REGIERUNGSERKLÄRUNG

VON STAATSMINISTERIN EVA KÜHNE-HÖRMANN
MINISTERIN DER JUSTIZ

BETREFFEND

„DIGITALE AGENDA FÜR DAS RECHT“

IN DER PLENARSITZUNG DES HESSISCHEN LANDTAGS
AM 21. JUNI 2016

– ES GILT DAS GESPROCHENE WORT –

Sehr geehrte Damen und Herren,

wir befinden uns inmitten einer Revolution.

Entgegen der üblichen Vorstellung, dass eine Revolution mit viel Knall und Rauch von statten gehen muss, kommt die digitale Revolution in Form von Updates, Beta-Versionen und technischen Innovationen daher.

Sie dringt dabei in Lebensbereiche ein, die wir bisher als ureigenste Intimsphäre verstanden haben und deshalb brauchen wir hier Schutzmechanismen, die nur mittels einer digitalen Agenda für das Recht gewährleistet werden können.

Die Digitalisierung verändert unsere Welt in einem Ausmaß, welches man nicht hoch genug einschätzen kann.

Dabei hat das Medium Internet unsere persönlichen, gesellschaftlichen und wirtschaftlichen Möglichkeiten signifikant erweitert.

Insbesondere die sozialen Medien haben dabei auch eine politische Komponente.

Vor allem die ortsungebundene, mobile Verfügbarkeit des Internets, aber auch die Möglichkeit der Vernetzung bislang getrennter Systeme treiben die Digitalisierung der Welt voran.

Niemals zuvor haben dabei die Menschen aller Schichten und aller Kontinente so stark von einer technischen Entwicklung profitiert - niemals zuvor waren aber auch so viele Menschen den Gefahren einer technischen Entwicklung ausgesetzt.

Denn was als Erleichterung des täglichen Lebens in allen Bereichen daher kommt, protokolliert und erfasst persönliche Daten, Standorte, Mobilität und Kommunikationsgewohnheiten, über die die Nutzer die Kontrolle teilweise oder ganz an die Anbieter solcher Programme verlieren können.

Dabei ist die Bequemlichkeit des Einzelnen die gefährliche Begleitmusik der digitalen Revolution.

Wie weit die umfassende Vernetzung unterschiedlicher Systeme reicht, zeigt ein Blick in die Fabrik der Zukunft, die mit dem Begriff „Industrie 4.0“ bezeichnet wird.

Mit dem Ziel, möglichst viele Informationen digital nutzbar zu machen, werden die verschiedenen IT-Systeme eines gesamten Unternehmens sowohl untereinander als auch nach außen vernetzt.

Allein in Deutschland werden bis zum Jahr 2020 Investitionen in Höhe von rund 11 Milliarden Euro in diesem Bereich erwartet.

Für den Privatanwender zeigt sich der Trend zur Vernetzung vor allem im sogenannten „Internet der Dinge“, also dem zunehmenden Einsatz von IT-gesteuerten, vernetzten Alltagsgegenständen im persönlichen Umfeld.

Statt – wie derzeit – selbst Gegenstand der menschlichen Aufmerksamkeit zu sein, soll das „Internet der Dinge“ den Menschen bei seinen Tätigkeiten unmerklich unterstützen, ohne abzulenken oder überhaupt aufzufallen.

Das am häufigsten zitierte Beispiel in diesem Zusammenhang ist der „intelligente Kühlschrank“, der selbsttätig über Internet zur Neige gehende Vorräte bestellt, die dann angeliefert werden.

Aber auch Interaktive-Smart-TVs, autonome Autos, vom Mobiltelefon aus steuerbare Rollläden und Heizungen sind hier die Stichworte.

Meine Damen und Herren,

in vielen Bereichen sind den technischen Fortschritten strukturelle Maßnahmen auf Ebene der Verwaltung, der Sicherheit, des Ausbaus der Breitbandnetze oder der Strafverfolgung gefolgt.

Das Ziel der Landesregierung ist es, dass jeder von den Vorteilen der Digitalisierung profitierten kann, denn sie schafft nicht zuletzt Wohlstand und Arbeitsplätze.

Wir wollen aber auch die Nutzer vor Angriffen aus dem Netz schützen.

