TAGUNGSBERICHT VON DER 18. HERBSTAKADEMIE DER DEUTSCHEN STIFTUNG FÜR RECHT UND INFORMATIK (06.-09. SEPTEMBER 2017 AN DER UNIVERSITÄT HEIDELBERG)

ALMAN HUKUK VE BİLİŞİM VAKFI ON SEKİZİNCİ GÜZ AKADEMİSİ TOPLANTI RAPORU (06-09 EYLÜL 2017, HEIDELBERG ÜNİVERSİTESİ)

Dr. Marian Alexander ARNING*

ÖZ

2017 yılının Eylül ayında, Heildelberg'de Alman Hukuk ve Bilişim Vakfı'nın[1] 18. Güz Akademisi gerçekleşmiştir. Akademinin bu seneki konusu, "Hukuk 4.0, Hukuk Laboratuvarlarından Yenilikler" olmuştur. Bilişim hukuku alanındaki gelişmelere ve sorunlara yönelik yaklaşık elli sunum yapılmış ve yaklaşık üç yüz katılımcı ile tartışmalar gerçekleştirilmiştir. Toplantının ağırlıklı konularından birisi AB Genel Veri Koruma Tüzüğü ve özellikle bu tüzük ile getirilen yeni gereksinimlerin uygulamaya nasıl aktarılacağı olmuştur. Örnek olarak şirketlerin veri koruma organizasyonu, veri taşınabilirliği hakkı, verilerin iş kotarımı, uluslararası veri transferi ve sağlık verilerinin tıbbi amaçlara yönelik olarak ya da araştırma amacıyla işlenmesine ilişkin meseleler zikredilebilir. Bir diğer ağırlıklı konu ise, otomasyona ilişkin hukuki sorunlar olmuştur. Bu konuya örnek olarak robotların ve "Ledger Tech" / "Blockchain" kullanımları verilebilir. Bu bağlamda konuşmacılar konuyu özellikle sözleşmeler, sorumluluk, tüketicinin korunması, rekabet ve fikri mülkiyet açılarından tartışmışlardır. Bu toplantı raporunda kısaca AB Veri Koruma Hukuku'na giriş niteliğinde seçilmiş bazı sunumlar takdim edilmiş ve açıklanmıştır. Geneline bakıldığında çok yönlülük ve nitelik bakımından seçkin sunumların yer aldığı başarılı bir etkinlik olan Güz Akademisi'ne, bu alana ilgi duyan hukukçuların katılımları tavsiye edilmektedir.

Anahtar Kelimeler: *Veri Koruma, AB Genel Veri Koruma Tüzüğü, Otomasyon, Yapay Zekâ, Botlar*

---

* Türk-Alman Üniversitesi Hukuk Fakültesi Medeni Hukuk Anabilim Dalı Öğretim Üyesi, (arning@tau.edu.tr). ORCID: 0000-0002-6290-1301

[1] Deutsche Stiftung für Recht und Informatik.

CONFERENCE REPORT: 18TH FALL ACADEMY OF THE GERMAN FOUNDATION FOR LAW AND INFORMATICS (06.-09. SEPTEMBER 2017, UNIVERSITY OF HEIDELBERG)

ABSTRACT

In September 2017 the 18th Fall Academy of the German Foundation for Law and Informatics[2] on "Law 4.0 – Innovations from legal laboratories" took place in Heidelberg/Germany. In app. 50 presentations recent developments and problems in the field of Information Technology Law were explained and then discussed with app. 300 participants. The conference focused on the General Data Protection Regulation (GDPR), especially on how the new requirements stemming from the GDPR can be implemented, e.g. with respect to data protection organisation, the right to data portability, the processing of data on behalf of a controller, international data transfers and the processing of health data for medical (research) purposes. Another focus of the conference was on the legal problems of the (increasing) automation, e.g. with respect to the use of bots and ledger tech/blockchain applications. In this context, the speakers dealt escpecially with contractual, liability, consumer protection, competition and intellectual property law issues. After a (short) introduction to the EU data protection law, this conference report focuses on selected presentations that were given at the Fall Academy. All in all, the Fall Academy was (again) a very successfull conference, especially due to the high number of excellent and interesting presentations, so that the Fall Academy is highly recommended for all lawyers interested in Information Technology Law.

Keywords: *Data Protection, General Data Protection Regulation, Automation, Artificial Intelligence, Bots*

[2] Deutsche Stiftung für Recht und Informatik.

EINLEITUNG

Vom 06.-09.09.2017 fand zum achtzehnten Mal die Herbstakademie der Deutschen Stiftung für Recht und Informatik statt, die sich mittlerweile zur wohl wichtigsten Tagung zum Informationstechnologierecht in Deutschland entwickelt hat.[3] Dieses Mal trafen sich die ca. 300 Teilnehmer, vor allem junge Juristen aus der Wissenschaft, aus Unternehmen und Kanzleien, an der Universität Heidelberg, um dort unter dem Tagungsthema „*Recht 4.0 - Innovationen aus den rechtswissenschaftlichen Laboren*" über aktuelle und zukünftige Entwicklungen im IT-Recht zu diskutieren. Die Schwerpunkte der Tagung mit ihren ca. 50 Vorträgen lagen dabei zum einen auf der neuen Datenschutz-Grundverordnung und zum anderen auf dem Bereich der Automatisierung.[4] Diese inhaltlichen Schwerpunkte werden im folgenden Beitrag näher betrachtet.

1. Das neue Datenschutzrecht in der EU

Um die Vorträge zur neuen Datenschutz-Grundverordnung besser nachvollziehen zu können, wird im Folgenden zunächst das europäische Datenschutzrecht in der gebotenen Kürze erläutert.

1.1. Die „alte" Rechtslage: die Datenschutzrichtlinie 95/46/EG

Das Datenschutzrecht in der EU hat im Jahr 2018 einen großen Umbruch erfahren. Bis zum 25. Mai 2018 wurde es auf EU-Ebene vor allem durch die Datenschutzrichtlinie 95/46/EG geregelt.[5] Wie jede Richtlinie musste sie von den EU-Mitgliedstaaten in nationales Recht umgesetzt

[3] Weitere Informationen zur Herbstakademie der Deutschen Stiftung für Recht und Informatik finden sich unter: http://www.dsri.de/herbstakademie/herbstakademie.html, (01.11.2018).

[4] Aufzeichnungen der einzelnen Vorträge finden sich unter: http://www.dsri.de/herbstakademie/herbstakademie_2017-vortraege.html, (01.11.2018).

[5] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A31995L0046. Daneben ist insbesondere noch die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) von Relevanz, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32002L0058, (02.11.2018).

werden. In Deutschland erfolgte dies insbesondere durch das Bundesdatenschutzgesetz a.F. (BDSG a.F.),[6] die Datenschutzgesetze der einzelnen Bundesländer a.F.[7] und – vor allem für Webseitenbetreiber - durch das Telemediengesetz (TMG).[8]

Auch wenn der EuGH in seiner Lindqvist-Entscheidung[9] in diesem Zusammenhang feststellte, dass die Datenschutzrichtlinie 95/46/EG nicht nur einen datenschutzrechtlichen Mindeststandard festgelegt, sondern das Datenschutzrecht innerhalb der EU grundsätzlich umfassend harmonisiert habe,[10] war in der Praxis zu beobachten, dass die Datenschutzgesetze in den einzelnen EU-Mitgliedstaaten mitunter doch erheblich voneinander abwichen.[11] Dies führte u.a. zu einem unterschiedlichen Schutzniveau im Hinblick auf die Privatsphäre der von der jeweiligen Datenverarbeitung betroffenen Personen, aber auch zu Schwierigkeiten im Hinblick auf das zweite Ziel der Datenschutzrichtlinie 95/46/EG: den freien Verkehr personenbezogener Daten zwischen den EU-Mitgliedstaaten (Art. 1 Datenschutzrichtlinie 95/46/EG).

