Der Deutsche Richterbund dankt der Kommission für die gestartete Initiative und die öffentliche Konsultation zu einem Thema, das zunehmende Bedeutung für die Strafverfolgung erhält. Die geltende Rechtslage wird den Problemen, die die digitale Kommunikation aufwirft, nicht mehr gerecht. Ein wesentlicher Umstand ist dabei, dass häufig Dienste mit Sitz im Ausland genutzt werden und Daten weltweit gespeichert werden können. Für den Nutzer macht es keinen Unterschied, wo sein Anbieter digitaler Dienste sitzt und wo dieser die Daten speichert. Auch die Strafverfolgung darf deshalb nicht mehr so starr an Staatsgrenzen gebunden sein, wie sie es zurzeit noch ist.

Der Fragebogen wendet sich zwei wichtigen Komplexen in diesem Bereich zu.

Es würde die Strafverfolgung in der Tat deutlich vereinfachen und verbessern, wenn Strafverfolgungsbehörden unmittelbar auf Anbieter digitaler Dienste in anderen Mitgliedstaaten zugehen könnten und sie verpflichten könnten, Bestandsdaten und Metadaten herauszugeben. Inhaltsdaten sollten grundsätzlich nicht einbezogen werden. Bei der Herausgabe von Inhaltsdaten handelt es sich um einen schwerwiegenden Grundrechtseingriff, der nur über die Justizbehörden der beiden betroffenen Staaten laufen sollte. Hilfreich wäre es aber, wenn die Strafverfolgungsbehörden des einen Mitgliedstaates die digitalen Dienste des anderen Mitgliedstaates unmittelbar auffordern könnten, Verkehrsdaten, aber auch Inhaltsdaten vorläufig zu sichern.

Dabei sollten die zu schaffenden gesetzlichen Regelungen verpflichtender Natur sein. Nur dann wird Rechtsklarheit und Rechtssicherheit für die Nutzer und für die Unternehmen geschaffen. Die Dienste können sich gegenüber ihren Kunden auf die gesetzliche Regelung berufen. Ein Wettbewerbsvorteil für Dienste, die damit werben, keine Daten herauszugeben, ist damit nicht mehr möglich. Es könnte daran gedacht werden, die digitalen Dienste zu verpflichten, der Kommission oder den nationalen Regierungen in bestimmten Abständen zu berichten, in wieviel Fällen sie an Justizbehörden welcher Staaten Daten übermittelt haben. So wird eine Evaluierung neuer Regelungen möglich. Da sowohl die Herausgabepflicht als auch die Pflicht, solche Transparenzberichte zu erstellen, die digitalen Dienste belasten, sollte an entsprechende finanzielle Entschädigungen für die Unternehmen gedacht werden.

Nicht weniger wichtig erscheint es, beim Zugriff auf gespeicherte Daten durch Strafverfolgungsbehörden nicht mehr darauf abzustellen, in welchem Staat die Daten gespeichert sind, sondern darauf abzustellen, wo sich das elektronische Medium des Nutzers befindet, von dem aus auf die Daten zugegriffen werden kann. In der Regel ist es für

den Nutzer völlig irrelevant, wo seine Daten gespeichert sind. Wichtig ist für ihn nur die Möglichkeit des unmittelbaren Zugriffs. Eine solche Regelung ist für die Strafverfolgungsbehörden auch deshalb besonders wichtig, weil nicht immer festgestellt werden kann, in welchem Staat die Daten gespeichert sind, und der Speicherort häufig wechseln kann. Die Regelungen der strafrechtlichen Zusammenarbeit werden diesem Umstand nicht gerecht. Dasselbe gilt auch bei der in dem Fragebogen aufgeworfenen Frage, ob der Staat, in dem die Daten gespeichert sind, benachrichtigt werden muss und ein Widerspruchsrecht erhalten soll. Eine solche Benachrichtigung ist gar nicht möglich, wenn der Speicherort unbekannt ist. Sie erscheint allerdings auch nicht erforderlich. Der virtuelle Raum, in dem Daten gespeichert sind, kann als Verlängerung des lokalen Speichers des elektronischen Mediums angesehen werden, das der Betroffene nutzt. Es ist kein Eingriff in die Souveränität des anderen Staates, wenn über das elektronische Medium auf Daten zugegriffen wird. Wird ein Telefonat abgehört, das mit einem Telefonpartner geführt wird, der sich im Ausland befindet, betrachtet der andere Staat dies auch nicht als Eingriff in seine Souveränität. Er wird nicht informiert und kann der Verwertung der durch die Telekommunikation gewonnenen Erkenntnisse auch nicht widersprechen.

Bei allen zu treffenden Regelungen erscheint es wichtig, auf eine Harmonisierung unterschiedlicher Rechtsinstrumente zu achten. So gibt es etwa bereits die Cybercrime Convention von 2001, die sehr gute Regelungen enthält, auf die aufgebaut werden sollte, und die Europäische Ermittlungsanordnung, die ein Instrumentarium zur gegenseitigen Anerkennung von Entscheidungen im Bereich der strafrechtlichen Zusammenarbeit zur Verfügung stellt.