7. DialogCamp 2018: „Meet in the LawCloud“

Mit einem neuen Besucherrekord fand am 23. Februar 2018 bereits zum 7. Mal das DialogCamp der Zeitschriften MMR und ZD in der FOM Hochschule für Oekonomie und Management in München statt. Interessiertes Fachpublikum aus Wissenschaft und Wirtschaft diskutierte lebhaft mit herausragenden Vortragenden über aktuelle Themen aus dem Bereich Datenschutz und IT-Recht.

„Wenn Algorithmen entscheiden – Chancen und Risiken im Lichte der DSGVO“ lautete der Titel der ersten Session, die *Peter Schaar* moderierte und die sich in zwei Keynotes aufteilte. *Dr. iur. habil. Martin Ebers* eröffnete mit einer ganzen Reihe an Beispielen für die bereits heute gängige Entscheidungsfindung auf Grundlage von Algorithmen – werbliches Targeting, Algo-Trading, Bonitätsermittlung (Scoring), Risikoanalyse von Versicherungen und Predictive Policing. Vorteile lägen in der gesteigerten Effizienz und Qualität der Entscheidungen aufgrund breiterer Tatsachenbasis sowie größerer Neutralität durch unvoreingenommene Algorithmen. Als problematisch erweise sich allerdings eine gesteigerte Intransparenz, da die Entscheidungsfindung durch Algorithmen auf neuronalem Lernen basiere, anstatt auf nachvollziehbaren Wenn-Dann-Fragen. Zudem führen mangelhafte Datenbestände zu fehlerhaften Ergebnissen und es drohe Diskriminierung. *Ebers* stellte folgende drei Hauptproblemfelder der Regulierung algorithmischer Entscheidungsfindung durch die DSGVO heraus: Erstens seien viele Regelungen darauf beschränkt, dass eine Entscheidung *ausschließlich* auf automatischer Entscheidungsfindung basiert – damit seien vielerlei Sachverhalte ausgeschlossen; zweitens könne die betroffene Person zwar *ex ante* die zugrundeliegende Logik erfahren, habe hingegen kein Recht auf Erläuterung ihres tatsächlich ermittelten Scorewertes; und drittens sei auch in diesem Bereich die Rechtsdurchsetzung problematisch.

Im zweiten Teil der Eröffnungssession referierte *RA Dr. Benjamin Werthmann* zum Thema Künstliche Intelligenz (KI) und Legal Tech. Er appellierte zunächst ganz allgemein daran, dass Juristen sich vor der Regulierung einer bestimmten Technologie im Klaren über deren angestrebte Verwendung werden sollten. Ausgerechnet bei der DSGVO sei dies jedoch missglückt. Der Vortrag umfasste verschiedene Schnittmengen von KI und Recht, beispielsweise die Robotik und die vieldiskutierte Frage der Haftung. Ein großes Gefahrenpotential sah *Werthmann* bei Drohnen, da hinter deren Steuerung eben keine künstliche, sondern menschliche Intelligenz stecke. Einen klaren Vorteil von KI sah er im Enforcement, da Richter fehlbar seien und ihre Performance – im Unterschied zur KI – von der jeweiligen Tagesform abhinge. Urteile unterlägen zudem dem Grundsatz größtmöglicher Publizität. Digitalisiere der Staat nicht selbst, seien Urteile letzten Endes nur über große Anbieter zugänglich, denen entsprechende Ressourcen zur Verfügung stehen. Auch die DSGVO sei – so schloss *Werthmann* – für Konzerne geschrieben, deren Rechtsabteilungen ihre Implementierung – im Unterschied zu kleinen Unternehmen – nicht überfordert.

Dipl.-Ing. (FH), M.A., M.Sc. Sven Müller (VDE e.V) präsentierte unter dem vielversprechenden Titel „Neues vom Stand der Technik“ in einer der beiden zweiten Sessions ein Potpourri an technischen Normen und Standards. Vertieft ging er auf die

ISO 2700X-Reihe, BSI-Grundschutz und -Standards ein. Er empfahl deren Begriffsbestimmungen um beispielsweise näher zu bestimmen, was „Personalsicherheit“ tatsächlich bedeute. Zudem stellte *Müller* unterschiedliche Leidfäden und Organisationen vor, die Tools zur Verfügung stellten, die es Unternehmen ermöglichten, den Stand der Technik zu bestimmen. Ganz zum Schluss bot er einen interessanten aber leider bloß flüchtigen Einblick in ein interdisziplinäres Forschungsprojekt, das bestehende Standards mit gesetzlichen Vorgaben abgeglichen und damit versucht hat den sogenannten *semantic gap* – die Übersetzungslücke – zwischen Recht und Technik zu verringern.