1.2. Die neue Rechtslage: die Datenschutz-Grundverordnung

Vor diesem Hintergrund und aufgrund der rasanten technologischen Entwicklung entschied sich der europäische Gesetzgeber daraufhin, die doch stark „in die Jahre gekommene" Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995 durch eine Verordnung zu ersetzen, die keiner Umsetzung mehr durch die einzelnen Mitgliedstaaten bedarf und somit das Datenschutzrecht innerhalb der EU vereinheitlicht.[12] Nachdem die EU-Kommis-

---

[6] Das BDSG a.F. ist z.B. abrufbar unter: https://dejure.org/gesetze/BDSG_a.F, (02.11.2018).

[7] Links zu den aktuellen Gesetzen finden sich z.B. unter: https://www.audatis.de/ratgeber/lexikon/aufsichtsbehoerden-landesdatenschutzgesetze/, (02.11.2018).

[8] Das TMG ist z.B. abrufbar unter: https://www.gesetze-im-internet.de/tmg/, (02.11.2018).

[9] EuGH, Urt. v. 6.11.2003, Rs. C-101/01, abrufbar unter: http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30d6e79237b6de094a5db2e0ec1d0a5f662a.e34KaxiLc3qMb40Rch0SaxyMbhz0?text=&docid=48382&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=522670, (03.11.2018).

[10] EuGH, Urt. v. 6.11.2003, Rs. C-101/01, Rz 96.

[11] Siehe z.B. *Kühling/Raab,* in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., Einführung Rn. 73.

[12] Die DSGVO enthält allerdings eine Vielzahl an Öffnungsklauseln. Unter den dort genannten Bedingungen dürfen die EU-Mitgliedstaaten und teilweise auch die EU selbst (nationale) Regelungen erlassen, welche die DSGVO ergänzen.

sion im Januar 2012 einen ersten Entwurf für die sogenannte „Datenschutz-Grundverordnung“ (DSGVO) veröffentlichte, [13] wurde sie im April 2016 nach schwierigen und langen Verhandlungen zwischen dem Rat der EU, dem Europäischen Parlament und der EU-Kommission beschlossen und trat – wie bei Verordnungen üblich – 20 Tage nach ihrer Veröffentlichung im Amtsblatt in Kraft.[14] Nach Art. 99 Abs. 2 DSGVO schloss sich hieran zunächst aber noch eine zweijährige Übergangszeit an, während der die DSGVO noch nicht anwendbar war und mithin die „alten“ Datenschutzgesetze zu beachten waren. So erforderten die Regelungen der DSGVO teilweise erhebliche Anpassungen der Datenverarbeitungsprozesse und der internen Organisation in Unternehmen, Behörden und anderen datenverarbeitenden Stellen. Die Übergangsfrist sollte es ihnen ermöglichen, diese vorzunehmen, bevor die neuen Regelungen anwendbar wurden. Der Stichtag hierfür war der 25. Mai 2018 – seit diesem Tag gilt die DSGVO.

1.3. Wesentliche Inhalte der DSGVO

Die DSGVO setzt die auch zuvor schon im Datenschutzrecht geltenden Grundprinzipien grundsätzlich fort. Die wichtigsten von ihnen lauten:

- **Sachlicher Anwendungsbereich: personenbezogene Daten**. Die DSGVO gilt gem. Art. 2 Abs. 1 DSGVO für personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO, also für Daten über zumindest identifizierbare natürliche Personen, die im Datenschutzrecht „betroffene Personen“ genannt werden. Hierbei muss die Identität der betroffenen Personen nicht zwingend direkt aus der verarbeiteten Information selbst hervorgehen. Es reicht unter Umständen auch aus, wenn sich die Information mit anderen Informationen verknüpfen lässt und sich die betroffene Person auf dieser Grundlage identifizieren lässt (Beispiel: „Die Person mit der Telefonnummer 12345 hat mich angerufen“. Aus dieser Information lässt sich die Identität des Anrufers nicht direkt entnehmen. Diese Information kann – sofern vorhanden - aber mit dem zu dieser Nummer gehörenden Telefonbucheintrag verknüpft werden (Max Mustermann: 12345). Durch die Verknüpfung mit dieser Information kann der Anrufer identifiziert wer-

[13] Der Entwurf ist abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF, (04.11.2018).

[14] Siehe z.B. die Übersicht unter: http://www.computerundrecht.de/26378.htm, (04.11.2018).

den, so dass es sich bei der Information „Die Person mit der Telefonnummer 12345 hat mich angerufen“ um ein personenbezogenes Datum handelt).[15]

- **Verarbeitungsverbot mit Erlaubnisvorbehalt**. Die DSGVO setzt auch das sogenannte „Verarbeitungsverbot mit Erlaubnisvorbehalt“ fort. Demnach ist die Verarbeitung personenbezogener Daten grundsätzlich verboten. Ausnahmsweise ist die Verarbeitung solcher Daten allerdings zulässig, wenn entweder eine Rechtsvorschrift diese Verarbeitung erlaubt oder die betroffene Person ihre Einwilligung hierzu erteilt hat. Rechtsvorschriften, die die Verarbeitung personenbezogener Daten erlauben, finden sich insbesondere in Art. 6 Abs. 1 DSGVO und in Art. 9 Abs. 2 DSGVO.

- **Zweckbindungsgrundsatz**. Nach Art. 5 Abs. 1 lit. b DSGVO und Art. 6 Abs. 4 DSGVO dürfen personenbezogene Daten grundsätzlich nur für den Zweck verarbeitet werden, für den sie erhoben wurden, also z.B. zur Durchführung eines bestimmten Vertrages. Die Verarbeitung zu einem anderen Zweck (z.B. zu Zwecken der Werbung) ist nur unter bestimmten, insbesondere den in Art. 6 Abs. 4 DSGVO festgelegten Bedingungen zulässig.

Allerdings hat die DSGVO auch erhebliche Änderungen im Vergleich zu den zuvor geltenden Datenschutzgesetzen mit sich gebracht. Die wohl wichtigsten Änderungen lauten:

- **Erweiterter räumlicher Anwendungsbereich**. Für türkische Unternehmen ist besonders die Erweiterung des räumlichen Anwendungsbereiches in Art. 3 DSGVO relevant. So findet die DSGVO nach Art. 3 Abs. 1 DSGVO – ähnlich wie zuvor die Datenschutzrichtlinie 95/46/EG – Anwendung, wenn die Datenverarbeitung im Rahmen der Tätigkeiten einer Niederlassung einer datenverarbeitenden Stelle in der EU erfolgt – und zwar unabhängig davon, ob die Verarbeitung (technisch) in der EU stattfindet oder nicht, also z.B. der verwendete Server in der EU steht oder

[15] Welche Mittel bei der Ermittlung des Personenbezugs zu berücksichtigen sind, ist umstritten (siehe z.B. *Klar/Kühling,* in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl., Art. 4 Nr. 1 Rn. 17 ff.; *Schmitz*, in: Moos/Schefzig/Arning (Hrsg.), Die neue Datenschutz-Grundverordnung, Kap. 2 Rn. 38 ff.) und war schon Gegenstand mehrerer Urteile höchstinstanzlicher Gerichte (siehe z.B. EuGH, Urt. v. 19.10.2016 – C-582/14 – Breyer – MMR 2016, 842 und BGH, Urt. v. 16.5.2017 – VI ZR 135/13, NJW 2017, 2416).

außerhalb (sog. „Niederlassungsprinzip“).[16] Verarbeiten also EU-Niederlassungen von türkischen Unternehmen personenbezogene Daten, müssen sie hierbei grundsätzlich die DSGVO beachten.

Eine wesentliche Neuerung der DSGVO besteht nun darin, dass Art. 3 Abs. 2 DSGVO den räumlichen Anwendungsbereich der DSGVO um das sogenannte „Marktortprinzip“ erweitert. Demnach sind die Vorgaben der DSGVO auch dann zu beachten, wenn sich eine datenverarbeitende Stelle nicht in der EU befindet, sie aber personenbezogene Daten von Personen verarbeitet, die sich in der EU befinden. Dies gilt aber nicht in jedem Fall, sondern nur dann, wenn die Datenverarbeitung im Zusammenhang damit steht

a) betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist; oder

b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der EU erfolgt.

