

Inhaltsübersicht

1	Einleitung, Methodik und Aufbau der Arbeit	1
2	Grundlagen.....	25
3	Technik und Verfahren IT-forensischer Untersuchungen	83
4	(Verfassungs-)Rechtliche Vorgaben, Funktion und Bedeutung.....	119
5	Chancen und Risiken IT-forensischer Systeme	141
6	Rechtliche Anforderungen an IT-forensische Systeme (A).....	183
7	Rechtliche Kriterien für IT-forensische Systeme (K).....	211
8	Gestaltungsziele IT-forensischer Systeme (Z).....	401
9	Zusammenfassung und Schlussbetrachtung – Gestaltungskatalog.....	453

Inhaltsverzeichnis

1	Einleitung, Methodik und Aufbau der Arbeit	1
1.1	Rechtsverträgliche Technikgestaltung	6
1.1.1	Verhältnis des Rechts zur Technik.....	7
1.1.2	Verhältnis der Technik zum Recht.....	8
1.2	Methode zur Konkretisierung rechtlicher Anforderungen	9
1.2.1	(Verfassungs-)Rechtliche Vorgaben (Vorstufe).....	10
1.2.2	Rechtliche Anforderungen (1. Stufe)	11
1.2.3	Rechtliche Kriterien (2. Stufe).....	12
1.2.4	Technische Gestaltungsziele (3. Stufe)	13
1.2.5	Technische Gestaltungsvorschläge (4. Stufe)	14
1.2.6	Anwendung von KORA und Grenzen	15
1.3	Ziel, Aufbau und Inhalt der Arbeit sowie Stand der Forschung.....	16
2	Grundlagen.....	25
2.1	Wirtschaftskriminalität	25
2.1.1	Begriff der Wirtschaftskriminalität und Entwicklung.....	25
2.1.2	Herausforderungen der Eindämmung	26
2.2	Versicherungsbetrug.....	27
2.2.1	Beteiligte Rechtssubjekte (Schädiger und Geschädigte).....	27
2.2.1.1	Versicherungsunternehmen (Versicherer)	28
2.2.1.2	Versicherungsnehmer und Versicherte	29
2.2.1.3	Versicherungsvermittler	30
2.2.1.4	Drittbeteiligte.....	30
2.2.2	Rechtliche Bewertung des Versicherungsbetrugs	31
2.2.2.1	Versicherungsrechtliche Bewertung	31
2.2.2.2	Strafrechtliche Bewertung	34
2.2.3	Fakten zum Versicherungsbetrug.....	38
2.2.4	Schadensersatz- und Regressansprüche des Versicherers	40
2.2.5	Rolle der Akteure im Zivilprozess und Möglichkeiten des Beweises	43
2.2.5.1	Regelungen und Grundsätze im zivilprozessualen Verfahren.....	43
2.2.5.2	Grundsätze des Beweisrechts.....	48
2.2.5.3	Beweismaß und Beweiswürdigung (§ 286 ZPO).....	51
2.2.5.4	Anscheinsbeweis	53
2.2.5.5	Beweismittel im Zivilprozess	55
2.2.5.5.1	Zeugenbeweis (§§ 373–401 ZPO).....	56
2.2.5.5.2	Sachverständigenbeweis (§§ 402–414 ZPO).....	57
2.2.5.5.3	Urkundsbeweis (§§ 415–444 ZPO).....	58
2.2.5.5.4	Augenscheinsbeweis (§§ 371–372a ZPO).....	59
2.2.5.6	eIDAS-Verordnung	63

