

# Inhaltsübersicht

Vorwort . . . . .	V
Inhaltsverzeichnis . . . . .	XI

Kapitel 1: Die Erhebung und Verwertung digitaler Beweismitteldaten als Herausforderung für das Strafverfahrensrecht . . . . .	1
-------------------------------------------------------------------------------------------------------------------------------------	---

I.    Allgemeingültige Vorgaben und Leitlinien für die Schaffung und Anwendung strafprozessualer Dateneingriffsbefugnisse zur Beweisdatengewinnung . . . . .	4
II.   Digitale Daten und Datenanalyse als Beweismittel in der Hauptverhandlung . . . . .	20
III.  Gang der Darstellung . . . . .	28

Kapitel 2: Analyse der verfassungsgerichtlichen Rechtsprechung zur Rechtfertigung von Eingriffen in die Datenschutzgrundrechte . . . . .	33
------------------------------------------------------------------------------------------------------------------------------------------------	----

I.    Methodische Vorbemerkung: Zu Zulässigkeit und Grenzen induktiver/abduktiver Schlussfolgerungen aus Entscheidungen des BVerfG . . . . .	34
II.   Die drei zentralen Säulen des grundrechtlichen Datenschutzes . . . . .	39
III.  Das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG . . . . .	39
IV.   Das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG . . . . .	153
V.    Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG . . . . .	174
VI.  Sonstige datenschutzrelevante Grundrechte . . . . .	201

VII. Ergebnis: Gemeinsame Vorgaben für die Auslegung und Ausgestaltung von strafprozessualen Eingriffsbefugnissen . . . . .	205
VIII. Offene Fragen und weiterer Gang der Untersuchung . . . . .	214
Kapitel 3: Kriterien zur Bestimmung der Eingriffsintensität . . . . .	243
I. Art der Daten . . . . .	244
II. Menge der Daten/Dichte und Vielfalt der Informationen . . . . .	265
III. Zugänglichkeit der Daten . . . . .	267
IV. Lesbarkeit der Daten . . . . .	275
V. Heimlichkeit der Maßnahme und Täuschungen durch die Ermittlungsbehörden . . . . .	277
VI. Streubreite der Maßnahme . . . . .	283
VII. Automatisierung der Maßnahme . . . . .	286
VIII. Dauer der Maßnahme . . . . .	301
IX. Sicherheit der Daten in staatlicher Obhut . . . . .	301
X. Veränderungen an bestehenden Datensätzen . . . . .	302
XI. Kenntnis, Kennenmüssen und fahrlässige Unkenntnis der Strafverfolgungsbehörden . . . . .	302
XII. Anlassbezogenheit/Anlasslosigkeit eines Dateneingriffs . . . . .	305
XIII. Folgen für den Betroffenen . . . . .	306
XIV. Ergebnis: Eine partielle Ordnung der Eingriffsschwerekriterien bei Dateneingriffen im Strafverfahrensrecht . . . . .	308
XV. Abstraktheit von Normen, ex ante-Perspektive und die relative ordinale Ordnung der Schwerekriterien . . . . .	318
Kapitel 4: Das Gewicht des staatlichen Strafverfolgungsanspruchs bzw. der Erfordernisse einer effektiven Strafrechtspflege . . . . .	353
I. Verfassungsrang und Gewicht des Strafverfolgungsanspruchs . . . . .	354
II. Schwere der Straftat . . . . .	354
III. Grad des Tatverdachts, insbesondere Tatverdachtsgewinnung im Wege (automatisierter) Datenverarbeitung . . . . .	357

IV.	Auffindewahrscheinlichkeit bzgl. verfahrens- und nachweis-relevanter Daten . . . . .	392
V.	Wechselwirkungen und Ordnung der Kriterien zur Bestimmung des Gewichts des Strafverfolgungsanspruchs . . . . .	393
Kapitel 5: Die Abhängigkeit der Schutzmechanismen und Eingriffsschwellen von der Intensität des Dateneingriffs . . . . .		397
I.	Die Abhängigkeit der notwendigen Eingriffsschwellen und Schutzmechanismen von der Eingriffsintensität . . . . .	399
II.	Ergebnis: Ein „Baukastensystem“ unter Berücksichtigung der Erforderlichkeit und der Verhältnismäßigkeit ieS . . . . .	458
Kapitel 6: Möglichkeiten und Grenzen neuartiger, unregulierter strafprozessualer Dateneingriffe . . . . .		465
I.	Problemaufriss: Schnelle technologische Entwicklung und langsame Gesetzgebungsverfahren . . . . .	466
II.	Die Grenzen der Auslegung von Ermittlungsbefugnissen . . . . .	469
III.	Ausweg technikoffene Eingriffsbefugnisse? . . . . .	497
IV.	Ergebnis und kriminalpolitische Überlegungen . . . . .	510
Kapitel 7: Europarechtliche Vorgaben für die Erhebung und Verwertung digitaler Daten im Strafverfahren . . . . .		515
I.	Bedeutung des Europarechts und untersuchte Rechtsquellen . . . . .	515
II.	Vorgaben aus der Richtlinie 2016/680/EU und §§ 45 ff. BDSG . . . . .	518
III.	Bedeutungsgewinn der europäischen Grund- und Menschenrechte für die strafprozessuale Datenverarbeitung . . . . .	628
IV.	Verhältnis der Vorgaben aus der Richtlinie zu den verfassungsrechtlichen Vorgaben und Leitlinien (Meistbegünstigungsprinzip) . . . . .	648
Kapitel 8: Zentrale Probleme der Verwendung von Daten und Datenanalysen als Beweismittel in der Hauptverhandlung . . . . .		651
I.	Das Übersetzungsproblem: Die fehlende unmittelbare Wahrnehmbarkeit von Daten und der Grundsatz des sachnäheren Beweismittels . . . . .	653
II.	Flüchtigkeit und Manipulierbarkeit: IT-forensische Standards und strafprozessuales Beweisrecht . . . . .	665

III.	Beweiswert und Beweiswürdigung von Datenanalyseergebnissen . . .	673
IV.	Das Blackbox-Problem und strafprozessuales Beweisrecht . . . . .	688
V.	Datenanalyse, Akteneinsicht und prozessuale Waffengleichheit . . . .	698

Kapitel 9: Schlussbetrachtungen: Zusammenfassung der Thesen und Erkenntnisse zu digitalen Daten als Beweismittel im Strafverfahren . . . . .		727
----------------------------------------------------------------------------------------------------------------------------------------------------	--	-----

I.	Kapitel 2 bis 6: Verfassungsrechtliche und verfassungsgerichtliche Vorgaben für die Normsetzung und Anwendung strafprozessualer Dateneingriffe zur Beweisdatengewinnung . . . . .	728
II.	Kapitel 7: Europarechtliche Vorgaben für die Schaffung und Auslegung strafprozessualer Dateneingriffsbefugnisse zur Beweisdatengewinnung . . . . .	773
III.	Kapitel 8: Zentrale Probleme der Verwendung von Daten und Datenanalysen als Beweismittel in der Hauptverhandlung . . . . .	789

Literaturverzeichnis . . . . .	801
Stichwortverzeichnis . . . . .	827

# Inhaltsverzeichnis

Vorwort . . . . .	V
Inhaltsübersicht . . . . .	VII

Kapitel 1: Die Erhebung und Verwertung digitaler Beweismitteldaten als Herausforderung für das Strafverfahrensrecht . . . . .	1
-------------------------------------------------------------------------------------------------------------------------------------	---

I.   Allgemeingültige Vorgaben und Leitlinien für die Schaffung und Anwendung strafprozessualer Dateneingriffsbefugnisse zur Beweisdatengewinnung . . . . .	4
1. Mangel an gesetzlichen Dateneingriffsbefugnissen . . . . .	4
a) Zu eng und zu spät geregelte Eingriffsbefugnisse . . . . .	4
b) Praktisch bedeutsame, aber unregelte Dateneingriffe . . . . .	6
c) „Kreative“ Rechtsauslegung vor den Schranken des Grundgesetzes . . . . .	7
2. Mangelhafte Systematisierung der bestehenden Dateneingriffs- befugnisse . . . . .	11
3. Bislang fehlende Leitlinien und Auslegungskriterien für die Rechtsanwendung . . . . .	14
4. Stand der Forschung und Beschränkungen des Untersuchungs- gegenstandes . . . . .	16
5. Ziele der Untersuchung . . . . .	19
II.   Digitale Daten und Datenanalyse als Beweismittel in der Hauptverhandlung . . . . .	20
1. Das „Übersetzungsproblem“ . . . . .	20
2. Das Problem der Flüchtigkeit und Manipulierbarkeit . . . . .	23
3. Problemkreise . . . . .	23
4. Stand der Forschung und Beschränkung des Untersuchungs- gegenstands . . . . .	25
5. Ziele der Untersuchung . . . . .	28
III.   Gang der Darstellung . . . . .	28
1. Kapitel 2 bis 6: Verfassungsrechtliche Vorgaben für strafprozessuale Dateneingriffe . . . . .	29
2. Kapitel 7: Europarechtliche Vorgaben . . . . .	30
3. Kapitel 8: Daten und Datenverarbeitungsvorgänge als Beweismittel . . . . .	30

Kapitel 2: Analyse der verfassungsgerichtlichen Rechtsprechung zur Rechtfertigung von Eingriffen in die Datenschutzgrundrechte . . . . .	33
I. Methodische Vorbemerkung: Zu Zulässigkeit und Grenzen induktiver/abduktiver Schlussfolgerungen aus Entscheidungen des BVerfG . . . . .	34
II. Die drei zentralen Säulen des grundrechtlichen Datenschutzes . . . . .	39
III. Das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG . . . . .	39
1. Eingriffe in das Telekommunikationsgeheimnis durch straßprozessuale Dateneingriffe zur Beweisdatengewinnung . . . . .	40
a) Unstreitiger Schutzbereich: Prozess, Produkt, Umstände der Telekommunikation . . . . .	40
b) Erfordernis eines personalen Bezugs der Kommunikationsinhalte? aa) Verzicht auf eine unmittelbare menschliche Veranlassung der Kommunikation . . . . .	41
bb) Aufbau einer unerwünschten Kommunikationsbeziehung durch Strafverfolgungsbehörden . . . . .	44
cc) Keine Notwendigkeit der Übertragung von personen- bezogenen Daten . . . . .	44
dd) Ergebnis: Lösen des Telekommunikationsgeheimnisses von seinen strengen personalen Bezügen . . . . .	45
c) Unterscheidung zwischen (nicht geschütztem) Herrschaftsbereich und (geschütztem) Übertragungsweg . . . . .	46
aa) Grundlegende Unterscheidung zwischen Herrschaftsbereich und Übertragungsweg . . . . .	46
bb) Unklarheiten bezüglich des „laufenden“ Telekommunika- tionsvorgangs . . . . .	48
cc) Das Beherrschbarkeitskriterium als entscheidendes Merkmal der Abgrenzung . . . . .	49
(1) Grundlagen . . . . .	49
(2) Technische Kommunikationsgeräte . . . . .	51
(3) Technische Infrastruktur Dritter . . . . .	52
(4) LAN und WLAN-Netzwerke . . . . .	52
(5) Ergebnis . . . . .	54
dd) Erhebung von Verkehrs- und Nutzungsdaten beim Tele- kommunikationsanbieter/Telemedienanbieter nach Ende eines laufenden Kommunikationsvorgangs . . . . .	54
ee) Zusammenfassung . . . . .	57
d) Das Beherrschbarkeitskriterium und das Erfordernis der Inter- subjektivität bei verschiedenen Formen des Cloud Computings . . .	61
aa) Digitale „tote Briefkästen“ . . . . .	62
bb) Sonstige E-Mail-Entwürfe . . . . .	63
cc) Cloud-Computing und „Kommunikation mit sich selbst“ . . . .	63
(1) Cloud-Dienstleister ist nicht Kommunikationspartner . . .	64
(2) Cloud-Nutzung ist Telekommunikation „mit sich selbst“ . .	65

