

CHRISTIAN RÜCKERT

Digitale Daten
als Beweismittel
im Strafverfahren

Jus Poenale

24

Mohr Siebeck

JUS POENALE
Beiträge zum Strafrecht

Band 24



Christian Rückert

Digitale Daten als Beweismittel im Strafverfahren

Mohr Siebeck

Christian Rückert, geboren 1986; Studium der Rechtswissenschaft an der Universität Erlangen-Nürnberg; Wissenschaftlicher Mitarbeiter an den Universitäten Erlangen-Nürnberg, Marburg und dem Karlsruher Institut für Technologie; 2011 Erstes Juristisches Staatsexamen; Rechtsreferendariat im Oberlandesgerichtsbezirk Nürnberg; 2013 Zweites Juristisches Staatsexamen; 2017 Promotion; Akademischer Rat a. Z. an der Universität Erlangen-Nürnberg; Post-Doc im DFG-Graduiertenkolleg „Cyberkriminalität und Forensische Informatik“; 2022 Habilitation; Lehrstuhlvertretung der Professur für Deutsches, Europäisches und Internationales Strafrecht, Strafprozessrecht und Wirtschaftsstrafrecht an der Universität Mannheim; Inhaber des Lehrstuhls für Strafrecht, Strafprozessrecht und IT-Strafrecht an der Universität Bayreuth.

Die Veröffentlichung dieser Habilitationsschrift wurde finanziell gefördert durch das DFG Graduiertenkolleg 2475 Cyberkriminalität und Forensische Informatik.

ISBN 978-3-16-162216-8 / eISBN 978-3-16-162217-5
DOI 10.1628/978-3-16-162217-5

ISSN 2198-6975 / eISSN 2568-8499 (Jus Poenale)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über <https://dnb.dnb.de> abrufbar.

© 2023 Mohr Siebeck Tübingen. www.mohrsiebeck.com

Dieses Werk ist lizenziert unter der Lizenz „Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International“ (CC BY-NC-ND 4.0). Eine vollständige Version des Lizenztextes findet sich unter: <https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>.

Jede Verwendung, die nicht von der oben genannten Lizenz umfasst ist, ist ohne Zustimmung des Verlags unzulässig und strafbar.

Das Buch wurde von Gulde Druck in Tübingen aus der Stempel Garamond gesetzt und auf alterungsbeständiges Werkdruckpapier gedruckt. Es wurde von der Buchbinderei Spinner in Ottersweier gebunden.

Printed in Germany.

Vorwort

Die vorliegende Arbeit wurde im Mai/Juni 2022 als habilitationswürdige Leistung vom Fachbereich Rechtswissenschaft der Rechts- und Wirtschaftswissenschaftlichen Fakultät der Friedrich-Alexander-Universität Erlangen-Nürnberg anerkannt. Für die Drucklegung konnten Rechtsänderungen, Rechtsprechung und Literatur bis Anfang Februar 2023 berücksichtigt werden. Angesichts der Länge des Werks und der daraus resultierenden Überarbeitungsdauer des Manuskripts wurden bei einigen nur online und periodisch erscheinenden Werken Ergänzungslieferungen und Neuauflagen nur bis Ende 2022 berücksichtigt. Details lassen sich dem Literaturverzeichnis entnehmen. Kolleg*innen, deren einschlägige Veröffentlichungen erst nach diesen Zeitpunkten erschienen sind oder aktualisiert wurden, mögen mir dies nachsehen.

“The whole concept of the self-made man or woman is a myth” (Arnold Schwarzenegger).

In diesem Sinne bin ich so vielen Menschen zu Dank verpflichtet. Nennen kann ich hier leider nur ein paar wenige. Dank gilt zunächst meinen akademischen Lehrern, Mentoren und Förderern Christoph Safferling, Hans Kudlich, Felix Freiling und Rainer Böhme sowie meinem „Entdecker“ Matthias Jahn und dem „Retter“ meiner akademischen Karriere Georg Caspers. Besonders hervorheben möchte ich Mustafa Oglakcioglu, den ich im wahrsten Sinne des Wortes als meinen Bruder im Geiste betrachte. Mustafa hat mich nicht nur gefördert und unterstützt, als guter Freund hat er auch großen Anteil daran, dass ich nicht zwischendurch die Flinte ins Korn geworfen habe. Dank gilt außerdem Gabriele Kett-Straub und Tobias Singelnstein für die äußerst zügige Erstellung der weiteren Habilitationsgutachten sowie meinem Onkel, Horst Rückert, für seinen unermüdlichen Einsatz bei den orthographischen Korrekturen dieser Arbeit.

Großen Einfluss auf die Forschung, die diesem Buch zugrunde liegt, hatten außerdem alle Mitglieder des DFG-Graduiertenkollegs 2475 Cyberkriminalität und Forensische Informatik, allen voran meine Mitstreiter*innen aus der AG StPO und IT-Forensik, Janine Schneider, Nicole Scheler, Dominic Deuber, Florian Nicolai, Benedikt Lorch, Jens Trautmann und Jenny Ottmann. Dankbar bin ich auch für wertvollen Input aus der Praxis der Strafverfolgung und Strafverteidigung. Hervorheben möchte ich hier vor allem die vertrauensvolle Zusammenarbeit mit der Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg, namentlich vertreten durch Thomas Goger, dessen scharfsinnige Argumente aus unseren Diskussionen häufig Eingang in meine eigenen Überlegungen gefunden haben.

Besonderer Dank gilt der Deutschen Forschungsgemeinschaft (DFG), die im Rahmen ihres Graduiertenkollegs 2475 Cyberkriminalität und Forensische Informatik sowohl die Erstellung als auch die Veröffentlichung dieser Arbeit – insbesondere auch als Open Access-Veröffentlichung – so großzügig gefördert und damit ermöglicht hat.

Für die Erhaltung meiner mentalen und emotionalen Stabilität während der Habilitationszeit, aber auch darüber hinaus, bedanke ich mich schließlich bei meiner Frau, meinen Eltern und meinen Freunden am Eisen und am Spielbrett.

Widmen möchte ich diese Arbeit meinem Sohn, der mich täglich daran erinnert, dass unsere Welt voller Wunder steckt, die es zu entdecken gilt.

Bayreuth, im Oktober 2023

Christian Rückert

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 strafprozessuale Dateneingriffe zur Beweisdatengewinnung	40
a) Unstreitiger Schutzbereich: Prozess, Produkt, Umstände der Telekommunikation	40
b) Erfordernis eines personalen Bezugs der Kommunikationsinhalte?	41
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. Hörfälle 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) unstrittige 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 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
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) Datenverarbeitung	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		
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-, Unverzughlichkeits- 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 Maßnahmedressaten 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 anonymisierter 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 Datenverarbeitung (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 Datenverarbeitungen	552
	(1) Risikoabschätzung	554
	(2) Abwägung nur hinsichtlich des „Wie“	554
	(3) Ziele der Maßnahmen	554
	(4) Zusammenfassung	555
dd)	Rechtsgrundlage für Verarbeitungsvorgänge zur Gewährleistung 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

e)	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 Beweismittelwürdigung, § 261 StPO	661
c) Hinreichende Sachverhaltsaufklärung und lückenlose Beweismittelwürdigung 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 Beweismittelwürdigung	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

Kapitel 1

Die Erhebung und Verwertung digitaler Beweismitteldaten als Herausforderung für das Strafverfahrensrecht

Die Digitalisierung hat – das kann man ohne Zweifel behaupten – mittlerweile alle Lebensbereiche der Menschen erfasst und verändert. Die Geschwindigkeit der Entwicklung von Datenverarbeitungs- und Datenübertragungstechnologie ist beeindruckend. „Neue“ Technologien können innerhalb weniger Jahre wieder veraltet, aus der Mode gekommen oder technisch erneut vollkommen umgestaltet sein. Dies betrifft nicht nur Hardwarekomponenten wie Prozessoren, Bildschirmtechnologien oder Übertragungsleitungen, sondern auch ganze Technologiekonzepte. So hat sich die Nutzung des Internets innerhalb relativ kurzer Zeit von einer reinen Kommunikationsinfrastruktur über die bloße Rezeption von Informationen von Internetseiten und Newslettern zu einer umfassenden Parallelrealität mit Teilhabe und Teilnahmemöglichkeiten für (fast) jedermann entwickelt (sog. user generated content oder Web 2.0).

Disruptive Technologien und Konzepte wie Suchmaschinen, Smartphones, soziale Medien, Machine Learning bzw. sog. künstliche Intelligenz (KI) und das sog. Internet of Things (IoT) bringen vollkommen neue Geschäftsmodelle hervor und verändern das Arbeits- und Freizeitleben von (fast) allen Menschen. Auch Kriminelle machen sich die neuen Technologien zunutze, um Straftaten zu begehen. Teilweise werden neue digitale Technologien lediglich als Werkzeuge genutzt, um bekannte Straftaten „effektiver“ zu begehen, z.B. die Nutzung moderner Telekommunikations- und Verschlüsselungstechnologie durch die Organisierte Kriminalität zur Abwicklung von Geschäften in der „Realwelt“.¹ In anderen Fällen ermöglicht die neue Technik die Begehung völlig neuer Arten von Straftaten oder zumindest die Neugestaltung der Begehungsweise von Straftaten. Besonders deutlich und prominent ist dies etwa beim Handel mit illegalen Gütern und Dienstleistungen im sog. Darknet² und der Verwendung von Kryptotrojanern zur Verschlüsselung von

¹ Siehe etwa zum sog. EncroChat-Verfahren: OLG Hamburg BeckRS 2021, 2226; OLG Schleswig NStZ 2021, 693; LG Berlin NStZ 2021, 696; KG MMR 2021, 917; *Singelstein/Derin* NStZ 2021, 449.

² Umfassend hierzu *Wüst*, Die Underground Economy des Darknets – Die Strafbarkeit des Betreibens „illegaler“ Handelsplattformen, Berlin 2022; siehe auch bereits *Bachmann/Arslan* NZWiSt 2019, 241; *Bäcker/Golla* VerfBlog, 2019/3/21; *Bartl/Moßbrucker/Rückert*, Angriff auf die Anonymität im Internet, https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Dokumente/Internetfreiheit/20190630_Darknet_Paragraf_StN-Bartl-Mossbrucker-Rueckert.pdf; *Beck/Nussbaum* HRRS 2020, 112; *Ceffinato* JuS 2017, 403; *ders.* ZRP 2019, 161; *Gercke* ZUM

Daten und Kryptowährungen als Zahlungsmittel bzw. als erpresstes Lösegeld in den sog. Ransomware-Fällen.³

Für die Strafverfolgung besonders misslich ist dabei der zunehmende Einsatz von Verschleierungs- und Anti-Forensik-Methoden durch Kriminelle, um einer Entdeckung oder zumindest einer Überführung zu entgehen. Neben moderner Verschlüsselungstechnologie sind hier auch Methoden der Identitätsverschleierung und gezielte Anti-Forensik-Maßnahmen, wie versteckte Speicherpartitionen oder automatische Datenvernichtung, zu nennen.

