Editorial - Grußwort des Forschungsprojektleiters «BayWiDI» Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

Herzlich willkommen zur fünften Ausgabe des BayWiDI-Newsletters. Kurz vor den bevorstehenden Sommerferien und der diesjährigen Urlaubszeit möchten wir auf aktuelle Entwicklungen im Bereich der IT-Sicherheit aufmerksam machen und einen Überblick über die Veranstaltungen der zurückliegenden Monate geben. Für diejenigen von Ihnen, die am 12. Internationalen For..Net Symposium meiner Forschungsstelle zum Thema IT-Fitness: Urheberschutz. Datenschutz.Blockchain am 27. und 28. April 2017 nicht teilnehmen konnten, wartet auf S. 2 und S. 3 ein spannender Tagungsbericht, der die Highlights der gesamten Veranstaltung für Sie zusammenfasst. Den diesjährigen 4. For.. Net Award nahm Thomas Fehn für den Preisträger Pyramics UG entgegen.

Besonders aufmerksam machen möchte ich auf das Interview mit Ferdinand Wessels, der als langjährige studentische Hilfskraft an meinem Lehrstuhl und als studentische Hilskraft von BayWiDI über seine Erfahrungen während der Projektlaufzeit berichtet. Hierbei erhalten Sie einige spannende Einblicke in das Tätigkeitsfeld einer studentischen Hilfskraft und über die Zukunftspläne von Herrn Wessels.

Der fünfte BayWiDI-Newsletter steht überwiegend im Zeichen der NIS-Richtlinie. Die Richtlinie zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU ist am 08.08.2016 in Kraft getreten. In diesem Newsletter erwartet Sie ein Vergleich mit dem IT-Sicherheitsgesetz, in dem Gemeinsamkeiten aber auch Unterschiede aufgezeigt werden. Darüber hinaus haben wir das deutsche Umsetzungsgesetz zur NIS-Richtlinie unter die Lupe genommen und die innerstaatlichen Änderungen aufgezeigt. Mit diesem Umsetzungsgesetz wird deutlich, dass dem Thema Cybersicherheit in Deutschland erhebliche Bedeutung zugemessen wird. Dies zeigt sich unter anderem anhand der Geschwindigkeit, mit der die europarechtlichen Vorgaben in deutsches Recht umgesetzt werden sollen. Die Frist seitens der EU läuft nämlich erst mit dem 09.05.2018 aus. Der letzte Beitrag befasst sich mit einer aktuell stark beachteten Entscheidung des Europäischen Gerichtshofs zur Verfassungswidrigkeit des § 15 Abs. 1 TMG und den Auswirkungen auf das innerstaatliche Recht. Zum Verfahrensablauf eines Vorabentscheidungsverfahrens vor dem Europäischen Gerichtshof sowie dessen Umsetzung durch nationale Gerichte findet sich eine verständlich erklärte Übersicht am Ende dieses Newsletters.

Mit diesen einleitenden Worten wünsche ich Ihnen eine unterhaltsame Lektüre beim Lesesen unseres fünften Newsletters. Abschließend möchte ich Ihnen auf diesem Wege bereits eine erholsame und entspannte Urlaubszeit wünschen.

Ihr
Prof. Dr. Dirk Heckmann,
Leiter des Forschungsprojekts «BayWiDI«

Inhalt

Tagungsbericht zum 12. Internationalen For..Net Symposium «IT-Fitness: Urheberschutz. Datenschutz. Blockchain.« am 27. und 28. April 2017

Die Referenten Max Schrems, Prof. Dr. Jochen Schneider, Prof. Dr. Louisa Specht, Dr. Hermann Waldhauser und Prof. Dr. Dirk Heckmann als Moderator in der Diskussion zum Thema «IT-Fitness als Herausforderung für Wissenschaft und Praxis«. © Robert Geisler

Zum 12. Mal fand in diesem Jahr das Internationale For..Net Symposium in Passau unter dem Thema «IT-Fitness : Urheberschutz. Datenschutz. Blockchain.« statt. Im Zentrum der Veranstaltung stand die Frage, ob Staat, Wirtschaft und Gesellschaft «fit« für die IT-Nutzung sind. «Fit« bedeutet in diesem Kontext in der Lage zu sein, rechtskonform und interessengerecht zu agieren. Die namhaften Referenten behandelten dabei zahlreiche Rechtsgebiete vom Datenschutzrecht bis zum Urheberrecht.

