Senta Bell: Strafverfolgung und die Cloud
Strafprozessuale Ermächtigungsgrundlagen und deren völkerrechtliche Grenzen

von Prof. Dr. Anja Schiemann

2019, Duncker & Humblot, ISBN: 978-3-428-15620-7, S. 225, Euro 79,90.

Die Dissertation von *Bell* zu Strafverfolgung und der Cloud wurde im Sommersemester 2018 eingereicht, so dass der Vorschlag einer Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen leider nicht in die Überlegungen mit einbezogen werden konnte. Gleichwohl handelt es sich um eine umfassende rechtliche Würdigung sämtlicher Ermittlungsmöglichkeiten der Strafverfolgungsbehörden im Zusammenhang mit dem Cloud Computing. Da angesichts der Kritik an dem Verordnungsvorschlag eine europäische Lösung vermutlich ohnehin noch auf sich warten lässt, bietet die vorliegende Arbeit einen guten Überblick über die derzeit bestehenden strafprozessualen Ermächtigungsgrundlagen und deren völkerrechtliche Grenzen.

Nach einer historischen Einführung nimmt die Verfasserin eine kurze Begriffsbestimmung vor, wobei sie angesichts der unterschiedlichen Definitionsansätze zum Cloud Computing letztlich auf eine kritische Auseinandersetzung mit den einzelnen Definitionen verzichtet (S. 25). Sie versteht unter Cloud Computing ein komplexes und dynamisches Angebot von Software- und Hardwareleistungen, die über ein Netzwerk „aus der Wolke“ zur Verfügung gestellt werden (S. 25 f.).

Der folgende Abschnitt zu den technischen Grundlagen macht deutlich, dass sich die Probleme bei der Lokalisierung der in der Cloud gespeicherten Daten daraus ergeben, dass dem Nutzer regelmäßig nur ein virtueller Speicherplatz zugewiesen wird. Zwar befinden sich die in der Cloud gespeicherten Daten letztlich auf einem reellen physischen Speichermedium, der Speicherort der Daten kann sich aber je nach Auslastung sehr kurzfristig ändern.

Die Verfasserin zeigt vielfältige Möglichkeiten auf, aus technischer und ermittlungspraktischer Sicht auf in der Cloud gespeicherte Inhalte zuzugreifen. Sie identifiziert 15 Fallgruppen (S. 53 ff.), die die Grundlage für die weitere Untersuchung bilden. Deutlich wird, dass die hinter dem Cloud Computing stehende Virtualisierungstechnik regelmäßig zu einer Konfrontation der Ermittlungsbehörden mit grenzüberschreitenden Sachverhalten führt, so dass völkerrechtlichen Anforderungen neben den deutschen strafprozessualen Ermächtigungsgrundlagen eine entscheidende Rolle zukommt (S. 56 f.).

Bell steckt zunächst den verfassungsrechtlichen Rahmen ab (S. 58 ff.), um dann dezidiert zu den strafprozessualen Ermächtigungsgrundlagen Stellung zu beziehen (S. 75 ff.). Sie kommt zu dem Ergebnis, dass Strafverfolgungsbehörden am Ort des verdächtigen Cloud-Nutzers sowohl die lokal gespeicherten Daten als auch die im externen Cloud-Speicher abgelegten Daten gem. § 102 StPO offen durchsuchen bzw. gem. § 110 Abs. 1 und 3 StPO offen durchsehen können. Auch bestehende Zusatzsicherungen dürfen überwunden werden. Die beweiserheblichen Daten können dann nach §§ 94 ff. StPO sichergestellt bzw. beschlagnahmt werden. Sollten die Strafverfolgungsbehörden am Durchsuchungsort noch nicht feststellen können, ob es sich um beweiserhebliche Daten handelt, könnten die Daten auch gem. § 110 StPO zur Durchsicht mitgenommen werden. Dies setze aber bei in der Cloud gespeicherten Daten voraus, dass sie vorher auf einem lokalen Speichermedium der Strafverfolgungsbehörden gespeichert werden.

