IT – Recht und Praxis

Beim 16. Österreichischen IT-Rechtstag wurden Gesetzesvorhaben der EU auf dem Gebiet des IT-Rechts, aber auch die praxisnahe Anwendung bestehenden Rechts auf IT-Sachverhalte erörtert.

Nachdem der 15. Österreichische IT-Rechtstag pandemiebedingt in virtueller Form abgehalten werden musste (*Öffentliche Sicherheit*, Nr. 7-8/21, S. 113-115), konnte am 5. und 6. Mai 2022 der 16. Österreichische IT-Rechtstag wie gewohnt als Präsenzveranstaltung im *Haus des Sports* in Wien stattfinden.

Prof. Dimitrios Linardatos, Universität Liechtenstein, gab einen Überblick über die Initiativen der EU zur Daten- und Digitalstrategie. Diese hat zum Ziel, die wachsenden Datenmengen wirtschaftlich zu nutzen und hierfür einen einheitlichen Rechtsrahmen in einem harmonisierten Binnenmarkt zu schaffen. Die „Union Values", der „Brussels Effect", sollen zum Wettbewerbsvorteil werden.

IT-Rechtstag 2022: Referenten Roland Marko, Prof. Dimitrios Linardatos und Rainer Knyrim.

EU-Gesetzesvorschläge.

Diese mit der DSGVO begonnene Strategie soll mit Gesetzesvorschlägen der Kommission fortgesetzt werden, nämlich mit dem Verordnungsentwurf für künstliche Intelligenz (KI-VO), dem Data-Governance-Act (DGA), dem Data-Act (DA) und dem Digital-Markets-Act (DMA). Als Verordnung werden diese Vorschläge, wenn sie Gesetzeskraft erhalten, zu unmittelbar anwendbarem Unionsrecht werden und weitgehende Auswirkungen haben, auf die man sich einstellen sollte.

Die KI-VO stuft Anwendungen der KI nach dem von ihnen ausgehenden Risiko ein. Bestimmte Praktiken sind verboten (Titel II). Dazu zählen Techniken der unterschwelligen Beeinflussung oder der Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen im öffentlichen Raum zur Strafverfolgung, außer es wird in bestimmten Fällen eine Genehmigung erteilt.

Als mit hohem Risiko behaftet (Titel III), mit Bedarf einer Konformitätsbewertung durch Dritte, wird der Einsatz von KI etwa bei Medizinprodukten und in Fahrzeugen eingestuft. Bloße Transparenz hingegen wird gefordert bei geringem Risiko (Titel IV), etwa bei Anwendungen zur Emotionserkennung, zur biometrische Kategorisierung oder zur Manipulation von Inhalten *(Chatbots, Deepfakes)*. Bestehen keine Risiken, können freiwillig Maßnahmen gesetzt werden. Die Einordnung ist allerdings nicht starr, betonte Linardatos. Es können sich Anwendungen durchaus in höhere Risikostufen, bis zum Verbot, entwickeln.

Ein Qualitäts- und Risiko-Management soll sicherstellen, dass fehlerhafte Produkte den Markt nicht erreichen bzw. zurückgenommen werden. Die Produkte unterliegen einem permanenten iterativen *PDCA*-Zirkel *(Plan-Do-Check-Act)*. Eine bloße Endkontrolle genügt nicht.

Die vom Europäischen Parlament am 6. April 2022 bereits verabschiedete Verordnung über Europäische Daten-Governance (DGA), über die RA Mag. Roland Marko berichtete, hat zum Ziel, eingeschränkte Daten des öffentlichen Sektors zur Weiterverwendung für nichtstaatliche Zwecke, etwa für private Innovationen, zur Verfügung zu stellen. Als Beispiel wurden Verkehrsdaten für Routenplaner genannt. Das Gesetz stellt die entsprechenden rechtlichen, technischen und organisatorischen Bedingungen für diese Weiterverwendung auf, etwa hinsichtlich des Schutzes der Integrität technischer Systeme, des Schutzes personenbezogener Daten, des geistigen Eigentums und des Schutzes von Geschäftsgeheimnissen. Es finden sich auch Regelungen für Datenaltruismus (freiwillige Datenspenden). Eine Verpflichtung zur Bereitstellung wird öffentlichen Stellen nicht auferlegt.

