Digitalisierung und Vernetzung

Neben Rechtsfragen zur Sharing Economy und zum E-Commerce wurden beim 11. österreichischen IT-Rechtstag in Wien Fragen zu autonomen Systemen und zur DSGVO diskutiert.

Zentraler Aspekt der Digitalisierung ist die Vernetzung“, sagte Rechtsanwalt Fritz-Ulli Pieper, *TaylorWessing (www.taylorwessing.com)* beim 11. österreichischen IT-Rechtstag, der vom Forschungsverein *Infolaw (www.infolaw.at)* veranstaltet, am 4. und 5. Mai 2017 in Wien stattfand. 2003 entfielen auf einen der damals 6,3 Milliarden Menschen weltweit 0,08 digitale Geräte, 2010 stieg dieses Verhältnis auf 1,84, und 2015 auf 3,47. 2020 werden 7,6 Milliarden Menschen 50 Milliarden dieser Geräte besitzen (Verhältnis 1:6,58).

Die Geräte werden „smart“ und interagieren zunehmend „autonom“. Autonomie ist der Grad der Eigenständigkeit einer Entscheidung, Intelligenz die Qualität der möglichen Lösungsalternativen. Je autonomer ein System handelt, desto schwieriger wird die Zuordnung zu einer verantwortlichen Person. Rechtsprobleme wirft schon auf, wenn zum Beispiel aus dem Internet der Dinge der Kühlschrank aus eigenem Nachbestellungen tätigt. Ist er Bote oder Stellvertreter?

Selbstlernende Systeme können sich vom Menschen wegentwickeln, sodass die Zuordnungskette nicht mehr nachvollziehbar werden kann. Die Lösung könnte die Schaffung einer „E-Person“ sein, die mit eigener Identität (Registereintragung) und eigenem Vermögen ausgestattet ist und für die Versicherungspflicht besteht.

Künstliche Intelligenz. „Das Internet of Things allein ist noch nicht intelligent“, hob Dr. Oliver Stiemerling, *ecambria systems (www.ecambria-experts.de),* den Unterschied zur künstlichen Intelligenz hervor. „Intelligenz beginnt dort, wo Entscheidungen getroffen werden.“ Selbst wenn Dinge untereinander kommunizieren, gehorchen sie immer noch strengen, programmierten Abläufen. Aus den vernetzten Datenquellen (Alltagsgeräte, Produktionsdaten, Umweltinformationen) samt ihren Sensoren entstehen allerdings große Datenmengen über realweltliche Sachverhalte („Big Data“).

Smart Home: Rechtlich problematisch ist es, wenn der Kühlschrank aus eigenem Nachbestellungen tätigt.

„Bereits die Daten aus einem Mobiltelefon erlauben viele Rückschlüsse“, sagte Stiemerling. Diese Datenmengen bilden den Rohstoff zu automatisiertem Erkennen, Lernen, Entscheiden und Planen und damit zu „Künstlicher Intelligenz“ (KI). Diese wiederum ermöglicht autonome Systeme, wie das selbstfahrende Auto, und könnte sich steigern bis zum Verlust der Kontrolle über die Systeme – als Vision der „Singularität“, dass Maschinen intelligenter sind als der Mensch.

Aber schon das Erkennen von Mustern und Strukturen, beispielsweise der Dreiecksform eines Verkehrszeichens, ist technisch anspruchsvoll. Der Computer muss aus einem bloßen „Datenrauschen“, das von Sensoren, Kameras oder Mikrofonen geliefert wird, schrittweise und analytisch relevante Informationen extrahieren. In weiterer Folge müssen Bedeutungszusammenhänge erkannt werden (maschinelles Lernen).