Neben einer offenen Durchsuchung beim verdächtigen Cloud-Nutzer käme zudem unter den strengen Voraussetzungen des § 100b StPO im Wege einer Online-Durchsuchung ein heimlicher Zugriff in Frage.

Im Falle des Zugriffs am Ort des Cloud-Anbieters auf Inhaltsdaten des verdächtigen Cloud-Nutzers, käme – je nach Kooperationsbereitschaft – eine Durchsuchung gem. § 102 oder § 103 StPO in Betracht. Wüssten die Strafverfolgungsbehörden, dass der verdächtige Cloud-Nutzer beweiserhebliche Daten in der Cloud gespeichert hat, könnten diese gem. § 95 StPO vom Cloud-Anbieter herausverlangt werden.

Sonstige Daten könnten vom Cloud-Anbieter über die Ermittlungsgeneralklausel gem. §§ 161, 163 StPO i.V.m. Art. 6 Abs. 1 lit. f DSGVO und § 24 Abs. 1 Nr. 1 BDSG herausverlangt werden.

Gesetzt den Fall, die Ermittlungsbehörden wollten die Inhaltsdaten des verdächtigen Cloud-Nutzers während der Übertragungsphase heimlich abfangen, käme § 100a StPO als Ermächtigungsgrundlage in Betracht. Der Datentransfer wäre aber nur dann als Telekommunikation zu qualifizieren, wenn der Cloud-Nutzer die Dienste des Cloud-Storage-Anbieters ausschließlich nutzt, um mit Dritten zu kommunizieren. Nur dann käme eine Telekommunikationsüberwachung nach § 100a StPO in Betracht.

Nachdem *Bell* das strafprozessuale Werkzeug im Hinblick auf die unterschiedlichen Fallkonstellationen vorgestellt hat, nimmt sie sich im dritten Kapitel der völkerrechtlichen Begrenzung der Ermittlungsbefugnisse an (S. 157 ff.). Sie stellt fest, dass der Zugriff auf im Ausland nicht öffentlich zugänglich gespeicherten Daten mit der

Zustimmung des Berechtigten gem. Art. 32 lit. b CCC oder über international anerkanntes Gewohnheitsrecht gerechtfertigt sein kann. Überwöge das Interesse des eingreifenden Staates das Abwehrinteresse des betroffenen Staates, so könne der Eingriff ausnahmsweise gerechtfertigt sein. Ein solch gewichtiges Interesse nimmt die Verfasserin bei Staatsschutzdelikten an, die den Bestand des handelnden Staates bedrohen oder zu einer schweren Erschütterung der inneren Sicherheit führen (S. 171).

Ob und unter welchen Voraussetzungen ein Verstoß der Strafverfolgungsbehörden gegen das Souveränitätsrecht fremder Staaten zu einem Verwertungsverbot im Strafprozess führt, will *Bell* zwar eigentlich nicht beleuchten (S. 173), positioniert sich dann aber doch: Die Annahme eines Beweisverwertungsverbots scheint ihr fraglich zu sein, da die Einhaltung der Verfahrensvorschiften dem Schutz des Beschuldigten dient. Aus den völkerrechtlichen Hoheitsrechten ließen sich jedoch keine subjektiven Rechte des Betroffenen ableiten (S. 174). Das ist meiner Meinung nach zu kurz gegriffen und die Verfasserin hätte gut daran getan, hier doch dezidierter Stellung zu nehmen, zumal es sich nicht erschließt, warum diese doch sehr wichtige praktische strafprozessuale Frage ausgeklammert wird.