Unter der wissenschaftlichen Leitung von Prof. Dr. Dirk Heckmann, Leiter der Forschungsstelle For..Net, sowie unter der Schirmherrschaft von MdB Dorothee Bär fanden sich am 27. und 28. April 2017 zahlreiche Vertreter von Wissenschaft und Praxis in der Redoute in Passau ein, um diese Themen näher zu beleuchten.

Nach den Grußworten von Prof. Dr. Carola Jungwirth (Präsidentin der Universität Passau), von Prof. Dr. Dirk Heckmann sowie von MdB Dorothee Bär, die per Videobotschaft zugeschaltet wurde, sprach der Wirtschaftskorrespondent der F.A.Z. Dr. Hendrik Wieduwilt aus Frankfurt die Keynote «Sind Staat, Wirtschaft und Gesellschaft fit für die digitale Transformation?«. Er zeigte ein defizitäres Bild der Digitalisierung in Deutschland auf. Sowohl Wirtschaft und Bürger als auch der Staat stünden der Digitalisierung häufig aus nicht nachvollziehbaren Gründen skeptisch gegenüber, wie am Beispiel des Netzwerkdurchsetzungsgesetzes und der Charta der digitalen Grundrechte zu sehen sei, da sie im Grunde nicht nötig oder sogar schädlich sein könnten.

Im Anschluss sprach Rechtsanwalt Prof. Dr. Jochen Schneider aus München über die «Regulierung des Unregulierbaren? IT-Nutzung zwischen Recht und Wirklichkeit«. Prof. Dr. Jochen Schneider stellte zahlreiche Ansätze zur Regulierung von IT-rechtlichen Fragestellungen vor, wie etwa das kontrovers diskutierte »Recht an Daten« oder die EU-Datenschutz-Grundverordnung. Dabei ging der Referent kritisch auf viele Regelungen ein, hob jedoch auch die digitale Erschöpfung im Urheberrecht oder Softwarepatente als gute normative Ausgangspunkte hervor.

Über den «Urheberschutz in Zeiten digitaler Verunsicherung« referierte Prof. Dr. Louisa Specht von der Universität Passau. Die Digitalisierung bringe zahlreiche Herausforderungen für das Urheberrecht mit sich, die bei Verabschiedung des Gesetzes im Jahr 1965 noch nicht absehbar waren. Verdeutlicht wurde dies anhand zahlreicher Fragestellungen, wie Filesharing, Verlinken von Werken, Teilen und «Liken« von Inhalten in sozialen Netzwerken, das Einstellen von Lehrmaterialien in das Internet für Studierende und Handel mit «gebrauchten« digitalen Gütern. Besprochen wurde zudem die jüngste Rechtsprechung des EuGHs zur Rechtmäßigkeit des Streamings von nicht lizensierten Inhalten.

Der österreichische Jurist und Datenschutzaktivist Max Schrems aus Wien sprach über den «Datenschutz in Zeiten digitaler Gleichgültigkeit«. Dass Nutzer dem Datenschutz tatsächlich gleichgültig gegenüberstehen, bezweifelte er. Die Nutzer seien sich der Bedeutung durchaus bewusst, hätten

jedoch häufig keine ernstzunehmenden Ausweichmöglichkeiten. Er wies vielmehr auf eine mögliche Gleichgültigkeit seitens der Aufsichtsbehörden hin. Abschließend befürwortete Max Schrems die Einführung von Sammelklagen und Verbandsklagerechten, um eine effektivere gerichtliche Durchsetzung des Datenschutzrechts zu ermöglichen.

Rechtsanwalt Peter Hense, widmete sich dem Thema «Was vom Recht übrig bleibt: Regulierung in der Technikwelt«. Im Rahmen dieser Problemstellung stellte er zahlreiche neue, nützliche, aber auch potentiell gefährliche Techniken wie Spracherkennung, künstliche Intelligenz, vernetzte Produkte oder selbstfahrende Autos vor. Diese Technologien werfen eine Fülle von rechtlichen und tatsächlichen Fragestellungen auf. In diesem Rahmen sah Peter Hense die Diskriminierung durch Algorithmen als besondere Herausforderung an.

Über «Das Offene Auto und seine Feinde – Neue technische und rechtliche Architekturen für vernetzte, selbstfahrende Fahrzeuge« handelte der Vortrag von Prof. Dr. Lothar Determann aus Palo Alto, Kalifornien. Unter verschiedenen Gesichtspunkten wurde die Sinnhaftigkeit von offenen Autos, u.a. hinsichtlich Verbraucherschutz, Sicherheit, Urheberrecht und Datenschutz thematisiert.