Die Durchdringung aller Lebensbereiche durch digitale Technologien erzeugt auf der anderen Seite eine nie zuvor dagewesene Menge an Informationen über die Aktivitäten und das Leben der Bürger*innen in digitaler Form. Die Daten entstehen – in vielen Fällen ohne „aktuelles“ Bewusstsein der Nutzer*innen – durch die Nutzung digitaler Technologien und werden in vielen Fällen von den Anbieter*innen der jeweiligen Technologien (wie Telekommunikations- und Mediendienstanbietern, aber auch den Herstellern und Betreibern von IoT-Geräten) erhoben, verarbeitet, gespeichert und mit anderen Unternehmen geteilt. Doch auch die Bürger*innen selbst verarbeiten, speichern und teilen Daten über sich selbst und andere in digitalen Terminkalendern, Notizen, Social Media Accounts, elektronischen Dokumenten, Bildern, Videos und Aktivitätenprotokollen (z. B. mittels sog. Wearables wie Fitness Trackern und Navigationsgeräten). Dies führt zu einer riesigen Menge an (prinzipiell) verfügbaren Daten mit Informationen über zahlreiche Aktivitäten der Bürger*innen. Diese Daten sind in vielen Fällen von Interesse für die Strafverfolgungsbehörden und können zur Aufklärung von Straftaten beitragen. Die Datenmengen, die in einem Strafverfahren hierbei verfahrensrelevante Informationen enthalten können, sind mittlerweile oft so groß geworden, dass die Strafverfolgungsbehörden auf den Einsatz von moderner Datenerhebungs- und Datenverarbeitungstechnologie bis hin zu Machine Learning Tools und künstlicher Intelligenz angewiesen sind.

Die Bedeutung von digitalen Daten als Spurenansatz und Beweismittel im Strafverfahren hat aufgrund der oben genannten Phänomene bereit spürbar zugenommen, in den kommenden Jahren und Jahrzehnten wird sich kaum mehr ein (über Bagatelldelikte hinausgehendes) Strafverfahren finden lassen, in dem digitale Daten nicht in irgendeiner Weise – und sei es nur als erster Spurenansatz – zur Aufklärung beigetragen haben.⁴ Dies gilt dabei nicht nur für die Delikte der sog. Cyberkrimi-

2019, 798; *Gerhold* ZRP 2021, 44; *Greco* ZIS 2019, 435; *Kubicjel*, Augsburger Papier zur Kriminalpolitik 1/2019; *Kubicjel/Mennemann*, jurisPR-StrafR 8/2019 Anm. 1; *Kusche* JZ 2021, 27; *Oehmichen/Weißenberger* KriPoz 2019, 174; *Rückert* Politische Studien Bd. 69 (2018 Mai/Juni), 479, S. 12; *ders.* StV 2019, I; *ders.* LTO v. 15.03.2019; *Safferling/Rückert* Analysen & Argumente 291 (2018); *Zöllner* LTO v. 11.03.2021; *ders.* KriPoz 2019, 274.

³ *Europol* IOCTA 2021, S. 14 ff. und 20 ff.; *Beukelmann* NJW-Spezial 2017, 376; *Vogelsang/Möllers* jM 2016, 381; *Kreikemeyer* Kriminalistik 2018, 627; *Ceffinato* NZWiSt 2016, 464 (466 f.); *Herzog/Hoch* StV 2019, 412 (414); Überblick bei *Rückert* in Maume/Maute (Hrsg.), HdB Kryptowerte, § 20 Rn. 7 f.

⁴ *Momsen/Hercher* Digitale Beweismittel im Strafprozess: Eignung, Gewinnung, Verwer-

nalität, sondern auch für Delikte der „Realwelt“ und des täglichen Lebens. Einige Ermittlungsmaßnahmen, die digitale Daten erheben und verarbeiten, gehören mittlerweile zum „Standardrepertoire“ der Strafverfolgungsbehörden. Hierzu zählen etwa Maßnahmen der Telekommunikationsüberwachung nach § 100a StPO, die Abfrage von Verkehrs-, Bestands- und Nutzungsdaten nach §§ 100g, 100j, 100k StPO, der Einsatz des sog. IMSI-Catchers nach § 100i StPO und die Funkzellenabfrage nach § 100g Abs. 3 StPO. Es lassen sich darüber hinaus bereits jetzt spektakuläre Beispielfälle nennen, in denen digitale Daten als Beweismittel in einem Strafverfahren wegen „Realwelt“-Delikten im Wege „kreativer“ Datenerhebung und Datenverarbeitung herangezogen wurden: So wurde ein Ehemann in Griechenland des Mordes an seiner Ehefrau überführt, weil die Daten eines sog. Fitness Trackers den von ihm dargestellten Geschehensablauf widerlegten.⁵ Das Landgericht Regensburg verurteilte unlängst einen Mann wegen Totschlags, dem es die Tötung aufgrund der Aufnahmen eines Sprach- und Heimassistenzsystems nachweisen konnte.⁶ Mehrere Verfahren wegen Terrorismusstraftaten stützen sich auf die Auswertung von Chatdateien aus Messengerdiensten (wie etwa WhatsApp); teilweise wurden diese Daten im Wege des sog. Account-Clonings erlangt.⁷

Die Bedeutungszunahme von digitalen Daten als Spurenansatz und Beweismittel stellt das gesamte Strafverfahrensrecht vor neue Herausforderungen. Die oftmals für eine rein „analoge“ Welt konzipierten Normen der StPO müssen auf „digitale“ Sachverhalte angewendet werden. Besonders relevant erscheinen dabei zwei Problemkreise in unterschiedlichen Stadien des Strafverfahrens. Zum einen stellt sich die Frage, ob das strafprozessuale Instrumentarium der Ermittlungsbefugnisse zur Datenerhebung und Datenverarbeitung im Ermittlungsverfahren hinreichend ausgestaltet ist, um alle praxisrelevanten Arten der strafprozessualen Dateneingriffe zur Beweisdatengewinnung abzudecken und gleichzeitig die verfassungs- und europarechtlichen Grenzen einzuhalten. Zum anderen muss die Strafprozessordnung Lösungen für den Umgang mit digitalen Daten als Beweismittel in der Hauptverhandlung bereithalten. Digitale Daten weisen im Vergleich zu anderen Beweismitteln einige spezifische Besonderheiten – wie etwa ihre Flüchtigkeit und („spurenlose“) Manipulierbarkeit – auf, die im Beweisrecht der Strafprozessordnung berücksichtigt werden müssen. Besondere Probleme stellen sich diesbezüglich auch hinsichtlich der Verwendung von Ergebnissen von komplexen Datenverarbeitungsvorgängen als Beweismittel. Soweit hierfür auf sog. statistische oder sogar selbstlernende Methoden der Datenverarbeitung („KI“) zurückgegriffen wird, muss sich das Tatgericht mit der Zuverlässigkeit und Nachvollziehbarkeit dieser Methoden

tung, Revisibilität, Beitrag zum 37. Strafverteidigertag, Freiburg 2013, S. 173 (S. 175); *Momsen*, FS Beulke, S. 871 (873 ff.).

⁵ <https://www.stern.de/panorama/stern-crime/griechenland--smartwatch-enthuehlt-luegen--ehemann-gesteht-mord-30577726.html> (Stand: 29.12.2021).

⁶ <https://www.tagesschau.de/investigativ/wdr/ermittlungen-digitalisierung-101.html> (Stand: 29.12.2021).

⁷ Siehe hierzu BGH BeckRS 2019, 2677; BGH BeckRS 2020, 49703.

auseinandersetzen, wenn es deren Ergebnisse als Beweismittel verwenden will. Bei den Problemkreisen widmet sich die nachfolgende Untersuchung.

I. Allgemeingültige Vorgaben und Leitlinien für die Schaffung und Anwendung strafprozessualer Dateneingriffsbefugnisse zur Beweisdatengewinnung

Wollen die Strafverfolgungsbehörden „vor der Lage bleiben“ bzw. – wie es *Jürgen Gause* vor einigen Jahren auf dem Erlanger Cybercrime Tag ausgedrückt hat – „die Lage nicht vollständig aus dem Blick verlieren“,⁸ müssen sie sowohl Zugang zu den o.g. Datenbeständen erhalten als auch moderne Technologien zu deren Erhebung und Verwertung einsetzen.

Das Legalitätsprinzip (§ 152 Abs. 2 StPO) und die Aufklärungspflicht bzw. die Pflicht zur Erforschung der materiellen Wahrheit (§ 244 Abs. 2 StPO), verfassungsrechtlich abgesichert durch den sog. staatlichen Straf(verfolgungs-)anspruch⁹, geraten angesichts dieser Gemengelage in besonderem Maße in Konflikt mit dem Datenschutz und den Grund- und Menschenrechten, in denen dieser verankert ist (v. a. Art. 10 GG, Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie Recht auf informationelle Selbstbestimmung jeweils nach Art. 1 Abs. 1 iVm Art. 2 Abs. 1 GG; Art. 8 EMRK, Art. 7, 8 GRC). Die Auflösung dieses Spannungsfeldes bzw. der Ausgleich zwischen Grundrechtseingriff und staatlichem Strafverfolgungsanspruch obliegt nach der Konzeption des Verfassungsrechts (Vorbehalt des Gesetzes und Wesentlichkeitsvorbehalt)¹⁰ vorrangig dem Gesetzgeber. Er muss die notwendigen Eingriffsbefugnisse für Grundrechtseingriffe durch Datenerhebungen- und -verarbeitungen schaffen und ausgestalten.

1. Mangel an gesetzlichen Dateneingriffsbefugnissen

a) Zu eng und zu spät geregelte Eingriffsbefugnisse

Dieser Verpflichtung kommt der Gesetzgeber im Bereich strafprozessualer Dateneingriffe nur bedingt nach. Zwar existieren mit den §§ 100a – 101b StPO zahlreiche und überaus detaillierte Regelungen für die Erhebung verschiedener Datenarten. Einerseits sind diese Regelungen jedoch (auch um dem Grundsatz der Normenklarheit und Bestimmtheit Rechnung zu tragen) teilweise auf erstaunlich eng gefasste Fallkonstellationen zugeschnitten. Zu nennen sind hier beispielhaft die §§ 100a Abs. 1 S. 2, S. 3, 100b StPO, welche ausschließlich den Eingriff in informa-

⁸ Vgl. *Rückert/Wüst* KriPoz 2018, 247 (249 ff.).

