Das Recht der inneren und äußeren Sicherheit

Band 35

Präventiv-polizeiliche Zugriffe auf Telekommunikationsinhaltsdaten

Eine verfassungsrechtliche und einfach-gesetzliche Analyse unter Einbeziehung kriminalistischer und technischer Implikationen

Von

Christoph Keller

Duncker & Humblot · Berlin

CHRISTOPH KELLER

Präventiv-polizeiliche Zugriffe auf Telekommunikationsinhaltsdaten

Das Recht der inneren und äußeren Sicherheit

Herausgegeben von Prof. Dr. Dr. Markus Thiel, Münster

Band 35

Präventiv-polizeiliche Zugriffe auf Telekommunikationsinhaltsdaten

Eine verfassungsrechtliche und einfach-gesetzliche Analyse unter Einbeziehung kriminalistischer und technischer Implikationen

Von

Christoph Keller

Duncker & Humblot · Berlin

Die Deutsche Hochschule der Polizei – Universität der Polizeien des Bundes und der Länder hat diese Arbeit Im Jahre 2024 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Satz: 3w+p GmbH, Rimpar
Druck: Beltz Grafische Betriebe GmbH, Bad Langensalza

ISSN 2199-3475
ISBN 978-3-428-19703-3 (Print)
ISBN 978-3-428-59703-1 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

Verlagsanschrift: Duncker & Humblot GmbH, Carl-Heinrich-Becker-Weg 9,
12165 Berlin, Germany | E-Mail: info@duncker-humblot.de
Internet: http://www.duncker-humblot.de

Vorwort

Die vorliegende Arbeit wurde von der Deutschen Hochschule der Polizei – Universität der Polizeien des Bundes und der Länder als Dissertation 2024 angenommen. Die mündliche Prüfung fand am 22. Juli 2025 statt.

Mein erster und herzlicher Dank gilt meinem geschätzten Doktorvater Prof. Dr. Dr. Markus Thiel für seine Unterstützung. Vor allem seine konstruktiven Anmerkungen und Hinweise haben wesentlich zum Gelingen der Arbeit beigetragen und waren für die Entstehung dieser Arbeit ebenso prägend wie bereichernd. Dabei hat Professor Thiel mir großen Freiraum bei der Auswahl des Themas und der Bearbeitung der Dissertation gelassen. Ohne ihn wäre diese Arbeit nicht möglich gewesen. Für die Aufnahme der Arbeit in die von ihm herausgegebene Schriftenreihe „Das Recht der inneren und äußeren Sicherheit“ bin ich ihm großen Dank schuldig.

Für die zügige Erstellung des Zweitgutachtens danke ich herzlich Prof. Dr. Claudio Franzius.

Auf dem Weg zu dieser Dissertation haben mich viele Menschen begleitet und in ihrer ganz eigenen Form unterstützt. Mein ganz besonderer Dank gilt dabei meiner Familie für ihre Unterstützung, Geduld und vor allem Nachsichtigkeit und damit der Gewährleistung meiner mentalen und emotionalen Stabilität während der Bearbeitungsphase. Ihr ist diese Dissertation gewidmet. Für eure uneingeschränkte Unterstützung danke ich euch von ganzem Herzen.

Im Hinblick auf die Veröffentlichung der Dissertation ergab sich das Erfordernis einer geringfügigen Überarbeitung. Ursächlich hierfür war der Koalitionsvertrag der Bundesregierung zwischen CDU, CSU und SPD vom 5. 5. 2025 sowie verfassungsgerichtliche Rechtsprechung, zuletzt die Entscheidungen des Bundesverfassungsgerichts zur polizeirechtlichen Ermächtigung der Telekommunikationsüberwachung nach § 20c PolG NRW (Beschl. v. 24. 6. 2025 – 1 BvR 2466/19 – Trojaner I) und zu den strafprozessualen Ermächtigungen zur Quellen-Telekommunikationsüberwachung und Online-Durchsuchung. (Beschl. v. 24. 6. 2025 – BvR 180/23 – Trojaner II).

Rechtsstand 15. 8. 2025

Mettingen, im August 2025 *Dr. Christoph Keller*

Inhaltsübersicht

Teil 2

Teil 3

Inhaltsverzeichnis

Teil 2

Abbildungsverzeichnis

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter sowie auf diverse und non-binäre Personen. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Einleitung

