Die Erhebung digitaler Beweismittel im Strafprozess – Unter besonderer Berücksichtigung grenzüberschreitender Aspekte

Mathias Eberli

Mathias Eberli, MLaw Rechtsanwalt, CAS Forensics, Staatsanwalt bei der Staatsanwaltschaft III des Kantons Zürich

Mathias Eberli beschäftigt sich beruflich hauptsächlich mit der Verfolgung schwerer Wirtschaftsdelikte. Zuvor war er während knapp fünf Jahren als Staatsanwalt für allgemeine Delikte tätig und besuchte den Studiengang MAS Economic Crime Investigation 15/17 am Institut für Finanzdienstleistungen der Hochschule Luzern. Abschluss dieser Weiterbildung bildete seine Masterarbeit über die Erhebung digitaler Beweismittel im Strafprozess.

Im Strafprozess von heute nehmen digitale Daten eine zunehmend wichtige Rolle als Beweismittel ein. Dabei befinden sich die Daten oftmals nicht mehr auf dem heimischen Computer, sondern auf einem Datenträger in einem Datencenter eines Clouddienstanbieters irgendwo auf der Welt. Dies stellt die Strafverfolgungsbehörden vor grosse Herausforderungen: Während der klassische Rechtshilfeweg für die Erhebung digitaler Daten oftmals träge ist, sind alternative Wege wie die internationale Polizeizusammenarbeit, Spezialabkommen oder die freiwillige Kooperation von Serviceprovidern mit den Behörden im Anwendungsbereich häufig eng beschränkt oder wenig verlässlich.

Die Strafverfolgungsbehörden kämpfen weltweit mit ähnlichen Problemen. Als Ansatz zur Erleichterung des Datenzugriffs setzen einzelne Länder Speicherortvorgaben ein und zwingen Serviceprovider so zur Datenspeicherung im Inland. Solche Regeln lassen sich gegen ausländische Serviceprovider jedoch nur schwer durchsetzen. Verbreiteter ist daher der Ansatz, die eigene Gebietshoheit mit Bezug auf digitale Daten weiter zu interpretieren als nach dem traditionellen Verständnis des Territorialitätsprinzips. So tendiert die Rechtsprechung verschiedener Staaten dazu, neben dem physischen Speicherort digitaler Daten vermehrt den Ort der effektiven Zugriffsmöglichkeit auf die Daten als entscheidender Faktor für die Befugnis zu hoheitlichem Handeln anzusehen. Auch jüngere Entscheide des Bundesgerichts deuten in diese Richtung: Gemäss BGE 143 IV 21 ff. und 1B_142/2016, beide aus dem Jahr 2016, kann eine Schweizer Gesellschaft, die über direkten Zugang zu beweisrelevanten Daten verfügt, von den Schweizer Strafverfolgungsbehörden unabhängig vom physischen Speicherort dieser Daten zur Herausgabe angehalten werden. Gemäss BGE 143 IV 270 ff. aus dem Jahr 2017 handelt eine Strafverfolgungsbehörde, die über einen Internetzugang im Inland auf digitale Beweismittel im Ausland zugreift, sodann nicht im Ausland.

Der physische Speicherort insbesondere von Daten in der Cloud ist heutzutage oftmals nicht zuverlässig ermittelbar. Eine weite Interpretation des Territorialitätsprinzips bei digitalen Daten scheint daher richtig. Die Probleme sind damit aber nicht vom Tisch. So versagt ein weites Verständnis der eigenen Territorialität, wenn die zu erhebenden Daten im Ausland gespeichert sind, die Strafverfolgungsbehörde keinen direkten Zugriff auf die Daten hat und der Inhaber nicht unter das Recht der betreffenden Behörde fällt. Der zentrale Lösungsansatz für den grenzüberschreitenden Zugriff auf digitale Daten muss daher sein, das Rechtshilfeverfahren insgesamt zu modernisieren. Auf internationaler Ebene ist diesbezüglich einiges im Gang: Die USA haben im Frühjahr 2018 den CLOUD-Act in Kraft gesetzt. Dieser eröffnet anderen Staaten die Möglichkeit, mit den USA ein bilaterales Abkommen abzuschliessen, das ihre Strafverfolgungsbehörden ermächtigen würde, US-Serviceprovider direkt aus dem eigenen Land heraus und nach eigenen Verfahrensregeln zur Herausgabe von Daten aufzufordern. Auf EU-Ebene wird derzeit ebenfalls über ein neues Gesetzespaket debattiert, das innerhalb der EU den direkten Verkehr von Strafverfolgungsbehörden und Serviceprovidern etablieren soll. Auch bestehen auf Ebene des Europarates Bestrebungen, ein zweites Zusatzprotokoll zur Cybercrime-Konvention zu verabschieden, mit dem die Rechtshilfe innerhalb der Mitgliedstaaten vereinfacht werden soll.

Die Schweiz tut gut daran, sich aktiv an den Arbeiten für ein zweites Zusatzprotokoll zur Cybercrime-Konvention zu beteiligen. Daneben muss für sie prioritär sein, sich um ein Verhandlungsmandat mit den USA zum Abschluss eines bilateralen CLOUD-Act-Abkommens zu bemühen. Ein solches Abkommen würde Beweiserhebungen mit US-Bezug massiv vereinfachen und beschleunigen. Angesichts der enormen Bedeutung von US-Techfirmen im Bereich der digitalen Datenspeicherung wäre damit schon einiges erreicht.

Hochschule Luzern - Wirtschaft
Institut für Finanzdienstleistungen Zug IFZ
Suurstoffi 1
CH-6343 Rotkreuz
+41 41 757 67 67
ifz@hslu.ch