Bundesministerium
für Ernährung
und Landwirtschaft

Bamberger Verbraucherrechtstage 2013 – Mobile Commerce

„Bamberger Verbraucherrechtstage 2013 – Mobile Commerce“

Fachtagung des Bundesministeriums für Ernährung,
Landwirtschaft und Verbraucherschutz
in Kooperation mit dem Lehrstuhl für Deutsches und
Europäisches Verbraucherrecht und Privatrecht sowie
Rechtsvergleichung der Universität Bayreuth
sowie der Forschungsstelle für
Verbraucherrecht an der Universität Bayreuth

am 11. und 12. November 2013
in Bamberg

Inhaltsverzeichnis

Arbeitsgruppe 1 „Mobiler Datenschutz“

Geolokalisierung von mobilen Endgeräten wie Smartphones etc. bedeutet die Standort-/Ortsbestimmung eines Objektes mittels technischer Verfahren, wie z. B. GPS. Die zunehmende Nutzung von Mobilfunkgeräten und mobilen Computern führt dazu, dass IT-Unternehmen über riesige Datenmengen einer Vielzahl von Personen verfügen. Unternehmen haben an diesen Daten ein hohes Interesse, da den Kunden spezielle, auf den Ort bezogene Angebote gemacht werden können, d. h. Werbung für das nächstgelegene Restaurant oder Spezialgeschäft, Smartphone als mitwandernder Stadtplan zur eigenen Standortbestimmung, Informationen über Facebook-„Freunde“ im nächsten Café, GPS-Überwachungssystem für Kinder. Die Geolokalisierung von mobilen Endgeräten wirft insbesondere aus Sicht des Datenschutzes erhebliche Rechtsfragen auf. Die Arbeitsgruppe „Mobiler Datenschutz“ soll sich mit folgenden Themenschwerpunkten befassen:

- Fakten zur Geolokalisierung, u. a. Umfang, Information des Nutzers
- technische Grundlagen, u. a. Möglichkeiten, das Werbeangebote auszuschalten und Komplexität des Vorgangs
- rechtliche Aspekte, u. a. status quo und Notwendigkeit einer Gesetzesänderung

Im Rahmen dieser Diskussionsthemen sind zunächst die Fakten der Geolokalisierung von mobilen Endgeräten zu erläutern, bevor die Teilnehmer die technischen und rechtlichen Aspekte herausarbeiten. Insbesondere ist zu klären, bei welchen Geräten überhaupt eine Geolokalisierung möglich ist, aus welchen Gründen diese vorgenommen wird, welche speziellen Angebote den Nutzern auf der Basis der Geolokalisierung gemacht werden und welche Geschäftsmodelle es in Zukunft geben wird. Vor diesem Hintergrund ist die Situation des Nutzers zu evaluieren, d. h. insbesondere die Erkennbarkeit der Geolokalisierung. Sodann stellen sich Fragen zur technischen Seite. Dazu gehört vor allem, welche Möglichkeiten der Nutzer hat, via Geräteeinstellung Werbeangebote auszuschalten. Am Ende sollen die Teilnehmer erörtern, ob die angewendete Art und Weise der Geolokalisierung überhaupt den datenschutzrechtlichen Vorgaben entspricht. Dabei geht es vornehmlich um die Ausgestaltung der Einwilligung. Aufgrund des technischen Fortschrittes ist darüber hinaus zu klären, ob die gesetzlichen Vorschriften im Telekommunikations- und im Bundesdatenschutzgesetz für die Regelung der Geolokalisierung noch ausreichend sind.

1

Patrick von Braunmühl

Mobiler Datenschutz – Geschäftsmodelle der Zukunft

I. Einleitung

Der Trend zur vermehrten Nutzung mobiler Endgeräte mit Internetanbindung hält nach wie vor an. Gerade in Kombination mit den vielfältigen technischen Möglichkeiten zur Ermittlung der Position eines Gerätes (sog. Geolokalisierung) entstehen immer neue Geschäftsmodelle, die darauf basieren, den Nutzern speziell auf deren Standort zugeschnittene Informationen zur Verfügung zu stellen (sog. Location Based Services). Wie bei Onlinedienstleistungen mittlerweile nicht unüblich wird auch hier zumeist auf klassische Bezahlmethoden verzichtet und die Finanzierung durch die Verwendung der Nutzerdaten zur Erstellung personalisierter Werbeangebote ermöglicht. Damit stehen die Dienste praktisch allen Nutzern solcher Endgeräte unabhängig von dem finanziellen Leistungsvermögen oder der -bereitschaft zur Verfügung. Insgesamt resultiert daraus ein großes Geschäftspotenzial, das jedoch durch Vertrauen auf Nutzerseite insbesondere in den Bereichen Datenschutz und Datensicherheit abgesichert werden muss. Denn nur so können langfristig die Vorteile der Nutzung überwiegen und die Dienste auf Akzeptanz stoßen. Nachfolgend soll der Blick auf aktuelle Entwicklungen sowie einige Hintergründe im Bereich der Location Based Services gerichtet werden.

II. Quellen der Geolokalisierung

Eine der meistgenutzten Methoden zur Positionsbestimmung von Geräten ist der Einsatz von satellitengestützten Technologien. Als bekanntestes Beispiel ist hier das Global Positioning System (GPS) zu nennen. Bei dieser Technologie senden Satelliten Radiosignale aus, um regelmäßig jeweils ihre Position und die Uhrzeit zu verbreiten. GPS-Empfänger auf der Erde sind dann in der Lage anhand der Laufzeiten von Signalen mehrerer Satelliten die eigene Position und ihre Geschwindigkeit zu ermitteln.[1] Während GPS ursprünglich der militärischen Nutzung vorbehalten war und in einer technisch präziseren Ausgestaltung nach wie vor ist,[2] sind seit der Freigabe für zivile Zwecke neben den klassischen reinen Navigationsgeräten inzwischen zahlreiche Endgeräte wie praktisch alle gängigen Smartphones und viele Tablet-Computer mit GPS-Empfängern ausgerüstet. Charakteristisch für die klassische satellitengestützte Positionsbestimmung ist, dass die signalverarbeitenden Geräte ausschließlich Signale empfangen und für die Ermittlung des genauen Standortes nicht als Sender fungieren müssen.[3] Daher ist eine externe Ortung der Geräte allein aufgrund des Einsatzes dieser Technologie ausgeschlossen. Da allerdings inzwischen eine Vielzahl an Geräten mit eingebauten GPS-Empfängern in der Lage ist, eine Internetverbindung aufzubauen, wird durch die Technologiekombination eine Weiterverbreitung der ermittelten Position an externe Stellen und damit auch eine Ortung anhand der GPS-Daten grundsätzlich ermöglicht.

Alle sonstigen, gängigen Methoden zur Positionsbestimmung unterschieden sich von GPS gerade in diesem letztgenannten Punkt, da sie technisch notwendig stets das Senden von Informationen von Geräteseite beinhalten. Es bedarf daher dabei keiner zusätzlichen technischen Voraussetzungen, damit eine externe Ortung der Geräte ermöglicht wird. Das trifft zunächst für die Lokalisierung etwa eines Mobiltelefons über die jeweils zur Kommunikation genutzten Funkzellen zu. Denn da die Standorte der Funkzellen und deren Funkreichweiten zumindest den Netzbetreibern bekannt sind, lassen sich daraus Rückschlüsse auf die ungefähre Position eines Gerätes im Funknetz ableiten.[4] Es handelt sich folglich um ein Tracking-System, bei dem zunächst nur der Provider die in seinem Netzwerk registrierten Geräte orten kann.[5] Die Geräte selbst können

---

1 S. ausf. dazu *Jandt/Schnabel*, K&R 2008, 723, 724; ausf. insgesamt zu der Technologie GPS: *Kaplan/Hegarty (Hrsg.)*, Understanding GPS – Principles and Applications, 2. Aufl. 2006; umfassend zu den technischen Spezifikationen: Department of Defense, GLOBAL POSITIONING SYSTEM STANDARD POSITIONING SERVICE PERFORMANCE STANDARD, 4. Aufl. 2008, abrufbar unter: http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

2 Department of Defense, GLOBAL POSITIONING SYSTEM STANDARD POSITIONING SERVICE PERFORMANCE STANDARD, 4. Aufl. 2008, S. 1, abrufbar unter: http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

3 *Kaplan/Hegarty (Hrsg.)*, Understanding GPS – Principles and Applications, 2. Aufl. 2006, S. 3.

4 Ausführlicher dazu *Jandt*, MMR 2007, 74.

5 *Schnabel*, Datenschutz bei profilbasierten Location Based Services, 2009, S. 269.

auf Basis dieser Technologie nur dann Kenntnis von der eigenen Position erhalten, wenn der Netzwerkbetreiber die Informationen zur Verfügung stellt und eine technische Möglichkeit – wie etwa eine Internetverbindung – vorhanden ist, die Positionsdaten auf das Endgerät zu übertragen.

Sobald ein mobiles Gerät eine Funkzelle für die Internetkommunikation nutzt, kann jedoch unabhängig von dem Netzbetreiber auch das Gerät selbst oder ein externer Dritter die Position anhand der – für die Internetkommunikation zwingend notwendigen – IP-Adresse feststellen. Ermöglicht wird dies durch den Umstand, dass IP-Adressen im Internet in Blöcken festen geografischen Positionen zugeordnet werden.[6] Dadurch ist stets ermittelbar, in welchem geografischen Block sich ein Gerät mit einer speziellen IP-Adresse im Netzwerk befindet. Diese sog. netzwerkbasierte Positionsbestimmung ist dementsprechend keineswegs auf Funknetze beschränkt, sondern vielmehr immer dann möglich, wenn die Internet-IP-Adresse eines Gerätes bekannt ist. Allerdings ist es durchaus möglich, die für die Kommunikation genutzte IP-Adresse eines Gerätes gegenüber einem Kommunikationspartner zu verbergen, indem die Daten über zwischengelagerte Netzwerke (etwa VPNs)[7] oder Proxy-Server umgeleitet werden. Hierbei bleibt es aber dabei, dass zumindest das Gerät selbst und die Stelle, die die Internetverbindung ermöglicht, die tatsächliche IP-Adresse des Gerätes kennen und eine Ortung für diese möglich bleibt. Ausgenommen von der Ortungsfähigkeit werden durch derartige Maßnahmen ausschließlich externe Kommunikationspartner, da ihnen nur die IP-Adressen der zwischengelagerten Systeme bekannt gegeben werden, die von ihnen die Daten anfordern und an die sie die Daten weiterleiten. Umgeleitete Zieladressen sind für sie nicht ohne weiteres erkennbar und dementsprechend allein auf Basis der Kommunikationsinformationen eine Ermittlung der korrekten aktuellen Position des Gerätes ausgeschlossen.

Für mobile Endgeräte wie die genannten Smartphones und zahlreiche der im Einsatz befindlichen Tablet-Computer bedeutet dies, dass eine Positionsbestimmung mittels mehrerer der standardmäßig verbauten Technologien sowohl für die Geräte selbst als auch für Dritte möglich ist. Ist das Gerät aus technischen Gründen gerade nicht in der Lage eine Lokalisierung anhand einer Methode vorzunehmen, verbleiben weitere Möglichkeiten. Zudem erlaubt die Kombination der Technologien eine Präzisierung der aktuellen Position bzw. einen Ausgleich der jeweiligen Nachteile einer einzelnen Technologie. So kann etwa zunächst eine weniger präzise aber schnelle Lokalisierung eines Gerätes über die Funkzelle oder die IP-Adresse erfolgen, während das Gerät noch auf die Signale von mehreren GPS-Satelliten wartet bzw. diese verarbeitet, um eine sehr genaue Positionsbestimmung vornehmen zu können. Die ungefähre Kenntnis von der aktuellen Position mittels anderer Technologien kann zudem für die Beschleunigung der Auswertung der GPS-Signale herangezogen werden (Assisted GPS). Gerade die Technologiekombination birgt jedoch das Risiko in sich, dass Maßnahmen zur Verbergung der Position gegenüber Dritten – etwa mittels der genannten Umleitung des Internetverkehrs – leerlaufen, da Dritte über mehrere Wege Kenntnis von der Position erlangen können.

III. Anwendungen und Geschäftsmodelle

Location Based Services kommen häufig bei klassischen Navigationsdiensten zum Einsatz. Hierbei wird entweder entsprechend einer angefragten Position aktuelles Kartenmaterial auf das Gerät übertragen oder bereits auf dem Gerät vorhandenes Kartenmaterial um aktuelle Informationen zu dem derzeitigen oder einem angefragten Standort ergänzt.[8] Die Geschäftsmodelle, die Zusatzinformationen zu reinem Kartenmaterial anbieten, sind inzwischen vielfältig. Zwar stehen nach wie vor insbesondere Informationen zu interessanten Orten wie Einkaufsmöglichkeiten, Museen, Restaurants oder Sehenswürdigkeiten in der Umgebung einer Position im Mittelpunkt,[9] der Ideenreichtum der Unternehmer bleibt aber keineswegs darauf beschränkt. So können etwa in Echtzeit Informationen über Stauentwicklungen und das Wetter auf einer Route,[10] über vorhandene Parkplätze am Ankunftsort[11] oder zu Interessenten für die Mitfahrt bei einer geplanten Wegstreckte[12] übermittelt werden. Neben der reinen Kenntnis von

6 Ausf. dazu *Kühn*, DuD 2009, 747, 748.
7 Abkürzung für Virtual Private Netzworks.
8 S. etwa als bekanntesten Vertreter dieser Dienste GoogleMaps: https://maps.google.com/.
9 S. etwa die Dienste des Unternehmens Tripadvisor: http://www.tripadvisor.de/.
10 S. etwa den Dienst HERE Traffic: http://here.com/traffic; sowie TOMTOM Live Services: http://www.tomtom.com/de_de/services/live/.
11 S. etwa die Live-Dienste der Firma GARMIN: http://sites.garmin.com/smartphonelink/.
12 S. etwa den Dienst flinc: https://flinc.org/.

Geschäften in der Umgebung können zudem direkt dazugehörige aktuelle Angebote eingesehen werden.[13] Die Verknüpfung von unterschiedlichen Gerätepositionen macht es zudem möglich, Dienstenutzern nicht nur Kenntnis über unbewegliche Objekte zu verschaffen, sondern auch über die Position anderer mobiler Geräte bzw. deren Nutzern. Dadurch wird beispielsweise der Informationsaustausch über die Standorte von Freunden oder Geschäftspartnern ermöglicht.[14] Aber auch Dating-Services setzen diese Funktionalitäten für die ortsabhängige Zusammenführung von Personen ein.[15] Car-Sharing-Anbieter bieten zudem ihren Kunden an, jederzeit die aktuellen Positionen der verfügbaren Fahrzeuge ihrer Flotte abzurufen und direkt dorthin zu navigieren.[16] Möglich ist ebenfalls, seinen Standort über spezielle Smartphone-Apps zu übermitteln, um direkt am Aufenthaltsort von einem Taxi abgeholt zu werden[17] oder Informationen zu den nächstgelegenen öffentlichen Verkehrsmitteln zu erhalten[18]. Darüber hinaus kann die eigene Position auch genutzt werden, um Fotos mit Daten anzureichern, die Auskunft über den Standort der Aufnahme liefern (sog. Geotagging). Neben den klassisch auf Gewinn ausgerichteten Geschäftsmodellen kommen Location Based Services aber auch etwa in den Bereichen der Grundrechteausübung sowie des Katastrophenschutzes bzw. der -bewältigung zum Einsatz. So wurde beispielsweise eine spezielle Software der Firma Ushahidi genutzt, um Protestversammlungen zu organisieren sowie bei Erdbeben, Überflutungen oder anderen Naturkatastrophen zu helfen, um Informationen über vermisste Personen und Schäden zu verbreiten.[19] Im Bereich der Altenpflege und bei Alzheimerkranken wird Geolokalisierung auch zur schellen Ortung von Patienten in Notfällen genutzt.

Neben Smartphones, Navigationsgeräten und Tablet-Computern zeichnet sich derzeit die Verbreitung einer weiteren Gerätekategorie an, die Location Based Services nutzt: Sogenannte „Wearables“. Hierbei handelt es sich um klassische Accessoires, die am Körper getragen werden, darüber hinaus aber Computerfunktionalitäten anbieten. Vergleichbar mit den Smartphones, also Telefonen mit integrierter Internetkonnektivität, sind nunmehr beispielsweise Uhren mit derartigen Erweiterungen unter der Bezeichnung Smartwatches auf dem Markt verfügbar.[20] Zudem testet die Firma Google unter dem Produktnamen „Google Glass“ seit einiger Zeit eine Computer-Brille.[21] Interessant ist in diesem Zusammenhang auch ein mit Elektronik ausgestatteter Babystrampler der Firma Intel, der über eine Datenverbindung die Eltern ständig über Schlafphasen, Atmung, Temperatur und auch Bewegungsmuster des Kindes informiert.[22] Auch wenn im Bereich des Wearable Computing die tatsächliche Entwicklung noch abzuwarten ist, zeigt sich doch ein Trend hin zu mehr mobilen Endgeräten mit Internetkonnektivität und immer umfassenderen Einsatzmöglichkeiten auch gerade im Bereich der Geolokalisierung.

IV. Chancen und Risiken

Anwendungen im Zusammenhang mit Location Based Services können Menschen erhebliche Erleichterungen in ihrem Alltag bieten. Sie bieten schnelle und zuverlässige Orientierung und erleichtern das Auffinden von speziellen Orten und Personen in der Umgebung oder Informationen zu der Umgebung selbst. Fahrten mit PKW oder Fahrrad sowie die Parkplatzsuche können effizienter gestaltet werden. Durch den schnellen Austausch von Aufenthaltsort und Reisezielen kann mittels „Car-Sharing“ das Verkehrsaufkommen reduziert werden. Insgesamt ist bei einer breiten Nutzung eine intelligente Verkehrssteuerung möglich. Neben der Verbesserung der Wirtschaftlichkeit resultieren aus der Optimierung des Ressourceneinsatzes mittelbar positive Effekte im Bereich des Klimaschutzes. An dem Beispiel Ushihadi wurden zudem die Vorteile solcher Dienste in Krisenfällen erkennbar.

Allerdings gehen – wie üblich – die Vorteile Hand in Hand mit neuen bzw. erhöhten Risiken. Vorwiegend spielen sich diese – wie bei zahlreichen neuen Techno-

13 S. etwa den Dienst KaufDA: http://www.kaufda.de/.
14 So etwa möglich über eine Funktion des sozialen Netzwerkes Google+: https://plus.google.com/.
15 S. etwa den Dienst MeetMoi: http://www.meetmoi.com/.
16 S. etwa das Angebot des Unternehmens DriveNow: https://de.drive-now.com.
17 S. etwa den Dienst mytaxi: https://www.mytaxi.com/home.html.
18 S. etwa den DB Navigator der Deutschen Bahn AG: http://www.bahn.de/p/view/buchung/mobil/db-navigator.shtml.
19 S. ausf. dazu: http://ushahidi.com/.
20 Beispiele sind die Smartwatches der Firmen Sony und Pebble sowie Samsungs Galaxy Gear.
21 S. http://www.google.com/glass/start/.
22 Waldt, Wearables: Intel SmartStrampler ist das Babyphone von heute, Engadget v. 7.01.2014, abrufbar unter: http://de.engadget.com/2014/01/07/wearables-intel-smartstrampler-ist-das-babyphone-von-heute/.

logien der automatisierten Datenverarbeitung – im Bereich der informationellen Selbstbestimmung ab. Die in jüngster Zeit bekannt gewordenen Vorgehensweisen der Geheimdienste und deren umfassenden Datensammlungen stellen dabei einen besonderen Missbrauchsfall dar, der praktisch alle automatisiert verarbeiteten Daten betrifft. Standortdaten sind hier keine Ausnahme. Diese umfassenden staatlichen Datensammlungen bergen die Gefahr, Bürger und Verbraucher zu verunsichern sowie Akzeptanz und Nutzung innovativer Dienste zu beeinträchtigen, soweit sie digitale Fußspuren erzeugen. Verbindliche internationale Abkommen zur Begrenzung der Ausspähungsaktivitäten der Geheimdienste wären ein wichtiger Schritt, um den Vertrauensverlust zu begrenzen. Gleichzeitig müssen auch Sorgen im Hinblick auf Datensammlungen der Unternehmen angemessen adressiert werden.

