REZENSIONEN

Rechtsanwalt Dr. Mayeul Hiéramente, Hamburg

Esther-Nicola Vehling, Die Auswirkungen des Völkerrechts auf die grenzüberschreitende Ermittlung digitaler Beweis nach der StPO

Duncker & Humblot 2023, 264 Seiten,
ISBN 978-3-428-18814-7, 89,90 EURO

I. Einleitung

Die von Kuhli betreute und im Jahr 2022 abgeschlossene Dissertation widmet sich einem für die Praxis hochrelevanten Thema. Vehling befasst sich darin mit der Frage, ob und unter welchen Umständen das Völkerrecht staatlichen Ermittlungen Grenzen zieht und was aus staatlichen Verstößen gegen das Völkerrecht resultiert. In der Praxis werden die territorialen Grenzen staatlicher Eingriffsbefugnisse vor allem im Hinblick auf die Reichweite des § 110 Abs. 3 S. 2 StPO diskutiert (vgl. u.a. LG Koblenz, Beschl. 24.8.2021 – 4 Qs 59/21). Die von Vehling verfasste Abhandlung lässt es dabei jedoch nicht bewenden und beleuchtet eine Vielzahl von Ermittlungsmaßnahmen, die faktisch einen Zugriff auf im Ausland befindliche Daten oder die Überwachung vom im Ausland sich befindlichen Zielpersonen ermöglichen. Diese Entscheidung zahlt sich für den Leser aus. Das Zusammenspiel aus technischen, strafprozessualen und völkerrechtlichen Darstellungen veranschaulicht nicht nur die Komplexität der Materie. Es zeigt auch, dass die internationale Gemeinschaft für die Regulierung des Zugriffs auf Daten im „Cyberspace" eine Vielzahl von komplementären Regelungen geschaffen hat und gleichzeitig dem unilateralen Zugriff auf im Ausland gespeicherte Daten klare Grenzen gesetzt hat.

II. Inhalt

Die Abhandlung ist in fünf Kapitel unterteilt. In einem kurzen ersten Kapitel werden die technischen Grundlagen der Telefonie sowie des Internets dargestellt. Hierbei werden kurz die Funktionsweise des Festnetzes und Mobilfunknetzes erläutert (S. 20 ff.), bevor die Architektur des Internets (S. 25 ff.) sowie wichtige Internetanwendungen (S. 32 ff.) aus technischer Sicht beleuchtet werden. Von besonderer Bedeutung für die grenzüberschreitende Datenerhebung im Bereich der Telekommunikation sind die Auslandsköpfe (S. 22), an denen Ermittlungsbehörden im Inland transnationale Telekommunikation überwachen können. Die Überwachung muss mithin nicht am konkreten Anschluss erfolgen, sondern kann auch an einem der 21 Auslandskopf-Vermittlungsstellen ansetzen. So sind Ermittlungsbehörden technisch in der Lage, einen ausländischen Anschluss zu überwachen, der mit Kommunikationspartnern im Inland kommuniziert. Für den Bereich des Internets erläutert Vehling die Funktionsweise des Datenaustausches via Internet, der – anders als beim klassi-

