INHALTSVERZEICHNIS

	Abkürzungen	11
	VORWORT VON WOLF-DIETER NARR	13
I.	EINLEITUNG: EINE NEUE STOFFLICHE SEITE - EIN NEUES GESETZ - EIN NEUER KONTROLLEUR	19
	Ein neues Gesetz	21
	"Beauftragte"	22
	Die Sonderstellung der Sicherheitsbehörden	22
	Datenschutz ist Grundrechtsschutz	25
	Offene Fragen	27
	Transparenzfunktion	30
	Untersuchungsgegenstand	31
	Untersuchungsgang	33
II.	DIE BESONDEREN GEFÄHRDUNGEN DES EINSATZES DER EDV IM SICHERHEITSBEREICH	37
1)	Die Polizei - keine Institution wie jede andere	38
2)	Effekte der Einführung der EDV bei den Sicherheitsbehörden	41
a)	Der Faktor Information	41
b)	Die Veränderung der traditionellen Sicherheitskonzepte unter Anwendung der EDV	44
3)	Durchbrechung bzw. Untauglichkeit bisheriger Kontrollmittel durch die Verwendung der EDV	47
	Informationsverantwortung contra Recht auf informationelle Selbstbestimmung	49
III.	DIE DATENSCHUTZBEAUFTRAGTEN - EINE ERSTE VERORTUNG EINER NEU GESCHAFFENEN INSTITUTION	53
1)	Die Datenschutzbeauftragten - ein unabhängiges, aber "rechtloses" Kontrollorgan	53
a)	Kontrollmacht: die gesetzlichen Sicherheitsvorbehalte	55
b)	Unabhängigkeit	57
c)	Die Kontrollmittel und Einflußnahme im Sicherheitsbereich	58
d)	Die gesetzliche Prärogative für juristische Kontrollstrategien	60

Bibliografische Informationen
http://d-nb.info/890030707

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

2) Die Exekutive bestimmt ihren Kontrolleur selbst 62
a) Datenschutzgesetze und die starke Position der Exekutive bei der Bestimmung ihres Kontrolleurs 62
b) Personalpolitik: Die Exekutive entscheidet sich für 'ihren' Mann oder Frau 64
c) Die Mitarbeiter: Personalpolitik als Kontrollstrategie 67
d) Der Personalkonflikt beim Bundesdatenschutzbeauftragten 71
3) Datenschutzbeauftragte: ein Konzept domestizierter Fremdkontrolle 72

IV. DATENSCHUTZ IM AUFBRUCH: DIE NEUE INSTITUTION FORMULIERT SELBSTVERSTÄNDNIS (1978-1982) 75
1) Der Anspruch: ein "Anwalt des Bürgers" 76
2) Zur Konfliktbereitschaft 82
3) Zwischen Konflikt und Kooperation 85

V. ENTTABUISIERUNG DES SICHERHEITSBEREICHES: DIE DATENSCHUTZBEAUFTRAGTEN UND IHRE TÄTIGKEITSBERICHTE 87
1) Datenschutzberichte und Öffentlichkeit 88
2) Die Datenschutzinstitutionen: 1972 bis 1977 91
a) Hessen 91
b) Rheinland-Pfalz 98
3) Die Phase von 1972 bis 1977: datenschützerische Ornamentik 100
4) 1978: die Enttabuisierung des Sicherheitsbereiches beginnt 104

VI. DAS INFORMATIONS- UND KONTROLLPROFIL DER DATENSCHUTZBEAUFTRAGTEN IM SICHERHEITSBEREICH 107
1) Die polizeilichen Informationssysteme und ihre Darstellung in den Tätigkeitsberichten anhand einzelner Beispiele 108
a) Das System PIOS - eine neue Qualität polizeilicher Datenverarbeitung 109
Das System PIOS in den Tätigkeitsberichten 111
Exkurs: Der Kriminalpolizeiliche Meldedienst in Staatsschutzsachen 122
PIOS-Verfahren und die KpS- bzw. die BKA-Richtlinien 126
PIOS - Leerlauf individualrechtlicher Regelungskonzepte 129