Gerade weil Location Based Services häufig auf klassische Bezahlmethoden verzichten und, wie inzwischen bei Internetdienstleistungen zunehmend der Fall, die Finanzierung über personalisierte Werbung erfolgt, kommt es zu einer Verarbeitung von personenbezogenen Daten der Nutzer, die teilweise auch die Erstellung von Bewegungsprofilen ermöglichen. Allerdings existieren auch Kontrollmöglichkeiten bzw. Gegenmaßnahmen auf Nutzerseite: Bezogen auf GPS bieten alle derzeit weit verbreiteten Betriebssysteme bei mobilen Endgeräten[23] Nutzern die Möglichkeit, die GPS-Ortung komplett – und teilweise sogar anwendungsbezogen –[24] zu deaktivieren und informieren stets mittels eines Symbols darüber, sobald das Gerät versucht über GPS seine Position zu bestimmen. So bleibt für die Nutzer trotz des vorhandenen Internet-Rückkanals immer die Wahl, ob überhaupt eine Ortung per GPS möglich sein soll und erkennbar, ob gerade eine Lokalisierung stattfindet, die ggf. an Dritte weiterübermittelt werden könnte. Zudem werden inzwischen spezielle Apps angeboten, die die GPS-Daten manipulieren können und damit falsche Positionsdaten erzeugen.[25] Für die Verfälschung der netzwerkbasierten Standortbestimmung durch Dritte anhand der IP-Adresse kann auf die dargestellte Möglichkeit der Umleitung der Internetkommunikation mittels VPN oder Proxy-Server zurückgegriffen werden.

Aber auch wenn Betriebssysteme mobiler Endgeräte die Deaktivierung der Positionsbestimmung per GPS oder anderer Methoden ermöglichen bzw. Techniken vorhanden sind, die Standortdaten zu manipulieren, bleibt es doch dabei, dass zumindest immer der Netzwerkprovider die Position eines in seinem Netzwerk registrierten Mobiltelefons ermitteln kann. Die Deaktivierung bzw. Verschleierung kann aber durchaus verhindern, dass Dritte für den Zeitraum der Deaktivierung Daten auf Basis dieser Methoden für ihre Bewegungsprofile erlangen. Das Mitführen mehrerer mobiler Endgeräte – wie etwa von Smartphones und den angesprochenen Wearables – erhöht jedoch die Wahrscheinlichkeit, dass zumindest immer ein von einem Nutzer mitgeführtes Gerät für externe Dritte lokalisierbar bleibt. Für viele Verbraucher sind die Funktionalitäten von Location Based Services gerade ein Grund zur Anschaffung mobiler Endgeräte. Daher werden sie an einer dauerhaften Deaktivierung der Geolokalisierung kaum interessiert sein. Für die Anbieter solcher Dienste und insbesondere für die Telekommunikationsanbieter gelten umfassende und strenge rechtliche Regelungen (s.u. VI.).

V. Nutzerverhalten

Das Nutzerverhalten ist spätestens seit der Entwicklung von personenbezogenen Daten zum Substitut für klassische Bezahlvorgänge eines der interessantesten aber auch widersprüchlichsten Themenfelder. Auf der einen Seite kommt es immer wieder zu lauten Aufschreien und Protesten seitens der Bevölkerung bzw. der Medien, wonach die informationelle Selbstbestimmung eines der bedeutendsten Rechte sei und geschützt werden müsse, gleichzeitig geben aber auffallend viele Personen bereitwillige ihre Daten etwa in sozialen Netzwerken preis und einschlägig ausgerichtete Internetdiensteanbieter veröffentlichen immer wieder neue Rekordbenutzerzahlen. Es zeichnet sich hier eine paradoxe Erwartungshaltung der Nutzer zwischen dem Wunsch ab, gewisse Dienste kostenlos nutzen zu wollen, gleichzeitig aber auch eine Finanzierung der Dienste über personalisierte Werbung auf Basis personenbezogener Daten abzulehnen. Für eine genauere Betrachtung des Nutzerverhaltens ist ein Blick in einige statistische Erhebungen angebracht.

Im Bereich des Nutzungsumfanges ist zunächst festzustellen, dass nach eigenen Angaben 33 Prozent der

23 Also Googles Android, Apples iOS und Microsofts Windows Phone.
24 So etwa möglich bei Apples iOS.
25 S. etwa die App für Googles Android Betriebssystem “My Fake Location”: https://play.google.com/store/apps/details?id=com.my.fake.location&hl=de.

Smartphone-Nutzer freiwillig ihren Standort mitteilen, um ortsbezogene Dienste zu nutzen.[26] Insgesamt setzen 21 Prozent die Lokalisierung ein, um Hinweise auf Geschäfte, Gaststätten oder Dienstleistungen in der Nähe zu erhalten.[27] 10 Prozent teilen ihren Standort mit, damit Freunde und Bekannte sehen können, wo sie sich aufhalten.[28] In der Gruppe der Vierzehn- bis Neunundzwanzigjährigen liegt dieser Anteil bei 18 Prozent.[29]

Konkret bezogen auf den Datenschutz und die Datensicherheit sind 54 Prozent der Smartphone-Nutzer bereit mehr für sichere Apps zu bezahlen.[30] Im Umkehrschluss bedeutet dies aber, dass das beschriebene Paradoxon zumindest für 46 Prozent der Nutzer bestätigt wird. Denn mangels einer höheren Zahlungsbereitschaft bei einem besseren Datenschutz sind die Unternehmen darauf angewiesen, ihre Finanzierung über alternative Methoden sicherzustellen. Personalisierte Werbung auf Basis von personenbezogenen Daten hat sich hier als die vorrangige Methode bei unentgeltlichen Diensten herausgebildet. Die andere Hälfte der Nutzer, also die Gruppe der Zahlungswilligen, stellt jedoch für Diensteanbieter durchaus eine kritische Masse dar, die für Geschäftsmodelle mit klassischen Finanzierungsmodellen durchaus attraktiv ist und mit speziell auf sie zugeschnittenen Angeboten adressiert werden kann.

Gleichzeitig zeichnet sich ein weiterer Widerspruch im Nutzerverhalten ab: Zwar sprechen sich 92 Prozent aller Smartphone-Nutzer für Datenschutzkontrollen durch die Betreiber von App Stores aus und 70 Prozent erachten Datensicherheit und Datenschutz bei Apps als mindestens wichtig.[31] Jedoch informieren sich dann nur 54 Prozent vor der Installation einer App auf ihrem Smartphone überhaupt über Risiken in den Bereichen Datenschutz und Datensicherheit und 51 Prozent sind sogar trotz Datenschutzbedenken bei beliebten Apps wie Facebook oder WhatsApp nicht bereit, auf die Nutzung zu verzichten.[32] Auch wenn der Wert von etwa der Hälfte sich informierender Nutzer durchaus beachtlich ist, steht doch insgesamt dem durchaus vorhandenen, ausgeprägten Sicherheitsbewusstsein in der Bevölkerung ein Verhalten zumindest von 46 Prozent der Nutzer gegenüber, die selbst nicht bereit sind Maßnahmen zum Schutz ihrer Daten zu ergreifen bzw. die Sicherheitsbedenken bei nützlichen Diensten zurückstellen.[33]

VI. Datenschutzrecht

Die datenschutzrechtlichen Fragen im Bereich der Location Based Services sind umfangreich und bereits Gegenstand zahlreicher Publikationen.[34] Die nachfolgende Betrachtung soll daher lediglich einen kurzen Überblick über die rechtlichen Grundlagen und wesentlichen Voraussetzungen liefern.

Zunächst ist für die Eröffnung des Anwendungsbereiches des Datenschutzrechtes zwingend erforderlich, dass es sich bei den Positionsinformationen um personenbezogene Daten i.S.d. § 3 Abs. 1 BDSG handelt. Mithin um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Grundsätzlich muss hier zwischen den Quellen der Geoinformationen unterschieden werden. Bezogen auf Standortdaten, die ein Telekommunikationsanbieter ermittelt, liegt aufgrund der auf Seiten des Anbieters vorhanden Zusatzinformationen wie der Rufnummer und den Vertragsdaten immer auch ein Personenbezug vor.[35] Bei anderen Lokalisierungsverfahren ist entscheidend, ob überhaupt Zusatzinforma-

---

26 Ergebnisse einer repräsentativen Umfrage im Auftrag von BITKOM e.V., Aug. 2013, abrufbar unter: http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Location_Based_Services_23_08_2013.pdf.

27 Ergebnisse einer repräsentativen Umfrage im Auftrag von BITKOM e.V., Aug. 2013, abrufbar unter: http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Location_Based_Services_23_08_2013.pdf.

28 Ergebnisse einer repräsentativen Umfrage im Auftrag von BITKOM e.V., Aug. 2013, abrufbar unter: http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Location_Based_Services_23_08_2013.pdf.

29 Ergebnisse einer repräsentativen Umfrage im Auftrag von BITKOM e.V., Aug. 2013, abrufbar unter: http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Location_Based_Services_23_08_2013.pdf.

30 Umfrage durchgeführt von mediaTest digital & testhub, Juli 2013, S. 20, abrufbar unter: http://mediatest-digital.com/wp-content/uploads/2013/08/mTd-testhub-Sicherheitsbewusstsein-Apps-13-07-31.pdf.

31 Umfrage durchgeführt von mediaTest digital & testhub, Juli 2013, S. 7, 21, abrufbar unter: http://mediatest-digital.com/wp-content/uploads/2013/08/mTd-testhub-Sicherheitsbewusstsein-Apps-13-07-31.pdf.

32 Umfrage durchgeführt von mediaTest digital & testhub, Juli 2013, S. 9 f., abrufbar unter: http://mediatest-digital.com/wp-content/uploads/2013/08/mTd-testhub-Sicherheitsbewusstsein-Apps-13-07-31.pdf.

33 So im Ergebnis auch: Umfrage durchgeführt von mediaTest digital & testhub, Juli 2013, S. 3, 22, abrufbar unter: http://mediatest-digital.com/wp-content/uploads/2013/08/mTd-testhub-Sicherheitsbewusstsein-Apps-13-07-31.pdf.

34 S. etwa *Weichert*, DuD 2007, 17; *Schnabel*, Datenschutz bei profilbasierten Location Based Services, 2009; *Jandt/Schnabel*, K&R 2008, 723; *Hellmich*, MMR 2002, 152; *Jandt*, MMR 2007, 74; *Steidle*, MMR 2009, 167; *Kühn*, DuD 2009, 747.

35 So auch und ausf. *Jandt/Schnabel*, K&R 2008, 723, 724.

tionen existieren, die eine Identifizierung des einzelnen Nutzers ermöglichen, und wer über diese Informationen verfügt. Bei Location Based Services wird aber in aller Regel der Anbieter selbst über solches Zusatzwissen verfügen, weswegen auch hier in den allermeisten Fällen von personenbezogenen Daten auszugehen ist und der Anwendungsbereich des Datenschutzrechts eröffnet ist.[36]

Liegen personenbezogene Daten vor, ist deren Verarbeitung durch Dritte grundsätzlich verboten, es sei denn, es liegt eine Einwilligung vor oder ein anderer gesetzlicher Erlaubnistatbestand ist erfüllt.[37] Den Telekommunikationsanbietern ist es nach § 98 TKG zunächst ausschließlich gestattet Standortdaten nach der Einwilligung der Teilnehmer für die Bereitstellung von Diensten mit Zusatznutzen anonymisiert zu verarbeiten. Die reine Nutzung der Positionsdaten durch den Anbieter eines ortsbezogenen Dienstes zur Erbringung seines Angebotes ist grundsätzlich über den Erlaubnistatbestand des § 15 Abs. 1 TMG gestattet. Für die Erbringung der Dienstleistung ist es jedoch nicht erforderlich, Profile der Nutzer zu erstellen, damit ihnen personalisierte Werbung angeboten werden kann. Für diese Fälle ist § 15 Abs. 3 TMG zu beachten, der eine Profilerstellung ausschließlich auf Basis der Nutzerdaten zu Werbezwecken in pseudonymisierter Form[38] gestattet. Umfassende Profile über Nutzer, bei denen eine Zusammenführung mit anderen Daten als den Nutzungsdaten erfolgt, sind jedoch danach unzulässig.[39] In diesen Fällen und denen der Weitergabe der Daten an Dritte sowie der Verwendung für andere Zwecke als die Werbung, die Marktforschung oder zur bedarfsgerechten Gestaltung der Dienste ist eine Einwilligung der Betroffenen erforderlich.[40] In jedem Fall muss aber der Diensteanbieter die Betroffenen ausführlich über die Verwendung der Daten unterrichten, § 13 Abs. 1 TMG.[41]

Dementsprechend ist in jedem Fall gegenüber dem Telekommunikationsanbieter und in einigen Fällen auch gegenüber den Anbietern von ortsbezogenen Diensten eine Einwilligung der Nutzer bei der Verarbeitung von Standortdaten erforderlich. Während dies im Rahmen des Vertragsschlusses eines Teilnehmers mit dem Telekommunikationsanbieter noch in rechtskonformer Weise ohne weiteres möglich ist, wirft die zweite Konstellation in der Praxis erhebliche Probleme auf. Denn nach § 4a Abs. 1 S. 2 BDSG sind die Betroffenen für eine datenschutzkonforme Einwilligung auf den vorgesehen Zweck der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten hinzuweisen. Ein Betroffener muss wissen, was genau mit welchen seiner Daten geschehen soll.[42] Der in der Praxis zumeist anzutreffende Hinweis bei der Installation einer Smartphone-App, dass Standortdaten bei der Nutzung eines Dienstes erhoben und verarbeitet werden, ist dafür keinesfalls ausreichend, da für die Betroffenen nicht erkennbar ist, wie umfassend die Profilbildung ist. Vielmehr ist eine umfassendere Aufklärung der Betroffenen erforderlich. Das gilt ebenfalls für Konstellationen des § 15 Abs. 3 TMG, bei denen zwar keine Einwilligung-, aber doch eine Unterrichtungspflicht besteht. Auch hier ist der reine Hinweis auf die Erhebung von Standortdaten unzureichend. Das gilt insbesondere für Angebote, die für die Erbringung keine Standortdaten der Nutzer benötigen und diese ausschließlich zur Profilerstellung erheben und verarbeiten. Hier ist in jedem Fall eine Einwilligung der Betroffenen erforderlich. Bekannt geworden ist in diesem Zusammenhang ein Fall, bei der eine Taschenlampen-App angeboten wurde, die ohne vorab darauf hinzuweisen auf den Aufenthaltsort der Nutzer zugegriffen hat.[43]

Allerdings muss auch festgehalten werden, dass das Lesen umfassender und detaillierter rechtlicher Texte

---

36 So auch *Jandt/Schnabel*, K&R 2008, 723, 724; auf den Streit, ob es ausreichend ist, dass irgendeine Stelle über das Zusatzwissen verfügt oder gerade die datenverarbeitende Stelle dieses Wissen haben muss, soll an dieser Stelle nur verwiesen werden. S. ausführlicher zu den unterschiedlichen Auffassungen mit weiteren Nachw.: *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 3 Rn. 10.

37 *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 4 Rn. 3.

38 Zum datenschutzrechtlichen Begriff der Pseudonymisierung s. *Dix/Schaar*, in: Roßnagel, TMG, 2013, § 15 Rn. 65: „Das Pseudonym ersetzt Einzelangaben, die den Betroffenen direkt identifizieren (z. B. seinen Namen, seine Konto oder Personalnummer) durch eine andere Angabe, so dass die gespeicherten Einzelangaben ohne Kenntnis der Zuordnungsregel nicht oder nur mit unverhältnismäßig großen Aufwand einer natürlichen Person zugeordnet werden kann.“

39 S. ausf. *Dix/Schaar*, in: Roßnagel, TMG, 2013, § 15 Rn. 61 ff.

40 S. ausf. *Dix/Schaar*, in: Roßnagel, TMG, 2013, § 15 Rn. 63 ff.

41 Ausf. dazu *Dix/Schaar*, in: Roßnagel, TMG, 2013, § 15 Rn. 69.

42 S. ausf. *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 4a Rn. 25 f.

43 Heise-online v. 06.12.2013, abrufbar unter: http://heise.de/-2062105.

auf relativ kleinen Smartphone-Bildschirmen kaum praktikabel ist. Dadurch wird der Umstand gefördert, dass Einwilligungen ohne tatsächliche Kenntnisnahme der aufklärenden Informationen erteilt bzw. Unterrichtungen der Anbieter über die Datenverwendung meist nicht gelesen werden. Daher sind rechtsvereinheitlichende Initiativen auf europäischer Ebene zu begrüßen, die diesbezüglich eine Beschränkung auf die wesentlichen Informationen in knapper Form (ggf. in Piktogrammen) und die Möglichkeit des Nachlesens an anderer Stelle anstreben. Für einen Verbesserungsbedarf in diesem Bereich spricht auch der Umstand, dass sich derzeit zwar 66 Prozent der Smartphone-Nutzer über die Berechtigungen einer App informieren, aber nur 21 Prozent davon angeben sich anschließend informiert zu fühlen.[44]

Die hier dargestellte rechtliche Bewertung gilt allerdings ausdrücklich nur für Fälle, in denen deutsches bzw. europäisches Datenschutzrecht tatsächlich anwendbar ist. Das ist grundsätzlich der Fall, wenn die relevanten Daten innerhalb Deutschlands bzw. anderen Staaten der EU oder des EWR erhoben oder verarbeitet werden. Viele Anbieter bieten jedoch ihre Dienste von außerhalb der EU an und verarbeiten die Daten auch dort, weswegen stets eine Einzelfallbetrachtung erforderlich ist, ob personenbezogene Daten tatsächlich innerhalb des europäischen Rechtsraumes erhoben werden.

VII. Ausblick

Aus der Darstellung wird erkennbar, dass die datenschutzrechtlichen Defizite nicht im Bereich des strengen materiellen Rechts liegen, sondern vielmehr in der Rechtsdurchsetzung. Zudem zeigen die Statistiken zum Nutzerverhalten, dass zwar durchaus ein Bewusstsein für Datenschutz und Datensicherheit vorhanden ist, aber individuell mögliche Schutzmaßnahmen oft unterbleiben. Im Interesse von Nutzern und Unternehmen wäre eine Vereinheitlichung und Modernisierung der datenschutzrechtlichen Regelungen auf europäischer Ebene durch die seit zwei Jahren diskutierte Datenschutz-Grundverordnung dringend erforderlich, um eine weitere Rechtszersplitterung zu vermeiden und die Rechtssicherheit zu verbessern.

Gleichzeitig wird an den zahlreichen neuen Entwicklungen erkennbar, wie kurz inzwischen die Innovationszyklen digitaler und global verbreiteter Geschäftsmodelle geworden sind. Klassische Regulierung stößt auf Basis nationaler Gesetze hier an seine Grenze. Erkennbar wird das etwa an der schwierigen rechtskonformen Ausgestaltung auf den relativ kleinen Smartphone-Displays, die sich in noch verstärkter Form bei den stark im Aufwärtstrend befindenden Wearables fortsetzen wird. Daher sollte zur Verbesserung des Schutzniveaus auch auf alternative Regulierungsinstrumente gesetzt werden, die schnell und flexibel anpassungsfähig sind und Vertrauen gegenüber den Diensten aufbauen können. Sinnvoll wäre ein komplementärer Ansatz zwischen gesetzlichem Rahmen und Konkretisierung durch regulierte Selbstregulierung zum Beispiel in Form von Verhaltenskodizes. Wichtig ist dabei, Mindestanforderungen der regulierten Selbstregulierung vorab zu definieren und seitens des Gesetzgebers Anreize zu schaffen, damit Unternehmen mehr Eigenverantwortung übernehmen. Als Bestandteil dieser Maßnahmen können dann etwa – idealerweise staatlich anerkannte – Gütesiegel eingesetzt werden, um auf dem Markt das vorhandene Sicherheitsbewusstsein der Bevölkerung zur Verbreitung von Angeboten mit entsprechend hohem Schutzniveau zu nutzen. So ist es möglich Akzeptanz auf Nutzerseite zu erzeugen und dauerhaft die Potenziale der Nutzung von Location Based Services auszuschöpfen.

---

[44] Umfrage durchgeführt von mediaTest digital & testhub, Juli 2013, S. 16, abrufbar unter: http://mediatest-digital.com/wp-content/uploads/2013/08/mTd-testhub-Sicherheitsbewusstsein-Apps-13-07-31.pdf.

