VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme zum Inception Impact Assessment: Europol Regulation (Ref. Ares(2020)2555219)

Berlin, 2. Juli 2020

Mit der voranschreitenden Digitalisierung stellen sich neue Herausforderungen an die Polizeiarbeit. Beweissicherung findet vermehrt im elektronischen Bereich statt. Durch die globale Natur digitaler Dienste und des Internets sind mit der Erhebung dieser Daten für Ermittlungsbehörden ebenso wie für Diensteanbieter und –betreiber Fragen und Probleme verbunden, die in jüngster Vergangenheit an verschiedenen Stellen diskutiert und teilweise auch regulatorisch adressiert worden sind. Die Debatte um die e-Evidence beweist dies ebenso wie die Diskussionen um die Cybercrime Konvention. Vor diesem Hintergrund möchte die Europäische Kommission auch die Rolle der europäischen Ermittlungsbehörde Europol neu definieren und eventuell ausweiten. Die Kommission hat ein Inception Impact Assessment (IIA) verfasst, das verschiedene Szenarien für die Weiterentwicklung der Behörde zeichnet.

I. Vorbemerkung

Die dargestellte Debatte stellt für die Anbieter digitaler Dienste eine enorme Herausforderung dar. Mit grenzüberschreitenden Anfragen zur Herausgabe von Daten, insbesondere personenbezogenen, vertraulichen oder sonstig gesetzlich geschützten Daten durch ausländische Ermittlungsbehörden geht für diese Unternehmen die Frage einher, inwieweit sie sich mit ihren jeweiligen nationalen Gesetzen in Einklang verhalten und ob sich durch die Herausgabe dieser Informationen für sie straf- oder zivilrechtliche Folgen für sie ergeben. Die Herausgabe von Daten und Informationen auf Verlangen einer Strafverfolgungsbehörde außerhalb der jeweils zuständigen nationalen Jurisdiktion kann so für die Unternehmen Haftungsfragen aufwerfen und Rechtsunsicherheit erzeugen.

Darüber hinaus besteht das Problem, dass mit entsprechenden Anfragen das „Double-Criminality“ Prinzip untergraben wird. Was evtl. bei Drogendelikten als geringfügiges Problem wahrgenommen wird, kann sich gänzlich anders darstellen, wenn es sich um Äußerungsdelikte handelt. Die Herausgabe von Informationen und Daten aus fremden Jurisdiktionen ist daher stets ein kritisches Problem, das entsprechender rechtsstaatlicher Sicherungsmechanismen bedarf.

II. Zum Inception Impact Assessment im Detail

- **Zum Abschnitt “Context”**

Die Digitalisierung stellt, wie anfangs dargestellt neue Herausforderungen an die Polizeiarbeit. Gerade in einem europäischen Kontext mit souveränen Mitgliedsstaaten auf relativ engem Raum kann Kriminalität und Strafverfolgung oft einen grenzüberschreitenden Bezugspunkt haben. Dementsprechend ist das Ansinnen der Kommission, Europol zu stärken nachvollziehbar. Auch ist davon auszugehen, dass auch Kriminelle sich verstärkt digitaler Technologien bedienen und diese für ihre Zwecke verwenden. Dies steht im Kontext einer generellen stärkeren Digitalisierung von Gesellschaft und Wirtschaft. Vor diesem Hintergrund ist die Stärkung von Europol mit entsprechenden digitalen Kompetenzen und Kapazitäten ein berechtigtes Anliegen. Gleichzeitig wird eine wichtige Prämisse außer Acht gelassen. Digitalisierung, die Nutzung verschlüsselter Messengerdienste und der sprunghafte Anstieg an Internetnutzern erfolgt vor allem durch Privatpersonen ohne kriminelle Absichten. Diesem Umstand tragen Ermittlungsbehörden bei Forderungen nach Zugriffsrechten und Möglichkeit zur Abfrage von Daten oftmals nicht ausreichend Rechnung. Es gilt hier eine angemessene Regelung zu finden, die die Rechte von Bürgerinnen und Bürgern schützt. Dies gilt auch beim grenzübergreifenden Zugriff auf entsprechende Informationen. Dementsprechend sollten angestrebte Regelungen diesen Umstand angemessen berücksichtigen.

