Inhaltsverzeichnis

Abkürzungsverzeichnis 15

Einleitung 17

Erster Teil: Die Fälschung beweiserheblicher Daten, § 269 StGB – Revision eines Fälschungsdelikts 19

§ 1 Datenfälschung als ein Aspekt der Computerkriminalität 19
A. Begriffs- und Inhaltsbestimmung der Computerkriminalität 20
B. Qualitative Bewertung unter Berücksichtigung kriminologischer Aspekte 21
C. Internationale Initiativen zur Bekämpfung der Computerkriminalität 23

§ 2 Die Fälschung beweiserheblicher Daten im Normgefüge der Urkundendelikte 24
A. Die Einführung des § 269 StGB durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität 1986 24
B. Das durch § 269 StGB geschützte Rechtsgut 26
I. Der Meinungsstand zum Rechtsgut von § 267 StGB 26
II. Stellungnahme und Lösung 27
1. Die herrschende Lehre und die Rechtsprechung 27
2. Der Schutz des Vertrauens in die Wahrheit der Form 29
3. Reinheit und Zuverlässigkeit des Beweises 31
4. Die Garantiefunktion der Urkunde 32
a) Das Interesse des Einzelnen und des Rechtsverkehrs an der Echtheit der Urkunde 32
aa) Echtheit von Urkunden 32
bb) Vorrangig ein Interesse des Einzelnen an der Echtheit 34
b) Die Garantiefunktion und qualifizierte elektronische Signaturen 34
aa) Erleichtertes Aufspüren von Veränderungen an Datenurkunden 34
bb) Überwiegend fakultativer Einsatz der Signatur 35
c) Die Inkompatibilität der Zufallsurkunde mit der Garantiefunktion 36

aa) Die dogmatische Konstruktion und ihre praktische Relevanz 36
bb) Signierte Datenurkunden sind Absichtsurkunden 37
III. Ergebnis 37
C. Objektiver Tatbestand: § 269 als Parallelvorschrift zu § 267 StGB 38
I. Die Merkmale des Tatobjekts Datenurkunde 38
1. Anlehnung an den Urkundenbegriff 38
2. Die Definitionsfiktion des § 269 StGB 39
a) Inhalt der Definitionsfiktion 39
b) Abstraktionsschritte bei der Anwendung der Fiktion 41
3. Fehlende visuelle Wahrnehmbarkeit als Merkmal der Datenurkunde 41
a) Die Unterscheidung nach dem Speichermedium 41
b) Anknüpfung an die Bestimmung der Daten 43
c) Lösung: Erfordernis der maschinellen Verarbeitung mit lesbarem Ergebnis 44
4. Die Form der Verkörperung 45
a) Verkörperung von Daten bedeutet Datenspeicherung 45
b) Anforderung an die dauerhafte Datenspeicherung 46
c) Fazit 47
5. Keine Unterscheidbarkeit von Originalverkörperung und Kopie 48
6. Beweiserhebliche Daten 49
7. Der Aussteller der Datenurkunde 50
a) Der Aussteller ist der Erklärende 50
b) Sonderproblem der mehrdeutigen Ausstellerangabe der signierten Erklärung 52
8. Unechtheit der Datenurkunde 53
9. Ergebnis: Die Definition der Datenurkunde 54
II. Begehungsmodalitäten 54
1. Speichern 54
2. Verändern gespeicherter Daten 54
3. Gebrauchen der Daten 55
D. Subjektiver Tatbestand 56

Zweiter Teil: Die technischen und rechtlichen Grundlagen qualifizierter elektronischer Signaturverfahren 57

§ 1 Begriffsklärung: Elektronische Signatur oder Digitale Signatur 57
A. Elektronische Signaturen 58
B. Digitale Signatur 59
C. Ergebnis 60

§ 2 Technische Funktionsweise eines digitalen Signaturverfahrens 60
A. Prinzipielle Funktionsweise der kryptographischen Verfahren 62