Wenn wir nicht wollen, dass mit jedem Innovationsschritt im Internet der Schutz der Bürgerinnen und Bürger erodiert, müssen wir der Digitalisierung auch ein rechtliches Rückgrat geben.

Das ist der Grund, warum wir als Landesregierung konsequent an einer „Digitalen Agenda für das Recht“ arbeiten.

Als Gesetzgeber sind wir dazu aufgerufen, Antworten und Regelungen für ganz unterschiedliche Lebensbereiche zu finden, die sich durch die Digitalisierung rasant verändern.

Meine Damen und Herren,

die hessische Landesregierung stellt sich den Herausforderungen, die die schnell voranschreitende Vernetzung und Digitalisierung für die Gesetzgebung und Rechtsanwendung mit sich bringen.

Mit vielen Initiativen auf Ebene der Fachministerkonferenzen, der Beteiligung an bundesweiten Arbeitsgruppen, Gesetzentwürfen auf Ebene des Bundesrates und selbstverständlich auf operativer Ebene bei Staatsanwaltschaften und Gerichten engagiert sich Hessen für eine grundlegende Überarbeitung des Rechts.

Unser Ziel ist es, dass die Bürgerinnen und Bürger in einem digitalisierten Umfeld rechtssicher, selbstbestimmt und frei leben und handeln können.

Das betrifft das Zivilrecht ebenso wie das Straf- und Strafprozessrecht.

Meine Damen und Herren,

die Digitalisierung und Vernetzung des Alltags eröffnet neue Angriffsflächen für kriminelle Aktivitäten in einem bisher nie dagewesenen Ausmaß.

Denn die Vernetzung macht die Dinge nicht nur intelligent, sondern auch verletzlich.

Das Internet ist längst der größte Tatort der Welt geworden.

Das ist keine Neuigkeit mehr.

Es werden aber immer mehr IT-Systeme, Anlagen und Geräte angreifbar, die bislang aus dem Internet gar nicht erreichbar waren.

Dadurch vergrößert sich das Risiko von Gefahrenlagen durch den Ausfall oder durch Fehlfunktionen von kritischen Infrastrukturen und von Produktions- oder Geschäftsprozessen erheblich.

Experteneinschätzungen gehen einhellig davon aus, dass Cybercrime eine bedeutende und schnell wachsende Kriminalitätsform darstellt.

Je mehr potentielle Ziele zur Verfügung stehen, desto mehr Straftaten können in diesem Umfeld begangen werden.

Europol rechnet derzeit mit rund drei Milliarden Internet-Nutzern und rund 10 Milliarden angeschlossenen Geräten.

Mit der Weiterentwicklung des Internets der Dinge steigt die Zahl potentieller Ziele wiederum an und bietet neue Einfallstore für Cyberkriminelle und potentielle Täter, die im digitalen Umfeld bislang wenig bis gar nicht aktiv waren.

Wie groß die Bedrohung ist, wird eindrucksvoll auch durch den Spähangriff auf das IT-Netz des deutschen Bundestages belegt.

Im letzten Jahr sind die Bundestags-Computer Ziel einer bislang beispiellosen Attacke unbekannter Hacker geworden.

Dem Angreifer war es gelungen, in das gesamte Bundestags-Netzwerk einzudringen und sensible Daten auszuspähen.

Der Urheber des Angriffs ist bislang nicht eindeutig identifiziert.

Experten gehen aber davon aus, dass es sich um einen ausländischen Nachrichtendienst handeln dürfte.

Erfolgreiche Cyber-Angriffe auf Unternehmen, Verwaltungen und Privatnutzer bedürfen jedoch keineswegs der nahezu unbegrenzten Ressourcen fremder Nachrichtendienste.

Dies spiegelt sich in der Masse der heutigen Cyber-Angriffe wieder.

Für erfolgreiche Cyberattacken braucht man derzeit vielfach nicht mehr als einen PC und einen Internetanschluss.

Diesen eher kleinen Investitionen stehen die vielfältigen Möglichkeiten gegenüber, durch kriminelle Handlungen Geld zu verdienen, vertrauliche Informationen zu erlangen oder Sabotageakte durchzuführen.