2.2.5.6.1	Anwendbarkeit und Bedeutung.....	65
2.2.5.6.2	Nichtqualifizierte und qualifizierte Vertrauensdienste.....	68
2.2.5.6.3	Beweisrechtliche Rechtsfolgen der Vertrauensdienste und ihres Einsatzes.....	69
2.2.6	Strafprozess	75
2.2.6.1	Regelungen und Grundsätze im strafprozessualen Verfahren.....	76
2.2.6.2	Grundsätze des Beweisrechts.....	78
2.2.6.3	Beweismittel im Strafprozess und Unterschiede zum Zivilprozess	80
2.2.7	Zusammenfassung rechtlicher Anknüpfungspunkte beim Versicherungsbetrug	81
3	Technik und Verfahren IT-forensischer Untersuchungen	83
3.1	IT-Forensik	83
3.1.1	Begriff der IT-Forensik und Eingrenzung.....	83
3.1.2	Historie der IT-Forensik	85
3.1.3	Repressive und präventive IT-Forensik	87
3.1.4	Verhältnis von IT-Forensik und Kriminalistik	89
3.1.5	Das Austauschprinzip und IT-Forensik.....	90
3.1.5.1	Physische Spuren – klassische Forensik	91
3.1.5.2	Digitale Spuren – IT-Forensik	92
3.1.5.2.1	Definition und Entstehung digitaler Spuren	92
3.1.5.2.2	Eigenschaften digitaler Spuren	93
3.1.5.3	Schlussfolgerungen.....	96
3.1.6	Anti-Forensik.....	97
3.2	Verfahrensschritte einer klassischen IT-forensischen Untersuchung.....	98
3.2.1	Sicherung	98
3.2.2	(Daten-)Analyse.....	101
3.2.3	Präsentation	103
3.3	IT-forensische Systeme im Umfeld von Versicherungen	104
3.3.1	Begriff „IT-forensisches System“	104
3.3.2	Bisherige Systeme zur Betrugserkennung bei Versicherungen.....	105
3.3.3	Neue IT-forensische Systeme im Versicherungsumfeld (Technikbeschreibung)	108
3.3.3.1	Systemkomponenten.....	109
3.3.3.1.1	Text-forensische Verfahren.....	109
3.3.3.1.2	Bild-forensische Verfahren.....	113
3.3.3.2	Zusammenfassung der Möglichkeiten der IT-Forensik und Einflussgrößen der Gestaltung.....	117

4 (Verfassungs-)Rechtliche Vorgaben, Funktion und Bedeutung.....	119
4.1 Bedeutung und Anwendbarkeit europäischen Rechts bei der Technikgestaltung.....	119
4.2 Mittelbare Drittwirkung und Grundrechte als Bezugspunkt der Technikgestaltung.....	122
4.3 Das Rechtsstaatsprinzip	124
4.4 Rechtsweggarantie.....	129
4.5 Anspruch auf rechtliches Gehör.....	130
4.6 Das Sozialstaatsprinzip	131
4.7 Die Menschenwürde	132
4.8 Freie Persönlichkeitsentfaltung.....	134
4.8.1 Allgemeine Handlungsfreiheit	134
4.8.2 Freiheit der Person.....	135
4.8.3 Das allgemeine Persönlichkeitsrecht.....	136
4.9 Gleichbehandlungsgrundsatz	137
4.10 Eigentumsschutz und Eigentumsfreiheit.....	138
5 Chancen und Risiken IT-forensischer Systeme	141
5.1 Einsatzumfeld der Technik und Szenarienbildung – Schadensbearbeitung in Versicherungsunternehmen.....	141
5.2 Chancen durch den Einsatz IT-forensischer Systeme im Szenario	146
5.2.1 Aufdeckung und Beweisführung von betrügerischem Verhalten.....	146
5.2.1.1 Effektivere Aufdeckungsmöglichkeiten und Nebeneffekte	146
5.2.1.2 Erhöhung der Beweisbarkeit und bessere Beweisführung	149
5.2.1.2.1 Zivilrechtlicher und zivilprozessualer Bereich.....	149
5.2.1.2.2 Strafrechtlicher und strafprozessualer Bereich.....	151
5.2.2 Optimierte Zusammenarbeit von Versicherer und Strafverfolgungsbehörden.....	153
5.2.3 Effizientere Bearbeitung von Schadensfällen	154
5.2.4 Verringerung menschlicher Fehler sowie subjektiver Einflussfaktoren..	157
5.3 Risiken durch den Einsatz IT-forensischer Systeme im Szenario	159
5.3.1 Zunahme zweifelhafter und unberechtigter Ablehnungen von Ansprüchen.....	160
5.3.1.1 Fehlerhafte Aufdeckung der Verfahren	161
5.3.1.2 Fehlbeurteilungen der Ergebnisse der Technik.....	164
5.3.1.2.1 Unumstößliche Ergebnisse und blindes Vertrauen.....	164
5.3.1.2.2 Missverständliche Darstellung der Ergebnisse (Präsentation).....	166
5.3.2 Funktionsfehler.....	167
5.3.2.1 Hardware- und gesamtsystembasierte Fehler.....	168
5.3.2.2 Softwarebasierte Fehler.....	169