(3) Lösung des Telekommunikationsgeheimnisses vom Erfordernis der Intersubjektivität . . . . .	67
e) Das Kriterium der Vertraulichkeitserwartung, insbesondere bei der sog. Hörfalle und bei Kommunikation über das Internet . . . . .	73
aa) Vertrauen in die Integrität der genutzten Infrastruktur . . . . .	73
bb) Erwartung der vertraulichen Behandlung durch den Infrastrukturbetreiber . . . . .	76
cc) Kein (berechtigtes) Vertrauen in die Identität der Kommunikationspartner . . . . .	78
dd) Keine (berechtigte) Erwartung in die vertrauliche Behandlung durch Kommunikationspartner . . . . .	79
ee) Vertrauen in die Begrenzung des Empfängerkreises . . . . .	83
(1) Adressierung an individualisierbare Empfänger . . . . .	86
(2) Technische Sicherungsmaßnahmen der Privatheit . . . . .	86
(3) Verteilungsmodus der Zugangsberechtigung . . . . .	87
(4) Autorisierung durch Kommunikationsteilnehmer . . . . .	87
(5) Sog. Zweifelsregel . . . . .	88
(6) Pauschale Erfassung jeder Daten- und Informationsübertragung . . . . .	88
(7) Eigene Lösung: Interesse an und Vertrauen in Privatheit der Kommunikation . . . . .	88
(a) Würdigung und Kritik der bisherigen Ansätze . . . . .	89
(b) Entwicklung eines eigenen Ansatzes . . . . .	94
f) Vom Telekommunikationsgeheimnis geschützte Datenarten . . . . .	101
aa) Problemfall: Bestandsdaten . . . . .	101
bb) Problemfall: Dynamische IP-Adressen . . . . .	103
cc) Problemfall: Zugangsdaten . . . . .	104
dd) Problemfall: Nutzungsdaten . . . . .	105
g) Schutz vor Datenerhebung durch heimliche Initiierung von Kommunikation durch staatliche Behörden? . . . . .	106
h) Recht auf Verschlüsselung der Kommunikation? . . . . .	110
i) Zwischenergebnis: Weiterentwicklung des Telekommunikationsgeheimnisses zu umfassendem Daten- und Informationsübertragungsgeheimnis . . . . .	113
2. Vorgaben für die Auslegung und Ausgestaltung strafprozessualer Dateneingriffsbefugnisse aus Art. 10 Abs. 1 GG . . . . .	114
a) Normenklarheit und Bestimmtheit . . . . .	114
b) Doppeltürmodell . . . . .	116
c) Grundsatz der Zweckbindung . . . . .	117
d) Kennzeichnungs-, Sperrungs- und Löschungspflichten . . . . .	119
e) Grundsatz der Offenheit der Erhebung und Nutzung von personenbezogenen Daten . . . . .	121
f) Benachrichtigungspflichten und Auskunftsrechte . . . . .	122
aa) Absolute Ausnahmen von der Benachrichtigungspflicht . . . . .	122
bb) Ausnahmen im Interesse des Betroffenen . . . . .	123
cc) Ausnahmen bei zufällig Mitbetroffenen . . . . .	124
dd) Einschränkung bei unverhältnismäßigem Aufwand zur Identitätsfeststellung . . . . .	126
ee) Pflicht zur regelmäßigen Überprüfung . . . . .	127

g) Kontrolle durch unabhängige Organe und Richtervorbehalt . . . . .	128
h) Kernbereichsschutz . . . . .	130
aa) Kernbereichsrelevante Daten . . . . .	130
(1) Konturen und Leitlinien des (realweltlichen) Kernbereichs privater Lebensführung . . . . .	130
(a) Die Formalisierung des Kernbereichs durch die hM . . .	132
(b) Vertraulichkeitserwartung und Geheimhaltungswille . .	134
(c) Selbstreflexive Äußerungen . . . . .	134
(d) Der inhaltliche Sozialbezug . . . . .	137
(2) Übertragung der Konturen und Leitlinien auf Daten . . . .	139
bb) Anforderungen aus Art. 10 Abs. 1 GG an eine strafprozessuale Datenverarbeitung . . . . .	142
(1) Das vierstufige Schutzkonzept . . . . .	142
(2) Die Abhängigkeit des Schutzniveaus von der konkreten Eingriffsbefugnis . . . . .	146
i) Verbot der Rundumüberwachung . . . . .	149
j) Besonderheiten bei der Verhältnismäßigkeitsprüfung . . . . .	150
aa) Wirksame Strafverfolgung und Wahrheitsermittlung als legitimer Zweck . . . . .	151
bb) Beschränkung auf schwere Straftaten bei heimlichen Eingriffen . . . . .	151
cc) Die Auswirkung der Wechselwirkungslehre auf den notwendigen Verdachtsgrad . . . . .	152
dd) Adressaten der Maßnahme . . . . .	152
3. Grundrechtskonkurrenzen . . . . .	153
IV. Das Recht auf informationelle Selbstbestimmung	
gem. Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG . . . . .	153
1. Eingriffe in das Recht auf informationelle Selbstbestimmung durch strafprozessuale Datenerhebung, -verarbeitung, -speicherung und -übermittlung . . . . .	153
a) (Weitgehend) unstreitige Eingriffe in den Schutzbereich . . . . .	153
b) Eingriff bei Erhebung öffentlich zugänglicher Daten? . . . . .	155
aa) Unklare Rechtsprechung des BVerfG . . . . .	155
bb) Eigene Auffassung: Umfassender Schutz auch öffentlich zugänglicher personenbezogener Daten . . . . .	156
cc) Wann sind Daten „öffentlich zugänglich“? . . . . .	159
c) Eingriff bei Kommunikation unter Identitätstäuschung . . . . .	160
d) Eingriff bei Erhebung anonymer Daten? . . . . .	162
e) Eingriff auch bei Nicht-Treffern . . . . .	163
f) Aufeinander aufbauende Grundrechtseingriffe . . . . .	167
2. Vorgaben für die Auslegung und Ausgestaltung strafprozessualer Dateneingriffsbefugnisse aus dem RiS . . . . .	168
a) Übertragung der Kernbereichsrechtsprechung auf Eingriffe in das RiS . . . . .	168
b) Kontrolle durch eine unabhängige Stelle . . . . .	169
c) Besonderheiten bei der Verhältnismäßigkeitsprüfung . . . . .	170
d) Unzulässigkeit der Erstellung von Persönlichkeitsprofilen . . . . .	170



aa) Der Begriff des Persönlichkeitsprofils in der juristischen Literatur . . . . .	170
bb) Der Begriff des Persönlichkeitsprofils in der psychologischen Literatur . . . . .	171
cc) Folgerungen für das verfassungsrechtliche Verbot der Persönlichkeitsprofilbildung . . . . .	172
e) Übertragung und Weiterentwicklung des Doppeltürmodells . . . . .	173
V. Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG . . . . .	174
1. Eingriffe in das IT-System-Grundrecht . . . . .	175
a) Eingriffe durch Bruch der Integrität eines Systems . . . . .	175
b) Eingriffe durch Aufhebung der Vertraulichkeit der vom System verarbeiteten Daten . . . . .	176
c) Schutzobjekt: Als eigene genutzte informationstechnische Systeme . . . . .	178
aa) Problem: Quantitative Abgrenzung . . . . .	179
bb) Problem: „Als eigene genutzte“ IT-Systeme . . . . .	180
cc) Problem: Vernetzte IT-Systeme, insbesondere Cloud-Computing und Webmail-Provider . . . . .	181
(1) Vom Nutzer kontrollierte vernetzte Systeme (LAN, WLAN) . . . . .	181
(2) Vom Nutzer nicht kontrollierte vernetzte Systeme (Cloud-Computing, VPNs) . . . . .	185
(a) Konkurrenz zum Telekommunikationsgeheimnis . . . . .	186
(b) Grenzen der Einbeziehung vernetzter Systeme in das IT-System-Grundrecht . . . . .	187
dd) Problem: Notwendigkeit technischer Sicherungsmaßnahmen? . . . . .	190
d) Abgrenzung zu Art. 10 Abs. 1 GG . . . . .	191
e) Abgrenzung zu Art. 13 GG . . . . .	193
aa) Bruch der Vertraulichkeit . . . . .	193
bb) Bruch der Integrität . . . . .	193
cc) Problemfall: Zufällige Miterhebung von Daten über Vorgänge in der Wohnung mittels audiovisueller Sensoren . . . . .	194
f) Abgrenzung zum RiS . . . . .	197
g) Keine Beschränkung auf heimliche Zugriffe . . . . .	197
2. Vorgaben für die Auslegung und Ausgestaltung prozessualer Eingriffsbefugnisse aus dem IT-System-Grundrecht . . . . .	198
a) Richtervorbehalt . . . . .	198
b) Kernbereichsschutz . . . . .	198
c) Höchstdauer und tatsächliche Dauer . . . . .	199
d) Sonstige Besonderheiten im Rahmen der Verhältnismäßigkeitsprüfung . . . . .	200
VI. Sonstige datenschutzrelevante Grundrechte . . . . .	201
1. Art. 4 GG, Religionsfreiheit, Seelsorge und Beichtgeheimnis . . . . .	202
2. Art. 5 Abs. 1 S. 2 GG, Quellenschutz für Journalisten . . . . .	203
3. Art. 6 GG (Daten-)Schutz von Ehe und Familie . . . . .	203