Im Anschluss folgte eine Podiumsdiskussion mit Max Schrems, Prof. Dr. Jochen Schneider, Prof. Dr. Louisa Specht und Dr. Hermann Waldhauser, Heussen Rechtsanwaltsgesellschaft mbH, unter der Moderation von Prof. Dr. Dirk Heckmann zum Thema «IT-Fitness als Herausforderung für Wissenschaft und Praxis«. Die Referenten stellten sich den Fragen des Moderators und des Publikums rund um das Urheber- und Datenschutzrecht.

Am Abend fand der traditionelle Galaabend auf der Veste Oberhaus statt. Neben einem festlichen Abendessen und der Verleihung des 4. For..Net Awards an das Unternehmen Pyramics UG wurde der Abend durch eine sportliche Einlage von Esther Bell (SHENTISPORTS) unter dem Motto «Fit trotz IT?! - For..Net bewegt sich« abgerundet.

Der Vorsitzende der Gesellschaft für Freiheitsrechte, Dr. Ulf Buermeyer, eröffnete den zweiten Tag des Symposiums mit der Keynote «Nudging für eine bessere IT-Sicherheit« und stellte die These auf, dass IT-Sicherheit nur durch eine Vermischung von Anreizen und Sanktionen hergestellt werden könne. Anreize für die Gewährleistung der IT-Sicherheit seien vor allem der Wettbewerbsvorteil oder die Vermeidung eines größeren Kostenrisikos. Sanktionen könnten vor allem durch die zivilrechtliche Haftung begründet werden.

Es folgten zwei Vorträge zum Thema «Blockchain«. Als Erstes referierte Prof. Dr. Dr. Walter Blocher, Universität Kassel, unter dem Titel «Next Generation IT: Blockchain als Herausforderung für das Recht«. Er ging unter anderem auf den Abschluss von Smart Contracts ein und nannte hierfür verschiedene Anwendungsbereiche, wie beispielsweise Crowdfunding, das Rechnungswesen, das Identitätsmanagement oder das digitale Notariat. Schließlich wies er ausführlich auf die Chancen und Grenzen der Blockchain-Technologie und Smart Contracts hin.

Der zweite Vortrag erfolgte mittels eines Videofilms von Florian Weigand unter dem Titel: «Blockchain in der Unternehmenspraxis: Praxisbeispiele für den erfolgreichen Einsatz der Blockchain Technologie«. Den Schlussvortrag zu dem Thema «Neue Wertschöpfung durch Digitalisierung« eröffnete Dr. Frank Rahmstorf, vbw, München. Dieser stellte die wirtschaftspolitische und die rechtspolitische Seite der Digitalisierung dar und wies darauf hin, dass zwischen den einzelnen Bereichen Wechselwirkungen entstehen können. Abschließend ging Prof. Dr. Dirk Heckmann auf die rechtliche Seite der Digitalisierung ein und stellte in diesem Zusammenhang nochmals einen Bezug zur Blockchain-Technologie her. Prof. Dr. Dirk Heckmann beendete seinen Vortrag mit dem Hinweis, dass die Blockchain-Technologie eine Weiterentwicklung des Netzwerkgedankens darstelle, die jedoch auch neue Herausforderungen mit sich bringe und für die neue Lösungsansätze entwickelt werden müssten.

Das 13. Internationale For..Net Symposium wird unter dem Thema «Wertschöpfung durch Digitalisierung. Innovation, Vertrauen und Sicherheit« am 11. und 12. April 2018 in Passau stattfinden. Die Aufzeichnungen der Vorträge des Symposiums können über die Webseite von For..Net (https://www.for-net.info/symposien/symposium-2017/programm/) abgerufen werden.

Prof. Dr. Dirk Heckmann mit Thomas Fehn, CEO von Pyramics UG, Gewinner des 4. For..Net Awards. ©Preinfalk/Opitz

Interview mit der studentischen Hilfskraft von BayWiDI über die Erfahrungen während des Projekts

v.l. Anne Paschke, Geschäftsführerin For..Net, Martin Scheurer, Stipendiat am GRK 1861/2 und Ferdinand Wessels, studentische Hilfskraft BayWiDi. © Robert Geisler

1. Wie lange sind Sie bereits als studentische Hilfskraft am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht von Herrn Prof. Dr. Heckmann beschäftigt und wie lange arbeiten Sie bereits am BayWiDI-Projekt?