schen Festnetz – nicht mittels einer feststehenden Leitung zwischen den Kommunikationsteilnehmern erfolgt, sondern auf eine Übertragung einzelner Datenpakete setzt (vgl. S. 29 ff.), was gerade bei transnationalen Sachverhalten zu technischen Schwierigkeiten bei der Überwachung führen kann (vgl. S. 69). Darüber hinaus geht mit der internetbasierten Datenspeicherung und -verarbeitung ein loss of knowledge of location einher (S. 34). Dies kann in der Praxis mit Schwierigkeiten bei der Bestimmung des Speicherorts und damit der Zuständigkeit nationaler Ermittlungsbehörden einhergehen.
Das zweite Kapitel widmet sich der Frage, welche Vorschriften der StPO die Erhebung digitaler Beweise ermöglichen. Dieses Kapitel ist angesichts der Fragestellung der Abhandlung überraschend lang geraten, ermöglicht dem nicht mit der Materie vertrauten Leser allerdings, sich einen Überblick über die strafprozessuale Materie und die in Rechtsprechung und Literatur geführten Debatten zu verschaffen. Zudem schafft das Kapitel eine Grundlage für die folgende Betrachtung. Vehling untersucht zunächst, was unter Telekommunikation iSd StPO zu verstehen ist, plädiert insoweit für einen genuin strafprozessualen Telekommunikationsbegriff (S. 46) und konstatiert völlig zu Recht, dass eine Überwachung maschineller Datenströme sowie der Internetnutzung in der Eingriffsintensität eher einer Online-Durchsuchung nahekommen (S. 49 ff.). Ob sich aus der Schaffung des § 100b StPO durch den Gesetzgeber ableiten lässt, dass damit eine Begrenzung des Anwendungsbereichs des § 100a StPO auf sozial-kommunikative Kommunikation intendiert war (S. 52 f.), ist allerdings unklar. Zwar dürfte sich im Lichte der verfassungsgerichtlichen Rechtsprechung, die Anlass für die Normierung einer Eingriffsbefugnis für Eingriffe in das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme war, begründen lassen, dass zumindest der (automatisierte) Datenaustausch zwischen Endgerät und Cloud nur nach § 100b StPO überwacht werden darf. Ob sich aus der Gesetzgebungshistorie allerdings ein deutlicher Schlussstrich unter die Debatte des strafprozessualen Telekommunikationsbegriffs herleiten ist, lässt sich jedoch bezweifeln. Vehling widmet sich auch der Frage, ob endgespeicherte Emails, die der Nutzung bewusst auf dem Server belassen hat, über § 100a StPO gesichert werden dürfen. Vehling diskutiert hier die verfassungsgerichtliche Rechtsprechung und kommt, in Abgrenzung zum BVerfG, zu dem zutreffenden Ergebnis, es liege insoweit kein Eingriff in Art. 10 GG vor, weshalb nicht § 100a StPO, sondern § 100b StPO einschlägig sei (S. 57 ff.). Hinzukommt, dass eine Anwendbarkeit des § 100a StPO bereits aus einfachrechtlichen Gründen zweifelhaft ist (vgl. dazu Grözinger NStZ 2021, 358). Vehling diskutiert ferner, wer Verpflichteter iSd § 100a Abs. 4 StPO ist und ob OTT-Dienstleistungen unter den Begriff des Telekommunikationsdiensteanbieters fallen (S. 61 ff.). Den Abschnitt zur TKÜ wird abgeschlossen durch eine Befassung mit § 4 Abs. 2 S. 1 TKÜV, der die Auslandskopfüberwachung regelt (S. 68 ff.), und der Quellen-TKÜ (S. 70 ff.).

Im folgenden Abschnitt widmet sich Vehling der Online-Durchsuchung nach § 100b StPO (S. 73 ff.) und diskutiert – und verneint – eine Anwendbarkeit des § 100b StPO auf Herausgabeverlangen (S. 79 f.). Dem schließen sich ein Abschnitt über § 100i StPO (S. 80 f.) sowie Ausführungen zu Datenabfragen (Verkehrs- und Nutzungsdaten, Bestandsdaten) bei Diensteanbietern (TKG, TMG) an (S. 81 ff.). Vehling diskutiert in der Folge die Anwendbarkeit des § 94 StPO auf die Beschlagnahme von Daten. Entgegen der hM und der Rechtsprechung des Bundesverfassungsgerichts lehnt sie die Anwendbarkeit ab, da die Norm nicht hinreichend bestimmt und zudem unverhältnismäßig sei (S. 96 f.). Zudem drohe so das Regelungskonzept der §§ 100a ff. StPO unterlaufen zu werden (S. 98 f.). Ob dies in dieser Absolutheit zutreffend ist – die §§ 100a ff. StPO erlauben heimliche und längerfristige Eingriffe, § 94 StPO grundsätzlich nur offene und Zugriffe zu bestimmten Zeitpunkten – mag dahinstehen. Zutreffend konstatiert Vehling aber, dass die verfassungsgerichtliche Rechtsprechung gewisse Fragen aufwirft, wenn sie im Bereich der §§ 100a ff. StPO ausdifferenzierte Regelungen fordert (vgl. z. B. BVerfG, Beschl. v. 27.5.2020 – 1 BvR 1873/13, 1 BvR 2618/13), den Gesetzgeber bei der Datenbeschlagnahme jedoch nicht in die Pflicht nimmt. Vehling lehnt konsequenterweise auch eine Anwendbarkeit des § 95 StPO auf Daten ab (S. 101). Offen bleibt, welche Auswirkungen dies auf § 110 Abs. 3 StPO hat. Dieser erlaubt einen Zugriff auf Daten (S. 101 ff.). Allerdings dürfte sich hier, würde man der Ansicht von Vehling folgen, die Frage stellen, ob eine solche Maßnahme überhaupt geeignet sein kann, wenn die Daten in der Folge nicht beschlagnahmt werden können. Vergleichsweise kurz spricht Vehling noch den Zugriff auf öffentlich zugängliche Daten im Internet an, den sie für nach der Ermittlungsgeneralklausel für zulässig erachtet (S. 103 f.). Eine informelle Kooperation mit Dateninhabern hält sie strafprozessual für unzulässig (S. 105).