⁹ BGHSt 52, 110 = NStZ 2008, 356; BGH NJW 2013, 1827 (1830); Meyer-Goßner/*Schmitt* Einl. Rn. 55a; *Paul* NStZ 2013, 489 (491).

¹⁰ BVerfGE 49, 89 (126 f.); 98, 128 (251); guter Überblick bei v. Münch/Kunig/*Kotzur* Art. 20 Rn. 156 ff. mwN.

tionstechnische Systeme regeln, die in der Praxis seit ihrer Einführung 2017 so gut wie keine Rolle spielen,¹¹ § 100i StPO, der – bis zur allerdings verfassungsrechtlich zweifelhaften Ausdehnung des Anwendungsbereichs der Vorschrift durch den BGH¹² auf die Versendung der Stillen SMS – nahezu ausschließlich den Einsatz des sog. IMSI Catchers regelt(e) und die §§ 100g, 100j und 100k StPO, welche jeweils die Erhebung ganz bestimmter Arten von Daten, die von ganz bestimmten Dienstleistern erhoben werden, regeln. Andererseits sind durch technologische Entwicklungen entstandene und teilweise äußerst praxisrelevante Konstellationen nicht, unzureichend oder in verfassungswidriger Weise geregelt. So hat es der Gesetzgeber über Jahrzehnte hinweg (die erste E-Mail der Welt wurde 1971 versendet,¹³ die erste Mail in Deutschland 1984¹⁴) Rechtsprechung und Wissenschaft überlassen, eine Rechtsgrundlage für die Erhebung des lange Zeit wichtigsten elektronischen Kommunikationsmediums zu „finden“. ¹⁵ In der vor Kurzem erfolgten „Neuregelung“ (in der Sache handelt es sich um eine Verfahrensregelung, welche die Zurückstellung von Benachrichtigungen betrifft) u. a. der „heimlichen E-Mail-Beschlagnahme“ in § 95a StPO wird die in der Wissenschaft über die richtige Rechtsgrundlage geführte Debatte vollständig ignoriert und eine verfassungswidrige Regelung geschaffen (die Regelung erfüllt nicht die Anforderungen des BVerfG an heimliche Eingriffe in das Telekommunikationsgeheimnis und das IT-System-Grundrecht).¹⁶

Auch der praktisch bedeutsame Bereich der Erhebung von sog. Nutzungsdaten iSv § 2 Abs. 2 Nr. 3 TTDSG war bis vor Kurzem nicht geregelt, obwohl die Abfrage der Nutzungsdaten von Telemediendiensteanbietern bereits seit Jahren vielfach durchgeführt wird. In der Praxis wurde sich mit der Anwendung von §§ 161, 163 StPO geholfen,¹⁷ was allerdings angesichts der in vielen Fällen bestehenden sachlichen Nähe von Nutzungs- zu Inhalts- und Verkehrsdaten (§§ 100a, 100b, 100g StPO) mehr als nur zweifelhaft war: In der Regel handelt es sich nicht um einen nur „geringfügigen“ Grundrechtseingriff, wie es für die Anwendung der Ermittlungsgeneralklauseln jedoch notwendig ist.¹⁸ Besonders kurios ist in der Konstellation der Nutzungsdatenabfrage, dass während der langen Zeit der „Nichtregulierung“

¹¹ Bundesamt für Justiz, Übersichten für 2019 Telekommunikationsüberwachung – Anordnungen nach § 100a StPO (korrigierte Fassung), Stand 12.02.2021 und Bundesamt für Justiz, Übersicht Telekommunikationsüberwachung für 2019 (Maßnahmen nach § 100b StPO), korrigierte Fassung, Stand: 19.02.2021.

¹² BGH NStZ 2018, 611 mit ablehnender Anmerkung *Rückert*.

¹³ <https://thenextweb.com/news/the-first-email-was-sent-40-years-ago-this-month> (Stand: 12.07.2021).

¹⁴ <https://web.archive.org/web/20110605072324/http://www.tagesschau.de/inland/email102.html> (Stand: 12.07.2021).

¹⁵ Siehe etwa die „Leitentscheidung“ des BVerfG in NJW 2009, 2431; Überblick über den Meinungsstand der Literatur bei MüKoStPO/*Rückert* § 100a Rn. 96 ff.

¹⁶ Siehe hierzu MüKoStPO/*Rückert* § 100a Rn. 104.

¹⁷ KMR/*Bär* § 100g Rn. 68; *Eckel/Rottmeier* NStZ 2021, 1 (9); zuneigend KK/*Bruns*, 8. Auflage, § 100g Rn. 3; siehe auch BT Drs. 19/17741, 38.

¹⁸ *Karg* DuD 2015, 85 (88); *Warken* NZWiSt 2017, 329 (337); *Bauer*, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 358 f.; MüKoStPO/*Rückert* § 100k Rn. 2.

dieser Maßnahme eine größere praktische Bedeutung zukam, als er in Zukunft der nun geschaffenen Regelung in § 100k StPO zukommen wird. Vor der Änderung des TMG, der Einführung des TTDSG und der Reform des TKG in Umsetzung der Richtlinie 2018/1972/EU zum 1. Dezember 2021 war die Gruppe der Dienstleister, welche Nutzungsdaten (damals noch nach § 15 TMG aF) verarbeitete, viel größer und praktisch bedeutsamer als nach der Reform. Dies betraf vor allem sog. Over-the-top-Dienstleister (OTT), welche zwar Kommunikationsdienste im weiteren Sinne erbrachten, wie z. B. Webmail-Provider, Voice-over-IP-Dienste und Messengerdienste, aber keine Telekommunikationsdienstleister nach § 3 Nr. 24 TKG aF und damit Telemediendienste iSv § 1 TMG waren. Nach der Reform des TKG fallen diese OTT-Dienstleister nun als sog. interpersonelle Telekommunikationsdienste in den Anwendungsbereich des Telekommunikationsrechts gem. § 3 Nr. 61, Nr. 24 TKG und verarbeiten damit keine Nutzungsdaten mehr, sondern jetzt Verkehrsdaten iSv §§ 9, 12 TTDSG. Der Gesetzgeber hat also pünktlich zur Abnahme der praktischen Bedeutung der Nutzungsdatenabfrage eine – im Detail auch verfassungsrechtlich problematische¹⁹ – Befugnisnorm eingeführt.

b) Praktisch bedeutsame, aber unregelte Dateneingriffe

Daneben gibt es zahlreiche Beispiele für bereits von Strafverfolgungsbehörden eingesetzte Ermittlungsmethoden zur Datenerhebung, welche keine eigenständige Regelung in der StPO erfahren haben, obwohl es sich teilweise um erhebliche Grundrechtseingriffe handelt. Hier bemühen sich die Strafverfolgungsbehörden, die Gerichte, soweit sie überhaupt mit diesen Fragen befasst werden, und (allerdings mit bislang zu wenig Beachtung) die Strafrechtswissenschaft darum, eine geeignete Rechtsgrundlage in den Vorschriften der Strafprozessordnung zu finden. Beispielhaft zu nennen sind hier etwa das IP-Catching,²⁰ das IP-Tracking,²¹ das WLAN-Catching,²² die sog. Stille SMS,²³ die Erhebung von Daten aus Cloud-Servern²⁴ und die Erhebung von Daten aus IoT-Geräten²⁵ (v. a. aus Heimassistenzsys-

¹⁹ Details bei MüKoStPO/Rückert § 100k Rn. 5 f.

²⁰ BeckOK StPO/Bär § 100g Rn. 26; Bär NZWiSt 2017, 81 (84); KK/Henrichs/Weingast § 100g Rn. 20; von der Grün, Verdeckte Ermittlungen S. 76 f.; MüKoStPO/Rückert § 100g Rn. 127 ff.

²¹ BGH wistra 2015, 395; zustimmend Meyer-Goßner/Schmitt/Köhler § 100g Rn. 45; Löwe/Rosenberg/Hauck § 100g Rn. 41; HeiKo/Gercke § 100g Rn. 13 aE; Warken NZWiSt 2017, 329 (336); Krause NSTZ 2016, 139; BeckOK StPO/Bär § 100g Rn. 24 f.; Bär NZWiSt 2017, 81 (84); Cef-finato JuS 2019, 337 (342); wohl auch BeckOK StPO/Graf § 100a Rn. 253; MüKoStPO/Rückert § 100g Rn. 124 ff.

²² Ulbrich, Die Überwachung lokaler Funknetzwerke („WLAN-Catching“), S. 226 ff.; MüKoStPO/Rückert § 100b Rn. 25 ff.

²³ BGH NSTZ 2018, 611; Krüger ZJS 2012, 606 (609) mN; Rückert NSTZ 2018, 613; SK-StPO/Wolter/Greco § 100h Rn. 29; Eisenberg/Singelstein NSTZ 2005, 62.

²⁴ Grözinger, Die Überwachung von Cloud-Storage, S. 157 ff.; ders. StV 2019, 406; MüKoStPO/Rückert § 100b Rn. 33 ff.

