegenüber Host-Providern und Nutzern	84
A.	Anonyme Nutzung von Diensten	85
1.	E-Mail	86
a)	Reguläre E-Mail-Diensteanbieter	86
b)	Remailer	88
(1)	Pseudonymisierende Remailer	88
(2)	Anonymisierende Remailer	89
c)	Zusammenfassung	91
2.	World Wide Web	91
3.	Weitere Internetdienste	94
a)	Datenaustausch	94
(1)	Herkömmliche Tauschbörsen	96
(2)	Anonyme Tauschbörsen	98
b)	Nachrichtenaustausch	100
4.	Zusammenfassung	102
B.	Anonyme wirtschaftliche Transaktionen	103
1.	Bargeld	103

2.	Online-Währungen	104
3.	Prepaid-Produkte	106
4.	Treuhänder	106
5.	Zusammenfassung	107
C.	Identitätsmanagement	108
1.	Protokolle zum Identitätsmanagement	112
a)	Platform for Privacy Preferences (P3P)	113
(1)	Funktionsweise	113
(2)	Kritik	115
(3)	Auswirkungen von P3P	117
b)	Liberty Alliance	118
2.	Clientseitiges Identitätsmanagement	120
a)	Allgemeine Ansätze	120
b)	Spezialisierte Produkte	122
3.	Serverseitiges Identitätsmanagement	125
4.	Schlussfolgerungen und Ausblick	128
D.	Anonymisierungsdienste	130
1.	Proxy-Dienste	132
2.	Crowds-Ansatz	135
3.	Dezentrale Anonymisierungssysteme: TOR	138
a)	Hidden Services	140
b)	Kompromittierungsmöglichkeiten	141
4.	Zentrale Anonymisierungssysteme: AN.ON/JAP/JonDonym	144
5.	Missbrauch von Anonymisierungsdiensten	147
a)	Statistische Informationen	150
b)	Lösungsmöglichkeiten	152
(1)	Einschränkung von Anonymisierungsdiensten	153
(2)	Einführung einer Vorratsdatenspeicherung	155
(3)	Einzelfallbezogene Speicherung für die Zukunft	156
6.	Schlussfolgerungen	157
III.	Anonymität gegenüber Access-Providern	159
A.	Faktisch anonyme Einstiegspunkte: „Public Networks“	161
B.	Drahtlose anonyme Einstiegspunkte	163
C.	Illegale Einstiegsmöglichkeiten	165
IV.	Anonymität auf Rechner-Ebene	167
A.	Kriminalistische Methoden zur Ermittlung von Nutzern im Einzelfall	168
1.	Forensisches Verfahren	168
2.	Ermittlungsansätze	170

B.	Verschlüsselte Kommunikation	172
1.	Verschlüsselte Webverbindungen	173
2.	Verschlüsselte E-Mail-Kommunikation	174
3.	Verborgene Informationen	177
4.	Entschlüsselung durch Dritte	180
a)	Entschlüsselungsmöglichkeiten	180
b)	Kritik	182
5.	Staatliche Online-Überwachung	183
a)	Installationsmöglichkeiten	184
b)	Funktionen	186
c)	Verwertung	189
d)	Bewertung	190
C.	Verschlüsselung im Dateisystem	190
D.	Wiping Tools	193
Teil 3: Rechtliche Analyse		195
I. Verankerung des Rechts auf Anonymität		195
A.	Überblick	196
B.	Verfassungsrechtliche Vorgaben	197
1.	Allgemeines Persönlichkeitsrecht	198
a)	Persönlicher Schutzbereich	199
b)	Sachlicher Schutzbereich	200
(1)	Schutz der Privat- und Intimsphäre	202
(a)	Abgrenzung zwischen privatem und öffentlichem Raum	203
aa)	Adressatenkreis	204
bb)	Subjektives Verständnis von Öffentlichkeit	206
cc)	Allgemeine Zugänglichkeit	208
dd)	Bewusstsein über Öffentlichkeit	211
(b)	Schutzumfang im engeren Sinne	212
(2)	Selbstdarstellung in der Öffentlichkeit	213
(a)	Recht am eigenen Bild	214
(b)	Recht am gesprochenen Wort	216
(c)	Recht auf eine unverfälschte Darstellung	218
(d)	Zusammenfassung	219
(3)	Informationelle Selbstbestimmung	219
(a)	Hintergrund	219
aa)	Kombinationsmöglichkeiten von Daten	219
bb)	Verteilung von Einzeldaten	221
(b)	Schutzbereich	224
aa)	Bestimmung des Schutzbereichs	225

