






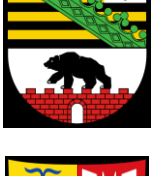

Kasseler Erklärung

Deutschland braucht eine digitale Agenda für das Straf- und Strafprozessrecht

Eine leistungsfähige Justiz ist der Garant der inneren Sicherheit. Ihre personelle und strukturelle Stärkung in den Ländern der Bundesrepublik Deutschland ist deshalb ein richtiger und notwendiger Beitrag zur Verbesserung der Sicherheit in Deutschland.

In zentralen Bereichen wurden in den letzten vier Jahren zudem wichtige rechtspolitische Ziele erreicht. Oft waren es Impulse aus den Ländern, die wichtige Reformen in Gang gebracht haben. Zu nennen sind die Verschärfung der Staatsschutzdelikte, zum Beispiel der §§ 89a ff. StGB („Ausreise in den Dschihad“), die Reformen des Sexualstrafrechts, sowohl im Bereich der Kinderpornografie im Internet als auch in den Reformen des § 177 StGB (sog. Vergewaltigungsparagraph, „Nein heißt Nein“ sowie der sexuellen Belästigung), die Einführung des Tatbestandes der Datenhehlerei, die Verschärfung des Stalking-Tatbestandes, die Ausweitung des Einsatzes der elektronischen Aufenthaltsüberwachung („elektronische Fußfessel“) auf Gefährder sowie die Schaffung rechtsstaatlicher Standards für die Verkehrsdatenspeicherung zum 1. Juli 2017 und für verdeckte Eingriffe in informationstechnische Systeme (Quellen-TKÜ und Online-Durchsuchung) durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens.

Der Einfluss der Digitalisierung auf alle Lebensbereiche wird weiter wachsen. Dies hat auch Auswirkungen auf die Sicherheitsdebatte, denn die Verbreitung extremistischer Positionen über die sozialen Netzwerke, Cyberattacken auf Unternehmen und

Pressesprecher: René Brosius
Luisenstraße 13 • 65185 Wiesbaden
Telefon: 0611 322695 • Telefax: 0611 322691

pressestelle@hmdj.hessen.de
http://www.justizministerium.hessen.de
https://twitter.com/justiz_hessen

Institutionen, gezielte Angriffe auf kritische Infrastrukturen oder Angriffe auf Wahlen und Abstimmungen im demokratischen Rechtsstaat nehmen rasant zu und gehören zu den neuen Herausforderungen der Sicherheits- und Strafverfolgungsbehörden. Gerade die Gefahren, die von Meinungsmanipulationen für unsere Demokratie und die Stabilität von Wirtschaft und Gesellschaft ausgehen, sind ebenso ernst zu nehmen wie die terroristische Bedrohung.

Vor diesem Hintergrund muss sich die rechtspolitische Diskussion in den nächsten Jahren stärker den Herausforderungen der Digitalisierung widmen – Deutschland braucht eine digitale Agenda für das Straf- und Strafprozessrecht. Die Justizministerinnen und Justizminister der Länder Bayern, Hessen, Nordrhein-Westfalen, Sachsen, Sachsen-Anhalt, Mecklenburg-Vorpommern, Baden-Württemberg und des Saarlandes sowie der Staatssekretär des Landes Schleswig-Holstein sind daher übereinstimmend der Ansicht, dass in der kommenden Legislaturperiode insbesondere folgende rechtspolitische Herausforderungen angegangen werden müssen:

1. „Digitalen Hausfriedensbruch“ konsequent sanktionieren!

Kriminelle oder Cyberterroristen greifen mittels Schadsoftware heimlich auf Tausende von Rechnern und Mobiltelefonen zu und nutzen die kombinierte Rechnerleistung für Cyberattacken. Die ahnungslosen User an den Computern merken allenfalls, dass ihre Systeme etwas langsamer laufen als normal. Die zu Bot-Netzen verbundenen Computersysteme arbeiten koordiniert gegen Firewalls, versenden Massen-E-Mails und Tweets oder legen durch DDos-Angriffe ganze Systeme lahm. Der Bundesrat hat auf Initiative der Länder bereits am 23. September 2016 den Entwurf eines Strafrechtsänderungsgesetzes „Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme – Digitaler Hausfriedensbruch“ beim Deutschen Bundestag eingebracht (BR-Drs. 338/16). Es ist bedauerlich, dass der Bundesjustizminister diese drängende Problematik immer noch nicht aufgegriffen hat.

2. Auskunftsverlangen gegenüber Postdienstleistern klar regeln!

Der - nicht selten anonyme und mittels Krypto-Währungen abgewickelte - Handel mit illegalen Waren wie Betäubungsmitteln, Falschgeld oder Waffen über das Darknet hat erheblich zugenommen. Erfolgsversprechende Ermittlungsansätze zur Identifizierung von Tatverdächtigen ergeben sich insbesondere bei der Aufgabe und Annahme entsprechender Sendungen. Es bedarf daher einer klaren gesetzlichen Regelung, die es den Strafverfolgungsbehörden ermöglicht, von Postdienstleistern Auskünfte auch über noch nicht ein- sowie bereits ausgelieferte Sendungen zu verlangen.

3. Beleidigungen im Internet wirksam sanktionieren!

Beleidigungen, die im Internet begangen werden und die wegen ihrer permanenten Verfügbarkeit und der Schwierigkeit, sie wieder zu beseitigen, die Opfer viel härter und nachhaltiger treffen als in der „realen Welt“, müssen konsequent sanktioniert werden. Dies bedeutet für bestimmte Fälle auch eine Überprüfung der Strafrahmen für Beleidigungsdelikte im Internet.