Entsprechende Angriffswerkzeuge und -methoden sind einfach und kostengünstig verfügbar.

Und diese Werkzeuge wollen wir den Kriminellen mit unserer Botnetz-Initiative wirksam aus der Hand schlagen.

Es existiert ein funktionierender globaler Markt, auf dem Angriffswerkzeuge, Schwachstellen oder Schadsoftware vollkommen anonym eingekauft oder als Dienstleistung in Auftrag gegeben werden können.

Auch illegal erlangte Daten wie Nutzer-Accounts und Kreditkarteninformationen werden dort gehandelt.

Aber nicht nur das: im sogenannten „Darknet“, einem anonymen und verschlüsselten Netzwerk innerhalb des Internet, werden Kinderpornographie, Drogen, Falschgeld, gefälschte Ausweise und Waffen angeboten und ganz normal mit der Post versandt.

Kinder werden zur sexuellen Ausbeutung angeboten und Bilder und Videos von schweren sexuellem Missbrauch auf Bestellung angefertigt und ins Netz gestellt.

Ich habe mich seit meinem Amtsantritt dafür eingesetzt, Strafbarkeitslücken im Bereich der Kinderpornographie zu schließen.

Nicht zuletzt aufgrund hessischer Initiativen im Bundesrat ist bereits Einiges zum Schutz der Kinder erreicht worden.

Ich werde auch weiterhin nachdrücklich dafür eintreten, dass der Versuch des sogenannten Cybergrooming – also der Versuch einer sexuellen Belästigung Minderjähriger über das Internet – unter Strafe gestellt wird.

Denn wenn fremde Personen sich als Kinder ausgeben und versuchen, über das Internet mit Kindern Kontakt aufzunehmen, um später an ihnen sexuellen Handlungen durchzuführen, dann sollten den Ermittlungsbehörden alle Möglichkeiten zur Verfügung stehen, um solche Täter zu ermitteln.

Meine Damen und Herren,

bei den Cyberkriminellen im „Darknet“ handelt es sich sowohl um Einzelpersonen als auch um gut organisierte Gruppen, die auf diesen kriminellen Online-Marktplätzen ihre Fähigkeiten, Dienstleistungen und illegale Waren anbieten.

Das dezentral und grenzenlos gestaltete Internet bietet für Angreifer vielfältige Tarnungsmöglichkeiten, die das Risiko, entdeckt zu werden, gegen Null gehen lassen.

Gleichzeitig stellt das Internet mit den sozialen Netzwerken und Instant-Messaging-Diensten die technische Mittel zur Verfügung, um verschlüsselt Straftaten in der analogen Welt zu planen und zu organisieren.

Diese verschlüsselte Kommunikation krimineller Täter ist für die Ermittlungsbehörden mangels ausreichender rechtlicher Grundlagen oftmals nicht aufklärbar.

Die Verwundbarkeit kritischer Infrastrukturen wie z.B. Kommunikationsunternehmen infolge ihrer Anbindung an das Internet machen sich nicht zuletzt auch Terroristen zunutze.

Der „Cyber-Terrorismus“ ist längst Realität.

Im Anschluss an die islamistischen Terroranschläge auf die Redaktion der Satirezeitschrift „Charlie Hebdo“ am 7. Januar 2015 in Paris hatten französische Cyber-Spezialisten wenigstens 19.000 Hacker-Attacken registriert.

Den Hackern war es auch gelungen, in die Computersysteme eines französischen TV-Senders einzudringen und über viele Stunden hinweg die Sendesignale zu kontrollieren.

IS-Propagandavideos wurden abgespielt und die Familien derjenigen französischen Soldaten bedroht, die sich am Kampf gegen die IS-Terroristen beteiligten.

Der Angriff war komplex und umfassend.

Es ging dabei zum einen um das Verbreiten eines Klimas der Angst, es war aber auch ein digitales Hineintragen des Terrorismus nach Europa.

Auch das gehört zur eingangs erwähnten politischen Komponente der sozialen Medien!

Meine Damen und Herrn,

der Kampf gegen Internetkriminalität, für eine Digitale Agenda für das Recht ist ein langwieriger Kampf.

