

Inhaltsverzeichnis

Seite Rand-
Nummer

Vorwort	5	
Inhaltsverzeichnis	7	
Abkürzungsverzeichnis	15	
1.	Politische Initiativen zum elektronischen Geschäftsverkehr	19 1 – 42
	<i>Prof. Dr. Bernd Holznapel / Tarik Tabbara</i>	
1.1	Bundesrepublik Deutschland	19 2 – 5
1.2	EU	21 6 – 25
1.2.1	Europäische Initiative für den elektronischen Zahlungsverkehr.	21 6
1.2.2	Bonner Erklärung	23 10
1.2.3	Towards A European Framework for Digital Signatures.	25 14
1.2.4	Aktivitäten der Kommission im Bereich des elektronischen Zahlungsverkehrs.	26 16
1.2.4.1	Mitteilung der Kommission: Stärkung des Ver- trauens der Kunden in elektronische Zahlungsmi- tel im Binnenmarkt	26 18
1.2.4.2	Empfehlung der Kommission: Zu den Geschäften, die mit elektronischen Zahlungsinstrumenten getätigt werden.	29 23
1.3	USA	30 26 – 30
1.4	Joint EU-US Statement on Electronic Commerce.	32 31
1.5	OECD	33 32 – 36
1.6	WTO	35 37
1.7	UN	35 38
1.8	Zusammenfassende Wertung	35 39 – 42
2.	Verletzlichkeitspotentiale	39 43 – 411
2.1	Öffentlichrechtliche Hemmnisse für die Einführung des elektronischen Zahlungsverkehrs	39 43 – 100
	<i>Prof. Dr. Bernd Holznapel / Tarik Tabbara</i>	
2.1.1	Einschränkungen beim Einsatz kryptographischer Verfahren	39 43
2.1.1.1	Bundesrepublik Deutschland	41 47

2.1.1.1.1	Keine Beschränkung der Verwendung kryptographischer Verfahren	41	47
2.1.1.1.2	Ausführbestimmungen für kryptographische Produkte	42	49
2.1.1.2	Europäische Union	42	51
2.1.1.3	USA	45	55
2.1.1.3.1	Restriktive Kryptographiepolitik der USA	45	56
2.1.1.3.2	Ausfuhr kryptographischer Produkte nach den Export Administration Regulations	47	60
2.1.1.3.3	Auswirkungen auf den elektronischen Zahlungsverkehr	50	66
2.1.1.4	OECD	54	75
2.1.1.5	Weitere Entwicklung	55	77
2.1.2	Währungsrechtliche Beschränkungen	56	80
2.1.2.1	Bundesrepublik Deutschland	57	82
2.1.2.1.1	Notenausgabemonopol	57	82
2.1.2.1.2	Keine unbefugte Ausgabe von Geldzeichen	57	83
2.1.2.1.3	Keine Mindestreservepflicht für elektronische Zahlungsmittel	58	85
2.1.2.2	EU	61	92
2.1.2.2.1	Monopolisierung der Herausgabe elektronischen Geldes bei der Europäischen Zentralbank	61	92
2.1.2.2.2	Einführung einer Mindestreservepflicht	62	93
2.1.2.3	USA	63	94
2.1.2.3.1	Währungsmonopol	63	94
2.1.2.3.2	Keine Mindestreservepflicht für elektronisches Geld	64	98
2.2	Zivil- und bankenrechtliche Hemmnisse für die Einführung technischer Sicherungsverfahren	66	101 – 172
	<i>Prof. Dr. Thomas Hoeren / Ute Decker</i>		
2.2.1	Bankenaufsichtsrecht als akzeptanzerhöhender Faktor	66	101
2.2.1.1	Die Bankenaufsicht nach deutschem Recht	67	– 103
2.2.1.1.1	Die grundlegenden Regelungen der Bankenaufsicht	67	103
2.2.1.1.2	Die Beurteilung von Ecash und Millicent nach der 6. KWG-Novelle: Einführung der Aufsichtsbefugnis über Netzgeldgeschäfte (§ 1 Nr. 11 und 12 KWG)	68	105
2.2.1.1.2.1	Einschätzung von Ecash als generell einsetzbares Tokensystem als Prämisse	70	108

