Inhaltsverzeichnis

Vorwort V
Inhaltsübersicht VII
Abkürzungsverzeichnis XVII

Einführung

§ 1 Die Vulnerabilität der digitalen Technik 3

I. Informationssicherheit als Systemrisiko 3

II. Informationssicherheit auf der rechtspolitischen Agenda 5

III. Informationssicherheitsdiskurs zwischen Extremen: „Going dark" vs. „Versicherheitlichung" 10

IV. Informationssicherheit als Herausforderung für Recht und Rechtswissenschaft 12

§ 2 Recht der Informationssicherheit – Annäherungen an einen regulatorischen Diskurs 17

I. Bestandsaufnahme: Vier Schlaglichter 18

1. Informationssicherheit im Informationsverwaltungsrecht und im Recht des E-Government 18
2. Informationssicherheit im Datenschutzrecht 21
3. Informationssicherheit im Recht der kritischen Infrastrukturen . . . 22
4. Informationssicherheit im Völkerrecht 23
5. Zur Notwendigkeit einer integrativen Perspektive 25

II. Begriffliche Konturierung: Datensicherheit, Informationssicherheit, IT-Sicherheit, Cybersicherheit? 26

III. Gang der Untersuchung 29

IV. Zur Methode: Nach der Neuen Verwaltungsrechtswissenschaft . 31

1. Informationssicherheit als regulatorische Aufgabe 31
2. Methodische Implikationen 38
3. Alter Wein in neuen Schläuchen?! 42

Erster Teil

Grundlagen des Informationssicherheitsrechts

§ 3 Informationssicherheitsrecht als Technikregulierung 49

I. Zur Gestaltbarkeit der Technik 50
1. Technik als Schicksal? 50
2. Technik jenseits von Mittel und Zweck 53
3. Technik als soziales System und als Möglichkeitsraum 58

II. „Recht und Technik" revisited 59
1. Von der Technikignoranz der Rechtswissenschaft 60
2. ... über die Anerkennung der staatlichen Verantwortung für die Risiken der Technik 63
3. ... zur Technikregulierung als Strukturierung des Kommunikationsprozesses zwischen Recht und Technik 65

III. Exkurs: Der Sonderweg des Datenschutzrechts 68

§ 4 Informationssicherheitsrecht in der Sicherheitsgesellschaft . 75

I. Sicherheit: Auftrag, Perspektive oder Dispositiv? 77
1. Sicherheit als staatlicher Auftrag 77
2. Vom „alten" zum „neuen" Sicherheitsrecht: Sicherheit als Perspektive 79
a) Transformationen des Sicherheitsrechts 79
b) Sicherheitsrecht als Risikorecht 80
c) Ein „neuer" Sicherheitsbegriff 82
d) Erscheinungsformen des „neuen" Sicherheitsrechts 84
3. Kritik der „Versicherheitlichung": Sicherheit als Dispositiv 88
a) Diagnose der Diskursverschiebung 88
b) Folgen für das Rechtssystem: Identifikation von Aufmerksamkeitsfeldern I 91
aa) Grundrechte 92
bb) Gewaltenteilung 92
cc) Föderale Kompetenzverteilung 93
4. Zwischenfazit 96

II. Versicherheitlichungstendenzen im Cyberraum 97
1. Der Informationssicherheitsdiskurs als illiberale Diskursverschiebung? 97
a) Entgrenzter Begriff und entgrenzter Diskurs 97
b) Zur Rolle des Militärs und der Nachrichtendienste im Bereich der Informationssicherheitsgewährleistung 99
c) Digitale Technik als „Ideologie" 101
d) Kritische Würdigung 102

2. Zur Notwendigkeit eines „All-Gefahren-Ansatzes" im Cyberraum 102
a) Komplexität der Problemlage 103
b) Attributionsproblem 104
c) Untauglichkeit der Unterscheidung von security und safety zur Erfassung von Informationssicherheitsrisiken 111
3. Folgen für das Rechtssystem: Identifikation von Aufmerksamkeitsfeldern II 112