4. Art. 8, 9 GG – Daten über Versammlungsteilnehmer/Mitglieder von Vereinigungen . . . . .	204
5. Art. 12 GG – Schutz von Daten, die Geschäfts- und Betriebsgeheimnisse enthalten . . . . .	204
VII. Ergebnis: Gemeinsame Vorgaben für die Auslegung und Ausgestaltung von strafprozessualen Eingriffsbefugnissen . . . . .	205
1. Grundlegende Erkenntnisse . . . . .	205
2. Zusammenfassung der einzelnen verfassungsrechtlichen Vorgaben . . . . .	206
3. Systematisierung der verfassungsrechtlichen Vorgaben . . . . .	207
a) Absolute Grenzen/Der Menschenwürdekern der digitalen Grundrechte . . . . .	207
aa) Ergebnisse zum Kernbereichsschutz . . . . .	207
bb) Ergebnisse zum Verbot der Erstellung eines Persönlichkeitsprofils . . . . .	209
cc) Ergebnisse zum Verbot der Rundumüberwachung . . . . .	210
b) Eingriffsschwellen und Schutzmechanismen als Ausprägungen des allgemeinen Verhältnismäßigkeitsprinzips . . . . .	210
c) Normenklarheit und Bestimmtheit als spezielle Ausprägung des Bestimmtheitsprinzips . . . . .	211
d) Zweckbindungsgrundsatz und Kennzeichnungs-, Sperrungs- und Löschungspflichten als „Verlängerung“ von Verhältnismäßigkeitsprinzip und Grundsatz der Normenklarheit und -bestimmtheit . . . . .	212
e) Vier Kategorien an verfassungsrechtlichen Vorgaben . . . . .	213
VIII. Offene Fragen und weiterer Gang der Untersuchung . . . . .	214
1. Rationalisierung des Abwägungsvorgangs der Verhältnismäßigkeitsprüfung ieS . . . . .	214
a) Verhältnismäßigkeit und strafprozessuale Ermittlungsmaßnahmen . . . . .	215
b) Die Verhältnismäßigkeit als prägendes Rechtsprinzip der Dateneingriffe im Strafverfahren . . . . .	217
aa) Auswirkungen des Verhältnismäßigkeitsprinzips auf Ebene der Gesetzgebung . . . . .	217
bb) Auswirkungen des Verhältnismäßigkeitsprinzips bei der Anwendung von Datenerhebungsbefugnisnormen . . . . .	220
cc) Mittelbarer Einfluss der Verhältnismäßigkeit auf die Frage des Bestehens eines Beweisverwertungsverbots . . . . .	223
dd) Bedeutung der Verhältnismäßigkeit im Rahmen der §§ 45 ff. BDSG/Richtlinie 2016/680/EU . . . . .	224
c) Grundlage des strafprozessualen Verhältnismäßigkeitsprinzips im Verfassungs- und Europarecht . . . . .	224
d) Wechselwirkungen des Verhältnismäßigkeitsprinzips mit anderen verfassungsrechtlichen Grundlagen für strafprozessuale Dateneingriffe . . . . .	225
e) Gesetzliche Struktur und Systematik der Verhältnismäßigkeit in den Dateneingriffsbefugnissen der StPO . . . . .	225
f) Die besondere Bedeutung der Verhältnismäßigkeit bei Datenerhebungs- und -auswertungseingriffen . . . . .	228
g) Das Problem: Bislang fehlende Kriterienkataloge und	

befugnisnorm-übergreifende Orientierungspunkte für die Verhältnismäßigkeitsprüfung . . . . .	230
aa) Problemlage . . . . .	230
bb) Spezifische Probleme auf Ebene der Rechtssetzung . . . . .	232
cc) Spezifische Probleme auf Ebene der Rechtsanwendung . . . . .	235
h) Ziele der nachfolgenden Untersuchung der Verhältnismäßigkeit . . . . .	237
aa) Erarbeitung von Kriterien und Leitlinien zur Bemessung der Eingriffstiefe strafprozessualer Dateneingriffe . . . . .	237
bb) Ausformung der Tatverdachts- und Erfolgswahrscheinlich- keitsdogmatik hinsichtlich der Besonderheiten bei Dateneingriffen . . . . .	237
cc) Erarbeitung von notwendigen Eingriffsschwellen und Schutzmechanismen bei Dateneingriffen in Abhängigkeit von der Eingriffsintensität . . . . .	238
2. Kreative Rechtsauslegung und technikoffene Eingriffsnormen im Lichte der verfassungsrechtlichen Prinzipien zu Normenklarheit und Bestimmtheit, Gesetzesvorbehalt und Wesentlichkeitstheorie . . . . .	238
a) Problemlage . . . . .	239
b) Ziele der Untersuchung . . . . .	240
 Kapitel 3: Kriterien zur Bestimmung der Eingriffsintensität . . . . .	243
I.   Art der Daten . . . . .	244
1. Personenbezug und Personenbeziehbarkeit der Daten . . . . .	245
2. Daten der Sozialsphäre/Privatsphäre/Intimsphäre bzw. Kernbereich . . . . .	247
a) Grobe Orientierung an Sphärentheorie . . . . .	247
b) Feinere Ausrichtung an der Gefahr einer Persönlichkeits- profilbildung . . . . .	250
c) Problem der Ex-ante-Bestimmung des Dateninhalts bei Datenerhebung . . . . .	253
3. Daten bzgl. derer ein anderes Vertraulichkeitsinteresse besteht (z. B. Geschäftsgeheimnisse, journalistischer Quellenschutz) . . . . .	255
4. Die Unterscheidung zwischen Inhalts-, Verkehrs-, Standort-, Bestands-, Nutzungs-, und Zugangsdaten als Indiz . . . . .	255
a) Gesetzliche Systematik . . . . .	255
b) Rechtsprechung des BVerfG . . . . .	256
c) Gesetzesbegründungen . . . . .	257
d) Sonderfall Zugangsdaten . . . . .	258
e) Inhalts-, Verkehrs-, Nutzungs-, Standortdaten . . . . .	259
f) Bestandsdaten . . . . .	262
g) Ergebnis . . . . .	264
II.   Menge der Daten/Dichte und Vielfalt der Informationen . . . . .	265
III.   Zugänglichkeit der Daten . . . . .	267
1. Öffentlich zugängliche Daten . . . . .	267
a) Wann sind Daten öffentlich zugänglich? . . . . .	267
b) Problem: Veröffentlichung durch Dritte . . . . .	269

2. Für einen begrenzten Empfängerkreis freiwillig zur Verfügung gestellte Daten . . . . .	271
3. Daten, die nicht für Drittzugriff bestimmt sind . . . . .	273
4. Veränderte Zugänglichkeit im Zeitverlauf . . . . .	273
5. Spezialfall: Gelöschte Daten . . . . .	273
IV. Lesbarkeit der Daten . . . . .	275
1. Erhöhung der Eingriffsintensität durch Verkörperung der Vertraulichkeitserwartung . . . . .	275
2. Absenkung der Eingriffsintensität bei faktischer Unmöglichkeit der Verwertung . . . . .	277
V. Heimlichkeit der Maßnahme und Täuschungen durch die Ermittlungsbehörden . . . . .	277
1. Offen durchgeführte Maßnahmen mit vorheriger oder aktueller Kenntnis des Betroffenen . . . . .	278
2. Offen durchgeführte Maßnahmen ohne aktuelle Kenntnis des Betroffenen . . . . .	279
3. Bewusst heimlich durchgeführte Maßnahmen . . . . .	279
4. Bewusst heimlich durchgeführte Maßnahmen ohne Einbindung eines Daten-Intermediärs . . . . .	280
5. Aktive Täuschungshandlungen . . . . .	281
VI. Streubreite der Maßnahme . . . . .	283
VII. Automatisierung der Maßnahme . . . . .	286
1. Intensitätssteigerung durch Verstärkung anderer Schwerekriterien aufgrund der verarbeiteten Datenmenge . . . . .	286
2. Einfluss der Richtigkeitswahrscheinlichkeit und Nachvollziehbarkeit automatisierter Datenverarbeitung . . . . .	287
a) Richtigkeitswahrscheinlichkeit und Nachvollziehbarkeit bei deterministischen Methoden . . . . .	289
b) Richtigkeitswahrscheinlichkeit und Nachvollziehbarkeit bei statistischen Methoden . . . . .	291
aa) Einfluss der Richtigkeitswahrscheinlichkeit bei statistischen Methoden . . . . .	292
bb) Einfluss der Nachvollziehbarkeit, insbesondere sog. Blackbox-Problem . . . . .	295
c) Richtigkeitswahrscheinlichkeit und Nachvollziehbarkeit bei selbstlernenden Methoden . . . . .	296
aa) Blackbox-Testing . . . . .	298
bb) Qualität der Trainingsdaten . . . . .	299
VIII. Dauer der Maßnahme . . . . .	301
IX. Sicherheit der Daten in staatlicher Obhut . . . . .	301
X. Veränderungen an bestehenden Datensätzen . . . . .	302
XI. Kenntnis, Kennenmüssen und fahrlässige Unkenntnis der Strafverfolgungsbehörden . . . . .	302

XII. Anlassbezogenheit/Anlasslosigkeit eines Dateneingriffs . . . . .	305
XIII. Folgen für den Betroffenen . . . . .	306
XIV. Ergebnis: Eine partielle Ordnung der Eingriffsschwerekriterien bei Dateneingriffen im Strafverfahrensrecht . . . . .	308
1. Wechselwirkungen der Kriterien untereinander . . . . .	308
2. Die Messbarmachung des Unmessbaren? . . . . .	309
a) Nur eine partielle Ordnung . . . . .	309
b) Inkommensurabilität und Rationalisierung des Abwägungs- prozesses . . . . .	311
c) Rationalisierung des Abwägungsvorgangs . . . . .	313
d) Die Ordnung des nicht vollständig Bekannten . . . . .	315
3. Die relative ordinale Ordnung der Eingriffsschwerekriterien als Tabelle . . . . .	315
XV. Abstraktheit von Normen, ex ante-Perspektive und die relative ordinale Ordnung der Schwerekriterien . . . . .	318
1. Gesetzliche Eingriffsbefugnisse für strafprozessuale Dateneingriffe . .	318
a) Abstrakt sehr schwere strafprozessuale Dateneingriffe . . . . .	320
aa) Online-Durchsuchung, § 100b StPO . . . . .	320
bb) Heimliche Zugriffe auf Cloud-Speicher mit Hilfe des Cloud-Providers . . . . .	322
cc) Heimliche Beschlagnahme größerer Datenmengen, § 95a StPO .	322
dd) Akustische Wohnraumüberwachung, § 100c StPO . . . . .	323
ee) „Rundum“-TKÜ, § 100a StPO . . . . .	325
b) Abstrakt schwere strafprozessuale Dateneingriffe . . . . .	326
aa) (Begrenzte) TKÜ, § 100a StPO . . . . .	327
bb) Heimliche E-Mail-Beschlagnahme beim Webmail-Provider, § 100a StPO . . . . .	327
cc) Quellen-TKÜ, § 100a Abs. 1 S. 2, S. 3 StPO . . . . .	328
dd) WLAN-Catching bei gesicherten Netzwerken . . . . .	328
ee) Nutzungsdatenauskunft bei inhaltsdatenähnlichen Nutzungsdaten, § 100k StPO . . . . .	330
ff) Erhebung von Standortdaten, §§ 100g Abs. 1 S. 3, S. 4 StPO, 100k Abs. 1 S. 2, S. 3 StPO . . . . .	332
gg) Stille SMS, §§ 100i, 100g StPO . . . . .	335
hh) Rasterfahndung, § 98a StPO . . . . .	336
ii) Erhebung von Verkehrsvorratsdaten, § 100g Abs. 2 StPO . . . .	337
jj) Funkzellenabfrage, § 100g Abs. 3 S. 1 StPO . . . . .	340
kk) IP-Catching . . . . .	341
c) Abstrakt mittelschwere strafprozessuale Dateneingriffe . . . . .	342
aa) (Einfache) Verkehrsdatenauskunft, § 100g Abs. 1 S. 1, S. 2 StPO . . . . .	342
bb) Nutzungsdatenauskunft bei verkehrsdatenähnlichen Nutzungsdaten, § 100k Abs. 1, Abs. 2 StPO . . . . .	342
cc) IP-Tracking, § 100g StPO . . . . .	342
dd) IMSI-Catcher, § 100i StPO . . . . .	343
ee) Offene Beschlagnahme größerer Datenmengen, § 94 StPO . . .	344

