Schriften zum Prozessrecht

Band 290

Die Auswirkungen des Völkerrechts auf die grenzüberschreitende Ermittlung digitaler Beweise nach der StPO

Von

Esther-Nicola Vehling

Duncker & Humblot · Berlin

ESTHER-NICOLA VEHLING

Die Auswirkungen des Völkerrechts auf die grenzüberschreitende Ermittlung digitaler Beweise nach der StPO

Schriften zum Prozessrecht

Band 290

Die Auswirkungen des Völkerrechts auf die grenzüberschreitende Ermittlung digitaler Beweise nach der StPO

Von

Esther-Nicola Vehling

Duncker & Humblot · Berlin

Der Fachbereich Rechtswissenschaft der Universität Hamburg
hat diese Arbeit im Jahre 2022 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: L101 Mediengestaltung, Fürstenwalde
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 0582-0219
ISBN 978-3-428-18814-7 (Print)
ISBN 978-3-428-58814-5 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2022 von der Juristischen Fakultät der Universität Hamburg als Dissertation angenommen. Für die Drucklegung wurde das Manuskript überarbeitet und auf den Stand von November 2022 gebracht.

Die Arbeit ist mit ihrem Beginn im Herbst 2019 nicht nur während Zeiten der Pandemie entstanden, sondern auch zu einer Zeit, in der sich sowohl der Gesetzgeber als auch die Gerichte immer wieder mit Fragen der digitalen Beweiserhebung auseinandergesetzt haben. Durch den teilweise eingeschränkten Zugang zu Literatur, durch die Aktualität des Themas und die fortwährende Anpassung der Gesetzeslage gestaltete sich das Erstellen der Dissertation als besonders herausfordernd, aber auch als besonders spannend. Insgesamt empfand ich die Zeit der Dissertationserstellung als lehrreiche, interessante und vor allem bereichernde Zeit.

An erster Stelle gebührt mein besonderer Dank meinem Doktorvater Herrn Professor Dr. Milan Kuhli. Er unterstützte mich nicht nur bei der Wahl des Themas, sondern stand während des Verfassens der Dissertation stets als Diskussionspartner zur Verfügung. Durch seine konstruktiven Anmerkungen, wertvollen Hinweise und sein ermunterndes Lob hatte ich stets das Gefühl gut betreut und auf dem richtigen Weg zu sein. Mein Dank gilt auch Herrn Professor Dr. Kai Cornelius für die Erstellung des Zweitgutachtens und seine wertvollen abschließenden Hinweise.

In privater Hinsicht gilt mein herzlicher und unermesslicher Dank meinen Eltern, Karl-Heinz Vehling und Doris Knops-Vehling, die es mir durch ihre fortwährende Unterstützung ermöglicht haben, meiner Freude am Lernen und am wissenschaftlichen Arbeiten nachzugehen. Darüber hinaus möchte ich mich bei meinen Schwestern bedanken, die mich stets in all meinen Vorhaben bestärkt haben. Nicht zuletzt gebührt mein Dank meinen Freunden, die immer wieder dafür gesorgt haben, dass es mir während des Verfassens der Doktorarbeit nie an hinreichend Motivation, Disziplin und notwendiger Erholung fehlte und somit wesentlich zum Gelingen dieser Arbeit beigetragen haben. Ganz besonderer Dank gilt in dieser Hinsicht meinem besten Freund Jacob, der mir von den Anfängen der Dissertation bis zu ihrer Verteidigung in jedweder Hinsicht wie kein anderer zur Seite stand.

Berlin, im Februar 2023 *Esther-Nicola Vehling*

Inhaltsverzeichnis

Kapitel 4

Bedeutung der völkerrechtlichen Grundsätze für die nationalen Ermittlungsbefugnisse der Strafverfolgungsbehörden nach der StPO 202