Ich bin bereits seit Januar 2014 als studentische Hilfskraft am Lehrstuhl von Herrn Professor Heckmann beschäftigt. Speziell dem Projekt BayWiDI bin ich seit Projektbeginn Mitte des Jahres 2015 zugeordnet.

2. Wie sind Sie auf den Forschungsbereich von Herrn Professor Heckmann während Ihres Jurastudiums aufmerksam geworden?

Zum Zeitpunkt meiner Bewerbung bei Herrn Prof. Heckmann fand ich den Bereich des IT-Rechts zwar durchaus interessant, hatte aber letztendlich noch keine genauen Vorstellungen von den einzelnen Teilbereichen. Meine «Leidenschaft« ist dann vor allem durch meine Tätigkeit am Lehrstuhl entstanden, die mich auch dazu bewogen hat, in diesem Bereich meinen Studienschwerpunkt zu absolvieren.

3. In welchem Bereich des IT-Rechts liegen Ihre persönlichen Stärken und Affinitäten?

Das größte Interesse habe ich für den Bereich des Datenschutzrechts. Dieser Teilbereich hat mich in der gesamten Zeit meiner Lehrstuhltätigkeit am meisten beschäftigt und aufgrund seiner gesellschaftlichen Relevanz und ständigen Aktualität immer begeistert. Die Arbeit am Lehrstuhl hat es mir zudem ermöglicht, bereits mehrere Fachbeiträge im Bereich des Datenschutzrechts zu publizieren (vgl. exemplarisch *Wessels*, Dashcams im Lichte des Datenschutzes – Beweissicherung vs. Informationelle Selbstbestimmung, JurPC Web-Dok. 186/2015). Mein gegenwärtiges Ziel ist es, nach erfolgreichem Abschluss der Ersten Juristischen Staatsprüfung in diesem Bereich zu promovieren.

4. Welche Aufgaben nehmen Sie im Bereich der BayWiDI-Projektarbeit wahr?

Als studentische Hilfskraft unterstütze ich den Lehrstuhl insbesondere im Rahmen der Bereitstellung des BayWiKIs. Dazu zählen insbesondere wissenschaftliche Recherchen und die Aufbereitung von aktuellen Themen der IT-Sicherheit sowie die Unterstützung der wissenschaftlichen Mitarbeiter bei der Kommentierung von Vorschriften des IT-Sicherheitsrechts. Daneben bin ich selbstständig mit der Aktualisierung der Online-Plattform betraut.

5. Was interessiert Sie besonders an der Projektarbeit bei BayWiDI?

Das IT-Sicherheitsrecht ist von hoher gesellschaftlicher Relevanz und wird voraussichtlich in den kommenden Jahren immer stärker an Bedeutung gewinnen. Das Projekt setzt auf die enge Zusammenarbeit von wissenschaftlicher Forschung mit betroffenen mittelständischen Unternehmen und ermöglicht eine praxisnahe und wirklichkeitsgetreue rechtliche Auseinandersetzung mit dem Thema «IT-Sicherheit«. Zudem ist das Recht der IT-Sicherheit ein sehr «junges« Rechtsgebiet, was juristisch gesehen zum einen großen Forschungsbedarf und zum anderen viele neue berufliche Perspektiven eröffnet. Ich könnte mir auch ein Praktikum bei einem der großen Projektpartner wie der Synaxon AG im Rahmen meines Studiums vorstellen.

6. Hat die Projektarbeit bei BayWiDI Auswirkungen auf Ihre IT-Rechts Affinität hinterlassen?

Durch die Projektarbeit konnte ich mich mit den Problemstellungen des Rechts der IT-Sicherheit vertraut machen und ein grundlegendes Bewusstsein für die Probleme der IT-Sicherheit (auch speziell in technischer Hinsicht) entwickeln. Gerade aber durch die Mitwirkung bei der Erstellung des BayWiKIs habe ich mir mein derzeitiges Wissen auf dem Bereich des IT-Sicherheitsrechts aneignen können.

Vertiefungshinweise:

- ***Wessels,*** http://www.jurpc.de/jurpc/show?id=20150186.

