VERBAND DER INTERNETWIRTSCHAFT E.V.

Eckpunkte:

Zum Inception Impact Assessment der Europäischen Kommission „Improving cross-border access to electronic evidence in criminal cases”

Berlin, 31. August 2017

Mit dem Inception Impact Assessment (IIA) der Europäischen Kommission sollen die Grundlagen für einen grenzübergreifenden Zugriff auf Daten und Informationen geregelt werden, die im Zuge der Strafverfolgung zum Einsatz kommen. eco - Verband der Internetwirtschaft verfolgt die Entwicklungen in diesem Themenbereich. Die Mitglieder des eco sind sowohl Anbieter von Telekommunikationsdiensten als auch von Telemediendiensten. Beide stehen damit im Spannungsverhältnis: Einerseits sollen sie hochwertige und vertrauenswürdige Dienstleistungen erbringen, das Fernmeldegeheimnis und den Grundrechtsschutz ihrer Kunden gewährleisten. Andererseits sollen sie, wo es geboten erscheint, an der Bekämpfung von schwerer und organisierter Kriminalität und in zunehmendem Umfang auch an einfacher Kriminalität mitwirken. Dieses Spannungsverhältnis stellt Diensteanbieter seit jeher vor Herausforderungen. Vor allem, wenn sie ihre Angebote grenzübergreifend zur Verfügung stellen, ist dies für Diensteanbieter wegen der unterschiedlichen Rechtsordnungen in den verschiedenen Mitgliedsstaaten eine besondere Situation.

Bei grenzübergreifenden Ermittlungen kann es aufgrund der nationalen Zuständigkeiten und der Territorialität des Rechts daher zu Problemen kommen. Das vorliegende IIA zeigt als mögliche Auflösung des von der EU Kommission antizipierten Durchsetzungsdefizits beim grenzübergreifenden Zugriff auf elektronische Daten eine umfassende Sammlung an Regeln auf.

Das IIA der Kommission führt mehrere Optionen für legislative Maßnahmen im Rahmen einer Richtlinie an, wobei es sich dabei noch um keine finalisierte Position der Kommission handelt:

Diskutiert wird in dem IIA ein Rechtsrahmen, der die Behörden zu direkten Anordnungen an Betreiber in Drittstaaten ermächtigt soll, sofern es sich um im Unionsgebiet verarbeitete Beweismittel handelt. Die Kommission wirft in ihrem IIA zwei Möglichkeiten einer Regelung auf:

- Es liegt im Ermessen des Betreibers ob dieser der Anordnung direkt nachkommt oder nicht,
- der Betreiber ist verpflichtet einer solchen Anordnung direkt nachzukommen.

Dieses im IIA diskutierte System könnte durch eine Verpflichtung für in Drittstaaten ansässige Betreiber ergänzt werden, die in der EU Dienstleistungen anbieten, einen gesetzlichen Vertreter in der EU für Zwecke der Zusammenarbeit auf der Grundlage solcher Anordnungen zu benennen.

Auch wird ein Rechtsrahmen aufgeworfen, welcher Strafverfolgungsbehörden den Zugang zu e-Evidence ohne Beteiligung des Betreibers oder des Eigentümers der Daten ermöglicht, etwa durch ein beschlagnahmtes Gerät oder ein Informationssystem. Dieses Modell könnte auch in Bezug auf Daten zur Anwendung kommen, deren Speicherort nicht bekannt ist oder Daten, die außerhalb der Union gespeichert sind.
Zuletzt werden noch Regeln erwähnt, durch welche die Arten von e-Evidence sowie die Betreiber, die in den Anwendungsbereich der vorgeschlagenen Maßnahmen fallen, näher definiert werden sollen.

I. Allgemeine Vorbemerkungen

eco unterstützt Initiativen zur Verbesserung der Strafverfolgung im Internet. Diese müssen aber verhältnismäßig in Bezug auf ihren Anwendungsbereich sein, zu dem im vorliegenden IIA keine Angaben gemacht werden, und in Bezug auf der Intensität des Eingriffs auch in der Rechtfertigung gegenüber Bürgerinnen und Bürgern. Letzteres ist mit dem vorliegenden IIA nicht erfolgt.