Prof. Dr. Gerald Spindler

Mobiler Datenschutz – Geolokalisierung und Datenschutz

I. Einleitung

Die Verbreitung von mobilen Endgeräten nimmt stetig zu, Smartphones und Tablet Computer laufen offensichtlich den traditionellen Verbraucherendgeräten wie PCs den Rang ab. Damit verdrängen oder zumindest ergänzen mobile Applikationen auch die gewohnten Internet-Webseiten, Apps werden zum Standard für fast jeden Anbieter im Netz. Aber auch neue Kombinationen aus der Verwendung der Standortdaten eines Nutzers mit entsprechenden Informationen und Kaufangeboten verbreiten sich immer mehr, sei es einen Freund in der Nähe zu finden, eine Pizza zu bestellen, ein Hotelzimmer zu buchen, einen Mietwagen zu suchen oder Konzerte zu finden. Nicht nur Anwendungen im Bereich des Vertriebs („commerce“) sind hier relevant, sondern auch Kommunikationsbeziehungen, Unterhaltungsangebote bis hin zum Einsatz im Rahmen von Arbeitsbeziehungen bei mobilen Diensten. Die Beispiele ließen sich beliebig verlängern. Die Verwendung von Standortdaten kann aber nicht nur für lokale Informationen und Angebote verwendet werden, sondern auch um Bewegungsprofile für eine bestimmte Person herzustellen, also quasi dynamische zeitlich-geographische Präferenzen erkennen lassen.

Die für den Datenschutz damit verknüpften Probleme liegen auf der Hand: Die Dauer des Verweilens an bestimmten Orten, die Häufigkeit von Besuchen bestimmter Häuser, Plätze etc. lassen den Nutzer gläsern werden, erst recht, wenn mit dem Standort bestimmte über das Netz ausgelöste Handlungen wie Einkäufe etc. verbunden sind.

Der typische Ablauf einer solchen Profilerkennung und Nutzung von Standortdaten lässt sich kurz wie folgt skizzieren: Mit Hilfe einer Sender-, teilweise auch Geräteerkennung wie früher bei Apple üblich unter dem sog. Apple Unique Device Identifier oder bei Android-Systemen mit der DeviceID kann der Besitzer eines mobilen Endgerätes identifiziert werden. Seine Standortdaten werden mit Hilfe von Funkzellenortung und -zuordnung sowie WLANs oder auch GPS-Daten (die die meisten Smartphones und mobilen Endgeräte inzwischen unterstützen) ermittelt, dann verknüpft mit weiteren Daten, etwa der Verweildauer oder der über das Netz vorgenommenen Aktivitäten. Derartig lassen sich die unterschiedlichsten Daten verarbeiten und zusammenführen sowie rückkoppeln, um für die jeweiligen Zwecke Profile der Nutzer zu erstellen.

Die rechtliche Behandlung wird dadurch erschwert, dass die jeweiligen Daten keineswegs nur durch einen Anbieter erhoben und (weiter)verarbeitet werden, sondern durch eine Vielzahl von Anbietern, angefangen von Netzwerkbetreibern über App-Anbieter bzw. hin zu den „hinter“ einer Applikation stehenden eigentlichen Shop- bzw. Dienstbetreibern. Wie Weichert zu Recht hervorhebt,[1] bestehen die Besonderheiten des Mobile Computing neben den Verknüpfungen mit Standortdaten in der häufigen Einschaltung von Cloud-Diensten (die hier aus Raumgründen nicht behandelt werden können)[2] sowie der Verbindung mit einem bestimmten Geräten.

II. Rechtsgrundlagen und Reformbedarf

A. Anwendbare Gesetze

Eigene Gesetze, die sich mit Standortdaten befassen würden, existieren bis auf wenige spezielle Ausnahmen nicht.[3] Daher muss der Blick zunächst auf die allgemeinen datenschutzrechtlichen Regelungen gerichtet werden:

Nähert man sich der datenschutzrechtlichen Behandlung de lege lata, wird man sowohl auf europäischer wie auch auf deutscher Ebene mit einer regelrechten Zersplitterung des Datenschutzes konfrontiert: Da bei mobilen Endgeräten notwendigerweise Telekommunikationsdaten als Verkehrsdaten anfallen und auch ver-

---

1 S. auch *Weichert* in diesem Band.

2 Zu datenschutzrechtlichen Fragestellungen bei Cloud-Computing s. *Giedke*, Cloud Computing, Diss. Jur. (München), 2013, S. 190 ff. mwNachw.

3 So das Geodatenzugangsgesetz (GeoZG) für Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischem Gebiet, das jedoch keinen Personenbezug von Daten voraussetzt und auch nicht dem Datenschutz dient.

wendet werden, ebenso die Bestandsdaten im Sinne des Inhabers des jeweiligen Netzanschlusses, kommen zunächst die Regelungen des TKG in Betracht. Allerdings fällt dies nicht notwendigerweise mit dem jeweiligen Telekommunikationsprovider z.B. eines Smartphone-Besitzers zusammen, da sich dieser auch anderer Verbindungen vor Ort, insbesondere WLAN-Verbindungen bedienen kann, die wiederum von anderen Providern bereit gestellt werden – ohne dass sich indes etwas an der Eigenschaft als Telekommunikationsanbieter ändern würde. Die Verkehrsdaten können dabei Dauer und Ort der jeweiligen Verbindung umfassen; zusammen mit den Daten des Anschlussinhabers erfüllen sie damit die Voraussetzungen des Personenbezugs.

Neben dem Telekommunikationsgesetz sind ferner die datenschutzrechtlichen Regelungen des TMG (Telemediengesetz) einschlägig; denn die Angebote gerade von Apps (bzw. entsprechenden Diensten) sind oftmals als Telemedien zu qualifizieren, da sie nicht überwiegend in dem Angebot von Telekommunikationsdiensten bestehen, § 1 Abs. 1 TMG. Auch hier sind die von Apps erhobenen Daten Verkehrs-, aber auch Bestandsdaten, etwa wenn bestimmte Accounts eingerichtet werden müssen, um die Dienste zu nützen.

Last but not least greift auch das BDSG ein, wenn die Verarbeitung personenbezogener Daten „hinter” den Telemedien in Rede steht. Klassisches Beispiel hierfür ist das Online-Banking, für das hinsichtlich des Zugangs zum eigentlichen Online-Portal das TMG Anwendung findet, so dass die entsprechenden Verkehrsdaten von § 15 TMG erfasst werden; wenn es aber um die Erhebung und Verarbeitung der Daten im Rahmen des Bankvertrages geht, ist das BDSG in vollem Umfang anwendbar, etwa § 28 BDSG.

Dass drei verschiedene Gesetze für einen einheitlichen Vorgang, etwa des Mobile Banking und Mobile Payment einschlägig sein können, zeigt schon auf den ersten Blick die damit einhergehenden Abgrenzungsprobleme auf.[4] So können für die reinen Standort- und Verbindungsdaten andere Voraussetzungen im TKG als für deren Erhebung im TMG gelten. Umgekehrt sieht etwa § 13 Abs. 2 TMG grundsätzlich die elektronische Einwilligung vor, während § 4a Abs. 1 BDSG in der Regel die Schriftform verlangt.[5]

Umgekehrt sind die Anbieter von Diensten und Apps keine Telekommunikationdienstleister im Sinne von § 3 Nr. 24 TKG;[6] dennoch werden die Standortdaten an die jeweiligen Apps übermittelt, so dass hier auf beiden Seiten §§ 92 ff. TKG einschlägig sein kann.[7] Werden die Standortdaten nur durch die App selbst erhoben, soll mangels Telekommunikationsdiensteigenschaft § 92 TKG nicht einschlägig sein;[8] allerdings bestehen daran durchaus Zweifel, da durch die App selbst ohne die nötigen Daten der Netzanbieter (egal ob Telekommunikation im engeren Sinne oder WiFi-Dienste) kaum der Standort zu bestimmen sein wird.

Die Verarbeitung der Daten und ggf. weiterer Anmeldedaten richtet sich dann bei den App- bzw. Diensteanbietern wiederum nach §§ 13, 15 TMG. Hinsichtlich der Nutzungsdaten können diese nach § 15 TMG nur mit (elektronischer) Einwilligung oder bei Erforderlichkeit der Vertragserfüllung bzw. Diensteerbringung erhoben und verarbeitet werden, andernfalls bedarf es der Pseudonymisierung. Ein personenbezogenes Tracking etwa ist ohne Einwilligung nicht möglich.[9] Die Verarbeitung der Inhaltsdaten richtet sich nach § 13 TMG, der insbesondere deren Verarbeitung zur Erfüllung der Vertragspflichten parallel zu § 28 Abs. 1 S. 1 Nr. 1 BDSG erlaubt.[10]

---

4 Diese Abgrenzungsprobleme treten indes auch beim normalen E-Commerce auf, da die Verkehrs- bzw. Verbindungsdaten im Rahmen eines Internetzugangs ebenfalls dem TKG unterfallen. S. auch *Weichert* in diesem Band.

5 Dabei ist nicht zu verkennen, dass die hM inzwischen für Internetanwendung das Regel-Ausnahme-Verhältnis in ihr Gegenteil verkehrt hat, s. dazu *Spindler*, Verhandlungen des 69. Deutschen Juristentages 2012, Band I Gutachten, Teil F, S. F 79; *Simitis*, in: *Simitis* (Hrsg.) BDSG, 7. Aufl., 2011, § 4a Rn. 33 ff., 43 ff..

6 *Lober/Falker* K&R 2013, 357, 360.

7 Zum Verpflichteten von §§ 92 ff. TKG siehe Eckhart, in *Spindler/Schuster* (Hrsg.), Recht der elektronischen Medien, 2. Aufl., 2011, § 91 Rn. 7, § 88 Rn. 16.

8 So Art. 29 Datenschutzgruppe, WP 185 vom 16.5.2011, „Opinion 13/2011 on Geolocation services on smart mobile devices“, S. 7, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf; *Lober/Falker* K&R 2013, 357, 360.

9 *Lober/Falker* K&R 2013, 357, 361.

10 S. zum Ganzen *Spindler/Nink*, in *Spindler/Schuster* (Hrsg.), Recht der elektronischen Medien, 2. Aufl., 2011, § 12 TMG Rn. 4.

Verkompliziert wird die Rechtslage durch § 1 Abs. 1 TMG, wonach Telekommunikationsdienste, die gleichzeitig Mehrwertdienste enthalten, nur nach dem TKG behandelt werden.[11] Bei reinen Apps wird dies selten der Fall sein; wenn aber mitsamt des Telekommunikationsdienstes gleichzeitig ein inhaltlicher Dienst erbracht wird, kann durchaus allein das TKG zur Anwendung gelangen.

Vergleichbare Abgrenzungsprobleme ergeben sich aber auch auf europäischer Ebene: So findet auf den Datenschutz in Telekommunikationsbeziehungen die jeweilige TK-Richtlinie Anwendung, während etwa cookies durch die ePrivacy-Richtlinie geregelt werden, deren Verhältnis zur Datenschutz-Richtlinie von 1995 ebenfalls nicht vollständig geklärt ist.[12] Dem versucht der Vorschlag einer EU-Datenschutz-GrundVO abzuhelfen,[13] indem Inhaltsdaten und Verkehrs- bzw. Benutzungsdaten zusammengeführt werden; allerdings bleibt auch hier ein potentieller Konflikt zu den anderen Richtlinien wie der ePrivacy-RL, der kaum durch einen sybellinischen Vorbehalt, dass andere Richtlinien nicht berührt seien, gelöst werden kann.

B. Personenbezogene Daten

Voraussetzung für jede Anwendung datenschutzrechtlicher Vorgaben ist das Vorliegen personenbezogener Daten; gerade dieser Personenbezug kann aber über das Gerät bzw. den Identifier und die Verknüpfung mit dem Anschlussinhaber hergestellt werden, so dass oftmals selbst bei strengeren Vorgaben (relative Theorie) ein Personenbezug gegeben sein wird,[14] was selbst bei reinem WiFi-Empfang gelten kann, indem diese Daten zusammengeführt werden können.[15] Bei Standortdaten und Identitätsangaben über ein TK-Netz gilt dies von vornherein, da jedem Anschluss eine Person zugeordnet ist. Selbst die Apps, die unabhängig vom Geräte-Identifier Daten erheben, sind oftmals in der Lage, mit Hilfe vorher eingegebener Daten, wie z. B. Kreditkartendaten oder Accounts, den Personenbezug herzustellen.[16] Aber auch wenn kein Identifier mehr für Apps zugelassen wird, sondern stattdessen eine Art Cookie, kann der Personenbezug gegeben sein.[17]

C. Internationale Aspekte

Selbstverständlich muss auch in internationaler Hinsicht das deutsche Datenschutzrecht Anwendung finden, was gerade bei mobilen Endgeräten und oftmals international tätigen Diensteanbietern keineswegs eine Selbstverständlichkeit ist. Zunächst ist dabei hervorzuheben, dass für die speziellen Datenschutzregeln des TKG und des TMG die internationale Anwendbarkeit den Regeln des BDSG folgt (vgl. § 3 Abs. 3 Nr. 4 TMG), da beide Gesetze keine eigenen kollisionsrechtlichen Regelungen enthalten.[18] Somit kommen die Normen des grundsätzlich subsidiären BDSG zur Anwendung.[19] Demgemäß ist nicht etwa ein (modifiziertes) Marktort-

---

11 *Piepenbrock*, in Beck’scher TKG Kommentar, 4. Aufl., 2013, § 3 Rn. 51; *Säcker*, in *Säcker*, (Hrsg.), Berliner Kommentar zum TKG, 2. Aufl, 2009, § 3 Rn. 43; kritisch zu der Zuordnung *Roßnagel*, NVwZ 2007, 743, 745.

12 Sog. E-Privacy- Richtlinie: Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. Nr. L 201 v. 31.7.2002 S. 0037; bezüglich Cookies geändert durch Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz Text von Bedeutung für den EWR, ABl.. Nr. L 337 v. 18.12.2009 S. 11; EU-Datenschutzrichtlinie: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 v. 23.11.1995 S. 31.

13 Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), abrufbar unter: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf; Kompromissvorschlag des LIBE-Komitees zu diesem Vorschlag vom 22.10.2013, abrufbar unter http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf

14 *Weichert* in diesem Band (als Vertreter der absoluten Theorie); die relative Theorie bejahend: OLG Hamburg K&R 2011, 54; AG München K&R 2008, 767; *Spindler/Nink*, in: *Spindler/Schuster* (Hrsg.), Recht der elektronischen Medien, 2. Aufl., 2011, TMG § 11 Rn. 5 b; *Dammann* in: *Simitis* (Hrsg.) BDSG, 7. Aufl., 2011, § 3 Rn. 33, 35, 37; *Gola/Schomerus*, BDSG, 10. Aufl., 2010, § 3 Rn. 10; *Roßnagel/Scholz*, MMR 2000, 721, 722 f.

15 S. Art. 29 Datenschutzgruppe, WP 185 vom 16.5.2011, „Opinion 13/2011 on Geolocation services on smart mobile devices“ S. 10, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

16 Art. 29 Datenschutzgruppe WP 185 S. 9.

17 S. *Lober/Falker* K&R 2013, 357, 358 zur neuen Technik von Apple einen Identifier for Advertising zu verwenden.

18 *Klesczweski*, in: *Säcker*, (Hrsg.), Berliner Kommentar zum TKG, 2. Aufl, 2009, § 91 Rn. 15; *Jotzo*, MMR 2009, 232, 234;.

19 Vgl. *Braun*, in: Beck’scher TKG Kommentar, 4. Aufl., 2013, § 91 Rn. 7 f; Eckhart, in: *Spindler/Schuster*, (Hrsg.), Recht der elektronischen Medien, 2. Aufl., 2011, § 91 TKG Rn. 3.

prinzip entscheidend, wie es der neue Vorschlag der EU-Datenschutz-GrundVO in Art.3 Abs. 2 a) vorsieht,[20] sondern der Sitz der verantwortlichen Stelle, sofern es sich um einen Datenverarbeiter aus der EU handelt, § 1 Abs. 5 S. 1 BDSG. Handelt es sich dagegen um einen Anbieter außerhalb der EU, hängt es davon ab, ob die verantwortliche Stelle eine Niederlassung in der EU hat – dann ist die Rechtsordnung dieses Landes gem. Art. 4 Abs. 1 c) Datenschutz-RL anwendbar, auch wenn der Wortlaut des BDSG zunächst etwas anderes nahelegt. Dementsprechend hat auch das OVG Schleswig in den Verfahren des ULD Schleswig-Holstein gegen Facebook allein irisches Datenschutzrecht für anwendbar gehalten, da über die Niederlassung in Irland die Datenverarbeitungsprozesse zumindest zum Teil gesteuert würden.[21]

Hinsichtlich der Übertragung von Daten außerhalb der EU sind schließlich auch im Mobile Commerce die Regeln der § 4a ff. BDSG zu beachten, so dass im Grundsatz ein der EU vergleichbares Datenschutzniveau im Ausland erforderlich ist; Standardvertragsklauseln, Binding Corporate Rules oder die Anerkennung von „safe harbors“ durch die EU erleichtern allerdings den Datentransfer und die -verarbeitung.

D. Rechtfertigung der Verbindung von Standortdaten mit mobilen Diensten

Die Erhebung von Standortdaten, die personenbezogen sind, muss gerechtfertigt sein, was entweder bei ihrer Notwendigkeit zur Vertragserfüllung oder bei einer Einwilligung der Fall ist:

1. Rechtfertigungstatbestände

Wie bereits angeführt, kommen vor allem die Rechtfertigungstatbestände nach § 28 Abs. 1 S. 1 BDSG sowie § 15 Abs. 1 u. 3 TMG hinsichtlich der Leistungserbringung bzw. Vertragserfüllung zum Tragen. Eine Navigationssoftware ist ebenso wie ein Dienst, der lokale Angebote darstellen soll, notwendigerweise auf Standortdaten angewiesen – allerdings nicht unbedingt auf die Identität des Nutzers, außer wenn er ausdrücklich seine persönlichen Präferenzen im Hinblick z. B. auf lokale Angebote nutzen will.

Hinsichtlich der mit Telekommunikationsdienstleistungen verbundenen Erhebung von Standortdaten regelt § 98 TKG (in Umsetzung von Art. 9 EU-TK-DSRL) die Voraussetzungen, wobei wiederum auf die Erforderlichkeit der Diensteerbringung auch mit Zusatznutzen abgestellt wird; zusätzlich bedarf es der Einwilligung des Teilnehmers oder der Anonymisierung der Daten. Diese kann in Form einer generellen Einwilligung erteilt werden, erfordert aber eine spezifische Information des Einwilligenden (obwohl dies nicht ausdrücklich von § 98 TKG gefordert wird, es gelten aber die allgemeinen Voraussetzungen für die Erteilung einer Einwilligung). Diese generelle Einwilligung kann durch einen Rahmenvertrag erfolgen, um nicht vor jeder Nutzung des Dienstes eine erneute Einwilligung erforderlich zu machen.[22] Allerdings wird zu Recht darauf hingewiesen, dass GPS-Dienste nicht als Telekommunikationsdienste erfasst werden, mithin auch nicht die Verknüpfung von deren Standortdaten mit Apps. etc.[23]

2. Einwilligung

a) Grundlagen

Die Voraussetzungen für eine wirksame Einwilligung regeln § 4a BDSG und § 12 Abs. 2 TMG, indem Angaben über die verantwortliche Stelle, den erlaubten Zweck und über Art und Umfang der Daten enthalten sein müssen. Ferner muss die Einwilligung freiwillig sein. Formal gesehen muss die Einwilligungserklärung gesondert hervorgehoben sein; ob sie dagegen in AGBs enthalten sein kann, ist bislang ungeklärt – insbeson-

---

20 Art. 3 Abs. 2 des Kompromiss-Vorschlags zur Datenschutzgrundverordnung des LIBE-Komitees vom 22.10.2013, abrufbar unter http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf; diese Herangehensweise empfiehlt zumindest für Verarbeiter außerhalb der EU auch die Artikel-29-Datenschutzgruppe der EU: Artikel-29-Datenschutzgruppe, WP 179 vom 16.12.2010„Stellungnahme 8/2010 zum anwendbaren Recht“, S.31, abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf.