I. Symmetrische Signaturverfahren (Private Key Cryptography) 62
II. Asymmetrische Signaturverfahren (Public Key Cryptography) 63
B. Funktionsweise der digitalen Signatur 65
I. Symmetrische Erzeugung eines digitalen Fingerabdruckes (Hashwert) 66
II. Erzeugung und Übermittlung der signierten Daten 67
III. Signaturprüfung 67
1. Sicherstellung der Datenintegrität 67
2. Sicherstellung der Datenauthentizität 68
C. Zusammenfassung 68

§ 3 Rechtliche Rahmenbedingungen für die qualifizierte elektronische Signatur 69
A. Technische Rahmenbedingungen des Signaturgesetzes 70
I. Der Regelungsumfang zum Fälschungsschutz 70
II. Unterscheidung zwischen drei Signaturverfahren 70
1. Einfache elektronische Signatur nach § 2 Nr. 1 SigG 70
2. Fortgeschrittene elektronische Signatur nach § 2 Nr. 2 SigG 71
3. Qualifizierte elektronische Signaturen 71
a) Qualifizierte elektronische Signatur nach § 2 Nr. 3 SigG 72
b) Akkreditierte qualifizierte elektronische Signatur nach § 2 Nr. 15 i.V.m. § 15 Nr. 1 SigG 73
B. Fälschungssensible Aufgaben der Zertifizierungsdienste nach dem Signaturgesetz 73
I. Identifikation des Antragstellers 74
II. Schlüsselgenerierung 74
III. Die Zertifizierung 74
1. Qualifizierte Zertifikate nach § 2 Nr. 7 SigG 74
2. Der Zertifikatsinhalt nach § 7 Abs. 1 bis 2 SigG 75
IV. Unterhaltung eines Verzeichnis- und Sperrdienstes 75
V. Zeitstempeldienste 76
VI. Unterrichtungspflicht 76
VII. Überwachungsmechanismen 76
C. Gleichstellung der qualifizierten elektronischen Signatur mit der herkömmlichen Unterschrift 77
I. Formanpassung im Zivilrecht 77
II. Formanpassung im Öffentlichen Recht 78

§ 4 Kurzer Überblick über die Einsatzfelder 79

Dritter Teil: Die Datenurkundenqualität der Elemente des Signaturverfahrens 81

§ 1 Die signierten Daten 81
A. Das Signieren einer Erklärung in Datenform 82
I. Inhalt und Aussteller der Erklärung – Privatautonomie 82

II. Funktionsäquivalenz mit einer Unterschrift 83
III. Gelangen in den Rechtsverkehr 83
IV. Fazit 83
B. *Exkurs:* Das Signieren anderer Daten als Erklärungsdaten 84
I. Die Signatur ist kein Verschlusszeichen 84
II. Die Signatur als mögliches Beweiszeichen 85
1. Übertragung des Konzepts der Beweiszeichen auf Datenerklärungen 85
2. Die Verbindung von Daten 86
a) Lösung der herrschenden Lehre 86
b) Gegenansichten und Stellungnahme 86
c) Die Verbindung zwischen Signatur und signierten Daten 87
3. Abgrenzung zu den Kennzeichen 88
III. Fazit 89
C. Die Vereinbarkeit der Verschlüsselung mit der Verständlichkeit der Erklärung 90
D. Erfüllung der übrigen Voraussetzungen einer Datenurkunde 91
I. Fehlende visuelle Wahrnehmbarkeit 91
II. Dauerhafte Verkörperung 91
III. Beweiserheblichkeit 92
E. Ergebnis 92