Große Datenbestände erlauben, Zusammenhänge zu erkennen. Beispielsweise konnten aus der Analyse von 200 Millionen aufgezeichneten Überholvorgängen beim Nachfahren hinter einem Lkw Vorhersagen getroffen werden, mit welcher Wahrscheinlichkeit ein hinter dem Lkw fahrendes Kfz ausscheren und es zu einem plötzlichen Fahrbahnwechsel kommen wird. Dennoch kann dies menschliches Hintergrundwissen nicht ersetzen.

Maschinelles Planen wiederum bedeutet, die „beste“ Handlungsalternative zu finden. Bei Schach oder dem Go-Spiel wurde der Mensch von der Maschine schon übertroffen. Im Straßenverkehr steht man bei autonomen Systemen erst am Anfang. Im Prinzip müssen Sensoren die Umgebungsparameter erfassen. Dann müssen diese erkannt und ausgewertet werden.

Auf dieser Grundlage sind die Aktionen zu planen. Letztlich setzen Aktoren (Antrieb, Bremse, Lenkung etc.) die Aktionen durch. Jede dieser Ebenen bietet Fehlermöglichkeiten. Es stellt sich die Frage, ab welcher Fehlerrate solche Systeme zugelassen werden können.

Autonome Fahrzeuge. Nach § 102 Abs. 3a und 3b KFG idF 33. KFG-Novelle, BGBl I 2016/67, in Kraft seit 2.8.2016, kann von den Verpflichtungen des Lenkers eines Kraftfahrzeuges abgewichen werden, dass dieser den Lenkerplatz bestimmungsgemäß einzunehmen und das Lenkrad mit mindestens einer Hand festzuhalten hat (§ 102 Abs. 2 erster Satz und Abs. 3 dritter Satz erster Fall KFG).

Diese Übertragung bestimmter Fahraufgaben an im Fahrzeug vorhandene Assistenzsysteme gilt aber nur, soweit dies durch Verordnung zugelassen ist und diese Systeme genehmigt sind oder den durch Verordnung festgelegten Anforderungen für Testzwecke entsprechen.

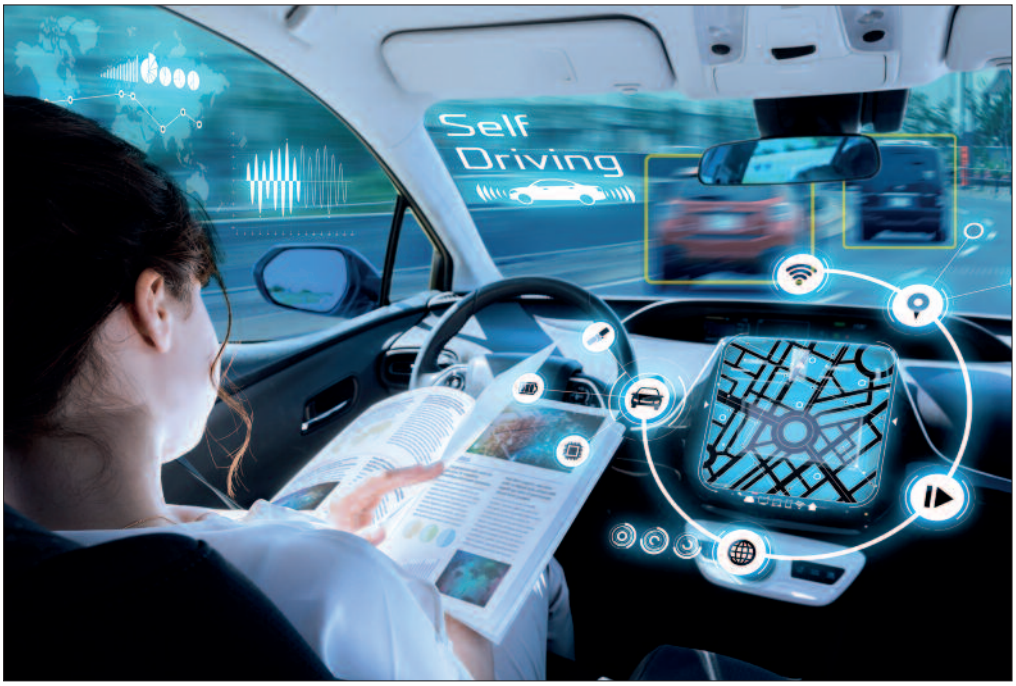
Der Lenker bleibt aber stets verantwortlich, seine Fahraufgaben wieder zu übernehmen. Die näheren Regelungen wurden durch die am 20.12.2016 in Kraft getretene Automatisiertes-Fahren-Verordnung – AutomatFahrV, BGBl II 2016/402 – getroffen.

