Daten und Persönlichkeitsschutz

Die Fülle an Daten, deren Auswertung und der Persönlichkeitsschutz waren unter anderem Schwerpunkte des 9. IT-Rechtstages am 7. und 8. Mai 2015 in Wien.

Facebook verarbeitet pro Tag mehr als 500 Terabytes an Daten. Mit dieser Feststellung leiteten die Rechtsanwälte Dr. Stephan Winklbauer und Dr. Rainer Knyrim ihren gemeinsamen Vortrag zu Beginn des *9. Österreichischen IT-Rechtstages* ein, der am 7. und 8. Mai 2015 in Wien abgehalten wurde. Veranstalter war der Verein „Infolaw – Forschungsverein für Informationsrecht und Immaterialgüterrecht“ *(www.infolaw.at, www.it-rechtstag.at)*.

Winklbauer und Knyrim umrissen eines der vier Merkmale von Big Data, nämlich das große Volumen der Datenmenge. Alle ein bis zwei Jahre verdoppelt sich die Datenmenge, die auf der Welt verarbeitet wird. *Google* verzeichnet 2 Millionen Suchanfragen pro Minute.

Kennzeichnend für Big Data ist weiters die Vielfalt der Daten, die von den verschiedensten Quellen stammen (von Menschen eingegeben, von Sensoren abgeleitet, von Smartphones und von Wearables übermittelt) und die unterschiedlichste Formate aufweisen.

Die beiden anderen Merkmale sind die Geschwindigkeit der Verarbeitung, die nahezu in Echtzeit erfolgt, und die fehlende Glaubwürdigkeit, weil die Daten vielfach unpräzise und unvorhersehbar sind.

Die großen, aus unterschiedlichsten Quellen stammenden Datenmengen können nach den unterschiedlichsten Gesichtspunkten ausgewertet werden und können zu neuen Erkenntnissen führen. „Daten sind das Öl des 21. Jahrhunderts.“

Rainer Knyrim: „Konzerne nutzen Geo- und Bewegungsdaten, um Standorte und Öffnungszeiten zu optimieren.“

Knyrim brachte Beispiele: Aus historischen Produktionsdaten, verbunden mit Daten über Wetter und Kaufverhalten konnte eine Skifirma ihre Produktion treffsicher auf den Markt zuschneiden, ohne dabei personenbezogene Daten zu verwenden. Ein Verkehrsunternehmen in einer deutschen Großstadt zog, um die Fahrpläne zu optimieren, in einem Pilotprojekt mit einem Mobilfunkbetreiber Mobilfunkdaten zur Analyse heran, wann welche Personengruppen welche öffentlichen Verkehrsmittel benützen. Zudem sollten noch Geschlecht, das Alter in Zehn-Jahresschritten und die Heimatregion erfasst werden.

Aus den Stammdaten des Mobilfunkbetreibers sowie den Standortdaten der Handys hätten die geforderten Daten abgeleitet werden können. Man hätte Handys beobachtet, die sich mit einer bestimmten Geschwindigkeit fortbewegen. Nach Protesten wurde das Projekt bereits in der Pilotphase eingestellt. Das Unternehmen wollte sich den großen Erhebungsaufwand von Fahrgastzählungen und -erhebungen ersparen. Aus der Kombination von Mobilfunkdaten, GPS- und Grundstücksdaten kann ermittelt werden, wo Leute wohnen und wohin sie zur Arbeit fahren, oder anhand der Aufenthaltsdauer an einem Ort, wo sie einkaufen. Der Standort und die Öffnungszeit von Supermärkten können auf diese Weise optimiert werden.

Clemens Thiele: „Das Fotografieren einer Person ist datenschutzrechtlich bedenklich.“

In den Niederlanden hat ein Hersteller von Navigationsgeräten Bewegungsprofile und die Fahrgeschwindigkeit der Benutzer der Geräte ausgewertet, um Staus bzw. verlangsamten Verkehr zu erkennen und die Verkehrsplanung zu unterstützen. Die Daten wurden an die niederländische Regierung verkauft. Von der Polizei wurden, als Nebeneffekt, die Daten nach Strecken mit den häufigsten Tempoüberschreitungen ausgewertet und dort Geschwindigkeitsmessungen durchgeführt.