21 *OVG Schleswig*, NJW 2013, 1977 = K&R 2013, 523 m. zust. Anm. *Meyer*; dazu *Rössel*, ITRB 2013, 155; *Steinrötter*, MMR 2013, 691; ebenso Art. 29 Datenschutzgruppe, WP 179 vom 16.12.2010, „Stellungnahme 8/2010 zum anwendbaren Recht“, S. 11 f., 24 f.; dagegen die Anordnung des Unabhängigen Landeszentrum für Datenschutz vom 14.12.2012, Az.: LD4-61/41./12.002, B. a); abrufbar unter https://www.datenschutzzentrum.de/facebook/20121214-anordnung-fb-inc.html; dazu auch Kremer, CR 2012, 438, 439 f.

22 *Eckhart*, in: *Spindler/Schuster*, (Hrsg.), Recht der elektronischen Medien, 2. Aufl., 2011, § 98 TKG Rn. 12; Klesczewski, in: *Säcker*, (Hrsg.), Berliner Kommentar zum TKG, 2. Aufl, 2009, § 98 Rn. 9.

23 *Weichert* in diesem Band.

dere die Rechtsprechung des BGH hält eine solche opt-out-Regelung in AGB für zulässig.[24] Elektronische Einwilligungen müssen gem. § 13 Abs. 2 TMG protokolliert und jederzeit abrufbar sein.

Die Art. 29 Datenschutzgruppe konzentriert sich demgegenüber in ihrem Empfehlungen auf die Einwilligung als grundsätzliches Instrument.[25] Demnach soll die Einwilligung freiwillig und „qualifiziert“ erfolgen, wozu nach Auffassung der Art. 29 Gruppe eine Einwilligung in AGB nicht ausreiche, ebenso wenig wie ein opt-out-Mechanismus – was im Gegensatz zur einschlägigen BGH-Rechtsprechung steht.[26] Zudem sieht die Art. 29 Gruppe eine pauschal erteilte Einwilligung nicht als wirksam an, da eine solche sich auf die Verarbeitung bestimmter Daten oder bestimmter Arten der Verarbeitung beziehen müsse. Aus diesem Grund könne das bloße Klicken auf eine ‚Installieren-Schaltfläche‘, wie sie in viele App-Stores üblich ist, nicht schon als Einwilligung in die Datenverarbeitung durch die zu installierende Applikation angesehen werden.[27] Auch verlangt die Art. 29 Gruppe laufende Warnhinweise, ebenso wie eine Erneuerung der Einwilligung nach 12 Monaten, wenn der Nutzer den Dienst nicht genutzt hat, ebenso eine Erinnerung selbst bei aktiver Nutzung an die Einwilligung.[28] Kritisch bleibt allerdings anzumerken, dass es schwer fällt, derart detaillierte Regelungen aus den Bestimmungen der Datenschutz-Richtlinie abzulesen.

b) Koppelung

In der Praxis werden oft Einwilligungserklärungen verknüpft mit der Erbringung der Dienste, so dass die Leistungen „gekoppelt“ werden mit der Herausgabe personenbezogener Daten. Verbote gegen diese Koppelungen findet man expressis verbis bislang nur in § 28 Abs. 3b BDSG, der aber darauf abstellt, dass die Leistung nicht anderweitig ohne eine solche Herausgabe von Daten zu erlangen ist – dieser Nachweis wird in der Praxis dem Nutzer häufig schwerfallen. Gleiches gilt für den Versuch, über die „Freiwilligkeit“ der Einwilligung, wenigstens für „existentiell“ nötige Dienste eine solche Koppelung abzulehnen.[29] Wird eine Leistung von der Einwilligung abhängig, liegt prinzipiell keine Freiwilligkeit mehr vor, und dem Erfordernis des § 4a ist nicht mehr genüge getan.[30] Um die Reichweite des Kopplungsverbots zu bestimmen, sind daher zusätzliche Kriterien erforderlich, bspw. ob andere, gleichwertige Leistungen nur unzumutbar in Anspruch genommen werden können.[31] Tatsächlich bleibt daher ein großer Freiraum auch im Mobile Computing für derartige Verknüpfungen von Einwilligung mit Datenherausgabe.

c) Minderjährigenschutz

Generell ist der Minderjährigenschutz im Datenschutz als eher „unterentwickelt“ zu bezeichnen: Wie im Medizinrecht soll generell auf die Einsichtsfähigkeit der Minderjährigen abgestellt werden, um ihrem Selbstbestimmungsrecht Rechnung zu tragen. So schlägt etwa die EU-Datenschutz-GrundVO vor, dass generell das Alter von 13 festgelegt wird für die Einsichtsfähigkeit. Abgesehen davon, dass es Anbietern auch von Mobile Computing-Diensten kaum möglich ist, das Alter der Nutzer zu bestimmen, erst recht nicht deren Einsichtsfähigkeit als quasi bewegliche Grenze, die von verschiedensten Kriterien abhängt,[32] ist nicht recht einzusehen, warum die Genehmigung der Eltern im Gegensatz zum sonstigen Minderjährigenschutz nicht erforderlich sein soll.[33] Die Einwilligung in eine Datenverarbeitung kann zu einer lebenslangen Abrufbarkeit von Daten durch eine möglicherweise nicht abschätzbare Anzahl von

---

24 BGH, BGHZ 177, 253, 262, Rn. 23 f. – Payback; BGH, BGHZ 156, 250, 252, Rn.13; BGH, NJW 2010,864, 866, Rn. 23 – Happy-Digits; BGH, GRUR 2005, 438, 440, Rn. 22; Munzin, in: v. *Westphalen/Thüsing*, (Hrsg.), AGB-Klauselwerke, 29. EL, 2011, Datenschutzklauseln Rn. 31; kritisch dazu: van *Raay/Meyer*, VuR 2009, 103, 108 f.; *Brisch/Laue*, CR 2008, 724, 725

25 Art. 29 Datenschutzgruppe, WP 185 vom 16.5.2011, „Opinion 13/2011 on Geolocation services on smart mobile devices“, S. 15 f..

26 S. oben Fn. 23

27 Art. 29 Datenschutzgruppe, WP 202 vom 27.02.2013, „Opinion 02/2013 on apps on smart devices“, S. 15, abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

28 Art. 29 Datenschutzgruppe, WP 185 vom 16.5.2011, „Opinion 13/2011 on Geolocation services on smart mobile devices“, S. 16,.

29 So im Ansatz aber *Weichert* in diesem Band.

30 Zum – nicht ausdrücklichen – Kopplungsverbot aus § 4 a Abs. 1 S. 1 BDSG: *Taeger* in: *Taeger/Gabel* (Hrsg.), 2010, BDSG, § 4 a Rn. 51; *Simitis* in: *Simitis* (Hrsg.) BDSG, 7. Aufl., 2011, § 4 a Rn. 63 f.; einschränkend *Buchner*, DuD 2010, 39, 41.

31 *Wedde*, in: *Däubler* u. a. (Hrsg.), BDSG, 3. Auflg., 2010, § 28 Rn. 135: größerer Zeitaufwand; demgegenüber *Holznagel/Sonntag*, in: *Roßnagel*, Handbuch Datenschutzrecht, 2003,Kap. 4.8 Rn. 83: je höher der Wert der Leistung, desto mehr Aufwand zumutbar: s. auch Begr RegE eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BT-Drs. 16/12 011, S. 43

32 Krit. dazu zu Recht *Lober/Falker* K&R 2013, 357, 361.

33 Nicht eindeutig hier die Empfehlungen der Art. 29 Datenschutzgruppe , WP 185 vom 16.5.2011, „Opinion 13/2011 on Geolocation services on smart mobile devices“, S. 16 f.: Elterliche Genehmigung erforderlich, dann aber doch Abstellen auf Einsichtsfähigkeit der Kinder.

Personen führen und reicht daher in ihrer Tragweite über den bloßen Zeitpunkt der Einwilligung hinaus.[34] Zwar wird das Erziehungsrecht der Eltern mit wachsender Einsichtsfähigkeit des Kindes abgeschwächt;[35] doch kann effektiver Minderjährigenschutz durch das Erfordernis einer zusätzlichen Einwilligung der Eltern besser gewährleistet werden.

d) Reformbedarf

Wie schon an anderer Stelle hervorgehoben,[36] ist gerade die Einwilligung ein besonders reformbedürftiger Bereich: Allein immer weitere Informationspflichten[37] vermögen nicht das rationale Defizit des normalen Nutzers zu überwinden. Gleiches gilt für das Problem der Koppelung.[38] Erfolgversprechend sind hier – gerade im mobilen Bereich – nur neue Formen der Einwilligungseinholung, etwa durch vorgeschaltete Prozeduren, ebenso wie verpflichtende Browsereinstellungen, die auf ein opt-in hinauslaufen.[39] Ebenso sollte eine zeitliche Befristung der Einwilligung erwogen werden, indem diese periodisch neu zu erteilen ist.[40]

E. Informationspflichten

Wie auch sonst im Mobile Commerce, bereiten die umfangreichen Informationspflichten im Datenschutzrecht nach § 13 TMG vor der erstmaligen Nutzung erhebliche Probleme, da sie kaum auf einem Bildschirm eines mobilen Endgerätes dargestellt werden können. Dem Umstand der erschwerten Lesbarkeit auf mobilen Endgeräten tragen indes die Datenschutzaufsichtsbehörden Rechnung, indem notfalls auch ein Link zu einem Download genügen soll. Allerdings führt die technische Entwicklung hinsichtlich Tablet-PCs und immer größeren Smartphones zu einer Verbesserung der Bildschirmerkennbarkeit. Zwar sind diese Geräte immer noch nicht so groß wie ein herkömmlicher Bildschirm, dafür ist jedoch das Scrollen auf Touchscreens in der Regel einfacher und schneller möglich als auf anderen Geräten. Die Art. 29-Gruppe verlangt neben der Angabe von Identität und Kontaktdaten der verantwortlichen Stelle insbesondere welche Kategorien von Daten aus welchem Grund verwendet werden, zudem ob diese Daten an Dritte übermittelt werden, weiterhin wie der Nutzer seine Rechte ausüben kann.[41] Darüber hinaus ist die ePrivacy-Richtlinie vor allem hinsichtlich der Cookie-Regelung anwendbar, so dass in der Regel eine Einwilligung und Information bei abgelegten Daten auf dem mobilen Endgerät erforderlich ist, allerdings auch in der Systemeinstellung eine entsprechende Einwilligung gegeben werden kann.

In der Praxis wird allerdings zu Recht kritisiert, dass diese Informationspflichten in einer „Buchstabenwüste“ untergehen, etwa im Rahmen von umfangreichen, kaum noch nachzuvollziehenden Datenschutzerklärungen.[42] Die Crux liegt allerdings auch darin, dass auf privatautonome Entscheidungen abgestellt, der „information overload“ indes nicht zur Kenntnis genommen wird – hier mögen neue Prozeduren und auch Datenschutzsiegel Abhilfe schaffen.[43]

---

34 *Ohly*, Volenti non fit iniuria, 2002, S. 320 f.; *Rixecker*, in: MünchKommBGB, Bd. 1, 6. Aufl., 2012 , Anhang zu § 12 Rn. 54.

35 BVerfGE 59, 360, 382 – Schülerberater; BVerfG NJW 1986, 1859, 1860, Rn. 49 f. – Elterliche Vertretungsmacht; BGH NJW 1974, 1947, 1949 f., Rn. 35 – Nacktaufnahmen; OLG Köln FamRZ 1996, 1027, 1028; *Klaas*, AfP 2005, 507, 516.

36 *Spindler*, Verhandlungen des 69. Deutschen Juristentages 2012, Band I Gutachten, Teil F,, S. F 104 ff.

37 Dazu sogleich

38 S. oben.

39 Ebenso *Weichert* in diesem Band.

40 Näher dazu *Spindler*, Verhandlungen des 69. Deutschen Juristentages 2012, Band I Gutachten, Teil F, S. F 109.

41 Art. 29 Datenschutzgruppe, WP 202 vom 27.02.2013, „Opinion 02/2013 on apps on smart devices“ S. 22.

42 *Weichert* in diesem Band.

43 Zum Informationsüberfluss: *Spindler*, Journal of Consumer Policy 2011, 315, 322; *Ben-Shahar/Schneider*, University of Pensylvania Law Review, Vol. 159 (2011), 647, 686; die Möglichkeit von Zertifizierungen zum Beweis der rechtskonformen Datenverarbeitung sieht der Vorschlag für eine Datenschutzgrundverordnung der EU nunmehr an verschiedenen Stellen vor, so soll die Kommission dafür zuständig sein, Standards für Datenschutzsiegel festzulegen und diese dann zu verleihen, vgl. Erwägungsgründe 77, 129 ff., Art. 26 Abs. 3a, Art. 39 und Art. 66 Abs. 1 Lit. gc des Kompromissvorschlags des LIBE-Komitees zum Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung); abrufbar unter: http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf;.mehr Transparenz durch Zertifizierungen mittels Datenschutzsiegeln erwog schon 2010die EU-Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Gesamtkonzept für den Datenschutz in der Europäischen Union, v. 4. 11. 2010, EU KOM(2010) 609 endg., S. 14, abrufbar unter: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf; schon früh zu Datenschutzaudits Roßnagel, DuD 1997, 505, 407.

F. Recht auf Löschung

Schließlich hat der Nutzer nach § 13 Abs. 7 TMG genauso wie nach §§ 34, 35 BDSG Ansprüche auf Auskunft und auch auf Löschung von nicht mehr erforderlichen Daten. Wie anderweitig zutreffend hervorgehoben wurde, geht auch eine Löschung einer App einher damit, dass der Grund für die Speicherung von Daten entfällt – wovon der Anbieter in der Regel aber nichts erfährt. Diesem Problem kann nur durch eine technische Ausgestaltung der App-Stores und der Apps Rechnung getragen werden, indem der Anbieter von der Löschung informiert wird.[44] Auch die Art. 29-Gruppe fordert entsprechende Vorkehrungen zur Anfrage der Löschung beim App-Anbieter.[45] In diesem Rahmen sollte auch das durch Art. 17 der EU-Datenschutz-GrundVO vorgeschlagene „Recht auf Vergessen“ fortentwickelt werden.

III. Das generelle Datenschutz-Problem: Vollzugsdefizit

Ein nicht auf das Mobile Computing beschränktes Problem betrifft das Datenschutzrecht generell: das Vollzugsdefizit. Aufsichtsbehörden sind generell kaum in der Lage, die Datenschutznormen durchzusetzen, die zivilrechtlichen Ansprüche erweisen sich in vielerlei Hinsicht als wenig effektiv, da sie zu wenig Anreize bieten, den Datenschutz durch Betroffene durchzusetzen. An anderer Stelle sind mögliche Weichenstellungen aufgeführt worden, um den Datenschutz zu effektuieren, etwa durch Verbandsklagemöglichkeiten, Aufnahme in wettbewerbsrechtliche Anspruchsgrundlagen etc.[46] Eine Crux, die auch von Weichert aufgeführt hat, besteht gerade beim Mobile Computing darin, dass die jeweils Verantwortlichen nur schwer festgestellt werden können.[47] Abhilfe vermag hier eine Art Portalverantwortlichkeit zu schaffen, gerade im Hinblick auf Apps, die von App-Store Anbietern im Verbund mit ihrem jeweiligen Betriebssystem und/oder Hardware geprüft werden; wenn diese Portalbetreiber als „end-of-the-pipeline“ dafür Sorge tragen müssten, dass die entsprechenden Vorschriften eingehalten werden – vergleichbar etwa der Rechtslage bei Importeuren – wäre bereits viel gewonnen.

IV. Fazit

Der Mobile Commerce schafft ohne Zweifel neue Bedrohungen für den Datenschutz; allerdings wirft der Mobile Commerce abgesehen von dem Wirrwarr um die anwendbaren Rechtsgrundlagen nur wenige eigenständige Rechtsfragen auf, die über die bekannten Probleme im Datenschutz bewältigt werden könnten. Fragen wie die Ausgestaltung der Einwilligung und deren Voraussetzungen oder der Vollzug sind sowohl für den „klassischen“ Datenschutz im Internet als auch für Mobile Computing weitgehend ähnlich. Dies gilt auch für die internationale Anwendbarkeit des Datenschutzrechts. Der Vorschlag der EU-Datenschutz-GrundVO enthält hier zahlreiche Ansätze, die es weiter zu verfolgen gilt.[48]

---

44 zutr. *Lober/Falker* K&R 2013, 357, 363.
45 Art. 29 Datenschutzgruppe, WP 202 vom 27.02.2013, „Opinion 02/2013 on apps on smart devices“, S. 21.
46 Ausführlich dazu *Spindler*, Verhandlungen des 69. Deutschen Juristentages 2012, Band I Gutachten, Teil F, S.F 128 ff.
47 *Weichert* in diesem Band.
48 S. dazu insgesamt auch *Spindler*, Verhandlungen des 69. Deutschen Juristentages 2012, Band I Gutachten, Teil F, S. F 114.

Prof. Niko Härting

Mobiler Datenschutz – Information der Nutzer

I. Die Herausforderungen der Mobilität

Das mobile Netz stellt das Datenschutzrecht vor eine Vielzahl von Herausforderungen:

- Das Smartphone ist zugleich Sender und Empfänger personenbezogener Daten. Dies wirft die Frage nach der Verteilung von Verantwortlichkeiten auf.
- Durch die ständige Erfassung, Speicherung und Verknüpfung von Geolokalisationsdaten schafft das Smartphone ideale Bedingungen für vielfältige Anwendungsformen von Big Data-Auswertungen. Profiling und Targeting stehen in einem dauernden Spannnungsverhältnis zum Persönlichkeitsschutz.
- Big Data erlaubt die unbegrenzte Erfassung und Speicherung unstrukturierter Daten, die durch Algorithmen ausgewertet werden.
- Die Verarbeitungsprozesse, die sich auf Algorithmen stützen, werden immer komplexer und intransparenter.
- Auch die Weitergabe von Daten („Sharing“) wird zunehmend komplex und intransparent.

II. Profilbildung: das Nutzungsprofil als Rechtsbegriff

Schon das Informations- und Kommunikationsdienste-Gesetz (IuKDG) vom 22.7.1997[1] bemühte sich, spezifische datenschutzrechtliche Regelungen zu schaffen für das Internet. Lange bevor Begriffe wie „Profiling“, „Targeting“ und „Big Data“ in aller Munde waren, führte das Gesetz über den Datenschutz bei Telediensten (TDDSG) in § 4 Abs. 4 eine Regelung für „Nutzungsprofile“ ein, die in § 15 Abs. 3 TMG in modifizierter Form bis heute Bestand hat. Die Norm bemühte sich um eine angemessene Balance zwischen den Interessen der Internetanbieter und dem Schutz der Nutzer. Die praktische Bedeutung der Vorschrift ist dennoch begrenzt geblieben, da das Verbotsprinzip und konkurrierende Normen des BDSG in einem ungeklärten Verhältnis zu § 15 Abs. 3 TMG stehen.

§ 4 Abs. 4 TDDSG lautete:

> „Nutzungsprofile sind nur bei Verwendung von Pseudonymen zulässig. Unter einem Pseudonym erfasste Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.“

Daten, die über die Nutzung Auskunft geben, durften somit zu einem Profil zusammengeführt werden, wenn dies unter einem Pseudonym des Nutzers erfolgte. Hinzu kam ein striktes Trennungsgebot, das es dem Anbieter untersagte, den „Schleier“ der Pseudonymität zu lüften[2]. Das strikte Gebot der Pseudonymität sollte einen adäquaten Schutz des Rechts auf informationelle Selbstbestimmung gewährleisten[3].

§ 4 Abs. 4 TDDSG ließ das Verhältnis zur Einwilligung offen, und es war streitig, ob eine Pseudonymisierung auch dann erforderlich war, wenn der Nutzer einer Profilanlegung zugestimmt hatte[4]. Der Begriff der Pseudonymität war dem Datenschutzrecht noch fremd, und es war unklar, wie man den neuen Begriff in der Dichotomie zwischen Personenbezug und Anonymität einordnen sollte:

> „Die Einführung pseudonymer Daten stellt gegenüber dem BDSG, das außer den personenbezogenen nur anonyme Daten kennt, eine Privilegierung dar, ändert aber im Grundsatz nichts daran, dass auch pseudonyme Daten personenbezogene Daten bleiben[5].“

---

1 BGBl. I, S. 1870.
2 Vgl. *Zscherpe*, in: *Taeger/Gabel* , BDSG, § 15 TMG Rdnr. 64 f.
3 Vgl. *Engel-Flechsig/Maennel/Tettenborn*, NJW 1997, 2981, 2987; Gesetzesbegründung, BT-Drucks. 13/7385, S. 24.
4 Vgl. Entwurf des EGG vom 17.5.2001, BT-Drucks. 14/6098, S. 29 f..
5 Imhof, CR 2000, 110, 115, Fn. 49.