²⁵ Janovsky/Goger RAW 2019, 99 (101 f.); Marosi/Skobel DÖV 2018, 837 (843 f.); Warken NZWiSt 2017, 329 (335); Heinrich ZIS 2020, 421 (422); MüKoStPO/Rückert § 100a Rn. 131 f.

temen). Auch im Bereich der Massendatenerhebung und -auswertung ist keine nennenswerte Tätigkeit des Gesetzgebers zu beobachten, obwohl OSINT und Data Mining (auch unter Einsatz von Machine Learning Tools und künstlicher Intelligenz) mehr und mehr Einzug in die tägliche Ermittlungsarbeit nehmen²⁶ und das BVerfG vor Kurzem die besondere Eingriffsintensität von Data Mining-Methoden festgestellt hat.²⁷

c) „Kreative“ Rechtsauslegung vor den Schranken des Grundgesetzes

Der Gesetzgeber – so kann ein Zwischenfazit lauten – tut jedenfalls bislang wenig, um strafprozessual „vor die Lage“ zu kommen. Freilich wird es niemals möglich sein, angesichts der langsamen Prozesse demokratischer Gesetzgebung mit der rasanten technischen Entwicklung mitzuhalten. Ob dies jedoch jahrzehntelange Nichtregulierung von Standardmaßnahmen rechtfertigt, steht auf einem anderen Blatt. Die strafprozessuale Praxis weiß sich aufgrund dieser gesetzgeberischen Untätigkeit nicht anders zu helfen, als die von ihr als notwendig empfundenen Ermittlungsmethoden mehr oder weniger „gewaltsam“ unter die in der StPO regulierten Eingriffsbefugnisse zu subsumieren. Nicht selten gerät sie dabei mit dem Wesentlichkeitsvorbehalt, den Grundsätzen der Normenklarheit und Bestimmtheit und/oder der Verhältnismäßigkeit in Konflikt. Ein Beispiel hierfür ist die Subsumtion des Versandes einer sog. Stillen SMS unter § 100i StPO, obwohl der Gesetzgeber selbst davon ausging, dass mit Schaffung des „neuen“ § 100g StPO der Versand Stillen SMS nicht mehr notwendig sein würde²⁸ und die Bundesregierung auf Anfrage §§ 100a, 100b (aF) und 100g StPO als Rechtsgrundlage für die Datenerhebung und §§ 161, 163 StPO als Grundlage für die Versendung nannte.²⁹ Ähnlich verhält es sich beim zweiten Beispiel, der Anwendung der §§ 161, 163 StPO als Grundlage der Nutzungsdatenerhebung bei Telemediendiensten³⁰ bis zur Neuregelung in § 100k StPO (siehe hierzu bereits oben). Aufgrund der Vergleichbarkeit von Nutzungsdaten mit Verkehrsdaten und – teilweise – sogar Inhaltsdaten (z. B. konkret aufgerufene URLs, Eingaben in Formularen und Suchmaschinen), kam eine Anwendung der Ermittlungsgeneralklauseln nie in Betracht – die wesentliche Frage, ob und unter welchen Voraussetzungen mittels einer Nutzungsdatenauskunft in Art. 10 Abs. 1 GG eingegriffen werden darf (siehe zur Frage, welches Grundrecht bei Nutzungsdatenabfragen betroffen ist, noch ausführlich Kapitel 2, III. 1. c) dd), S. 54), musste vom Gesetzgeber beantwortet werden (was nunmehr in § 100k StPO geschehen ist).³¹ Beim heimlichen Zugriff auf LAN- und WLAN-

²⁶ Meyer-Goßner/Schmitt/Köhler § 163 Rn. 28a; Rückert ZStW 129 (2017), 302 ff.

²⁷ BVerfG NVwZ 2021, 226 (233 Rn. 109).

²⁸ BT-Drs. 16/5846, 51.

²⁹ BT-Drs. 17/8544, 17.

³⁰ KMR/Bär § 100g Rn. 68; Eckel/Rottmeier NStZ 2021, 1 (9); zuneigend KK/Bruns, 8. Auflage, § 100g Rn. 3.

³¹ Karg DuD 2015, 85 (88); Warken NZWiSt 2017, 329 (337); Bauer, Soziale Netzwerke und strafprozessuale Ermittlungen, S. 358 f.; MüKoStPO/Rückert § 100k Rn. 2.

Netzwerke (sog. WLAN-Catching) sorgt die vom Gesetzgeber den Gerichten und der Wissenschaft überlassene Ausfüllung des Begriffs der „Telekommunikation“ (§ 100a StPO) und des „informationstechnischen Systems“ für Schwierigkeiten. Wer einen rein technischen Telekommunikationsbegriff zugrunde legt, gelangt hier leicht zu einer Anwendung von § 100a StPO für das heimliche Mitschneiden des Netzwerkverkehrs,³² während andere – unter Verwendung eines an Art. 10 GG angelehnten Telekommunikationsbegriffs – danach differenzieren, ob „nach außen gehender“ Netzwerkverkehr oder Netzwerkverkehr von Nutzer*innen, die nicht gleichzeitig Betreiber*innen des Netzwerks sind, überwacht wird (dann § 100a StPO), während im Übrigen (also bei Überwachung des netzwerkinternen Datenverkehrs des Betreibers des Netzwerks) § 100b StPO zur Anwendung gelangt.³³ Beim Einsatz virtueller verdeckter Ermittler im Internet ist zwar richtigerweise davon auszugehen, dass dieser ebenfalls nach den §§ 110a ff. StPO zulässig ist, weil dies sowohl vom Wortlaut der Vorschrift gedeckt ist als auch die sich grundsätzlich stellenden grundrechtlichen Fragen nicht „wesentlich“ anders sind als beim Einsatz in der Realwelt.³⁴ Allerdings ist unklar, wie im virtuellen Raum „echte“ verdeckte Ermittler von nicht öffentlich ermittelnden Polizeibeamten (noePs) abgegrenzt werden müssen. Auch hier kommt es maßgeblich auf die Intensität des Grundrechtseingriffs an, weil die §§ 161, 163 StPO (Einsatz von noePs) nur zu geringfügigen Grundrechtseingriffen berechtigen.³⁵ Bislang nicht in der StPO vorgesehen ist dagegen die Übernahme von „beschlagnahmen“ Accounts von Tatverdächtigen, um so deren digitale Identität zu übernehmen. Da es sich hierbei um eine wesentlich andere Eingriffsart handelt (Verwendung einer fremden Identität gegen den Willen des Identitätsinhabers statt Verwendung einer erfundenen Identität) muss hierfür eine neue gesetzliche Grundlage geschaffen werden. Ein im IT-Sicherheitsgesetz 2.0-Entwurf (§ 163g StPO-Entwurf) vorgesehener Vorschlag wurde bislang vom Bundestag nicht wieder aufgegriffen.³⁶ Im Rahmen der Anwendung von § 100a StPO ist zwar die Anwendung auf zahlreiche „neue“ Wege der Datenübertragung vom Wortlaut („Telekommunikation“) gedeckt, allerdings stellt sich nicht selten die Frage, ob die Eingriffsschwellen und Schutzmechanismen der §§ 100a, 100d, 100e StPO angesichts der Informationstiefe und -vielfalt, welche sich aus der Erhebung der entsprechenden übertragenen (oder im Fall des Zugriffs auf Webmail-Provider und andere Cloud-Services: zwischenzeitlich ruhenden) Daten ergeben können, ausreichend sind. Mit anderen Worten: Ob die konkrete Anwendung im Einzelfall dem Grundsatz der Verhältnismäßigkeit genügt. Dies betrifft beispielsweise die Überwachung des vollständigen Internetverkehrs (inklusive des

³² *Ulbrich*, Die Überwachung lokaler Funknetzwerke („WLAN-Catching“), S. 226 ff.; *Kleib*, Die strafprozessuale Überwachung der Telekommunikation, S. 115 ff.

³³ Für Details hierzu siehe *MüKoStPO/Rückert* § 100b Rn. 25 ff.

³⁴ *Rückert* in *Maume/Maute* (Hrsg.), *HdB Kryptowerte*, § 23 Rn. 15 ff.

³⁵ Siehe hierzu *Rückert* in *Maume/Maute* (Hrsg.), *HdB Kryptowerte*, § 23 Rn. 18 ff.

³⁶ <https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/> (Stand: 14.07.2021).

Surfverhaltens),³⁷ den heimlichen Zugriff auf vollständige E-Mail-Postfächer bei Webmail-Providern,³⁸ den Zugriff auf Cloud-Server³⁹ (soweit hier nicht – richtigerweise – die Anwendung von § 100b StPO bevorzugt wird⁴⁰) und den Datenverkehr von IoT-Geräten wie Heimassistenten-Systemen.⁴¹ Ein letztes Beispiel, das hier detaillierter dargestellt werden soll (es lassen sich zahlreiche weitere Beispiele finden, um das Problem zu illustrieren genügen jedoch mE die hier genannten), betrifft das sog. IP-Catching, bei dem die Ermittlungsbehörden durch technische Maßnahmen (mit oder ohne Kooperation des Betreibers) die IP-Adressen der Nutzer*innen bestimmter Internetdienstleistungen über einen begrenzten Zeitraum hinweg erheben bzw. protokollieren (in letzter Zeit medial und im politischen Diskurs auch gelegentlich als „Login-Falle“ bezeichnet). Im Regelfall wird im Anschluss eine Bestandsdatenabfrage bei Telekommunikationsdienstleistern nach § 100j StPO durchgeführt, um die Identitäten der Nutzer*innen zu ermitteln.⁴² Unabhängig davon, ob die Rechtsgrundlage für eine solche Maßnahme stets in § 100g StPO⁴³ zu sehen ist oder danach differenziert wird, bei welchem Internetdienstleister (Telekommunikationsdienstleister iSd TKG, dann § 100g StPO, oder Telemediendienstleister iSd TMG, dann § 100k StPO) die Maßnahme durchgeführt wird,⁴⁴ weist das IP-Catching jedenfalls eine sehr große Streubreite auf, da eine Vielzahl von IP-Adressen und damit eine große Menge personenbezogener Daten einer Vielzahl von Nutzer*innen erhoben werden. Die Maßnahme steht damit in sachlicher Nähe zu einer Funkzellenerhebung nach § 100g Abs. 3 StPO. Letztere Vorschrift wird wegen der großen Grundrechtsintensität von der Instanzrechtsprechung eng ausgelegt⁴⁵ und enthält zu Recht strengere Eingriffsschwellen im Vergleich zu § 100g Abs. 1, Abs. 2 und § 100k StPO (wenn auch wohl nicht streng genug⁴⁶). Da § 100g Abs. 3 StPO jedoch eine analogiefeindliche Spezialnorm für Funkzellenabfragen ist, wird von der Literatur eine Anwendung auf das IP-Catching abgelehnt;⁴⁷ wie der *Verfasser* an anderer Stelle dargelegt hat, müssen jedoch Verhältnismäßigkeit und Maßnahmerichtung aufgrund der sachlichen Nähe

³⁷ BVerfG ZD 2017, 132; so nun auch BGHSt 62, 22 = NJW 2017, 2631; ausführlich *Hiéramente* HRRS 2016, 448; aA *Heinrich* ZIS 2020, 421 (422 ff.).

³⁸ BGH BeckRS 2020, 36910; Überblick über den Meinungs- und Streitstand bei MüKoStPO/Rückert § 100a Rn. 96 ff.

³⁹ Löwe/Rosenberg/Hauck § 100a Rn. 85; Bär MMR 2013, 700 (703); siehe auch *Kudlich* GA 2011, 193 (207 f.).

⁴⁰ Ausführliche Begründung bei MüKoStPO/Rückert § 100b Rn. 33.