2.2.1.1.2.2	Das Kriterium des bargeldähnlichen Inhaberpapiers	70	108
2.2.1.1.2.2.1	Vergleich von Ecash mit Bargeld nach funktio- nalen Kriterien	71	109
2.2.1.1.2.2.1.1	Darstellung des Zahlungsvorgangs aus bankrecht- licher Sicht	71	110
2.2.1.1.2.2.1.2	Juristische Bewertung des Zahlungsvorgangs	72	112
2.2.1.1.2.2.2	Fazit	74	114
2.2.1.1.2.3	Abgrenzung von Netzgeld über die Eignung zur Substitution von Bargeld	74	115
2.2.1.1.2.4	Abgrenzung über die Unabhängigkeit von Buchgeldkonten	75	118
2.2.1.1.2.5	Ergebnis der Erarbeitung der Abgrenzungskriterien	76	119
2.2.1.1.2.6	Anwendung der Kriterien auf Millicent.	76	120
2.2.1.1.2.6.1	Die Verwaltung und der Einsatz von Millicent . . .	76	121
2.2.1.1.2.6.2	Beurteilung von Millicent nach § 1 I KWG.	77	123
2.2.1.1.2.6.3	Ergebnis für Millicent	78	124
2.2.1.1.3	Aufsicht über den Einsatz von SET nach allgemeinen Grundsätzen des KWG	79	125
2.2.1.1.4	Konsequenzen der Aufsicht.	80	127
2.2.1.2	Die Bankenaufsicht nach europäischer Regulierung	82	131
2.2.1.2.1	Der Status Quo.	82	132
2.2.1.2.1.1	Der Entwurf einer Richtlinie über die Aufnahme und das Betreiben des Geschäfts mit elektroni- schen Zahlungsmitteln und dessen Beaufsichtigung (on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions)	83	133
2.2.1.3	US-amerikanische Tendenzen im Bankrecht.	85	138
2.2.2	Geldwäschekontrolle als absolutes Hindernis für einen konsequenten Datenschutz.	88	144
2.2.2.1	Die Problematik der Geldwäschekontrolle im Lichte des Datenschutzrechts.	88	144
2.2.2.2	Die Geldwäschekontrolle nach deutschem Recht .	89	146
2.2.2.2.1	Adressaten des Gesetzes: Wer ist betroffen?	89	147
2.2.2.2.2	Pflichten der Adressaten nach dem GeldwäscheG	91	150
2.2.2.2.2.1	Allgemeine Identifizierungspflicht	91	150
2.2.2.2.2.2	Pflicht zur Identifizierung bei Kontoeröffnung . . .	92	153
2.2.2.2.2.3	Pflicht zur Identifizierung bei Kenntnis von Ver- dachtsmomenten	93	154
2.2.2.2.2.4	Die Pflicht zur Vornahme interner Sicherungsmaß- nahmen.	94	155

2.2.2.2.3	Gesetzgebungsvorhaben	95	158
2.2.2.3	Die Europäische Dimension der Geldwäschekon- trolle.	96	159
2.2.2.3.1	Die bekannte Richtlinie vom 10. Juni 1991	96	160
2.2.2.3.2	Weitere Initiativen innerhalb der Europäischen Union:	97	161
2.2.2.4	Die Tendenzen in den USA.	98	163
2.2.2.5	Begrenzung zukünftiger Entwicklungen durch das Bedürfnis nach Transparenz der Zahlungsströ- me zu Zwecken der Bekämpfung des organisierten Verbrechens.	100	168
2.2.2.6	Internationale Initiativen	101	171
2.3	Erfordernis positiver Strukturleistungen beim Aufbau eines Sicherungssystems.	102	173 – 260
	<i>Prof. Dr. Bernd Holznagel / Regine Lorenz</i>		
2.3.1	Festschreiben von Standards	102	173
2.3.1.1	Datensicherheit	103	174
2.3.1.1.1	Sicherheit von Telekommunikationsnetzen.	105	179
2.3.1.1.1.1	Bundesrepublik Deutschland.	105	180
2.3.1.1.1.2	EU	107	185
2.3.1.1.1.3	USA	109	189
2.3.1.1.1.4	Zusammenfassung	110	191
2.3.1.1.2	Verschlüsselung.	111	192
2.3.1.1.2.1	Deutschland.	111	193
2.3.1.1.2.2	EU	112	195
2.3.1.1.2.3	USA	114	198
2.3.1.1.2.4	International.	116	203
2.3.1.1.3	Sichere Gestaltung der Softwareumgebung	116	204
2.3.1.2	Authentizität und Verbindlichkeit	118	208
2.3.1.2.1	Bundesrepublik Deutschland.	119	210
2.3.1.2.1.1	Infrastruktur.	120	211
2.3.1.2.1.2	Implementierung der von uns näher untersuchten Systeme in diese Infrastruktur.	122	217
2.3.1.2.1.2.1	Technische Voraussetzungen	122	218
2.3.1.2.1.2.2	Einbindung in die zweistufige Hierarchie des SigG124 Europa	125	223
2.3.1.2.2	USA	128	231
2.3.1.2.3.1	Regelungsansätze in den Bundesstaaten	129	232
2.3.1.2.3.2	Bundesregelungen	131	235
2.3.1.2.3.2.1	Kongress	131	236
2.3.1.2.3.2.2	ABA Guidelines	133	239