ff) Automatisierte OSINT-Maßnahmen . . . . .	345
d) Abstrakt leichte strafprozessuale Dateneingriffe . . . . .	346
aa) Bestandsdatenauskunft, § 100j StPO . . . . .	346
bb) Zugangsdatenauskunft, § 100j Abs. 1 S. 2, S. 3 StPO . . . . .	347
cc) Offene Beschlagnahme kleinerer Datenmengen, § 94 StPO . . . . .	348
dd) Manuelle OSINT-Maßnahmen . . . . .	349
ee) WLAN-Catching bei ungesicherten Netzwerken . . . . .	349
2. Schwere des strafprozessualen Dateneingriffs im Einzelfall . . . . .	350

#### Kapitel 4: Das Gewicht des staatlichen Strafverfolgungs- anspruchs bzw. der Erfordernisse einer effektiven Strafrechtspflege . . . . . 353

I. Verfassungsrang und Gewicht des Strafverfolgungsanspruchs . . . . .	354
II. Schwere der Straftat . . . . .	354
III. Grad des Tatverdachts, insbesondere Tatverdachtsgewinnung im Wege (automatisierter) Datenverarbeitung . . . . .	357
1. Grundlagen der verschiedenen Verdachtsgrade in der StPO und deren Auslegung durch Rspr. und Lehre . . . . .	358
a) Tatverdachtsgrade in der StPO . . . . .	358
b) Anforderungen an die einzelnen Tatverdachtsgrade der StPO . . . . .	358
c) Gemeinsame Fragestellungen . . . . .	360
2. Systematisierung und Strukturierung der Grundlagen zur Bewertung der Stärke des Tatverdachts und Besonderheiten bei Daten und Datenverarbeitungen als Tatverdachtsgrundlagen . . . . .	362
a) Subjektive und objektive Elemente des Tatverdachts . . . . .	363
b) Zur Tatsachenbasis . . . . .	364
aa) Allgemeines . . . . .	364
(1) Das Problem der Unbegrenztheit des Tatsachenstoffs im Ermittlungsverfahren . . . . .	365
(2) Die Bestimmung der Qualität der Tatsachenbasis . . . . .	366
bb) Die Qualität von Daten als Anknüpfungstatsachen für einen Tatverdacht . . . . .	367
(1) Die Flüchtigkeit von Daten . . . . .	367
(2) Die Manipulierbarkeit von Daten . . . . .	368
c) Schlussfolgerungen aus den vorhandenen Tatsachen und die Bildung von Heuristiken und Algorithmen . . . . .	370
aa) Kriminalistische Erfahrung und Anwendung der Regeln über die Beweiswürdigung . . . . .	370
(1) Notwendigkeit einer „kleinen“ Beweiswürdigung . . . . .	371
(2) Die Regeln der „kleinen“ Beweiswürdigung . . . . .	371
(3) Unterschiede zur „großen“ Beweiswürdigung im Urteil . . . . .	373
bb) Tatverdachtsgewinnung durch (automatisierte) Daten- verarbeitung . . . . .	374
(1) Der Einfluss von Standards der IT-Forensik . . . . .	375
(2) Deterministische Methoden . . . . .	378
(3) Statistische Methoden . . . . .	379

(a) Allgemeines . . . . .	379
(b) Das sog. Blackbox-Problem . . . . .	381
(c) Kein rein statistischer Tatverdacht in der StPO . . . . .	381
(d) Das sog. Garbage-in-garbage-out-Problem . . . . .	382
(4) Besonderheiten beim Einsatz von Machine Learning und künstlicher Intelligenz . . . . .	382
d) Bildung von Hypothese und Alternativhypothesen . . . . .	385
aa) Bildung von Alternativhypothesen zur Vermeidung des Confirmation Bias . . . . .	385
bb) Bias und Diskriminierung durch selbstlernende Programme . . . . .	386
e) Wahrscheinlichkeit . . . . .	388
aa) Grundsätzlich keine prozentuale Angabe der Wahrscheinlichkeit . . . . .	388
bb) Angabe von Genauigkeitswerten bei statistischen und selbstlernenden Programmen? . . . . .	389
IV. Auffindewahrscheinlichkeit bzgl. verfahrens- und nachweis- relevanter Daten . . . . .	392
V. Wechselwirkungen und Ordnung der Kriterien zur Bestimmung des Gewichts des Strafverfolgungsanspruchs . . . . .	393
 Kapitel 5: Die Abhängigkeit der Schutzmechanismen und Eingriffsschwellen von der Intensität des Dateneingriffs . . . . .	397
I. Die Abhängigkeit der notwendigen Eingriffsschwellen und Schutzmechanismen von der Eingriffsintensität . . . . .	399
1. Unabhängig von der Eingriffsintensität geltende Schutzmechanismen . . . . .	399
2. In Abhängigkeit von spezifischen Eingriffskriterien geltende Schutzmechanismen . . . . .	400
a) Art der Daten/Stärke des Personenbezugs: Anonymisierungs- und Pseudonymisierungspflichten . . . . .	400
b) Art der Daten: Eignung zur Persönlichkeitsprofilerstellung – Beschränkungen der Datenzusammenführung/Verbot der Erstellung von Persönlichkeitsprofilen . . . . .	402
aa) Vorfilterung von Datenbeständen . . . . .	403
(1) Filterung bei Datenextraktion aus Speichermedien . . . . .	404
(2) Aufzeichnungsfiler bei Datenströmen . . . . .	405
(3) Manuelle Filterung . . . . .	406
(4) Datenreduktion zur Effektivitätssteigerung . . . . .	407
bb) Begrenzung der Zusammenführung von Daten und Mindest- qualität der verfolgten Straftat als Eingriffsschwelle für den Einsatz von Data Mining-Methoden . . . . .	407
c) Art der Daten/Zuordnung zu Sphären des Persönlichkeitsrechts: Kernbereichsschutz . . . . .	410
d) Spezielle Vertraulichkeitsverhältnisse: Erhebungs- und Verwertungsverbote . . . . .	410
e) Streubreite: Filter-, Unverzögerlichkeits- und Löschungspflichten . . . . .	411

f) Automatisierung der Datenverarbeitung: Pflicht zum Einsatz von Programmen mit hoher Richtigkeitsgewähr, Zertifizierungs- und Offenlegungspflichten . . . . .	413
g) Heimlichkeit der Ermittlungsmaßnahme: Benachrichtigung, Richtervorbehalt und Subsidiarität . . . . .	416
aa) Benachrichtigungspflichten . . . . .	416
bb) Präventive Kontrolle durch unabhängige Stelle . . . . .	417
cc) Subsidiarität heimlicher Dateneingriffe . . . . .	418
h) Unkenntnis hinsichtlich intensitätserhöhender Faktoren: Pflicht zu Vorermittlungen oder Anpassung der Maßnahme? . . . . .	420
i) Mögliche Folgen für den Betroffenen: Pflicht zur „unauffälligen“ Durchführung, Pflicht zur Begrenzung der Datenzugänglichkeit und Pflicht zur Maximierung der Richtigkeitsgewähr? . . . . .	423
aa) Pflicht zur Maximierung der Richtigkeitswahrscheinlichkeit eingesetzter Datenverarbeitungsprogramme . . . . .	423
bb) Pflicht zur unauffälligen Durchführung von Datenerhebungsmaßnahmen . . . . .	424
cc) Beschränkung des Zugangs zu Daten . . . . .	425
3. Schutzmechanismen/Eingriffsschwellen in Abhängigkeit von der Eingriffsintensität . . . . .	426
a) Eingriffsschwellen . . . . .	426
aa) Besondere Qualitätsanforderungen an Straftaten und Straftatenkataloge als Mindestgewicht der Schwere der Straftat . . . . .	427
(1) Vorgaben des BVerfG zur notwendigen Straftatschwere und Straftatenkatalogen . . . . .	427
(2) Konkretisierung und Kritik anhand der bisherigen Ergebnisse . . . . .	429
(a) Anwendung der entwickelten Kriterien zur Bemessung der Tatschwere . . . . .	430
(b) Kritik an den bisherigen Strafrahmengrenzen . . . . .	431
(aa) Besonders schwere Straftaten . . . . .	431
(bb) Schwere Straftaten . . . . .	434
(cc) Straftaten von erheblicher Bedeutung . . . . .	435
(dd) Reformbedarf . . . . .	435
bb) Notwendige Verdachtsgrade als Mindeststärke des Tatverdachts . . . . .	437
cc) Beschränkungen des Kreises der Maßnahmeadressaten als Ausdruck des Veranlasserprinzips . . . . .	440
dd) Anforderungen an die Auffindewahrscheinlichkeit? . . . . .	441
(1) Nur vereinzelte gesetzliche Regelungen . . . . .	441
(2) Mindestanforderungen an die Auffindewahrscheinlichkeit von Verfassungen wegen . . . . .	443
b) Schutzmechanismen . . . . .	444
aa) Beschränkungen der Dauer der Maßnahme . . . . .	445
bb) Subsidiaritätsklauseln als vertyppte Erforderlichkeitsschranken und gesetzgeberische Wertung der Eingriffsintensität . . . . .	445
(1) Gesetzliche Regelung . . . . .	446
(2) Kritik und eigene Einordnung . . . . .	447
(3) Reformvorschläge . . . . .	449