Hieraus folgt, dass z.B. auch Unternehmen mit Sitz in der Türkei die DSGVO beachten müssen, wenn sie offensichtlich beabsichtigen, betroffenen Personen in einem oder mehreren Mitgliedstaaten der EU Waren oder Dienstleistungen anzubieten.[17] Dies kann z.B. im Rahmen eines Web-Shops erfolgen, der sich gerade an Kunden in Deutschland richtet. Auch der Einsatz von Technologien zur Beobachtung des Verhaltens von Personen in der EU, wie z.B. von Cookies und anderen Tracking-Technologien, führt grundsätzlich zur Anwendbarkeit der DSGVO.

- **Ausweitung der Betroffenenrechte**. Personen, deren Daten verarbeitet werden, haben gegenüber den hierfür Verantwortlichen bestimmte Rechte, die sogenannten „Betroffenenrechte“. Hierzu zählen u.a. das Recht der betroffenen Person auf Information über die Verarbeitung ihrer

[16] Siehe zu den Einzelheiten, insbesondere zu der Frage, wann Daten im Rahmen der Tätigkeiten einer Niederlassung verarbeitet werden, z.B. *Piltz,* in: Gola (Hrsg.), DS-GVO, 2. Aufl., Art. 3 Rn. 7 ff.; *Meyerdierks*, in: Moos/Schefzig/Arning (Hrsg.), Die neue Datenschutz-Grundverordnung, Kap. 3 Rn. 31 ff.; siehe hierzu auch EuGH, Urt. v. 1.10.2015 – C-230/14 – Weltimmo - Rn 24 ff. und EuGH, Urt. v. 13.5.2014 – C-131/12 – Google Spain - Rn 52 ff.

[17] Erwägungsgrund 23 S. 2 DSGVO; siehe zu den Einzelheiten z.B. auch *Piltz,* in: Gola (Hrsg.), DS-GVO, 2. Aufl., Art. 3 Rn. 24 ff.; *Meyerdierks*, in: Moos/Schefzig/Arning (Hrsg.), Die neue Datenschutz-Grundverordnung, Kap. 3 Rn. 44 ff.

Daten (Art. 13 und 14 DSGVO), das Recht auf Auskunft über die bei einem Verantwortlichen gespeicherten Daten (Art. 15 DSGVO), das Recht auf Berichtigung von Daten (Art. 16 DSGVO), das Recht auf Löschung (Art. 17 DSGVO) und das Recht auf Datenportabilität (Art. 20 DSGVO).

Diese Rechte wurden durch die DSGVO teilweise erheblich ausgeweitet (so z.B. das Recht auf Auskunft gem. Art. 15 DSGVO). Außerdem wurden im Rahmen der DSGVO zwei neue Betroffenenrechte eingeführt: (i) das Recht auf Datenportabilität (Art. 20 DSGVO), welches – vereinfacht ausgedrückt – insbesondere Nutzern von Sozialen Netzwerken das Recht gibt, die von ihnen bereitgestellten Daten von dem Netzwerkbetreiber zu erhalten, um sie bei einem „Umzug" in ein anderes Netzwerk „mitnehmen" zu können, und (ii) das Recht auf Vergessenwerden (Art. 17 Abs. 2 DSGVO), nach dem ein Verantwortlicher unter Umständen verpflichtet ist, andere Verantwortliche über die Löschung von Daten zu informieren, vorausgesetzt, dass er diese zuvor, z.B. über eine Website, öffentlich gemacht hat. In diesem Fall können die anderen Verantwortlichen dann prüfen, ob auch sie die Daten löschen müssen. Nach dem Erwägungsgrund 66 DSGVO soll hierdurch dem Recht auf Vergessenwerden im Netz mehr Geltung verschafft werden.

- **Ausweitung der Anforderungen an den organisatorischen Datenschutz**. Außerdem hat die DSGVO die Anforderungen an den organisatorischen Datenschutz erheblich ausgeweitet. Dies zeigt sich an vielen Stellen der DSGVO. Die wohl wichtigste Neuerung in diesem Zusammenhang ist die Einführung des „Accountability"-Prinzips in Art. 5 Abs. 2 und Art. 24 DSGVO. Hierbei handelt es sich – vereinfacht ausgedrückt – vor allem um Rechenschaftspflichten, die den für die Datenverarbeitung Verantwortlichen auferlegt werden. So müssen diese nunmehr nachweisen, dass sie die DSGVO einhalten. Dies führt zu einer Art Beweislastumkehr.[18] So mussten vorher insbesondere die Datenschutzaufsichtsbehörden prüfen, ob eine datenverarbeitende Stelle eventuell gegen das Datenschutzrecht verstößt und dies ggf. auch nachweisen.

Ausdruck dieser neuen organisatorischen Anforderungen ist zudem die Pflicht gem. Art. 35 DSGVO, unter bestimmten Voraussetzungen Datenschutz-Folgeabschätzungen durchführen zu müssen, bei denen die Folgen einer Datenverarbeitung für den Schutz personenbezogener Daten

[18] Siehe z.B. *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, Teil 2 Rn. 18.

zu ermitteln sind. Weitere Beispiele sind die Pflicht zur Dokumentation von Datenverarbeitungen gem. Art. 30 DSGVO, die Pflicht zur Ergreifung interner Strategien zur Einhaltung der DSGVO gem. Erwägungsgrund 78 S. 2 DSGVO sowie die Pflicht nach Art. 25 DSGVO, Datenverarbeitungen möglichst datenschutzfreundlich auszugestalten.

- **Ausweitung des Bußgeldrahmens**. Während Verstöße gegen das BDSG gem. § 43 Abs. 3 BDSG grundsätzlich „nur" mit einer Höchststrafe von 300.000 EUR geahndet werden konnten, hat die DSGVO diesen Bußgeldrahmen signifikant erhöht, um Datenverarbeiter wirksamer von Verstößen gegen die DSGVO abzuhalten. So können diese gem. Art. 83 Abs. 5 DSGVO mit einer Geldbuße in Höhe von 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden, je nachdem, welcher der Beträge höher ist.

1.4. Inhalte der Diskussion auf der DSRI Herbstakademie

Vor diesem Hintergrund wurden im Rahmen der Herbstakademie verschiedene Problembereiche im Zusammenhang mit der DSGVO diskutiert. Es zeigte sich insbesondere, dass sich noch erhebliche Fragen stellen, wie die neuen Anforderungen der DSGVO in der Praxis umzusetzen sind.

So sind die Regelungen in der DSGVO häufig sehr abstrakt formuliert. Dies ist oftmals auch notwendig, da der rasante technologische Fortschritt immer neue (bei Verabschiedung der DSGVO unbekannte) Arten der Datenverarbeitung ermöglicht, die auch von DSGVO geregelt werden müssen und bei denen die DSGVO das (berechtigte) Interesse der Wirtschaft bzw. der Behörden an der Datenverarbeitung und das schutzwürdige Interesse der von der Datenverarbeitung betroffenen Personen am Schutz ihrer Daten und ihrer Privatsphäre zu einem gerechten und angemessenen Ausgleich bringen muss. Möchte man die DSGVO nicht ständig (im Nachhinein) an die technologische Entwicklung anpassen, verbleibt i.d.R. nur die Möglichkeit, die Verarbeitung personenbezogener Daten durch abstrakte und damit auslegungsbedürftige Vorschriften zu regeln. An anderen Stellen sind die abstrakten Regelungen aber auch einfach der Tatsache geschuldet, dass sich das Europäische Parlament, der Rat der EU und die EU-Kommission im Rahmen der Trilog-Verhandlungen auf keine konkretere Regelung einigen konnten.

So wurde im Rahmen der Herbstakademie z.B. über die folgenden (Auslegungs-)Probleme diskutiert:

- *Dr. Sebastian Brüggemann, M.A.*[19] stellte das neue Recht der betroffenen Personen auf Datenportabilität gem. Art. 20 DSGVO dar. Demnach dürfen betroffene Personen unter gewissen Voraussetzungen vom für die Datenverarbeitung Verantwortlichen verlangen, dass dieser ihnen die sie betreffenden Daten zur Verfügung stellt, die sie ihm zuvor bereitgestellt haben. Dadurch soll insbesondere der „Umzug" in ein anderes Soziales Netzwerk erleichtert werden. *Brüggemann* beschrieb in diesem Zusammenhang insbesondere zwei Problemkreise, die sich in der Praxis stellen. So sei unklar, ob ein Soziales Netzwerk bzw. ein anderer Anbieter verpflichtet sei, Daten von einer betroffenen Person entgegenzunehmen und in seinen Dienst einzufügen, die die betroffene Person zuvor auf Grundlage von Art. 20 DSGVO von einem anderen Anbieter/Sozialen Netzwerk erhalten hat. *Brüggemann* verneinte zu Recht eine solche Verpflichtung.