2.3.1.2.4	Internationale Organisationen	134	242
2.3.1.2.4.1	OECD	134	242
2.3.1.2.4.2	ICC	135	244
2.3.1.2.4.3	UN	136	246
2.3.1.2.5	Zusammenfassung	137	248
2.3.2	Gewährleistung dieser Standards	138	250
2.3.2.1	Bundesrepublik Deutschland	138	251
2.3.2.2	EU	139	253
2.3.2.3	USA	140	254
2.3.2.4	International	141	257
2.3.3	Zusammenfassung und Ausblick	141	258
2.4	Strafrechtliche Fragen	143	261 – 299
	<i>Prof. Dr. Bernd Holznapel / Regine Lorenz</i>		
2.4.1	Deutschland	143	262
2.4.1.1	Prozessuale Fragen	143	262
2.4.1.1.1	Anwendbarkeit des deutschen materiellen Strafrechts	143	262
2.4.1.1.2	Behandlung von Daten im Strafverfahren	144	265
2.4.1.2	Materiellrechtliche Fragen	145	266
2.4.1.2.1	Verletzung der privaten und/oder beruflichen Geheimnissphäre: Ausspähen von Daten § 202 a StGB, Verletzung des Fernmeldegeheimnisses § 206 StGB, Verrat von Betriebsgeheimnissen § 17 UWG, § 43 BDSG	146	267
2.4.1.2.2	Datenveränderung, Computersabotage, Fälschung beweisheblicher Daten	147	270
2.4.1.2.3	Computerbetrug	148	272
2.4.1.2.4	Sonstige Straftatbestände	148	273
2.4.2	EU und Europarat	149	274
2.4.3	USA	152	281
2.4.3.1	Gesetzgebungskompetenzen	152	281
2.4.3.2	Örtliche und sachliche Zuständigkeiten	153	283
2.4.3.3	Materielles Bundesrecht	153	284
2.4.3.4	Staatenrecht	155	288
2.4.4	OECD, Vereinte Nationen, AIDP; Bank for International Settlement	157	292
2.4.4.1	OECD	158	293
2.4.4.2	Vereinte Nationen	158	294
2.4.4.3	AIDP	159	295
2.4.4.4	Bank for International Settlements	159	296

2.4.5	Zwischenergebnis und mögliche Entwicklungstendenzen	160	297
2.5	Zivilrechtliche Haftung beim elektronischen Zahlungsverkehr im Internet	161	300 – 411
	<i>Prof. Dr. Thomas Hoeren / Rufus Pichler</i>		
2.5.1	Gegenstand und Gang der Darstellung	162	301
2.5.2	Ecash	163	302
2.5.2.1	Technischer Hintergrund und Funktionsweise aus spezifisch haftungsrechtlicher Sicht	163	303
2.5.2.1.1	Beteiligte	163	304
2.5.2.1.2	Darstellung des Zahlungsverganges	164	305
2.5.2.1.3	Besonderheiten mit Bedeutung für die haftungsrechtliche Beurteilung	169	315
2.5.2.2	Denkbare Haftungs- und Risikofälle	171	319
2.5.2.3	Haftungsrechtliche Beurteilung der Problemfälle	172	323
2.5.2.3.1	Übergreifende rechtliche Fragestellungen – Rechtsbeziehungen und Rechtsnatur	172	323
2.5.2.3.1.1	Vertragsrechtliche Betrachtungsweise	173	325
2.5.2.3.1.2	Wertpapierrechtlicher Ansatz	181	341
2.5.2.3.2	Haftung in einzelnen Problemfällen	186	351
2.5.2.3.2.1	Datenverlust	186	352
2.5.2.3.2.1.1	Verhältnis Kunde – Bank	187	352
2.5.2.3.2.1.2	Verhältnis Kunde – Händler	193	366
2.5.2.3.2.2	Datenmißbrauch	193	367
2.5.2.3.2.2.1	Verhältnis Kunde – Bank	194	368
2.5.2.3.2.2.2	Verhältnis Kunde – Händler	198	377
2.5.2.3.2.3	Sonstige Probleme	199	381
2.5.3	SET	200	382
2.5.3.1	Funktionsweise aus spezifisch haftungsrechtlicher Sicht	200	383
2.5.3.1.1	Beteiligte	201	384
2.5.3.1.2	Zahlungsvergang	201	385
2.5.3.2	Mögliche Haftungsfälle	202	387
2.5.3.3	Haftungsrechtliche Beurteilung der problematischen Fälle	202	388
2.5.3.3.1	Übergreifende rechtliche Fragestellungen – Rechtsbeziehungen zwischen den Beteiligten	203	389
2.5.3.3.2	Einzelne Haftungsprobleme bei Verwendung von SET	205	394
2.5.4	Millicent	206	397