Eine für Smartphones entwickelte App, dazu gedacht, sich mit anderen Autofahrern in Echtzeit über Verkehrs- und Straßenverhältnisse auszutauschen, wurde auch dazu verwendet, anderen den Standort gesichteter „Radarfallen“ mitzuteilen. Die Polizei von Los Angeles brachte dieses Feature in Verbindung mit einem tödlichen Angriff auf zwei Polizisten und forderte seine Entfernung. Polizeibeamte im Miami begannen, falsche Daten über die Anwesenheit von Polizisten zu verbreiten, um die Sicherheit der Beamten, aber auch die Verkehrssicherheit allgemein zu erhöhen.

Durch die Häufigkeit von Anfragen zum Suchbegriff einer Krankheit, etwa Grippe, lassen sich beginnende Krankheitswellen oder Epidemien vorhersagen. Bricht an einem Ort eine ansteckende Krankheit aus, lassen sich durch die Auswertung von Mobilitätsdaten Reiserouten ersehen, woraus erkannt werden kann, wohin die Krankheit verschleppt werden wird. Es können dann gezielte Abwehrmaßnahmen getroffen werden.

Big Data und DSG 2000. Nach § 6 Abs. 1 Z 2 DSG dürfen Daten außer zu wissenschaftlicher Forschung und Statistik (§ 46) nur für festgelegte Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden. Das Sammeln von personenbezogenen Daten, um sie später einmal zu einem noch nicht bekannten Verwendungszweck auszuwerten, ist demnach unzulässig. Auf einen solchen Fall wird sich auch eine erteilte Zustimmung (Einwilligung in Kenntnis der Sachlage für den konkreten Fall; § 4 Abs. 1 Z 14 DSG) wohl kaum beziehen können. Für Zwecke wissenschaftlicher oder statistischer Untersuchungen

FOTOS: KURT HICKISCH

(somit nicht für kommerzielle Zwecke) dürfen nach § 46 Abs. 1 DSG personenbezogene Daten verwendet werden, die öffentlich zugänglich sind, für andere Zwecke ermittelt wurden oder indirekt personenbezogen sind. Sonst dürfen derartige Daten nur auf Grund besonderer gesetzlicher Vorschriften oder mit Zustimmung des Betroffenen oder mit Genehmigung der Datenschutzbehörde verwendet werden (§ 46 Abs. 2). Für diese Genehmigung ist unter anderem das Vorliegen eines öffentlichen Interesses erforderlich (§ 46 Abs. 3). Kommerzielle Zwecke sind somit wiederum nicht erfasst.

Big Data sollte laut Knyrim auf anonymisierten Daten aufbauen. Auf diese ist das DSG nicht anwendbar. Allerdings kann durch geschickt angelegte Auswahlbegriffe eine Eingrenzung auf kleine Personengruppen erzielt werden. Eine gewisse Aufweichung des strengen Zweckbindungsprinzips könnte sich durch eine abgeänderte Fassung des Art. 6 Abs. 4 der Datenschutz-Grundverordnung (DSGVO) ergeben, die derzeit als Vorschlag des Rates vorliegt. Es würde dann auf eine Interessenabwägung abgestellt.

Mobilitätsdaten. Sind Kraftfahrzeuge ein vernetztes System, und wenn ja, was geschieht mit den Daten? Antworten auf diese Fragen gab Dr. Michael M. Pachinger an Hand von *E-Call* und *Pay-as-you-Drive*. Bei der *Pay-as-you-Drive*-Versicherung *(PAYD)* wird das Fahrverhalten zur Berechnung der Versicherungsprämie herangezogen. Die technische Umsetzung erfolgt über GPS-basierte Lösungen durch die „On-Board-Unit".