Die europäische NIS-Richtlinie und das deutsche IT-Sicherheitsgesetz - Ein Vergleich

Das europäische Gesetzgebungsverfahren zum Erlass der Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS-Richtlinie) ist mit der Annahme des Rechtssetzungsakts durch das EU-Parlament am 06.07.2016 abgeschlossen worden. Die Richtlinie trat am 08.08.2016 nach der Veröffentlichung im Amtsblatt der EU am 19.07.2016 in Kraft. Auch der Name der Richtlinie hat sich im Gesetzgebungsverfahren geändert. Die aktuelle Fassung lautet «Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU«. Die wichtigsten Meilensteine der Richtlinie sind folgende:

- **09.02.2017: Ablauf der Frist für die Vertretung in der Kooperationsgruppe und im CSIRTs (Computer Security Incident Response Teams) -Netzwerk**
- **09.05.2018: Ablauf der Umsetzungsfrist zur Schaffung der neuen, durch die Richtlinie geforderten Rechts- und Verwaltungsvorschriften für die EU-Mitgliedstaaten**
- **10.05.2018: Anwendung der neuen mitgliedstaatlichen Regelungen zur NIS-Richtlinie**
- **09.11. 2018: Ablauf der Ermittlungsfrist für die Betreiber «wesentlicher Dienste«**
- **09.05.2019: Erstellungsfrist für den Kohärenzbericht zur Ermittlung der Betreiber wesentlicher Dienste**
- **09.05.2019: Erster Erfahrungsbericht der EU-Kommission zur RL-Umsetzung**

Nach Art. 4 NIS-RL sind von dem Begriff der «Betreiber wesentlicher Dienste« sowohl öffentliche als auch private Anbieter umfasst. Insofern scheint der

Anwendungsbereich der NIS-Richtlinie gegenüber dem IT-Sicherheitsgesetz auf den ersten Blick deutlich erweitert zu sein. Im Anhang II der Richtlinie fehlt allerdings eine Benennung der Kategorie «Staat und Verwaltung«. Eine zentrale Zielsetzung der NIS-RL liegt im Schutz von Betreibern «wesentlicher Dienste«. Obwohl der Begriff nicht deckungsgleich mit dem der «kritischen Infrastruktur« im IT-Sicherheitsgesetz ist, wird hierunter wohl dasselbe zu verstehen sein. Die Mitgliedstaaten müssen bis zum 09.11.2018 die Betreiber solcher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet ermitteln.

Ein weiterer inhaltlicher Schwerpunkt der NIS-RL liegt in dem Schutz von Anbietern digitaler Dienste, vgl. Art. 16 ff. NIS-RL. Hierunter versteht man jede, in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers, erbrachte Dienstleistung. Eine Konkretisierung der Arten von digitalen Diensten findet sich im Anhang III der Richtlinie als Online-Marktplatz, Online-Suchmaschine und Cloud-Computing-Dienst. Im Vergleich zum IT-Sicherheitsgesetz richten sich die Voraussetzungen für einen «digitalen Dienst« nach Art. 13 Abs. 7 TMG. Die NIS-Richtlinie schreibt hingegen vor, dass die Anbieter digitaler Dienste geeignete und verhältnismäßige technische sowie organisatorische Maßnahmen ergreifen müssen, um unter Berücksichtigung des Stands der Technik, Risiken für die Netz- und Informationssicherheit zu bewältigen.

Obwohl die Umsetzung der NIS-Richtlinie umfangreicher als anfangs geplant ausgefallen ist, werden sich die Befürchtungen eines «doppelten Regulierungsaufwands« wohl nicht bewahrheiten. Dass es zu einer Änderung oder gar Erweiterung der Sektoren kritischer Infrastrukturen kommt, ist nach derzeitigem Kenntnisstand wohl nicht zu erwarten. Es wird den Betreibern Kritischer Infrastrukturen von Experten empfohlen, die Anforderungen des IT-Sicherheitsgesetzes umzusetzen (vgl. Kipker, a.a.O.).

Vertiefungshinweise:

- ***Kipker,*** ZD-Aktuell 2016, 05261
- ***Voigt/Gehrmann,*** ZD 2016, 355
- ***Freudenberg/Witt,*** CR 2016, 657

Das Umsetzunggesetz zur NIS-Richtlinie

Im August 2016 trat die NIS-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union in Kraft. Die NIS-Richtlinie sieht nach Art. 25 Abs. 1 NIS-RL vor, dass die Vorgaben von den Mitgliedstaaten bis zum 9. Mai 2018 in nationales Recht umzusetzen sind. Der deutsche Gesetzgeber hatte bereits 2015 das IT-Sicherheitsgesetz erlassen und hiermit umfangreiche Vorgaben für die IT-Sicherheit geschaffen, dennoch bedarf es in einigen Punkten der Nachbesserung. Deshalb hat der Deutsche Bundestag am 27. April 2017 das entsprechende Umsetzungsgesetz beschlossen.