5.3.2.3 Zwischenfazit	171
5.3.3 IT-Angriffe und Steigerung der Verwundbarkeit.....	171
5.3.4 Beweisverbote aufgrund unzulässiger Grundrechtseingriffe.....	174
5.3.5 Steigerung der Objektivierung des Einzelnen	177
5.3.6 „Verschmutzung“ (straf-)prozessualer Erkenntnisquellen	179
5.4 Zusammenfassung der identifizierten Chancen und Risiken für die Gestaltung	182
6 Rechtliche Anforderungen an IT-forensische Systeme (A).....	183
6.1 Gewährleistung effektiven Rechtsschutzes (A1)	183
6.2 Rechtssicherheit (A2)	186
6.3 Wahrheitsfindung (A3).....	188
6.4 Chancengleichheit (A4)	190
6.5 Informationelle Selbstbestimmung – Datenschutz (A5)	192
6.6 Selbstdarstellungsschutz (A6).....	196
6.6.1 Recht am eigenen Wort.....	197
6.6.2 Recht am eigenen Bild.....	198
6.7 Selbstbelastungsfreiheit?	201
6.8 Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme?	204
6.9 Verhältnismäßigkeit (A7)	206
6.10 Zusammenfassung	208
7 Rechtliche Kriterien für IT-forensische Systeme (K).....	211
7.1 Beweiseignung (K1)	213
7.1.1 Herleitung aus rechtlichen Anforderungen	213
7.1.2 Auswirkungen auf IT-forensische Systeme	214
7.1.2.1 Generelle Beweiseignung – Einordnung in das System der Strengbeweismittel	215
7.1.2.1.1 Daten als elektronische Dokumente und als Beweismittel des Augenscheins.....	216
7.1.2.1.2 Daten und System als Gegenstand von Sachverständigengutachten	228
7.1.2.1.3 Daten als Privatgutachten.....	231
7.1.2.1.4 Zwischenfazit.....	233
7.1.2.2 Abstrakt-materielle Beweiseignung – Ausschluss völliger Ungeeignetheit.....	234
7.1.2.2.1 Zuverlässigkeit der Verfahren.....	235
7.1.2.2.1.1 Bewertung text-forensischer Verfahren.....	237
7.1.2.2.1.2 Bewertung bild-forensischer Verfahren.....	240
7.1.2.2.2 Zusammenfassung.....	241
7.1.2.3 Konkret-materielle Beweiseignung – Tatbestandsrelevante Ergebnisse	241