Die Umsetzung des automatischen Notrufsystems *E-Call (Emergency Call)* beruht auf der am 19. Mai 2015 im Amtsblatt der EU veröffentlichten Verordnung (EU) 2015/758 vom 29.4.2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden E-Call-Systems in Fahrzeugen.

IT-Rechtstag: Raimund Wagner, Michael Pachinger.

Die Verordnung gilt nach ihrem Art. 14 im Wesentlichen ab dem 31. März 2018. Ab diesem Zeitpunkt muss in allen neuen Pkw-Modellen und leichten Lkws E-Call installiert sein. Bei Auslösen des Airbags ruft das System selbstständig die europäische Notrufnummer 112. Es wird ein genormter Mindestdatensatz (Fahrzeugkennung und -typ, Treibstoff, Unfallzeit, Ortsangabe und Anzahl der Insassen) übermittelt und es wird eine Sprechverbindung hergestellt. In der Folge wird die Rettungskette in Gang gesetzt. Durch die Einführung von E-Call wird erwartet, dass jährlich bis zu 2.500 Menschenleben gerettet werden können und sich die Zahl der Unfalltoten um zehn Prozent pro Jahr verringert. Der Privatsphäre und dem Datenschutz wird in Art. 6 der Verordnung Rechnung getragen. Beispielsweise dürfen, bevor der E-Call ausgelöst wird, diese Daten außerhalb des bordeigenen E-Call-Systems für keine Einrichtung zugänglich sein. Für „Privacy by Design" ist vorzusorgen. Die Rechtsgrundlage für die Verarbeitung dieser Daten ist damit gegeben. Ein Kfz generiert jedoch, über rein Technisches wie Betriebszustand, Geschwindigkeit und Treibstoffverbrauch hinaus, eine Menge von Daten, die wirtschaftlich von Interesse sein können.

Versendete Orts- und Zeitdaten können dazu führen, Hinweise auf den nächsten Schnellimbiss oder die nächste Tankstelle zu erhalten – aber auch den Nachweis über falsches Parken liefern. Auch wenn der jeweilige Benützer des Kfz nicht unmittelbar feststeht, wird er mit rechtlich zulässigen Mitteln bestimmt werden können, sodass die Daten als personenbezogen anzusehen sind (§ 4 Z 1 DSG). Derartige Daten dürfen nur für rechtmäßige Zwecke verwendet werden (§ 6 Abs. 1 Z 2), etwa zur Prämienberechnung bei PAYD, nicht aber zur Auswertung nach einem Unfall.

Eine gegebene Zustimmung ist möglicherweise nicht ganz ohne Zwang, wenn eine Prämienreduktion in Aussicht gestellt wird. Ein Widerruf der Zustimmung hätte Auswirkungen auf den Versicherungsvertrag.

Derartige datenschutzrechtliche Probleme werden umgangen, wenn Daten anonymisiert werden. Ein E-Call-geeigneter „Anonymiser" als On-Board-Unit für Telematik-Daten, der das *European Privacy Seal* erhalten hat, wurde von Raimund Wagner vorgestellt *(AMV Networks GmbH, www.amv-networks.com)*.

Persönlichkeitsrechte. Rechtsanwalt Dr. Clemens Thiele wies darauf hin, dass § 16 ABGB, wonach jeder Mensche angeborene, schon durch die Vernunft einleuchtende Rechte hat, und daher als eine Person zu betrachten ist, wegen fehlender Rechtsfolge lange Zeit als Programmsatz betrachtet worden sei. „Mittlerweile wurde diese Bestimmung in der österreichischen Rechtsprechung zu einer zentralen Norm der Persönlichkeitsrechte." Zu diesen zählen, neben Leben, Gesundheit und Freiheit, das Recht auf den eigenen Namen, am eigenen Bild und am eigenen Wort, auf Ehre und Wahrung der Privatsphäre.