Dieses bringt unter anderem neue Verpflichtungen für die Anbieter digitaler Dienste. Diese werden zukünftig als besonders wichtig für die Funktionsfähigkeit des EU-Binnenmarkts definiert und erhalten somit einen Status der vergleichbar mit dem kritischer Infrastrukturen ist. Somit kommen auf die Anbieter digitaler Dienste vergleichbare Maßnahmen technischer und organisatorischer Art zu wie sie bereits für Anbieter kritischer Infrastrukturen bestehen. Ebenso ist für diese Anbieter fortan eine Meldepflicht vorgesehen.

Betreiber von Energieversorgungsnetzen und Energieanlagen trifft nun gleichfalls eine neue Meldepflicht. Zukünftig sind Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten oder Prozesse, die tatsächlich zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben zu melden. Gleiches gilt bei erheblichen Störungen des IT-Systems, seiner Komponenten oder Prozesse, die lediglich zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit führen können. Auch hier wird sich an die Kriterien für kritische Infrastrukturen angepasst.

Ferner wurden Änderungen im Telekommunikationsgesetz vorgenommen. Hiervon sind hauptsächlich datenschutzrechtliche Aspekte und das Vorgehen im Falle von technischen Störungen betroffen. § 100 Abs. 1 TKG, sog. «kleine Vorratsdatenspeicherung«, wird so geändert, dass es Diensteanbietern nun erlaubt ist die Steuerdaten des informationstechnischen Protokolls zur Datenübertragung zu erheben und für Zwecke der IT-Sicherheit zu verwenden. Da Kommunikationsdaten hiervon nicht betroffen sind, wurden gleichfalls Änderungen vorgenommen, welche personenbezogenen Daten den Eingang in das TKG eröffnen. Der Diensteanbieter darf künftig die Nutzung des TK-Dienstes einschränken, wenn von den informationstechnischen Systemen der Nutzer Gefahren für das TK-Netz ausgehen.

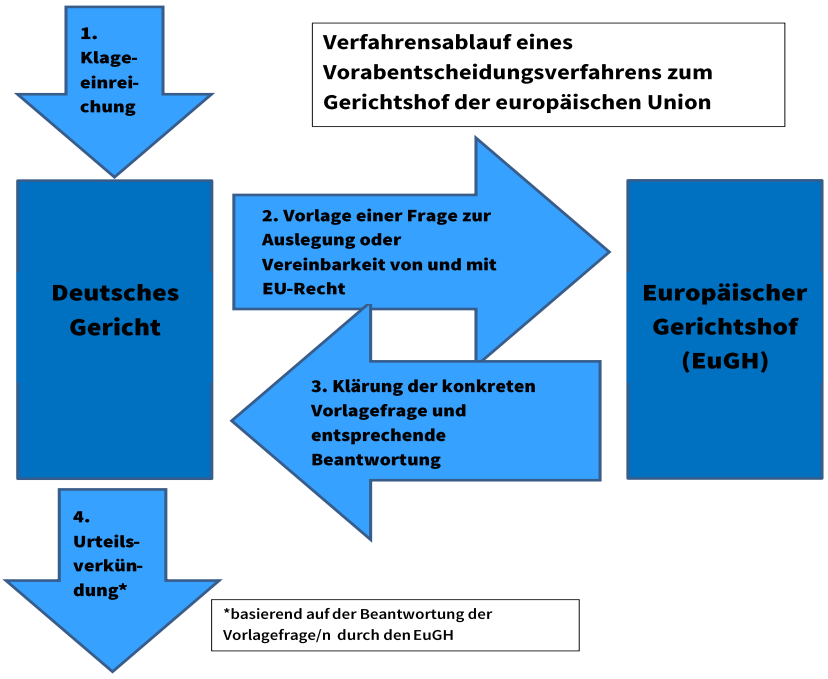
Mit dem Umsetzungsgesetz der NIS-RL erreicht die Cybersicherheits-Gesetzgebung der letzten Jahre ihren vorläufigen Endpunkt. Diese wurde von Cyber-Sicherheitsstrategien der Bundesregierung 2011 und 2016 sowie der Europäischen Kommission 2013 eingeleitet. Auch dieses Umsetzungsgesetz zeigt – Deutschland ist im europäischen Vergleich im Bereich der IT-Sicherheit weit voraus. So bringt es kaum Überraschungen für die Betreiber betroffener Dienste mit sich. Obwohl der Endpunkt dieser Gesetzgebung zwar zunächst erreicht sein mag, bedarf er wohl dennoch in einigen Jahren der Novellierung aufgrund der sich stets ändernden Bedrohungslage. Bis dahin ist jedoch die Umsetzung und Zertifizierung der neuen rechtlichen Vorgaben im Mittelpunkt.