7.1.2.3.1	Bewertung text-forensischer Verfahren	243
7.1.2.3.2	Bewertung bild-forensischer Verfahren	244
7.1.2.3.3	Schlussfolgerung.....	248
7.1.3	Zusammenfassung	249
7.2	Beweissicherheit (K2).....	249
7.2.1	Herleitung aus rechtlichen Anforderungen	250
7.2.2	Auswirkungen auf IT-forensische Systeme	251
7.2.2.1	Typische Beweisinreden	252
7.2.2.1.1	Zivilprozess.....	253
7.2.2.1.1.1	Einrede des fehlenden Beweisobjekts (Nr. 1).....	254
7.2.2.1.1.2	Einrede der Manipulation des Beweisobjekts (Nr. 2).....	257
7.2.2.1.1.3	Einrede der Echtheit des Beweisobjekts (Nr. 3).....	270
7.2.2.1.1.4	Einrede der Verlässlichkeit der Analyse und Generierung (Nr. 4)	275
7.2.2.1.1.5	Einrede der Mehrdeutigkeit des Beweisobjekts (Nr. 5).....	279
7.2.2.1.2	Strafprozess – Übertragbarkeit der Beweisinreden und Auswirkungen auf die Gestaltung	282
7.2.2.2	Schlussfolgerungen für die beweisichere Gestaltung IT- forensischer Systeme	284
7.2.3	Zusammenfassung	286
7.3	Nachvollziehbarkeit (K3).....	287
7.3.1	Herleitung aus rechtlichen Anforderungen	288
7.3.2	Auswirkungen auf IT-forensische Systeme	289
7.3.3	Zusammenfassung	292
7.4	Datenqualität (K4)	293
7.4.1	Herleitung aus rechtlichen Anforderungen	293
7.4.2	Auswirkungen auf IT-forensische Systeme	294
7.4.2.1	Zivilprozess	295
7.4.2.2	Strafprozess	297
7.4.3	Zusammenfassung	300
7.5	Beweismittelverfügbarkeit (K5)	301
7.5.1	Herleitung aus rechtlichen Anforderungen	301
7.5.2	Auswirkungen auf IT-forensische Systeme	302
7.5.3	Zusammenfassung	306
7.6	Zurechenbarkeit (K6).....	307
7.6.1	Herleitung aus rechtlichen Anforderungen	307
7.6.2	Auswirkungen auf IT-forensische Systeme	308
7.6.2.1	Personen- und Sachverhaltsebene.....	309

7.6.2.2 Daten- und Dateiebene	310
7.6.3 Zusammenfassung	313
7.7 Zusammenfassende Bewertung der beweisrechtlichen Kriterien für IT-forensische Systeme.....	314
7.8 Zweckfestlegung und Zweckbindung (K7).....	317
7.8.1 Herleitung aus rechtlichen Anforderungen	317
7.8.2 Auswirkungen auf IT-forensische Systeme	318
7.8.3 Zusammenfassung	324
7.9 Erforderlichkeit (K8)	325
7.9.1 Herleitung aus rechtlichen Anforderungen	325
7.9.2 Auswirkungen auf IT-forensische Systeme	326
7.9.2.1 Be- und Eingrenzung des Datenumfangs – Datenminimierung ...	326
7.9.2.2 Zeitliche Begrenzung – Speicherbegrenzung.....	332
7.9.2.3 Einzelfallbezogene Begrenzung – Daten- und Betroffenendifferenzierung.....	334
7.9.3 Zusammenfassung	335
7.10 Transparenz (K9).....	336
7.10.1 Herleitung aus rechtlichen Anforderungen	337
7.10.2 Auswirkung auf IT-forensische Systeme	338
7.10.2.1 Informationspflichten	339
7.10.2.2 Auskunftspflichten.....	344
7.10.2.3 Korrekturrechte der betroffenen Personen	347
7.10.2.4 Dokumentationspflichten.....	353
7.10.2.4.1 Verzeichnis von Verarbeitungstätigkeiten	354
7.10.2.4.2 Dokumentation bei Verletzung des Schutzes personenbezogener Daten	356
7.10.2.4.3 Zwischenfazit.....	359
7.10.3 Zusammenfassung	359
7.11 Verbot automatisierter Einzelentscheidungen (K10)	360
7.11.1 Herleitung aus rechtlichen Anforderungen	360
7.11.2 Auswirkung auf IT-forensische Systeme	361
7.11.3 Zusammenfassung	366
7.12 Datenrichtigkeit (K11).....	367
7.12.1 Herleitung aus rechtlichen Anforderungen	367
7.12.2 Auswirkung auf IT-forensische Systeme	368
7.12.2.1 Sachliche Richtigkeit von Daten.....	368
7.12.2.1.1 Datenaktualität	371
7.12.2.1.2 Datenvollständigkeit	372
7.12.2.1.3 Beurteilung der Richtigkeit von Daten bei technischen Bewertungen	373
7.12.2.1.4 Schlussfolgerungen	376

