Ermittlungsbefugnisse über Grenzen hinweg! – Sind nationale Zuständigkeiten bei der Bekämpfung der Cyberkriminalität noch zeitgemäß?

Diskussionsveranstaltung in der Landesvertretung NRW in Brüssel am 22.02.2018

„Das Internet kennt keine Grenze!

Immer mehr Straftaten werden im sogenannten Cyberspace begangen und verursachen dabei erheblichen wirtschaftlichen und sozialen Schaden. Eine beträchtliche Anzahl der Delikte bleibt jedoch ungeahndet, weil zum einen die Fälle nicht gemeldet werden, lange Ermittlungszeiten und ein erschwerter Zugang zu elektronischen Beweismitteln für die Strafverfolgungsbehörden bestehen. Denn die Strafverfolgungsbehörden sind in ihren Eingriffsbefugnissen auch bei Ermittlungen im Internet an den Souveränitätsgrundsatz gebunden, der ihnen hoheitliche Eingriffe in die Internetinfrastruktur auf dem Gebiet ausländischer Staaten verbietet. Da die relevanten Serviceprovider und die Infrastruktur häufig in anderen europäischen Mitgliedstaaten oder Drittstaaten wie z.B. den USA angesiedelt sind, haben die Strafverfolgungsbehörden häufig Schwierigkeiten, einen erfolgreichen Zugang zu den „elektronischen Beweismitteln (electronic evidence)“ zu bekommen, Die Ermittlungstätigkeit hat daher grenzüberschreitende Implikationen, weswegen die Behörden bisher auf justizielle Zusammenarbeit wie Rechtshilfe oder, innerhalb der EU, gegenseitige Anerkennung oder direkte Zusammenarbeit mit Serviceprovidern angewiesen sind. Diese Ermittlungskanäle sind jedoch häufig aufwendig und haben eine lange Verfahrensdauer.

Der Rat der Innen- und Justizminister hat daher bereits im Juni 2016 eine Verbesserung der Strafjustiz im Cyberspace angemahnt. Für den besseren Zugang zu „elektronischen Beweismitteln“ sei ein europäischer Rechtsrahmen vonnöten, einschließlich harmonisierter Vorschriften für die Bestimmung des Status eines inländischen oder ausländischen Anbieters. Aktuell hat die Kommission einen Gesetzgebungsvorschlag hierzu angekündigt, der voraussichtlich im Laufe des Jahres beschlossen wird. Seit Mai 2017 besteht bereits das Instrument der „Europäischen Ermittlungsanordnung (EEA)“, mit welchem die Justizbehörde eines EU-Mitgliedstaats („Anordnungsstaat“) grenzüberschreitend einen anderen Mitgliedstaat („Vollstreckungsstaat“) in Strafverfahren zur Durchführung von Ermittlungsmaßnahmen in Strafverfahren oder Überlassung von Ermittlungsergebnissen ersuchen kann. Einen konkreten gesetzlichen Rahmen für den Zugang zu „elektronischen Beweismitteln“ enthält die Europäische Ermittlungsanordnung jedoch nicht.

Doch welche Konsequenzen hätte die Zulassung grenzüberschreitender Ermittlungsbefugnisse für Polizei- und Justizbehörden hinsichtlich des Schutzes der Grundrechte und insbesondere der datenschutzrechtlichen Gewährleistungen? Was bedeutet dies für einen Wirtschaftsstandort, dessen Reputation im Bereich IT-Dienstleistungen von einem hohen Datenschutzstandard abhängt?

Diese und andere Fragen waren Gegenstand der Diskussionsveranstaltung in der Landesvertretung NRW in Brüssel am 22.02.2018, zu welcher der Justizminister des Landes NRW, Herr Peter Biesenbach, eingeladen hatte. In seiner Begrüßungsrede betonte der Justizminister den unaufhaltsamen Prozess, der zur Digitalisierung des Lebens führe und dass der Cyberspace keine nationalen Grenzen mehr kenne. Dies zeige auch der derzeit beim US Supreme Court anhängige Fall „US vs. Microsoft“, in welchem sich Microsoft gegen die Überlassung von außerhalb der USA gespeicherten Daten (nämlich Account-Daten eines Nutzers auf einem Rechner in Irland) an US-Behörden wehrt. Zurzeit bestehe das Problem, dass die grenzüberschreitende Kooperation der Ermittlungsbehörden hinsichtlich der Verfolgung von Straftaten im Cyberspace zu viel Zeit in Anspruch nehme. So würden z.B. Rechtshilfeersuchen an die USA bis zu 10 Monate dauern. Zudem würden sich die verschiedenen nationalen Rechtsordnungen teilweise überlagern und zueinander im Widerspruch stehen. Aus diesem Grunde seien Lösungen auf internationaler Ebene, die schnell und effektiv seien und einen klaren Rechtsrahmen bieten würden, erforderlich und in Gestalt einer Initiative der Europäischen Kommission zu begrüßen.