cc)	Anforderungen an die Form einer Anordnung zur Absicherung der materiellen Beschränkungen . . . . .	450
(1)	Gesetzliche Regelungen . . . . .	451
(2)	Ausdifferenzierung der Begrenzungs- und Begründungspflichten durch Rspr. und Literatur . . . . .	452
4.	Fazit: Ableitung der Schutzmechanismen und Eingriffsschwellen aus dem Verhältnismäßigkeitsprinzip . . . . .	457
II.	Ergebnis: Ein „Baukastensystem“ unter Berücksichtigung der Erforderlichkeit und der Verhältnismäßigkeit ieS . . . . .	458
1.	Hinreichende Normen und Regelungslücken . . . . .	458
a)	Unmittelbar kraft Verfassungsrecht geltende Eingriffsschwellen und Schutzmechanismen . . . . .	458
b)	Hinreichend vom Gesetzgeber geregelte Eingriffsschwellen und Schutzmechanismen . . . . .	459
c)	Durch Auslegung in bestehende Regeln hineinlesbare Eingriffsschwellen und Schutzmechanismen . . . . .	460
d)	Unzureichend geregelte Eingriffsschwellen und Schutzmechanismen . . . . .	460
2.	Anwendung (auch) der nicht vom Gesetzgeber geregelten notwendigen Eingriffsschwellen und Schutzmechanismen . . . . .	462
3.	Die Eingriffsschwellen und Schutzmechanismen als „Baukastensystem“ . . . . .	462
Kapitel 6: Möglichkeiten und Grenzen neuartiger, unregulierter strafprozessualer Dateneingriffe . . . . . 465		
I.	Problemaufriss: Schnelle technologische Entwicklung und langsame Gesetzgebungsverfahren . . . . .	466
II.	Die Grenzen der Auslegung von Ermittlungsbefugnissen . . . . .	469
1.	(Grundrechtlicher) Vorbehalt des Gesetzes . . . . .	470
a)	Grenzen aus spezifischen grundrechtlichen Gesetzesvorbehalten . . . . .	470
b)	Zitiergebot . . . . .	471
c)	Weitere Vorgaben des grundrechtlichen Gesetzesvorbehalts . . . . .	474
2.	Bestimmte und normenklare Dateneingriffsbefugnisse . . . . .	476
a)	Das Prinzip der Normenklarheit und Bestimmtheit als Grenze für die extensive Auslegung bestehender Normen . . . . .	476
b)	Das Doppeltürmodell und seine Begrenzungswirkung . . . . .	478
3.	Die Wesentlichkeitslehre . . . . .	478
a)	Bereichsspezifische Wesentlichkeit . . . . .	479
b)	Bereichsspezifische Wesentlichkeit des Rechts der strafprozessualen Dateneingriffe . . . . .	480
aa)	Wesentlichkeit des betroffenen Grundrechts . . . . .	481
bb)	Wesentlichkeit der erlaubten Eingriffsintensität . . . . .	482
cc)	Wesentlichkeit der Art und Weise des strafprozessualen Dateneingriffs . . . . .	482
dd)	Die Wesentlichkeit der Verhältnismäßigkeit . . . . .	483
ee)	Wesentlichkeit einer Zweckbeschränkung . . . . .	484

c)	Wechselwirkung zwischen Wesentlichkeit und Eingriffsintensität . . . . .	484
d)	Der Wesentlichkeitsvorbehalt und das Erfordernis flexibler Regelungen . . . . .	484
e)	Ergebnis: Vorgaben der Wesentlichkeitslehre für die ausdehnende Auslegung strafprozessualer Dateneingriffsbefugnisse . . . . .	485
aa)	Vom Gesetzgeber gewollte Ausdehnung auf neuartige Ermittlungsmethode . . . . .	486
bb)	Bewusste Nichtregelung durch den Gesetzgeber . . . . .	487
cc)	Unbewusste Nichtregelung durch den Gesetzgeber . . . . .	488
(1)	Gewährleistung der Verhältnismäßigkeit des Daten- eingriffs durch die angewendete Befugnisnorm . . . . .	488
(2)	Abwägung zwischen Eingriffsintensität und Notwendigkeit flexibler Regelungen . . . . .	489
4.	(Kein generelles) Analogieverbot im Recht der strafprozessualen Ermittlungsmaßnahmen . . . . .	491
a)	Kein generelles Analogieverbot für strafprozessuale Ermittlungsbefugnisse . . . . .	491
b)	Voraussetzungen der analogen Anwendung einer straf- prozessualen Dateneingriffsbefugnis . . . . .	493
5.	Zusammenfassung der Grenzen der erweiternden Auslegung von Ermittlungsbefugnissen zur Ermöglichung neuartiger straf- prozessualer Dateneingriffe . . . . .	494
a)	Abstrakte Beschreibung der Grenzen extensiver Rechtsauslegung im Bereich strafprozessualer Dateneingriffe zur Beweisdaten- gewinnung . . . . .	494
b)	Folgen für die extensiven Auslegungsmethoden der Rechtspraxis . . . . .	495
III.	Ausweg technikoffene Eingriffsbefugnisse? . . . . .	497
1.	Verfassungsrechtliche Grenzen technikoffener Regulierung . . . . .	497
2.	Vor die Klammer gezogene allgemeine Regelungen . . . . .	498
a)	Allgemeine Kernbereichsschutzvorschrift . . . . .	499
b)	Gesetzliches Verbot der Rundumüberwachung . . . . .	501
3.	Neue Regelungen allgemeiner Fragestellungen bei strafprozessualen Dateneingriffen . . . . .	502
a)	Eigenständige Regelung des Einsatzes von Data Mining- Methoden zur Datenanalyse . . . . .	502
b)	Eigenständige Regelung zum „Knacken“ von Verschlüsselungen . . . . .	507
4.	Gesetzliche Erweiterung bestehender Eingriffsbefugnisse zur besseren Erfassung neuartiger strafprozessualer Dateneingriffe . . . . .	508
a)	Erweiterung der Erhebungsmodalitäten bestehender Eingriffs- befugnisse . . . . .	508
b)	Ausdehnung von Spezialregeln . . . . .	509
IV.	Ergebnis und kriminalpolitische Überlegungen . . . . .	510
Kapitel 7: Europarechtliche Vorgaben für die Erhebung und Verwertung digitaler Daten im Strafverfahren . . . . .		515
I.	Bedeutung des Europarechts und untersuchte Rechtsquellen . . . . .	515

II.	Vorgaben aus der Richtlinie 2016/680/EU und §§ 45 ff. BDSG . . . . .	518
1.	Anwendungsvorrang der Richtlinie und (Teil-)Unionsrechts- widrigkeit von § 500 Abs. 2 StPO und § 1 Abs. 2 BDSG . . . . .	518
a)	Umsetzung der Richtlinie in den §§ 45 ff. BDSG und Geltungs- anordnung für Landesbehörden bei Anwendung der StPO in § 500 Abs. 1 StPO . . . . .	518
b)	Exkurs: Subsidiäre Geltung der Umsetzung der Richtlinie in den Landesdatenschutzgesetzen? . . . . .	519
c)	(Teil-)Unionsrechtswidrigkeit der lex specialis-Regelungen in § 1 Abs. 2 BDSG und § 500 Abs. 2 Nr. 1 BDSG . . . . .	520
2.	Strafgerichte als „öffentliche Stellen“ und Verantwortliche iSd Richtlinie und des BDSG . . . . .	522
3.	Aus der Untersuchung ausgeklammerte Vorschriften . . . . .	524
4.	Ergänzungen und Konkretisierungen der verfassungsrechtlichen Vorgaben durch die Richtlinie . . . . .	524
a)	Zweckbindungsgrundsatz und Zweckänderungen §§ 47 Nr. 2, 49 BDSG, Art. 4 Abs. 1 b), Abs. 2, Art. 9 Abs. 1 RL . . . . .	525
aa)	Festlegung der Erhebungszwecke, § 47 Nr. 2 BDSG, Art. 4 Abs. 1 b) RL . . . . .	525
bb)	Voraussetzungen der Zweckänderung, § 49 BDSG, Art. 4 Abs. 2, 9 Abs. 1 RL . . . . .	527
(1)	Zweckänderung für Zwecke nach § 45 BDSG . . . . .	527
(2)	Zweckänderung für andere Zwecke . . . . .	528
(3)	Rechtmäßigkeit der ursprünglichen Datenerhebung als Voraussetzung für die Rechtmäßigkeit einer Zweckänderung? . . . . .	528
b)	Allgemeine Anforderungen an die Verarbeitung personen- bezogener Daten, § 47 BDSG, Art. 4 Abs. 1 RL . . . . .	529
aa)	Rechtmäßige Verarbeitung nach Treu und Glauben . . . . .	530
bb)	Verhältnismäßigkeit . . . . .	531
cc)	Grundsatz der Richtigkeit von Daten . . . . .	531
dd)	Verbot der übermäßig langen Speicherung von Daten in nicht anonymer Form . . . . .	532
c)	Konkretisierung des Grundsatzes der Normenklarheit und Bestimmtheit, Art. 8 RL . . . . .	533
d)	Verarbeitung besonderer personenbezogener Daten, § 48 BDSG, Art. 10 RL . . . . .	535
aa)	§ 48 Abs. 1 BDSG als Rechtsgrundlage . . . . .	535
bb)	§ 48 BDSG als materielle Zulässigkeitsvoraussetzung für die Verarbeitung sensibler Daten . . . . .	537
cc)	Notwendigkeit geeigneter Garantien für die Rechtsgüter der betroffenen Person . . . . .	539
dd)	Rechtsfolgen eines Verstoßes gegen Art. 48 BDSG . . . . .	541
e)	Inhaltliche Konkretisierung der Mitteilungs- und Benach- richtigungspflichten, Art. 13 RL, § 56 BDSG . . . . .	542
aa)	Mindestinhalt von Benachrichtigungen . . . . .	542
bb)	Vorgaben für das Aufschieben der oder das Absehen von der Benachrichtigung . . . . .	543