§ 2 Das qualifizierte Zertifikat 92
A. Der Inhalt des Zertifikats nach § 7 SigG 93
I. Das Zertifikat als Kennzeichen 93
II. Modifikation des Beweis-Kennzeichen-Regulativs 95
1. Bisherige Modifikationen durch die Rechtssprechung 95
2. Modifikation in Bezug auf qualifizierte Zertifikate 95
a) Erteilungsumstände 96
b) Erfüllung der gesetzlichen Vorgaben an Inhalt und technische Gestaltung 96
III. Fazit 97
B. Gelangen in den Rechtsverkehr - Die Zuteilung des Zertifikats 97
C. Erfüllung der übrigen Voraussetzungen einer Datenurkunde / Zwischenergebnis 97
D. Das qualifizierte Zertifikat als öffentliche Datenurkunde 97
I. Amtsträgereigenschaft des Ausstellers 98
1. Die Rechtslage unter dem ersten Signaturgesetz von 1997 98
2. Die Unterscheidung zwischen akkreditierten und genehmigten Zertifizierungsdiensten nach dem Signaturgesetz von 2001 98
a) Freiwillig akkreditierte Zertifizierungsdienste 99
b) Genehmigungsfrei betriebene Zertifizierungsdienste 100
3. Fazit 101
E. Ergebnis 101
F. Urkundenqualität des Zertifikatsverzeichnisses 101

§ 3 Die Signaturkarte 102
A. Daten und Karte als zusammengesetzte Datenurkunde 103
I. Auswirkung der Nichtunterscheidbarkeit von Originaldaten und Datenkopie 103
II. Lösungsansatz von *Puppe* 103
III. Stellungnahme und Ergebnis 103
B. Anwendung auf die Signaturkarte 104
I. Bezugnahme der Daten 104
II. Theorie des Inkarnationsschutzes 105
1. Darstellung 105
2. Stellungnahme und Ergebnis 106
III. Weitere Überlegungen zur Urkundenqualität der Signaturkarte 106
C. Ergebnis 107

§ 4 Der qualifizierte Zeitstempel 108
A. Die mit dem qualifizierten Zeitstempel abgegebene Erklärung 108
B. Erfüllung der übrigen Voraussetzungen einer Datenurkunde 108
C. Der qualifizierte Zeitstempel als öffentliche Datenurkunde 109
D. Ergebnis 109

Vierter Teil: Die Strafbarkeit der Fälschung signierter Datenurkunden 110

§ 1 Missbrauch einer fremden Signaturkarte 111
A. Kenntnis der PIN aufgrund Nachlässigkeit des Karteninhabers, § 269 StGB 112
I. Grundsätze der zivilrechtlichen Rechtsscheinhaftung 112
II. Rechtscheinhaftung bei qualifizierten elektronischen Signaturen 113
1. Aussage des Signaturgesetzes zur Rechtsscheinhaftung 113
2. Voraussetzungen der Rechtsscheinhaftung für signierte Erklärungen 114
a) Rechtsscheintatbestand 114
b) Gutgläubigkeit des Empfängers 115
c) Zurechnung 115
d) Fazit 115
III. Einfluss der Rechtsscheinhaftung auf die Echtheit im Sinne des § 267 StGB 115
1. Meinungsstand 116
2. Stellungnahme 116
IV. Vorliegen der Voraussetzungen der Rechtsscheinshaftung / Ergebnis 117
B. Ausforschen und Verwenden der Zugangs-PIN 117
I. Ausforschen der Zugriffs-PIN, § 202a StGB 117
II. Verwendung der ausgeforschten Zugriffs-PIN zur Signaturerzeugung, § 269 StGB 118
C. Kopieren einer Signaturkarte 118

D. Ergebnis 118

§ 2 Vortäuschen einer Identität gegenüber dem Zertifizierungsdienst 119
A. Erzeugung eines qualifizierten Zertifikats und Signierschlüssels durch den Zertifizierungsdienst nach Identitätstäuschung 120
I. § 269 StGB 120
II. Täuschung gegenüber Zertifizierungsdiensten 120
B. Einsatz des mittels Identitätstäuschung erwirkten Zertifikats und Signierschlüssels im Rechtsverkehr, § 269 StGB 121
C. Ergebnis 121