Der bei der Umsetzung der E-Commerce-Richtlinie neu gefasste § 6 Abs. 3 TDDSG[6] (heute: § 15 Abs. 3 TMG) sollte (unter anderem) klarstellen, dass pseudonyme Nutzungsprofile angelegt werden dürfen, ohne dass es (zusätzlich) einer Einwilligung der Nutzer bedarf[7]:

> „Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht .... hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.“

1. Opt-Out-Prinzip

Trotz der Neufassung der Norm blieben Unsicherheiten über das Erfordernis einer Einwilligung bestehen. So wurde vertreten, dass das Widerrufsrecht nichts daran ändere, dass es (zusätzlich) einer Einwilligung der Nutzer bedarf[8]. Vereinzelt wurde § 6 Abs. 3 TDDSG zwar – zutreffend – entnommen, dass für Nutzungsprofile ein „Opt-Out-Prinzip“ (statt des Erfordernisses einer Einwilligung) gilt, gegen das jedoch verfassungsrechtliche Zweifel im Hinblick auf das Volkszählungsurteil des BVerfG[9] geltend gemacht wurden[10].

2. Beschränkung auf Nutzungsdaten

Roßnagel meinte, dass es bei pseudonymen Daten an einem Personenbezug fehle und die Profilbildung schon aus diesem Grund keiner Einwilligung des Betroffenen bedürfe. Allerdings gelte § 6 Abs. 3 TDDSG nur für Nutzungsdaten gemäß § 6 Abs. 1 TDDSG (jetzt: § 15 Abs. 1 TMG). Jegliche Kombination mit anderen Daten oder auch eine „anbieterübergreifende“ Erstellung von Profilen bedürfe der Einwilligung des Betroffenen[11].

Hullen/Roggenkamp vertreten (zu § 15 Abs. 3 TMG) die Ansicht, dass es sich um einen Erlaubnistatbestand handelt, der eng auszulegen sei und sich nur auf Nutzungsdaten gemäß § 15 Abs. 1 TMG beziehe[12]. Soweit allerdings das Profil lediglich mit einer IP-Adresse verknüpft sei, handele es sich um ein „anonymes Profil“, auf das das TMG (ebenso wie das BDSG) nicht anwendbar sei[13].

3. Personenbezug trotz Pseudonymität

§ 15 Abs. 3 Satz 1 TMG gibt dem Datenverarbeiter keine Gewähr für einer Befreiung vom Verarbeitungsverbot gemäß § 4 Abs. 1 BDSG[14], zumal Pseudonyme zugleich personenbezogene Daten sein können, wenn bekannt ist oder mit zugänglichem Zusatzwissen festgestellt werden kann, auf welche Person sie sich beziehen[15]. Schaar vertrat bereits 2002 die Auffassung, dass das Pseudonym im Normalfall den Personenbezug nicht aufhebt[16]. Dies ist die logische Folge des von den Datenschützern überwiegend befürworteten “absoluten” Begriffs des Personenbezugs. Eine theoretische Möglichkeit, den Schleier des Pseudonyms zu lüften, gibt es immer.

III. Pseudonymisierung und Pseudonyme

Der Begriff des Pseudonyms hat sich erst durch das Internet im Datenschutzrecht eingebürgert[17] und dient dazu, die Identität der Person zu verschleiern, deren Daten gespeichert sind[18].

---

6 Gesetz über rechtliche Rahmenbedingungen des elektronischen Geschäftsverkehrs (EGG) vom 14.12.2001, BGBl. I, S. 3721.
7 Vgl. Entwurf des EGG vom 17.5.2001, BT-Drucks. 14/6098, S. 29 f..
8 *Rasmussen*, CR 2002, 36, 43.
9 BVerfG vom 15.12.1983, BVErfGE 65, 1 ff. – Volkszählung.
10 *Schmitz* in *Spindler/Schuster/Geis*, TDG, München 2004, § 6 TDDSG, Rdnr. 30; Schmitz in: *Hoeren/Sieber/Holznagel*, Hnadbuch Multimeida-Recht, Stand Dezember 2012, teil 16.2, Rdnr. 222.
11 *Roßnagel* in: *Roßnagel/Banzhaf/Grimm*, Datenschutz im Electronic Commerce, Heidelberg 2003, S. 223; ebenso *Schaar*, Datenschutz im Internet, München 2002, Rdnr. 706 ff..
12 *Hullen/Roggenkamp* in Plath, BDSG, Köln 2012, § 15 TMG, Rdnr. 21 f.
13 *Hullen/Roggenkamp* in Plath, BDSG, Köln 2012, § 15 TMG, Rdnr. 23.
14 Vgl. Peifer, K&R 2011, 543, 545.
15 *Schaar*, Datenschutz im Internet, München 2002, S. 59, Rdnr. 162.
16 *Dammann* in *Simitis*, BDSG, § 3, Rdnr. 67.
17 Vgl. *Scholz* in *Simitis*, BDSG, § 3 Rdnr. 212 f.
18 *Schmitz* in *Spindler/Schmitz/Geis*, § 4 TDDSG Rdnr. 44.

§ 3 Abs. 6a BDSG versteht die Pseudonymisierung als das „Ersetzen“ des Namens oder anderer Identifizierungsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Dieser Definition liegt die Perspektive eines Datenverarbeiters zugrunde, der über einen Bestand an personenbezogenen Daten verfügt und diese Daten in pseudonymisierte Daten verwandelt: An die Stelle des Namens bzw. der (anderen) Identifizierungsmerkmale tritt jeweils ein „Kennzeichen“, das keinen Rückschluss auf die Person des Betroffenen zulässt.

Beim Pseudonymisieren gibt es im Normalfall eine Zuordnungsregel bzw. Referenzliste oder Referenzdatei, die es dem Kenner dieser Regel bzw. Liste oder Datei ermöglicht, die Pseudonymisierung rückgängig zu machen[19]. In einem solchen Fall haben die Daten jedenfalls für den Datenverarbeiter Personenbezug, sodass trotz der Pseudonymisierung das Verbot mit Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG) gilt.

Hat der Datenverarbeiter keine Kenntnis von der Zuordnungsfunktion und auch keine Möglichkeit der Kenntnisnahme, besteht aus seiner Sicht kein Unterschied zu anonymen Daten[20], und es hängt von dem („absoluten“ oder „relativen“) Verständnis des Begriffs des Personenbezugs ab, ob die Daten § 4 Abs. 1 BDSG unterfallen oder nicht[21]. Bei einem absoluten Verständnis des Begriffs reicht die bloße Existenz der Zuordnungsregel für einen Personenbezug aus[22]. Bei einem relativen Verständnis kommt es dagegen darauf an, ob der Datenverarbeiter den Personenbezug ohne unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder herstellen kann[23].

Nicht von § 3 Abs. 6a BDSG erfasst sind Datenbestände, die von vornherein weder Namen noch andere Identifizierungsmerkmale enthalten[24]. Derartige Datenbestände sind originär „pseudonym“, ohne dass es einer „Pseudonymisierung“ bedarf. Diese Art der „Pseudonymität“ ist bei Online-Diensten weitverbreitet.

IV. „IT-Grundrecht“ – ein Blick in die Zukunft

In dem Urteil zur Online-Durchsuchung hat das BVerfG ein neues Grundrecht geschaffen: das „IT-Grundrecht“ (Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme)[25]. Dass es eines solchen „neuen“ Grundrechts bedarf, hat das BVerfG unter anderem damit begründet, dass das Recht auf informationelle Selbstbestimmung Schutzlücken aufweist[26]. Das Gefahrenpotential, gegen das das „IT-Grundrecht“ schützt, liegt nach dem BVerfG darin, dass ein Dritter sich durch Zugriff auf ein informationstechnisches System einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen kann, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein[27]. Der heimliche Blick auf die Computerfestplatte lässt sich mit dem althergebrachten Blick durch das Schlüsselloch vergleichen. Unbemerkt gelangt ein „Eindringling“ in die Privatsphäre.

Obwohl Einigkeit darüber besteht, dass das in der Online-Durchsuchung geschaffene „IT-Grundrecht“ Drittwirkung hat und den Gesetzgeber zu schützenden Maßnahmen im Bereich der Privatwirtschaft aufruft, ist die Diskussion um gesetzgeberische Konsequenzen[28] bislang in ersten Anfängen stecken geblieben. Die Grundrechtsgefahren durch Spuren vernetzter Kommunikation erfordern indes eine umfassende Anpassung des Persönlichkeits- und Datenschutzrechts an die Gegebenheiten der Informationsgesellschaft[29].

---

18 *Schmitz* in *Spindler/Schmitz/Geis*, § 4 TDDSG Rdnr. 44.
19 Vgl. *Gola/Schomerus*, § 3, Rdnr. 46; *Buchner* in Taeger/Gabel, BDSG, § 3, Rdnr. 47; *Zscherpe* in *Taeger/Gabel*, BDSG, § 3a, Rdnr. 46.
20 Vgl. *Arning/Forgó/Krügel*, DuD 2006, 701 f.
21 Vgl. *Plath/Schreiber* in *Plath*, BDSG, § 3, Rdnr. 62; *Buchner* in *Taeger/Gabel*, BDSG, § 3, Rdnr. 47.
22 Vgl. *Buchner* in *Taeger/Gabel*, BDSG, § 3, Rdnr. 50.
23 *Plath/Schreiber* in *Plath*, BDSG, § 3, Rdnr. 63; Scholz in Simitis, BDSG, § 3, Rdnr. 220 a; *Buchner* in *Taeger/Gabel*, BDSG, § 3, Rdnr. 49.
24 Vgl. *Plath/Schreiber* in *Plath*, BDSG, § 3, Rdnr. 63; *Scholz* in *Simitis*, BDSG, § 3, Rdnr. 220 a; *Buchner* in *Taeger/Gabel*, BDSG, § 3, Rdnr. 49.
25 BVerfG vom 27.2.2008, NJW 2008, 822 ff. – Online-Durchsuchung.
26 BVerfG vom 27.2.2008, NJW 2008, 822, 824 – Online-Durchsuchung.
27 BVerfG vom 27.2.2008, NJW 2008, 822, 826 – Online-Durchsuchung.
28 Vgl. *Bartsch*, CR 2008, 613 ff.; Kutsche, DuD 2011, 461, 462 f.; *Luch*, MMR 2011, 75 ff.; *Roßnagel/Schnabel*, NJW 2008, 3534 ff.
29 Vgl. *Hoffmann-Riem*, JZ 2008, 1009, 1010.

1. Profiling im Zeichen von Big Data

Amazon, Google und Facebook gehören zu den Vorreitern des „Profiling“. Hierunter versteht man die systematische Auswertung des Nutzerverhaltens. Es wird erfasst, für welche Seiten, Bücher, Werbebanner und Suchbegriffe ein Besucher der Website sich interessiert hat. Algorithmen errechnen sodann, welche Suchergebnisse, Waren oder Werbeanzeigen den Besucher voraussichtlich interessieren werden. Der Internetnutzer erhält auf diese Weise „maßgeschneiderte“, zielgerechte („targeted“) Werbung und erfährt (nur noch) das, was ihn mutmaßlich interessiert[30].

Die Entwicklung immer intelligenterer Algorithmen steht noch am Anfang. Immer größere Datenmengen („Big Data“) erfassen das Nutzerverhalten, und die Daten werden immer raffinierter ausgewertet und analysiert. Der Besucher einer Nachrichtenseite erhält dann nur noch Nachrichten, die (voraussichtlich) zu seinem Leseverhalten passen. Und der Nutzer einer Musikplattform wird laufend mit Musikvorschlägen konfrontiert, die den individuellen Musikgeschmack treffen sollen.

Die Daten, die beim algorithmengesteuerten „Profiling“ gesammelt werden, sprengen den Rahmen des § 15 Abs. 1 TMG, da als Nutzungsdaten nur Daten gelten, deren Erhebung und Verwendung „erforderlich“ ist, um die Inanspruchnahme des Telemediums zu ermöglichen. Von einer solchen „Erforderlichkeit“ kann beim Profiling zumeist nicht die Rede sein. Schon aus diesem Grund empfiehlt es sich für jedes Unternehmen, das „Profiling“ vornimmt, auf weitreichende Einwilligungserklärungen der Nutzer zu setzen und sich nicht auf eine großzügige Auslegung des § 15 Abs. 3 TMG zu verlassen.

2. Profiling als Anwendungsfall für das IT-Grundrecht

In der Heimlichkeit der Beobachtung liegt eine Parallele zwischen der Onlinedurchsuchung einerseits und der unbegrenzten und unkontrollierbaren Anlegung von Nutzungsprofilen im Internet: Die umfangreiche Speicherung von Daten bei Google stellt nach dem Empfinden vieler Nutzer einen Eingriff in die Privatsphäre dar. Dieser Eingriff wird nicht dadurch nennenswert abgemildert, dass die Betreiber von Google keine Kenntnis von der Identität der Person erlangen können, die hinter dem Nutzungsprofil stehen. Die Vorstellung, dass ein Internetanbieter über eine genaue Protokollierung besuchter Seiten die Möglichkeit hat, Interessen, Eigenheiten und Vorlieben des Nutzers sehr präzise zu analysieren, ist vielen Internetnutzern unangenehm. Die heimliche und unkontrollierte Protokollierung und Auswertung der Nutzergewohnheiten stellt ein „Ausspähen“ des Bürgers dar, das sich von der gezielten Online-Durchsuchung einer Computerfestplatte allenfalls graduell unterscheidet.

Bei der Diskussion um die Personenbezogenheit von Daten beim Profiling geht es im Wesentlichen darum, ob die Gefahr besteht, dass die anfallenden Datenspuren einem Nutzer zugeordnet werden, der Google namentlich bekannt ist. Für Dienste wie Facebook und Google sind Namen jedoch unwichtige Störgeräusche („Noise“)[31]. Und beim Webtracking oder beim Profiling liegt der Eingriff in die Privatsphäre nicht darin, dass der Internetnutzer ernsthaft befürchten muss, von einem Google-Mitarbeiter namentlich identifiziert zu werden, wobei unter einer Identifizierung die Verbindung von Informationen zu einem Individuum zu verstehen ist[32].

Nicht die Sorge vor der Deanonymisierung ist es, die ein ungutes Gefühl bereitet, sondern der heimliche Blick durch das virtuelle Schlüsselloch. Wie beim Blick durch das Schlüsselloch liegt das Unbehagen nicht darin, dass der Eindringling weiß, wer ich bin. Der Internetnutzer nimmt es vielmehr als freiheitsbeschränkend wahr, dass er sich – anonym - beobachtet fühlt, ohne genau abschätzen zu können, mit welcher Genauigkeit die Beobachtung erfolgt. Bei der Diskussion um Cookies und IP-Adressen geht es letztlich darum, dass ein „potentiell äußerst großer und aussagekräftiger Datenbestand“ entsteht, der den tiefen Einblick in die Persönlichkeit ermöglicht, aus dem das BVerfG das „IT-Grundrecht“ abgeleitet hat[33]. Google Analytics ruft das „IT-Grundrecht“ auf den Plan und nicht die informationelle Selbstbestimmung.

---

30 Zu datenschutzrechtlichen Aspekten verhaltensbezogener Onlinewerbung vgl. *Rammos*, K&R 2011, 692 ff.
31 Vgl. *Hardy*, Rethinking Privacy in an Era of Big Data, New York Times v. 4.6.2012, http://bits.blogs.nytimes.com/2012/06/04/rethinking-privacy-in-an-era-of-big-data/?ref=technology.
32 Vgl. *Solove*, Understanding Privacy, Cambridge/London 2009, S. 122.
33 BVerfG vom 27.2.2008, NJW 2008, 822 ff. – Online-Durchsuchung.

3. „Diffuse Bedrohlichkeit“ und Transparenz

Wenn das Verhalten des Internetnutzers systematisch beobachtet, erfasst und analysiert wird, kann dies beim Nutzer ein „diffus bedrohliches Gefühl des Beobachtetseins“[34] hervorrufen. Hierin liegt eine erhebliche Herausforderung für den Schutz von Persönlichkeitsrechten. Die „diffuse Bedrohlichkeit“ verlangt nach Transparenz. In seiner Entscheidung zur Vorratsdatenspeicherung hat das BVerfG daran erinnert, dass Regelungen zur Information der von Datenerhebungen oder -nutzungen Betroffenen zu den elementaren Instrumenten des grundrechtlichen Datenschutzes gehören[35].

Transparenz ist eine notwendige Grundbedingung selbstbestimmten Handeln. Der Nutzer, der in verständlicher und ausführlicher Form Informationen darüber abrufen kann, wie ein Anbieter mit Daten umgeht, kann eine informierte Entscheidung darüber treffen, ob er einen Internetdienst nutzen möchte. Dies wird den Gegebenheiten der Netzwelt wesentlich gerechter als eine starre Fixierung auf Einwilligungserfordernisse[36].

V. Ein Blick in die Zukunft

Der Regelungsansatz des § 15 Abs. 3 TMG könnte sich trotz aller Unzulänglichkeiten als beständig erweisen, da die Norm einerseits die Risiken nicht leugnet, die die Profilbildung mit sich bringt, andererseits aber anerkennt, dass Persönlichkeitsrisiken bei pseudonymen Daten anders zu bewerten sind als bei der Verwendung von „Klarnamen“. Allerdings bedarf es auch bei allen Formen der Pseudonymität verstärkter Transparenz.

Für angemessene Verbraucherinformationen lassen sich folgende Grundanforderungen skizzieren:

- Zu viel Information gibt es nicht. Auch wenn es nur sehr wenige Nutzer geben wird, die die Zeit und Mühe aufwenden, seitenlange Datenschutzbestimmungen zu studieren, ist kein vernünftiger Grund ersichtlich, der gegen ausführliche Informationen spricht.
- Die Ausführlichkeit darf nicht zu Lasten der Transparenz gehen. Daher sind Bemühungen zu begrüßen, Standards für Kurzinformationen zu schaffen, die den Verbraucher in die Lage versetzen, in kurzer Zeit Kerninformationen in verständlicher Form zu erfassen.
- „One Size Fits All“ ist ein untauglicher Ansatz für Verbraucherinformationen. Standards, die für Internetplattformen größerer Anbieter entwickelt werden, werden sich nicht unmodifiziert auf kleinere Anbieter oder gar auf Offline-Prozesse übertragen lassen.
- Der Verbraucher wird durch Informationen mündig und nicht durch das Anklicken einer vorformulierten Einwilligung. Die Einwilligung ist als zentrales Schutzinstrument untauglich.
- Niemand wird das Rad in die vordigitale Welt zurückdrehen können. Die digitale Wirklichkeit zeichnet sich dadurch aus, dass Daten ein zentraler Rohstoff der Kommunikation und Wertschöpfung sind. Vom Grundsatz der Datensparsamkeit sollte sich das Datenschutzrecht verabschieden, wenn es nicht realitätsblind bleiben möchte.
- Je mehr Algorithmen unsere Wirklichkeit beherrschen, desto mehr stellt sich die Frage ihrer Transparenz. Algorithmen sind „man made“. Wie bei anderen technologischen Verfahren bedarf es klarer Transparenzstandards, die eine gesellschaftliche Kontrolle ermöglichen.
- „Big Data“-Anwendungen schaffen einen Informationsfundus, der der Wissenschaft und Forschung offen stehen sollte. Es bedarf einer gesellschaftlichen Diskussion über „Open Data“-Standards, die den gesellschaftlichen Nutzen von Datenbeständen fördern.
- Wenn über das Smartphone Geodaten und andere (sehr) persönliche Daten des Nutzers erfasst werden, sollte der jederzeitige Zugriff des Nutzers auf diese Daten möglich sein. Dabei geht es weniger um ein Verfügungsrecht des Nutzers als darum, dass der Nutzer frei sein sollte, die Daten jederzeit einer Auswertung zuzuführen, aus denen er Nutzen für seinen Gesundheit, für sein Selbstbild oder für sein berufliches und privates Fortkommen ziehen kann.

---

34 BVerfG vom 2.3.2010, BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 – Vorratsdatenspeicherung, Rdnr. 212.
35 BVerfG, a.a.O., Rdnr. 242.
36 *Härting*, AnwBl 2011, 246, 248.

