B u c h r e z e n s i o n

Ulrich Sieber/Nicolas von zur Mühlen (Hrsg.), Access to Telecommunication Data in Criminal Justice, A Comparative Analysis of European Legal Orders, Duncker & Humblot, Berlin, 2016, 770 S., € 58.

I. Bedeutung von Telekommunikationsdaten im Strafverfahren

Aus dem modernen Strafverfahren ist der staatliche Zugriff auf Telekommunikationsdaten nicht mehr wegzudenken. Die Ausweitung des Zugriffs durch Einführung neuer Ermächtigungsgrundlagen scheint unumkehrbar. Umso bedeutsamer ist die rechtspolitische Debatte wie auch die konkrete Auseinandersetzung in der Praxis, inwiefern der Eingriff in das Persönlichkeitsrecht des Betroffenen durch den Zugriff auf seine Bestands-, Verkehrs- und Inhaltsdaten gerechtfertigt sein kann.

Eine wissenschaftlich-fundierte Grundlage dazu bietet das Werk der Herausgeber *Ulrich Sieber* und *Nicolas von zur Mühlen*. Es erschien in der Schriftenreihe „Strafrechtliche Forschungsberichte" des Max-Planck-Instituts für ausländisches und internationales Strafrecht, welche 1985 begründet und seit 2004 von *Sieber* fortgeführt wird. Er ist Leiter der strafrechtlichen Abteilung des Max-Planck-Instituts. Computerkriminalität bzw. Cybercrime gehört zu seinen Forschungsschwerpunkten. Mit dem vorliegenden, 2016 erschienenen Werk gelang es ihm und seinem Mitherausgeber, einen weiteren Meilenstein für die Grundlagenforschung in diesem Bereich zu setzen.

II. Möglichkeiten der Erhebung von Telekommunikationsdaten de lege lata

Der Zugriff auf Telekommunikationsdaten im Strafverfahren hat viele Facetten. Maßnahmen der Strafverfolgungsbehörden zur Erhebung von Daten betreffen nicht nur Beschuldigte, sondern auch Dritte, insbesondere Diensteanbieter. Nach deutschem Recht können die Ermittlungsmaßnahmen offen erfolgen, wie es bei Durchsuchung (§§ 102, 103 StPO), Durchsicht (§ 110 StPO), Sicherstellung (§ 94 StPO), Herausgabeverlangen (§ 95 StPO) und Verkehrsdatenabfrage (§ 100g StPO) der Fall ist. Besonders eingriffsintensiv sind die heimlichen Ermittlungsmaßnahmen, wobei zur klassischen Telekommunikationsüberwachung (§ 100a Abs. 1 S. 1 StPO) seit dem 24.8.2017 die Quellen-TKÜ (§ 100a Abs. 1 S. 2 StPO) und die Online-Durchsuchung (§ 100b StPO) hinzugekommen sind. Geht es um elektronische Beweismittel, besteht jedoch oft ein grenzüberschreitender Bezug. Die Gerätenutzer sind mobil, der Sitz des Diensteanbieters bzw. seine Datenkontrollzentren und die Speicherorte der Daten befinden sich häufig nicht im Inland.

Dieser Rechtswirklichkeit werden die Herausgeber mit einer klaren Zweiteilung gerecht: In einem Teil stellen sie in Form von Länderberichten eingehend die Rechtslage in Deutschland sowie Belgien, Tschechische Republik, Frankreich, Niederlande, Spanien, Schweden und Großbritannien dar. Hier flossen sowohl Berichte von Rechtswissenschaftlern als auch Interviews mit Polizeien und Justiz ein (Teil 3, S. 121–738). Der eigentliche Schwerpunkt des in englischer Sprache erschienenen Werks liegt sodann – wie es der Titel schon verrät – in dem den einzelnen Länderberichten vorangestellten Vergleich der Rechtssysteme der acht europäischen Staaten (Teil 2, S. 9–120).

III. Fortentwicklung des Rechts

Die Herausgeber haben die Schaffung neuer Ermächtigungsgrundlagen für die Strafverfolgungsbehörden antizipiert. Zutreffend nahmen sie die Notwendigkeit multilateraler Abkommen vorweg, soweit es für die Datenerhebung zu einem virtuellen Grenzübertritt kommt.

Am 17.4.2018 (eineinhalb Jahre nach Erscheinen des vorliegenden Werks) stellte die EU-Kommission ihre Regelungsvorschläge für zwei neue Instrumente zur Strafverfolgung vor (KOM [2018] 225 endg.), mit denen der Zugriff auf elektronische Beweismittel – sprich: Telekommunikationsdaten – beschleunigt werden soll: Mit Hilfe der Europäischen Sicherungsanordnung und der Europäischen Herausgabeanordnung sollen Strafverfolgungsbehörden ihre Anfragen zukünftig nicht mehr an ihr Pendant im Ausland, sondern direkt an den privaten Diensteanbieter stellen.[1] Anfragen auf Übermittlung von Beweismitteln beim Diensteanbieter haben zwar bereits in den letzten Jahren rasant zugenommen. Die Antwort der „big six" (Facebook, Google, Microsoft, Twitter, Apple und Yahoo), die den Großteil der relevanten Daten und damit Beweismittel verwalten, hängt jedoch von der jeweiligen Kooperationsbereitschaft und den unternehmensinternen Regelungen ab. Die Übermittlung von Bestands- und Verkehrsdaten erfolgt jedoch freiwillig, die Entscheidung des Diensteanbieters ist nicht justiziabel. Die Gesetzgebungsvorschläge zielen nunmehr auf eine Verpflichtung der Diensteanbieter zur Sicherung und Herausgabe von Telekommunikationsdaten im Strafverfahren ab, die durch Rechtsschutzmöglichkeiten flankiert werden soll. Unabhängig davon, wo die Daten physisch gespeichert sind (Territorialprinzip), soll die Verpflichtung Diensteanbieter treffen, die in der EU ihre Dienste anbieten (Marktortprinzip).