Außerdem führte *Brüggemann* aus, dass unklar sei, wer prüfen müsse, ob durch die Herausgabe der Daten Rechte und Freiheiten anderer Personen beeinträchtigt würden und das Recht auf Datenportabilität daher nach Art. 20 Abs. 4 DSGVO ausnahmsweise ausgeschlossen sei. *Brüggemann* vertrat insoweit die Ansicht, dass der Anbieter, der die Daten herausgibt, die Prüfung durchzuführen habe.[20]

- *Raphael Born, LL.M.*[21] beschäftigte sich mit der Verarbeitung von allgemein zugänglichen Daten auf Grundlage der DSGVO, also von personenbezogenen Daten, die z.B. auf einer Webseite stehen, die von jedermann aufgerufen werden kann. Solche Daten könnten insbesondere auch zur Beurteilung der Kreditwürdigkeit einer Person verwendet werden. *Born* stellte dar, dass die DSGVO anders als das BDSG a. F. in Deutschland keine Privilegierung für die Verarbeitung derartiger Daten enthalte. Allerdings sei ihre Verarbeitung auch ohne eine solche Privilegierung nach der DSGVO i.d.R. zulässig, da diese Daten nicht sehr schutzwürdig seien und in diesem Fall die Interessen des Verantwortlichen an der Datenverarbeitung i.d.R. die schutzwürdigen Interessen der betroffenen Personen am Ausschluss der Datenverarbeitung überwiegen würden. In diesem Fall erlaube Art. 6 Abs. 1 lit. f DSGVO die Verarbeitung.[22]

---

[19] Lehrbeauftragter an der Universität Tübingen.

[20] Siehe ausführlich: *Brüggemann*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 1 ff.

[21] Referent Recht bei der SCHUFA Holding AG.

[22] Siehe ausführlich: *Born*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 13 ff.

- *Dr. Jens Schefzig*[23] erläuterte, dass für die Datenverarbeitung Verantwortliche nach Art. 24 DSGVO verpflichtet seien, geeignete technische und organisatorische Maßnahmen zu treffen, um die Einhaltung der DSGVO sicherzustellen. *Schefzig* stellte sodann einen Vorschlag vor, welche organisatorischen Maßnahmen die Geschäftsleitung eines Unternehmens zu diesem Zweck treffen sollte. Gerade bei größeren Unternehmen würde es häufig nicht ausreichen, einen Datenschutzbeauftragten zu bestellen. Vielmehr müssten innerhalb der (operativen) Abteilungen des Unternehmens Mitarbeiter benannt werden, die als „Risk Owner" die datenschutzrechtlich relevanten Prozesse in ihrem Bereich erkennen und für die Einhaltung des Datenschutzrechts sorgen sollen. Dabei sollte ihnen die Rechtsabteilung des Unternehmens beratend zur Seite stehen. Der Datenschutzbeauftragte solle sich hingegen vorwiegend auf seine Kernaufgaben konzentrieren, die in der Überwachung/Auditierung von Datenverarbeitungen und der Schulung von Mitarbeitern im Datenschutzrecht bestünden.[24]

- *Dr. Johannes Baumann*[25] beschäftigte sich in seinem Vortrag mit sogenannten „Binding Corporate Rules", bei denen es sich – vereinfacht ausgedrückt – um verbindliche interne Datenschutzvorschriften innerhalb eines Konzerns handelt. Erfüllen diese bestimmte, in Art. 47 DSGVO normierte Voraussetzungen, dürfen teilnehmende Unternehmen aus dem Europäischen Wirtschaftsraum (EWR) personenbezogene Daten dann auch an andere teilnehmende Unternehmen übermitteln, die ihren Sitz in einem Land außerhalb des EWR haben, in dem kein Datenschutzniveau existiert, welches von der EU-Kommission als angemessen anerkannt wurde. Dies ist nach Art. 44 DSGVO grundsätzlich unzulässig. Allerdings existieren von diesem Verbot Ausnahmen, wie z.B. im Fall der Vereinbarung von Binding Corporate Rules.

Diese Möglichkeit zur internationalen Datenübermittlung werde laut *Baumann* für Unternehmen mit der DSGVO noch interessanter. So habe es diese Möglichkeit zwar schon nach dem „alten" Datenschutzrecht gegeben. Allerdings hätten einige nationale Datenschutzgesetze vorgesehen, dass die zuständige Datenschutzaufsichtsbehörde trotz des Abschlusses von Binding Corporate Rules den Export von Daten in ein

[23] Rechtsanwalt bei Osborne Clarke, Hamburg.
[24] Siehe ausführlich: *Schefzig*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 43 ff.
[25] Rechtsanwalt bei Bird&Bird, München.

Land außerhalb des EWR noch genehmigen musste. Eine solche Genehmigungspflicht bestehe unter der DSGVO nicht mehr, weshalb der Datenexport auf Grundlage von Binding Corporate Rules vereinfacht werde.[26]

- *Jan Spittka*[27] stellte praktische Probleme bei der Auftragsverarbeitung in Multi-Tier-Processing-Systemen dar. Verarbeitet eine Stelle personenbezogene Daten, ist sie datenschutzrechtlich gesehen i.d.R. entweder ein Verantwortlicher oder ein Auftragsverarbeiter. Der Unterschied zwischen diesen beiden Rollen besteht darin, dass der Verantwortliche gem. Art. 4 Nr. 7 DSGVO über die Mittel, mit denen die Daten verarbeitet werden sowie über die Zwecke entscheidet, für die die Daten verarbeitet werden. Auftragsverarbeiter sind hingegen weisungsgebundene Dienstleister, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeiten (Art. 4 Nr. 8 DSGVO). Möchte ein Verantwortlicher Daten von einem solchen Auftragsverarbeiter/Dienstleister verarbeiten lassen, muss er mit diesem einen Auftragsverarbeitungsvertrag schließen, dessen Inhalt in Art. 28 DSGVO näher vorgegeben wird. Bedient sich der Auftragsverarbeiter bei der Datenverarbeitung für den Verantwortlichen seinerseits eines (Unter-)Auftragsverarbeiters, sieht Art. 28 Abs. 4 S. 1 DSGVO u.a. vor, dass diesem (Unter) Auftragsverarbeiter dieselben vertraglichen Pflichten auferlegt werden müssen, wie dem Auftragsverarbeiter selbst. Mithin müssen die Pflichten des Auftragsverarbeiters aus seinem Auftragsverarbeitungsvertrag mit dem Verantwortlichen grundsätzlich an den (Unter-)Auftragsverarbeiter „weitergereicht“ werden.

Hierzu sei es laut *Spittka* aber nicht erforderlich, dass der Verantwortliche ein direktes Weisungsrecht gegenüber dem (Unter) Auftragsverarbeiter eingeräumt bekomme. Vielmehr sei es ausreichend, wenn der Verantwortliche gegenüber dem Auftragsverarbeiter weisungsbefugt und dieser verpflichtet und berechtigt sei, seinerseits den (Unter) Auftragsverarbeiter entsprechend anzuweisen.

Außerdem sollten der Verantwortliche bzw. der Auftragsverarbeiter zumindest als ultima ratio auch ein Recht zur Vor-Ort-Kontrolle der Datenverarbeitung beim (Unter-)Auftragsverarbeiter besitzen. Im Regelfall sei aber eine entsprechende Auditierung durch Dritte ausreichend. In der Praxis stelle sich dabei allerdings oftmals das Problem,

---

[26] Siehe ausführlich: *Baumann*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 59 ff.