2.5.4.1	Funktionsweise von Millicent aus spezifisch haftungsrechtlicher Sicht.	207	398
2.5.4.2	Haftungsrechtliche Beurteilung von Millicent.	208	401
2.5.4.2.1	Übergreifende rechtliche Fragestellungen	209	402
2.5.4.2.2	Haftungsrechtliche Beurteilung einzelner Konstellationen.	212	409
3.	Datenschutzrechtliche Aspekte des elektronischen Zahlungsverkehrs.	215	412 – 470
	<i>Prof. Dr. Bernd Holznagel / Regine Lorenz / Tarik Tabbara</i>		
3.1	Einleitung.	215	412 – 416
3.2	Datenschutz in der Bundesrepublik Deutschland	217	416 – 435
3.2.1	Anwendbares Recht	217	417
3.2.2	Datenschutzrechtliche Probleme der Anwendung	220	424
3.2.2.1	Konzepte der Zahlungsmittel.	221	425
3.2.2.2	Potentielle Gefährdungen aus allgemeinen Anwendungen des Internet.	222	428
3.2.2.2.1	DNS-Spoofing	223	429
3.2.2.2.2	Ausspähung von Daten mittels CGI	223	430
3.2.2.2.3	Cookies	223	431
3.2.2.2.4	Datamining.	225	434
3.2.2.2.5	Einsatz mobiler und/oder intelligenter Agenten	225	435
3.3	EU	226	436 – 448
3.3.1	Geltende Regelungen.	226	437
3.3.2	Anforderungen nach politischen Initiativen.	231	446
3.4	USA	232	449 – 463
3.4.1	Bestehende gesetzliche Bestimmungen zum Schutz personenbezogener Daten beim elektronischen Zahlungsverkehr.	233	451
3.4.2	Diskussion datenschutzrechtlicher Bestimmungen im Zusammenhang mit der National Information Infrastructure	237	458
3.5	OECD.	240	464 – 467
3.6	Zusammenfassung	242	468 – 470
4.	Zusammenfassungen	245	471 – 489
4.1	Zusammenfassung des Kapitels „Politische Initiativen zum elektronischen Geschäftsverkehr“.	245	471 – 472

4.2	Zusammenfassung des Kapitels „Einschränkungen beim Einsatz kryptographischer Verfahren“	245	473 – 474
4.3	Zusammenfassung des Kapitels „Währungsrechtliche Beschränkungen“	246	475 – 476
4.4	Zusammenfassung des Kapitels „Festschreibung von Standards“	247	477 – 478
4.5	Zusammenfassung der Beiträge zu den rechtlichen Rahmenbedingungen des elektronischen Zahlungsverkehrs	248	479 – 481
4.5.1	Bankenaufsichtsrecht als vertrauensbildender Faktor	248	479
4.5.2	Geldwäschekontrolle als absolutes Hindernis für einen konsequenten Datenschutz	248	480
4.6	Zusammenfassung des Kapitels „Strafrechtliche Fragen“	249	482 – 483
4.7	Zusammenfassung des Abschnitts: „Zivilrechtliche Haftung beim elektronischen Zahlungsverkehr im Internet“	250	484 – 486
4.8	Zusammenfassung des Kapitels „Datenschutzrechtliche Aspekte des elektronischen Zahlungsverkehrs“	251	487 – 489
	Literaturverzeichnis	253	
	Stichwortverzeichnis	275	