III. Facetten der Informationssicherheit 115

Zweiter Teil

Gewährleistung von Informationssicherheit durch Recht

§ 5 Unions- und verfassungsrechtliche Rahmenbedingungen des Informationssicherheitsrechts 121

I. Grundrechte als Grenze staatlicher Informationssicherheitsregulierung 122
1. Grundrechte als Abwehrrechte gegen Maßnahmen zur Erhöhung des Informationssicherheitsniveaus 122
a) Schutz privater Betreiber informationstechnischer Systeme 122
aa) Systemische Natur und Kaskadeneffekte von IT-Sicherheitsrisiken 124
bb) Mangelnde IT-Sicherheit kein Ausdruck privater Macht . . . 125
cc) Informationssicherheitsregulierung kein Eingriff in den Kernbereich der Digitalwirtschaft 126
dd) Zwischenfazit 127
b) Schutz der Privatheitsinteressen Dritter 127
2. Abwehrrechte gegen Maßnahmen zur Senkung des Informationssicherheitsniveaus 129
a) Schutz der Vertraulichkeit und Integrität der Telekommunikation 130
b) Schutz des Zugangsbestimmungsrechts über die eigene Wohnung 134
c) Schutz des allgemeinen Persönlichkeitsrechts 140
aa) Recht auf informationelle Selbstbestimmung 140
bb) Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme 145
3. Informationssicherheit als übergreifendes Grundrechtsproblem . . . 152

II. Grundrechtliche Gewährleistungsverantwortung für die IT-Sicherheit 156
1. Maßstäbe: Grundrechtsschutz durch Informationssicherheit 157
2. Pflicht zur risikobasierten Regulierung 161

III. Zur Organisation hoheitlicher Interventionen in die Informationstechnik 163
1. Kompetenzrechtliche Determinanten für die Informationssicherheitsregulierung im Mehrebenensystem 163
a) Gesetzgebungskompetenzen 163
aa) Grundgesetz 164
bb) Unionsrecht 164
b) Verwaltungskompetenzen 167
aa) Grundgesetz 167
bb) Unionsrecht 170
2. Demokratische Legitimation der Informationssicherheitsverwaltung 172
a) Unabhängige Behörden? 173
b) Grenzen der Delegation 178
aa) Indienstnahme privaten Sachverstands 178
bb) Ermächtigung der Exekutive 180
IV. Folgerungen 181

§ 6 Gewährleistung von Informationssicherheit: Ein regulatorisches Schutzkonzept 183

I. Zur Ordnung komplexer Regulierungsregime 183
II. Strukturen des Informationssicherheitsrechts 188
1. Primat der Aufgabe: Ziele und sachlicher Umfang der Regulierung 188
a) Von den Schutzzielen zur Aufgabe Informationssicherheit 188
b) ... Aufgabe Informationssicherheit: Ein Schichtenmodell 191
aa) System- und Netzwerksicherheit 192
bb) Komponentensicherheit 196
cc) Internetsicherheit 198
c) ... von der Aufgabenbeschreibung zur rechtlichen Regulierung . 206
2. Territorialisierung des Informationssicherheitsproblems 209
a) Informationssicherheit als globales Problem 209
b) Expansive Jurisdiktionsregeln 212
c) Koordination und Kooperation 214
d) Lokalisierungspflichten 216
e) Zwischenfazit 217
3. Aufbau einer regulatorischen Kommunikations- und Wissensinfrastruktur 217
a) Informationssicherheit als Wissensproblem und als öffentliches Gut 217
b) Forschungs- und Innovationsförderung zwischen Staat und Markt 220