Auf Initiative Hessens haben wir seit dem letzten Herbst den neuen strafrechtlichen Tatbestand der Datenhehlerei im Strafgesetzbuch stehen.

Mit unserer Bundesratsinitiative zur Bekämpfung der Botnetzkriminalität setzen wir unseren Weg konsequent fort.

Mit dieser Initiative verfolgen wir den Gedanken, bereits das schlichte Gebrauchsrecht an IT-Systemen, unabhängig davon, ob bereits Daten auf diesen Systemen verändert, ausgespäht oder zerstört worden sind, einem strafrechtlichen Schutz zu unterstellen.

Der sogenannte digitale Hausfriedensbruch soll unter Strafe gestellt werden.

Die Justizministerinnen und -minister haben sich meiner Auffassung, dass hier ein dringender Handlungsbedarf besteht, einstimmig angeschlossen.

Einen entsprechenden Gesetzentwurf, der die Anforderungen des Bundesverfassungsgerichts, das Grundrecht auf Integrität und Vertraulichkeit von IT-Systemen zu schützen, erfüllt, hat die Landesregierung bereits im Bundesrat eingebracht.

Bei unseren Vorstößen zur Bekämpfung der Datenhehlerei und zur Bekämpfung des massenhaften Infizierens von vernetzten IT-Systemen liegt der Fokus darauf, das Strafrecht an das digitale Zeitalter anzupassen.

Es gilt aber auch, das Strafprozessrecht in den Blick zu nehmen.

In Hessen haben wir mit der Zentralstelle zur Bekämpfung der Internetkriminalität eine bundesweit führende Strafverfolgungsbehörde geschaffen, die weit über die Grenzen Deutschlands bekannt und geschätzt ist.

Vertreter der Justiz arbeiten auch eng mit Wissenschaftlern des Frauenhofer-Instituts in Darmstadt zusammen und tauschen sich über neue Entwicklungen im IT-Bereich, aktuelle Sicherheitslücken und deren strafrechtliche Bewertung aus.

In der täglichen Arbeit unserer hochspezialisierten Staatsanwältinnen und Staatsanwälte bei der Zentralstelle zur Bekämpfung der Internetkriminalität wird immer wieder offenbar, dass deren gesetzgeberisches Handwerkszeug, das Strafgesetzbuch und die Strafprozessordnung, im Kern aus dem Jahr 1877 stammen.

Diese Gesetze weisen empfindliche Lücken in Bezug auf die neuartigen Herausforderungen der digitalen Gesellschaft auf.

Zahlreiche Rechtsprobleme, die durch die Nutzung des Mediums Internet aufgeworfen werden, sind ungelöst.

Zu nennen wären hier beispielsweise:

- fehlende gesetzliche Regelungen für die E-Mail-Überwachung,

- für die Quellen-Telekommunikationsüberwachung,

- für die Online-Durchsuchung elektronischer Speichermedien

- sowie für die beschleunigte grenzüberschreitende Sicherung digitaler Beweismittel.

Die Strafverfolgungsbehörden und Gerichte behelfen sich, soweit rechtlich möglich, mit der Anwendung von Rechtsnormen, die ursprünglich für völlig andere Sachverhalte und Kommunikationsformen vorgesehen waren.

Beispielsweise wird bei der E-Mail-Überwachung teilweise auf überkommene Regelungen zur Postbeschlagnahme und teilweise auf Regelungen zur Beschlagnahme von körperlichen Gegenständen zurückgegriffen.

Teilweise muss auch mit rechtlichen Konstruktionen gearbeitet werden, die mangels ausdrücklicher gesetzlicher Regelung mitunter sehr umstritten sind, so etwa bei der Quellen-Telekommunikationsüberwachung - also der softwaregestützten Ausleitung von Täterkommunikation am Endgerät, bevor diese verschlüsselt wird.

Vielfach lässt sich das Fehlen zeitgemäßer und notwendiger Ermächtigungsgrundlagen aber nicht kompensieren, so etwa bei der Online-Durchsuchung elektronischer Speichermedien.

Täter verschlüsseln ihre Endgeräte oder speichern ihre Daten in der Cloud.

Herkömmliche Durchsuchungs- und Beschlagnahmemaßnahmen sind damit wirkungslos, da die Täterdaten wegen der Verschlüsselung der Speichermedien nicht auswertbar sind oder - bei externer Speicherung in der Cloud - nicht aufgefunden werden können.