f) Anforderungen an die IT-Sicherheit strafprozessualer Daten- verarbeitung (Datensicherheit), § 64 BDSG, Art. 29 RL . . . . .	545
aa) Zielvorgaben . . . . .	545
bb) Erforderliche technische und organisatorische Maßnahmen . . .	548
(1) Richtlinienkonforme Auslegung von § 64 Abs. 1 BDSG . . .	548
(2) Risikoabschätzung . . . . .	548
(3) Abwägung und Ergreifen von Maßnahmen . . . . .	549
(4) Zu ergreifende Maßnahmen der Datensicherheit . . . . .	550
cc) Spezifische Maßnahmen für automatisierte Daten- verarbeitungen . . . . .	552
(1) Risikoabschätzung . . . . .	554
(2) Abwägung nur hinsichtlich des „Wie“ . . . . .	554
(3) Ziele der Maßnahmen . . . . .	554
(4) Zusammenfassung . . . . .	555
dd) Rechtsgrundlage für Verarbeitungsvorgänge zur Gewähr- leistung der IT-Sicherheit . . . . .	555
ee) Rechtsfolgen bei Verstößen gegen § 64 BDSG . . . . .	556
5. Neue Vorgaben für strafprozessuale Dateneingriffe aus der Richtlinie und Teil 3 des BDSG . . . . .	557
a) Pflichten zur Berichtigung und Löschung von Beweisdaten, § 75 BDSG, Art. 16 RL . . . . .	557
aa) Angaben zur Wahrscheinlichkeit der Richtigkeit bei statistischen und selbstlernenden Methoden . . . . .	558
bb) Löschungspflichten . . . . .	558
cc) Verhältnis von § 75 Abs. 2 BDSG zu § 101 Abs. 8 StPO . . . . .	559
(1) Löschungspflicht aus § 75 Abs. 2 BDSG auch für nicht in § 101 Abs. 1 StPO genannte Maßnahmen . . . . .	560
(2) Zurückstellung der Löschung zugunsten einer Einschränkung der Verarbeitung . . . . .	560
(3) Markierung von Daten, deren Verarbeitung eingeschränkt ist nach § 75 Abs. 3 iVm § 58 Abs. 4 BDSG . . . . .	563
(4) Mitteilung der Löschung an weitere Stellen, nach § 75 Abs. 3 iVm § 58 Abs. 5 S. 2 und S. 3 BDSG . . . . .	564
(5) Überprüfungsfristen, § 75 Abs. 4 BDSG . . . . .	564
dd) Exkurs: Verhältnis von § 75 Abs. 2 BDSG zu § 489 StPO . . . . .	565
ee) Rechtsfolgen bei unterbliebener Berichtigung oder Löschung . .	567
b) Verbot der automatisierten Entscheidung, Art. 11 RL, § 54 BDSG . .	568
aa) Nachteilige Rechtsfolgen und erhebliche Beeinträchtigungen . .	569
bb) Ausschließlich automatisiert getroffene Einzelfallentscheidung .	570
(1) Vollständig automatisierter Tatverdacht . . . . .	570
(2) Automatisierte Individualisierung eines Tatverdachts . . . .	571
(3) Notwendigkeit einer Rechtsgrundlage für den Einsatz von statistischen und selbstlernenden Data Mining- Methoden im Strafverfahren . . . . .	573
cc) Anforderungen aus Art. 11 RL, § 54 BDSG an eine spezifische Rechtsgrundlage für ausschließlich automatisiert getroffene nachteilige Entscheidungen . . . . .	573
dd) Verbot des diskriminierenden Profilings . . . . .	576

ee) Rechtsfolge eines Verstoßes gegen das Verbot der automatisierten Einzelfallentscheidung . . . . .	577
c) Anforderungen für eine strafprozessuale Datenverarbeitung auf Grundlage einer Einwilligung, §§ 51, 46 Nr. 17 BDSG, Art. 8 RL, Erwägungsgrund 35 RL . . . . .	577
aa) Einwilligung nur noch mit maßnahmespezifischer Rechtsgrundlage . . . . .	578
bb) Freiwilligkeit der Einwilligung – echte freie Entscheidung bei Duldungs- und Mitwirkungspflichten? . . . . .	581
cc) Weitere formelle Voraussetzungen der Einwilligung und Widerrufsmöglichkeit . . . . .	583
(1) Beweislast für das Vorliegen einer Einwilligung . . . . .	583
(2) Belehrungspflichten . . . . .	583
(3) Verarbeitung besonderer personenbezogener Daten auf Grundlage einer Einwilligung . . . . .	584
(4) Widerrufsrecht . . . . .	585
dd) Rechtsfolgen bei Verstößen gegen die Regeln zur Einwilligung in die Datenverarbeitung . . . . .	585
d) Data Protection by Design and by Default, § 71 BDSG, Art. 20 RL . . . . .	586
aa) Data Protection by Design, Abs. 1 . . . . .	586
(1) Risikoabschätzung und Abwägung . . . . .	587
(2) Keine Beschränkung auf rein technische Maßnahmen . . . . .	587
(3) Zu ergreifende technische und organisatorische Maßnahmen . . . . .	588
(4) Zeitpunkte und Adressaten der Pflicht zur Maßnahmen-ergreifung . . . . .	590
(5) Vorrang technischer Lösungen . . . . .	592
bb) Data Protection by Default, Abs. 2 . . . . .	593
cc) Rechtsfolge bei Verstößen gegen § 71 BDSG . . . . .	594
e) Protokollierungspflichten bei automatisierter Datenverarbeitung, § 76 BDSG, Art. 25 RL . . . . .	595
aa) Automatisiertes Datenverarbeitungssystem . . . . .	595
bb) Zu protokollierende Datenverarbeitungsvorgänge . . . . .	595
cc) Inhalt und Form der Protokollierung . . . . .	598
dd) Konkurrenz zu fachgesetzlichen Protokollierungspflichten, insbesondere § 100a Abs. 6 StPO . . . . .	599
ee) Verwendungsbeschränkungen – insbesondere Verstoß gegen nemo tenetur-Prinzip? . . . . .	600
ff) Herausgabe- und Löschungspflichten, Abs. 4, Abs. 5 . . . . .	601
gg) Rechtsnatur und Rechtsfolge . . . . .	602
f) Differenzierungsgebot nach § 72 BDSG, Art. 6 RL . . . . .	602
g) Differenzierungs- und Kennzeichnungsgebot nach § 73 BDSG, Art. 7 Abs. 1 RL . . . . .	604
aa) Pflicht zur Differenzierung, § 73 S. 1 BDSG, Art. 7 Abs. 1 RL . . . . .	605
bb) Abgrenzung zwischen Tatsachen und persönlichen Einschätzungen . . . . .	606
cc) Kennzeichnungspflicht, § 73 S. 2 BDSG . . . . .	608
dd) Transparenz hinsichtlich der Grundlagen einer persönlichen Einschätzung, § 73 S. 3 BDSG . . . . .	609

ee) Unmöglichkeits- und Angemessenheitsvorbehalt . . . . .	609
ff) Rechtsfolgen von § 73 BDSG, Art. 7 Abs. 1 RL? . . . . .	609
gg) Praktische Bedeutung beim Teilen und Annotieren von Informationen . . . . .	611
h) Datenschutzfolgenabschätzung, § 67 BDSG, Art. 27 RL . . . . .	612
aa) Notwendigkeit einer DFA . . . . .	612
bb) Notwendiger Inhalt einer DFA . . . . .	615
cc) Verfahrensregeln für eine DFA . . . . .	616
dd) Pflicht zur Überprüfung . . . . .	619
ee) Strafprozessuale Rechtsfolgen bei unterlassener oder nicht richtig vorgenommener DFA . . . . .	619
ff) Strafprozessuale Rechtsfolgen bei Verstoß gegen Vorgaben der DFA . . . . .	619
i) Anhörung/Beteiligung des Bundes-/Landesdatenschutz- beauftragten bei besonders risikoreichen Dateisystemen, § 69 BDSG, Art. 28 RL . . . . .	620
aa) Bindungswirkung der Empfehlungen des Datenschutz- beauftragten . . . . .	621
bb) Beginn der Datenverarbeitung in Eilfällen . . . . .	622
j) Überprüfung von Daten vor ihrer Übermittlung, § 74 BDSG, Art. 7 Abs. 2, Art. 9 Abs. 3 und Abs. 4 RL . . . . .	623
aa) Sicherung der Datenqualität vor Übermittlung, § 74 Abs. 1 BDSG . . . . .	624
(1) Angemessene Maßnahmen . . . . .	624
(2) Spezifische Überprüfungspflicht, § 74 Abs. 1 S. 2 BDSG . . . . .	625
(3) Informationspflicht, § 74 Abs. 1 S. 3 BDSG . . . . .	625
bb) Mitteilung besonderer Verarbeitungsbedingungen, Abs. 2 . . . . .	626
cc) Rechtsnatur und Rechtsfolgen bei Verstoß . . . . .	627
III. Bedeutungsgewinn der europäischen Grund- und Menschenrechte für die strafprozessuale Datenverarbeitung . . . . .	628
1. Europarechtliche Überlagerung des Rechts der strafprozessualen Datenverarbeitung zur Gewinnung von Beweisdaten . . . . .	628
2. Auswirkungen der europarechtlichen Überlagerung des Rechts der strafprozessualen Beweisdatengewinnung und -verwertung auf die Bedeutung der europäischen Grund- und Menschenrechte . . . . .	630
a) Bisherige Auswirkung der europäischen Grund- und Menschenrechte auf das Recht der strafprozessualen Beweisdaten- gewinnung und -verwertung . . . . .	630
b) Paradigmenwechsel durch die Richtlinie 2016/680/EU? . . . . .	631
aa) Strafprozessuale Erhebung und Verarbeitung personen- bezogener Daten als Durchführung von Recht der EU? . . . . .	633
(1) Rspr. des EuGH . . . . .	633
(2) Rspr. des BVerfG . . . . .	634
(3) Strafprozessuale Dateneingriffsbefugnisse als Durch- führung europäischen Rechts? . . . . .	635
(a) Deckungsgleichheit der Ziele von Richtlinie und StPO . . . . .	635
(b) Voraussetzungen der BVerfG-Rspr. . . . .	636