Dem Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz, Data-Act) liegt zugrunde, dass das Potenzial vor allem maschinengenerierter Daten weitgehend ungenutzt und auf eine geringe Anzahl sehr großer Unternehmen konzentriert ist. Die mit den Daten verbundene Wertschöpfung soll durch neue rechtliche Rahmenbedingungen für Datenzugang und -nutzung, in Form einer horizontalen Regelungsstruktur, gerechter verteilt werden. Dazu gehören auch Anforderungen an die technische Interoperabilität. Der Nutzer soll direkten, elektronischen Zugang zu den von ihm generierten Daten erhalten *(Access by Design)*. Die Nutzung nicht personenbezogener Daten durch den Dateninhaber soll nur mit vertraglicher Vereinbarung mit dem Nutzer möglich sein. Öffentliche Stellen der EU-Staaten sollen die im Wirtschaftsleben generierten Daten dann nutzen dürfen *(B2G Data Sharing)*, wenn außergewöhnlicher Bedarf besteht, etwa bei Pandemien oder Naturkatastrophen oder wenn die Daten zur Erfüllung einer Aufgabe im öffentliche Interesse erforderlich sind und nicht anderweitig beschafft werden können (Stadtentwicklung).

Dem Gesetz über digitale Märkte (DMA) liegt der Schutz von gewerblichen und Endnutzern gegen unlauteres Verhalten von Gatekeepern auf digitalen Plattformen zu Grunde. Da diese (Beispiel Suchmaschinen) gleichzeitig als Vermittler und Wettbewerber auftreten, soll die Verwendung generierter Daten zur (gezielten) Konkurrenzierung beschränkt und, permanent und in Echtzeit, ein Zugangsrecht gewerblicher Nutzer auf die über sie generierten Daten geschaffen werden. Über die Leitlinien des Eu-

Fotos: Kurt Hickisch

ropäischen Datenschutzausschusses zum vernetzten Fahren und den aktuellen Stand der E-Privacy-VO, über die weiterhin keine Einigung erzielt werden konnte, berichtete RA Dr. Rainer Knyrim.

IT-Sachverhalte – Bewertungen. Über eine Lehrer/innen/bewertungs-App konnten namentlich genannte Lehrer in acht Einzelkriterien (unter anderem Vorbereitung, Fairness und Motivationsfähigkeit) mit einem bis zu fünf Sternen bewertet werden. Aus diesen Einzelbewertungen ergab sich eine Gesamtbewertung. Der Bewertende musste sich über eine Telefonnummer registrieren. Die Bewertung erfolgte ohne Anzeige eines Benutzernamens, somit anonym. Die Datenschutzbehörde hatte ein amtswegiges Prüfungsverfahren eingeleitet, dieses aber eingestellt.

Ein von der Bewertung betroffener Lehrer klagte zivilrechtlich gegen die Verarbeitung seiner personenbezogenen Daten und begehrte deren Löschung. Er sei in seinem Recht auf Datenschutz und in seinen Persönlichkeitsrechten verletzt. Durch organisierte Schlechtbewertung bestehe die Gefahr einer Prangerwirkung. Zudem gebe es keine Möglichkeit der Stellungnahme.

Vom Erstgericht wurde die Klage abgewiesen, vom Berufungsgericht hingegen die Unterlassung der Datenverarbeitung verfügt. Das hinsichtlich der Revision beider Streitparteien letztlich ergangene Urteil des OGH vom 22. Februar 2022, 6 Ob 129/21w, stellte das Ersturteil wieder her. Die Schlussfolgerungen aus dem Urteil fassten RA Mag. Andreas Kezer und Mag. Stefan Knotzer dahingehend zusammen, dass keine Gründe vorliegen, Bewertungen von eigenen Schülern zu untersagen. Die Bewertungen betreffen die Berufsausübung, nicht jedoch das Privat- oder Familienleben. Die Sozialsphäre unterliegt einem geringeren Schutz als der höchstpersönliche Lebensbereich. Dem Lehrer drohen keine beruflichen Nachteile durch eine schlechte Durchschnittsbewertung; die Gefahr schlechter Bewertungen ist hinzunehmen. Eine ausschließliche Sternebewertung schließt Beleidigungen aus. Für passive User ist klar, dass Bewertungen subjektive Einschätzungen sind. Auch unsachlich motivierte Werturteile (etwa durch Ärger) sind von der Meinungsäußerungsfreiheit gedeckt. Zu verlangen, dass die Bewertenden unter ihrem Klarnamen auftreten, würde eine Selbstzensur bewirken.

