Neues im EU-Recht

Beim 6. IT-Rechtstag des Vereins Infolaw wurden aktuelle Entwicklungen im europäischen Datenschutz- und E-Commerce-Recht erörtert.

Das Internet ist global; Gesetze, die ihm einen Rahmen geben sollen, sind national – alte Rechtsprobleme treten wieder auf und werden drängender. Rechtsverletzungen (zivil- und strafrechtlich) können im Internet überall erfolgen, der Schaden überall eintreten (Ubiquität des Internets).

Das Spannungsfeld zwischen der Territorialität der Rechtsordnungen und der Internationalität des Internets wurde beim 6. IT-Rechtstag am 10. und 11. Mai 2012 im Haus des Sports in Wien von Referenten aus verschiedenen Blickwinkeln beleuchtet. Organisiert wurde der IT-Rechtstag vom Verein Infolaw, Forschungsgruppe für Informationsrecht und Immaterialgüterrecht, Wien *(www.infolaw.at)*.

Datenschutzrecht. Über die bevorstehenden Neuerungen im Datenschutzrecht der EU referierte Dr. Rainer Knyrim (Preslmayr Rechtsanwälte OEG). Der am 25. Jänner 2012 von der EU-Kommission veröffentlichte Vorschlag für eine „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)“, KOM (2012) 11 endgültig sieht nicht wie bisher eine von den Mitgliedstaaten in nationales Recht umzusetzende Richtlinie vor, sondern eine direkt anwendbare Verordnung.

Eine Zersplitterung des Datenschutzrechtes innerhalb der EU soll dadurch vermieden und ein „kohärenter“ Rechtsrahmen (Erwägungsgrund [im Folgenden: ErwG] 6) geschaffen werden. In einem Kohärenzverfahren (Art. 57 ff) soll nach dem Entwurf in Fällen mit Bedeutung für mehrere Mitgliedstaaten die EU-Kommission entscheiden und nationale Aufsichtsbehörden zur Aussetzung von geplanten Maßnahmen auffordern können (Art. 60).

Max Schrems: „Schattenprofile aus Facebook-Daten sollen gezieltere Werbung ermöglichen.“

Axel Anderl: „Alle nationalen Verbraucherschutz-Richtlinien der EU sollen harmonisiert werden.“

Als „betroffene Person“ (Art. 4) werden nach dem Vorschlag nur natürliche Personen angesehen, also nicht, wie derzeit nach dem DSG 2000, auch juristische Personen oder Personengesellschaften.

Nach Art. 7 trägt der für die Verarbeitung von Daten Verantwortliche die Beweislast dafür, dass die betroffene Person ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für eindeutig festgelegte Zwecke erteilt hat.

Bei schriftlicher Erklärung muss die Einwilligung äußerlich erkennbar von einem anderen Sachverhalt getrennt sein, beispielsweise also getrennt von den AGBs. Art. 8 sieht besondere Regelungen für die Einwilligung von Eltern bei der Verarbeitung personenbezogener Daten eines Kindes bis zum vollendeten 13. Lebensjahr vor.

Schon bei der Erhebung personenbezogener Daten hat der für die Verarbeitung Verantwortliche die betroffene Person umfangreich zu informieren, auch, wie lange die Daten gespeichert werden (Art. 14); der Person kommt ein Auskunftsrecht zu (Art. 15).

Art. 17 sieht ein „Recht auf Vergessenwerden und auf Löschung“ vor, mit der Verpflichtung des Verarbeitenden, auch alle jene von der begehrten Löschung zu verständigen, an die die Daten weitergegeben wurden. Jederzeit kann von der betroffenen Person gegen die Verarbeitung personenbezogener Daten Widerspruch eingelegt werden (Art. 19).

Ein Recht auf Datenübertragbarkeit ist vorgesehen (Art. 18). Den für die Verarbeitung Verantwortlichen treffen Dokumentationspflichten (Art. 28). Er hat Vorkehrungen für die Datensicherheit zu treffen und eine Datenschutz-Folgeabschätzung (Art. 33; Privacy Impact Assessment) durchzuführen (Art. 22). Datenschutz ist unter Berücksichtigung des Standes der Technik bereits durch die Technik und datenschutzfreundliche Voreinstellungen sicherzustellen (Art. 23; Privacy by Design; Privacy by Default).

Verletzungen des Schutzes personenbezogener Daten sind der Aufsichtsbehörde zu melden (Art. 31; Data Breach Notification Duty). Die betroffene Person ist ohne unangemessene Verzögerung zu benachrichtigen (Art. 32).