A. Forschungsgegenstand

Zur staatlichen Aufgabe der Gewährleistung der Sicherheit und des Spezialgebiets der Cybersicherheit bedient sich der Staat insbesondere der Mechanismen der Gefahrenabwehr, also dem präventiven Einschreiten zur Verhinderung oder Minimierung von Schäden.[1] In diesem Aufgabenfeld gehören sicherheitsbehördliche Informationseingriffe zu den zentralen Arbeitsgrundlagen der Sicherheitsbehörden. Durch – vor allem verdeckte – Datenerhebungen wird primär der Zweck verfolgt, eine ausreichende Informationsgrundlage zu erhalten, um Gefahren näher auszuforschen und sodann die erforderlichen präventiven (und/oder repressiven) Maßnahmen zu treffen. Die Notwendigkeit verdeckter Datenerhebungen speziell zur Bekämpfung der Terrorismusbekämpfung oder der sog. Organisierten Kriminalität (OK) ergibt sich daraus, dass diesen Kriminalitätsphänomenen mit klassischen kriminalistischen Methoden wirksam nicht begegnet werden kann. Insbesondere im Bereich des internationalen Terrorismus ist zu beobachten, dass sich Personen moderner Technologien bedienen, um bei ihren Vorhaben einer Entdeckung zu entgehen und damit eine wirksame Gefahrenabwehr zu vereiteln.[2] Auch im militärpolitischen Geschehen sind entscheidende Änderungen eingetreten, die unter der Bezeichnung „hybride Kriegsführung“ diskutiert werden. Kennzeichnend ist die Verschleierung der Urheberschaft von schädigenden Maßnahmen, insbesondere auch Cyberattacken.[3] Zunehmend werden elektronische Kommunikationswege genutzt, um Straftaten zu planen und zu begehen. Die Sicherheitsbehörden sind daher verstärkt auf Beweismittel in elektronischer Form angewiesen. So kommen derzeit bei 85 % aller strafrechtlichen Ermittlungen digitale Daten zum Einsatz.[4] Bei den Informationseingriffen gehört die Kenntnisnahme der Sicherheitsbehörden von den Inhalten der Telekommunikation zu den tiefgreifendsten Eingriffen in die Rechte der von dieser Überwachung Betroffenen. Die Telekommunikationsüberwachung (TKÜ) gehört zu den bedeutsamsten Mitteln der verdeckten Informationsbeschaf-

[1] Vgl. *Brodowski*, in: Kipker, Cybersecurity, Kap. 17 Rn. 89.

[2] Vgl. *Graulich*, in: Lisken/Denninger, Hdb Polizeirecht, Kap. E. Rn. 794.

[3] Vgl. *Spies-Otto*, in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 19 Rn. 1 f.

[4] Vgl. *Weiß/Pradel*, CCZ 2024, 102.

fung, ist aber zugleich in ihren verschiedenen Facetten ein rechtlich und technisch komplexer Ausschnitt verdeckter Datenerhebungen. Im Rahmen von TKÜ-Maßnahmen stoßen die Sicherheitsbehörden vor dem Hintergrund einer (stetig) fortschreitenden Digitalisierung allerdings dann an ihre Grenzen, wenn informationstechnologische Endgeräte unter Nutzung kryptologischer Verfahren zur Vorbereitung schwerer Straftaten genutzt werden. In diesem Zusammenhang steht insbesondere die Referenzgruppe der Messenger-Dienste („Instant-Messaging-Dienste") im Fokus der Betrachtung, z. B. „WhatsApp", „Telegram" oder „Signal". Sind solche kryptografischen Sicherungen standardmäßig in dem technischen Repertoire von Kommunikationsanwendungen integriert, ist der Zugriff auf den verwertbaren Inhalt der Information grundsätzlich nur noch an der Quelle (d. h. auf dem Endgerät des Absenders oder Empfängers) möglich, solange die Kommunikationsinhalte dort noch unverschlüsselt bzw. wieder entschlüsselt vorliegen. Messenger-Dienste sind einer der Hauptgründe für die Einführung von Befugnissen zur sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), bei der typischerweise – etwa durch das gezielte Ausnutzen von Sicherheitslücken – mit Überwachungssoftware („Staatstrojaner") in von Zielpersonen genutzte informationstechnische Systeme eingegriffen wird, um Kommunikationsdaten von dort noch vor einer Verschlüsselung ausleiten zu können. Das zum Zwecke der Quellen-TKÜ vielfach erforderliche Ausnutzen von Sicherheitslücken birgt indes Risiken für die IT-Sicherheit. Der sich als (Schutz-)Pflichtenkollision darstellende Zielkonflikt („Kryptokontroverse") zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung bedarf einer näheren Betrachtung. Im Diskussionskern steht die Frage, ob die „fragile Balance zwischen Sicherheit und Freiheit"[5] gewahrt wird. Insbesondere stellt sich die Frage des Umgangs mit Sicherheitslücken, die vielfach erst ein unbemerktes „Einschleusen" technischer Mittel („Trojaner") in das informationstechnische System als Zielobjekt ermöglichen. Ein geordnetes und kontrollierbares Schwachstellenmanagement mit formalisierten Rahmenbedingungen gibt es bislang in Deutschland nicht. Im Hinblick auf die angesprochene Quellen-TKÜ ist zu untersuchen, ob die in einigen Polizeigesetzen (Mecklenburg-Vorpommern, Saarland, Zoll) eingeführte sog. „erweiterte Quellen-TKÜ" („kleine Online-Durchsuchung"[6]) den verfassungsrechtlichen Maßstäben genügt. Der Gesetzgeber lässt zu, gespeicherte Inhalte und Umstände verschlüsselt erfolgender Telekommunikationsvorgänge („während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form") zu überwachen, die hätten überwacht werden können, wenn sie unverschlüsselt erfolgt wären. Das Ergebnis ist von Bedeutung im Hinblick auf die an Eingriffsermächtigungen zu stellenden Anforderungen und führt zu der Frage, ob die derzeit angewandten Ermittlungsmethoden überhaupt durch vorhandene Eingriffsgrundlagen gedeckt sind bzw. ob die präventiv-polizeilichen Befugnisse für Zugriffe auf Telekommunikationsdaten mit den