4. Die Reichweite des Telekommunikationsrechts für OTT-Dienste klären!

Over-the-Top (OTT)-Kommunikationsdienste wie WhatsApp, Skype, Facebook & Co. erfreuen sich wachsenden Zuspruchs. Dabei verwischen die Grenzen zu den klassischen Telekommunikationsdienstleistungen. Das Verwaltungsgericht Köln hat bereits entschieden, dass der E-Mail-Dienst Google Mail einen öffentlich zugänglichen Telekommunikationsdienst darstellt, dessen Aufnahme der Bundesnetzagentur zu melden ist (VG Köln, Urteil vom 11. November 2015 – 21 K 450/15 –, juris). Um Rechtssicherheit für Provider wie für Nutzer herzustellen, ist eine Diskussion dazu erforderlich, welche Sicherheitsstandards des bereichsspezifischen Telekommunikationsrechts zukünftig auf welche OTT-Kommunikationsdienste übertragen werden müssen.

5. Die Sicherung von Cloud-Daten verbessern!

Die Durchsuchung sowie die Beschlagnahme sind als „offene“ Ermittlungsmaßnahmen ausgestaltet, sodass der Beschuldigte zeitnah hiervon in Kenntnis zu setzen ist. Soll eine mögliche Datenveränderung oder ein drohender

Datenverlust verhindert werden, zwingt dies derzeit dazu, ein verdeckt geführtes Verfahren offenzulegen. Dies beeinträchtigt nicht nur größere Strukturermittlungen, sondern auch kleinere Ermittlungsverfahren, nachdem im Zeitalter des Smartphones die Datenauslagerung alltäglich geworden ist. Zu begrüßen sind deshalb auch die Überlegungen der Cloud-Evidence-Group des Europarates, die Zusammenarbeit mit Dienstanbietern zur Sicherung von Beweismitteln zu stärken.

6. Private Unternehmen im Schadensfall zur Kooperation ermutigen!

Unternehmen, die Kommunikationsdienstleistungen im Internet anbieten, sollten ermutigt werden, beim Erkennen strafrechtlicher relevanter Inhalte (z.B. Kinderpornografie, Anschlagsplanung, Cyberattacken, Geldwäsche) intensiver mit den Behörden zusammenzuarbeiten. Die Länder verfügen inzwischen über hochprofessionelle Zentralstellen und spezielle Ermittlungseinheiten, die auch bei sensiblen Anfragen schnell und kompetent die notwendigen Maßnahmen treffen.

7. Sympathiewerbung für Terrorismus unter Strafe stellen!

Längst ist bekannt, dass Gruppen wie der sogenannte Islamische Staat mit aufwendig produzierten Videos bei Twitter, YouTube oder Facebook versuchen, junge Menschen für ihre abscheuliche Ideologie zu gewinnen. Im Jahr 2016 gab der Nachrichtendienst Twitter bekannt, im Jahr 2015 ca. 125.000 Nutzer im Zusammenhang mit IS-Inhalten gesperrt zu haben. Je früher in diesem Bereich die Strafbarkeit greift, desto besser können die Strafverfolgungsbehörden Strukturen aufdecken und zerschlagen. Die im Jahre 2002 abgeschaffte Strafbarkeit der Sympathiewerbung für Terrororganisationen muss deshalb so schnell wie möglich wieder eingeführt werden.

8. Den ökonomischen Dschihad austrocknen!

Die Mechanismen der Terrorfinanzierung und der organisierten Kriminalität ähneln sich. In beiden Fällen geht es um großflächige „Legalisierung“ von Finanzmitteln aus illegalen Quellen. Das Geld kann dabei aus Erpressungen von kleinen Unternehmern auch in Deutschland, illegalem Waffenhandel oder auch dem

Verkauf von Öl durch den IS stammen. Zur Bekämpfung dieser Taten muss das Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen, das am 26. Juni 2017 in Kraft getreten ist, zügig mit Leben gefüllt werden. Insbesondere ist auf eine ausreichende personelle und sachliche Ausstattung der neuen Zentralstelle zu achten und deren vertrauensvolle Zusammenarbeit mit den Spezialeinheiten der Länder sicherzustellen.

9. Den Betrieb krimineller Cyberstrukturen konsequent unterbinden!

Der Betrieb von Underground-Economy-Verkaufsplattformen, über die in zunehmendem Ausmaß inkriminierte Waren und Dienstleistungen jeglicher Art gehandelt werden, kann nach derzeitiger Gesetzeslage zwar als Beihilfe strafbar sein, setzt aber im Einzelfall den Nachweis einer strafbaren Haupttat voraus. Es sollte untersucht werden, ob bereits der Betrieb krimineller Cyberinfrastrukturen pönalisiert werden kann, damit auch in diesem Punkt das Strafrecht den Strukturen der digitalen Welt gerecht wird.

10. Internationale Zusammenarbeit stärken!

Die Grenzenlosigkeit des Internets begünstigt Straftäter und Terroristen, da viele Instrumente der internationalen Zusammenarbeit der Strafverfolgungsbehörden sehr schwerfällig und den Notwendigkeiten des Internetzeitalters noch nicht angepasst sind. Hier ist es sowohl auf europäischer Ebene (Eurojust, Europol) notwendig, enger zusammenzuarbeiten, als auch die Kooperation zwischen internationalen, europäischen und nationalen Behörden zu stärken, um in Fällen mit Auslandsberührung künftig effektiver handeln zu können.