Dem Ziel, die Eigenverantwortung zu stärken, entspricht, neben den Dokumentationspflichten, auch die Installierung von Datenschutzbeauftragten. Während Behörden oder öffentliche Einrichtungen immer einen solchen zu benennen haben, müssen das nur Unternehmen, die 250 oder mehr Mitarbeiter beschäftigen (Art. 35 Z 1).

Damit sind, so Knyrim, in Österreich nur 0,3 Prozent aller Unternehmen betroffen, in Deutschland 0,2 Prozent. Der Datenschutzbeauftragte ist unabhängig und weisungsfrei (Art. 36). Er ist unter anderem Ansprechpartner für die Aufsichtsbehörde (Art. 37).

Die von jedem Mitgliedstaat einzurichtende nationale Aufsichtsbehörde (Art. 46) ist unabhängig und weisungsfrei (Art. 47). Die für die Hauptniederlassung eines Unternehmens zuständige Aufsichtsbehörde ist auch für die sonstigen Niederlassungen in anderen Ländern zuständig (Art. 51; Prinzip des One-Stop-Shops).

FOTOS: KURT HICKISCH

IT-Rechtstag: Referenten Michael Pachinger, Eva Souhrada-Kirchmayer, Rainer Knyrim, Moderator Wolfgang Freund.

Foto: Kurt Hickisch

Aufsichtsbehörde. Über die Stellung der Aufsichtsbehörde und im Besonderen ihre Aufgaben (Art. 52) informierte Dr. Eva Souhrada-Kirchmayer von der Datenschutzkommission. Die Leistungen der Aufsichtsbehörde sind für die betroffene Person, außer bei Missbrauch, kostenlos. Für Verbandsklagen stellt die Aufsichtsbehörde Beschwerdeformulare zur Verfügung. Der Europäische Datenschutzausschuss (EDSA; Art. 64 ff), bei dem die Aufsichtsbehörden mitwirken, wird die Nachfolge der „Art.-29-Gruppe" sein. Zu den Befugnissen der Aufsichtsbehörde (Art. 53) zählt, die Berichtigung, Löschung oder Vernichtung von Daten anzuordnen und eine Verarbeitung vorübergehend oder endgültig zu verbieten. Eine generelle Meldepflicht (wie derzeit an das DVR) ist nicht vorgesehen, sondern eine „vorherige Genehmigung" bzw. „vorherige Zuratezieh-ung" der Aufsichtsbehörde durch den Auftraggeber im Zuge der Datenschutz-Folgenabschätzung (Art. 33 ff). Die Aufsichtsbehörde kann den Zugriff auf alle personenbezogenen Daten verlangen. Ihr ist der Zugang zu den Geschäftsräumen und Datenverarbeitungsanlagen zu gestatten. Sie kann Klage vor Gericht erheben und Verwaltungsstrafen verhängen.

In manchen Fällen, etwa auch bei der erwähnten Datenverarbeitung ohne vorherige Genehmigung oder ohne Zurateziehung der Aufsichtsbehörde, können diese Strafen (Geldbußen) bis zu 1 Million Euro oder im Fall eines Unternehmens bis zur Höhe von zwei Prozent seines weltweiten Jahresumsatzes betragen (Art. 79 Z 6). Lediglich bei natürlichen Personen oder KMUs (Unternehmen mit weniger als 250 Beschäftigten) kann bei einem ersten, unabsichtlichen Verstoß anstelle einer Sanktion eine schriftliche Verwarnung erfolgen (Art. 79 Z 3).

Die Verordnung soll nach ihrem Art. 91 zwei Jahre nach ihrer Veröffentlichung im Amtsblatt der EU anzuwenden sein. Geht man davon aus, dass sie bis Ende 2012/Anfang 2013 den Europäischen Rat und das Europäische Parlament passiert haben wird, wird sie somit wohl frühestens Anfang 2015 das DSG 2000 ersetzen.

Social Media. Wie es um die praktische Durchsetzung des europäischen Datenschutzes bestellt ist, schilderte Max Schrems am Beispiel seiner bei der irischen Datenschutzbehörde als Verfahren anhängigen Auseinandersetzungen mit *Facebook (http://europe-v-facebook.org)*. Durch eine Niederlassung in Irland (Facebook Ireland Ltd.) ist das Datenschutzrecht der EU für *Facebook* anwendbar geworden. Schrems kritisiert die mangelnde Transparenz über die von *Facebook* gesammelten Daten, über die nach seinen Erfahrungen nicht oder nur zögerlich Auskunft gegeben wird. Die letztlich über seine Daten erhaltene Auskunft umfasste 1.222 Seiten mit 57 Datenkategorien, wobei er es als fraglich bezeichnet, inwieweit im Einzelfall die geforderte „informierte Zustimmung" für die Speicherung sowie für die Weiterleitung vorgelegen hat. Immerhin wird eine Zustimmung zur Weitergabe von Daten bereits dann angenommen, wenn sie durch Dritte („Freunde") erfolgt.