Das effektivste Mittel für einen erfolgreichen Zugriff auf die Täterdaten im unverschlüsselten Zustand und bei externer Speicherung ist die verdeckte Online-Durchsuchung, die aber derzeit in der Strafprozessordnung keine Rechtsgrundlage hat.

Staatsanwaltschaften, Gerichte und die Polizei benötigen aber dringend zeitgemäße Mittel, um Datenspuren zu sichern und Täter überführen zu können.

In diesem Zusammenhang gilt es auch, mit adäquaten rechtlichen Instrumenten der Grenzenlosigkeit des Internets zu begegnen.

Auf der einen Seite profitieren nämlich die Täter ungehindert von der Möglichkeit, über Internet in Echtzeit weltweit grenzüberschreitend Straftaten zu begehen.

Auf der anderen Seite erschweren Unterschiede in nationalen Gesetzeswerken und die Erforderlichkeit von Maßnahmen der internationalen Rechtshilfe in Strafsachen eine effektive Strafverfolgung.

Im Zusammenhang mit den Terroranschlägen von Brüssel sind die Unzulänglichkeiten der grenzüberschreitenden Datenübermittlung und Sicherung digitaler Beweismittel leider deutlich zutage getreten.

Deshalb habe ich Anfang des Monats auf der Justizministerkonferenz in Brandenburg einen Vorschlag unterbreitet, wie Deutschland seinen internationalen Verpflichtungen in diesem Bereich effektiver nachkommen kann.

Bislang hat es der Bundesjustizminister nämlich versäumt, die Vorgaben zur beschleunigten grenzüberschreitenden Sicherung digitaler Beweismittel aus der Cybercrime Convention, dem Budapester Abkommen über Computerkriminalität aus dem Jahre 2001 in nationales Recht umzusetzen.

Wir müssen, wie es in der Cybercrime Convention verpflichtend vorgesehen ist, eine nationale Rechtsgrundlage schaffen.

Diese Regelung muss es den deutschen und ausländischen Strafverfolgungsbehörden ermöglichen, beweiserhebliche Daten in den Händen deutscher Provider vor der Löschung zu bewahren und sie zu verpflichten, diese Daten für einen Zeitraum von bis zu 90 Tagen zu speichern.

Damit würde den Ermittlern die benötigte Zeit verschafft, diese Daten auf der Grundlage einer richterlichen Anordnung und im Wege der Rechtshilfe, die zeitaufwändig ist, abzurufen.

Andere europäische Länder haben derartige Normen längst eingeführt, Deutschland muss hier nachziehen!

Die Justizministerinnen und Justizminister der Länder waren sich hierüber einig und haben den Beschlussvorschlag Hessens einstimmig angenommen.

Für die Umsetzung dieses Vorhabens werden wir uns auch weiterhin auf Bundesebene und auf europäischer Ebene einsetzen.

Für den 27. September 2016 werden wir zu einem Expertengespräch mit Vertretern der EU-Kommission und des EP zum Thema „Grenzüberschreitende Verbesserung der Sicherung digitaler Beweismittel“ einladen.

Damit greifen wir auch die Diskussion auf, die die niederländische Ratspräsidentschaft bis Anfang des Monats mit großem Elan vorangebracht hat.

Meine Damen und Herren,

Der Kampf gegen Internetkriminalität ist auch der Kampf gegen Hasskriminalität im Internet.

Der Anstieg extremistisch motivierter Straftaten - unabhängig davon, ob sie einen politischen, religiösen oder anderweitigen Hintergrund haben - muss jedem von uns Sorgen bereiten.

Im vermeintlichen Schutz der Anonymität werden Beleidigungsdelikte begangen, die bis in den Bereich der Volksverhetzung gehen.

Es werden Drohungen ausgestoßen und ganze Personenkreise verunglimpft.

Nicht selten findet der Hass den Weg von der digitalen in die analoge Welt - in Form von Körperverletzungsdelikten, Anschlägen gegen Flüchtlingseinrichtungen oder auch in ganz konkrete Morddrohungen.