Prof. Dr. Thomas Städter sprach in der dritten Session über *Entpersonalisierung*. Nach definitorischen Abgrenzungen – Daten mit und ohne Personenbezug – betonte er den dringend benötigten Informationsgewinn von Big Data als Fusion zwischen verschiedenen Datenquellen. Am Beispiel eines Fitness-Trackers erläuterte er, dass damit nicht mehr ganz intuitive Analysen möglich seien, wie etwa ob jemand rauche, schwanger sei, Alkohol konsumiere und in welcher Hierarchie er sich sozial befinde (ob er etwa Sympathie empfinde). Vertieft ging *Städter* auf die Abgrenzung zwischen IT-Sicherheit und Datenschutz ein – Schutzzwecke, Funktionen, Maßnahmen – und betonte, dass man nur mit einer *stabilen Anonymisierung* dem Anwendungsbereich der DSGVO entkäme. Er ging auf das sog. Standard Datenschutzmodell und dessen Schutzziele ein, stellte *Nichtverkettbarkeit Nichtverfolgbarkeit* gegenüber und betonte, dass *Intervenierbarkeit* die Schaffung von Datenfeldern (z.B. öffentlich/vertraulich) erfordere. Abschließend stellte er die *privacy by design* Strategien der ENISA vor, namentlich den Vorschlag der Anonymisierung durch Tokenyzation, Obfuscation und stabile Anonymisierung, die er in einer Kombination zwischen Hashing und Verschlüsselung durch eine trusted third party sah. Mit „Boxcrypto“ stellte er eine Möglichkeit vor, wie man Cloud Computing-Dienste seiner Meinung nach datenschutzkonform nutzen könne.

Dr. Stefan Schleipfer fragte sich in der vierten Session, ob der Gesetzgeber in der ePrivacy-Verordnung (im Entwurf des Parlaments) gezeigt habe, aus den Fehlern der Cookie-Richtlinie gelernt zu haben. Besonders betonte er, dass Cookies für sich genommen keine Tracking-Technologien darstellten, sondern lediglich für Tracking verwendet würden. Er stellte fünf Designfehler der CookieRL heraus und zeigt jeweils auf, ob diese durch die ePriacyVO behoben seien: (1) Kein Koppelungsverbot in der CookieRL – diesen Kritikpunkt habe das Parlament in Art. 8 Abs. 1 a ePrivVO behoben; (2) Keine Beschränkung auf personenbezogene Daten: Die ePrivacyVO verweise für die Definition der Einwilligung allerdings auf die DSGVO, die wiederum die Einwilligung auf personenbezogene Daten beschränke. Darin liege ein Systemfehler, weil man offensichtlich nicht in die Verarbeitung nichtpersonenbezogener Daten einwilligen könne, die aber von der ePrivacyVO umfasst seien. (3) Beschränkung auf das Endgerät: Die Datenverarbeitung im Rahmen des Tracking erfolge nicht im Endgerät des Betroffenen – dort würde nur ein Cookie platziert, der später ausgelesen und wiedererkannt werde. Die CookieRL verlange dazu eine Einwilligung. Großer Regelungsbedarf bestehe aber hinsichtlich der Verarbeitung *danach*. Letzten Endes regle die ePrivacyVO das Wichtigste nicht – die Erstellung von Nutzungsprofilen. (4) Schlechte Integration in die DSGVO: Z.B. sei eine Einwilligung in das Setzen eines

Cookies erforderlich, wobei dann die DSGVO einen Widerspruch gegen Tracking vorsehe. (5) Zu viele Einwilligungen seien erforderlich. Problematisch sei zudem künftig, dass in dem Moment, in dem der Nutzer in ein Nutzerkonto eingeloggt sei, nur noch ein sog. Session-Coockie gesetzt werden müsse (das für die Erbringung des Dienstes erforderlich und deshalb einwilligungsfrei möglich ist). Also sei die Lösung, dass man Dienste nur noch mit Nutzerkonten erbringe. Im Ergebnis drohe folgendes Szenario: Pseudonymes (Thirdparty-) Tracking ohne Nutzerkonto steht dem personenbezogenen Tracking für einen bezahlten Dienst gegenüber. Der Nutzer zahlt also für etwas, das datenschutzfeindlicher ist.