[27] Rechtsanwalt bei DLA Piper, Köln.

dass eine solche Konstellation häufig bei IT-Projekten auftrete, bei denen sich ein Dienstleister weiterer Dienstleister bediene, die über eine erhebliche Marktmacht verfügen, so z.B. Cloud-Dienste-Anbieter, die zudem in vielen Fällen in den USA sitzen würden. Diese wären häufig nur bereit, ihre eigenen (Muster-)Auftragsverarbeitungsverträge zu verwenden. Deshalb sei bereits bei Beginn eines solchen IT-Projekts zu prüfen, inwieweit dieser (Muster-)Auftragsverarbeitungsvertrag den Vorgaben der DSGVO entspreche.[28]

- *Thomas Kahl*[29] erläuterte sodann die Haftung von Auftragsverarbeitern. Nach „alter" Rechtslage sei eine Haftung des Auftragsverarbeiters – solange er sich an die Weisungen des Verantwortlichen gehalten habe – in der Praxis faktisch ausgeschlossen gewesen. Dies ändere sich jedoch durch die DSGVO. So habe nach Art. 82 Abs. 1 DSGVO jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden sei, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Dieser Grundsatz werde aber durch Art. 82 Abs. 2 DSGVO eingeschränkt. Demnach hafte ein Auftragsverarbeiter nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen sei oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt habe. Allerdings könne sich der Auftragsverarbeiter nach Art. 82 Abs. 3 DSGVO exkulpieren, wenn er nachweise, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich sei.

Im Hinblick auf die Haftungsverteilung zwischen Verantwortlichem und Auftragsverarbeiter sehe Art. 82 Abs. 4 DSGVO eine gesamtschuldnerische Haftung vor, vorausgesetzt, dass beide Stellen nach Art. 82 Abs. 1-3 DSGVO der betroffenen Person zum Ersatz des Schadens verpflichtet seien.

In der Praxis stelle sich vor diesem Hintergrund die Frage, ob der Verantwortliche und der Auftragsverarbeiter die Haftung des Auftragsverarbeiters im Innenverhältnis beschränken können. Auch wenn der generell repressive und präventive Charakter des Art. 82 DSGVO ggf. dadurch untergraben würde, befürwortete *Kahl* diese Möglichkeit, wobei

---

[28] Siehe ausführlich: *Spittka*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 73 ff.

[29] Rechtsanwalt bei Taylor Wessing, Frankfurt.

er sich vor allem auf den Wortlaut von Art. 82 DSGVO stützte, der eine Haftungsbeschränkung des Auftragnehmers im Innenverhältnis nicht verbiete.[30]

- *Thanos Rammos, LL.M.*[31] beschäftigte sich sodann mit Einwilligungserklärungen im Rahmen der medizinischen wissenschaftlichen Forschung. Grundsätzlich schreibt die DSGVO vor, dass die Einwilligung freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich erteilt werden muss (Art. 4 Nr. 11 DSGVO). Werden besonders sensible Daten, wie z.B. Gesundheitsdaten oder genetische Daten verarbeitet, muss die Einwilligung zudem ausdrücklich erfolgen (Art. 9 Abs. 2 lit. a DSGVO). In jedem Fall ist der Verantwortliche verpflichtet, im Rahmen der Einwilligungserklärung die Zwecke anzugeben, für die er die Daten verarbeiten möchte (Erwägungsgrund 42 S. 4 DSGVO bzw. Art. 9 Abs. 2 lit. a DSGVO).

Würden die Daten zu Zwecken der medizinischen wissenschaftlichen Forschung verarbeitet, stelle dieses Erfordernis laut *Rammos* in der Praxis oftmals ein großes Problem dar. So könne zum Zeitpunkt der Einholung der Einwilligung häufig noch gar nicht genau angegeben werden könne, für welche Zwecke die Daten genau verarbeitet würden, weil sich diese während der Laufzeit eines Forschungsprojektes noch ändern könnten oder zukünftige Forschungsprojekte noch nicht absehbar seien. Lege man an die Wirksamkeit der Einwilligung die „üblichen" Anforderungen an, hätte dies zur Folge, dass betroffene Personen oftmals erneut kontaktiert und gefragt werden müssten, ob sie einer bestimmten weiteren Verarbeitung auch noch zustimmen würden, weil die ursprüngliche Einwilligung die weitergehende Datenverarbeitung nicht mit „abdecke". Da aber die DSGVO die wissenschaftliche Forschung privilegiere, befürwortete *Rammos* in diesem Bereich die Zulässigkeit des sogenannten „Broad Consent". Demnach sollen insoweit ausnahmsweise auch pauschalere Einwilligungserklärungen zulässig sein, mit denen die betroffenen Personen z.B. in die Verarbeitung ihrer Daten für ganze Bereiche der Wissenschaft zustimmen können.[32]

---

[30] Siehe ausführlich: *Kahl*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 101 ff.

[31] Rechtsanwalt bei Taylor Wessing, Berlin.

[32] Siehe ausführlich: *Rammos*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 359 ff.

• *Dr. Flemming Moos*[33] stellte in seinem „Update Datenschutz“ u.a. die Urteile des EuGH und des BGH in Sachen Breyer vor. Diese Urteile sollten endlich Klarheit im Hinblick auf eine der großen Streitfragen im Datenschutzrecht bringen: Wann liegen personenbezogene Daten vor? Wie oben bereits erläutert, ist es insoweit ausreichend, dass die betroffene Person identifizierbar/bestimmbar ist. Umstritten war allerdings, welche Mittel bei der Ermittlung, ob eine Person identifizierbar/bestimmbar ist, berücksichtigt werden müssen. Nur die Mittel (z.B. das Wissen) der datenverarbeitenden Stelle selbst oder auch die Mittel von anderen Stellen? In dem zu entscheidenden Fall konnte der verklagte Webseitenbetreiber die von ihm erhobene dynamische IP-Adresse, deren Löschung der Kläger begehrte, z.B. nicht mit eigenen Mitteln einer Person zuordnen. Der Access-Provider des Anschlussinhabers hätte dies aber ggf. gekonnt.

Moos erläuterte, dass der EuGH entschieden habe, dass ein Personenbezug für einen Webseitenbetreiber dann vorliege, wenn dieser „vernünftigerweise“ über „rechtliche Mittel“ verfüge, die es ihm erlauben würden, die betreffende Person anhand der Zusatzinformationen, über die der Access-Provider bzgl. dieser Person verfügt, bestimmen zu lassen. Der BGH habe dann auf dieser Grundlage entschieden, dass Webseitenbetreiber im Hinblick auf IP-Adressen über solche Mittel verfügen würden, da Strafverfolgungs- und Gefahrenabwehrbehörden nach § 100j Abs. 2 und 1 StPO, § 113 TKG Auskunft über die Anschlussinhaber, die eine bestimmte IP-Adresse verwenden, erhalten könnten. Dadurch könnten laut BGH „*die gewonnenen Informationen zusammengeführt und der Nutzer bestimmt werden*“.[34]

Moos kritisierte diese Entscheidungen, da die Gerichte nicht ausgeführt hätten, durch wen die Zusammenführung erfolgen können müsse, damit die IP-Adressen für den Webseitenbetreiber als personenbezogen anzusehen seien. Durch die soeben zitierte passive Formulierung könnte zumindest der BGH so verstanden werden, dass er es ausreichend finde, dass die Ermittlungsbehörde die Daten zusammenführen könne. *Moos* hielt dies dagegen nicht für ausreichend. Vielmehr müsse gerade der Webseitenbetreiber die zur Identifikation notwendigen Zusatzinformationen erhalten und die Zuordnung vornehmen können.

Zudem stellte *Moos* in diesem Zusammenhang fest, dass das Urteil des BGH insoweit auch in sich widersprüchlich sei. So lege es die oben zitierte Formulierung nahe, dass es zur Annahme des Personenbezugs dieser

[33] Rechtsanwalt bei Osborne Clarke, Hamburg.
[34] BGH, Urt. v. 16.05.2017 – VI ZR 135/13, WM 2017, 1320.