All diese Handlungen sind in der realen Welt strafbar, und sie sind es auch in der digitalen Welt. Wir müssen deshalb den Strafverfolgungsbehörden entsprechende Möglichkeiten in die Hand geben, solche Straftaten schnell und wirkungsvoll aufzuklären.

Ich bin dabei der festen Überzeugung: Wenn wir Hasskriminalität wirksam bekämpfen wollen, brauchen wir rechtsstaatlich abgesicherte Möglichkeiten, um Straftaten im Internet wirksamer als derzeit zu bekämpfen.

Hessens Kampf gegen Internetkriminalität ist deshalb auch das Bemühen, solchen Phänomenen mit Mitteln des Rechtsstaats wirksam entgegenzutreten.

Und ich betone – mit Mitteln des Rechtsstaats.

Ich spreche mich ausdrücklich dagegen aus, politisch eingesetzte Task-Forces in irgendwelchen Hinterzimmern einzusetzen, die mit Facebook und Co. verhandeln, welche Kommentare aus dem Netz genommen werden und welche im Netz bleiben.

Die Grenze der Meinungsfreiheit darf weiterhin nur demokratisch entstandenes Recht bilden.

Ich sehe insbesondere an einer Stelle Änderungsbedarf:

Betreiber von Social-Media-Plattformen, Anbieter von Instant-Messaging-Diensten und Microblogger sollten künftig verpflichtet

werden, den Strafverfolgungsbehörden auf Verlangen Auskünfte über die Identität der Nutzer unmittelbar zu erteilen.

Außerdem wollen wir, dass strafbare Inhalte, insbesondere Äußerungen mit rassistischem, fremdenfeindlichem oder sonst menschenverachtendem Charakter, vor ihrer Entfernung gesichert werden.

Und das auch dann, wenn die Unternehmen ihren Sitz in den USA oder in einem anderen Drittstaat haben.

Denn es kann nicht sein, dass Anbieter sozialer Medien zwar in Deutschland ihr Geld verdienen, mit den Strafverfolgungsbehörden aber nur über den langwierigen Weg der internationalen Rechtshilfe zusammenarbeiten.

Hier geht es auch darum, dass Unternehmen ihre gesellschaftliche Verantwortung stärker als bisher wahrnehmen.

Meine Damen und Herren,

In Hessen profitieren wir davon, schon lange eines der führenden Länder im Bereich der eJustice zu sein.

Denn die Digitalisierung hat auch ganz erheblichen Einfluss auf die Gerichtsverfahren.

Es kam nicht von ungefähr, dass das Verwaltungsgericht Gießen eines der ersten Gerichte bundesweit war, das die Kommunikation mit dem Bundesamt für Migration und Flüchtlinge vollständig auf elektronische Kommunikation umstellen konnte.

Wie wertvoll solche Beschleunigungseffekte sind, können wir jetzt bei der Bearbeitung streitiger Asylsachen erleben.

Aber auch in anderen Bereichen haben wir Strukturen für die Zukunft geschaffen.

Am 1. Januar 2016 ist das Zentrale Elektronische Schutzschriftenregister an den Start gegangen.

Schutzschriften sind vorbeugende Verteidigungsschriftsätze gegen erwartete Anträge auf Arrest oder einstweilige Verfügungen.

Früher hat jedes Gericht in Deutschland ein eigenes analoges Schutzschriftenregister geführt.

Das Zentrale Elektronische Schutzschriftenregister ist nun das erste offizielle Register, das bundesweit bei allen Gerichten hinterlegt ist.

Entwickelt wurde es von der Landesjustizverwaltung Hessen!

Wir haben darüber hinaus auch den laufenden Betrieb des Zentralen Elektronischen Schutzschriftenregisters übernommen.

Meine Damen und Herren,

das mehr als hundertjährige Bürgerliche Gesetzbuch enthält Regelungen, die in vielen Fällen erstaunlich gute und sachgerechte Antworten auf die Rechtsfragen des digitalen Zeitalters bieten.

Die Digitalisierung wirft aber auch Rechtsfragen auf, die das Bürgerliche Gesetzbuch nicht eindeutig oder nur unbefriedigend beantwortet.

Zum Beispiel:

Wie kommt ein Vertrag zustande, wenn der Kühlschrank selbständig Waren bestellt?