⁴¹ *Marosi/Skobel* DÖV 2018, 837 (843 f.); offengelassen von *Warken* NZWiSt 2017, 329 (335); aA *Heinrich* ZIS 2020, 421 (422).

⁴² Weitere Details zur technischen Durchführung der Maßnahme bei BeckOK StPO/Bär § 100g Rn. 26; KMR/Bär § 100g Rn. 66; MüKoStPO/Rückert § 100g Rn. 127.

⁴³ So BeckOK StPO/Bär § 100g Rn. 26; Bär NZWiSt 2017, 81 (84); KK/Henrichs/Weingast § 100g Rn. 20.

⁴⁴ Details und Begründung bei MüKoStPO/Rückert § 100g Rn. 128 ff.

⁴⁵ AG Dortmund 06.01.2016 – 701 Gs 18/16, juris; LG Dortmund 23.02.2016 – 36 Qs-121 UJs 60/16-25/16, juris; siehe auch LG Arnsberg 29.04.2019 – 2 Qs – 410 UJs 254/19 – 43/19, juris.

⁴⁶ Zu diesem Problem, vgl. MüKoStPO/Rückert § 100g Rn. 87.

⁴⁷ BeckOK StPO/Bär § 100g Rn. 26.

zur Funkzellenabfrage besonders streng geprüft werden.⁴⁸ Die Anwendung von §§ 100g, 100k StPO steht vor diesem Hintergrund jedenfalls aber auf sehr wackligen Füßen, da der Gesetzgeber die „wesentlichen“ Grundrechtsfragen aufgrund der großen Streubreite eigentlich selbst hätte beantworten müssen.

Noch mehr „alleingelassen“ werden die Rechtsanwender*innen vom Gesetzgeber im Bereich moderner Datenerhebungs- und Datenverarbeitungsmaßnahmen. Ein besonders praxisrelevantes Beispiel sind hier Open Source Intelligence-Maßnahmen (OSINT) und Data Mining-Methoden bzw. die Kombination aus beidem (sog. Forensic Web Mining).⁴⁹ Unter OSINT wird dabei die manuell oder automatisiert (mittels sog. Scraper oder Crawler) durchgeführte Erhebung von öffentlich zugänglichen Daten aus dem Internet (z. B. soziale Medien, Foren, Marktplätze, Webpages etc.) verstanden.⁵⁰ Der Begriff Data Mining fasst dagegen Methoden zusammen, bei denen mit Datenanalyseprogrammen (oftmals auch unter Einsatz von statistischen Methoden und/oder Machine Learning bis hin zu künstlicher Intelligenz) extrem große Datenmengen durchsucht, ausgewertet und mit anderen Daten verknüpft werden.⁵¹ Mangels gesetzgeberischer Regelung werden OSINT-Maßnahmen in der Praxis pauschal auf §§ 161, 163 StPO gestützt. In der Literatur wird dagegen überwiegend danach differenziert, ob die Maßnahme manuell oder automatisiert durchgeführt wird⁵² oder ob die Maßnahme auf die Erhebung von sog. Beweisdaten (also zur Überführung einzelner Tatverdächtiger) oder sog. Rasterdaten (zur Gewinnung eines Kreises von möglichen Tatverdächtigen) abzielt.⁵³ Die Verwendung von Data Mining-Methoden ist in der StPO nicht im Besonderen geregelt. Die §§ 483 ff. StPO regeln lediglich die Datenverarbeitung im Allgemeinen, ohne jedoch im Besonderen auf die Verwendung von Data Mining-Methoden einzugehen. Außerdem entspricht es der zutreffenden hM, dass die §§ 483 ff. StPO gerade nicht auf solche Daten angewendet werden können, die als Beweismittel erhoben und sichergestellt wurden.⁵⁴ §§ 98a und 98c StPO regeln dagegen spezifisch den „maschinellen Abgleich“ von Daten aus unterschiedlichen Quellen (§ 98a StPO) bzw. von Daten, über welche die Strafverfolgungsbehörden bereits verfügen (§ 98c StPO). Allerdings wird in der Literatur zu Recht eingewandt, die voraussetzungslose Norm des § 98c StPO könne nur „geringfügige Grundrechtseingriffe“ rechtfertigen und erfasse nicht das sog. Data Mining.⁵⁵ Außerdem wird – aus demselben Grund – eine Beschränkung der Anwendung von § 98c StPO auf den maschinellen Abgleich von Daten vorgeschlagen, die in demselben Strafverfahren (iSv § 264 StPO) erhoben wurden, zu dessen Aufklärung der maschinelle Abgleich er-

⁴⁸ MüKoStPO/Rückert § 100g Rn. 128 ff.

⁴⁹ Vgl. Rückert ZStW 129 (2017), 302 (327 f.).

⁵⁰ Siehe Grütznert/Jakob, Compliance von A-Z, Stichwort „OSINT“.

⁵¹ Siehe BVerfG NVwZ 2021, 226; Golla NJW 2021, 667.

⁵² KK/Moldenbauer § 163f Rn. 13.

⁵³ Meyer-Goßner/Schmitt/Köhler § 163 Rn. 28a; Rückert ZStW 129 (2017), 302 ff.

⁵⁴ Basar/Hieramente NStZ 2018, 681 (684); OLG Karlsruhe NStZ 2015, 606 (608); OLG Rostock BeckRS 2017, 119395; BeckOK StPO/Wittig § 483 Rn. 1.

⁵⁵ BeckOK StPO/Gerhold § 98c Rn. 11; Körfner DANA 2014, 146 (149).

Stichwortverzeichnis

- Abwägungslehre 223, 270, 528, 541, 545, 556f., 567, 577, 586, 595, 602, 610, 619–621, 623, 627, 747, 786, 816
- Access-Provider 76, 263
- Account Cloning 3, 96, 239f., 467f., 614, 784
- Accuracy 380f., 389–392, 504, 558, 609, 759, 825
- Adversarial Attacks 300, 387, 575
- Ähnlichkeitsanalysen 21, 680
- Akteneinsichtsrecht 25, 28, 291, 297, 383, 416, 698–701, 705, 708f., 711f., 714, 716f., 797f., 825, 701, 703f., 707–712, 714, 716–721, 723f., 726, 799, 807
- Aktenvollständigkeit 547, 725
- Aktenwahrheit 725, 798
- Aktivitätsprofil 322
- akustische Wohnraumüberwachung 229, 319f., 325, 439, 441, 447, 449, 461, 753
- Algorithmus 293, 299, 409, 570
- Amtsaufklärungspflicht 22, 24, 660, 664, 690, 707, 789, 793
- Analogie 66, 469, 491–494, 805
- Analogieverbot 240, 465, 491f.
- Anlasslosigkeit 285, 304f., 310, 336f., 339, 341f.
- Annexkompetenz 11, 475, 507
- anonym 164, 247, 629
- anonymisierte Daten 162, 401
 - Anonymisierung 162f., 246f., 379, 400–402, 460, 504, 533, 552, 588f., 591, 629, 763, 825
- Anti-Forensik-Maßnahmen 2, 25, 123, 413, 700, 710f., 715f., 797
- Anwendungsvorrang 518f., 561f., 649, 774
- Assoziations-Analysen 294, 389
- Auffindewahrscheinlichkeit 29, 238, 313, 392–395, 441–444, 451f., 461, 483, 549, 746, 750, 754f., 759f., 762, 766
- Aufzeichnungsfilter 405–407, 451, 592, 764, 782
- Augenscheinsobjekt 654, 656f., 662, 673
- Auskunftsrechte 122, 168, 524, 542, 646, 741
- Ausreißer-Analysen 21, 294, 389, 680
- Authentizität 23–25, 278, 290, 368f., 376, 626, 665f., 669–674, 699, 702, 756f., 776, 785, 790f.
- automatisierte Kennzeichenerfassung 401
- Automatisierung 43, 143, 286–288, 293, 304, 310, 316, 337, 347, 413, 418, 420, 549, 552, 575, 752, 761
- Begründungspflichten 206, 219, 423, 450–454, 483, 611, 635, 645
- Belehrung 584
- Benachrichtigung 13, 121–125, 127f., 219, 223, 279f., 331, 416, 418f., 425, 530, 542–545, 547, 552, 575, 589f., 744, 762, 765, 775–777, 781
- Berichtigung 280, 400, 483, 524, 547, 552, 557f., 567, 590, 596, 761, 778
- Berufsheimlichkeitsverpflichtung 125, 559, 716
- Beschlagnahme 5, 16, 48f., 64, 141, 143, 151, 176, 178, 186, 193, 195–197, 200, 210, 219, 221f., 229, 234–236, 239, 256, 278f., 283f., 304, 307f., 318–320, 322f., 326–328, 342, 344–346, 348, 351, 402f., 406, 417, 419, 421f., 424, 439f., 444–447, 449f., 461f., 467, 471, 485, 490f., 500f., 526, 534, 560, 579, 582, 591, 603, 626, 692, 753f., 821, 823
- Bestandsdaten 54, 56, 76, 92, 101–103, 108, 113, 211, 248, 255, 259, 262–264, 280, 346f., 351, 417f., 497, 564, 735, 748
- Bestandsdatenabfrage 9, 108, 127, 244, 256f., 337, 344, 347, 421, 438, 450, 485, 490f., 591, 658, 735
 - Bestandsdatenerhebung 284, 346, 448

- Bestandsdatenauskunft 116f., 122, 169, 173f., 217, 251, 257, 280, 319, 332, 346f., 424, 440f., 446, 448f., 462, 642, 754, 802, 809
- Bestimmtheit 4, 7, 11, 30, 114–117, 168, 174, 206, 211–213, 217, 238, 240, 261, 399, 458f., 462, 465, 470, 476, 477f., 482, 496f., 508, 510, 525, 530, 533f., 536, 539f., 568, 599, 637, 741, 745, 747, 766–770, 776f.
- Beurteilungsspielraum 16, 361, 363, 388f., 428f., 438, 755
- Bewegungsprofil 261, 334, 340
- Beweisantrag 660, 720
- Beweisregeln 22, 371, 661, 674
- Beweisverwertungsverbot 223, 388, 541, 545, 556f., 567, 577, 586, 594f., 602, 610, 619–621, 623, 627, 747, 786
- Beweiswürdigung 20, 22, 24–27, 200, 300, 366, 370–375, 377f., 406, 413f., 438f., 454, 456, 583, 610, 653, 660f., 664f., 669–678, 682, 684–691, 694, 696f., 705, 707, 757, 783, 789–796, 815, 819
- Bias 287, 289, 300, 385–388, 414, 438, 575f., 758, 814, 822
- Blackbox 22, 24f., 295–299, 381, 383–385, 416, 504–506, 510, 573, 575, 668, 688f., 691–698, 708, 722, 757f., 772f., 780, 793–796, 817
- Blockchain 345, 379f., 673, 679, 682, 814
- Brute-Force 184, 326, 329, 486