Aus Sicht des eco sind daher bei der weiteren Prüfung von gesetzgeberischen Maßnahmen auf europäischer Ebene folgende Aspekte allgemein zu gewährleisten:

- **Rechtsstaatlichkeit der Verfahren**
  eco hat Bedenken bezüglich der rechtsstaatlich sicheren Ausgestaltung eines grenzübergreifenden Mechanismus zur elektronischen Beweissicherung. Der Zugriff auf elektronische Kommunikations- und Verbindungsdaten stellt immer einen mehrseitigen Grundrechtseingriff dar, welcher in Deutschland unter der engen juristischen Auflage eines Richtervorbehalts steht. Entsprechende Sicherungsmaßnahmen sind im Ausland oftmals nicht vorhanden, so dass hier insbesondere bei Grundrechtsträgern das Risiko einer Verletzung der Grundrechte bzw. bei Providern die Verpflichtung zur Mitwirkung an einer solchen besteht.

- **Hoheitliche Aufgaben nicht an Provider übertragen**
  eco sieht in dem vorliegenden Entwurf das Problem, dass das Herkunftslandprinzip der e-Commerce Richtlinie (Erwägungsgrund 22 und Artikel 3 Richtlinie 2000/31/EG) untergraben werden könnte, da das geplante Regime den unmittelbaren Zugriff weiterer Behörden aus EU-Mitgliedsstaaten auf die Daten und Informationen von Telekommunikations- und Telemediendiensten ermöglicht. Die Verschiebung hoheitlicher Aufgaben auf Betreiber von Diensten lehnt eco ab. Eine Verbesserung der Zusammenarbeit von Ermittlungsbehörden bei der Strafverfolgung ist in diesem Kontext der sinnvollere und nachhaltige Weg zur Rechtsdurchsetzung. Der Datenschutz und das Fernmeldegeheimnis dürfen nicht aufgeweicht werden. Dies ist sowohl im Interesse der Rechtssicherheit von Unternehmen, die vertrauenswürdige

und zuverlässige Dienste anbieten, als auch im Sinne der Rechtssicherheit der Nutzer solcher Dienste.

- **Aufwand für Unternehmen muss transparent werden**
  Das IIA sieht zwei verschiedene Lösungen für den Umgang mit den Anfragen von Ermittlungsbehörden aus EU-Staaten vor. In beiden Fällen muss gewährleistet bleiben, dass der erhebliche personelle und sachliche Aufwand, vor den Unternehmen durch solche Anfragen gestellt werden, beherrschbar bleibt. Das IIA macht derzeit keine Angaben zur Rechtssicherheit und zu Haftungsfragen für Unternehmen im Rahmen der Bearbeitung von Anfragen.

II. Zu den Vorschlägen im Einzelnen

Zu den Vorschlägen der Kommission hat eco folgende Anmerkungen:

- **Rechtlicher Rahmen zum grenzübergreifenden Zugriff auf elektronische Beweismittel**
  Das IIA sieht im Rahmen legislativer Optionen vor, dass „ein Rechtsrahmen, der es Behörden ermöglicht, einen Diensteanbieter in einem anderen EU-Mitgliedsstaat unmittelbar darum bitten oder ihn dazu verpflichten können, elektronische Beweismittel, die innerhalb der EU verarbeitet wurden, herauszugeben, sowie dafür angemessene Sicherheitsmaßnahmen und Bedingungen.[1]“ Im weiteren werden zwei Optionen eröffnet, die Diensteanbieter dazu verpflichten, die Beweise zu übermitteln, bzw. die die Übermittlung dem Diensteanbieter überlassen. Eine direkte Übermittlung von Daten und Informationen auf Anfrage einer ausländischen Stelle ist problematisch. Je nach Land, geltender Strafgesetzgebung, bestehenden Sicherheitsauflagen und Behördenstruktur sind die Regeln für eine Verpflichtung zur Herausgabe von Daten unterschiedlich. Eine direkte Übermittlung greift aber in die Unabhängigkeit von Telemedien- und Telekommunikationsdiensten ein. Für diese existiert aber bereits ein exakt beschriebenes und mit Sicherheitsauflagen unterlegtes nationales Rechtsgefüge. Unter anderem das BKA-Gesetz, verschiedene Landespolizeigesetze, das G-10-Gesetz, das Telekommunikations- und das Telemediengesetz, die Strafprozessordnung und weitere Verordnungen enthalten präzise Vorgaben dazu, unter welchen Rahmenbedingungen welche Behörden wie auf verschiedene Informationssysteme und Daten zugreifen dürfen und welche Auflagen sie vor einem Zugriff bzw. der Erwirkung einer Herausgabe zu erfüllen haben.
  Auch durch die e-Commerce Richtlinie sind bereits genügend Regeln definiert, welche vorgeben, unter welchen Rahmenbedingungen Daten herausgegeben werden können. Die bestehenden Mechanismen der