Daten für den Webseitenbetreiber ausreiche, dass dieser die Identifizierung durch die Ermittlungsbehörde veranlasse. An anderer Stelle führe der BGH (wie der EuGH) aber aus, dass die Möglichkeit der Identifizierung durch den Access-Provider dem Webseitenbetreiber nicht zuzurechnen sei. Für den Webseitenbetreiber sei es jedoch unerheblich, ob nun der Access-Provider oder die Ermittlungsbehörde die Person identifizieren könne, solange er die Zusatzinformationen nicht erhalte. Mithin mache die Unterscheidung zwischen Access-Provider und Ermittlungsbehörde durch die Gerichte nur dann Sinn, wenn es ihnen für den Personenbezug der Daten gerade auch darauf ankomme, dass der Webseitenbetreiber diese Zusatzinformationen von der Ermittlungsbehörde (z.B. im Rahmen eines Akteneinsichtsrechts) erhalten könne. Vom Access-Provider könne der Webseitenbetreiber die Daten jedenfalls nicht erhalten. Da diese Aspekte aber insbesondere im Urteil des BGH nicht erläutert worden seien, hätten die Gerichte den Personenbezug von IP-Adressen (leider) nicht vollständig geklärt.[35]

Darüber hinaus gab es eine Vielzahl sehr interessanter und praxisrelevanter Vorträge zu weiteren Aspekten der DSGVO, die hier im Einzelnen nicht dargestellt werden können, so z.B. zu „Datenschutzrechtlichen Fragen der digitalen/virtuellen Zusammenarbeit im Konzern“,[36] zu „Internationalen Datentransfers im Lichte des Brexit“,[37] „Datenschutzklauseln in Arbeitsverträgen“,[38] zum Erfordernis eines „kollektiven Datenschutzes“[39] oder auch zur „Rasterfahndung in der Bundesliga“.[40]

2. Automatisierung

Der zweite Schwerpunkt der Tagung lag auf dem Bereich der Automatisierung.

---

[35] Siehe ausführlich: *Moos*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 211 ff.

[36] *Seiler*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 115 ff.

[37] *Gräfin von Brühl/Nietsch* in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 171 ff.

[38] *Schneider*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S.185 ff.

[39] *Golla,* in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S.199 ff.

[40] *Haumann* in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 373 ff.

2.1. Automatisierung und künstliche Intelligenz

Die Automatisierung prägt nicht nur zunehmend die Wirtschaft, sondern auch das normale Alltagsleben der Menschen. Das bekannteste Beispiel hierfür ist sicherlich das selbstfahrende Auto. Wir kommunizieren mit Bots, wie z.B. Siri und Alexa, die uns unterstützen, beraten oder aber Produkte und Dienstleistungen verkaufen sollen. Auch im Bereich der Rechtsberatung schreitet die Automatisierung immer weiter voran. So sind derzeit schon Angebote auf dem Markt verfügbar, die automatisiert Verträge generieren bzw. analysieren oder Passagiere bei der Wahrnehmung und Durchsetzung ihrer Fluggastrechte unterstützen. Die Digitalisierung des Rechtsbereichs wird auch als „Legal Tech" bezeichnet.[41]

Die Automatisierung immer weiterer Lebensbereiche kann einerseits das Leben der Menschen erleichtern und verbessern, z.B. wenn sie dazu führt, dass dem Menschen schwere Tätigkeiten abgenommen werden oder sie es ermöglicht, Operationen mit einer Präzision durchzuführen, zu der ein Mensch nicht in der Lage ist. Andererseits warnen aber auch immer mehr Wissenschaftler und IT-Unternehmer vor den Gefahren einer (unkontrollierten und unregulierten) künstlichen Intelligenz, also der Automatisierung intelligenten Verhaltens.[42]

Elon Musk z.B., der Gründer von Tesla und SpaceX, sieht künstliche Intelligenz als die größte Gefahr für die Menschheit an. Laut dem britischen Physiker Stephan Hawking könnte die Entwicklung vollständiger künstlicher Intelligenz gar das Ende der Menschheit bedeuten.[43] So bes-

---

[41] Siehe hierzu z.B. *Scherer*, Automatisch Recht bekommen, in: Die Zeit, Nr. 40/2016 v. 22.09.2016, abrufbar unter: http://www.zeit.de/2016/40/legal-tech-algorithmen-juristen-ersatz, (06.11.2018); *Jung*, Recht und Code, in: FAZ, abrufbar unter: http://www.faz.net/aktuell/wirtschaft/recht-steuern/digitale-rechtsunterstuetzung-deutsche-juristen-reagieren-ablehnend-auf-legal-tech-15033852.html, (06.11.2018).

[42] „Künstliche Intelligenz" ist ein Teilgebiet der Informatik, welches sich mit der Automatisierung intelligenten Verhaltens beschäftigt, siehe z.B. *Bundesministerium für Unterricht, Kunst und Kultur (Hrsg.)*, Als die künstliche Intelligenz laufen lernte, S. 4 m.w.N., abrufbar unter: https://www.bmb.gv.at/schulen/service/mes/14048_23394.pdf?61ebt4, (07.11.2018). Siehe ausführlich zur künstlichen Intelligenz: *Pieper*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 555 ff.

[43] Siehe z.B. *Heuzeroth*, Tesla-Chef Musk warnt vor tödlichen Robotern, in: Die Welt, abrufbar unter: https://www.welt.de/wirtschaft/article166725047/Tesla-Chef-Musk-warnt-vor-toedlichen-Robotern.html, (08.11.2018).

tehe die Gefahr, dass sich die künstliche Intelligenz irgendwann selbständig mache und sie gegen die Interessen von Menschen handele.[44] Diese Gefahr könne sich insbesondere dann realisieren, wenn künstliche Intelligenz erschaffen würde, die klüger als der Mensch sei und sich auch noch ständig selbst verbessern könne.[45] Wann dieser Zeitpunkt eintritt, der auch als „Technologische Singularität" bezeichnet wird, lässt sich derzeit aber nicht seriös abschätzen.

Andere Wissenschaftler, wie z.B. der italienische Philosoph Luciano Floridi,[46] und IT-Unternehmer, wie z.B. der Gründer von Facebook, Mark Zuckerberg, sehen die Entwicklung von künstlicher Intelligenz hingegen optimistisch und lehnen die u.a. von Musk und Hawking beschworenen Gefahren ab.[47] So könnten Maschinen zwar einzelne Arbeitsschritte (besser als der Mensch) verrichten, allerdings nur solche, für die es keiner eigenen Intelligenz bedürfe, da eine Maschine keine Intelligenz an sich entwickeln könne. Vielmehr stelle sich die Frage nach der Verantwortung für diese Maschinen, z.B. bei einem selbstfahrenden Auto.[48]

2.2. Inhalte der Diskussion auf der DSRI Herbstakademie

Auch wenn die künstliche Intelligenz derzeit noch „in den Kinderschuhen steckt", wurde im Rahmen der Herbstakademie über rechtliche Herausforderungen und Lösungen für die Automatisierung diskutiert, so z.B. über die folgenden:

---

[44] *Heuzeroth*, Tesla-Chef Musk warnt vor tödlichen Robotern, in: Die Welt, abrufbar unter: https://www.welt.de/wirtschaft/article166725047/Tesla-Chef-Musk-warnt-vor-toedlichen-Robotern.html, (09.11.2018).

[45] Siehe z.B. *Stöcker*, Wir sind zu dumm für künstliche Intelligenz, in: Spiegel Online, abrufbar unter: http://www.spiegel.de/wissenschaft/mensch/mark-zuckerberg-und-elon-musk-zukunft-der-kuenstlichen-intelligenz-a-1160095.html, (10.11.2018).

[46] So z.B. im Interview in *Crocoll*, Elon Musks Warnung vor künstlicher Intelligenz ist unmoralisch, in: Die Welt, abrufbar unter: https://www.welt.de/wirtschaft/bilanz/article167943544/Elon-Musks-Warnung-vor-kuenstlicher-Intelligenz-ist-unmoralisch.html, (11.11.2018).

[47] Siehe z.B. *Stöcker*, Wir sind zu dumm für künstliche Intelligenz, in: Spiegel Online, abrufbar unter: http://www.spiegel.de/wissenschaft/mensch/mark-zuckerberg-und-elon-musk-zukunft-der-kuenstlichen-intelligenz-a-1160095.html, (12.11.2018).