§ 3 Unterschieben eines Dokuments zur unbemerkten Signatur 121
A. Einschmuggeln in das Signierverzeichnis 122
I. §§ 269 Abs. 1 Alt. 1, 25 Abs. 1 Alt. 2 StGB 123
II. § 274 Abs. 1 Nr. 2 StGB 124
III. Fazit 124
B. Abfangen und Austauschen der zur Signaturerzeugung an die Chipkarte gesendeten Daten 125
I. §§ 269 Abs. 1 Alt. 1, 25 Abs. 1 Alt. 2 StGB 125
II. Fazit 126
C. Unterschieben durch Beeinflussung der Datenpräsentation 126
I. Manipulation der Datenpräsentation beim Erzeuger der Signatur 128
1. Das Kriterium des Erklärungsbewusstseins 128
2. Korrektur durch den Sorgfaltsmaßstab der Rechtsscheinhaftung 129
3. Fazit 130
II. Manipulation der Datenpräsentation beim Empfänger signierter Daten 130
III. Fazit 130
D. Ergebnis 131

§ 4 Veränderung signierter Erklärungen nach der Signaturerzeugung 131
A. Veränderung der signierten Erklärung durch einen Dritten 131
B. Die Problematik der „Fälschung" durch den Aussteller 132
I. § 269 Abs. 1 Alt. 1 StGB 132
II. § 274 Abs. 1 Nr. 2 StGB 132
III. § 303a Abs. 1 StGB 133
C. Ergebnis 133

§ 5 Manipulation eines qualifizierten Zertifikats im öffentlichen Verzeichnis des Zertifizierungsdienstes 133
A. Veränderung eines qualifizierten Zertifikats, § 269 Abs. 1 Alt. 2 StGB 134
B. Löschung eines qualifizierten Zertifikats, §§ 274 Abs. 1 Nr. 2 StGB 135
C. Ergebnis 135

§ 6 Rückdatiertes Signieren von Daten 135

A. Rückdatiertes Signieren in den Gültigkeitszeitraum des Zertifikats durch den Inhaber, § 269 Abs. 1 Alt. 1 StGB 136
B. Rückdatiertes Signieren in den Gültigkeitszeitraum des Zertifikats durch einen Dritten, § 269 Abs. 1 Alt. 1 StGB 137
C. Ergebnis 137

§ 7 Rekonstruktion eines gelöschten signierten Dokuments 137
A. § 269 Abs. 1 Alt. 1 StGB 138
B. Ergebnis 139

§ 8 Brute-Force-Attacke auf den Kryptoalgorithmus 139
A. Ausgangselemente für den Angriff 140
B. Einschätzung der Erfolgsaussichten unter Berücksichtigung des Sicherheitsmechanismus des SigG und der SigVO 140
C. Strafrechtliche Würdigung 142
I. Errechnen des Signierschlüssels, § 202a StGB 142
II. Verwendung des Signierschlüssels zum Signieren von Erklärungen, § 269 Abs. 1 Alt. 1 StGB 143
III. Erzeugung einer Vielzahl von Signaturen, §§ 269 Abs. 3, 267 Abs. 3 Nr. 3 StGB 143
D. Ergebnis 144

§ 9 Geburtstagsattacke auf die Hashfunktion 144
A. Regelmäßiges Vorliegen der Ausgangselemente für den Angriff 145
B. Einschätzung der Erfolgsaussichten unter Berücksichtigung des Sicherheitsmechanismus des SigG und der SigVO 145
C. Strafrechtliche Würdigung 146
I. Errechnen von Daten mit kollidierendem Hashwert, § 202a Abs. 1 StGB 146
II. Anhängen einer existierenden Signatur an die errechneten Daten, § 269 Abs. 1 Alt. 2 StGB 146
III. § 303a Abs. 1 StGB 147
D. Ergebnis 147

Zusammenfassung in Thesen 148

Literaturverzeichnis 150