In der fünften Session sprach *RA Dr. Tim Wybitul* über Betriebsvereinbarungen nach der DSGVO. Er appellierte daran, für eine klare Verteidigungsstrategie im Ernstfall frühzeitig klare Ziele festzusetzen. In der Praxis seien Ressourcen für Betriebsvereinbarungen ebenso knapp wie das Verständnis in der Vorstandsebene für dieses Thema. *Wybitul* zeigte Schwierigkeiten und Unklarheiten des Art. 88 DSGVO auf, der – in Deutschland systemwidrig – Mitgliedsstaaten den Abschluss von Betriebsvereinbarungen zuschriebe. Aus Wirtschaftlichkeitsgründen empfehle sich eine Rahmenvereinbarung für diverse bestehende Betriebsvereinbarungen, deren Vorrangstellung aber eindeutiger Klärung bedürfe. Unklarheit herrsche über die nach der DSGVO erforderlichen Granularität der Beschreibung der Verarbeitungszwecke. *Wybitul* plädierte für einem relativen Maßstab, der je nach Risiko der Verarbeitung variiere. Eine Prognose wagte er hinsichtlich künftiger Klageverfahren. Namentlich erwarte er, dass insbesondere der immaterielle Schadensersatzanspruch aus der DSGVO im Rahmen arbeitsgerichtlicher Streitigkeiten die Arbeitgeberseite belasten dürfte, weil diese aufgrund der Beweislastumkehr des Art. 24 DSGVO künftig für die Datenschutzkonformität der Erlangung ihrer Beweise beweisbelastet sei. Es sei geboten, so schloss er, Schadensersatzansprüche zu vermeiden oder zumindest durch eine ausreichende Dokumentation die Umsetzung der DSGVO nachweisen und interne Prozesse, Verfahren und die IT-Architektur darlegen zu können. Die ersten Bußgelder dürften aus anderen EU-Staaten kommen und eine Hektik auslösen, die nicht zu unterschätzen sei.

Unter der Moderation von *Dr. Eugen Ehmann* hielten *Renate Nicolay* (Kabinettchefin von *Vera Jourová*), *RA Michael Neuber* (Justiziar des BVDW) und *Dr. Stefan Hanloser* (Vice President Data Protection Law bei der ProSiebenSat.1 Group) in der sechsten und letzten Session kurze Statements zum Privacy Shield und zur ePrivacyVO. Die Kommission werde sich, so *Nicolay*, kurz vor dem Stichtag am 25. Mai 2018 an die Bürgerinnen und Bürger wenden und eine Informationskampagne für Kinder und Schulen starten. Derzeit befinde man sich in Verhandlungen zu Adäquanzentscheidungen mit Japan und Südkorea. Interessant seien zudem die Entwicklungen in Brasilien und Indien. Wenn es hingegen nach *Neuber* geht, bräuchte die ePrivacyVO gar nicht (so schnell) zu kommen. Er kritisierte den Systembruch, dass man Daten- und Vertraulichkeitsschutz in einem regele, jedenfalls hinsichtlich der Dienste der Informationsgesellschaft. Die ePrivacyVO sei nicht kohärent. Auf jeden Fall müsse deren Art. 10 verschwinden, denn er offenbare ein mangelndes Technikverständnis des Gesetzgebers. Zudem entspreche das Koppelungsverbot nicht den Marktgegebenheiten. *Hanloser* hob hervor, dass das berechtigte Interesse möglicherweise datenschutzfreundlicher sei, als die beispielsweise im US-amerikanischen Raum übertrieben oft gebrauchte Einwilligung. Diese nämlich

verlange einen Nachweis, der oftmals erstmalig eine Verarbeitung personenbezogener Daten erfordere. Art. 11 DSGVO gelte ausgerechnet nicht für diesen Nachweis, sondern sei auf die Betroffenenrechte beschränkt. Er endete mit der Frage, ob die Lösung wirklich in sogenannten Registration-Walls zu suchen sei. Das Publikum beteiligte sich rege an der Diskussion, angefangen bei einer DSGVO 2.0 über Kritik an der DSGVO – insgesamt unverständlich, Öffnungsklauseln verhindern Harmonisierung, es droht Forum Shopping bei Behörden – bis hin zur Forderung nach mehr Guidance seitens der Kommission für eine einheitliche Anwendung der Grundverordnung.

Unter dem Titel "Literature meets Law" stellte Matthias Göritz seinen neuen, beim Beck Verlag erschienenen Roman "Parker" vor und sprach darüber mit Prof. Dr. Martin Hielscher. Insgesamt ist den Organisatoren damit eine "runde" Veranstaltung gelungen, die den Teilnehmern Impulse und Anregungen für die weitere Vertiefung diverser offener Fragestellungen, die eine grundliegende Neuordnung eines ganzen Rechtsgebiets naturgemäß mit sich bringt, mit auf den Weg gab und gleichzeitig genügend Raum und eine angenehme Atmosphäre für Networking bot.