

Prof. Dr. Martin Kutscha/Sarah Thomé, LL.M.

Grundrechtsschutz im Internet?



Nomos

Inhaltsverzeichnis

A. Erster Teil	11
<i>Martin Kutscha</i>	
I. Einführung	11
1. Die aktuelle Herausforderung	11
2. Das Untersuchungsprogramm	14
II. Privatsphäre und Öffentlichkeit	16
1. Privatsphäre – ein Auslaufmodell?	16
2. Abgrenzungsversuche im Wandel der Zeiten	18
3. Öffentliches Recht und Privatrecht: verschwimmende Grenzen	21
4. Das Internet – ein privatrechtlich organisierter öffentlicher Raum	23
III. Das Recht auf informationelle Selbstbestimmung	24
1. Der technische Hintergrund	24
2. Der Schutzzweck des Grundrechts	26
3. Vielfalt der Eingriffsformen	28
a. Das weite Eingriffsverständnis	29
b. Eingriffe durch Ermittlungen im Netz?	30
4. Anforderungen an die Rechtfertigung von Eingriffen	34
a. Die Maßstäbe des Volkszählungsurteils	34
b. Implementation mit fragwürdigen Ergebnissen	36
c. Widersprüchliche Verfassungsrechtsprechung – von der Rasterfahndung zur Beschlagnahme von Computern und der Auswertung von E-Mails	37
d. Ermittlungsbefugnisse in der StPO – Generalermächtigungen für den Zugriff auf elektronische Daten?	40
5. Grundrechtsschutz gegenüber Privatunternehmen?	42
a. Vertragsfreiheit und informierte Einwilligung?	43
b. Die Schutzpflicht des Staates	46
c. Gesetzgeberischer Handlungsbedarf – in welcher Richtung? – Bausteine eines Datenschutzrechts der Zukunft	48
d. Welcher Grundrechtsschutz für Internetanbieter?	51

IV. Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („Computer-Grundrecht“)	53
1. Der Anlass für die „Neuentdeckung“	53
2. Die Kontroverse um die Notwendigkeit des neuen Grundrechts	55
3. Begrenzung von Eingriffen	58
4. Schutzwirkung gegenüber Privaten?	60
V. Das Fernmelde- bzw. Telekommunikationsgeheimnis	61
1. Der Schutzzweck des Grundrechts	61
2. Fragwürdige Abgrenzung des Schutzbereichs – Differenzierung nach der Art der IP-Adresse?	62
3. Das Arsenal der Eingriffsvarianten – technischer Fortschritt als Motor für neue Überwachungsmethoden?	65
a. Kenntnisnahme vom Inhalt der Telekommunikation; Problematik der „Quellen-TKÜ“	65
b. „Die Jagd nach den Verbindungsdaten“	68
c. „Beschlagnahme“ von E-Mails beim Provider	71
VI. Menschenwürde, Kernbereichsschutz und Herstellung von Persönlichkeitsprofilen	72
1. Ursprung und Reichweite der Objektformel	73
2. Der Kernbereich privater Lebensgestaltung – Inkonsequenzen eines Schutzkonzepts	75
a. Variierende Bestimmungen des Kernbereichs	76
b. Ein hinreichendes Schutzkonzept für „Online-Durchsuchungen“ und Telekommunikationsüberwachungen?	78
c. Abschied von der Abwägungsfestigkeit der Menschenwürde?	80
3. Das Verbot umfassender Persönlichkeitsprofile	83
VII. Personenbewertungsportale im Internet als Grundrechtsproblem	85
1. Die Reichweite der Meinungsfreiheit	85
2. Die widerstreitenden Grundrechte	88
3. Fragwürdige Abwägungskriterien	90
VIII. Die Debatte um eine Reform des Urheberrechts	91
1. Der Urheber als grundrechtlich geschützter Eigentümer – ein Mythos?	92
2. Grundrecht auf freien Informationszugang?	93
IX. Zusammenfassung in Thesen	95

B. Zweiter Teil	101
<i>Sarah Thomé</i>	
I. Einleitung	101
II. Die Bedeutung der Neukonzeption der externen Datenschutzkontrolle für einen effektiven Grundrechtsschutz	103
1. Kontrolle des Datenschutzes: Eine stetig wachsende Aufgabe	103
2. Die Entwicklung der Datenschutzaufsicht in Deutschland	104
a. Fremd- und Selbstkontrolle	104
b. Datenschutzkontrolle als Verwaltungsaufgabe?	105
3. Datenschutzkontrolle als Grundrechtsschutz durch Verfahren	107
a. Bedeutung des Volkszählungsurteils für die Datenschutzkontrolle	107
b. Institutionalisierung einer adäquaten Kontrolle	108
4. Nationales Kontrollmodell und europarechtliche Vorgaben	109
a. Europäische Datenschutzrichtlinie	109
b. Nationale Umsetzung der europäischen Vorgaben	112
c. Mangelnde Unabhängigkeit der Aufsichtsbehörden	114
5. Neue Herausforderungen und Reformbedarf	116
III. Internationale Perspektive am Beispiel des Datenschutzes	118
1. Effektiver Grundrechtsschutz stößt an territoriale Grenzen	118
2. Regulierungsbedürftigkeit des internationalen Datenverkehrs	119
3. Anwendbarkeit der Datenschutzrichtlinie	122
a. Art. 4 Abs. 1 Buchst. a Datenschutzrichtlinie: Niederlassungsprinzip	122
b. Art. 4 Abs. 1 Buchst. c Datenschutzrichtlinie: Automatisierte Mittel	123
c. Zukünftige Erweiterung?	125
4. Anwendbarkeit des BDSG: Territorialprinzip	126
5. Internationaler Datentransfer	127
a. Art. 25, 26 Datenschutzrichtlinie	127
b. §§ 4b, 4c BDSG	128
c. Entscheidung über die Angemessenheit	129
d. Safe Harbor und PNR-Abkommen	131
6. Ausblick	134
Literaturverzeichnis	137