Christian Rückert

Digitale Daten als Beweismittel im Strafverfahren

[Digital Data as Evidence in Criminal Proceedings.]

2023. XXXVI, 834 pages. JusPoen 24

ISBN 978-3-16-162216-8
cloth 164,00 €

ISBN 978-3-16-162217-5
eBook PDF 0,00 €

Published in German.
Due to increasing digitalization, law enforcement agencies and criminal courts have access to more and more accurate information in digital form. Christian Rückert examines which standards arise from constitutional, European and criminal procedural law for the collection, use and evaluation of digital data as evidence in criminal proceedings.

Survey of contents

Kapitel 1 – Die Erhebung und Verwertung digitaler Beweismitteldaten als Herausforderung für das Strafverfahrensrecht
I. Allgemeingültige Vorgaben und Leitlinien für die Schaffung und Anwendung strafprozessualer Dateneingriffsbefugnisse zur Beweisdatengewinnung
II. Digitale Daten und Datenanalyse als Beweismittel in der Hauptverhandlung
III. Gang der Darstellung

Kapitel 2 – Analyse der verfassungsgerichtlichen Rechtsprechung zur Rechtfertigung von Eingriffen in die Datenschutzgrundrechte
I. Methodische Vorbemerkung: Zu Zulässigkeit und Grenzen induktiver/abduktiver Schlussfolgerungen aus Entscheidungen des BVerfG
II. Die drei zentralen Säulen des grundrechtlichen Datenschutzes
III. Das Telekommunikationsgeheimnis gem. Art. 10 Abs. 1 GG
IV. Das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG
V. Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG
VI. Sonstige datenschutzrelevante Grundrechte
VII. Ergebnis: Gemeinsame Vorgaben für die Auslegung und Ausgestaltung von strafprozessualen Eingriffsbefugnissen
VIII. Offene Fragen und weiterer Gang der Untersuchung

Kapitel 3 – Kriterien zur Bestimmung der Eingriffsintensität
I. Art der Daten
II. Menge der Daten/Dichte und Vielfalt der Informationen
III. Zugänglichkeit der Daten
IV. Lesbarkeit der Daten
V. Heimlichkeit der Maßnahme und Täuschungen durch die Ermittlungsbehörden
VI. Streubreite der Maßnahme
VII. Automatisierung der Maßnahme
VIII. Dauer der Maßnahme
IX. Sicherheit der Daten in staatlicher Obhut
X. Veränderungen an bestehenden Datensätzen 309
XI. Kenntnis, Kennenmüssen und fahrlässige Unkenntnis der Strafverfolgungsbehörden
XII. Anlassbezogenheit/Anlasslosigkeit eines Dateneingriffs
XIII. Folgen für den Betroffenen
XIV. Ergebnis: Eine partielle Ordnung der Eingriffsschwerekriterien bei Dateneingriffen im Strafverfahrensrecht
XV. Abstraktheit von Normen, ex ante-Perspektive und die relative ordinale Ordnung der Schwerekriterien

Kapitel 4 – Das Gewicht des staatlichen Strafverfolgungsanspruchs bzw. der Erfordernisse einer effektiven Strafrechtspflege
I. Verfassungsrang und Gewicht des Strafverfolgungsanspruchs
II. Schwere der Straftat
III. Grad des Tatverdachts, insbesondere Tatverdachtsgewinnung im Wege (automatisierter) Datenverarbeitung
IV. Auffindewahrscheinlichkeit bzgl. verfahrens- und nachweisrelevanter Daten
V. Wechselwirkungen und Ordnung der Kriterien zur Bestimmung des Gewichts des Strafverfolgungsanspruchs

Kapitel 5 – Die Abhängigkeit der Schutzmechanismen und Eingriffsschwellen von der Intensität des Dateneingriffs
I. Die Abhängigkeit der notwendigen Eingriffsschwellen und Schutzmechanismen von der Eingriffsintensität
II. Ergebnis: Ein »Baukastensystem« unter Berücksichtigung der Erforderlichkeit und der Verhältnismäßigkeit ieS

Kapitel 6 – Möglichkeiten und Grenzen neuartiger, unregulierter strafprozessualer Dateneingriffe
I. Problemaufriss: Schnelle technologische Entwicklung und langsame Gesetzgebungsverfahren
II. Die Grenzen der Auslegung von Ermittlungsbefugnissen
III. Ausweg technikoffene Eingriffsbefugnisse?
IV. Ergebnis und kriminalpolitische Überlegungen

Kapitel 7 – Europarechtliche Vorgaben für die Erhebung und Verwertung digitaler Daten im Strafverfahren

Mohr Siebeck

Mohr Siebeck GmbH & Co. KG
Postfach 2040
D-72010 Tübingen
info@mohrsiebeck.com
www.mohrsiebeck.com

I. Bedeutung des Europarechts und untersuchte Rechtsquellen
II. Vorgaben aus der Richtlinie 2016/680/EU und §§ 45 ff. BDSG
III. Bedeutungsgewinn der europäischen Grund- und Menschenrechte für die strafprozessuale Datenverarbeitung 641
IV. Verhältnis der Vorgaben aus der Richtlinie zu den verfassungsrechtlichen Vorgaben und Leitlinien (Meistbegünstigungsprinzip)

Kapitel 8 – Zentrale Probleme der Verwendung von Daten und Datenanalysen als Beweismittel in der Hauptverhandlung
I. Das Übersetzungsproblem: Die fehlende unmittelbare Wahrnehmbarkeit von Daten und der Grundsatz des sachnäheren Beweismittels
II. Flüchtigkeit und Manipulierbarkeit: IT-forensische Standards und strafprozessuales Beweisrecht
III. Beweiswert und Beweiswürdigung von Datenanalyseergebnissen
V. Datenanalyse, Akteneinsicht und prozessuale Waffengleichheit

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

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.

Order now:
https://www.mohrsiebeck.com/en/book/digitale-daten-als-beweismittel-im-strafverfahren-9783161622168?no_cache=1
order@mohrsiebeck.com
Phone: +49 (0)7071-923-17
Fax: +49 (0)7071-51104

Mohr Siebeck

Mohr Siebeck GmbH & Co. KG
Postfach 2040
D-72010 Tübingen
info@mohrsiebeck.com
www.mohrsiebeck.com