FOTO: NICOELNINO/FOTOLIA

Rechtsanwalt Dr. Wolfgang Tichy, *Schönherr Rechtsanwälte (www.schoenherr.eu)* referierte über Haftungsfragen bei autonomen Systemen. Eine strafrechtliche Verantwortlichkeit des Lenkers eines Fahrzeuges ist nach § 88 StGB gegeben, wenn er die im Verkehr erforderliche Sorgfalt außer Acht lässt. Welche Sorgfalt bei einem autonomen System aufzuwenden ist, wird wohl in der Rechtsprechung herausgearbeitet werden müssen. Bei einer Manipulation des Systems durch einen Hacker könnte § 118 StGB (Widerrechtlicher Zugriff auf ein Computersystem) als Strafbestimmung in Betracht kommen. Unbefugter Gebrauch von Fahrzeugen (§ 136 StGB) betrifft lediglich das unbefugte Benützen von Fahrzeugen.

Bei der zivilrechtlichen Haftung des Lenkers wird es auf den Grad der Automatisierung ankommen, inwieweit diese dem Stand der Technik entspricht und sich der Lenker darauf verlassen konnte. Der schuldtragende Programmierer wird schwer zu finden sein. Eine Deliktshaftung des Herstellers nach § 1315 ABGB (Verwendung habituell untüchtiger oder wissentlich gefährlicher Mitarbeiter) oder aus Vertragshaftung (§ 1313a ABGB) wird schwer zu beweisen sein.

Die Gefährdungshaftung nach dem Eisenbahn- und Kraftfahrzeughaftpflichtgesetz (EKHG) ist hingegen verschuldensunabhängig. Sie kommt zum Tragen, wenn durch einen Unfall beim Betrieb eines Fahrzeuges ein Mensch getötet, verletzt oder eine Sache beschädigt wird. Die Ersatzpflicht ist lediglich dann ausgeschlossen, wenn der Unfall durch ein unabwendbares Ereignis verursacht worden ist, das weder auf einem Fehler in der Beschaffenheit noch auf einem Versagen der Verrichtungen (der Eisenbahn oder) des Kraftfahrzeuges beruhte. Für Softwarefehler muss damit eingestanden werden. Offen bleibt, wer oder was den Fehler in der Beschaffenheit verursacht hat, wenn etwa durch Hacking eine fehlerhafte Entscheidung verursacht wurde.



Autonomes Fahren: Eine strafrechtliche Verantwortlichkeit des Lenkers eines Fahrzeuges ist gegeben, wenn er die im Verkehr erforderliche Sorgfalt außer Acht lässt.

Nach dem Produkthaftpflichtgesetz (PHG) haftet der Hersteller des Endprodukts für Personenschäden und Schäden an vom Produkt verschiedenen körperlichen Sachen. Strittig ist, ob auch der Hersteller eines Teilprodukts für Schäden am Endprodukt haftet, und ob Software ein Produkt im Sinn des PHG ist. Haftet der Hersteller für ein fehlerhaftes Update? Jedenfalls aber, sagt Tichy, wird die Bedeutung der Herstellerhaftung stark zunehmen.