bb)	Abgrenzung zu anderen Grundrechten	229
cc)	Sonderproblem: Einheitliches Personen- kennzeichen	231
(4)	Gewährleistung von Vertraulichkeit und Integrität	234
(a)	Hintergrund	234
(b)	Schutzbereich	235
(c)	Abgrenzung zu anderen Grundrechten	238
c)	Eingriff und Rechtfertigung	239
(1)	Staatliche Eingriffe	240
(a)	Verhältnis von Sicherheit und Freiheit	240
(b)	Abstufungen des Schutzes	242
aa)	Sphärentheorie	243
bb)	Datenkategorien	244
cc)	Bewertung	245
(c)	Grundlegende Anforderungen an einschränkende Maßnahmen	245
aa)	Wirksame Zustimmung	245
bb)	Förmliches Gesetz	247
(d)	Besondere Anforderungen bei der Datenverarbeitung ...	251
aa)	Besondere organisatorische und prozedurale Maßnahmen	252
bb)	Erhebung für statistische Zwecke	253
cc)	Anonymisierung von Daten	254
(2)	Nicht-staatliche Eingriffe	254
d)	Zusammenfassung und Folgerungen für die elektronische Anonymität	257
2.	Brief-, Post- und Fernmeldegeheimnis	261
a)	Persönlicher Schutzbereich	261
b)	Sachlicher Schutzbereich	263
(1)	Briefgeheimnis	264
(2)	Postgeheimnis	264
(3)	Fernmeldegeheimnis	265
(a)	Individualkommunikation	266
(b)	Selbstschutz	268
(c)	Umstände der Kommunikation	269
c)	Eingriff und Rechtfertigung	272
(1)	Betriebsbedingte Eingriffe	275
(2)	Gezielte Überwachungsmaßnahmen	277
(3)	Eingriffe Privater	277
d)	Zusammenfassung und Folgerungen für die elektronische Anonymität	280
3.	Verfassungsrechtliche Folgerungen für ein Recht auf Anonymität	280

C.	Schutz durch internationale und supranationale Vorschriften	282
1.	Europäische Menschenrechtskonvention	283
a)	Art. 8 EMRK	283
(1)	Persönlicher Schutzbereich	284
(2)	Sachlicher Schutzbereich	284
(a)	Privat- und Familienleben	285
(b)	Wohnung	288
(c)	Briefverkehr	290
(3)	Eingriff	292
(4)	Rechtfertigung	293
b)	Art. 10 EMRK	297
c)	Zusammenfassung und Folgerungen für die elektronische Anonymität	299
2.	Europäische Grundrechtscharta	300
3.	Vertrag über eine Verfassung für Europa und EU-Reformvertrag	302
4.	Europäische Datenschutzrichtlinien	303
a)	Entwicklung	303
b)	Richtlinie zur Vorratsdatenspeicherung	304
(1)	Inhalt	305
(2)	Kritik	306
5.	Internationaler Pakt über bürgerliche und politische Rechte	308
6.	Allgemeine Erklärung der Menschenrechte	311
7.	Unverbindliche Empfehlungen	312
a)	Empfehlung zum Schutz personenbezogener Daten bei Telekommunikationsdiensten	312
b)	Empfehlung zum Schutz der Privatsphäre im Internet	315
c)	Deklaration zur Kommunikationsfreiheit im Internet	317
d)	OECD Empfehlung zur Kryptopolitik	318
8.	Zusammenfassung	320
D.	Einfachgesetzliche Vorschriften	320
1.	Allgemeines Datenschutzrecht	321
a)	Personenbezug	322
b)	Zweckbindung und Erforderlichkeit	323
2.	Besondere Vorschriften	324
a)	Besondere Vorschriften für Access-Provider	325
(1)	Datenschutz im TKG	328
(a)	Grundlagen	329
aa)	Begriffe	329
bb)	Telekommunikationsfernmeldegeheimnis	331
cc)	Technische Schutzmaßnahmen	332
(b)	Erhebung und Verwendung von Bestandsdaten	332
aa)	Erhebung von Telekommunikationsbestandsdaten	332

bb)	Verwendung von Bestandsdaten	336
cc)	Löschung von Bestandsdaten	340
dd)	Zusammenfassung	340
(c)	Erhebung und Verwendung von Verkehrsdaten	340
aa)	Personenbezug von IP-Adressen	342
bb)	Einordnung von dynamisch zugewiesenen IP-Adressen	345
cc)	Protokollierung von IP-Adressen	346
dd)	Änderungen durch die Einführung der Vorratsdatenspeicherung	352
(d)	Erhebung von Inhaltsdaten	365
(2)	Rechtliche Möglichkeiten für einen anonymen Internet-Access	365
(a)	Angebote ohne Bezahlung	366
aa)	Arbeitsverhältnisse	366
bb)	Wissentlich offene kabellose Netzwerke	368
cc)	Unwissentlich offene drahtlose Netzwerke	373
(b)	Angebote mit pauschaler Bezahlung	375
(c)	Angebote mit Bezahlung im Vorfeld	376
b)	Besondere Vorschriften für Router und andere durchleitende Stationen	378
c)	Besondere Vorschriften für Host-Provider und Diensteanbieter	379
(1)	Rechtliche Einordnung von Diensten	380
(a)	E-Mail	380
(b)	WWW	381
(c)	Anonymisierungsdienste	383
aa)	Einordnung	384
bb)	Auswirkungen	386
(2)	Anonymität im TMG	389
(a)	Anonyme Nutzung	389
(b)	Einschränkungen	391
(3)	Technische und organisatorische Anforderungen	393
(4)	Änderungen durch die Einführung der Vorratsdaten speicherung	395
(a)	Auswirkungen für E-Mail-Anbieter	396
aa)	Speicherung von Bestandsdaten	396
bb)	Speicherung von Verkehrs- und Nutzungsdaten ...	397
cc)	Kritik	399
(b)	Auswirkungen für Anonymisierungsdienste	400
(5)	Missbrauchsvorkehrungen	403
d)	Besondere Vorschriften für einzelne Nutzer – Selbstschutz ...	404
3.	Zusammenfassung	406