[48] So z.B. Floridi im Interview in *Crocoll*, Elon Musks Warnung vor künstlicher Intelligenz ist unmoralisch, in: Die Welt, abrufbar unter: https://www.welt.de/wirtschaft/bilanz/article167943544/Elon-Musks-Warnung-vor-kuenstlicher-Intelligenz-ist-unmoralisch.html, (13.11.2018).

• *Tim Juelicher*[49] gab in seinem Vortrag einen Überblick über die rechtlichen Implikationen von Bots, also von Computerprogrammen, die eine oder mehrere festgelegte Aufgaben (teil-) autonom ausführen. Dabei ging er insbesondere auf sogenannte Social Bots ein, die zur Steuerung kommunikativer Prozesse verwendet werden.[50] Diese könnten z.B. Kundenbewertungen erstellen, Produkte „liken" oder Kunden in automatisierte Verkaufsdialoge verwickeln. In diesem Zusammenhang seien insbesondere die lauterbarkeitsrechtlichen Regelungen im UWG zu beachten. So könne der Einsatz derartiger Bots z.B. nach § 3 Abs. 3 UWG i.V.m. Nr. 23 unzulässig sein, wenn eine Kundenbewertung veröffentlicht und hierbei vorgetäuscht werde, dass ein Verbraucher diese abgegeben habe. Auch könne insoweit eine unzulässige Identitätsverschleierung bei Werbung mit Nachrichten i.S.d. § 7 Abs. 2 Nr. 4 lit. a UWG in Betracht kommen. Getarnte Werbung verstoße im Übrigen gegen § 5a Abs. 6 UWG. Würden Mitwettbewerber durch Bots verunglimpft, sei dies i.d.R. nach § 4 Nr. 1 UWG unlauter. Außerdem würden viele Plattformen und Netzwerke den Einsatz von Bots auch bereits im Rahmen ihrer Nutzungsbedingungen ausschließen, wie z.B. Twitter.[51]

• *Dr. Johannes Franck* und *Philipp Müller-Peltzer*[52] gingen u.a. der Frage nach, ob Kunden darüber informiert werden müssen, dass ein Bot mit ihnen kommuniziert. Hierbei kamen die Vortragenden zunächst zu dem Zwischenergebnis, dass sich eine solche Pflicht nicht aus den allgemeinen verbraucherschutzrechtlichen Vorschriften (§ 312d Abs. 1 BGB und Art. 246 Abs. 1 Nr. 2 EGBGB) ergebe. So würden diese nur eine Information über den Vertragspartner des Kunden erfordern. Dies sei aber i.d.R. das „dahinterstehende" Unternehmen und eben nicht der Bot selbst. Allerdings ergebe sich die Pflicht, den Kunden entsprechend zu unterrichten, aus den datenschutzrechtlichen Informationspflichten (Art. 13 DSGVO). So erfordere eine transparente Information über die Zwecke der Verarbeitung auch eine Information über den Umstand, dass der Kunde mit einem Bot und nicht mit einem Menschen kommuniziere.[53]

---

[49] Wissenschaftlicher Mitarbeiter am Institut für Informations-, Telekommunikations- und Medienrecht, Universität Münster.

[50] Siehe *Röttgen/Juelicher*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 227 (228).

[51] Siehe ausführlich auch zu Bots in Computerspielen und Cyberkriminalität: *Roettgen/Juelicher,* in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 227 ff.

[52] Rechtsanwälte bei Schürmann Wolschendorf Dreyer, Berlin.

[53] Siehe ausführlich: *Franck/Müller-Peltzer*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 241 ff.

• *Thomas Köbrich*[54] und *Dr. Oliver Froitzheim*[55] beschäftigten sich u.a. mit Willenserklärungen, die durch Chatbots abgegeben werden, also von Bots, die ein Gespräch mit einem oder mehreren Menschen simulieren.[56] Diese seien i.d.R. dem Betreiber des Chatbots zuzurechnen, da die Ergebnisse des Bots auf dem Willen des Betreibers beruhen würden. Insoweit sei die Situation vergleichbar mit der eines Warenautomaten.

Der Betreiber eines Chatbots gebe die Erklärung dabei direkt gegenüber dem Kommunikationspartner ab. So sei der Chatbot mangels Geschäftsfähigkeit kein Vertreter des Betreibers. Auch sei er kein Bote. Vielmehr handele es sich bei ihm nur um das Medium, mittels dessen die Erklärung des Betreibers abgegeben werde.

Anschließend setzten sich die Vortragenden mit der Auslegung solcher Willenserklärungen auseinander. Zwar seien sie grundsätzlich nach §§ 133, 157 BGB auszulegen, doch bestünden auch einige Besonderheiten, so z.B. im Fall von Fehlfunktionen des Chatbots. Jedenfalls wenn es dem Kommunikationspartner bewusst sei, dass er mit einem Chatbot kommuniziere und es sich ihm aufdrängen musste, dass eine Fehlfunktion vorliegt und der Betreiber die Erklärung so nicht abgeben wollte, sei die Willenserklärung nach dem offensichtlichen (und nicht nach dem durch den Chatbot „erklärten“) Betreiberwillen gem. §§ 133, 157 BGB auszulegen.

Sei ein Fehler für den Kommunikationspartner hingegen nicht erkennbar, komme ein Erklärungsirrtum des Betreibers nach § 119 Abs. 1 Alt. 2 BGB in Betracht, wenn ein Irrtum in der Erklärungshandlung des Chatbots vorliege. Erkläre der Chatbot hingegen das vom Betreiber Gewollte und liege dennoch ein Irrtum vor, könne dies einen Inhaltsirrtum gem. § 119 Abs. 1 Alt. 1 BGB darstellen. Verspreche der Chatbot aufgrund eines Datenfehlers eine unmögliche Leistung (z.B. weil der Artikel ausverkauft ist), liege ein unbeachtlicher Motivirrtum vor. Dies gelte ebenso für den Fall, dass ein Chatbot den Preis falsch berechne und sich dies dem Kommunikationspartner nicht aufdränge. So stelle das Angebot über einen Chatbot eben auch keine invitatio ad offerendum dar, sondern ein für den Betreiber bindendes Angebot.[57]

---

[54] Syndikusrechtsanwalt bei der artegic AG.

[55] Wissenschaftlicher Mitarbeiter am Institut für Bankrecht, Universität Köln.

[56] *Köbrich/Froitzheim*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 259.

[57] Siehe ausführlich: *Köbrich/Froitzheim*, in: Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 259 ff.

Auch darüber hinaus gab es eine Vielzahl an interessanten und lehrreichen Vorträgen zur Automatisierung, so z.B. zur „Rechtlichen Behandlung algorithmischer Kommunikate“[58] und zur Datenverarbeitung zu Zwecken der Unfallrekonstruktion beim hoch- und vollautomatisierten Fahren nach § 63a Abs. 1 StVG.[59] Einen weiteren Schwerpunkt bildete in diesem Zusammenhang der Bereich „Legal Tech“, in dem u.a. Vorträge zu folgenden Themen gehalten wurden: „Vertragsgestaltende Legal Techs und Rechtsdienstleistung“,[60] „Rechtsprobleme der Beratung durch Robo Advisors“,[61] „AGB 4.0: Allgemeine Geschäftsbedingungen im Rahmen autonomer Vertragsschlüsse“,[62] „Automatisierte Dokumentengeneratoren – Wer haftet?“[63] und „Smart Labor Contracts – Arbeiten für die Maschinen“.[64] Abgerundet wurde der Bereich durch Vorträge zum Thema „Ledger Tech/Blockchain“. Hierbei handelt es sich um eine Technologie, die z.B. virtuellen Währungen wie „Bitcoin“ zugrunde liegt, aber auch ganz generell Transaktionen technisch und ohne Zwischenschaltung von Intermediären, wie Banken, rechtssicher abwickeln soll.[65] Die Vorträge hierzu behandelten u.a. vertrags-, haftungs-, verbraucherschutz-, datenschutz- und immaterialgüterrechtliche Fragestellungen sowie Aspekte des IT-Sic-

[58] Siehe *Krupar*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 275 ff.

[59] Siehe *Spiegel,* in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 691 ff.

[60] Siehe *Wettlaufer*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 573 ff.