b)	Spurendokumentationssysteme (SPUDOK)	131
	SPUDOK-Systeme in den Tätigkeitsberichten	134
	Meldung der SPUDOK-Anwendungen an die Datenschutzinstanzen	141
	Festlegung des betroffenen Personenkreises bzw. der Speicherungsvoraussetzungen	142
	Die Forderung nach kurzen Speicherfristen	144
	Zweckbindungsgrundsatz und SPUDOK-Dateien	148
	Zusammenfassung: SPUDOK	149
c)	Der Kriminalaktennachweis (KAN)	151
	Der KAN in den Tätigkeitsberichten	155
	Die physikalische Verfügbarkeit des gesamten KAN beim BKA	157
	KAN: Ein Konzept wird unterlaufen	163
	Der KAN und die Struktur der Datenverarbeitung des INPOL	167
2)	Die geheimdienstlichen Informationssysteme	174
a)	Verfassungsschutz und "Linksextremismus"	179
	Erfassung ist nicht gleich Erfassung	186
b)	Amtshilfe zwischen Polizei und Nachrichtendiensten	
	Die So-GK	190
	Amtshilfe zwischen Nachrichtendiensten und übriger Polizei	194
	Das Trennungsgebot - vergebliches Mühen	198
c)	Sicherheitsüberprüfung - ein wenig bekannter Bereich	202
	Der datenschützerische Forderungskatalog	206
	Zur Praxis der Sicherheitsüberprüfungen beim MAD	207
	Sicherheitsprüfungen zur Eigensicherung	211
	Sicherheitsüberprüfungen und Transparenz: eine Kernforderung der Datenschutzbeauftragten	212
	Das Gebot der Zweckbindung und Sicherheitsüberprüfungen	219
d)	Die Sonderrolle der Geheimdienste in den Tätigkeitsberichten	225
	Geheimdienste - überwiegend weiße Flecken	226
	Geheimhaltung und Transparenz	232
	Kritik und ihre Verpackung	234
3)	Gemeinsame Problemlagen bei Polizei und Geheimdiensten	236
a)	"Altfälle"	236
aa)	"Altfälle" bei der Polizei	236
	Die Angst vor Informationsverlusten: Das Beispiel Baden-Württemberg	242
aa)	"Altfälle" bei den Geheimdiensten	245
b)	Einführung der Zeitspeicherung	248
c)	Informationsosmose der Sicherheitsbehörden:	
	Verdachtsstreuung und Parallelspeicherung	255
	Die Abhilfe: Nachberichtung?	261
	"Versteckte" Parallelspeicherung: Die Anfrage-Speicherung	263
d)	Datenübermittlung und Relevanzprüfung	267
e)	Protokollbänder/Sicherungsbänder	274
	Dateninhalte der Protokolldateien	275
	Aufbewahrungsdauer	276
	Verwertung der Protokolldateien	277
	Protokollierung und Datenschutz	280

4)	Datenschutzrechtliche Kontrolle und ihre Behinderung	282
a)	Die Staatswohlklausel und ihre Anwendung	283
b)	Bestreiten der Kontrollkompetenz: Akten-Dateien	286
	Beispiel Niedersachsen	288
	Beispiel Bund	290
	Fazit	292
c)	Kontrollausschluß bei G 10-Daten	293
d)	Das Steuergeheimnis: Wie "linkt" man einen Datenschutzbeauftragten?	296
e)	Politik der Nadelstiche: aus dem Arsenal der Kontrollbehinderungen	301
5)	Das Kontrollprofil der Datenschutzbeauftragten: Fazit	305
	Zwischen Transparenz und Konspiration	307
	Kontrollausschuß und Kontrollkompetenz	310
	Erfolge: eine erste Bilanz	311
	Kontrollprofil: Nachbesserung	314

VII.	DIE ROLLE DER DATENSCHUTZBEAUFTRAGTEN BEI DER SCHAFFUNG BEREICHSSPEZIFISCHER REGELUNGEN	317
1)	Das Melderechtsrahmengesetz des Bundes	322
a)	Zur Vorgeschichte	322
b)	Das Melderechtsrahmengesetz von 1980 - ein datenschutzrechtliches Mißverständms	326
	Zum Umfang des Datensatzes	327
	Von der Personenkennziffer zum Personenkennzeichen	328
	Statt Landesadreßregister online-Zugriff für die Polizei	332
	Fazit	338
2)	Das Gesetz zur Einführung des maschinenlesbaren Personalausweises	338
a)	Der maschinenlesbare Ausweis im Konzept der polizeilichen Sicherheitswahrnehmung	341
b)	Die Fiktion: der <datenschutzgerechte> maschinenlesbare Personalausweis	343
	November 1983: Noch immer der <datenschutzgerechte> Ausweis	347
c)	Späte Einsicht: Vorsichtige Zweifel an der verfassungsrechtlichen Zulässigkeit der Maschinenlesbarkeit	348
d)	Zusammenfassung: Von den Folgen eines Mißverständnisses	351
3)	ZEVIS - von der normativen Kraft des Faktischen	354
a)	ZEVIS - die drittgrößte Datensammlung der Republik erweckt Begehrlichkeiten	357
	Das sicherheitsbehördliche Interesse an ZEVIS	359
b)	ZEVIS und die Kritikpunkte der Datenschutzbeauftragten	361
	Die Verwaltung setzt Fakten	362
ba)	Die bürgerrechtliche Brisanz der online-Abfrage: die coupierte Kritik der Datenschutzinstanzen	366
bb)	Kritik ohne Spitze: die Kritik an der H-Abfrage	369
bc)	ZEVIS und die Frage der Kontrollierbarkeit	371

c) ZEVIS - kein Datenschutz 375
4) Bereichspezifische Regelungen: Ein Konzept scheitert 378
Die unbegründetete Angst der Exekutive 381
Bereichsspezifische Regelungen: Die Exekutive erkennt ihre Chance 384

VIII. DER INSTITUTIONELLE DATENSCHUTZ: KEIN GRUND ZUR BERUHIGUNG 387

Der informationstechnische Effizienzschub steht noch bevor 389
1) Transparenz als Chance 391
2) Institutioneller Datenschutz - gebremster Datenschutz 395
3) Resüme: Ein Organ fachspezialisierter exekutiver Öffentlichkeitsarbeit 398
Zwischen Kooperation und Kontrolle 402
Abschaffung der Datenschutzbeauftragten? 404

Literaturverzeichnis 411