(c) Kein Verstoß gegen die Verfassungsidentität und kein Ultra-vires-Rechtsakt . . . . .	637
(d) Zusammenfassung . . . . .	639
bb) Verhältnis der deutschen Grundrechte zu GRC/EMRK im Rahmen strafprozessualer Dateneingriffe und der Richtlinie 2016/680/EU . . . . .	639
(1) Recht auf Vergessen I und II . . . . .	640
(2) Europäischer Haftbefehl III (u. a.) . . . . .	642
(3) Prüfungsmaßstab für die Umsetzungsnormen der Richtlinie 2016/680/EU . . . . .	642
(a) Umsetzungsspielräume in den Richtliniennormen . . . . .	643
(b) Keine gewollte Grundrechtseinheit bei bestehenden Umsetzungsspielräumen . . . . .	645
(c) Europäische Grundrechte „nur“ als Mindeststandard . . . . .	647
3. Ergebnis: Bedeutungsgewinn der europäischen Grundrechte im Bereich der strafprozessualen Verarbeitung personenbezogener Daten . . . . .	647
IV. Verhältnis der Vorgaben aus der Richtlinie zu den verfassungsrechtlichen Vorgaben und Leitlinien (Meistbegünstigungsprinzip) . . . . .	648
 Kapitel 8: Zentrale Probleme der Verwendung von Daten und Datenanalysen als Beweismittel in der Hauptverhandlung . . . . .	651
I. Das Übersetzungsproblem: Die fehlende unmittelbare Wahrnehmbarkeit von Daten und der Grundsatz des sachnäheren Beweismittels . . . . .	653
1. Der Einfluss der gewählten Beweismittelart auf den zur Verfügung stehenden Informationsgehalt . . . . .	654
a) Beschränkung der verwertbaren Informationen durch die gewählte „Übersetzungsart“ . . . . .	655
b) Der Datensatz selbst als qualitativ „bestes“ Beweismittel . . . . .	656
2. Pflicht zur Verwendung des „besseren“ bzw. sachnäheren Beweismittels? . . . . .	659
a) Amtsaufklärungspflicht, § 244 Abs. 2 StPO . . . . .	660
b) Prinzip der freien richterlichen Beweiswürdigung, § 261 StPO . . . . .	661
c) Hinreichende Sachverhaltsaufklärung und lückenlose Beweiswürdigung bei Daten als Beweismittel . . . . .	661
aa) Pflicht zur Heranziehung des sachnächsten und bestmöglichen Beweismittels . . . . .	662
bb) Verbot der Beweisantizipation . . . . .	662
cc) Ermittlungsbeamte als sachverständige Zeugen . . . . .	664
3. Ergebnis: Einzelfallfrage unter Berücksichtigung der Amtsaufklärungspflicht und der Grundsätze der freien richterlichen Beweiswürdigung . . . . .	664
II. Flüchtigkeit und Manipulierbarkeit: IT-forensische Standards und strafprozessuales Beweisrecht . . . . .	665
1. Authentizität und Integrität in der IT-Forensik . . . . .	665

2.	Folgen fehlender (nicht beweisbarer) Authentizität und Integrität im Beweisrecht der StPO . . . . .	669
a)	Stand der Forschung: Maximierung des Beweiswerts . . . . .	669
b)	Berücksichtigung der Authentizität und Integrität im Recht der freien Beweiswürdigung . . . . .	669
aa)	Lückenlosigkeit der Beweiswürdigung . . . . .	670
bb)	Verbot der Berücksichtigung nicht existenter Erfahrungssätze . . . . .	671
cc)	Pflicht zur erschöpfenden Beweiswürdigung . . . . .	672
III.	Beweiswert und Beweiswürdigung von Datenanalyseergebnissen . . . . .	673
1.	IT-forensische Standards für Datenanalysen . . . . .	673
2.	IT-forensische Standards für Datenanalysen im Beweisrecht . . . . .	674
3.	Gesicherte wissenschaftliche Erkenntnisse und sonstige Erfahrungssätze im Beweisrecht der StPO . . . . .	675
a)	Wissenschaftlich gesicherte Erkenntnisse . . . . .	675
b)	Neue wissenschaftliche Erkenntnisse und Untersuchungsmethoden . . . . .	676
c)	Wissenschaftliche Erkenntnisse mit wissenschaftlich fundierter Richtigkeitswahrscheinlichkeit . . . . .	677
d)	Sonstige Erfahrungssätze . . . . .	677
4.	IT-forensische Standards der Datenanalyse als Erfahrungssätze oder gesicherte wissenschaftliche Erkenntnis? . . . . .	677
a)	Deterministische Methoden als gesicherte wissenschaftliche Erkenntnisse . . . . .	678
b)	Statistische Methoden als Erfahrungssätze mit wissenschaftlich fundierter Wahrscheinlichkeitsaussage? . . . . .	680
aa)	Wissenschaftlich fundierte Aussagen zur Richtigkeitswahrscheinlichkeit und Annahmen . . . . .	681
bb)	Änderung der Richtigkeitswahrscheinlichkeit von Annahmen im Zeitverlauf . . . . .	682
cc)	Garbage-in-garbage-out-Problem . . . . .	683
c)	Selbstlernende Methoden (Machine Learning, künstliche Intelligenz) . . . . .	684
d)	Standardisierte und nicht standardisierte Methoden . . . . .	684
aa)	DNA-Analysen . . . . .	685
bb)	Automatisierte Geschwindigkeitsmessungen . . . . .	686
cc)	Fehlende Standardisierung bei IT-forensischen Untersuchungen und Datenanalysemethoden . . . . .	687
IV.	Das Blackbox-Problem und strafprozessuales Beweisrecht . . . . .	688
1.	Blackbox-Tools und gerichtliche Aufklärungspflicht, § 244 Abs. 2 StPO . . . . .	689
a)	Vorrang von Tools mit bekannter Funktionalität . . . . .	690
b)	Pflicht zur Aufklärung der Funktionalität von Untersuchungs- und Datenanalysemethoden . . . . .	691
2.	Blackbox-Tools in der Beweiswürdigung . . . . .	694
a)	Anwendung von Interpretations-Tools und Testverfahren . . . . .	694
b)	Beweiswürdigung in Abhängigkeit von der Aussagekraft über die Richtigkeitswahrscheinlichkeit . . . . .	696



c)	Entgegenstehen von Geheimhaltungsinteressen der Polizei/ Staatsanwaltschaft und von Software-Herstellern? . . . . .	698
V.	Datenanalyse, Akteneinsicht und prozessuale Waffengleichheit . . . . .	698
1.	Zu berücksichtigende Interessen . . . . .	699
2.	Recht auf Einsicht in Akten und Besichtigung von Beweisstücken, § 147 StPO . . . . .	700
a)	Einfluss des verwendeten Aktenbegriffs . . . . .	701
b)	Aktenbestandteil oder Beweisstück – Einfluss der Kopierbarkeit . . . . .	703
aa)	Kopie der Beweisdaten als Aktenbestandteil . . . . .	704
bb)	Informationen über Datenanalysemethoden . . . . .	705
(1)	Art und Weise des Zugangs zu den Programmen . . . . .	705
(2)	Erwerb eines Datenanalyseprogramms als notwendige Auslagen iSv § 464a Abs. 2 StPO . . . . .	706
(3)	Besichtigungsrecht des „Original-Programms“ als kostengünstige Alternative . . . . .	707
(4)	Programme mit Plattformzugängen . . . . .	708
(5)	Akteneinsichtsrecht und Quellcode . . . . .	708
cc)	Zwischenergebnis . . . . .	709
c)	Verweigerung des Einsichtsrechts aufgrund entgegenstehender Interessen? . . . . .	709
aa)	Beschränkungen während des noch laufenden Ermittlungs- verfahrens . . . . .	710
bb)	Keine Beschränkungen aus § 32f StPO . . . . .	711
cc)	Beschränkung des Akteneinsichtsrechts des unverteidigten Beschuldigten . . . . .	711
d)	Beschränkungen der Weitergabe der Daten und der Datenanalyseprogramme durch den Verteidiger und/oder den Beschuldigten an Dritte . . . . .	712
aa)	Weitergabe der Informationen durch den Verteidiger an den Beschuldigten oder Dritte . . . . .	712
(1)	(Keine) Beschränkung der Weitergabebefugnis an den Beschuldigten durch Geheimhaltungsinteressen . . . . .	713
(2)	Beschränkung der Weitergabe an Dritte . . . . .	715
bb)	Weitergabe der Informationen durch den Beschuldigten an Dritte . . . . .	717
e)	Ergebnis zum Akteneinsichtsrecht . . . . .	718
3.	Recht auf Zugang zu verfahrensrelevanten Informationen außerhalb der Verfahrensakten und der Beweisstücke . . . . .	719
a)	Informationsrecht als Ausfluss des Rechts auf ein faires Verfahren und praktische Bedeutung . . . . .	719
b)	Begrenzungen des Informationsrechts . . . . .	721
c)	Art und Weise der Informationsgewährung . . . . .	723
d)	Ergebnis . . . . .	724
4.	Ergebnis und Überlegungen de lege ferenda . . . . .	724

## Kapitel 9: Schlussbetrachtungen: Zusammenfassung der Thesen und Erkenntnisse zu digitalen Daten als Beweismittel im Strafverfahren . . . . .

727

I.	Kapitel 2 bis 6: Verfassungsrechtliche und verfassungsgerichtliche Vorgaben für die Normsetzung und Anwendung strafprozessualer Dateneingriffe zur Beweisdatengewinnung . . . . .	728
1.	Abgeleitete Thesen und Erkenntnisse aus der Analyse der verfassungsgerichtlichen Rechtsprechung zu strafprozessualen Dateneingriffen . . . . .	728
a)	Eingriffe in das Telekommunikationsgeheimnis, Art. 10 Abs. 1 GG . . . . .	728
aa)	Aufgabe des personalen Bezugs der Telekommunikation iSv Art. 10 Abs. 1 GG . . . . .	728
bb)	Das Beherrschbarkeitskriterium zur Bestimmung der zeitlich-örtlichen Grenzen des Schutzbereichs . . . . .	729
cc)	„Ruhende“ Telekommunikation und Aufgabe der intersubjektivität der Telekommunikation . . . . .	731
dd)	Probleme im Zusammenhang mit der Vertraulichkeitserwartung . . . . .	732
ee)	Einbeziehung verschiedener Datenarten in den Schutzbereich des Art. 10 Abs. 1 GG . . . . .	735
ff)	Heimliche Initiierung eines Kommunikationsvorgangs durch die Strafverfolgungsbehörden als Eingriff in Art. 10 Abs. 1 GG? . . . . .	735
gg)	Recht auf Verschlüsselung der Telekommunikation . . . . .	736
hh)	Zentrale These: Weiterentwicklung des Fernmeldegeheimnisses über das Telekommunikationsgeheimnis hin zum umfassenden „Daten- und Informationsübertragungsgeheimnis“ . . . . .	736
b)	Eingriffe in das RiS, Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG . . . . .	737
aa)	Eingriff auch bei Erhebung öffentlich zugänglicher Daten . . . . .	737
bb)	Eingriff bei Erhebung von Daten unter Identitätstäuschung . . . . .	737
cc)	Das Verdichtungskriterium bei den sog. Nichttreffer-Fällen . . . . .	738
c)	Eingriffe in das IT-System-Grundrecht, Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG . . . . .	738
aa)	Eingriffe durch Datenerhebung aus dem IT-System – Verhältnis zum RiS . . . . .	738
bb)	Vernetzte Systeme 1: WLANs und LANs . . . . .	739
cc)	Vernetzte Systeme 2: Cloud-Dienste und VPNs . . . . .	739
dd)	Verhältnis zum Telekommunikationsgeheimnis (Quellen-TKÜ) . . . . .	740
ee)	Verhältnis zu Art. 13 GG (Überwachung des Wohnraums durch Infiltration des IT-Systems) . . . . .	740
d)	Verfassungsrechtliche Vorgaben zu Eingriffsschwellen und Schutzmechanismen . . . . .	741
aa)	Kernbereichsschutz . . . . .	741
bb)	Verbot der Erstellung von Persönlichkeitsprofilen . . . . .	743
cc)	Verbot der Rundumüberwachung . . . . .	743