Thilo Weichert

„Sind die gesetzlichen Schutzregelungen im Telekommunikationsgesetz und im Bundesdatenschutzgesetz für die Nutzenden ausreichend?“

Dass es Gesetzgebungsbedarf im Bereich „Mobile Computing“ geben muss, drängt sich allein angesichts der anwendbaren Regelungen auf. Diese – das Bundesdatenschutzgesetz (BDSG), das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) sowie flankierend das Verbraucherrecht, z. B. im Bürgerlichen Gesetzbuch (BGB) – stammen teilweise aus Vor-Internet-Zeiten, in denen dem Gesetzgeber die Möglichkeiten und Herausforderungen des mobilen Netzes im Hinblick auf Verbraucherinnen und Verbraucher noch nicht im Ansatz erkennbar waren.

„Mobiler Datenschutz“ hat viel mit den Themen „Mobile Shopping“ und „Mobile Payment“ zu tun, geht aber in der Praxis weit darüber hinaus: Es geht nicht nur um Einkaufen und Bezahlen, wenn Verbraucher mit ihren mobilen Geräten unterwegs sind. Es geht auch um die Mobilität selbst, im Individualverkehr ebenso wie im öffentlichen Personenverkehr. Es geht um Familie und Freizeit, wobei das Einkaufen von analogen Waren nur eine Facette ist und Informations-, Service- und Unterhaltungsangebote einen zunehmenden Marktanteil einnehmen. Es geht um „Mobile Marketing“ in den unterschiedlichsten Gestaltungsformen, beispielsweise als standortbezogene Werbeangebote im Rahmen von „Location Based Services“ (LBS) oder sonstige standortbezogene Dienstleistungen. Es geht weiterhin um die Schnittmengen, die den Menschen als Verbraucher mit seinen anderen Rollen verbinden, also etwa als Arbeitnehmer, wenn dieser sein „Bring-Your-Own-Device“-Gerät verwendet. Es geht um die Rolle der Privatperson und des Familienmenschen, um den politisch handelnden Bürger oder um die sozial sich austauschenden Person auf den unterschiedlichsten technischen Ebenen und in den unterschiedlichsten Gruppenzusammenhängen.

Die Komplexität des Themas entsteht zudem durch die vielen unterschiedlichen Player auf dem Feld, die an der mobilen Datenverarbeitung der Verbraucher teilhaben:

1. Die Hersteller der mobilen Geräte und ihrer Betriebssysteme sowie die Anbieter von Kommunikationssoftware wie Browsern haben den ersten Zugriff auf den Kunden.
2. Die Netzbetreiber sind nicht nur für die technische Ermöglichung der Kommunikation verantwortlich, sondern haben zu den Kunden mit Zusatzangeboten vielfältige Vertragsbeziehungen.
3. Eine eigenständige Relevanz haben die Portalanbieter, die mit den Browseranbietern nicht identisch sein müssen. Eine Spezialität der Portalanbieter liegt zumeist in Werbeangeboten für Shop-Betreiber.
4. Auf dem Mobilmarkt hat sich ein unüberschaubares Angebot von Applikationen entwickelt, die über sog. App-Stores oder Apps-Marketplaces online zur Verfügung gestellt und von App-Anbietern betrieben werden.
5. Die Shop-Betreiber haben bzw. suchen regelmäßig den direkten Kundenkontakt und führen ein oft durch viele digitale Zusatzinformationen angereichertes Customer Relation Management (CRM) System.
6. Die Bezahlverfahren im Online-Bereich sind vielfältig. Payment-Anbieter sind neben klassischen Banken und Kreditkartenunternehmen weitere involvierte oder selbstständige Dienstleister.

Die Komplexität der Rechtsbeziehungen erhöht sich dadurch, dass bei vielen Internetanwendungen nicht nur ein Nutzer, sondern ein oder mehrere Kommunikationspartner einbezogen sind. Dies gilt für die zweiseitige Kommunikation, aber erst recht für Konferenzkommunikationen, wie sie beruflich wie privat (beispielsweise bei Onlinespielen) vielfältig praktiziert werden.

Nicht nur die Rollen, auch die technischen Infrastrukturen, auf denen der mobile Datenschutz aufsetzen oder in denen er nach Möglichkeit integriert sein sollte, sind alles andere als überschaubar und homogen:
So kommen nebeneinander unterschiedliche Netze zur Anwendung: Dies sind zum einen verschiedene Mobilnetze nach unterschiedlichen technischen Standards. Der GSM-Standard (Global System for Mobile Communications) wird zunehmend durch UMTS (Universal

Mobile Telecommunications System) abgelöst. Inzwischen haben wir es mit einer vierten Generation von Mobilfunkstandards, den LTE-Netzwerken (Long Term Evolution), zu tun. Parallel dazu spielen WLANs (Wireless Local Area Networks) eine Rolle, die jenseits der Funkstationen der Netzbetreiber von kommerziellen und privaten Anbietern den Kontakt zum Endverbraucher herstellen können.

Der datenschutzrechtliche Gesetzgebungsbedarf in Bezug auf Mobile Computing ist zumindest teilweise identisch mit dem Gesetzgebungsbedarf zum Schutz des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme im Bereich der Netzkommunikation generell. Die Besonderheit des Mobile Computing liegt in folgenden Aspekten:

- die Erhebung und Verarbeitung von Standortdaten,
- die technischen Eigenheiten von Funknetzen gegenüber kabelbasierten Netzen,
- die intensive, oft dauernde personale Verbindung der Mobilgeräte mit einer natürlichen Person,
- die aus Gründen der Mobilität, dem Bedarf einer Synchronisierung mit verschiedenen Geräten und der oft geringeren Ressourcen häufig gewählte oder standardmäßig aktivierte Verbindung mit Cloud-Diensten.

Im Folgenden will ich – angesichts der vielen auftretenden datenschutzrechtlichen Fragestellungen – einige zentrale Fragen besonders herausgreifen und anhand der bestehenden und künftigen Rechtslage überprüfen. Hierbei können nicht alle Fragestellungen behandelt werden, die von Relevanz sind. So werden z. B. die Nutzung von Mobildiensten durch Kinder, die Nutzung am Arbeitsplatz oder die Verknüpfung von dienstlich-privater Nutzung hier nicht weiter thematisiert. Auch die Datenschutzprobleme, die in Zusammenhang stehen mit der Nutzung von Cloud-Diensten, mit globaler Kommunikation und den Zugriffsmöglichkeiten und faktischen Zugriffen durch Geheimdienste sowie mit den aktuellen Cybersecurity-Initiativen auf nationaler und europäischer Ebene werden an dieser Stelle nicht weiter ausgeführt.

Vor der Klammer ist auf ein praktisches wie rechtliches Problem hinzuweisen: Bei der Netzdatenverarbeitung wird zwischen drei Datenkategorien unterschieden: Inhaltsdaten, Nutzungs- bzw. Verkehrsdaten und Stamm- bzw. Bestandsdaten. Mit dieser Unterscheidung soll zum einen eine Abstufung nach der Sensibilität erfolgen, wobei grds. davon ausgegangen wird, dass Inhaltsdaten am sensitivsten und Bestandsdaten am wenigsten schützenswert seien, was sich auch an den materiell-rechtlichen und den verfahrensrechtlichen Eingriffsvoraussetzungen festmacht. Tatsächlich ist aber die Einordnung der anfallenden Daten oft nicht eindeutig. Zudem sind insbesondere die Nutzungsdaten teilweise von erheblich höherer persönlichkeitsrechtlicher Aussagekraft als viele Inhaltsdaten. Dies gilt für Service-, Partner-, Ort- und Zeitangaben beim Mobile Computing, über die elektronisch Bewegungs-, Kontakt- und Interessenprofile erstellt werden können.

Ebenfalls vor die Klammer gehört, dass die Trennung zwischen Telekommunikations- und Telemedienrecht im Hinblick auf Internet-Datenverarbeitung generell willkürlich erscheint und in der Praxis oft nicht sinnvoll möglich ist. Regelmäßig handelt es sich bei mobilen Angeboten um Telemediendienste gem. § 1 Abs. 1 TMG, so dass als Datenschutzvorschriften die §§ 11 ff. TMG anwendbar sind. Die rechtliche Abgrenzung erfolgt danach, ob der Dienst gem. § 3 Nr. 24 TKG ein Telekommunikationsdienst ist, also ein Dienst, der ganz oder überwiegend in der Übertragung von Signalen über die Telekommunikationsnetze besteht. Diese auf den Schwerpunkt eines Dienstes abstellende rechtliche Abgrenzung führt dazu, dass klassische, das Telefon ersetzende Kommunikationsdienste weitgehend als Telemediendienst einzustufen sind.

Art. 10 Grundgesetz in Form des Telekommunikationsgeheimnisses spielt also auch bei der Nutzung von Telemedien eine zentrale Rolle. Telekommunikationsangebote werden von Telemedienanbieter erbracht. Es wäre zu wünschen, dass die Regelungsmaterien, deren Aufteilung unserer föderalen Aufteilung der Gesetzgebungskompetenzen geschuldet ist – den Rahmenregelungen der Europäischen Union (EU) folgend – zusammengeführt würden.

Auf europäischer Ebene haben wir derzeit eine zweigliedrige Regelungsstruktur: Für Inhaltsdaten gilt die Europäische Datenschutzrichtlinie 1995 (EU-DSRl), für die Verkehrs- und Nutzungsdaten die E-Privacy-Richtlinie, die „Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ (EU-TK-DSRl). Die Europäische Datenschutz-Grundverordnung (EU-DSGVO), welche die Richtlinie 1995 ersetzen soll, beschränkt sich nicht auf die Regulierung von Inhaltsdaten, sondern zielt gerade im Hinblick auf die Internet-Datenverarbeitung auch auf Nutzungs- und Bestandsdaten. Nach einem ersten Entwurf Anfang

2012 beschloss der Innen- und Rechtsausschuss des Europaparlaments Oktober 2013 einen Vorschlag, der eine Grundlage der weiteren Darstellungen ist. Misslich bleibt, dass auf europäischer Ebene neben der künftig anzuwendenden EU-DSGVO nationales Telekommunikations- und -medienrecht anwendbar sein soll, das lediglich über die EU-TK-DSRl vereinheitlicht, nicht aber vollständig und direkt anwendbar ist. Es ist zu wünschen, dass bald nach Beschluss der EU-DSGVO auch eine einheitlich gültige EU-Telekommunikations-Datenschutzverordnung in Angriff genommen wird. Einige wichtige datenschutzrechtliche Konfliktpunkte sind folgende:

1. Wann ist ein personenbezogenes Datum anzunehmen?
2. Wer ist für welche Datenverarbeitung verantwortlich?
3. Welches Recht ist anwendbar?
4. Welche materiell-rechtlichen Voraussetzungen bestehen für die Verarbeitung von Standortdaten und -profilen?
5. Wie kann für die Betroffenen die nötige Transparenz hergestellt werden?
6. Welche Anforderungen sind an wirksame Betroffeneneinwilligungen bzw. -widersprüche zu stellen?
7. Wie können die Betroffenenrechte in der Praxis umgesetzt werden?

Diese Fragen sollen nun bearbeitet werden:

1. Wann ist ein personenbezogenes Datum anzunehmen?

Eine der aus Datenschutzsicht nutzlosesten und zugleich gefährlichsten Debatten ist die über den Personenbezug. Sie wurde erstmals erschöpfend über durch dynamische IP-Adressen erschlossene Daten geführt. Von Wirtschaftsseite wurde diese Debatte ausschließlich mit dem Ziel geführt, sich dem Datenschutzregime zu entziehen, wenngleich unbestreitbar war und ist, dass dynamische IP-Adresse und Zeitangabe in den allermeisten Fällen eine Zuordnung zu einen Gerätebesitzer und zu einem Nutzenden, also zu einer natürlichen Person, erlaubt. Eine vergleichbar fruchtlose Debatte wurde zu den Cookies geführt, die uns aber die grds. datenschutzfreundliche Regelungen des Art. 5 Abs. 3 EU-TK-DSRl einbrachte. Inzwischen gibt es – insbesondere im Mobilbereich – viele zusätzliche Identifikatoren, die an Hard- oder Software anknüpfen und die wegen ihrer Zuordenbarkeit zu natürlichen Personen regelmäßig ebenso personenbeziehbar sind.

Dies gilt für die Kennungen der Mobilgeräte (Unique Device Identifiers (UDID) wie beim iPhone oder andere Geräte-IDs), die weltweit eindeutig sind und nicht geändert werden können. Diese ermöglichen es App-, Portal- und Werbeanbietern, anwendungsübergreifend Zuordnungen vorzunehmen und diese Gerätenutzungen zu verfolgen, also zu tracken, und beispielsweise für Werbezwecke zu vermarkten. Über lange Zeit hinweg war es üblich, dass Apps die Geräte-ID ohne Einwilligung des Betroffenen erhoben und nutzten. Diese nach deutschem Recht unzulässige Praxis wird zunehmend von Anbietern, wie z. B. Apple, technisch nicht mehr zugelassen, ist aber weiterhin verbreitet. Apple hat als Ersatz für die Nutzung der UDID einen Identifier for Advertising (IDFA) eingeführt, dem ebenso ein Personenbezug zukommt, selbst wenn Nutzer durch Einstellungen dessen Nutzung beschränken können.
Ein Personenbezug liegt auch dann vor, wenn die mobile IT Bestandteil einer umfassenderen Hardware, etwa eines Kfz ist. Darüber wird evtl. selbst das Kfz-Kennzeichen oder die Fahrzeug-Identifizierungsnummer zu einem datenschutzrechtlich relevanten Identifikator (vgl. § 39 Abs. 1 StVG).

Bei einer Fortschreibung des Rechts muss beachtet werden, dass Identifikatoren in immer schwieriger erkennbarem Gewand daherkommen: An die Stelle von Cookies oder Geräte-IDs wird auf Merkmalskombinationen zurückgegriffen, mit denen Nutzer eindeutig identifiziert werden können, ohne dass dies sofort erkennbar ist, z. B. indem ein Browser-Fingerprint zum Tracken verwendet wird. Eine gesetzgeberische Antwort hierauf darf sich nicht in einer technikbezogenen Präzisierung dessen erschöpfen, was unter Personenbeziehbarkeit zu verstehen ist; die Technik würde dazu jeweils Ausweichstrategien entwickeln. Eine wirksame Antwort liegt aber in der Einschränkung von Profilbildungen, so wie dies Art. 20 EU-DSGVO versucht.

2. Wer ist für welche Datenverarbeitung verantwortlich?

Der Frage nach der datenschutzrechtlichen Verantwortlichkeit wurde über viele Jahre hinweg als geklärt bzw. irrelevant angesehen. Dies hat sich mit der Nutzung von Internet-Diensten und erst recht von mobilen Smartphones geändert. Durch die Einschaltung vieler

Stellen, durch die Unklarheit, welche dieser Stellen welche Datenverarbeitung durchführt, und durch die Angewiesenheit auf diese Verarbeitungsketten besteht die Gefahr, dass die Verantwortlichen nicht feststellbar sind. Dies führt zwangsläufig dazu, dass sich Beteiligte ihrer Verantwortung entziehen und ihre Geschäftsmodelle auf einer datenschutzwidrigen Datenverarbeitung aufbauen. Bei der Mobilkommunikation sind regelmäßig Endnutzer, Webseitenanbieter, App-Anbieter und bzw. oder Portalbetreiber für bestimmte Formen der Datenverarbeitung verantwortlich.

Der ursprüngliche Ansatz, dass nur verantwortlich ist, wer die Hoheit über Daten hat, wird schon bei der Auftragsdatenverarbeitung aufgehoben. Besteht aber hier zumindest noch ein rechtlicher Zugriff auf die Daten, so geht dieser bei weisungsfreier Arbeitsteilung völlig verloren. Die Definition in § 3 Abs. 7 BDSG gibt keine Auslegungshilfe, wenn dort die Stelle für verantwortlich erklärt wird, die „Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“. Etwas klarer ist Art. 2 lit. d) EU-DSRl, wonach verantwortlich ist, wer „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Hier wird auf die Möglichkeit der Arbeitsteilung hingewiesen, ohne aber klarzustellen, wie groß der Anteil bei der Entscheidung sein muss. Davon unbeeindruckt meinte nun das Verwaltungsgericht (VG) Schleswig, dass keine Verantwortlichkeit besteht, soweit eine Stelle eine vorgegebene Form der Datenverarbeitung nutzt, ohne Verfügungsgewalt über die Daten zu haben (U. v. 09.10.2013, u. a. Az. 8 A 218/11). Dass eine Stelle durch Einrichtung eines Dienstes erst die Grundlage für die Verarbeitung und auch deren Art und Weise schafft, wurde vom Gericht ausgeblendet. Das ULD vertrat und vertritt in dem Verfahren die Ansicht, dass jede Zweckveranlassung zu einer Verantwortlichkeit führt, also wenn bewusst eine unabdingbare Voraussetzung für eine personenbezogene Datenverarbeitung durch eine Stelle gesetzt wird.

Leider ist insofern auch der aktuelle Parlamentsentwurf in Art. 4 Abs. 5 EU-DSGVO unklar, der inhaltlich nicht von der bisherigen Regelung der EU-DSRl abweicht. Die restriktive Auslegung z.B. durch das VG Schleswig führt dazu, dass eine Stelle in Deutschland einen datenschutzwidrigen Dienst auswählen kann und hierfür datenschutzrechtlich nicht zur Verantwortung gezogen werden kann, wenn die Festlegungen zur Datenverarbeitung von dort einfach übernommen werden. Um insofern Rechtssicherheit zu bekommen, sollte klargestellt werden, dass jede Zweckveranlassung einer Datenverarbeitung zu einer Verantwortlichkeit hierfür führt. Eine solche Zweckveranlassung kann ebenso der Betrieb einer Portalseite sein wie die Installation einer App oder von Plugins.

3. Welches Recht ist anwendbar?

Ebenso ungeklärt war lange Zeit, welches Datenschutzrecht anwendbar ist. § 1 Abs. 5 BDSG in Umsetzung von Art. 4 EU-DSRl gibt dazu bisher eine Antwort, die aber Interpretationsspielraum eröffnet: Anwendbar ist danach bei Vorliegen einer Niederlassung das nationale Recht der Niederlassung. Das VG Schleswig wie auch das OVG Schleswig-Holstein betrachteten aber nicht jede Art von Niederlassung als relevant, sondern nur eine, in der über die konkrete Datenverarbeitung entschieden wird (OVG SH, B. v. 22.04.2013, 4 MB 11/13). Dass eine deutsche Stelle für ein Unternehmen tätig ist, z. B. für das Marketing und die Akquise, soll keine Rolle spielen. Es wird also einem Unternehmen überlassen festzulegen, wo die wesentlichen Entscheidungen getroffen werden und damit welches Recht anwendbar ist. Diese anbieterzentrierte, nicht am Verbraucher oder am Grundrechtsschutz orientierte Gesetzesinterpretation ermöglicht es Unternehmen, ihre Standortentscheidungen danach zu treffen, wo das geringste Datenschutzniveau besteht bzw. wo Datenschutzrecht am schwierigsten für die Betroffenen durchzusetzen ist.

Dieses fragwürdige Ergebnis soll mit der EU-DSGVO verändert werden: Europaweit soll einheitlich dieselbe Verordnung anwendbar sein, egal ob die Verarbeitung in der EU erfolgt oder nicht. Gemäß Art. 3 Abs. 2 a) soll es darauf ankommen, dass Betroffenen in der EU Waren oder Dienstleistungen angeboten werden. Nach Art. 51 Abs. 1 des Parlamentsvorschlages gilt das Territorialitätsprinzip. Jeder Betroffene hat nach Art. 73 EU-DSGVO die Möglichkeit, bei jeder Aufsichtsbehörde seine Beschwerde einzureichen. Vorrangig zuständig ist nach Art. 54 a die „Lead Authority“, also die Behörde am Ort der Hauptniederlassung. Vor einer Entscheidung muss aber eine Beteiligung der anderen betroffenen Aufsichtsbehörden erfolgen, wobei Konsens angestrebt werden muss und eine Anrufung des letztentscheidenden Europäischen Datenschutzbords möglich ist.