Informationsschutz. In einem Auto sind schon jetzt im Schnitt einhundert Sensoren eingebaut, die den Zustand des Kraftfahrzeuges überwachen, erklärte Univ.-Prof. Dr. Andreas Wiebe, Universität Göttingen. Wenn dann noch Daten über Fahrverhalten, die Fahrumgebung und den Straßenzustand dazukommen, wird ein Auto zum Endgerät für die großen Internet-Anbieter. Zum anderen aber werden die Daten, über den Fahrzeughalter hinaus, für die „Stakeholder" interessant, wie den Produzenten des Fahrzeugs, Versicherungen („pay as you drive"), die öffentliche Verwaltung (Stadtplanung; Verkehrsleit- und Mautsysteme; e-Call; sicherheitspolizeiliche Erfordernisse).

Das wirft Fragen nach dem Verfügungsrecht über die (Maschinen-)Daten auf. Besitz bzw. Eigentum gibt es nur an körperlichen Sachen. Urheberrechtlich ist als geistige Schöpfung nur die Datenbank als Ordnungsprinzip geschützt, nicht aber die in ihr enthaltenen Daten. Dem Know-how-Schutz unterliegen nur Geschäftsgeheimnisse. Maschinendaten haben einen vom Markt regulierten wirtschaftlichen Wert, weshalb auf europäischer Ebene Regelungen nach einem Sharing-Prinzip gesucht werden, mit abgestuften Zugangsrechten.

Datenschutz. Nach Art. 28 der am 25. Mai 2018 in Kraft tretenden Datenschutz-Grundverordnung der EU (DSGVO) darf der Verantwortliche (bisherige Diktion: Auftraggeber) nur mit Auftragsverarbeitern (bisher: Dienstleister) zusammenarbeiten, die hinreichend Garantien dafür bieten, dass technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Der Auftragsverarbeiter kann den Nachweis hinreichender Garantien durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 erbringen.

Ein derartiger Nachweis impliziert, wie Dr. Axel Anderl, Kanzlei *Dorda (www.dorda.at)* ausführte, dass der Verantwortliche die Erfüllung seiner Pflichten nachgewiesen hat (Art. 24 Abs. 3 DSGVO), dem Datenschutz durch Technikgestaltung *(Privacy by design)*

FOTO: CHOMBOSAN/FOTOLIA




Referenten beim IT-Rechtstag: Andreas Wiebe, Oliver Stiemerling, Georg Fellner, Eva Souhrada-Kirchmayer.

und durch datenschutzfreundliche Voreinstellungen *(Privacy by Default)* nachgekommen ist (Art. 25 Abs.3) und die erforderlichen Sicherheitsmaßnahmen bei der Verarbeitung der Daten einhält (Art. 32 Abs. 3). Die Datenübermittlung in Drittländer wird durch einen solchen Nachweis erleichtert (Art. 46 Abs. 2).

Die Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren stellt weiters einen Strafmilderungsgrund dar (Art. 82 Abs. 2 lit. j). Art. 28 Abs. 3 legt den Mindestinhalt für den vom Verantwortlichen mit dem Auftragsverarbeiter abzuschließenden Vertrag fest.

Bis zum Inkrafttreten der Datenschutz-Grundverordnung wird als praktischer Handlungsbedarf empfohlen, die getroffene Auswahl der Auftragsverarbeiter zu überprüfen, bestehende Verträge anzupassen und die Auftragsverarbeiter rechtzeitig in die Datenschutz-Folgenabschätzung (Art. 35) einzubinden.

Maßnahmen. Die technischen und organisatorischen Maßnahmen zur Erfüllung der Anforderungen der DSGVO erläuterte DI Dr. Walter Hötzendorfer, *Research Institute (www.researchinstitute.at)*. Die in Art. 32 Abs. 1 beispielhaft umschriebenen Maßnahmen zur Herstellung eines dem Risiko angemessenen Schutzniveaus werden praktisch in der Einführung eines Informationssicherheits-Managementsystems (ISO 27000 Normenreihe) bestehen, und zwar als kontinuierlicher Verbesserungsprozess (Art. 32 Abs. 1 lit.d).