Im folgenden dritten Kapitel geht Vehling auf die Kernthematik der Abhandlung ein. Dabei wird in drei Stufen vorgegangen. In einem ersten Schritt wird untersucht, ob das Telefonnetz und der Cyberspace überhaupt von territorialen Hoheitsansprüchen der Staaten erfasst wird. Eine Einordnung hinsichtlich der Telefonnetze fällt insoweit leicht (S. 112). Hinsichtlich des Cyberspace kommt Vehling zu dem detailliert begründeten Schluss, dass Staaten über den Cyberspace zwar nicht per se Hoheitsrechte ausüben können, wohl aber über die bedingende (nationale) Infrastruktur und die Nutzer (S. 117). Anders als die Weltmeere, die dort sind, wo die Staaten nicht sind, setzt sich der Cyberspace aus der Infrastruktur der Staaten zusammen (S. 118 f.).

Auf der zweiten Stufe prüft Vehling, unter welchen Voraussetzungen eine Exterritorialität vorliegt und ob eine exterritoriale Datenermittlungen als völkerrechtliches Delikt, also den Verstoß gegen eine Primärnorm anzusehen ist. Zu Recht meldet sie für den klassischen Fall der Datenermittlung Zweifel an, ob ein Verstoß gegen das Interventionsverbot vorliegt (S. 154 ff.). Zudem überzeugen die Ausführungen, die die Achtung der Souveränität fremder Staaten als verbindliches völkerrechtliches Gebot einstuft (S. 160). Auf dieser Grundlage analysiert Vehling, ob und unter welchen Bedingungen ein extraterritorialer Datenzugriff eine extraterritoriale Ausübung von Hoheitsmacht darstellt (S. 120 ff.) und ob dieser als Verstoß gegen die Souveränität zu werten ist (S. 162 ff.). Hierzu im Einzelnen:

Zunächst widmet sich Vehling der Frage, wann eine Extraterritorialität bei der Überwachung einer leitungsgebundenen Telekommunikation vorliegt (S. 123 ff.) und kommt zu dem Schluss, dass die gezielte Überwachung eines Inhabers einer Zielperson im Ausland ein Eingriff in die fremde Souveränität vorliege, da bei der Echtzeitüberwachung die Zielperson quasi zum Beweismittel werde (S. 127 ff.). Einen Eingriff in die staatliche Souveränität sieht Vehling auch beim Zugriff auf Daten, die lokal auf dem Gerät eines Nutzers im Ausland gespeichert sind (S. 129 ff.). Gleiches gelte bei dem Direktzugriff auf den Daten, die serverbasiert gespeichert seien (S. 132 ff.). Hier entspreche es der opinio juris, auf den Speicherort der Daten abzustellen und insoweit territoriale Herrschaftsansprüche anzunehmen (S. 136). Zwar sieht Vehling insoweit einen Bedarf, für völkerrechtliche Sonderregelungen, betont aber zugleich, dass derzeit der Speicherort als traditionelles Zuordnungskriterium maßgeblich sei (S. 138 f.). Dies zeige sich auch an bestimmten Rechtshilfeverträgen aus dem Bereich Cybercrime, die in Kenntnis der praktischen Hindernisse nur Regelungen zur Vereinfachung der Rechtshilfe getroffen haben (S. 137). Diese völlig zutreffende Auffassung Vehlings wird von der staatsanwaltschaftlichen und landgerichtlichen Praxis allerdings teilweise in Frage gestellt. Diese, im Zeitpunkt des Abfassens der Abhandlung wohl noch nicht bekannten (vgl. LG Koblenz, Beschl. 24.8.2021 – 4 Qs 59/21 m. Anm, Hiéramente/Basar, juris PR-StrafR 6/2022 Anm. 1) – und zum Teil auch noch nicht veröffentlichen – Entscheidungen blenden diesen klaren Regelungswillen bedauerlicherweise aus. Die gilt insbesondere für (vermeintliche) Fälle der sog. loss of knowledge of location, für die Vehling keine Ausnahme vom völkerrechtlichen Verbot des Direktzugriffs macht (S. 168 ff.).