- Carving 405, 597, 663, 817, 823
- Chain of Custody 377
- Chilling Effects 154, 158, 173, 272, 279, 283, 286, 288, 305f., 309, 415, 548, 587, 612
- Chip Off 667
- Cloud 6, 8f., 17, 19, 41f., 44, 51f., 57, 61–72, 74f., 77, 141, 176, 181, 185–190, 195, 208f., 229, 232f., 239f., 273, 319, 321f., 325, 328, 351, 439, 447, 449, 461, 467f., 489, 497, 500f., 613, 665, 708, 729, 731–733, 739f., 753, 802–804, 808f., 814, 817, 823, 825
- Cloud-Anbieter 64, 66, 72, 322
- Cloud-Computing 62f., 66, 68–70, 72, 77, 181, 185, 613, 739
- Cloud-Daten 64, 69, 239, 322, 328, 467
- Cloud-Dienste 66, 208, 731
- Cloud-Dienstleistungen 64, 176, 186f., 731
- Cloud-Nutzer 69, 71
- Cloud-Provider 239, 467
- Cloud-Server 9, 64 - 66, 69–71, 186, 188, 240, 468, 497
- Cloud-Service 67
- Cloud-Speicher 67, 69–71, 141, 186, 229, 232, 319, 322, 439, 447, 449, 461, 489, 500f., 665, 729, 731f., 739, 753, 804
- Cluster-Analysen 21, 292, 294, 389, 680
- Confirmation Bias 385f., 438, 758, 822
- Coppolino*-Standard 674
- Cyberkriminalität 2, 652, 817
- Cyber-Mobbing 466

- Darknet 1, 94, 100, 244, 269, 291, 345, 380, 466, 651, 679, 801, 808, 812f., 819
- Hidden Services 94, 100, 269
- Dark Web Monitor 269, 291, 652, 673, 679
- Data Mining 7, 10f., 21f., 150, 163, 170, 210, 228, 266, 287, 289, 292, 294, 297, 321, 325, 350, 380, 389–391, 407–409, 413, 437, 444, 481, 484, 502–505, 509–512, 517, 570f., 573–575, 592, 613f., 680, 743, 764, 771, 773, 780, 784, 805, 814
- Data Mining-Methoden 7, 10f., 150, 163, 350, 380, 407, 444, 484, 502–505, 509–511, 570, 573–575, 592, 613f., 771, 780, 784
- Data Protection by Default 593, 764
- Data Protection by Design 586, 594, 764, 781
- Datenminimierung 586, 588, 806
- Datenschutzbeauftragter 505
- Datenschutzfolgenabschätzung 224, 612, 784
- Datensicherheit 224, 277, 301, 425, 459, 540, 545f., 550f., 553–556, 763f., 777f., 815
- Daubert*-Standard 674
- DDoS 466
- De-Anonymisierung 162f., 246f., 379, 401f., 629
- Deep Web 94, 99, 269
- deterministische Methoden 21, 349, 378, 409, 608, 679, 757, 792
- Digitalisierung 1, 25f., 40, 141, 147, 153, 174, 207, 376, 500f., 652–654, 657, 663,

- 666, 674, 742, 747, 804, 806, 809f., 815, 819–821
- Diskriminierung 300, 307, 386f., 424, 576, 749, 780, 812
- DNA-Analysen 684, 685
- Dokumentation 23, 198, 290, 377, 548, 552, 666f., 674, 678, 699, 757, 791f.
- Doppeltürmodell 13, 116, 173f., 212, 225, 418, 478, 494, 498, 534, 769
- Doxing 466
- Effet-utile-Grundsatz 521, 610
- Einwilligung 161f., 183, 268, 270, 345, 506, 577–586, 596, 637, 692, 737, 772, 781, 806, 823
- E-Mail 5, 9, 14, 16, 41, 49, 51, 55, 59–63, 66, 68, 72, 76, 78, 83, 85, 98f., 104, 106–108, 127, 137, 139f., 178, 221f., 234–236, 244, 256, 259–261, 263, 269, 281–283, 291, 299, 321, 325–328, 330, 341f., 346, 369, 380, 382, 402–404, 421f., 445, 449, 462, 471, 477, 490, 572, 588f., 655, 663, 679, 683, 731, 744, 804, 821
- E-Mail-Adresse 14, 99, 244, 261, 291, 346, 382, 589, 679, 683
- E-Mail-Beschlagnahme 5, 49, 178, 221f., 234f., 256, 326–328, 402f., 445, 449, 462, 471, 490
- EMRK 4, 20, 25, 30, 224, 282, 288f., 355, 383, 416, 515, 517, 528, 601, 604, 630–632, 639–641, 643, 645, 647f., 650, 685, 699, 702, 711, 727, 774, 782, 786–788, 808, 811, 814, 816, 820, 824
- EncroChat 1, 263
- Endgerät 40, 46–48, 50, 57–60, 69–71, 76, 80–84, 87f., 96f., 108, 111, 141, 182, 185, 188–190, 240, 258, 272, 468, 730, 731–734, 740
- Erfahrungssätze 366f., 371, 373f., 443, 669–671, 675, 677, 680–682, 696, 708, 756f., 792f.
- Ermittlungsgeneralklausel 5, 7, 115, 222f., 230, 249, 409, 418, 449, 468f., 470f., 485, 487, 496, 511, 530, 534, 589, 768, 770, 809
- Fangschaltung 77, 80, 82, 93, 733
- File Carving 823
- Filterung 21, 253, 266, 403–406, 412, 499, 502, 593f.
- Flüchtigkeit 3, 23, 135f., 367f., 665, 670, 756, 790
- formeller Aktenbegriff 719
- freie richterliche Beweiswürdigung 660, 815
- Frye-Standard 674
- Funktionsfähigkeit der Strafrechtspflege 126, 744
- Funkzelle 41f., 44, 106f., 109, 333, 335, 340, 343, 351, 448, 475, 736
- Funkzellenabfrage 3, 10, 319, 327, 336, 340–343, 351, 420f., 440, 446, 449, 462, 490, 493, 505, 509, 592, 602, 754
- Garbage-in-garbage-out 299, 382, 575, 683
- Geeignetheit 115, 200, 225f., 392, 443, 615
- Geheimhaltungswille 134f., 139f., 148, 169, 208, 500, 742
- Geschäftsgeheimnisse 24f., 39, 119, 204, 255, 295, 383, 410f., 414f., 470, 504, 693f., 698, 700, 711, 714, 716, 795, 797
- Gesetzesvorbehalt 114, 238, 240, 465, 470–474, 492, 494, 496f., 508, 568, 570, 573, 580f., 588, 768, 770
- Gesichtserkennung 149, 163, 296, 299, 384, 385, 390f., 517, 572, 576, 695f.
- Gesundheitsdaten 140, 247, 249, 535, 629
- GPS 151, 334, 427, 466, 477
- Ground Truth 380, 391, 680f., 758, 793
- Hash-Funktion 368
- Hash-Summen 376, 546, 552, 592, 668, 671f., 756, 791
- Hashwert 368f., 404
- Hatespeech 466, 805
- Heimlichkeit 15, 108, 121, 128, 158, 200, 206, 219, 231, 235, 277f., 281, 304, 310, 316, 321, 324, 329, 331, 340, 416–418, 420, 447, 748, 752, 762
- Herrschaftsbereich 46–49, 53, 70, 86, 90, 95, 108, 182, 192, 222
- Beherrschbarkeitskriterium 49, 56, 61, 82, 108, 112, 185, 729f., 736, 739f.
- Heuristik 21, 244, 292f., 295, 380, 680–682
- Hörfälle 47, 73, 79, 160, 729, 733f.
- ICCID-Daten 239, 467, 469, 508
- IMSI-Catcher 41, 106f., 109, 122, 343, 405, 446, 475, 489, 592, 728

- Inaugenscheinnahme 656 f., 659, 662, 692
in dubio pro reo 360
informationstechnische Systeme 4, 70, 176,
178, 185, 187 f., 232 f., 486, 497, 739, 822
Inhaltsdaten 7, 12 f., 45, 101, 103, 113, 234,
255–257, 259–261, 265, 332, 337 f., 348,
539, 735
Integrität 4, 19, 23–25, 35, 38 f., 46, 53 f., 58,
67–70, 72 f., 76, 78, 81, 83, 97, 106, 112,
114, 153, 168, 174 f., 177, 181 f., 185,
190–194, 197, 205, 217, 224, 232, 237, 290,
368 f., 376, 489, 507, 545 f., 552, 600, 626,
665 f., 669–674, 699, 702, 704, 728,
739–741, 756 f., 776, 785, 789–791, 804,
810, 820, 825
Internet of Things 1, 42, 95, 180, 466, 729
interpersoneller Telekommunikations-
dienst 6, 262–264, 339
Interpretations-Tools 297 f., 383–385, 694,
696, 796
Intimsphäre 170, 244, 247 f., 250, 253, 256,
259, 264, 319 f., 332, 336 f., 344, 346, 348,
350, 747
IoT 1, 2, 6, 9, 42, 180 f., 240, 325, 422, 466,
468, 500, 729
IP-Adresse 14, 75, 96, 100–104, 106, 108,
113, 127, 244, 256, 263, 341–343, 406, 422,
477, 490 f., 572, 611, 655
– dynamische 102, 104, 113, 260, 289, 422
IP-Catching 6, 9, 106, 122, 127, 239, 319,
327, 341, 440, 449, 459, 462, 467, 485,
490 f., 493, 509, 512, 588, 592, 602, 614,
617, 754, 773, 784
IP-Tracking 6, 14, 44, 107 f., 114, 122, 239,
319, 342 f., 440, 449, 462, 467, 469, 476 f.,
485, 491, 508, 512, 614, 617, 735, 754, 784,
812 f.
ISO/OSI-Modell 50
IT-Forensik 17, 19, 23, 25 f., 247, 253, 288,
290, 367 f., 375–377, 380, 404, 413, 532,
596, 651 f., 656–660, 662, 664–667, 669,
671, 673 f., 679, 681, 688, 696, 708, 757,
759, 789 f., 792, 794, 807, 809, 825
IT-Sicherheit 184, 192, 201, 302, 329, 400,
462, 483, 499, 533, 545 f., 551, 555 f., 590 f.,
637, 749, 761, 777 f., 805
IT-System-Grundrecht 5, 35, 39, 58, 76,
157, 168 f., 174–178, 181–193, 195–198,
200–202, 205, 233, 239, 245, 273, 302,
312, 467, 470, 472 f., 475, 489, 494, 497,
500, 507, 526, 728, 730, 732 f., 737–740,
744, 768
IT-Systeminhaber 325, 327, 331, 333, 338,
340
Kennzeichnung 119 f., 213, 400, 506, 547,
605, 608 f., 746, 761, 772, 779, 784
Kernbereich 15, 130–132, 134–142, 144,
146–148, 203, 207 f., 231, 233, 244, 247,
250, 253 f., 304, 310, 320, 325, 327, 332,
337, 344, 348, 350, 489, 500, 511, 538, 742,
771, 807, 813, 819, 825
– Selbstgespräch 69, 132, 134–136, 141,
208, 324, 742, 811
– Tagebuch 130, 134, 136, 138, 141
– Kernbereichsdaten 13, 133, 142–148, 150,
168 f., 198 f., 209, 222, 318, 323, 330, 332,
336, 346, 349, 400, 477, 482, 499–501, 538,
540, 559, 564, 742 f.
– Kernbereichsregelung 13, 142, 168, 501,
508, 764
– Kernbereichsschutz 129 f., 132, 139–141,
146 f., 149, 169, 198, 207–209, 213, 410,
462, 500 f., 539, 741–743, 750, 761
KI 1, 3, 22, 26, 253, 288, 298 f., 316, 364,
376, 384, 387, 392, 416, 504, 517, 535, 576,
613 f., 651, 684, 689, 694 f., 697 f. 705, 748,
752, 758, 784, 793, 806, 810, 821
Klassifizierung 17, 264, 267, 293, 389, 392,
504, 634, 665, 825
kognitive Dissonanz 388
kriminalistische Erfahrung 374, 443, 757
Kryptowährungen 2, 100, 189, 264, 269,
682, 812
LAN 7, 52–54, 181–184, 191, 730, 811
Legalitätsprinzip 4, 362, 364, 388, 805 f.
Legitimer Zweck 225
Lesbarkeit 267, 275, 304, 310, 316, 319, 325,
350, 420, 748, 751
Letzte Meile 52
Live-Sicherung 667, 671
Log-Dateien 341, 404
Löschung 49, 120 f., 130, 144–146, 148, 166,
208 f., 266 f., 274, 275, 279 f., 373, 400,
406 f., 412, 425, 483, 499, 504, 506, 524,
529, 533, 542, 547 f., 552, 557 f., 560–567,