7.12.2.2 Angemessenheit der zu ergreifenden Maßnahmen	377
7.12.3 Zusammenfassung	379
7.13 Daten- und Systemsicherheit (K12)	380
7.13.1 Herleitung aus Anforderungen	380
7.13.2 Abgrenzung zwischen Datensicherheit und IT-Sicherheit	381
7.13.3 Auswirkung auf IT-forensische Systeme	383
7.13.3.1 Sicherheit personenbezogener Daten (Art. 32)	384
7.13.3.2 Verletzungen des Schutzes personenbezogener Daten (Art. 33 und 34 DSGVO)	393
7.14 Zusammenfassende Bewertung der datenschutzrechtlichen Kriterien für IT- forensische Systeme	395
7.15 Bedeutung compliance-rechtlicher Regelungen für die Technikgestaltung	396
8 Gestaltungsziele IT-forensischer Systeme (Z)	401
8.1 Automatisierte Datensicherung und Datenaufbewahrung (Z1)	402
8.2 Einsatz von elektronischen Vertrauensdiensten (Z2)	405
8.3 Datenpriorisierung und -kategorisierung (Z3)	411
8.4 Vermeidung von Datensелеktionen (Z4)	413
8.5 Interoperabilität (Z5)	414
8.6 Formatunabhängige Analysier- und Auswertbarkeit (Z6)	415
8.7 Unverändertheit technischer System- und Analyseparameter (Z7)	417
8.8 Sichere Übermittlungswege zur Nutzung im Gerichtsverfahren (Z8)	419
8.9 Importfunktionen (Z9)	420
8.10 Exportfunktion (Z10)	421
8.11 Beweisorientierte Reproduzier- und Darstellbarkeit der Daten (Z11)	422
8.12 Intervenierbarkeit (Z12)	425
8.13 Menschliche Letztentscheidungskompetenz nach Ausgabe der Analyse (Z13)	427
8.14 Verwechslungssichere Kennzeichnung und Zuordnung (Z14)	427
8.15 Robustheit des Systems und der Analyseverfahren (Z15)	429
8.16 Datenorientierte Kongruenz der Analyse (Z16)	430
8.17 Automatische Datenlöschung (Z17)	431
8.18 Dokumentations- und Protokollierungsfunktion (Z18)	432
8.19 Pseudonymisierungsfunktionen (Z19)	435
8.20 Zugangs- und Zugriffskontrolle (Z20)	436
8.21 Automatisierte und autarke Analyse und Generierung der Ergebnisse (Z21) ...	437
8.22 Möglichkeit zur Erfassung von Kontext (Z22)	438
8.23 Gesicherte Integration von Kontext(-meta)daten (Z23)	439
8.24 Echtzeitanalyse (Z24)	441
8.25 Sensitivität und Neutralität der Analyseverfahren (Z25)	442
8.26 Wissenschaftliche Akzeptanz eingesetzter Verfahren (Z26)	443
8.27 Fachkenntnis im Umgang mit IT-forensischen Systemen (Z27)	447

8.28 Authentifizierungsdienst (Z28).....	448
8.29 Beschwerdemanagement für betroffene Personen (Z29)	449
8.30 Zertifizierungen IT-forensischer Systeme (Z30).....	450
9 Zusammenfassung und Schlussbetrachtung – Gestaltungskatalog.....	453
Literaturverzeichnis.....	461