- **Zum Abschnitt “Problem the initiative aims to tackle”**

Das Problem, dass Europol von privaten Akteuren keine Daten direkt erhalten kann, stellt für die Arbeit der Behörde nachvollziehbarerweise ein Problem dar. Dies ist in der Natur der Organisation von Strafverfolgung in Europa begründet und muss dort adressiert werden. Die Herausforderung in diesem Kontext eines operativen Problems für Europol darzustellen, ist aus der Sicht von eco fehlgeleitet.

- **Zum Abschnitt “Objectives and Policy Options”**

Die unter Objective no. 1 festgeschriebene Stärkung der Zusammenarbeit von Europol mit privaten Akteuren bietet die Chance der Schaffung eines rechtskonformen und einheitlichen Rahmens für die Abfrage bestimmter Daten und Informationen. Dabei muss aber grundsätzlich darauf geachtet werden, dass die unter Option no. 2 und Option no. 3 aufgeführten Maßnahmen transparent, verhältnismäßig und für die entsprechenden Unternehmen handhabbar sind. Die Zusage, die jeweils betroffenen

Mitgliedsstaaten in die Herausgabe mit einzubeziehen muss dahingehend klargestellt sein, dass Unternehmen sich bei der Herausgabe von Informationen auf die Rechtmäßigkeit des Ersuchens verlassen können und ein Rechtsschutz erreicht wird, der mindestens so hoch ist bei den bestehenden Rechtsbeihilfeersuchen.

Für die unter Objective no. 2 aufgeführten Optionen möchte eco darauf hinweisen, dass im Falle einer Einführung von Rechten zur Datenabfrage für Europol dringend eine rechtliche Klarstellung zur Durchführung der Abfragen und deren rechtlichem Rahmen erfolgen sollte. Im Zuge dieser Klarstellung sollte auch erwogen werden, in welchem Umfang Aufwände, die den Unternehmen durch etwaige Herausgabe von Informationen entstehen, erstattet werden können.

III. Einordnung und Fazit:

Die Neuregelung des Mandats von Europol bietet die Chance, die grenzüberschreitende Strafverfolgung innerhalb Europas effektiver zu gestalten. Aus Providersicht wäre eine Europäische Zentralbehörde für grenzüberschreitende Datenausleitungen denkbar und unter Umständen wünschenswert. Gegebenenfalls könnte Europol eine geeignete Behörde hierfür werden. Es bedarf jedoch zuvor eines transparenten, nachvollziehbaren und einheitlichen Rechtsrahmens für den grenzüberschreitenden Zugang zu Daten. Dies sollte in einem EU-Gesetz und nicht allein über die Ausweitung der Befugnisse von Ermittlungsbehörden geregelt werden. Letztendlich muss eine Agentur wie Europol auch gegenüber EU-Institutionen rechenschaftspflichtig und kontrollierbar sein. Ebenso stellt sich die Frage, wer eine Datenweitergabe an die USA oder an das Vereinigte Königreich kontrolliert.

Folgende Aspekte sollten bei der Regelung des grenzüberschreitenden Zugriffs auf Daten immer berücksichtigt werden:

- Die Übermittlung der Daten muss im Einklang mit dem Recht des betroffenen Mitgliedsstaates stehen. Neben einer konsequenten Einbindung der zuständigen Behörden des Mitgliedstaates ist es wichtig, dass Ausleitungen nur bei bestimmten Straftaten, auf die sich alle EU-Mitgliedsstaaten geeinigt haben, zulässig sind. Sinnvoll ist hier ein gemeinsamer Straftatenkatalog gemäß dem Prinzip der doppelten Kriminalität.

- Die Verantwortung für den Grundrechtschutz und die Rechtmäßigkeit der Strafverfolgung muss bei den staatlichen Behörden verbleiben.

Der Provider kann die Rechtmäßigkeit nicht überprüfen oder eine Haftung hierfür übernehmen.

- Technische Standards für eine sichere Datenübermittlung sind erforderlich.
- Es ist eine angemessene Aufwandsentschädigung für die privaten Unternehmen vorzusehen.

eco hofft, dass in der weiteren Debatte die hier aufgezeigten Aspekte berücksichtigt werden. Die Neudefinition der Rolle von Europol sollte nicht dazu führen, dass Diensteanbieter und –betreiber mit größerer Rechtsunsicherheit konfrontiert sind.

Über eco

Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.