[1] Eigene Übersetzung.

gegenseitigen Rechtshilfe (MLAT) und der europäischen Ermittlungsanordnung in Strafsachen ergänzen dieses Rechtsgefüge und stellen gleichzeitig sicher, dass auch im Ausland nur befugte Stellen Zugang zu den entsprechenden Informationen erhalten.
Unternehmen müssten - sollte dieser Ansatz geändert werden - zukünftig deutlich mehr Ressourcen für die Überprüfung der Rechtmäßigkeit von Anfragen und deren Bearbeitung vorhalten. Eine Gewährleistung, wie sie mit dem bestehenden System existiert, ist mithin nicht mehr gegeben. Stattdessen werden Unternehmen für die Ausführung hoheitlicher Aufgaben herangezogen. Es besteht zudem die Herausforderung bei Diensteanbietern, dass diese auf die Anfragen in allen EU-Amtssprachen reagieren können müssten, was erhebliche Mehrkosten im Personalbereich mit sich bringen würde, da entsprechende Kapazitäten redundant und ständig vorgehalten werden müssten.
Unklar ist auch, wie Anbieter mit Anfragen umzugehen haben, die im Sitzland des Dienstes keinen Straftatbestand darstellen.
Problematisch sind zudem Ausführungen zu Ansprechpartnern für Dienste, die innerhalb der EU angeboten werden, ihren Sitz aber nicht dort haben.
Die Aushöhlung rechtsstaatlicher Prinzipien ist - auch im Rahmen der Strafverfolgung - nicht akzeptabel. Sinnvoller wäre es, die Zusammenarbeit von Ermittlungsbehörden grenzübergreifend zu verbessern und so sicherzustellen, dass Ermittlungen reibungslos verlaufen, anstatt Unternehmen für hoheitliche Aufgaben in einem grundrechtssensiblen Bereich zu beanspruchen.

- **Rechtlicher Rahmen für den Zugriff auf Daten und Informationssysteme ohne Mitwirkung des Diensteanbieters**
  Der IIA sieht auch vor, dass Rechtsdurchsetzungsinstitutionen auch ohne Mitwirkung oder die Zusammenarbeit mit Diensteanbietern auf mögliche elektronische Beweismittel zugreifen können sollen. Diese Maßnahme ist kritisch zu bewerten, da sie zusätzlich zu den vorne beschriebenen Problemen außerdem noch die Integrität der Kommunikationsdienste infrage stellt. Dies gilt insbesondere beim Zugriff auf „beschlagnahmte Informationssysteme“, die hier ein sehr unklarer Begriff sind. Da davon auszugehen ist, dass solche Zugriffe ohne Bekanntgabe gegenüber nationalen Sicherheitsbehörden oder Dienstebetreibern geschieht, bleibt zudem unklar, inwieweit eine solche Maßnahme überhaupt praktisch umsetzbar wäre. Betrachtet man die Intensität eines solchen Eingriffs, so stellt sich hier die Frage, ob eine solche Maßnahme überhaupt unter rechtsstaatlichen Gesichtspunkten wünschen∂‘swert ist. Sie würde in jedem Fall einen schwerwiegenden Eingriff in das Fernmeldegeheimnis darstellen, der das Vertrauen von Nutzern in digitale Dienste untergraben würde, aber auch das Vertrauen der Diensteanbieter in die Arbeit von Ermittlungs- und Sicherheitsbehörden. Darüber hinaus wird aus dem äußerst unpräzise formulierten Passus nicht klar, inwieweit ein Zugriff auf Daten und Informationssysteme ohne Mitwirkung des Diensteanbieteres technisch erfolgen kann, so dass dessen Inanspruchnahme bereits vorweggenommen wird. eco lehnt sämtliche Maßnahmen in Richtung

staatlicher Backdoors und massenhaft anlasslos erhobener und gespeicherter Kommunikation ab.

---

eco – Verband der Internetwirtschaft e.V. versteht sich als Interessenvertreter und Förderer aller Unternehmen, die mit dem Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit rund 1000 Mitgliedsunternehmen. Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunternehmen. eco ist damit der größte nationale Internet Service Provider-Verband Europas.