Foto: Gregor Wenda

Plenarsaal des EU-Parlaments: Am 6. April 2022 wurde die Verordnung über Europäische Daten-Governance (DGA) verabschiedet, mit dem Ziel, eingeschränkte Daten des öffentlichen Sektors zur Weiterverwendung für nicht staatliche Zwecke zur Verfügung zu stellen.

§ 1330 ABGB betrifft den Schutz der Personenwürde (Abs. 1; Ehrenbeleidigung) und den Schutz des wirtschaftlichen Rufs (Abs. 2, Rufschädigung durch Verbreitung unwahrer Tatsachen – wobei auch das Weglassen einer Information eine Tatsachenbehauptung unwahr machen kann).

Bei Sternebewertungen ist fraglich, ob es sich um ein Werturteil oder eine Tatsachenbehauptung handelt. Infolge des Fehlens einer österreichischen Judikatur hiezu leiteten Kezer und Knotzer aus der deutschen Judikatur ab, dass unkommentierte Online- Bewertungen mit Sternen grundsätzlich als Meinungsäußerung einzuordnen seien. Allerdings müsse der Bewertende in irgendeiner Weise mit dem Bewerteten in Kontakt gekommen sein. Ansonsten würde es an der erforderlichen Tatsachengrundlage fehlen und damit an einer Rechtfertigung für den Eingriff in das Persönlichkeitsrecht des Bewerteten.

Eine schlechte Bewertung kann einen positiven Schaden bewirken (Sinken des Unternehmenswertes), einen negativen infolge entgangenen Gewinns und einen immateriellen Schaden. Ein positiver Schaden ließe sich etwa durch Gutachten belegen. Beim entgangenen Gewinn wird dies eher schwerfallen, wie auch beim immateriellen Schaden, dessen Geltendmachung noch am ehesten über das Datenschutzrecht erfolgversprechend wäre. Hinsichtlich unwahrer, erwerbs-, kreditschädigender oder strafrechtlich relevanter Bewertungen besteht ein Anspruch auf Löschung. Sie sind nicht von der Meinungsfreiheit gedeckt.

Vorgangsweise. Ist der Verfasser bekannt, wäre er zunächst zur Löschung der Bewertung bzw. deren Abänderung aufzufordern. Unterlässt er dies, kann auf Schadenersatz nach § 1330 ABGB geklagt und allenfalls, bei Verleumdung, Strafanzeige eingebracht werden.

Ist der Bewertende unter einem Pseudonym aufgetreten, kann vom Betreiber der Plattform gemäß § 18 Abs. 4 ECG Auskunft über Namen und Adresse (auch E-Mail) registrierter Nutzer verlangt werden. Erforderlich ist dazu, den rechtswidrigen Sachverhalt sowie ein überwiegendes rechtliches Interesse an der Identität des Nutzers glaubhaft zu machen und dass die verlangte Information eine wesentliche Voraussetzung für die Rechtsverfol-

gung darstellt. Bei nicht registrierten Nutzern oder Fake-Accounts liegt die Schwierigkeit im Herausfinden der Kontaktdaten. Zudem kann der User behaupten, die Bewertung nicht verfasst zu haben.

Wie in den anderen angeführten Fällen ist es möglich, gegen den Betreiber der Plattform vorzugehen. Dieser ist als Host-Provider nach § 16 ECG verantwortlich, außer er ist in Unkenntnis rechtswidriger Tätigkeiten oder Informationen oder er wird unverzüglich tätig durch Sperren des Zugangs oder Entfernung der Information bei Kenntnis. Eine allgemeine Prüfpflicht trifft den Provider nicht.

Bei Meldungen können die Melde- bzw. Missbrauchsbuttons großer Bewertungsplattformen anhand konkreter Begründungen und Belege genützt werden mit dem Antrag auf Entfernung der Bewertung bei Falschbehauptungen. Es besteht ein Rechtsanspruch auf Löschung. Allerdings hat der Betreiber nach § 21 DSGVO ein Widerspruchsrecht, wozu er zwingend schutzwürdige Gründe nachweisen muss, die gegen die beantragte Löschung sprechen.