dd) Einschränkungen der Mitteilungspflichten . . . . .	744
e) Zentrale Thesen aus der Analyse der verfassungsrechtlichen Vorgaben für strafprozessuale Dateneingriffe zur Beweisdatengewinnung . . . . .	744
aa) Umfassender Schutz von Daten vor strafprozessualen Dateneingriffen . . . . .	744
bb) Unabhängigkeit der Eingriffsschwellen und Schutz- mechanismen vom betroffenen Grundrecht . . . . .	745
cc) Eingriffsintensität als entscheidendes Kriterium für Eingriffsschwellen und Schutzmechanismen . . . . .	745
dd) Systematisierung der Eingriffsschwellen und Schutzmechanismen . . . . .	745
ee) Offene Fragen und Definition der weiteren Untersuchungsziele . . . . .	746
2. Ergebnisse und Thesen hinsichtlich der Kriterien zur Eingriffstiefbestimmung . . . . .	747
a) Die Kriterien zur Bestimmung der Intensität eines strafprozessualen Dateneingriffs zur Beweisdatengewinnung . . . .	747
b) Die relative ordinale Ordnung der Eingriffsschwerkriterien . . . .	749
c) Anwendung der relativen ordinalen Ordnung der Schwerekriterien auf bestehende und neuartige strafprozessuale Dateneingriffe . . . .	753
3. Ergebnisse und Thesen zu den Kriterien zur Bestimmung des Gewichts des staatlichen Strafverfolgungsanspruchs . . . . .	754
a) Schwere der Straftat . . . . .	755
b) Stärke des Tatverdachts . . . . .	755
aa) Objektive und subjektive Kriterien zur Bestimmung der Stärke des Tatverdachts . . . . .	755
bb) Tatsachenbasis . . . . .	756
cc) Nachvollziehbarkeit der Schlussfolgerungen . . . . .	757
dd) Hypothese und Alternativhypothese . . . . .	758
ee) Wahrscheinlichkeit der Tatbegehung und Tatbeteiligung . . . .	758
c) Auffindewahrscheinlichkeit . . . . .	759
d) Wechselwirkungen und Ordnung der Kriterien zur Bestimmung des Gewichts des Strafverfolgungsanspruchs . . . . .	759
4. Ergebnisse und Thesen zu den aus dem Verfassungsrecht abgeleiteten Eingriffsschwellen und Schutzmechanismen für strafprozessuale Dateneingriffe . . . . .	760
a) Unabhängig von der Eingriffsintensität geltende Schutzmechanismen . . . . .	761
b) In Abhängigkeit von spezifischen Eingriffskriterien geltende Schutzmechanismen . . . . .	761
c) Schutzmechanismen/Eingriffsschwellen in Abhängigkeit von der (Gesamt-)Eingriffsintensität . . . . .	762
d) Identifizierung hinreichender gesetzlicher Regelungen und bestehender Regelungslücken . . . . .	762
aa) Hinreichend umgesetzte Eingriffsschwellen und Schutzmechanismen . . . . .	762
bb) Durch Auslegung gewinnbare Eingriffsschwellen- und Schutzmechanismusregelungen . . . . .	763

cc) Unzureichende und fehlende gesetzliche Regelungen zu den Eingriffsschwellen und Schutzmechanismen . . . . .	764
dd) Unmittelbar geltende Verfassungsprinzipien . . . . .	766
e) „Baukastensystem“ und Verhältnismäßigkeitsprinzip . . . . .	767
5. Ergebnisse und Thesen zu Bestimmtheit, Wesentlichkeit und unregulierten strafprozessualen Dateneingriffen . . . . .	767
a) Grenzen der erweiternden Auslegung von Ermittlungsbefugnissen zur Ermöglichung neuartiger strafprozessualer Dateneingriffe . . .	768
aa) Grenzen der erweiternden Auslegung bestehender Eingriffsbefugnisse . . . . .	768
bb) Folgerungen für die „kreative“ Rechtsauslegung im Bereich strafprozessualer Dateneingriffe . . . . .	769
b) Möglichkeiten und Grenzen der Schaffung „technikoffener“ Eingriffsgrundlagen . . . . .	771
II. Kapitel 7: Europarechtliche Vorgaben für die Schaffung und Auslegung strafprozessualer Dateneingriffsbefugnisse zur Beweisdatengewinnung . . . . .	773
1. Vorgaben aus der Richtlinie 2016/680/EU und den §§ 45 ff. BDSG . . .	774
a) Geltungsvorrang der Richtlinie und (Teil-)Unionsrechtswidrigkeit von § 500 Abs. 2 StPO und § 1 Abs. 2 BDSG . . . . .	774
b) Adressaten der Richtlinien und BDSG-Normen . . . . .	774
c) Ergänzungen und Konkretisierungen der verfassungsrechtlichen Vorgaben durch Richtlinienvorschriften und das BDSG . . . . .	774
aa) Zweckbindungsgrundsatz und Zweckänderungen, §§ 47 Nr. 2, 49 BDSG, Art. 4 Abs. 1 b), Abs. 2, Art. 9 Abs. 1 RL . . . . .	775
bb) Allgemeine Anforderungen an die Verarbeitung personenbezogener Daten, § 47 BDSG, Art. 4 Abs. 1 RL . . . . .	775
cc) Konkretisierung des Grundsatzes der Normenklarheit und Bestimmtheit, Art. 8 RL . . . . .	776
dd) Verarbeitung besonderer personenbezogener Daten, § 48 BDSG, Art. 10 RL . . . . .	776
ee) Inhaltliche Konkretisierung der Mitteilungs- und Benachrichtigungspflichten, § 56 BDSG, Art. 13 RL . . . . .	777
ff) Anforderungen an die IT-Sicherheit strafprozessualer Datenverarbeitung (Datensicherheit), § 64 BDSG, Art. 29 RL . .	777
d) Neue Vorgaben für strafprozessuale Dateneingriffe aus der Richtlinie und Teil 3 des BDSG . . . . .	778
aa) Pflichten zur Berichtigung und Löschung von Beweisdaten, § 75 BDSG, Art. 16 RL . . . . .	778
bb) Verbot der automatisierten Entscheidung, § 54 BDSG, Art. 11 RL . . . . .	779
cc) Anforderungen für eine strafprozessuale Datenverarbeitung auf Grundlage einer Einwilligung, §§ 51, 46 Nr. 17 BDSG, Art. 8 RL, Erwägungsgrund 35 RL . . . . .	781
dd) Data Protection by Design and by Default, § 71 BDSG, Art. 20 RL . . . . .	781
ee) Protokollierungspflichten bei automatisierter Datenverarbeitung, § 76 BDSG, Art. 25 RL . . . . .	782

ff) Differenzierungsgebot nach § 72 BDSG, Art. 6 RL . . . . .	782
gg) Differenzierungs- und Kennzeichnungsgebot nach § 73 BDSG, Art. 7 Abs. 1 RL . . . . .	783
hh) Datenschutzfolgenabschätzung, § 67 BDSG, Art. 27 RL . . . . .	784
ii) Anhörung/Beteiligung des Bundes- bzw. Landesdatenschutz- beauftragten bei besonders risikoreichen Dateisystemen, § 69 BDSG, Art. 28 RL . . . . .	785
jj) Überprüfung von Daten vor ihrer Übermittlung, § 74 BDSG, Art. 7 Abs. 2, Art. 9 Abs. 3 und Abs. 4 RL . . . . .	785
e) Strafprozessuale Rechtsfolgen bei Verstößen gegen §§ 45 ff. BDSG (iVm § 500 Abs. 1 StPO) . . . . .	786
2. Bedeutungsgewinn der europäischen Grund- und Menschenrechte für die strafprozessuale Datenverarbeitung . . . . .	786
a) Strafprozessuale Erhebung und Verarbeitung personenbezogener (Beweis-)Daten als Durchführung von Recht der EU . . . . .	786
b) Verhältnis der deutschen Grundrechte zu GRC/EMRK im Rahmen strafprozessualer Dateneingriffe und der Richtlinie 2016/680/EU . . . . .	787
c) Großer Bedeutungsgewinn der GRC und EMRK . . . . .	788
III. Kapitel 8: Zentrale Probleme der Verwendung von Daten und Datenanalysen als Beweismittel in der Hauptverhandlung . . . . .	789
1. Das Übersetzungsproblem: Daten, Informationen und der Grundsatz des sachnäheren Beweismittels . . . . .	789
a) Der Einfluss der gewählten Beweismittelart auf den zur Verfügung stehenden Informationsgehalt . . . . .	789
b) Pflicht zur Verwendung des „besseren“ bzw. sachnäheren Beweismittels . . . . .	789
2. Flüchtigkeit und Manipulierbarkeit: IT-forensische Standards und strafprozessuales Beweisrecht . . . . .	790
3. Beweiswert und Beweiswürdigung von Datenanalyseergebnissen . . . . .	791
a) IT-forensische Standards der Datenanalyse als Erfahrungssätze oder gesicherte wissenschaftliche Erkenntnis . . . . .	792
aa) Deterministische Methoden als gesicherte wissenschaftliche Erkenntnisse . . . . .	792
bb) Statistische Methoden als Erfahrungssätze mit wissen- schaftlich fundierter Wahrscheinlichkeitsaussage . . . . .	792
cc) Selbstlernende Methoden (Machine Learning, künstliche Intelligenz) . . . . .	793
b) Standardisierte und nicht standardisierte Methoden . . . . .	793
aa) Reduzierte Anforderungen bei standardisierten Unter- suchungsmethoden . . . . .	794
bb) Fehlende Standardisierung der Analysemethoden der IT-Forensik . . . . .	794
4. Das Blackbox-Problem und strafprozessuales Beweisrecht . . . . .	794
a) Blackbox-Tools und gerichtliche Aufklärungspflicht, § 244 Abs. 2 StPO . . . . .	795
aa) Vorrang von Tools mit bekannter Funktionalität . . . . .	795

bb) Pflicht zur Aufklärung der Funktionalität von Untersuchungs- und Datenanalysemethoden . . . . .	795
b) Blackbox-Tools in der Beweiswürdigung . . . . .	796
aa) Anwendung von Interpretations-Tools und Testverfahren . . . .	796
bb) Beweiswürdigung in Abhängigkeit von der Aussagekraft über die Richtigkeitswahrscheinlichkeit . . . . .	796
5. Datenanalyse, Akteneinsicht und prozessuale Waffengleichheit . . . .	796
a) Umfangreiches Recht des Verteidigers und des unverteidigten Beschuldigten auf Einsichtnahme . . . . .	797
b) Keine dauerhafte Beschränkung der Einsichtsrechte möglich . . . .	798
c) Lückenhafter Schutz der Geheimhaltungsinteressen . . . . .	798
 Literaturverzeichnis . . . . .	 801
Stichwortverzeichnis . . . . .	827