Vertiefungshinweise:

- ***Gehrmann,*** DSRITB 2016, 263.
- ***Kipker,*** ZD-Aktuell 2016, 05261.
- ***Kipker,*** MMR-Aktuell 2017, 389121.

EuGH: § 15 Abs. 1 TMG ist europarechtswidrig!

Der Europäische Gerichtshof, das oberste Gericht der europäischen Union, hat am 19. Oktober 2016 § 15 Abs. 1 TMG für europarechtswidrig erklärt. Der europäische Gerichtshof hatte hierüber im Rahmen eines Vorabentscheidungsverfahrens durch den Bundesgerichtshof zu entscheiden. Die betreffende Vorschrift regelt die Erhebung und Verwendung personenbezogener Daten im Zusammenhang mit Telemediendiensten in Deutschland und wurde im Rahmen der Umsetzung einer Richtlinie eingeführt.



Im deutschen Ausgangsverfahren wurde die Aufzeichnung und Speicherung von IP-Adressen beim Zugriff auf Webseiten der Bundesrepublik moniert. Gegen das Urteil der Berufungsinstanz legten die Parteien Rechtsmittel ein, sodass der Rechtsstreit am BGH anhängig war. Nach deutschem Recht handelt es sich bei IP-Adressen um Nutzungsdaten, weshalb deren Erhebung und Verarbeitung den speziellen Vorschriften des TMG unterliegt. Eine Erhebung und Verarbeitung wäre nach dem hier einschlägigen § 15 Abs. 1 TMG nur rechtmäßig, wenn die Daten für die Nutzung des Dienstes erforderlich wären.

Die §§ 11 ff. TMG beruhen auf der Umsetzung der EU-Datenschutzrichtlinie und § 15 Abs. 1 TMG im Konkreten auf Art. 7 der RL. Richtlinien sind von der EU erlassene Rechtsakte, die durch nationale Rechtsakte wiederum umgesetzt werden und so Wirksamkeit erlangen. Ist ein nationales Gericht der europäischen Union bzgl. der Auslegung einer solchen Richtlinie und des national umgesetzten Rechts unsicher, kann es zur Auslegung dessen den EuGH anrufen und um Spezifizierung bitten (siehe Schaubild zum Verfahrensablauf eines Vorabentschiedungsverfahrens). Dies dient einer einheitlichen und effektiven Auslegung und Anwendung des Unionsrechts in den einzelnen Mitgliedstaaten.

Verfahrensgang:

1. AG Berlin-Tiergarten - Urt. v. 13.08.2008 – 2 C 6/08
2. LG Berlin - Urt. v. 31.01.2013 – 57S 87/08
3. BGH - Urt. v. 28.10.2014 – VI ZR 135/13
4. EuGH – Urt. v. 19.10.2016 – C-582/14
5. BGH – Urt. v. 16.05.2017 - VI ZR 135/13.

In diesem Fall legte der BGH folgende Vorlagefrage bzgl. der Auslegung des Art. 7 lit. f der Datenschutzrichtlinie vor:

Steht Art. 7 der RL einer Auslegung entgegen, nach der Anbieter von Online-Mediendiensten die personenbezogenen Daten eines Nutzers ohne dessen Einwilligung nur erheben und verwenden dürfen, wenn dies erforderlich ist, um konkrete Dienste beanspruchen zu können, ohne dass der Zweck (die Funktionsfähigkeit zu gewährleisten) die Verwendung über den eigentlichen Nutzungsvorgang hinaus rechtfertigen kann.

Art. 7 lit. f der RL rechtfertigt eine Verarbeitung personenbezogener Daten, wenn der Verarbeitende ein berechtigtes Interesse an der Verarbeitung hat und nicht das Interesse oder die Grundrechte bzw. Grundfreiheiten des Betroffenen überwiegen. Der EuGH hatte bereits in einem anderen Verfahren entschieden, dass die in Art. 7 der RL aufgeführten Rechtfertigungsgründe abschließend seien und weder neue Grundsätze, noch zusätzliche Bedingungen durch die Mitgliedstaaten gestellt werden dürfen.