Unter anderem ist der Risikofaktor Mensch zu berücksichtigen (Art. 32 Abs. 4), beispielsweise durch Verhaltensrichtlinien, restriktive Zugriffsregelungen, Zugriffsprotokollierung; Schulungen, Awarenessbildung.

Privacy by Design als Verwirklichung des Schutzes personenbezogener Daten schon vom System her kann durch nachstehende Strategien erreicht werden: Minimize (Geringhalten der Datenmenge), Hide (Daten und Zusammenhänge verborgen halten), Separate (Verteilte Bearbeitung und Speicherung), Aggregate (Verarbeitung im höchsten Aggregationsniveau, bei niedrigstem Detailgrad), Inform (Angemessene Information der Betroffenen), Control (Betroffene sollen Kontrolle über die Verarbeitung ihrer Daten erhalten), Enforce (Datenschutzregeln sollen vorhanden sein und durchgesetzt werden) und Demonstrate (Einhaltung der gesetzlichen Bestimmungen muss nachgewiesen werden können).

Privacy by Default bedeutet, dass von vornherein die datenschutzfreundlichsten Einstellungen getroffen sind, wenn ein Produkt in Betrieb genommen oder eine Dienstleistung in Anspruch genommen wird. Nachträgliche bewusste Änderung ist aber möglich. Beispielsweise soll das Hochladen eines Fotos nur einem bestimmten Personenkreis zugänglich sein, wobei die Möglichkeit besteht, diesen Kreis nachträglich zu erweitern.

Die als Sicherheitsmaßnahme verpflichtend vorgesehene Pseudonymisierung von personenbezogenen Daten (Art. 4 Z 5; Art. 25 Abs. 1) sieht der Experte als schwierig an. Selbst wenn identifizierende Attribute (Name etc.) entfernt werden, kann aus den Daten heraus eine Zuordnung zum Betroffenen möglich sein, wie etwa bei individuellen medizinischen Daten.

Wenngleich bei Maßnahmen zum Datenschutz, neben dem Stand der Technik, auch die Implementierungskosten zu berücksichtigen sind (Art. 25 Abs. 1; Art. 32 Abs. 1), kann ein unzureichendes Schutzniveau nicht mit wirtschaftlichen Erwägungen gerechtfertigt werden.

Dr. Eva Souhrada-Kirchmayer, Richterin am Bundesverwaltungsgericht, gab einen Überblick über die jüngste datenschutzrechtliche Judikatur dieses Gerichtes, des Verwaltungsgerichtshofes und des EuGH.

Unter anderem ist bemerkenswert das Erkenntnis des VwGH vom 12.9.2016, Ro 2015/04/001, nach dem aus dem Umstand, dass im öffentlichen Raum gefilmt wird (im vorliegenden Fall mit einer Dash-Cam von einem Auto aus), für sich genommen noch nicht auf das Fehlen einer rechtlichen Befugnis geschlossen werden kann.

Die Unzulässigkeit wurde, aus dem Grundsatz des Einsatzes des gelindesten Mittels darin gesehen, dass eine dauerhafte Speicherung von Bilddaten jederzeit durch Drücken eines „SOS-Button“ erfolgen konnte.

Rechtsanwalt Mag. Georg Fellner, *bkp Rechtsanwälte (www.bkp.at)*, gab einen Überblick über die wichtigsten Öffnungsklauseln der DSGVO. Diese – je nach Zählweise zwischen 50 und 70 – erlauben ergänzende nationale Regelungen. In der Zwischenzeit sind in Österreich diese Anpassungen durch das Datenschutz-Anpassungsgesetz 2018, BGBl I 2017/120, und in Deutschland durch das Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU, dBGBl I 2017/44 – bereits erfolgt.

Kurt Hickisch
www.it-rechtstag.at

Fotos: Kurt Hickisch