Vehling widmet sich dann einer weiteren Zugriffsmöglichkeit: Der Anfrage beim Diensteanbieter. Dies Ausführungen sind besonders instruktiv, weil eine saubere Trennung zwischen Anfragen an territoriale Diensteanbieter und extraterritoriale Anbieter erfolgt. Insoweit werden Bestrebungen erläutert territoriale Diensteanbieter zur Übermittlung unternehmensinterner Daten zu verpflichten, die möglicherweise in einem anderen Staat belegen sind (S. 140 ff.). Insoweit bestehe bereits Uneinigkeit, wann von einem Diensteanbieter im Inland auszugehen sei. Insbesondere bestehe selbst innerhalb der EU kein Konsens, ob der Sitz, der Marktort oder der Ort, indem die Infrastruktur vorgehalten wird, maßgeblich sein soll. Sollte der Provider im Inland ansässig sein, hält Vehling eine Anordnung, auch unternehmensinterne Daten aus dem Ausland zu beschaffen, für völkerrechtskonform (S. 148), sofern dies faktisch möglich ist (S. 143). Sollte der Diensteanbieter hingegen keine Inlandspräsenz haben, stellt sich die Frage, ob eine Herausgabeanordnung an einen ausländischen Serviceprovider erfolgen kann (S. 143 ff.). Insoweit bejaht Vehling einen Verstoß gegen Hoheitsrechte des betroffenen Staates, auch wenn eine Durchsetzung mittels Zwangsmaßnahmen ausscheide (S. 144 f.). Anders bewertet sie den Fall einer informellen Anfrage bei einem ausländischen Serviceprovider. Eine Vielzahl der Staaten habe bestätigt, dass eine derartige Zusammenarbeit erfolge (S. 149 ff.). Zwar könne das Handeln eines Privaten einem Staat im Einzelfall zugerechnet werden. Die Voraussetzungen für eine Zurechnung seien aber nicht erfüllt. Dieser agiere vielmehr freiwillig. Ob eine solche Kooperation in der Praxis allerdings tatsächlich stets freiwillig ist und ob Staaten nicht möglicherweise in der Lage sind, mittelbar Zwang auf Dienstleister auszuüben, steht auf einem anderen Blatt und ist naturgemäß nicht Gegenstand der Betrachtungen gewesen.

In einem dritten Schritt geht Vehling auf völkervertragsrechtliche Ausnahmen ein und bespricht u.a. kurz die Rechtshilfe in Europa (S. 178), Rechtshilfe mit den USA (S. 179), die Cybercrime-Konvention (S. 180 ff. und den Entwurf der E-Evidence-Verordnung der EU (S. 182). Diese Regelungswerke werden für die TKÜ (S. 184 ff.) und den Zugriff auf Daten (S. 187 ff.) noch einmal detailliert dargestellt.

Im vierten Kapitel wendet Vehling die völkerrechtlichen Erkenntnisse auf die strafprozessualen Maßnahmen an. Das fünfte Kapitel wendet sich der Frage zu, ob bei Verstößen Beweisverwertungsverbote existieren. Hier werden die gängigen Ansichten zu unselbstständigen Beweisverwertungsverboten dargestellt (S. 216 ff.). Vehling selbst spricht sich für besonders weitgehende Beweisverwertungsverbote aus (S. 221 ff.) und wendet diese dann auf den Fall des Verstoßes gegen die Souveränität fremder Staaten an (S. 228 ff.). Ihrem sehr weiten – und von der Rechtsprechung bewusst abweichenden – Verständnis von Beweisverwertungsverboten folgend, nimmt sie grundsätzlich ein Beweisverwertungsverbot an und lässt ein solches auch bei nachträglicher Zustimmung des betroffenen Staates grundsätzlich nicht entfallen (S. 232 f.).

III. Resümee

Die Abhandlung befasst sich einem rechtlich und technisch komplexen Thema. Durch die Anzahl der Themen sind einzelne Ausführungen allerdings recht komprimiert dargestellt. Die Entscheidung Vehlings, sowohl technische Grundlagen als auch strafprozessuale und völkerrechtliche Fragen zu beleuchten, ist Stärke und Schwäche zugleich. Die Vielseitigkeit der Abhandlung ermöglicht dem Leser einen sehr guten Überblick über die Materie und veranschaulicht die enormen Herausforderungen für Wissenschaft und Praxis und die praktische Notwendigkeit, die Entwicklungen auf Ebene des Völker- und Europarechts genau im Blick zu behalten.