4. Welche materiell-rechtlichen Voraussetzungen bestehen für die Verarbeitung von Standortdaten und -profilen?

Standortdaten sind – im Zusammenhang mit Geräte- oder Nutzeridentifikatoren – personenbezogene Daten, die regelmäßig Auskunft darüber geben, wo sich ein Nutzer aufhielt bzw. aufhält. In Kombination mit weiteren Inhalts- und Nutzungsdaten, z. B. von Location Based Services, kommt diesen Daten eine hohe Aussa-

gekraft zu. Der Standort lässt sich auf unterschiedliche Weise feststellen. Möglich ist dies über Satellitennavigationssysteme wie GPS (Global Positioning System), über den lokalisierten WLAN-Zugang und dessen MAC-Adresse (Media Access Control) oder durch die Ortung über Mobilfunkbasisstationen, die bei eingeschaltetem und eingebuchtem mobilen Gerät nutzerseitig nicht unterbunden werden kann.

Standortdaten werden regelmäßig als Verkehrs- oder Nutzungsdaten erhoben. Denkbar ist aber auch, z. B. durch Einsatz von GPS, dass sie unabhängig vom Verbindungsaufbau erhoben und verarbeitet werden. Die Verarbeitung von Standortdaten scheint knapp und befriedigend geregelt: Gemäß § 98 TKG ist die Verarbeitung erlaubt, wenn und soweit dies „zur Bereitstellung von Diensten mit Zusatznutzen“ erforderlich ist. Für sämtliche weiteren Nutzungen bedarf es der ausdrücklichen Einwilligung des Teilnehmers. Mitbenutzende sind über erteilte Einwilligungen zu unterrichten. Selbst bei Bestehen einer Generaleinwilligung muss die Möglichkeit bestehen, die Erfassung „auf einfache Weise und unentgeltlich zeitweise zu untersagen“. Ansonsten muss vor einer Verarbeitung eine Anonymisierung erfolgen. § 98 TKG setzt Art. 9 der EU-TK-DSRl um.

Problematisch ist jedoch, dass das Abgreifen von Standortdaten oft nicht im Zusammenhang mit der Erbringung eines TK-Dienstes und durch den TK-Dienstebetreiber erfolgt. § 98 TKG ist nicht direkt auf Telemedienanbieter und auf gesondert erhobene GPS-Daten anwendbar. Dessen ungeachtet können und müssen – wegen des generell im Datenschutzrecht geltenden Verbotsprinzips mit Erlaubnisvorbehalt – bei der Verwendung von Standortdaten, die nicht zur Erbringung des Mediendienstes erforderlich sind, Einwilligungen eingeholt werden. Fraglich ist, was zur Erbringung eines Dienstes nötig ist: Die Festlegung erfolgt einseitig durch den Anbieter, etwa einer App. Handelt es sich bei den dann erhobenen Daten nicht um Nutzungs-, sondern um Inhaltsdaten, so ist nicht einmal § 15 Abs. 3 TMG anwendbar mit der Folge, dass nach § 28 Abs. 3 BDSG eine Werbenutzung dieser Angaben schnell so begründet wird. Wegen des hohen Risikopotenzials von Standortdaten sind an Einwilligungen dem gegenüber hohe Anforderungen zu stellen.

Dass z. B. von App-, Portal- und weiteren System-Anbietern in zu großem Maße – und damit unzulässig – Standortdaten erhoben und verarbeitet werden, ist weniger den materiellen Regelungen zuzuschreiben als dem Umstand, dass von den Betroffenen einzuholende Einwilligungen unzureichend sind oder – unzulässigerweise – völlig auf diese verzichtet wird.

5. Wie kann für die Betroffenen die nötige Transparenz hergestellt werden?

Mobile Geräte haben regelmäßig ein kleineres Display als die hochauflösenden Bildschirme von stationären Rechnern. Zwar lassen sich auf Tablets fast ähnlich große Informationsmengen wie auf einem PC-Bildschirm anzeigen, doch gelten für Mobilgeräte einheitliche Standards, die auch für Hosentaschengeräte anwendbar sein müssen.

Gemäß § 13 Abs. 1 TMG sind Nutzende zu Beginn eines Vorgangs über die Art, den Umfang und die Zwecke der Erhebung und Verwendung der Daten sowie über die Verarbeitung außerhalb von Europa „in allgemein verständlicher Form zu unterrichten“. Nur so ist eine selbstbestimmte Entscheidung darüber möglich, ob und wie der Dienst genutzt werden soll. Die Transparenzpflichten gehen aber noch weiter: § 5 TMG verpflichtet zur erreichbaren Anzeige von Impressumsangaben, bei kommerziellen Angeboten nach § 6 TMG mit zusätzlichen Hinweisen. Im Fall einer Weitervermittlung muss dies nach § 13 Abs. 5 TMG angezeigt werden. Für den Fall der Profilbildung, also beispielsweise bei der Datenzusammenführung für Werbezwecke, muss nach § 15 Abs. 3 TMG hierüber sowie über das bestehende Widerspruchsrecht informiert werden. Zu diesen Anforderungen des TMG kommen weitere Transparenzpflichten nach dem BDSG: die Pflicht zur Information über Werbenutzungen und über die Einräumung der Widerspruchsmöglichkeit hiergegen nach § 28 Abs. 4 BDSG und die Pflicht zur Bereitstellung von Verfahrensverzeichnissen (§§ 4e, 4g Abs. 2 BDSG). Bei besonderen Übermittlungen sind nach § 33 BDSG und bei bestimmten automatisierten Entscheidungen nach § 6a BDSG weitere Benachrichtigungspflichten vorgesehen. Gesetzlich gar nicht geregelt, aber dringend nötig wäre zur Sicherung der Betroffenenrechte die Mitteilung der Erreichbarkeit des betrieblichen Datenschutzbeauftragten (§ 4f BDSG) und die Benennung dieser Betroffenenrechte (§§ 6, 34, 35 BDSG).

Soll ein Nutzer eine Erklärung abgeben, etwa seine Einwilligung zur Datenverarbeitung, so müssen weitere Informationen vermittelt werden, in jedem Fall Angaben über verantwortliche Stelle, Art und Zweck der Datenverarbeitung (§ 4a BDSG) sowie über die Widerrufbarkeit (§ 13 Abs. 3 TMG).

Viele Anbieter machen es sich bei der Vermittlung dieser Informationsfülle einfach, indem sie die gesamten Angaben in eine Buchstabenwüste von Privacy Policies oder Nutzungsbestimmungen packen, verbunden mit der Vermutung, dass diese ohnehin nicht zur Kenntnis

genommen werden. Hiergegen gibt es bisher rechtlich keinen wirksamen Schutz. Es bedarf aufwändiger Verfahren und zumeist Gerichtsprozesse, z. B. durch Verbraucherschutzverbände, um gegen diese Buchstabenwüsten nach den Regeln zu Allgemeinen Geschäftsbedingungen (AGBs) gemäß den §§ 305 ff. BGB vorgehen. Wegen der Vielfalt der technischen Gestaltung und deren verbaler Darstellungen haben selbst gerichtliche Festlegungen nur eine geringe Bindungs- und Vorbildwirkung.

In der Praxis gibt es inzwischen Lösungen, die Informationsgehalt einerseits und Aufnahmefähigkeit und -bereitschaft des Nutzers andererseits aufeinander abstimmen. Derartige verbraucherfreundliche Lösungen laufen darauf hinaus, dass Informationen nicht pauschal und vorab erteilt werden, sondern situationsbezogen und nur wenn erforderlich. Außerdem kann mit einem mehrschichtigen Informationsangebot zunächst ein Hinweis, evtl. per Icon, dann eine generelle – gesetzlich geforderte – Information und nur im Bedarfsfall eine – gesetzlich möglicherweise nicht zwingende, aber vertieften Verbraucherinteressen entsprechende – Hintergrundinformation gegeben werden. Derartiges „Layered Policy Design“ mag wegen seiner hohen differenzierten Anforderungen im Detail gesetzlich schwer zu erzwingen sein. Wohl aber ist es möglich, solche vorbildlichen Angebote über unabhängige Zertifizierungen oder Siegel für den Verbraucher erkennbar zu machen.

Art. 39 EU-DSGVO sieht solche Datenschutzzertifizierungen generell vor. Praktiziert werden sie bisher durch das Unabhängige Landeszentrum für Datenschutz (ULD) in Kiel sowohl gemäß nationalem als auch europäischem Recht – dem Gütesiegel Schleswig-Holstein und dem European Privacy Seal – EuroPriSe. An einer nationalen Vereinheitlichung versucht sich derzeit die Stiftung Datenschutz.

6. Welche Anforderungen sind an wirksame Betroffeneneinwilligungen bzw. -widersprüche zu stellen?

Die datenschutzrechtlichen Anforderungen an wirksame Einwilligungen sind in § 4a BDSG und § 13 Abs. 2 TMG geregelt. Einwilligungen müssen Angaben über die verantwortliche Stelle, den erlaubten Zweck und über Art und Umfang der Daten enthalten. Die Erklärung darf also nicht pauschal, sondern muss qualifiziert erfolgen. Die Einwilligung muss freiwillig sein. Dies ist nicht der Fall – unabhängig von expliziten Koppelungsverboten –, wenn die Einwilligung mit der Erbringung einer für den Betroffenen existenziellen Leistung zwingend verknüpft wird. Die Einwilligungserklärung muss gesondert hervorgehoben werden und darf nicht in AGBs versteckt sein. Weitere Voraussetzung ist die künftige Widerrufbarkeit (vgl. auch § 28 Abs. 3a BDSG). Bei elektronischen Einwilligungen wird nach § 13 Abs. 2 TMG zusätzlich gefordert, dass die Erklärung protokolliert wird und jederzeit abrufbar ist.

Die Neigung der Wirtschaft, sich pauschale unbestimmte Einwilligungen ohne hinreichende Information einzuholen, ist weit verbreitet. Ebenso wie bei der Erfüllung der Informationspflichten besteht die Problematik, dass die Formulierungen stark dienste- und technikabhängig sind und deshalb die sehr voraussetzungsvolle Durchsetzung der rechtlichen Anforderungen in der Praxis zu kurz kommt.

Auch im Hinblick auf die Einwilligung kann gemäß dem schon erwähnten „Layered Policy Design“ vorgegangen werden. Eine weitere praktikable Sicherung des Erklärungswillens des Einwilligenden beruht im Prinzip des „Privacy by Default“, also einer datensparsamen und damit datenschutzfreundlichen Grundeinstellung, die durch qualifizierte Einzeleinwilligungen durch den Betroffenen bewusst erweitert werden muss. Dieser Grundsatz ist bisher gesetzlich noch nicht explizit festgelegt, lässt sich aber schon heute aus den Prinzipien der Erforderlichkeit und Datensparsamkeit und den rechtlichen Anforderungen an Einwilligungen zwingend ableiten. Eine explizite Regelung, wie sie nun in Art. 23 Abs. 2 EU-DSGVO vorgesehen ist, ist aber dringend erforderlich, um die bestehenden Vollzugsdefizite abbauen zu können.

Einwilligungen im Online-Bereich können auf den unterschiedlichsten Ebenen erteilt werden. Es ist nicht zwingend, dass dies erst auf der konkreten Anwendungsebene erfolgt. Deshalb bietet es sich an, standardisierte Einwilligungen schon durch Browsereinstellungen vorzunehmen, die einmal festgelegt generell für die Browsernutzung gelten. Voraussetzung ist aber auch hier die Anwendung des Grundsatzes „Privacy by Default“. Weiterhin ist nötig, dass gewährleistet wird, dass Browsereinstellungen von den konkreten Online-Anwendungen auch verstanden und akzeptiert werden. Hierfür ist eine möglichst weltweite Standardisierung wünschenswert, wie sie durch das Konsortium W3C angestrebt wird. Wie schwierig diese Standardisierung ist, zeigt sich bei den bisherigen Bemühungen, Standards für das Tracken von Nutzern („Do-Not-Track“) und die damit verbundene Werbung festzulegen.

Basiert eine Datenverarbeitung auf einer voreingestellten Einwilligung, so können schnell Transparenzprobleme entstehen, da den Betroffenen regelmäßig nicht

präsent ist, welche Erklärungen sie in der Vergangenheit abgegeben haben. Deshalb ist es erforderlich, durch einfach erkennbare Signale, Icons o. Ä., zu erkennen, welcher Einwilligungsstatus derzeit besteht. Diese Notwendigkeit besteht zudem bei Geräten, die von mehr als einer Person genutzt werden und dadurch die Person des Einwilligenden von der des Betroffenen abweichen kann. Diese Anforderung gilt für bestimmte Zwecke, etwa für die Werbenutzung, aber insbesondere auch für bestimmte sensible Daten, im Bereich der Mobilkommunikation vor allem für die Standortdaten.

Die Art. 29-Datenschutzgruppe empfiehlt zudem, dass individuelle Einwilligungen „nach einer gewissen Zeitspanne“ zu erneuern sind. Dies muss in jedem Fall gelten, wenn ein Dienst längere Zeit, z. B. über ein Jahr, nicht mehr genutzt wurde. In einem solchen Jahresturnus könnte auch eine Pflicht zur Erinnerung an bestehende Einwilligungen festgelegt werden. Hierfür gibt es aber bisher keine klare gesetzliche Grundlage.

Art. 7 EU-DSGVO sieht präzise Bedingungen für wirksame Einwilligungen vor. Diese müssen eindeutig erkennbar sein. Der verantwortlichen Stelle obliegt eine Beweispflicht. Die Widerrufsmöglichkeiten werden präzise festgelegt. Ursprünglich geplante Einschränkungen bei technisch und vertraglich überlegenen verantwortlichen Stellen haben sich im aktuellen Parlamentsentwurf nicht durchgesetzt.

7. Wie können die Betroffenenrechte in der Praxis umgesetzt werden?

Ein großes Problem bei Internet-Diensten ist die technische, rechtliche und letztlich praktische Durchsetzung der Betroffenenrechte, also insbesondere des Rechts auf Auskunft (§ 13 Abs. 7 TMG, § 34 BDSG) sowie die Rechte auf Berichtigung, Löschung und Sperrung von Daten (§ 35 BDSG). Bei der Mobilkommunikation werden noch mehr Daten als bei der stationären Datenverarbeitung beiläufig erfasst, für die es oft nur einen kurzfristigen Speicherbedarf gibt. Dies gilt insbesondere für App- und Portalanbieter.

Die rechtlichen Anforderungen an Auskunftserteilung und Datenkorrektur sind klar und weitgehend unstreitig. So ist z. B. unbestreitbar, dass die Betroffenenrechte sich auch auf pseudonym erfasste Daten erstrecken. Probleme bestehen jedoch bei der Realisierung der Betroffenenrechte.

Für die technische Umsetzung des Auskunftsanspruchs genügt es nicht, Profildaten etwa über ein sog. Dashboard zum Abruf bereitzustellen. Vielmehr müssen auch die (z. B. für Werbezwecke) unter Pseudonym abgelegten Daten sowie Metadaten, also Verkehrsdaten und Auswertungsdaten, beauskunftet werden.

Erfolgt eine Datenlöschung durch einen Nutzenden auf seinem Profil, so müssen diese Daten auch real gelöscht werden, wenn diese nicht für einen zulässigen Zweck weitergespeichert werden dürfen. Ein solcher Zweck besteht nicht darin, einem Nutzer später die Reaktivierung von Daten oder eines gesamten Accounts anbieten zu können. Allenfalls für eine kurze Zeitspanne kann eine Zwischenspeicherung erlaubt sein, wenn die Gefahr besteht, dass ungewollt bzw. versehentlich Daten gelöscht werden. Unabhängig davon ist die turnusmäßige Löschung von Nutzerdaten vorzusehen, etwa wenn eine App gelöscht bzw. ein Nutzungsvertrag gekündigt wird. Bei unentgeltlichen Nutzungsverhältnissen, bei denen den Anbietern oft nicht bekannt wird, dass eine Nutzung nicht mehr erfolgen soll, sind nach kurzen Fristen Regellöschungen vorzusehen.

Zusammenfassung und Ausblick

Die Untersuchung der vordringlichen Datenschutzfragen des Mobile Computing zeigt, dass diese weitgehend identisch sind mit den allgemeinen Fragen moderner Internet-Datenverarbeitung. Die insofern bestehenden Regulierungsdefizite werden beim Mobile Computing oft noch verstärkt. Dies gilt etwa für die ungeklärten Fragen zur Verantwortlichkeit und zum anwendbaren Recht. Die Entwürfe zu einer EU-DSGVO versprechen insofern nur teilweise Abhilfe.

Eine Zusammenführung der Datenschutzmaterien im TKG und TMG auf nationaler Ebene und eine einheitliche Wahl des Regelungsinstruments, also perspektivisch von Verordnungen, auf europäischer Ebene sind erstrebenswert.

Die Besonderheit des Mobile Computing liegt in den extensiven Nutzungspotentialen der Standortdaten. Deren Verarbeitung jenseits der Erbringung der jeweiligen Dienste ist von ausdrücklichen Einwilligungen abhängig.

Unbestreitbar ist, dass die bestehenden rechtlichen Anforderungen in der Praxis oft nicht beachtet werden. Der Abbau von Vollzugsdefiziten ist insofern von größter Bedeutung. Hierfür ist nicht nur eine bessere Ausstattung der Aufsichtsbehörden relevant; förderlich können auch die Verbesserung des Instrumentariums der Aufsichtsbehörden, eine Verschärfung der Sanktionen, die Erhöhung der Praktikabilität der Betroffenen-

rechte sowie eine Erleichterung der Klagemöglichkeiten sein. Einiges hiervon wird in den Entwürfen zur EU-DSGVO vorgesehen.

Nicht zwingend regulierungsbedürftig, aber regulierungsfähig und zweifellos begrüßenswert sind Infrastruktur-Verbesserungen für den Datenschutz: Privacy by Default, Standardisierungen und Zertifizierungen können das Datenschutzniveau bei der Internet-Datenverarbeitung generell und beim Mobile Computing speziell massiv verbessern.

Es ist absehbar, dass Trends des mobilen Computings künftig noch zu einer stärkeren Relevanz für Individuen und Gesellschaft entfalten werden. Diese sollten daher in Bezug auf regulatorische Möglichkeiten oder Notwendigkeiten politisch diskutiert werden. Dazu gehören der Einsatz von NFC-Technologie (z.B. zum Bezahlen, zur Interaktion mit anderen Personen oder zur Konfiguration eines Smart Homes), die Verwendung von Handys als Multifunktionsdevices (z.B. gleichermaßen zur Individualkommunikation wie etwa zur Fernsteuerung von Geräten, z.B. Drohnen), die Erfassung und Auswertung biometrischer Daten der Nutzenden (z.B. zu medizinischen Zwecken, zur Selbstvermessung oder zur Unterstützung wie in Sprachassistenzsystemen) oder die Übertragung und Analyse von Daten der Umgebung (z.B. Google Glass).

Schließlich sollte auch das Potenzial von Mobile Computing für ein Mehr an Datenschutz ausgelotet werden, beispielsweise indem die Nutzerinnen und Nutzern mit Hilfe solcher Geräte gerade in der komplexer werdenden Welt der ubiquitären Datenverarbeitung in der Risikoeinschätzung, im Identitätenmanagement und insgesamt in ihrer informationellen Selbstbestimmung effektiv unterstützt werden.

