Schriften zum Prozessrecht

Band 254

Strafverfolgung und die Cloud

Strafprozessuale Ermächtigungsgrundlagen und deren völkerrechtliche Grenzen

Von

Senta Bell

Duncker & Humblot · Berlin

SENTA BELL

Strafverfolgung und die Cloud

Schriften zum Prozessrecht

Band 254

Strafverfolgung und die Cloud

Strafprozessuale Ermächtigungsgrundlagen und
deren völkerrechtliche Grenzen

Von

Senta Bell

Duncker & Humblot · Berlin

Die Juristische Fakultät der Universität Würzburg
hat diese Arbeit im Sommersemester 2018
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 buchbücher.de GmbH, Birkach
Printed in Germany

ISSN 0582-0219
ISBN 978-3-428-15620-7 (Print)
ISBN 978-3-428-55620-5 (E-Book)
ISBN 978-3-428-85620-6 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

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

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2018 von der Juristischen Fakultät der Julius-Maximilians-Universität Würzburg als Dissertation angenommen. Für die Drucklegung wurde das Manuskript überarbeitet und auf den Stand von Juni 2018 gebracht.

An erster Stelle gebührt mein ganz besonderer Dank meinem Doktorvater Herrn Professor Dr. Frank Peter Schuster. Er stand mir während der gesamten Promotionszeit mit Rat und Tat zur Seite und hat durch seine klugen und konstruktiven Anmerkungen und wertvollen Hinweise ganz maßgeblich zum Gelingen dieser Arbeit beigetragen. Mein besonderer Dank gilt auch Herrn Professor Dr. Dr. Eric Hilgendorf, für die Erstellung des Zweitgutachtens.

Die Arbeit ist während meiner Zeit als wissenschaftliche Mitarbeiterin am Dekanat der Juristischen Fakultät der Julius-Maximilians-Universität Würzburg entstanden. Die Erstellung der Arbeit war für mich eine Herausforderung und eine außergewöhnlich bereichernde Erfahrung zugleich. Mein herzlicher Dank gilt den Menschen, die mich während dieser Zeit unterstützt und begleitet haben, insbesondere auch meinen lieben und geschätzten Kollegen, die mir bei der Erstellung der Arbeit in jeder erdenklichen Weise unterstützend zur Seite standen und dadurch ebenfalls maßgeblich am Gelingen der Arbeit beteiligt sind.

Ganz besonders danken möchte ich schließlich auch denjenigen Menschen, die während des Studiums zu besonderen Freunden wurden und nach dem Examen mit mir den Weg gemeinsam gegangen sind. Auch dank Euch werde ich die Promotionszeit immer in besonders schöner Erinnerung behalten.

Heilbronn, im Oktober 2018 *Senta Bell*

Inhaltsverzeichnis

Einleitung

„Ich mache mir wirklich große Sorgen, weil alles in die Datenwolke geht. Ich denke, es wird schrecklich. Wir werden innerhalb der nächsten fünf Jahre eine ganze Menge Probleme haben."[1] Diese Worte stammen von *Steve Wozniak*, dem Mitbegründer von Apple, am Rande einer Theatervorstellung in der US-amerikanischen Hauptstadt Washington im Jahre 2012.

Der erste Teil von *Wozniaks* Warnung hat sich bereits bestätigt: Immer mehr Nutzer speichern ihre Daten in der Cloud. Allein Apple hat die Zahl seiner iCloud-Nutzer 2016 auf 782 Millionen ausgebaut.[2] Das 2008 gegründete Unternehmen Dropbox zählte im Juli 2016 500 Millionen Nutzer weltweit.[3] 30 Millionen Nutzer alleine in Deutschland, Österreich und der Schweiz.[4] Bis 2017 sollen 73 % aller Daten „in der Wolke" sein.[5] Diese Zahlen belegen eindrücklich, dass Cloud-Dienste immer beliebter werden. Bei den Nutzern handelt es sich dabei nicht nur um Unternehmen, die den Vorteil nutzen, keine eigenen Ressourcen vorhalten zu müssen, sondern vor allem auch um Private, die mit dem angemieteten Cloud-Speicher die heimische Festplatte ersetzen oder ihre Endgeräte synchronisieren.