In Anschluss an diese einleitenden Worte trug Herr Oberstaatsanwalt Hartmann von der Zentralen Ansprechstelle Cyberkriminalität NRW (ZAC NRW) seine Erfahrungen aus der täglichen Praxis der internationalen Rechtshilfe vor. Das ZAC ist in herausgehobenen Fällen der Cyberkriminalität zuständig und unterstützt die Justiz in Zusammenarbeit mit der Polizei bei der Aufklärung von hochtechnischen Sachverhalten. Herr Hartmann machte anhand von Fallbeispielen deutlich, dass in Fällen der Cyberkriminalität Daten teilweise innerhalb von Stunden ihre Standorte wechseln würden, was ein sehr zeitnahes Handeln erforderlich mache, um erfolgreich zu sein. Aus seiner Sicht sei es für eine erfolgreiche Bekämpfung der Cyberkriminalität sinnvoll, die Prozesse zu vereinfachen und zu verschlanken und den Zeitansatz zu optimieren. Die internationale Zusammenarbeit der Strafverfolgungsbehörden müsste noch weiter verstärkt und praktikabler gestaltet werden, wie z.B. durch sog. Joint Investigation Teams unter Einbeziehung von Eurojust oder dadurch, dass durch Zertifikat berechtigte Personen in einem schnellen Verfahren Rechtshilfeersuchen stellen könnten. Zusätzlich könne Art. 32 der Cybercrime-Convention von 2001, der bereits einen rechtlichen Rahmen für den direkten Zugriff auf Zugangsdaten eines Nutzers bei vorliegendem Einverständnis des Beschuldigten biete, geändert werden.

Frau Claudia Warken, Nationale Sachverständige in der Europäischen Kommission in der Generaldirektion Migration und Inneres, erklärte, dass innerhalb der Kommission eine Taskforce für die Erstellung eines Gesetzgebungsvorschlags zu dem heutigen Thema bestehe. Aufgrund der Komplexität der Thematik und des internen kommissionsweiten Abstimmungsbedarfs stehe jedoch der genaue Termin der Veröffentlichung eines solches Vorschlags noch nicht fest. Sie beleuchtete die derzeit bestehenden Probleme aus Sicht der Strafverfolgungsbehörden und aus Sicht des Internetservicedienstleisters. Als praktische Maßnahmen zur Verbesserung der Bekämpfung der Cyberkriminalität zeigte sie einerseits auf, dass in den Mitgliedstaaten zentrale Anlaufstellen gebildet werden könnten, wie z.B. in Finnland, wo alle Rechtshilfeersuchen über eine zentrale Stelle liefen. Des Weiteren sollten die Verfahren weiter standardisiert werden, in dem u.a. einheitliche Antragsformulare verwendet würden. Auch sei eine verbesserte Kommunikation mit US-amerikanischen Behörden und Dienstleistern erforderlich, weswegen Europol zuletzt Fördermittel erhalten habe. Die Rechtshilfeverfahren könnten dadurch verbessert werden, dass das bereits vorhandene Instrument der Europäischen Ermittlungsanordnung (EEA) auf elektronische Daten zugeschnitten werde. Letztlich solle bis Ende 2019 eine Online-Plattform bereitstehen, über welche Anfragen

über EEA direkt gestellt und beantwortet werden könnten.

Prof. Dr. Christoph Burchard, Professor für Straf- und Strafprozessrecht, Internationales und Europäisches Strafrecht an der Goethe-Universität Frankfurt am Main, betonte in seinem Vortrag, dass bei jeglicher zukünftigen Regelung die Grundprinzipien der internationalen Zusammenarbeit wie Souveränität und Territorialhoheit, Solidarität und Grundrechtsschutz weiterhin beachtet werden sollten. Auch spiele insoweit das Nutzervertrauen in den territorial verankerten Datenschutz eine wichtige Rolle. Als gangbaren Weg, der diese Prinzipien einhalte, zeigte er einen sog. „unechten" unilateralen Zugriff auf Daten mit Zustimmung des Staates auf, in dem die Daten belegen sind. Eine solche gegenseitige Anerkennung von Direktzugriffen und Beibringungsanordnungen dürfe jedoch nicht „blind" laufen. Es bedürfe Zustimmungsverweigerungs-/widerrufsgründe, wie z.B. einen Missbrauchsverweigerungs-grund.

Als letzter Redner hielt Herr Thomas Langkabel, National Technology Officer bei Microsoft, einen anschaulichen Vortrag über die Herausforderungen und Lösungsansätze aus Anbieterperspektive. Er stellte heraus, dass Microsoft Cloud in über 100 Rechenzentren in 40 Ländern und 38 Regionen bestehen würde. Dies biete dem Kunden die Möglichkeit, zu entscheiden, in welcher Region die Daten gespeichert werden sollten, der Kunde habe also selbst die Steuerungsmöglichkeit und könne daher auch entscheiden, ob sein Anbieter dem europäischen Datenschutzrecht unterliege. Microsoft selbst habe ein internes Compliance Team, welches sich ausschließlich mit externen Anfragen nach Daten (z.B. im Zeitraum Jan-Juni 2017 allein aus Deutschland 3.409 Auskunftsersuchen) beschäftige. Dabei würde intern die Leitlinie gelten, dass nur spezifizierte Anfragen beantwortet und nur die aufgeführten Daten bearbeitet würden. Zudem verweise Microsoft die Behörden, jedenfalls bei Firmen mit betroffenen Mitarbeitern, immer an die Kunden selber. Auf Kundendruck hin habe Microsoft nunmehr das „sog. Souveräne Cloud Modell" in Deutschland geschaffen, welches aus zwei deutschen Rechenzentren in Frankfurt a.M. und in Magdeburg bestehe. Diese seien eigenständige, deutsche, vom öffentlichen Internet getrennte Datennetzwerke. Sämtliche Kundendaten und erforderliche System könnten in den deutschen Rechenzentren gelagert werden, wobei ausschließlich ein deutscher Datentreuhänder (und nicht mehr Microsoft) die Kontrolle über den Zugang zu den Kundendaten habe.