In den verfassungsgesetzlich gewährleisteten Schutz der Privatsphäre (Art. 8 EMRK) fällt inhaltlich auch der ebenfalls auf Verfassungsebene verankerte Datenschutz (§ 1 DSG).

Wurde bisher die Auffassung vertreten, § 78 UrhG verbiete bloß die Verbreitung der Bildnisse von Personen, nicht aber die Herstellung der Bildnisse selbst, ist dies unter Einbeziehung von Art. 8 EMRK und § 16 ABGB durch die Judikatur insofern relativiert worden, als eine umfassende Interessenabwägung im Einzelfall stattzufinden hat. Das allgemeine Privatrecht wird dazu herangezogen, Lücken in Spezialgesetzen zu schließen. Eine Aufnahme mit einer Digitalkamera ohne Einverständnis des Fotografierten bloß „zur Belustigung" stellt einen Eingriff in dessen Persönlichkeitsrecht dar (OGH 27.2.2013, 6 Ob 256/12h). Es kommt somit zu einem relativen Bildherstellungsverbot,

FOTOS: KURT HICKISCH

wie auch bei einer Aufnahme des gesprochenen Wortes, unabhängig von einer weiteren Verbreitung. Die (zivilrechtlichen) Rechtsfolgen können sein ein Feststellungs- und Unterlassungsanspruch, Anspruch auf Beseitigung bzw. Vernichtung, auf Entschädigung, Veröffentlichung und ein Verwendungsanspruch nach § 1041 ABGB. Es kann sogar ein Kontrahierungszwang entstehen, etwa, wenn Menschen aus ethnischen Gesichtspunkten der Eintritt in ein Lokal verwehrt wurde. Ein Auskunftsanspruch besteht hingegen nicht („Peilsender", OGH 22.1.2014, 3 Ob 197/13m).

Soweit eine Person erkennbar ist, werden, wenn sie fotografiert wird, personenbezogene Daten verarbeitet. Diese Verarbeitung fällt datenschutzrechtlich unter die §§ 7 und 8 DSG und ist, sofern keine Zustimmung des Betroffenen vorliegt, zulässig, wenn dies überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten erfordern.

Eine Interessenabwägung kommt allerdings nicht in Betracht, wenn sensible Daten (§ 4 Z 2 DSG) vorliegen. Sofern keine der in § 9 DSG taxativ aufgezählten Tatbestände gegeben sind, besteht ein Verbot der Verarbeitung.

Eine Rechtsauffassung geht dahin, Bilddaten insofern als sensible Daten einzustufen, als sie Ausdruck des Gesundheitszustandes eines Menschen seien (Brillenträger; aber auch ein „gesunder" Mensch zu sein, ist ein „Gesundheitsdatum") oder indem seine rassische oder ethnische Herkunft aus Bildern ableitbar ist.

Damit kommt man aus Gründen des Datenschutzes zu einem absoluten Fotografierverbot gegenüber natürlichen Personen. Nach der derzeitigen Rechtslage (und bis zu einer höchstgerichtlichen

E-Call: Daten dürfen außerhalb des bordeigenen E-Call-Systems für keine Einrichtung zugänglich sein.

Klärung) sind Ausnahmen nur auf der Basis der „Household Exemption" des Art. 3 Abs. 2 2. Gedankenstrich der DS-RL 95/46/EG (bei Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten; hiezu Vorabentscheidung des EuGH im Urteil vom 11.12.2014, C 212/13) zu ersehen oder, unter Interessenabwägung, wenn die Verarbeitung allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt (Art. 9 DS-RL; Vorabentscheidung EuGH vom 16.12.1008, C 73/07; „Satamedia I").

Über die rechtlichen und faktischen Auswirkungen des Urteils des EuGH vom 13.5.2014, C-131/12 *(Google Spain* SL gegen spanische Datenschutzbehörde) referierte Rechtsanwalt Dr. Arthur Stadler. Mit diesem Urteil wurde klargestellt, dass auch eine ursprünglich rechtmäßige Verarbeitung sachlich richtiger Daten im Laufe der Zeit (im Anlassfall 16 Jahre zurückliegend) nicht mehr der Datenschutz-RL entsprechen kann. Ein Recht auf „Vergessenwerden" kann der Entscheidung allerdings nicht entnommen werden.