Diese Weiterentwicklung führt dazu, dass Ermittlungsbehörden bei ihrer Arbeit zwangsläufig zunehmend mit Cloud-Lösungen in Berührung kommen. Waren beweiserhebliche Gegenstände bei einer Durchsuchung zunächst noch in körperlicher Form in den Räumen des Verdächtigen zu finden, werden die Informationen längst digital gespeichert. Nutzt der Verdächtige einen Cloud-Dienst und speichert so seine Daten über ein externes Datennetz, werden die zuständigen Behörden beim Verdächtigen nur ein Endgerät vorfinden, auf dem möglicherweise nichts gespeichert ist, über welches sie aber auf eine Cloud zugreifen können.

---

[1] Zitiert nach *Fuest*, Die Welt vom 11.08.2012, https://www.welt.de/finanzen/article108575608/Wie-die-Datenwolke-zum-Albtraum-der-Nutzer-wird.html (zuletzt besucht am 20.03.2018).

[2] *Beiersmann* ZDNet, 15.02.2016.

[3] Quelle Dropbox: https://de.statista.com/statistik/daten/studie/326447/umfrage/anzahl-der-weltweiten-dropbox-nutzer/ (zuletzt besucht am 20.03.2018).

[4] Heise Online: https://www.heise.de/newsticker/meldung/Dropbox-eroeffnet-erste-deutsche-Niederlassung-in-Hamburg-3213322.html (zuletzt besucht am 20.03.2018).

[5] *Kroker*, Wirtschaftswoche vom 12.08.2015.

Die vorliegende Arbeit widmet sich der Untersuchung, ob auch die Strafverfolgungsbehörden bei Ermittlungen „in der Cloud“ – um es mit *Wozniaks* Worten zu sagen – „eine ganze Menge Probleme haben“ und wie diese zu lösen sind.

I. Heranführung an den Untersuchungsgegenstand

Hinter dem Konzept des Cloud Computing verbirgt sich zwar keine neue Technik, jedoch eine neue Geschäftsidee, IT-Ressourcen nicht mehr zu besitzen, sondern sie bei Bedarf zuzuschalten, sie als Dienstleistung zu beziehen.[6] Die hinter dem Cloud Computing stehende Virtualisierungstechnik abstrahiert logische Systeme von der physischen Implementierung. Datenspeicherungen oder Programmabläufe werden daher nicht mehr einem klar zu lokalisierenden Server, sondern schlicht der „Cloud“ zugeordnet.[7] Auch wenn alle Vorgänge in der Cloud letztendlich auf eine physische Hardware zurückgeführt werden können, über die ein territorialer Bezug hergestellt werden kann, bereitet die Festlegung eines territorialen Anknüpfungspunktes große Probleme. Die Daten eines Nutzers werden meist nicht en bloc, sondern als Datenversatzstücke gespeichert. Um bei Störungen Dienstunterbrechungen zu vermeiden, legt der Cloud-Anbieter meist noch Sicherungskopien der gespeicherten Daten an, welche wiederum bruchstückhaft gespeichert werden. Auf welche Daten dann im Falle eines Abrufs tatsächlich zugegriffen wird, entscheidet die Virtualisierungstechnik nach Kapazitätsgesichtspunkten.