Nach § 15 Abs. 1 TMG wäre eine Verarbeitung personenbezogener Daten über das Ende des tatsächlichen Vorgangs hinaus generell nicht möglich. Somit ist das innerstaatliche Recht deutlich enger gefasst als die Grundsätze des Art. 7 der EU-Datenschutzrechtlinie.

Die deutsche Umsetzung definiert den Begriff der RL nicht nur näher, sondern schränkt ihn darüber hinaus ein. Art. 7 lit. f der RL soll nach Ansicht des EuGHs den generellen Ausschluss einer solchen Verarbeitung gerade vermeiden und vielmehr eine Einzelfallabwägung im konkreten Fall ermöglichen. Die deutsche Regelung nimmt jedoch eine solche Abwägung vorweg, indem sie keinen Raum für konkrete Umstände im Einzelfall lässt. Aus dieser Auslegung des EuGHs

folgt, dass die Zweckbegrenzung des § 15 Abs. 1 TMG dem Art. 7 der RL entgegensteht und somit europarechtswidrig ist.

Die Europarechtswidrigkeit des § 15 Abs. 1 TMG ist für die Praxis von enormer Bedeutung. Dies gilt jedoch nur bis zum Inkrafttreten der Datenschutzgrundverordnung (DS-GVO) im Mai 2018. Bis dahin muss § 15 Abs. 1 TMG richtlinienkonform ausgelegt werden. Hierzu muss eine Einzelfallabwägung im Rahmen der Erforderlichkeit vorgenommen werden um Art. 7 der RL nicht weiter einzuschränken.

So verfährt auch der BGH in der Praxis. In dem auf die Entscheidung des EuGHs folgendem Urteil, stellte der 6. Senat des Bundesgerichtshofs fest, dass nur dynamische IP-Adressen personenbezogene Daten sind, da die BRD über die rechtlichen Mittel verfügt, um den konkreten Nutzer zu identifizieren. Offen blieb hingegen die Frage, ob eine Speicherung für die Funktionsfähigkeit der angebotenen Dienste erforderlich sei. Für die Beantwortung dieser Frage sei die Beweisführung im Ausgangsverfahren vor dem LG Berlin nicht ausreichend gewesen.

Ab Mai 2018 gibt es in Deutschland durch die Umsetzung der Datenschutzgrundverordnung keinen Erlaubnistatbestand für die Verarbeitung von personenbezogenen Daten für die durch Private betriebene Webseiten. Obwohl die Europarechtswidrigkeit demnach nur noch von kurzer Dauer ist, bleibt Art. 7 lit. f der RL weiterhin unmittelbar relevant.

Letztendlich bedeutet dies, dass die Speicherung dynamischer IP-Adressen zur Abwehr von Gefahren durch Cyberattacken zulässig sein kann. Im Rahmen einer Interessenabwägung müssen die betroffenen Grundrechte miteinander abgewogen werden. Für den konkreten Fall hat dies das Berufungsgericht zu entscheiden.

Vertiefungshinweise:

- ***Kartheuser/Gilsdorf***, MMR-Aktuell 2016, 382533.
- ***Mitterer/Wiedemann/Zwissler,*** BB 2017, 3.
- ***Schüßler***, jurisPR-ITR 2/2012 Anm. 3.

Der nächste Newsletter erscheint am 15. Oktober 2017.

Sie finden den Newsletter und die Möglichkeit, sich an-, bzw. abzumelden auch unter https://www.baywidi.de/

Hinweise, Anregungen, Lob und Kritik sind herzlich Willkommen. Schreiben Sie einfach an baywidi@uni-passau.de

Impressum

Universität Passau
Innstraße 41
94032 Passau
Telefon: 0851/509-0
Telefax: 0851/509-1005
E-Mail: praesidentin@uni-passau.de
Internet: www.uni-passau.de
USt-Id-Nr.: DE 811193057

Organisation
Gemäß Art. 4 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

Vertretung:
Die Universität Passau wird von der Vorsitzenden des Leitungsgremiums, Präsidentin Prof. Dr. Carola Jungwirth, gesetzlich vertreten. Verantwortliche im Sinne des § 5 TMG (Telemediengesetz) ist die Präsidentin. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.