- 588–592, 594, 597, 619f., 629, 738, 742f.,
746, 761, 772, 778f.
- Machine Learning 1, 2, 7, 10, 229, 300, 324,
380–382, 386f., 389–391, 576, 684, 748,
758, 793, 795, 811, 814f., 817f., 823, 825
– Deep Learning 229
- Manipulation 120, 172, 200, 370, 607, 655f.,
660, 662f., 665, 668, 670f.
- Manipulierbarkeit 3, 23, 25, 368, 656, 665,
671, 756, 790
- maschinelles Lernen 297, 382, 576, 683,
694, 812
- Massenkommunikation 85–88, 94f., 113,
734
- Maßnahmedressaten 258, 344, 394, 398,
402, 426, 440, 459, 483, 567, 635, 637, 645,
762f.
- Maßnahmedauer 221, 286, 310, 317, 320,
347, 445, 458, 635, 752, 763, 766
- Menschenwürde 146, 149, 173, 312
– Menschenwürdegarantie 35, 311
- Messengerdienste 3, 6, 41, 49, 59, 83, 85, 94,
96–98, 110, 133, 139f., 147, 208, 229, 240,
249, 263, 325f., 328, 404, 467f., 655, 730,
734
- Metadaten 28, 253, 325, 655, 657, 662, 812
- Mobilfunkforensik 667, 688, 817
- Nachrichtenmittler 306, 325, 327, 333, 338,
340, 351, 402, 441
- Nachvollziehbarkeit 3, 16, 22, 24, 211, 228,
287f., 291, 295–297, 299, 314–316, 322,
337, 346, 349, 372, 375, 380f., 383, 395,
413–416, 460, 505, 517, 609, 611, 666,
694f., 697, 699, 748, 752, 757f., 760, 765,
767
- nemo tenetur 160, 282, 507, 582, 584, 600f.,
782
- Netzwerk-Sniffer 184, 329, 350
- Nichtverkettung 460, 547, 552, 589
- Normenklarheit und Bestimmtheit 4, 7, 11,
30, 114–117, 168, 174, 206, 211–213, 217,
238, 240, 261, 399, 458f., 462, 465, 470,
476–478, 482, 496f., 508, 510, 525, 530,
533f., 536, 539f., 568, 599, 637, 741, 745,
747, 766, 768–770, 776f.
– Bestimmtheitsgebot 33
- nullum crimen-Grundsatz 491
- Nutzungsdaten 3, 5–7, 12, 54–56, 77, 96,
101, 105, 113, 211, 222, 234, 255–257,
259–262, 325–327, 330–332, 341f., 346,
422, 439f., 445, 448f., 461f., 478, 485, 487,
493, 497, 508–510, 512, 539, 730, 735, 754,
773, 811
– Nutzungsdatenabfrage 5f., 12f., 55, 257,
260, 330f., 422, 446, 487, 512
– Nutzungsdatenerhebung 7, 11, 234, 239,
256, 265, 331, 338, 342, 412, 422, 448, 460,
467, 469
- öffentlich zugängliche Daten 157, 159, 267,
303, 316, 318, 349, 498, 509, 737, 751
- Online-Durchsuchung 11, 17, 19, 48, 64,
70, 75f., 108, 120, 122, 133, 143, 146f.,
149, 151f., 156, 183, 185f., 190, 193–199,
203, 209f., 218–221, 232–235, 239, 251,
254, 281, 301f., 318–326, 328f., 348, 350,
405, 409, 421, 427, 438f., 441, 444–447,
449, 451, 461, 466f., 469f., 473, 485, 490,
499, 505, 512, 526, 591, 599f., 614, 652,
699, 705, 749, 753, 803–805, 807–809, 818,
822
- OSINT 7, 10f., 123, 163, 178, 221, 223, 230,
239, 285, 291, 319, 342, 345f., 349f., 380,
401, 411, 417f., 440, 444, 449, 462, 467,
469, 485, 491, 502, 509f., 512, 530f., 534,
560, 589, 602, 613f., 679, 754, 773, 784,
819
– OSINT-Maßnahmen 10f., 221, 239, 319,
342, 345f., 349f., 411, 417, 440, 444, 449,
462, 467, 469, 485, 491, 502, 509f., 512,
530f., 534, 560, 602, 613f., 754, 773, 784
- OTT 6, 263f., 326
- OTT-Dienstleister 6, 263f.
- Parlamentsvorbehalt 479
- Passwort 85, 87, 94, 99f., 104, 258, 260,
276f., 348, 422, 486, 733
- Personenbezug 45, 104, 162–164, 244–247,
258, 262, 266, 287, 302, 310f., 318f.,
321–323, 325, 332, 336f., 344, 347, 350,
401, 421, 484, 489, 504, 506, 533, 551, 772,
810
- Persönlichkeitsprofil 153, 170, 206, 209,
250f., 254, 315, 321, 559, 743, 747, 751
– Big-Five-Modell 171f., 210, 251
- Post-Mortem-Sicherung 667

- Precision 389–392, 504, 558, 609, 759
- Privatsphäre 146, 177, 193f., 244, 247, 249f., 253f., 304, 315, 320, 323–325, 327, 330, 332, 337, 344, 346, 348, 349f., 421, 489, 538, 750f., 801, 803
- Profiling 576
- Protokollierung 552, 591f., 595–600, 602, 782
- prozessuale Waffengleichheit 698, 722, 725, 796, 820
- Pseudonymisierung 163, 400–402, 460, 533, 540, 550–552, 588f., 591, 603, 763
- Quellcode 24, 27, 296, 298, 692f., 700f., 708f., 716, 725, 748, 795, 797–799
- Quellen-TKÜ 57f., 70, 81, 83, 87, 95, 108, 122, 182, 192, 197, 219, 233f., 239, 281, 302, 319, 326, 328, 405, 449, 461, 466f., 469, 473, 475, 486, 490, 499, 512, 599f., 614, 652, 699, 705, 729f., 734, 740, 754, 804f., 807, 818f.
- Ransomware 2, 245, 466, 572, 824
- Rasterfahndung 11, 164, 170, 284f., 318f., 327, 336f., 401, 411, 440, 444, 449, 462, 490, 509, 592, 602, 754, 812
- Recall 389–392, 505, 558, 609, 759
- Recht auf Achtung des Familien- und Privatlebens 224
- Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme 4, 39, 68f., 72, 78, 83, 97, 112, 168, 174, 224
- Recht auf informationelle Selbstbestimmung 4, 19, 38f., 56, 63, 68f., 77, 80, 103–105, 109, 114, 116, 118, 153, 177f., 193, 197, 217, 224, 237, 489
- Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme 19, 38, 53, 217, 237
- Rechtsschutz 120, 124, 127f., 149, 226, 277, 279, 323, 344, 419, 450, 471, 575, 744
- Rechtsstaatsprinzip 160, 216, 354
- relativ mildestes Mittel 446, 527, 531
- Reproduzierbarkeit 298, 376f., 379, 384, 757, 808
- Reverse Engineering 414, 692f., 708, 724, 795, 797
- Richtervorbehalt 128f., 198, 209, 211, 219–221, 227, 278, 416, 459, 480, 484, 637, 741, 743, 762, 814
- Richtigkeitsgewähr 22, 287–289, 293, 295f., 298, 300, 307, 316f., 322, 337, 346, 349, 369, 375, 377f., 380, 383–385, 387, 413f., 416, 423, 458, 460, 502, 504f., 675, 678, 695f., 748f., 752f., 757, 761f., 765
- Richtigkeitswahrscheinlichkeit 21f., 24, 287–296, 298–300, 362–364, 371, 373f., 389, 391, 395, 423, 463, 517, 558, 572, 609, 677f., 681–683, 685, 687–691, 694–698, 702, 705–708, 748, 756–760, 776, 778, 780, 792–796
- Richtlinie 2016/680/EU 20, 30, 154, 224f., 245, 387, 459, 499, 515, 518f., 521f., 527, 528f., 553, 562, 628, 631–633, 635–639, 642f., 645, 647–649, 727, 773f., 786f., 817
- richtlinienkonforme Auslegung 20, 546, 602, 610, 612, 617, 621, 775
- Risikoabschätzung 548, 549, 554f., 587, 778, 781
- Rundumüberwachung 133, 149f., 206f., 210, 213, 309f., 400, 445, 447, 458, 462, 483, 501, 511, 741, 743, 745, 761, 765f., 771
- Sachverständige 22, 24, 26, 294, 383, 659, 684, 689f., 692, 694f., 698, 708, 715
- Schuldprinzip 355
- selbstlernende Methoden 3, 22, 296, 337, 506, 608, 678, 722, 771
- Selbstreflexion 136, 208f., 742
- sensitive Daten 536, 540, 575, 780
- SIM-Karte 48, 104, 106
- Smartphone 1, 42, 49, 133, 137, 140, 180f., 183, 191, 197, 208, 228f., 232, 239, 254, 273, 320, 328, 333, 370, 421, 466f., 469, 477, 489, 500, 507, 512, 655f., 658, 667f., 742, 772f., 801, 816, 823
- Soziale Medien 1, 2, 10, 85, 94, 133, 140, 161, 250, 325, 734
- Sozialsphäre 244, 247f., 315, 324, 350, 538, 564, 751
- Spähprogramm 58f., 192, 194, 200, 226, 281, 328
- Sperrung 120, 281, 400, 425, 483, 548, 552, 746, 761, 779
- Sphärentheorie 15, 231, 247–250, 258
- Sprachassistenzsysteme 42, 466