IV. Ausschluss des Zugriffs bei Berufsgeheimnisträgern

Für den wissenschaftlichen Diskurs von grundlegender Bedeutung ist daher die von den Herausgebern gemeinsam mit *Tatiana Tropina*, der *Autorin* dieses Abschnitts, erarbeitete rechtvergleichende Analyse. Im Rahmen des europäischen Gesetzgebungsverfahrens umstrittene Punkte wie der Ausschluss des Zugriffs bei Berufsgeheimnisträgern sind im vorliegenden Werk bereits exemplarisch für verschiedene Rechtskreise aufgearbeitet (S. 35–52).

Die *Autorin* analysiert dazu zunächst die bestehende Gesetzeslage. Sie stellt fest, dass die größten Unterschiede in der Gesetzgebung und Praxis der untersuchten Länder hinsichtlich des Verbots der Beweiserhebung von geschützter Kommunikation bestünden. Es existiere eine große Bandbreite von detaillierten und umfangreichen Regelungen in Deutschland und Frankreich einerseits und eng umgrenzten Regelun-

[1] Zur Entstehungsgeschichte eingehend *Burchard*, ZIS 2018, 190.

gen in der Tschechischen Republik anderseits. Alle untersuchten Länder schützten das Vertrauen in Berufsgeheimnisträger, Deutschland darüber hinaus auch den Kernbereich privater Lebensgestaltung. Zutreffend und hellsichtig in Bezug auf die aktuellen gesetzgeberischen Aktivitäten (nach Erscheinen des vorliegenden Werks) fasst die *Autorin* zusammen, dass ein Direktzugriff beim Diensteanbieter im Rahmen grenzüberschreitender Strafverfolgung problematisch sei, soweit dies auch zur Erhebung geschützter Kommunikation führen könne.

Unterschiedliche Gesetzgebungstechniken bestünden hinsichtlich der Art und Weise des Schutzes. In Deutschland werde in § 160a Abs. 1 und 2 StPO zwischen einem absoluten und einem relativen Beweiserhebungsverbot unterschieden. In Frankreich und Belgien werde zwischen dem (eng gefassten) Verbot der Erlangung und dem (weitergehenden) Verbot der Verschriftlichung geschützter Kommunikation unterschieden. Demgegenüber würden die Rechtsordnungen in Schweden, Niederlande und Spanien lediglich ein Zeugnisverweigerungsrecht für Berufsgeheimträger und einen damit einhergehenden Schutz vor Telekommunikationsüberwachung für diese Personen vorsehen. In der Tschechischen Republik seien nur Verteidiger und Beschuldigter von dem Schutz umfasst. In Großbritannien hänge der Schutz vertraulicher Informationen davon ab, ob sie zielgerichtet oder zufällig erlangt wurden.

In allen acht untersuchten Ländern werde die Kommunikation zwischen Anwalt und Mandant umfassend geschützt. Hinsichtlich anderer Berufsgeheimnisträger wie Geistliche, Ärzte, Journalisten, Notare und Mitglieder des Parlaments bestünden signifikante Unterschiede. In allen untersuchten Ländern existierten Ausnahmen, soweit Berufsgeheimnisträger der Beteiligung an einer Straftat verdächtig sind.

Schließlich untersucht die *Autorin* die technische und prozessuale Umsetzung der Schutzvorschriften. Sie unterscheidet zwischen einem Erhebungsverbot bzw. Löschungsgebot im Ermittlungsverfahren (Deutschland, Schweden, Tschechische Republik, Niederlande), einer Zugangsbeschränkung (Belgien) und einem bloßen Verwendungsverbot in der Hauptverhandlung (Frankreich, Spanien, Großbritannien).

V. Ausblick

Das Werk ist Teil des Forschungsgruppenprojekts „Internationale Zusammenarbeit in der TKÜ“. Die Studie wird finanziert durch das Bundesministerium des Innern. Nach Erscheinen des vorliegenden ersten Teils zu acht ausgewählten Rechtsordnungen sind derzeit im Rahmen des seit 2017 durchgeführten zweiten Teils Landesberichte zu zwölf weiteren Staaten – darunter die USA – in Arbeit. Der nächste Teil wird mithin letzte Lücken schließen. Schließlich richten sich in Strafverfahren die Anfragen auf Übermittlung von Beweismitteln faktisch überwiegend an die in den USA gelegenen Diensteanbieter, sog. „big six“. Die vorliegende Publikation bildet mithin einen Baustein für die Erforschung internationaler Kooperationsmöglichkeiten, auf der die Zukunft des Strafverfahrens fußen wird. Der (Europäische) Gesetzgeber wird nicht umhinkommen, auf die grundlegenden Vorarbeiten von Sieber/von zur Mühlen zurückzugreifen.

Rechtsanwältin Diana Nadeborn, Berlin