Bell widmet sich dann noch der Fallkonstellation, nach der nicht geklärt werden kann, wo sich der tatsächliche Speicherort befindet und mehrere Länder für den Datenverarbeitungsprozess in Betracht kommen. Der „eigene Lösungsansatz", den sie präsentiert, ist eigentlich der von *Wicker*, auf die sie allerdings auch Bezug nimmt (S. 180 ff.). Ein Zugriff auf einen Cloud-Server mit grenzüberschreitenden Serverfarmen sei völkerrechtlich nicht zu beanstanden, so lange der Serververbund auch den handelnden Staat mit umfasst. Denn dann läge entweder tatsächlich überhaupt kein Eingriff in fremde Hoheitsrechte vor oder der Eingriff sei völkerrechtlich gerechtfertigt, da das Eingriffsinteresse das Abwehrinteresse des betroffenen Staates überwiegt (S. 184). Warum hier das Abwehrinteresse des betroffenen Staates ein geringes sein soll, nur weil die Daten verschoben werden können, bleibt aber unklar. Denn befinden sich die Daten auf einem ausländischen Server, bleibt das Eingriffsinteresse sowie das Abwehrinteresse gleich den Fallkonstellationen, in denen sich die Daten von vornherein und ausschließlich auf dem ausländischen Server befinden.

Anschließend widmet sich die Verfasserin dem Herausgabeanspruch. Sie kommt zu dem Ergebnis, dass die CCC umfassende Rechtfertigungsmöglichkeiten für das auf im Ausland gespeicherte Daten gerichtete Herausgabeverlangen bereithält (Art. 18 Abs. 1 CCC). Allerdings ist nach der Datenart zu differenzieren (S. 191).

Im letzten Kapitel zeigt *Bell* verbleibenden Handlungsbedarf auf (S. 195 ff.). Auch wenn sich die Cloud mit den bestehenden strafprozessualen Mitteln durchaus erschließen lässt, ergäben sich insbesondere bei der Frage nach der völkerrechtlichen Zulässigkeit strafprozessualer Ermittlungstätigkeiten in der Cloud Probleme (S. 220). So schlägt sie vor, Cloud-Anbieter auf internationaler und nationaler Ebene gesetzlich zu verpflichten, die Standorte der Server hinsichtlich der Staatsgrenzen verbindlich festzulegen. Hierdurch könne nicht nur das Handeln der Strafverfolgungsbehörden in völkerrechtlicher Hinsicht aus der bestehenden Grauzone gehoben werden, sondern auch für den Nutzer wäre eine Offenlegung der Speicherorte ein Zugewinn an Transparenz (S. 221). Auch sollte der Cloud-Anbieter verpflichtet werden, die Zugangsdaten vorzuhalten (S. 222).

In völkerrechtlicher Hinsicht sieht *Bell* Novellierungsbedarf der CCC, da diese nur unzureichende Rechtfertigungstatbestände bezüglich der im Ausland gespeicherten Daten bereithält (S. 224). Schade, dass sich die Verfasserin noch nicht mit dem Vorschlag einer Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen befassen konnte. Dennoch bietet die Dissertation eine wichtige Grundlagenarbeit, die den Status quo strafprozessualer Ermittlungsmöglichkeiten in der Cloud aufzeigt und – wenn auch leider nur sehr zurückhaltend – Handlungsbedarfe aufzeigt. Konsequent ist dies aber schon allein deshalb, weil die Verfasserin im Fahrwasser von *Wicker* und *Meyer-Goßner/Schmitt* keine Probleme damit hat, den Strafverfolgungsbehörden Zugriff auf Clouddaten zu gewähren, sobald die Daten auch in Deutschland gespeichert sein könnten. Dies ist sicher ein streitbarer Punkt, aber durchaus vertretbar. Recht zu geben ist *Bell* darin, dass – auch angesichts der insoweit zumindest strittigen und unklaren Rechtslage – die völkerrechtlichen Möglichkeiten und Grenzen von Ermittlungen in der Cloud gesetzlich konkretisiert und präzisiert werden sollten.