[61] Siehe *Reiter/Methner*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 587 ff.

[62] Siehe *Groß*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 611 ff.

[63] Siehe *Dulle/Galetzka/Partheymüller*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 625 ff.

[64] Siehe *von Chrzanowski*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 641 ff.

[65] Siehe zur Funktionsweise z.B. *Geiling*, Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain, abrufbar unter: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2016/fa_bj_1602_blockchain.html, (15.11.2018); siehe z.B. auch *Seitz*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 777 (778 ff.); *Willecke*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 833 (834 ff.); *Kolain/Wirth*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 845.

herheitsrechts im Hinblick auf Ledger Tech- und Blockchain-Anwendungen. [66] Zudem stellten einige Vortragende auch konkrete Anwendungsmöglichkeiten für solche Anwendungen vor, so z.B. bei der Errichtung von Registern.[67]

3. Fazit

Insgesamt bot die 18. Herbstakademie (wieder einmal) eine hervorragende Auswahl an aktuellen bzw. zukunftsweisenden und qualitativ hochwertigen Vorträgen im Bereich des Informationstechnologierechts. So ist es aufgrund der rasanten Entwicklungen selbst für auf diesen Bereich spezialisierte Juristen unmöglich, über sämtliche Aspekte des Informationstechnologierechts sowie der Informationstechnologie selbst laufend auf dem aktuellsten Stand zu sein. Vor diesem Hintergrund war die 18. Herbstakademie wieder eine sehr gute Gelegenheit, sich auch über Aspekte zu informieren, mit denen man sich in der eigenen Beratungs- bzw. Forschungspraxis eher weniger beschäftigt hat. Zudem gaben sowohl die Herbstakademie selbst als auch die Pausengespräche mit vielen der teilnehmenden Experten eine Menge neuer Denkanstöße. Es bleibt somit zu hoffen, dass die Veranstalter auch für folgenden Herbstakademien wieder ein so gutes Gespür bei der Auswahl der aktuellen Themen und exzellenten Vortragenden haben werden.

ZUSAMMENFASSUNG

Während der 18. Herbstakademie der Deutschen Stiftung für Recht und Informatik, die vom 06.-09. September 2017 an der Universität Heidelberg stattfand, wurden aktuelle Rechtsprobleme vor allem in den Bereichen des Datenschutzrechts und der Automatisierung diskutiert.

Die datenschutzrechtlichen Diskussionen konzentrierten sich dabei insbesondere auf Problembereiche im Zusammenhang mit der Datenschutz-Grundverordnung, also dem „neuen“ Datenschutzrecht in der EU, welches seit dem 25. Mai 2018 Anwendung findet. Zu den Themen, die im Rahmen von Vorträgen erläutert und sodann im Plenum diskutiert wurden, gehörten u.a. das „neue“ Betroffenenrecht auf Datenportabilität,

[66] Für die Beiträge siehe *Taeger (Hrsg.)*, Tagungsband Herbstakademie 2017 - Recht 4.0, S. 777 ff.

[67] So z.B. *Kolain/Wirth*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 845 (853 ff.) und *Gorlow/Notheisen/Simmchen*, in Taeger (Hrsg.), Tagungsband Herbstakademie 2017 - Recht 4.0, S. 859 ff.

die Verarbeitung allgemein zugänglicher Daten auf Grundlage der DSGVO, die Anforderungen an die Datenschutzorganisation innerhalb eines Unternehmens, der Abschluss von Binding Corporate Rules zur Rechtfertigung von internationalen Datentransfers in „unsichere" Drittländer, die Auftragsverarbeitung in Multi-Tier-Processing-Systemen, die Haftung von Auftragsverarbeitern, die Anforderungen an Einwilligungserklärungen im Rahmen der medizinischen wissenschaftlichen Forschung sowie der Personenbezug von Daten nach den Urteilen des EuGH und des BGH in Sachen Breyer.

Im Rahmen des zweiten Schwerpunkts der Tagung wurde über rechtliche Herausforderungen diskutiert, die durch die fortschreitende Automatisierung immer weiterer Lebensbereiche entstehen, insbesondere, wenn besondere Computerprogramme, sogenannte Bots, Aufgaben übernehmen, die bisher von Menschen erledigt wurden. So wurde in diesem Zusammenhang u.a. über die lauterbarkeitsrechtlichen Anforderungen an Social Bots, die z.B. Kundenbewertungen erstellen, Produkte „liken" oder Kunden in automatisierte Verkaufsdialoge verwickeln können, über die Frage, ob eine Pflicht zur Information von Kommunikationspartnern besteht, dass diese mit einem Bot kommunizieren und über rechtliche Probleme von Willenserklärungen, die durch einen Chatbot abgegeben werden, referiert und anschließend diskutiert.

Zusammenfassend ist festzustellen, dass sowohl im Zusammenhang mit der DSGVO als auch der Automatisierung immer weiterer Lebensbereiche erhebliche rechtliche Herausforderungen bestehen, die auch zukünftig einer tiefgehenden Auseinandersetzung bedürfen – und zwar sowohl aus rechtswissenschaftlicher als auch aus ethischer, technischer und praktischer Sicht. Hierfür bot auch die 18. Herbstakademie der Deutschen Stiftung für Recht und Informatik wieder ein hervorragendes Forum.

ÖZET

06-09 Eylül 2017'de, Heidelberg Üniversitesi'nde gerçekleştirilen Alman Hukuk ve Bilişim Vakfı'nın 18. Güz Akademisinde öncelikle veri koruma hukuku ve otomasyon alanlarında olmak üzere, güncel hukuki meseleler tartışılmıştır.

Veri koruma hukuku tartışmaları, özellikle AB'de 25 Mayıs 2018 tarihi itibariyle uygulama alanı bulan yeni veri koruma hukukuna ilişkin AB Genel Veri Koruma Tüzüğü

kapsamındaki problemlere odaklanmıştır. Sunumlar çerçevesinde, "yeni" veri taşınabilirliği, AB Genel Veri Koruma Tüzüğü çerçevesinde kamuya açık bilgilerin işlenmesi, bir şirkette veri koruma organizasyonunun gerekliliği, "güvenli olmayan" üçüncü ülkelere uluslararası veri transferini meşru kılma amacıyla Bağlayıcı Kurumsal Esaslar'ın akdedilmesi, çok katmanlı veri işleme sistemlerinde verilerin iş kotarımı, veri işleyenlerin sorumluluğu, tıbbi bilimsel araştırmalar kapsamında rıza beyanının gerekliliği, Avrupa Adalet Divanı kararları ve Alman Federal Yargıtayı'nın "Breyer" ihtilafında verdiği karar bağlamında verinin kişiyle olan bağı gibi konular izah edilmiş ve tartışılmıştır.

Toplantının ikinci gündemi kapsamında, her geçen gün daha da ilerleyen otomasyon sonucunda yaşam alanlarında daha geniş bir şekilde ortaya çıkan, özellikle de botlar olarak adlandırılan özel bilgisayar programlarının, daha önce insanlar tarafından gerçekleştirilen görevleri üstlenmesi halinde ortaya çıkan hukuki zorluklar tartışılmıştır. Müşteri değerlendirmeleri hazırlayan, ürünleri beğenen ("like") veya müşterileri otomatik satış diyaloglarının içine çeken sosyal botlar ile ilgili olarak haksız rekabet hukukuna ilişkin gereklilikler ile bir robotla iletişim kurulması halinde iletişim kurulan kişiye ilişkin bilgi hususunda bir yükümlülük bulunup bulunmadığı sorunu ve bir sohbet ("chat") botu tarafından verilen irade beyanına ilişkin hukuki problemler üzerine bilgi verilip, sonrasında değerlendirmelere geçilmiştir.

Özetle, hem AB Genel Veri Koruma Tüzüğü ile hem de daha fazla yaşam alanının otomasyonuyla bağlantılı olarak, gelecekte etik, teknik ve pratik bakış açısından derinlemesine bir tartışma gerektirecek hukuki meseleler vardır. Alman Hukuk ve Bilişim Vakfı'nın 18. Güz Akademisi, bu önemli hususlar için mükemmel bir tartışma ortamı sağlamıştır.