IT-Sachverhalte – immaterieller Schaden. Wie RA Mag. Nino Tlapak ausführte, hat nach Art. 82 Abs. 1 DSGVO jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Nach § 29 DSG gelten dafür die allgemeinen Bestimmungen des bürgerlichen Rechts. Somit sind auch juristische Personen anspruchsberechtigt.

Als Schaden gilt nach § 1293 ABGB jeder Nachteil, den eine Person erleidet. Die DSGVO betrachtet als Schaden primär den Verlust von Vertraulichkeit und Integrität von Daten, doch bezieht ErwG 75 unter anderem auch Identitätsdiebstahl, Rufschädigung und Verlust der Kontrolle über personenbezogene Daten mit ein.

Hinsichtlich Umfang oder Erheblichkeitsschwelle ist auf das allgemeine Zivilrecht zurückzugreifen, da die DSGVO diesbezüglich keine Regelungen enthält. Es sind zwar, so Tlapak, nicht alle Unlustgefühle ersatzfähig, doch reicht nach der Judikatur des OGH bereits eine „massive Genervtheit“ aus, dass ein spürbarer und nachvollziehbarer immaterieller Schaden vorliegt, dessen Ermittlung aus freier richterlicher Überzeugung erfolgt (§ 273 StPO). Die Rechtsverletzung muss für den eingetretenen Schaden kausal sein; der Schaden ist wirksam und vollständig zu ersetzen. Darüber hinaus besteht, anders als im angelsächsischen Recht, kein Anspruch auf eine weitere Geldbuße (Strafschadenersatz). Sachlich zuständig ist in erster Instanz das Landesgericht (§ 29 Abs. 2 DSG). Drei Jahre ab Kenntnis des Schadens und des Schädigers ist der Anspruch verjährt.

Anspruch auf Schadenersatz wurde beispielsweise zuerkannt bei unzulässiger GPS-Ortung im Dienstwagen *(OGH 9 ObA 120/19s)*, bei Veröffentlichung eines Bildes in einem Printmedium und Vorwurf eines Drogenproblems *(OLG Wien 18 Bs 213/16d)* oder für bloßstellende Fotos *(OLG Wien 30 R 20/11y-17)*. Dazu kommen noch etliche, von Tlapak angeführte Urteile von Gerichten aus dem EU-Raum. „Wesentliche Auslegungsfragen sind seit 2021 beim EuGH anhängig“, führte Tlapak aus, der auch eine Entwicklung der Judikatur in

Richtung Strafschadenersatz *(punitive damages)* nicht ausschloss.

Datenschutzrecht. Aus dem Referat von Prof. Dr. Eva Souhrada-Kirchmayer, Richterin am Bundesverwaltungsgericht (BVwG), ist hervorzuheben das unter Zahl W214 2232551-1/20E beim BVwG protokollierte Verfahren. Mehrere Polizisten wurden bei einer Kontrolle von Musikern in einem Park mit Smartphones gefilmt. Die Videos wurden in sozialen Netzwerken veröffentlicht, zum Teil mit gesprochenen Kommentaren und der Behauptung eines „Ethnic-Profiling". Der wegen Verletzung des Rechts auf Geheimhaltung eingebrachten Beschwerde wurde von der Datenschutzbehörde (DSB) nur insofern stattgegeben, als die Polizisten in den Videos offensichtlich lächerlich gemacht wurden. Das Bundesverwaltungsgericht gab der Beschwerde nach mündlicher Verhandlung mit Erkenntnis vom 1. Dezember 2021 statt. Eine Unkenntlichmachung der Polizisten wäre möglich gewesen. Deren Persönlichkeitsrecht wurde verletzt, ebenso auch, wegen der Eingriffstiefe, der Grundsatz der Datenminimierung.

Die zu privaten Zwecken vorgenommene Abfrage einer Polizeibeamtin im *Polizeilichen Aktendokumentationssystem (PAD)* hat nicht nur zu einer Disziplinarstrafe, sondern auch zu einer Bestrafung wegen Verwaltungsübertretung nach Art. 83 Abs. 5 lit. a DSGVO geführt *(BVwG 22.11.2021, W214 2238581-1/17E)*.

Die Installierung einer Videoüberwachung in einem Mehrparteienhaus, die auch den Haupteingang umfasst hat und überdies nicht geeignet gekennzeichnet war, war rechtswidrig. Das entsprechende Straferkenntnis der DSB wurde dem Grunde nach bestätigt *(BVwG 12.10.2021, W176 2239662-1/7E)*.