II. Aufhebung und Einschränkung von Anonymität	407
A. Zugriff auf bestehende Daten im Einzelfall	408
1. Maßnahmen im Rahmen der Strafverfolgung	411
a) Bestandsdaten	411
(1) Auskunftsverfahren	412
(a) Auskunft bei Telemediendiensten	412
aa) Übermittlungsbefugnis	413
bb) Befugnisnormen	413
(b) Auskunft bei Telekommunikationsdiensten	415
(2) Problembereiche	416
(a) Ermittlung einer E-Mail-Adresse	417
(b) Ermittlung eines Namens zu einer IP-Adresse	419
(c) Ermittlung einer IP-Adresse anhand eines Namens	423
(d) Sonderfall: Rasterfahndung	423
(1) Abgrenzung zu anderen Ermittlungsmaßnahmen ..	424
(2) Einsatzhäufigkeit	428
(3) Präventive Rasterfahndung	428
b) Nutzungs- und Verkehrsdaten	429
(1) Erhebung bei Telemedienanbietern	430
(2) Erhebung bei Teilnehmern einer Telekommunikation	431
(3) Erhebung bei Anbietern von Telekommunikationsdiensten ...	434
(a) Identifizierung des zu überwachenden Anschlusses	435
(b) Herauszugebende Informationen	437
c) Inhaltsdaten	438
(1) Inhaltsdaten einer Individual-Kommunikation	439
(a) Zugriff mit Hilfe des Providers	440
aa) Rechtliche Einordnung	440
bb) Durchführung von Maßnahmen	444
(b) Zugriff mit bekanntem Passwort („Online-Abruf“)	446
(c) Heimliche Online-Zugriffe („Online-Durchsuchung“) ..	450
aa) Maßnahmen gegen den Provider	451
bb) Maßnahmen gegen Private	453
(d) Quellen-Telekommunikationsüberwachungen	460
(2) Sonstige Inhaltsdaten	461
2. Maßnahmen durch Sicherheitsbehörden	462
a) Bundesnachrichtendienst	464
(1) Zugriff auf Bestands-, Verkehrs- und Nutzungsdaten	464
(2) Zugriff auf Inhaltsdaten	465
(a) Überprüfung von Maßnahmen	466
(b) Kennzeichnung	467
(3) Sonstige Informations- und Auskunftsmöglichkeiten	468

(4) Informationsaustausch	469
(a) Grundlagen	470
(b) Antiterrordatei	471
(c) Projektbezogene gemeinsame Dateien	473
(5) Zusammenfassung	473
b) Bundes- und Landesämter für Verfassungsschutz	474
c) Militärischer Abschirmdienst	476
d) Zollfahndungsdienst	476
e) Polizei	477
3. Maßnahmen durch private Dritte	479
a) Datenweitergabe durch Provider	479
b) Datenweitergabe an private Dritte	481
B. Erhebung von zukünftigen Daten im Einzelfall	484
1. Maßnahmen im Rahmen der Strafverfolgung	484
a) Überwachung von Verkehrsdaten	485
b) Überwachung von Inhaltsdaten	487
c) Sonderproblem: Anordnungsgegner bei mehrstufigen Anonymisierungsdiensten	488
2. Maßnahmen zur präventiven Überwachung	490
a) Polizeilich-präventive Überwachung	490
b) Präventive Überwachung nach dem ZFdG	492
3. Maßnahmen durch andere Stellen	493
C. Verdachtsunabhängige Datenerfassung	494
1. Arbeitsverhältnisse	494
a) Veröffentlichung identifizierender Angaben	495
(1) Telefonverzeichnisse	495
(2) Nutzung durch Dritte	497
b) Überwachung in Arbeitsverhältnissen	500
2. Strategische Überwachung	504
a) Technische Aspekte der strategischen Überwachung	506
b) Staatliche Souveränität	507
c) Einschränkungen der strategischen Überwachung	509
(1) Individualisierung	510
(2) Informationsübermittlung	510
(3) Kontrollen	511
3. Vorratsdatenspeicherung	512
III. Fazit	514
A. Rechtliche Situation	514
1. Anonymität	514
2. Überwachung	516
3. Weitere Entwicklung	517

XVIII

a) Datensammlungen	517
b) Datenaustausch	520
c) Folgerungen	522
B. Technische Situation	522
C. Auswirkungen auf die Strafverfolgung	524
D. Schlussbemerkungen	525
Literaturverzeichnis	529
Stichwortverzeichnis	597