

Inhaltsübersicht

Einleitung	1
<i>Teil 1: Das Verhältnis von Freiheit und Sicherheit in der Informationsgesellschaft</i>	
A. Die Freiheit	5
I. Umfassender Freiheitsbegriff	6
II. Der verfassungsrechtliche Freiheitsbegriff	6
III. Der technologische Freiheitsbegriff	7
IV. Die verfassungsgerichtliche Begründung der informationellen Freiheit	8
B. Die Sicherheit	10
I. Sicherheit durch den Staat	10
II. Die Sicherheitsrenaissance des 11. September 2001	11
III. Staatliche Akteure öffentlicher Sicherheit	14
IV. Staatliche Methoden öffentlicher Sicherheit	15
V. Sicherheit nicht als bloßer Selbstzweck	18
C. Informationelle Freiheit oder staatliche Sicherheit?	19
I. Keine staatliche Sicherheit ohne (informationelle) Freiheit	20
II. Keine informationelle Freiheit ohne staatliche Sicherheit	21
D. Der Ausgleich zwischen (informationeller) Freiheit und staatlicher Sicherheit	22
<i>Teil 2: Maßstäbe des Ausgleichs zwischen informationeller Freiheit und staatlicher Sicherheit</i>	
A. Vermeidung von Grundrechtseingriffen durch eine prozedural geschützte automatisierte Datenverarbeitung	27
I. Voraussetzungen für die Annahme von Grundrechtseingriffen im Rahmen von automatisierten Auswertungsverfahren	28
II. Vorteile der mit prozeduralen Schutzmechanismen ausgestatteten automatisierten Datenverarbeitung	30
III. Technische Anforderungen an ein System automatisierter Datenauswertung	35

IV.	Derzeitige Realisierbarkeit eines Systems automatisierter Datenauswertung	37
B.	Vermeidung von unberechtigter Kriminalisierung im Rahmen der automatisierten Datenverarbeitung	38
I.	Die rechtliche Verortung des Schutzes vor unberechtigter Kriminalisierung im sicherheitsbehördlichen Ermittlungsverfahren	39
II.	Maßnahmen gegen unberechtigte Kriminalisierung für die automatisierte Datenverarbeitung	45
III.	Erweiterung des parlamentarischen Transparenzgedankens der Schwellenwertbestimmung hin zur bevölkerungsinitiierten Kriminalprävention	64
C.	Kontrolle und Begrenzung der staatlichen Datenverarbeitung	66
I.	Kontrolle in der Gesetzgebung	69
II.	Kontrolle in der Rechtsanwendung	81
III.	Parlamentarische Kontrolle	94
IV.	Kontrolle durch die G 10-Kommission	104
V.	Kontrolle durch die Regierungskommission zur Überprüfung der Sicherheitsarchitektur und -gesetzgebung in Deutschland nach dem 11. September 2001	107
VI.	Weitere Kontrollmechanismen	113
VII.	Theoretisch ausreichender Kontrollstatus bei praktisch teils unzureichender Effektivität von Kontrollmaßnahmen	114
D.	Grundrechtsschutz bei behördlichen Verbunddateien	115
I.	Antiterrordatei und Antiterrordateigesetz	116
II.	Rechtsextremismusdatei und Rechtsextremismusdateigesetz	117
III.	Keine aus dem informationellen Trennungsprinzip folgende Unzulässigkeit der Einrichtung von Verbunddateien	118
IV.	Gesetzentwurf zur Änderung des ATDG und anderer Gesetze vom 15. 10. 2014	126
V.	Gewährleistung eines hinreichenden Betroffenen schutzes auch für zukünftige Verbunddateien	132
E.	Begrenzung und Regulierung der Kooperation mit Privatunternehmen bei der sicherheitsbehördlichen Datenverarbeitung	133
I.	Der „Staatstrojaner“ als intensiver Eingriff in das IT-Grundrecht	134
II.	Outsourcing als datensicherheitsrechtliches Problem	137
III.	Zukünftige Anforderungen an die Kooperation mit Privatunternehmen bei der sicherheitsbehördlichen Datenverarbeitung	149
IV.	Praktikabilität und Realisierungsstand der neuen Anforderungen an die behördliche Kooperation mit Privatunternehmen	158
F.	Verbesserung der Beweismitteltauglichkeit digitaler Daten	161
I.	Datenauthentizität und Datenintegrität als Kriterien für die Manipulationssicherheit digital gespeicherter Daten	163

II. Maßnahmen zur Verbesserung der Beweismitteltauglichkeit digitaler Daten	175
III. Ausblick auf die Zukunft digitaler Daten in der sicherheitsbehördlichen Ermittlung	187
<i>Teil 3: Zusammenfassung der gefundenen Ergebnisse und Fazit</i>	<i>189</i>
<i>Literaturverzeichnis</i>	<i>195</i>
<i>Internetquellen</i>	<i>211</i>
<i>Sachregister</i>	<i>217</i>