Welche Vertragsbeziehungen bestehen beim Streaming oder in Sozialen Netzwerken?

Besteht ein Bedürfnis für eigentumsähnliche Rechte an Daten, die man übertragen kann, in die man vollstrecken kann oder die Teil der Insolvenzmasse werden?

Was gehört zum „digitalen Nachlass“?

Welche Rechte haben Erben an den elektronischen Accounts der Erblasser, den darin befindlichen Daten wie E-Mails und Kunden-Bewertungen oder an Nutzungsrechten für E-Books, Musik und Videos?

Es sind die kleinen Alltagsfragen, die die großen rechtlichen Herausforderungen im Internet darstellen.

Und es kommt nicht von ungefähr, dass es die Länder sind, die in diesen Bereichen Druck auf den Bundesjustizminister machen, an dieser Stelle aktiv zu werden.

Denn die praktischen Fälle laufen bei den Staatsanwaltschaften und Gerichten vor Ort auf.

Hessen hat deshalb die Initiative des Landes NRW von Beginn an unterstützt, das Bürgerliche Gesetzbuch gründlich unter diesen Gesichtspunkt zu überarbeiten.

Gerade im Kontext vertraglicher Beziehungen stellt sich für mich die Frage, ob unser Persönlichkeitsrecht gut genug geschützt ist, wenn wir uns in der digitalen Welt bewegen.

Für die Aufarbeitung dieses Themas hat das Hessische Ministerium der Justiz die Federführung im Dialog mit Bund und Ländern übernommen.

Der Schutz des Persönlichkeitsrechts betrifft uns alle und macht gleichzeitig die Herausforderungen der Digitalisierung an das Recht offenbar.

Meine Damen und Herren,

in der digitalisierten Welt muss das Recht die Bürger nicht nur umfassend vor möglichen Eingriffen in ihre Privatsphäre schützen.

Das Recht muss zugleich auch Gestaltungsmöglichkeiten eröffnen, wie mit den neuen Möglichkeiten umzugehen ist.

Das gilt für Bürger und für staatliche Stellen.

Auch der Staat muss neue technische Möglichkeiten nutzen können, zum Beispiel, um den Opferschutz weiter zu verbessern.

Sie haben sicherlich noch alle die Bilder der gewalttätigen Ausschreitungen angeblicher Fußballfans bei der Europameisterschaft in Frankreich vor Augen.

Solche gewaltbereiten Hooligans sind nicht nur für friedliche Fußballfans eine Gefahr, sie binden auch Sicherheitskräfte, die die zum Schutz gegen terroristische Attacken dringend gebraucht werden.

Deshalb fordere ich, gerade bei einschlägig vorbestraften Straftätern darüber nachzudenken, ob man Ausreiseverfügungen nicht mittels elektronischer Fußfesseln durchsetzen kann.

Damit könnte man Großereignisse wie die EM insgesamt zur Schutzzone erklären und ein entsprechendes Reiseverbot europaweit wirksam durchsetzen.

Die Justizministerkonferenz hat 2015 auf meinen Vorschlag hin verabredet, die Möglichkeiten einer erweiterten elektronischen Überwachung besonders gefährlicher Straftäter - insbesondere zur Verbesserung des Opferschutzes - zu prüfen.

Meine Damen und Herren,

die digitale Gesellschaft verlangt nach zeitgemäßen rechtlichen Grundlagen, die den Bürgerinnen und Bürgern Schutz bieten und Handlungssicherheit gewähren.

Ein effektiver Schutz sowohl der Bürgerinnen und Bürger, aber auch von Verwaltung und Unternehmen ist nur möglich, wenn man die vorhandenen Spezialisten der Strafverfolgung mit den rechtlichen Mitteln versieht, die sie für ihre tägliche Arbeit brauchen.

Dies sollte nicht durch gesetzgeberisches Stückwerk, getrieben durch aktuelle Vorfälle, sondern durch eine durchdachte und abgestimmte digitale Agenda für das Recht geschehen.

Als Justizministerin werde ich für diese digitale Agenda weiterhin maßgebliche Impulse liefern!

Vielen Dank für Ihre Aufmerksamkeit!