[5] *Herrmann*, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, S. 21.

[6] *Thiel*, in: Dietrich et al., Hdb Sicherheits- und Staatsschutzrecht, § 24 Rn. 14.

technologischen Entwicklungen Schritt gehalten haben. Während der rechtliche Umgang mit Technik in den vergangenen Jahrzehnten zur Routine geworden war – die ganz überwiegend abstrakt gefassten Gesetze, Verordnungen und Richtlinien konnten in einem mehr schleichenden Prozess auf durch Technik veranlasste Probleme konkretisiert werden –, gehört die Frage, ob das in Grundrechte eingreifende Recht mit der neuen Entwicklung Schritt halten kann, zu den derzeit vieldiskutierten Aspekten.[7] Auszugehen ist davon, dass die enorme Geschwindigkeit der technologischen Entwicklung die Informations- und Kommunikationstechnologie zwar schneller und zuverlässiger gemacht hat, auf der anderen Seite aber neue Bedrohungen für die Cybersicherheit verursacht hat. Angesichts der zunehmenden Abhängigkeit moderner Gesellschaften von der Informations- und Kommunikationstechnologie ist Cybersicherheit zu einem vorrangigen Thema geworden und gilt als „komplexe globale Herausforderung“[8]. Ob Rechtsprechung und Rechtswissenschaft neue Techniken, ihre Wirkweisen, Gefahrenpotenziale sowie Möglichkeiten der Risikominimierung hinreichend berücksichtigen,[9] bedarf einer näheren Untersuchung, vor allem im Hinblick auf die Frage, ob die derzeitigen Rechtsgrundlagen ausreichend sind, um neue (technisch-basierte) Eingriffe rechtssicher zu bewerten. Die herausragende Bedeutung von informationstechnischen Systemen für den Alltag der meisten Menschen hat für präventiv-polizeiliches Handeln essenzielle Informationen bereits seit längerem kontinuierlich in digitale Sphären verlagert.[10] Die Datenerhebung durch Sicherheitsbehörden aus digitalen Sphären stellt inzwischen einen „Grundpfeiler moderner Gefahrenabwehr“[11] dar. Mittlerweile sehen sowohl der Bund als auch alle Bundesländer spezielle Ermächtigungsgrundlagen für präventiv-polizeiliche Eingriffe in das Telekommunikationsgeheimnis vor. Die Ermächtigungen legitimieren Eingriffe in das Grundrecht des Art. 10 Abs. 1 Var. 3 GG und knüpfen in ihrer Rechtsfolge an den Begriff „Telekommunikation“ an, der den sachlichen Anwendungsbereich der TKÜ-Ermächtigungen umschreibt und zugleich begrenzt. Während die TKÜ bei herkömmlichen Telefongesprächen vor allem auf Gesprächsinhalte beschränkt ist, können die Sicherheitsbehörden allerdings weitaus mehr Informationen erlangen, da in der Praxis nicht nur auf laufende („flüchtige“) Kommunikationsprozesse zugegriffen wird, sondern vielmehr auch – mitunter bereits seit Jahren – gespeicherte Nachrichten („Nicht-Kommunikationsdaten“) erhoben werden, die sich häufig auf alle Bereiche des privaten und beruflichen Lebens des Nutzers beziehen. In der Folge kann ohne größeren Aufwand anhand der Daten ein konkretes Persönlichkeits-, Kommunikations- und Bewegungsprofil des Betroffenen erstellt und in seiner Entwicklung nachverfolgt werden. Vor diesem Hintergrund ist Gegenstand der Untersuchung die Frage, ob derartige Formen der Datenkommunikation noch unter das Telekommunikationsgeheimnis

[7] Vgl. *Ensthaler*, ZRP 2022, 55.

[8] *Christen/Knieps/Inversini*, Kriminalistik 2022, 305.

[9] Zweifelnd diesbezüglich *Ensthaler*, ZRP 2022, 55 (58).

[10] Vgl. *Ruppert*, in: Dietrich et al., Hdb Sicherheits- und Staatsschutzrecht, § 23 Rn. 2.

[11] *Ruppert*, in: Dietrich et al., Hdb Sicherheits- und Staatsschutzrecht, § 23 Rn. 2.