In den ersten Wochen nach dem Urteil sind bei *Google* 70.000 Anträge auf Löschung eingegangen. Google hat dafür ein Online-Formblatt aufgelegt. Mit Stand 7. Mai 2015 waren 251.433 Löschungsanträge eingelangt. In 41 Prozent der Fälle wurden Löschungen durchgeführt. Löschungsansprüche bei unrichtigen Inhalten haben schon bisher bestanden (§ 1330 ABGB).

Digitaler Nachlass. Wenn jemand stirbt, hinterlässt er Daten in sozialen Netzwerken, E-Mails, in der Cloud, bei Online-Versanddiensten, in Suchmaschinen usw. Rechtsanwalt Dr. Thomas Höhne präsentierte zum Thema „Tod im Internet" eine Umfrage, wonach auf die Frage „Haben Sie Ihren digitalen Nachlass geregelt?" 50,6 Prozent der Befragten mit „nein" geantwortet haben und 45,8 Prozent mit der Gegenfrage „Wie geht das?". 3,6 Prozent hatten Regelungen getroffen.

Hat der Erbe Zugriff auf die entsprechenden Daten, darf er sie auch benutzen. Briefe, Tagebücher und ähnliche vertrauliche Mitteilungen dürfen nicht verbreitet werden, wenn dies nahe Angehörige verletzen würde (§ 77 UrhG).

Hat der Erbe keinen Zugang zu Telekommunikationsdiensten, steht er vor demselben Problem wie ein Erbe, der keinen Wohnungsschlüssel hat. Dem Erben stünde zwar der gesamte Kommunikationsvorgang des Erblassers zu, doch steht dem von Seiten der Provider das Kommunikationsgeheimnis des § 93 TKG entgegen. Sind E-Mails noch nicht abgerufen, ist der Erbe bei Eintritt in das Account-Vertragsverhältnis berechtigt, diese abzurufen. Ein Konto bei einer Online-Bank wird nicht anders als bei konventionellen Banken behandelt; es ist im Verlassenschaftsverfahren offenzulegen.

Daten bei Social Media können bei Nachweis mit der Sterbeurkunde gelöscht oder im Gedenkzustand („In Erinnerung an") aufrecht erhalten werden. Bei Einrichtung einer virtuellen Totengedenkstätte kann ein „Verunehren" im Sinne des § 190 StGB (Störung der Totenruhe), das Handlungen voraussetzt, durch bloße Missachtungsäußerungen (Postings) zwar nicht erfolgen, wohl aber durch einen Hackerangriff, der die Gedenkstätte verunstaltet.

Bei Online-Archiven, den Bibliotheken des digitalen Zeitalters, ist das Interesse der Öffentlichkeit höher zu werten als ein aus persönlichen Gründen entgegenstehendes Interesse. War allerdings eine Veröffentlichung schon ursprünglich rechtswidrig, muss der Betreiber sie wieder aus dem Archiv entfernen.

Wurde der Artikel zu Recht veröffentlicht, erfolgte ein Widerruf oder eine Gegendarstellung, ist der Artikel im Archiv zu belassen, muss aber mit dem Widerruf oder der Gegendarstellung verknüpft werden (OGH 19.2.2004, 6 Ob 190/03i).

Nahe Angehörige können für einen Verstorbenen Persönlichkeitsschutz geltend machen, wenn die Interessenabwägung zu Lebzeiten des Verstorbenen zu dessen Gunsten ausgegangen wäre (OGH 17.2.2014, 4 Ob 203/13a – „Russenanwalt"; OGH 25.3.2014, 4 Ob 224/13i; OGH 29.8.2002, 6 Ob 283/01p). *Kurt Hickisch*

FOTO: FOTOLIA/FOTOHANSEL