Daten werden laut Schrems nicht physisch gelöscht, sondern nur als gelöscht markiert, bleiben also bestehen, und es würden auch Geo-Daten ermittelt und gespeichert, etwa durch die Auswertung der Daten von Bildern.

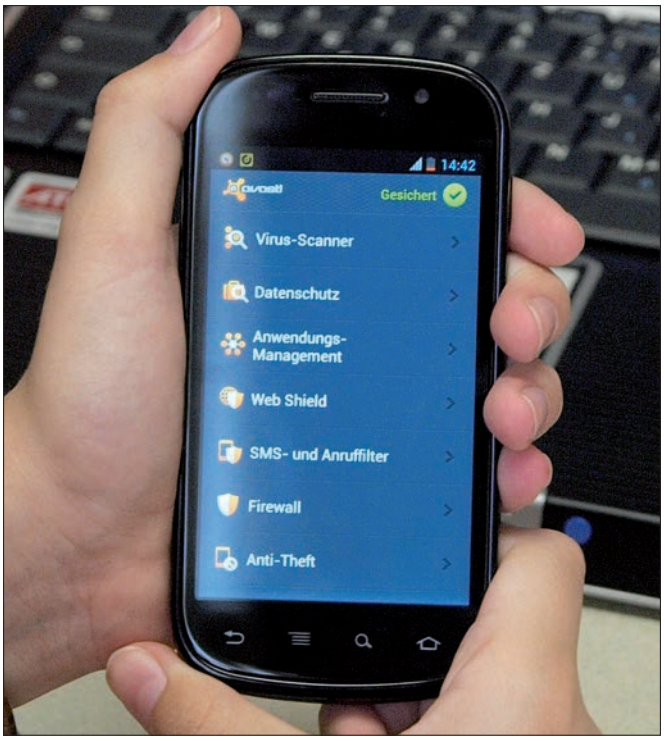
Die bei jedem Aufruf, auch bloß beim Laden des „Like"-Buttons, von *Facebook* gesammelten Daten ergeben, so Schrems, Schattenprofile, die nach den verschiedensten Suchkriterien ausgewertet werden können. Der Zweck liegt darin, Werbung gezielter einsetzen zu können. Die kostenlose Nut-

zung von sozialen Netzen wird mit den preisgegebenen persönlichen Daten bezahlt.

Eine Technik, die individuelle, auf den Nutzer abgestimmte Werbung ermöglicht, ist das Online-Targeting, über das Rechtsanwalt Mag. Michael M. Pachinger berichtete. Im Besonderen geht es um die Auswertung von Cookies, die auf dem Rechner des Nutzers hinterlassen werden (§ 96 Abs 3 TKG idF BGBl I 2011/102).

Verbraucherschutz. Bereits in Kraft getreten ist die bis 13. Dezember 2013 in nationales Recht umzusetzende neue Verbraucherrechte-RL der EU vom 25. Oktober 2011, RL 2011/83/EU, über die Rechtsanwalt Dr. Axel Anderl berichtete. Ziel der Richtlinie ist es, alle Verbraucherschutz-Richtlinien der EU zusammenzufassen und eine Vollharmonisierung innerhalb der EU zu erreichen. Ferner soll ein echter Binnenmarkt im Fernabsatz geschaffen und das im Versandhandel brachliegende grenzüberschreitende Potenzial ausgeschöpft werden (Erwägungsgründe 4 und 5) sowie größerer Rechtsschutz mit vorhersehbaren Kosten/Risiken für Unternehmer geschaffen werden.

Die Rechtslage gilt für alle Verträge zwischen Unternehmern und Verbrauchern (B2C), bezieht sich in diesem Rahmen aber auch ausdrücklich auf Vertragsabschlüsse im Fernabsatz und außerhalb von Geschäftsräumen („Haustürgeschäfte"). Die Regelungen über den Fernabsatz sind weitgehend unverändert geblieben. Dieser ist definiert (Art. 2 Z 7) durch ein organisiertes Vertriebssystem ohne gleichzeitige körperliche Anwesenheit der Vertragspartner. Eine öffentliche Versteigerung stellt auf die Möglichkeit persönlicher Anwesenheit ab



Mobiles Payment: Bezahlen mit dem Handy.