Kapitel 5

Die Verwertbarkeit völkerrechtswidrig erlangter Beweise 212

Einleitung

Die voranschreitende Globalisierung und Digitalisierung verändern nach wie vor die Gesellschaft. Nationale Grenzen werden durch die Bürger immer weniger wahrgenommen. Moderne Technik erlaubt es Personen, sich weltweit zu vernetzen und auch Dienstleistungen aus dem Ausland in Anspruch zu nehmen. Die Phänomene der Globalisierung und Digitalisierung bergen viele Vorteile für die Zivilgesellschaft. Die Strafverfolgungsbehörden stellen sie jedoch vor nicht zu unterschätzende Probleme: Strafverfolgungsbehörden sind als Teil der Staatsmacht in ihren Handlungen grundsätzlich auf das eigene Staatsgebiet beschränkt.[1] Die Strafprozessordnung, die den Behörden Befugnisse für bestimmte Ermittlungsmaßnahmen an die Hand gibt, ist insofern in ihrer Anwendung geografisch beschränkt und kann im Grundsatz nur Maßnahmen auf deutschem Hoheitsgebiet legitimieren.[2] Diese örtliche Beschränkung folgt aus dem völkerrechtlichen Souveränitätsprinzip, zu dessen Ausprägungen das Recht zur Selbstständigkeit und zur Selbstbestimmung auf dem eigenen Staatsgebiet zählen.[3] Das aus diesen Rechten folgende Gebot der Achtung der Souveränität anderer Staaten macht es erforderlich, die Erlaubnis eines betroffenen fremden Staates einzuholen, bevor hoheitliche Tätigkeiten auf dessen Staatsgebiet ausgeübt werden.[4] Ohne eine solche Erlaubnis bleibt der ermittelnde Staat nach den Grundsätzen des Völkerrechts darauf verwiesen, die behördliche Mithilfe des betroffenen Staates im Rechtshilfeverfahren zu ersuchen, um Ermittlungen auf dessen Staatsgebiet vorzunehmen oder vornehmen zu lassen.[5]

Während Ermittlungsbefugnisse sich also auf das eigene Staatsgebiet beschränken, weisen Ermittlungsverfahren aufgrund der Globalisierung und

---

[1] *Frank P. Schuster*, „Verwertbarkeit von Beweismitteln bei grenzüberschreitender Strafverfolgung", ZIS 2016, S. 564, 564; *Daskal*, „Transnational Government Hacking", Journal of National Security Law & Policy 2020, S. 677, 680; *Bell*, „Strafverfolgung und die Cloud: Strafprozessuale Ermächtigungsgrundlagen und deren völkerrechtliche Grenzen", Duncker & Humblot 2019, S. 159.

[2] *Marberth-Kubicki*, „Computer- und Internetstrafrecht", Beck 2005, S. 236.

[3] *Epping*, in: Epping/Heintschel von Heinegg (Hrsg.), Ipsen, Völkerrecht, 2018, § 7 Rn. 261.

[4] *Tiedemann*, „Die Auslandskopf-Überwachung nach der TKÜV 2005", CR 2005, S. 858, 862.

[5] *Seitz*, „Transborder Search: A New Perspective in Law Enforcement?", Yale Journal of Law and Technology 2005, S. 22, 27.

Digitalisierung immer mehr internationale Bezüge auf. Moderne Telekommunikations- und Informationstechnologie erlaubt es Tätern, sich international zu vernetzen. Insbesondere in den Bereichen des Terrorismus und der organisierten Kriminalität zeigt sich eine große Prävalenz an internationalen Tätergruppierungen: Kaum eine groß angelegte OK-Gruppierung ist heutzutage nicht international tätig. So wurden in Deutschland für das Jahr 2019 426 OK-Verfahren mit Auslandsbezug gemeldet, bei denen Verbindungen der Täternetzwerke in insgesamt 123 verschiedene Länder nachgewiesen werden konnten.[6] Aber auch außerhalb der internationalen organisierten Kriminalität kann schon die Nutzung des Internets per se Ermittlungsverfahren einen internationalen Einschlag geben.[7] Grund dafür ist die Architektur und technische Funktionsweise des Internets, wie sich exemplarisch anhand des Unternehmens „Google" verdeutlichen lässt: Im Oktober 2018 waren bei *Google Mail* (Gmail) 1,5 Milliarden Nutzer registriert.[8] Unabhängig davon, ob die Nutzer den Webmail-Service (Abruf des E-Mail-Postfachs über den Browser) oder einen E-Mail Client (z. B. Gmail App auf dem Smartphone oder Tablet) nutzen, wird jede E-Mail, die über einen Gmail-Account gesendet oder empfangen wird, inklusive Anhang auf den Servern von Google gespeichert.[9] Google verfügt neben Rechenzentren in Nord-, Mittel- und Südamerika und in Asien auch über Server in Europa. Letztere befinden sich allerdings nicht in Deutschland, sondern in Irland, Finnland, Belgien und den Niederlanden.[10] Für das Strafverfahren bedeutet dies, dass die Strafverfolgungsbehörden nicht auf die bei Gmail vorgehaltenen E-Mails eines Verdächtigen zugreifen können – sofern er diese nicht lokal auf seinem Computer gespeichert hat – ohne auf Rechenzentren in anderen Jurisdiktionen zuzugreifen.

In Ermittlungsverfahren, denen die eben dargelegten internationalen Bezüge anhaften, ist es für die Ermittlung digitaler Beweise, anders als bei der Ermittlung gegenständlicher Beweise, nicht notwendig, dass die deutschen Ermittlungsbehörden physisch auf fremdem Staatsgebiet anwesend sind.