c) Aufbau spezialisierter Organisationseinheiten und administrativer Netzwerke zur Verarbeitung gesellschaftlich generierten Wissens . . . 221
d) Aufbau kooperativer Plattformen zum Informationsaustausch zwischen Staat und Gesellschaft . . . 224
e) Transparenzförderung durch Melde- und Informationspflichten . . . 226
f) Formen und Verfahren der Wissensdistribution . . . 230
g) Zwischenfazit . . . 231
4. Ausgestaltung der Verantwortungsarchitektur . . . 232
a) Akteure der Informationssicherheit . . . 232
b) Wandel der Verantwortlichkeitsstruktur: Von der Störerhaftung zur Inpflichtnahme privater Dritter für die Risiken der Informationstechnik . . . 233
c) Adressaten des Informationssicherheitsrechts . . . 237
aa) System- und Netzwerksicherheit . . . 237
bb) Komponenten- und Internetsicherheit . . . 241
d) Zwischenfazit . . . 244
5. Konkretisierung des Pflichtenprogramms für die Netzwerk- und Systemsicherheit . . . 244
a) Verpflichtung zu technischen und organisatorischen Maßnahmen . . . 244
b) Formen der Konkretisierung des Pflichtenprogramms („Stand der Technik") . . . 247
c) Risikobasierter Ansatz . . . 253
d) Zwischenfazit . . . 255
6. Konkretisierung des Pflichtenprogramms für die Komponentensicherheit . . . 257
a) Komponentensicherheit als neues Aufmerksamkeitsfeld des Informationssicherheitsrechts . . . 257
b) Der EU Cybersecurity Act (CSA) als risikobasierte Rahmenregelung für Zertifizierungen . . . 258
c) Der CSA im Kontext weiterer Zertifizierungsregime . . . 262
d) Produktwarnungen, -empfehlungen und -untersuchungen . . . 264
e) Zwischenfazit . . . 266
7. Internetsicherheit als terra incognita des Informationssicherheitsrechts . . . 266
8. Durchsetzung und Kontrolle . . . 268
a) Allgemeine ordnungsrechtliche Durchsetzungs- und Kontrollbefugnisse . . . 268
b) Operative Tätigkeiten: CSIRT/CERT und MIRTs . . . 269
c) Haftung . . . 270
d) Strafrechtliche Sanktionen . . . 272
III. Fazit: Vom „patchwork of confusion" zur integrativen Regulierung . . . 274

§ 7 Sicherheitsgewährleistung durch Manipulation der Informationstechnik? 279

I. Zur Doppelrolle des Staats als Garant und Gefährder der Informationssicherheit 279

II. Staatliche Governance von IT-Schwachstellen 281

1. Implikationen der Nicht-Offenlegung und Nutzung von Schwachstellen für die IT-Sicherheit: Kollisions-, Proliferations- und Einsatzrisiken 282
2. Zur staatlichen Nutzung von Schwachstellen am Beispiel der Quellen-TKÜ 285
   a) Unvollständige Würdigung der Einsatzrisiken 286
   b) Vernachlässigung der Kollisions- und Proliferationsrisiken . . . 289
3. Grundzüge einer staatlichen Schwachstellen-Governance 292
   a) Orientierungspunkte: Der Vulnerabilities Equities Process . . . 293
   b) Gestaltungselemente 295
      aa) Ziele und gesetzliche Grundlagen 295
      bb) Maßstäbe für die (Nicht-)Veröffentlichung 297
      cc) Informationssicherheit 300
      dd) Organisation und Verfahren der Schwachstellen-Governance 300
   c) Ausblick 307

III. Regulierung von Verschlüsselung 308

1. Ambivalenzen der Kryptopolitik: „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ 309
2. Ansätze staatlicher Verschlüsselungsregulierung für Online-Kommunikation 311
3. Ziele und Grenzen der staatlichen Regulierung von Verschlüsselungstechnologien 315
   a) Gewährleistungsverantwortung und Förderpflicht 315
   b) Beeinträchtigungen der Integrität von Verschlüsselungsmechanismen 315
   c) Grenzen der Verschlüsselungsregulierung 316

IV. Fazit 317

Schluss

§ 8 Ausblick 321

§ 9 Zusammenfassung in Leitsätzen 323

I. Ausgangsproblem, Gegenstand und Ziel der Untersuchung . . . 323

II. Grundlagen und Kontexte der Informationssicherheitsregulierung 324
III. Unions- und verfassungsrechtliche Rahmenbedingungen der Informationssicherheitsregulierung 326
IV. Grundzüge eines regulatorischen Schutzkonzepts 328
V. Grenzen für staatliche Manipulationen der Informationssicherheit 332

Bibliographie 333
Sachregister 407