Schwerpunkte des 16. Österreichischen IT-Rechtstags im Haus des Sports in Wien: EU-Gesetzesvorhaben und praxisnahe Anwendung des IT-Rechts.

Einem auf einer Plattform zur Ärztebewertung veröffentlichten Erfahrungsbericht hat der betreffende Arzt unter Nutzung der Meldefunktion seine Sichtweise gegenübergestellt. Diese E-Mail wurde veröffentlicht und trotz mehrmaliger Aufforderung nicht gelöscht. Zu Unrecht, denn die Nutzung der Meldefunktion diene (im Gegensatz zur Kommentarfunktion) erkennbar nicht der Veröffentlichung der dort mitgeteilten Informationen. Die Voraussetzungen für das Medienprivileg (§ 9 DSG; „journalistische Zwecke") liegen bei Bewertungsplattformen nicht vor *(BVwG 15.12.2021, W176 2245370-1/2E)*.

TKG 2021. Am 1. November 2021 ist das *Telekommunikationsgesetz 2021 – TKG 2021* in Kraft getreten *(Art. I BGBl I 190/2021)*. Das in vollem Umfang den *Europäischen Kodex für die elektronische Kommunikation (EKEK), RL (EU) 2018/1972,* umsetzende Gesetz ersetzt das Telekommunikationsgesetz 2003. Die meisten Übergangsbestimmungen sind mit 1. Mai 2022 ausgelaufen. Aus polizeilicher Sicht sind etwa die Bestimmungen über Sperre betrügerisch genützter Rufnummern und Nummernbereiche durch die RTR (§ 121), SMS-Warnungen bei Notfällen und Katastrophen im Auftrag der zuständigen Behörde (Notrufe, § 122), öffentliches Warnsystem (§ 125), Fangschaltung, belästigende Anrufe (§ 141) oder Not- und Katastrophenfunkverkehr (§ 148; Amateurfunker) von Bedeutung.

Das Gesetz wurde, wie Maximilian Kemetmüller des VKI berichtete, um „interpersonelle Kommunikationsdienste" (§ 4 Z 6) erweitert, unterteilt in nummerngebundene und nummernunabhängige Kommunikationsdienste (§ 4 Z 7 und 8). Die Bestimmungen des 14. Abschnitts (Kommunikationsgeheimnis und datenschutzrechtliche Bestimmungen) gelten auch für nummernunabhängige Kommunikationsdienste.

Aus Sicht des Verbrauchers sind von Bedeutung die Pflicht des Internetzugangsdienstanbieters, die Leistung an einem neuen Wohnsitz zu erbringen (§ 135 Abs. 11); der kostenlose „Nachsendeauftrag" für E-Mails (§ 144); die, bis einen Monat nach Vertragsende mögliche, kostenlose Rufnummernmitnahme (§§ 119, 120) und der Wechsel des Internetzugangsanbieters unter Leitung des neuen Anbieters (§ 118).

Die Vertragslaufzeit beträgt mindestens 12 und maximal 24 Monate (§ 135 Abs.1). Es besteht eine einmonatige Kündigungsfrist (§ 135 Abs. 5). Die Vertragszusammenfassung (§ 129 Abs. 4) muss in verständlicher und leicht lesbarer Form einen Überblick über wichtige Teile des Vertrages bieten. Bei nummerngebundenen interpersonellen Kommunikationsdiensten müssen Preis- bzw. AGB-Änderungen mindestens drei Monate vor Inkrafttreten auf einem dauerhaften Datenträger bekanntgegeben werden, samt einer Belehrung über ein Sonderkündigungsrecht.

Zeitnah vor Ende einer Mindestvertragsdauer oder automatischen Verlängerung hat eine Information über das Ende der vertraglichen Bindung und über die Möglichkeit der Vertragskündigung zu erfolgen (§ 135 Abs. 6). Bei automatischer Verlängerung muss der Anbieter jährlich zumindest einmal informieren, welcher aktuelle Tarif in Bezug auf das Nutzungsverhalten des Verbrauchers die beste Wahl ist (§ 135 Abs. 7). Der Tarif- und Angebotsvergleich (§ 134) soll eine selbstständige und informierte Entscheidung ermöglichen, und zwar auch hinsichtlich der Qualität (§ 46) des jeweiligen Dienstes. *Kurt Hickisch*

FOTO: KURT HICKISCH