---

6 *Bundeskriminalamt*, „Bundeslagebild Organisierte Kriminalität 2019", 2019, S. 58; ähnliche Ergebnisse auch auf Landesebene, vgl: *Ministerium des Innern Brandenburg*, „Organisierte Kriminalität wird internationaler: Nr. 154/2005", 25.08.2005, zuletzt geprüft am: 29.12.2019, wo 81 % der OK-Verfahren internationale Bezüge aufwiesen.

7 *M. Gercke*, „Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden", MMR 2008, S. 291, 296.

8 Vgl. Twitter-Post von Googlemail vom 26.10.2018, abrufbar unter: https://twitter.com/gmail/status/1055806807174725633?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1055806807174725633%7Ctwgr%5E%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Fstadt-bremerhaven.de%2Fgmail-15-milliarden-aktive-nutzer%2F, zuletzt geprüft am: 30.05.2021.

9 *Spoenle*, „Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?", 2010, S. 5.

10 https://www.google.com/about/datacenters/inside/locations/index.html.

Vielmehr können die Beweise mittels Fernzugriff erlangt werden und somit quasi auf das eigene Staatsgebiet „herübergezogen werden".

Vor dem Hintergrund dieser Problematik drängt sich – aus deutscher Sicht – die folgende Überlegung auf: Dürfen die Ermittlungsbehörden aufgrund der Möglichkeit, bei den Ermittlungsmaßnahmen im eigenen Hoheitsgebiet zu verweilen, ihren Arm aus Deutschland heraus ins Ausland „ausstrecken" und so auch sich im Ausland befindliche Anschlüsse überwachen und Daten von Servern in fremden Hoheitsgebieten abrufen? Oder müssen sie vielmehr auch bei ihren Ermittlungshandlungen bezüglich digitaler Beweise strikt auf das deutsche Staatsgebiet beschränkt bleiben und bei Auslandsbezügen stets um Rechtshilfe des betroffenen Staates ersuchen? Wenn Letzteres zutrifft, welche Konsequenzen hat es für die Beweisverwertung im Strafverfahren, wenn ein Zugriff auf digitale Daten unter Verstoß gegen völkerrechtliche Grundsätze erfolgt?

Die Untersuchung der Frage, wie das Völkerrecht die *deutschen* Ermittlungsbehörden bei der Ermittlung digitaler Beweise begrenzt, wird in der vorliegenden Arbeit in drei Schritten erfolgen, wobei internationale Ermittlungsbehörden wie die Europäische Staatsanwaltschaft, die zum 01. Juni 2021 ihre Arbeit aufnahm[11], Inter- und Europol außen vor bleiben. In einem ersten Teil wird untersucht, welche nationalen Ermittlungsbefugnisse den Ermittlungsbehörden für einen Zugriff auf Daten nach der StPO zur Verfügung stehen, wobei andere Gesetze zur Strafverfolgung, wie das Zollfahndungsdienstgesetz, außen vor bleiben. Dabei wird auch auf die im Jahr 2021 eingeführten Erweiterungen der Verkehrs-, Nutzungs- und Bestandsdatenauskunft eingegangen werden. In einem zweiten Teil wird dargestellt, wie völkerrechtliche Grundsätze diese Ermittlungsmaßnahmen räumlich begrenzen. Dafür wird zunächst die Anwendbarkeit des Völkerrechts auf internationale Telefonnetze und das Internet erörtert, bevor geprüft wird, ob Ermittlungshandlungen, die ausschließlich von deutschem Territorium aus durchgeführt werden, überhaupt völkerrechtliche Relevanz zukommen kann. Nach der Feststellung, dass auch Zugriffe auf Daten, die aus dem Inland initiiert werden, gegen das Völkerrecht verstoßen können, werden die einschlägigen Rechtshilfeinstrumente der Bundesrepublik Deutschland dargestellt. Im dritten und damit letzten Schritt wird untersucht, welche Konsequenzen die Völkerrechtswidrigkeit einer Beweiserhebung auf die Verwertbarkeit der Beweismittel im Verfahren gegen den Beschuldigten hat. Bearbeitungsstand der vorliegenden Arbeit ist der 30.10.2021. In Hinblick auf die Änderung der Rechtslage durch das Inkrafttreten des neuen TKG und des TTDSG und durch den Beschluss des Zweiten Zusatzprotokolls zur Cybercrime Convention wurde die Arbeit zur Drucklegung diesbezüglich auf den Stand November 2022 aktualisiert.

---

[11] https://www.consilium.europa.eu/de/policies/eppo/#, zuletzt geprüft am: 30.09.2020.