(Art. 2 Z 13; ErwG 23); somit sind reine Internetauktionen keine öffentlichen Versteigerungen und es gelten die Regelungen über den Fernabsatz, insbesondere hinsichtlich des Rücktrittsrechtes. E-Mails werden als dauerhafte Datenträger angesehen (Art. 2 Z 10; ErwG 23).

Es werden Pflichten zu einer Information vor Vertragsabschluss und Bestätigungspflichten festgelegt, die spätestens zum Zeitpunkt der Lieferung oder vor Ausführung der Dienstleistung zu erfüllen sind. Der Schwerpunkt liegt auf der Belehrung über das Widerrufsrecht (Art. 10). Ein Verstoß gegen diese Belehrung verlängert das Widerrufsrecht um zwölf Monate. Der Bestellbutton muss auf die Zahlungspflicht hinweisen (Art. 8 Abs. 2). Erfolgt das nicht, ist der Verbraucher nicht gebunden. Dadurch sollen „Abzock-Seiten" verhindert werden.

Die Frist zur Ausübung des Rücktrittsrechts beträgt 14 Tage ab Erhalt der Ware durch den Verbraucher. Entscheidend ist der Zeitpunkt der Absendung. Die Rücktrittserklärung kann formfrei erfolgen (Art. 11), also auch telefonisch, mündlich oder durch Rücksenden mit entsprechender Erklärung. Der Unternehmer kann ein Muster-Formular für einen Widerruf beifügen. Bei Verwendung eines elektronischen Formulars ist das verpflichtend.

Die Rücksendung der Ware hat spätestens 14 Tage nach Abgabe der Rücktrittserklärung zu erfolgen. Der Verbraucher hat generell die Rücksendekosten zu tragen (bisher, wenn dies vereinbart wurde), außer der Verkäufer würde nicht auf die Kosten hinweisen oder sich zur Kostentragung verpflichten. Bei Rücktritt sind sämtliche Zahlungen rückabzuwickeln (Art. 13 und 14). Ausnahmen vom Rücktrittsrecht (Art. 16) bestehen unter anderem für aus Gesundheits- oder Hygienegründen nicht zur Rücksendung geeignete, versiegelt gelieferte Waren, digitalen Inhalt oder für bei öffentlichen Versteigerungen erworbene Waren.

Die Gefahrtragung geht erst dann auf den Verbraucher über, wenn er die Ware erhalten hat (Art. 20). Die Gefahr des Versandes geht somit, anders als nach § 429 ABGB, jedenfalls zu Lasten des Verkäufers, es sei denn, dass der Verbraucher einen anderen Beförderer als den vom Verkäufer vorgesehenen bestimmt hätte.

Mobile Payment. Smartphones können mit der Smartphones können mit der Technik der „Near Field Communication" (NFC), die zum Austausch von Daten über kurze Strecken (bis etwa 4 cm Entfernung) entwickelt wurde, auch zu Bezahlvorgängen eingesetzt werden, die noch schneller ablaufen als andere Zahlungsformen. Rechnet man für die Bezahlung mit Kreditkarte (Beleg und Unterschrift) 57 Sekunden, für Bargeldbezahlung 29 Sekunden, für die Bankomatkarte (Eingabe des Codes) 25 Sekunden, sind es bei Nutzung der NFC nur mehr 0,5 Sekunden.

Erfolgen die Zahlungen über den IT-Provider als zwischengeschaltete Stelle, fällt dies, wie Dr. Roland Marko ausführte, unter das Zahlungsdienstegesetz (ZaDiG; digitalisiertes Zahlungsgeschäft nach § 1 Abs. 2 Z 6). Für Zahlungen auf Guthabenbasis gilt das E-Geldgesetz 2010, BGBl I 2010/107. Zahlungen bis 30 Euro im Einzelfall oder bis zu einer Ausgabenobergrenze von 150 Euro (für Zahlungen im Inland 60 bzw. 300 Euro; bei E-Geld bis zu 400 Euro) fallen unter die Sonderbestimmungen für Kleinbetragszahlungen (Micropayments) nach § 33 ZaDiG. Für diese gelten erleichterte Informationspflichten. Der Zahler trägt das Missbrauchsrisiko. Bei Bestreitung der Autorisierung trifft ihn die Beweislast. *Kurt Hickisch*

FOTO: ADOLF ACHTSNIT