Für die Wahl der strafprozessualen Ermächtigungsgrundlage ist der tatsächliche Speicherort der Daten jedoch zunächst zweitrangig. Weder die Vorschriften zur Durchsuchung (§§ 102 ff. StPO) und Beschlagnahme (§§ 94 ff. StPO) noch die auf die Herausgabe von Daten gerichteten Normen (§ 95 StPO beziehungsweise §§ 161 Abs. 1, 163 Abs. 1 StPO) oder die Vorschriften zu den heimlichen Ermittlungsmaßnahmen (§ 100a und § 100b StPO) setzen einen bestimmten Speicherort der in Rede stehenden Daten voraus. Dennoch sind die Maßnahmen der Strafverfolgungsbehörden grundsätzlich auf das eigene Hoheitsgebiet beschränkt. Dies ergibt sich aus völkerrechtlichen Grundsätzen, namentlich dem Territorialprinzip, an welches die Ermittlungsbehörden gebunden sind. Findet ein Eingriff in fremde Souveränitätsrechte statt, bedarf dieser einer völkerrechtlichen Rechtfertigung. Ein Eingriff in fremde Hoheitsrechte setzt dabei keinesfalls voraus, dass der Hoheitsakt auf fremdem Staatsgebiet vorgenommen wird, die Behörden sich also physisch auf fremdes Staatsgebiet begeben. Ein Eingriff in fremde Hoheitsrechte liegt möglicherweise bereits dann vor, wenn eine Handlung aus

---

[6] Vgl. *Schorer*, in: Hilber, Teil 1 C, Rn. 7.

[7] So: *Giedke*, Cloud Computing, S. 48; *Lehmann/Giedke*, CR 2013, 608 (611).

dem Inland in fremdes Hoheitsgebiet hineinwirkt. Dies wäre vielleicht auch schon dann der Fall, wenn deutsche Strafverfolgungsbehörden von einem Rechner im Inland auf im Ausland gespeicherte Daten zugreifen. Eine Verletzung fremder Hoheitsrechte liegt ebenfalls vor, wenn die Ermittlungsbehörden eine Person – egal wo sich diese aufhält – zur Herausgabe von im Ausland gespeicherten Daten auffordern, denn in beiden Fällen werden Datenverarbeitungsprozesse im Ausland in Gang gesetzt, die – zumindest mittelbar – auf das Verhalten der Ermittlungsbehörden zurückzuführen sind.

II. Darstellung

Um sämtliche Ermittlungsmöglichkeiten der Strafverfolgungsbehörden im Zusammenhang mit dem Cloud Computing einer rechtlichen Beurteilung zuführen zu können, muss zunächst einmal festgestellt werden, in welchen Situationen die Behörden mit Cloud-basierten Diensten in Berührung kommen können. Im ersten Teil der Arbeit sollen daher zunächst die für die rechtliche Beurteilung der strafprozessualen Ermittlungsmöglichkeiten notwendigen Grundlagen des Cloud Computings erarbeitet werden. Nach einem kurzen Überblick über die historische Entwicklung, der Technologie und der Begriffsbestimmung findet eine Darstellung der technischen Grundlagen statt. Neben den einzelnen Servicemodellen und den verschiedenen Erscheinungsformen werden insbesondere die Virtualisierungstechnik und die damit verbundenen Schwierigkeiten der Lokalisierbarkeit der in der Cloud gespeicherten Daten eingehend beleuchtet. Anschließend werden die beim Cloud Computing anfallenden Daten medienrechtlich kategorisiert. Nach dieser Darstellung wird deutlich, wann die Behörden mit der Cloud des Verdächtigen in Berührung und welche tatsächlichen Zugriffsmöglichkeiten als ermittlungstechnische Ansatzpunkte in Betracht kommen. Zum Ende des ersten Kapitels werden daher denkbare Fallkonstellationen aufgeworfen, die im Fortgang der Arbeit unter allen Aspekten beleuchtet werden. Dabei wird stets davon ausgegangen, dass es sich bei dem Nutzer des Cloud-Dienstes um den Verdächtigen handelt, gegen den das Ermittlungsverfahren eingeleitet beziehungsweise die spätere Hauptverhandlung geführt werden soll. Die Untersuchung beschränkt sich dabei auf die Ermittlungen gegen Nutzer von Storage as a Service (StaaS)- beziehungsweise Infrastructure as a Service (IaaS)-Angeboten. Die denkbaren Fallkonstellationen werden einer Grobgliederung unterworfen, die für die weitere Struktur der Arbeit prägend ist. Anknüpfungspunkt ist der Zugriff am Ort des verdächtigen Cloud-Nutzers selbst über den unverdächtigen Cloud-Anbieter und in der Phase der Übertragung der Daten in und aus der Cloud.