- Standard-Datenschutzmodell 550f., 588f., 592, 616
- Stand der Technik 120, 143, 162, 209, 245, 369, 401, 406, 458, 484, 504, 506, 549–551, 555f., 576, 587–589, 591, 594, 666, 743, 756, 759, 772, 776, 778, 781
- Standortdaten 55, 109, 155, 253–257, 259, 326, 332–335, 339f., 342, 344, 448f., 461, 473, 475, 539, 628, 655
- statistische Methoden 21, 266, 294, 316, 379, 409, 680, 722, 748, 752, 757, 792
- Stigmatisierung 317, 424, 749, 753, 766
- Stille SMS 6, 107f., 114, 122, 239, 319, 335, 440, 446, 459, 467, 470, 474, 508, 512, 735, 754, 806, 812
- Straftatenkatalog 118, 151, 220, 257, 398, 427, 430, 436, 480, 483, 504–506, 510, 771–773
- Strafverfolgungsanspruch 4, 15, 204, 211, 223, 230, 354, 393f., 399, 438, 444, 452, 457, 479, 483, 490, 538, 541, 556, 755, 786
- Streubreite 9f., 15, 201, 231, 283–285, 287, 304, 307, 309f., 316, 318, 321, 324f., 327, 330, 332f., 336f., 339–342, 344f., 347, 349–351, 406, 411, 413, 417, 420, 442, 444, 461, 482, 484, 488, 503f., 509, 549, 592, 602, 744, 748f., 752, 761, 765f.
- Subsidiaritätsklausel 11, 216, 220, 232, 446f., 449, 462
- Subsidiaritätsprinzip 639
- Suchmaschine 87, 268, 732
- Tatverdacht 14, 118f., 124, 163, 200f., 206, 231, 244f., 285, 293, 295, 305f., 355, 358f., 362, 364f., 367, 371, 374–377, 379–381, 383–385, 387f., 392, 394, 398, 408f., 429, 438, 441f., 452, 480, 505, 536, 570–572, 606, 611, 629, 658, 718, 758–760
- Anfangsverdacht 14, 227, 231, 303, 358f., 361, 364f., 371, 379, 408, 439, 536, 741, 766, 809, 811
 - dringender Tatverdacht 231, 571
 - hinreichender Tatverdacht 231, 358
 - qualifizierter Tatverdacht 231
 - Tatsachenbasis 14, 152, 359, 364–366, 368f., 388f., 571, 610f., 756, 783
 - Tatsachengrundlage 152, 231, 365, 368, 453, 456, 567, 605, 661, 669f., 686, 756, 790
 - Verdachtsgrad 152, 227, 358f., 361, 363, 370, 373, 378, 397, 567, 756, 758
- TCP/IP-Modell 50
- Telekommunikation 8, 12, 40, 50f., 62, 65, 83, 103, 105, 124, 137, 142, 146f., 178, 181, 183, 201, 239, 247, 259–261, 263, 277, 284, 338–340, 404, 447, 466f., 480, 486f., 497, 728, 731, 733, 735f., 739, 801, 803, 810, 812, 822
- Telekommunikationsanbieter 47, 52, 102, 117, 326, 332, 339, 478
 - Telekommunikationsdienst 6, 147, 262–264, 326, 339, 341, 343, 486
 - Telekommunikationsdienstleister 6, 9, 43, 117, 424, 487, 551
- Telekommunikationsgeheimnis 5, 19, 35, 38–40, 43f., 46f., 53, 55, 64, 70–73, 80, 82–84, 101, 105, 113, 151, 153, 160, 183, 186, 188, 192, 198, 201f., 205f., 217, 221, 224, 237, 245, 333, 344, 470–473, 475, 728, 732f., 735f., 739f., 744
- Fernmeldegeheimnis 35, 39, 43, 48, 56, 59, 63, 67f., 71, 74–80, 82, 84f., 86, 89–91, 93, 95f., 97–101, 103–106, 108–114, 122, 128, 729, 809, 825
- Telekommunikationsüberwachung 3, 5, 15, 48f., 59–61, 68, 73, 75f., 93, 96, 127, 131f., 142f., 146f., 151, 164, 188, 191f., 195, 200, 226, 231, 233, 236, 248, 280f., 319f., 325f., 337f., 347f., 402, 405, 411, 421, 424, 427, 438, 445–448, 450f., 473, 480, 485f., 534, 575, 658, 804, 809, 813, 818, 820
- Telemedienanbieter 54, 101, 331, 419
- Telemediendienst 234, 260, 262, 330, 332, 341f., 422
- Telemediendienstanbieter 5, 55, 104f., 222, 264, 424, 534
- Telemediendienste 6, 260, 330, 346, 422, 802
- Telemediendienstleister 9, 116f., 424
- Treu und Glauben 530, 588f., 775
- Underground Economy 1, 110, 466, 819f., 825
- Untersuchungshaft 27, 215, 307, 358, 360, 363, 371, 454, 492
- Urkunde 654f., 659, 673

- Verbindungsdaten 42, 47, 102
 Verdunkelung 711
 Verfahrensfairness 25, 160, 660, 687, 714
 Verkehrsdaten 5, 6f., 12, 48, 55f., 61, 76, 101, 104f., 107–109, 113, 117, 211, 234, 255–257, 259f., 265f., 277, 280, 284, 325, 332f., 335, 337–341, 343f., 406, 445, 448, 487, 497, 509, 534, 539, 542, 655, 735, 773, 802
 – Verkehrsdatenabfrage 12f., 107, 256, 260, 331, 333, 421f., 424, 443, 473, 485, 491
 – Verkehrsdatenerhebung 13, 108, 226, 265, 319, 335, 337f., 342f., 351, 427, 446, 448, 450, 475
 Verschlüsselung 1, 51, 58, 60, 86f., 91, 110–112, 114, 182, 188, 190, 226, 275–277, 316, 321, 325f., 328, 330, 333, 337, 347, 350, 466, 507, 540, 550–552, 591, 614, 736, 739, 748, 751, 812, 815, 824
 Vertraulichkeitserwartung 42f., 73, 75, 101, 134, 139f., 148, 159, 169, 180, 249, 259f., 267, 270f., 273–276, 318, 498, 500, 732, 734, 737
 Vertraulichkeitsinteresse 208, 249f., 255, 258–260, 266, 309, 311, 338, 716, 742, 747
 Verwahrungskette 666
 virtueller verdeckter Ermittler 8, 239, 467, 512, 773
 Voice-over-IP 6, 49, 58, 73, 78, 92, 94, 139, 195f., 208, 263, 324–326, 730
 – Voice-over-IP-Dienste 6
 – Voice-over-IP-Telefonie 49, 58, 73, 78, 196, 324, 730
 Vorbehalt des Gesetzes 4, 167, 470f., 479, 485, 530, 568, 768
 Vorfilterung 166, 222, 253, 266, 392, 403, 407, 484, 761
 Vorratsdatenspeicherung 47, 49, 55, 77, 117, 121, 173, 211, 248, 256, 301, 339, 400, 467, 487, 630f., 730, 807, 818f., 826
 VPN 53f., 187, 189, 341, 806
 Webmail-Provider 6, 8, 151, 181, 187, 221, 234, 239f., 263, 279, 326f., 422, 439, 467f., 471, 485, 490, 731, 739, 754
 Wechselwirkungslehre 152
 Wesentlichkeitstheorie 30, 167, 238, 465, 495f., 568, 768–770
 – Wesentlichkeitsvorbehalt 4, 7, 484, 496, 770
 Wiederholbarkeit 23, 290, 376f., 379, 414, 674, 678, 708, 757, 791f.
 WLAN 6–8, 17, 19, 50–54, 181–184, 191, 239, 319, 326, 328f., 346, 349f., 405, 417, 439f., 449, 459, 461f., 467, 485f., 491, 614, 729f., 754, 784, 824
 WLAN-Catching 6, 8, 17, 19, 52f., 181, 184, 239, 319, 326, 328f., 346, 349f., 405, 417, 439f., 449, 459, 461f., 467, 486, 491, 614, 729, 754, 784, 824
 Write-Blocker 369, 667f.
 Zeitstempel 75, 253, 260, 404, 422, 599, 655, 657
 Zertifizierung 415, 507, 772
 Zeugen 131, 493, 602, 654f., 664, 673, 692, 695
 Zielwahlsuche 164, 239, 467, 487f.
 Zitiergebot 33, 471–474, 494, 768
 Zugangsdaten 12, 62, 78, 104f., 113, 176, 186, 255–258, 264f., 311, 348, 497, 735, 748
 Zuverlässigkeit 3, 22, 24, 171, 210, 251, 293f., 296, 298, 366–368, 375, 380–382, 384f., 389, 391, 438, 507, 623, 625f., 672, 683f., 689, 695, 697, 702, 705, 756f., 772, 785
 Zweckänderung 118–120, 168, 198, 212, 224, 408, 458f., 522, 524, 527–529, 540, 547, 566, 579, 585, 589, 600, 623, 636f., 713, 741, 746, 763, 775
 Zweckbindung 18, 117, 119f., 168, 198, 206, 399f., 408, 458f., 483, 525, 547, 589, 600, 623, 627, 637, 724, 741, 761, 763, 806