Arbeitsgruppe 2 „Mobile Shopping“

„Mobile Shopping“ – Mobile Commerce im engeren Sinne – lässt sich über den gerade mit dem Smartphone online geschlossenen Fernabsatzvertrag definieren. Die Arbeitsgruppe „Mobile Shopping“ soll sich inhaltlich mit Fragen des Rechtsrahmens im M-Commerce befassen. Dabei sind unterschiedliche Vertragsgestaltungen denkbar: M-Shopping-Verträge können klassische Fernabsatzverträge über Waren und Dienstleistungen sein, Fernabsatzverträge, die unter Verwendung einer speziellen M-Shopping-App geschlossen werden (sog. „In-App-Käufe“), oder auch nur der Kauf derartiger Anwendungsprogramme für das Gerät.
Für all diese unterschiedlichen Erscheinungsformen des M-Shoppings stellt sich aus Sicht des Verbraucherschutzes eine Reihe von rechtlichen Fragen. In der Arbeitsgruppe „Mobile Shopping“ sollen die folgenden Themenschwerpunkte behandelt werden:

- Vertragsbeziehungen beim Kauf von Apps, bei kostenlosen Apps und Folgen insbesondere für die Haftung
- Informationspflichten
- Technikneutralität
- die rechtliche Behandlung von Verträgen über digitale Inhalte

Zu den Diskussionsthemen gehören dabei unter anderem die Fragen nach dem Vertragspartner sowie nach der Pflichtenverteilung und Haftung beim App-Kauf im Dreiecksverhältnis App-Plattform, App-Entwickler und Verbraucher. Es sollen die Fragen erörtert werden, wie die Informationspflichten beim Mobile Shopping rechtssicher und verbraucherfreundlich erfüllt werden können und wie einem drohenden Informationsüberfluss vorgebeugt werden kann. Unter anderem in Bezug auf die Einbeziehung von Allgemeinen Geschäftsbedingungen möchten wir mit den Teilnehmern darüber diskutieren, ob sich das Recht der technischen Entwicklung oder die Technik dem geltenden Recht anpassen muss. Sowohl die Verbraucherrechterichtlinie als auch der Verordnungsvorschlag der Europäischen Kommission für ein Gemeinsames Europäisches Kaufrecht enthalten Ansätze, die bei der Diskussion berücksichtigt werden sollten. Dazu gehören unter anderem besondere Regelungen in Bezug auf Verträge über digitale Inhalte. Vor diesem Hintergrund und unter Berücksichtigung der Verträge über kostenlose Apps soll auch die Frage beleuchtet werden, ob wir Sondervertragsrecht für digitale Inhalte brauchen.

2

Jutta Gurkmann

Was ist „mobile Commerce“ und welchen Rechtsrahmen brauchen wir für ihn?

1. Was ist „mobile Commerce“?

„Mobile Commerce im engeren Sinne – lässt sich insbesondere den gerade mit dem Smartphone oder dem Tablet online geschlossenen Fernabsatzvertrag definieren.“
Diese dem Veranstaltungsprogramm entnommene Aussage entspricht sicherlich der aktuellen (Tatsachen-) Lage. Dies darf aber nicht dazu führen, diese Situation als Prämisse für die weitere rechtliche Diskussion festzuschreiben! Eine gesetzliche Definition des „mobile Commerce“ gibt es nicht. Gerade angesichts der technischen Entwicklungen darf sich die Definition nicht über den Status des genutzten Endgeräts definieren. Bereits jetzt nutzen viele Verbraucher mobile Endgeräte auch anstelle des „klassischen“ Computers zuhause als Ersatz für ein stationäres Endgerät. So kommt es wohl zum einen auf die technischen Möglichkeiten des Endgeräts, aber auch die Form dessen Nutzung an. Befindet sich der Verbraucher etwa in seinem Heimnetzwerk? Befindet er sich dann außerhalb des „mobile Commerce“? Kann es dabei einen Unterschied machen, ob er dabei eine LAN- oder eine WLAN-Verbindung nutzt? Darf der Unterschied beim Zugang zum Internet eine differenzierte rechtliche Behandlung der dabei geschlossenen Verträge rechtfertigen? Wie würde die Antwort lauten, wenn dieselbe Frage auf die Nutzung unterschiedlicher Endgeräte abzielte?

Bei dieser Betrachtung haben wir uns nur auf den Vertriebsweg, nämlich einem (rein) digitalen, konzentriert. Müssen wir bei der Definition des „mobile Commerce“ nicht auch eine zweite Komponente mitdenken? Denken wir bei „mobile Commerce“ nur an die Inanspruchnahme digitaler Güter und Dienstleistungen oder aber auch vom Erwerb „analoger“ Güter? Auch hier gibt es keine rechtsverbindliche Definition. Aus einem rein tatsächlichen Verständnis auf der Grundlage der aktuellen Nutzungssituation würde man zurzeit sicherlich dazu tendieren, beides – also sowohl den Erwerb „analoger“ als auch die Inanspruchnahme digitaler Güter und Dienstleistungen – vom Anwendungsbereich des Begriffs „mobile Commerce“ erfasst zu sehen.

Dies sind sicherlich Fragen, die zunächst geklärt werden müssen, bevor wir uns der Behandlung des Folgeproblems widmen können.

2. Gibt es für den „mobile Commerce“ rechtliche Regelungen oder befinden wir uns in einer „rechtsfreien Zone“?

Nachdem wir die Fragen rund um die mögliche Definition des „mobile Commerce“ gewidmet haben, müssen wir uns einem weiteren Problem zuwenden: Es geht um die Frage, ob die Regelungen des „analogen“ BGB-Vertragsrechts auch für den „mobile Commerce“ gelten und – wenn ja – ob diese ausreichen? Definieren wir den „mobile Commerce“ als eine Vertriebsform von Waren - nämlich eine Sonderform des Fernabsatzes –, so fallen diese zweifelsohne unter die Regelungen des Fernabsatzes, und zwar – zumindest bislang – unterschiedslos, ob der Vertragsschluss über mobile oder stationäre Endgeräte erfolgt. Spezielle Regelungen zum „mobile Commerce“ gibt es bislang nicht.

Ebenso wenig gibt es ausdrückliche Regelungen für den Erwerb digitaler Güter. Es gibt lediglich Rechtsprechung, die den Erwerb von „Standardsoftware“ als Kaufvertrag einordnet: Im Hinblick auf den Schutz der Verbraucher war und ist hier vor allem die Frage nach dem Bestehen oder Nichtbestehen eines Widerrufsrecht streitig: Vielfach – und vor allem von der Anbieterseite – wird ein Widerrufsrecht mit dem Hinweis auf § 312d Abs. 4 Nr. 1 BGB abgelehnt. Die Ware sei zur Rücksendung nicht geeignet. Aus Sicht des Verbraucherschutzes kann diese Ausnahmevorschrift vom Widerrufsrecht jedoch nicht einschlägig sein, da eine Software selbstverständlich rückstandslos zurückgegeben werden kann. Lediglich ist es den Anbietern u.a. aufgrund datenschutzrechtlicher Gründe nicht vergönnt, dies zu kontrollieren. Dieses Problem rechtfertigt aber nicht die Ausdehnung eines Ausnahmetatbestands, der ja als solcher eng auszulegen ist. Es ist also grundsätzlich vom Bestehen eines Widerrufsrechts auch bei digitalen Gütern auszugehen, das dann z.B. auch für den „Kauf“ von Apps gelten muss.

Mit Umsetzung der Verbraucherrechterichtlinie wird es ab dem 13. Juni 2014 ausdrückliche Regelungen zum Erwerb digitaler Güter und auch zum „mobile Commerce“ geben: nämlich erstens die reduzierten Informationspflichten bei „räumlich und zeitlich begrenzten Darstellungsmöglichkeiten“. Damit ist sicherlich der „mobile Commerce“ erfasst. Er wird aber zum einen

nicht vollständig der Ausnahmeregelung unterliegen: Denn die Frage, ob der Darstellungsplatz reduziert ist, hängt vom benutzten Endgerät ab. Es gibt auch mobile Endgeräte wie zum Beispiel Tablets, die aufgrund ihrer Größe vergleichbare Darstellungsmöglichkeiten aufweisen wie „stationäre“ Endgeräte. Zum anderen wird die Ausnahmeregelung nicht nur den „mobile Commerce“ betreffen: Denn im Hinblick auf den limitierenden Faktor Zeit könnte z.B. Teleshopping oder auch Telefonwerbung als „Kandidaten“ für den Anwendungsbereich in Betracht kommen.

Wo und wie wird hier eine Abgrenzung vorgenommen werden? Wird es auf die Darstellungsgröße des benutzten Endgeräts ankommen? Oder auf die Frage, wie sich der Verbraucher ins Internet einwählt – über WLAN-Hotspots, über ein Heimnetzwerk – also auf die Frage des Zugangs zum Internet?

Zweitens wird es spezifische Informationspflichten über digitale Güter u.a. über die sog. Interoperabilität und Trackingfunktionen geben. Gerade letzteres würde im Hinblick auf den Datenschutz ein deutliches Plus gegenüber der aktuellen Situation bedeuten. In diesem Zusammenhang wird die Frage nach der „Entgeltlichkeit“ z.B. von Apps geklärt werden müssen. Die deutsche Umsetzungsregelung eröffnet den Anwendungsbereich der o.g. Regelungen nämlich nur für Verbraucherverträge, „die eine entgeltliche Leistung des Unternehmers zum Gegenstand haben“. In vielen Fällen „bezahlen“ Verbraucher aber gerade für die Nutzung kostenloser Apps mit ihren Daten. Hier hatten wir uns für eine ausdrückliche Aufnahme einer Klarstellung dahingehend ausgesprochen, dass auch andere Leistungen des Verbrauchers im Gegenzug für die Zurverfügungstellung einer Ware oder Dienstleistung ausreichen muss, um die o.g. Informationspflichten auszulösen. Diesem Ansinnen wurde zwar leider nicht entsprochen, doch geht aus der Beschlussempfehlung und dem Bericht des Rechtsausschusses zum Entwurf eines Gesetzes zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung (BT-Drs.) hervor, dass das Merkmal „Entgelt“ weit auszulegen ist. Es genüge irgendeine Leistung des Verbrauchers ohne dass es dabei auf die Gleichwertigkeit von Leistung und Entgelt oder auf deren Bezeichnung ankomme. Ganz ausdrücklich findet sich dort der Hinweis darauf, dass auch Verträge, bei denen der Verbraucher als Gegenleistung personenbezogene Daten mitteilt und in deren Speicherung, Nutzung oder Weitergabe einwilligt, erfasst seien.

Ein letzter Hinweis sei gestattet: Die Idee, dass sich die Welt immer weiter „digitalisiert“, scheint sich in den letzten Monaten auch wieder als nicht mehr so ganz zutreffend herauszustellen. Wie bereits oben dargestellt, dürfen wir beim e- oder m-Commerce nicht nur an den Erwerb digitaler Inhalte denken. Es geht auch immer um (die Kombination mit) digitalen Vertriebswegen. Hier hat sich die lange beobachtete Tendenz nach immer weiterer „Digitalisierung“ des Vertriebs in die Vermarktung von Mischvertriebsformen gewandelt. Zum einen häuften sich die Meldungen über Händler, die ihren „Ausflug“ in den Internethandelt wieder einstellen, bzw. klassische Internethändler, die vermehrt auf klassische Ladengeschäfte setzen. Zum anderen gibt es mehr und mehr Vertriebsmodelle, die den klassischen Fernabsatz bzw. e- oder m-Commerce mit dem noch klassischeren Ladengeschäft vermischen.

Als Beispiele hierfür seien genannt, die Möglichkeiten, die im Internet bestellte Ware in einem Ladengeschäft zu bezahlen oder auch im Ladengeschäft nicht geführte bzw. nicht vorrätige Ware über einen Terminal im Ladengeschäft zu bestellen. Lebensmittelhändler bieten im Internet Ware an, schließen aber ein Fernabsatzgeschäft mit der Begründung aus, der Verbraucher könne sich bei der Lieferung an der Haustür entscheiden, ob und welche Ware er erwirbt. Bei solchen Modellen muss noch einmal genau über eine Zuordnung zu den Kategorien Fernabsatz, Haustür- und Ladengeschäft nachgedacht werden. Auswirkungen wird dies nicht nur auf die Frage nach dem Bestehen oder Nichtbestehen eines Widerrufsrechts haben, sondern auch das Ob und Wann von Informationspflichten beeinflussen.

Beides – die digitalen Güter und die neuen Vertriebsformen – muss mitgedacht und bei einer Erneuerung des BGB unter dem Stichwort „Technikneutralität“ umgesetzt werden.

Adél Holdampf-Wendel

Informationspflichten beim Mobile Shopping

Informationspflichten beim Mobile Shopping

Adél Holdampf-Wendel, LL.M., BITKOM e.V.
Bereichsleiterin, Medien- und Netzpolitik, Wettbewerbs- und Verbraucherrecht

Bamberg, 11.11.2013

BITKOM

Inhalt

1. Aktuelle Zahlen zum E-Commerce auf mobilen Endgeräten
2. Status Quo & Neuerungen durch die Verbraucherrechterichtlinie
3. Perspektivische Vorschläge des BITKOM
4. Fazit

BITKOM

1. Aktuelle Zahlen zum E-Commerce auf mobilen Endgeräten

BITKOM

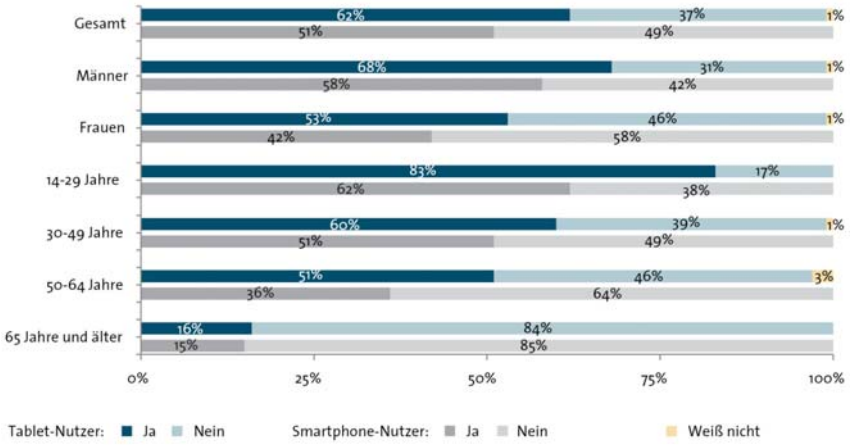
Tablet- und Smartphone-Shopping

- 62 Prozent der Tablet-Besitzer haben bereits mit ihrem Gerät online eingekauft.
- Bei den Smartphone-Nutzern hat gut die Hälfte (51 Prozent) schon einmal Einkäufe über das Handy getätigt.
- Bei den Warenkategorien wird der Erwerb von kostenpflichtigen Apps für das Mobiltelefon per Download (35 Prozent) am häufigsten genannt.
- Mit dem Smartphone werden ferner eingekauft: Produkte (22 Prozent), Download von Musik (17 Prozent), Kauf bzw. Buchung einer Dienstleistung sowie Download von Spielen (jeweils 10 Prozent).

BITKOM-Studie: Trends im E-Commerce; Konsumverhalten beim Online-Shopping, 2013

BITKOM

Tablet- und Smartphone-Shopping – nach Geschlecht und Alter



BITKOM-Studie: Trends im E-Commerce; Konsumverhalten beim Online-Shopping, 2013

BITKOM

5

Das Internet als Entscheidungshilfe im Vorfeld des Kaufs

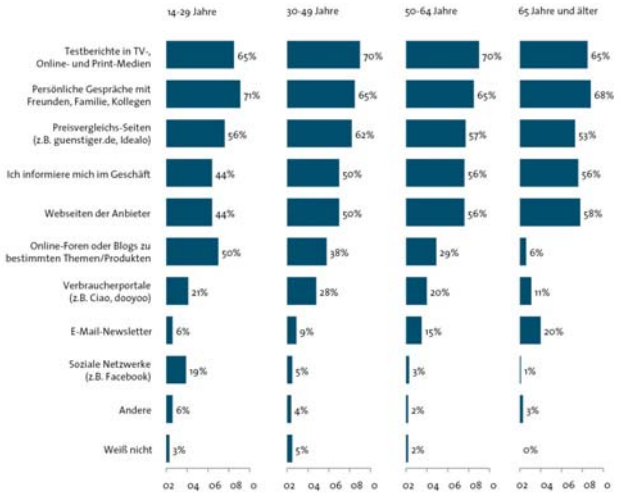
- Verbraucher informieren sich im Internet über Produkte und Anbieter – egal, ob der Kauf im Geschäft oder im Online-Shop erfolgt.
- Bei den webbasierten Entscheidungshilfen rangieren Preisvergleichsseiten ganz vorne (58 Prozent), sogar noch vor den Webseiten der eigentlichen Anbieter (51 Prozent).
- Gut ein Drittel nutzt spezielle Online-Foren oder Blogs, in denen sich die Verbraucher austauschen (35 Prozent).

BITKOM-Studie: Trends im E-Commerce; Konsumverhalten beim Online-Shopping, 2013

BITKOM

6

Entscheidungshilfen im Vorfeld des Kaufs – nach Alter



BITKOM-Studie: Trends im E-Commerce; Konsumverhalten beim Online-Shopping, 2013

BITKOM

7

2. Informationspflichten – Status Quo

BITKOM

»Lose-lose« Situation – nachteilig für die Verbraucher und die Anbieter

- Die Unternehmen sind derzeit gefordert, einen Spagat zu machen:
  - Sie bemühen sich, eine einfachere und verständlichere Sprache bei den Informationspflichten zu verwenden.
  - Sie müssen gleichzeitig sämtliche aus Gesetzen und Rechtsprechung stammenden Anforderungen erfüllen.
- Die Frage, wie sich Regelungsdichte und -tiefe mit der Aufnahmefähigkeit von Verbrauchern besser in Einklang bringen lässt, betrifft sämtliche Vertragsabschlüsse im B2C-Bereich, nicht nur online.
- M-Commerce ist im Grunde rechtlich nichts anders als E-Commerce – die Problematik spitzt sich aber im M-Commerce angesichts der eingeschränkten Platzverhältnisse zu.

BITKOM

9

Neuerungen durch die Verbraucherrechte-Richtlinie (VRRL)/1

- EU-Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25.10.2011 über Rechte der Verbraucher – in Kraft seit 12.12.2011.
- Vollharmonisierung statt Mindestharmonisierung, d.h. nationale Gesetzgeber dürfen – mit wenigen Ausnahmen – keine abweichenden Vorschriften erlassen und auch keine zusätzlichen Pflichten einführen (Art. 4 VRRL).
- »Button-Lösung« trat in Deutschland bereits zum 01.08.2012 in Kraft.
- Das Umsetzungsgesetz für die Verbraucherrechterichtlinie wurde in Deutschland durch die Abstimmungen am 14.06.2013 im Bundestag und am 05.07.2013 im Bundesrat verabschiedet.
- Die neuen Regelungen werden EU-weit ab dem 13.06.2014 anwendbar sein.
- Derzeit läuft die praktisch-technische Umsetzung dieser Bestimmungen.

BITKOM

10

Neuerungen durch die Verbraucherrechte-Richtlinie (VRRL)/2

- Art. 6 VRRL (innerstaatlich umgesetzt in Art. 246a § 1 n.F. EGBGB) regelt die Informationspflichten für den E-Commerce.
- Im Mobile Commerce-Bereich weist Art. 8 Abs. 4 VRRL (innerstaatlich umgesetzt in Art. 246a §§ 3 und 4 n.F. EGBGB) den ersten Schritt in die richtige Richtung, indem er
  - die Anzahl der unmittelbar zur Verfügung zu stellenden Pflichtinformationen im Fernabsatz bei Mobilgeräten jedenfalls einschränkt und
  - bezüglich der übrigen Informationen die Möglichkeit eröffnet, diese „in geeigneter Weise” – z.B. durch Angabe einer gebührenfreien Telefonnummer oder eines Hypertext-Links – zu erteilen.
- Diese Erleichterungen werden relativiert durch Art. 8 Abs. 7 VRRL (innerstaatlich umgesetzt in § 312f Abs. 2 n.F. BGB). Dieser fordert, dass spätestens bei der Lieferung der Ware oder bevor mit der Ausführung der Dienstleistung begonnen wird, die Informationen bezgl. des Vertragsschlusses auf einem dauerhaften Datenträger zur Verfügung zu stellen sind.

BITKOM

11

3. Perspektivische Vorschläge des BITKOM

BITKOM

Weitere Vereinfachung der Informationspflichten

- Nutzung einfacher und verständlicher Sprache;
- Fokussierung auf die für den Nutzer bzw. die Kaufentscheidung wesentlichen Angaben – ausgerichtet an dem Leitbild eines aufgeklärten und informierten Verbrauchers – ;
- Erweiterte Möglichkeiten, Informationspflichten durch Verlinkung auf Webseiten zu erfüllen – insbesondere bezgl. Informationen, die für den durchschnittlichen Nutzer für die Kaufentscheidung oder die Entscheidung zur Nutzung eines mobilen Angebots eine untergeordnete Rolle spielen.

BITKOM

13

Symbole – charmante Idee mit praktischen Umsetzungsschwierigkeiten

- Symbole können zur Verständlichkeit beitragen und sinnvoll sein, wenn sie die gegenwärtigen gesetzlichen Anforderungen ersetzen können und nicht als zusätzliche Verpflichtungen eingeführt werden.
- Gesetzlich verpflichtende und bestimmte optische Darstellungen verbergen praktische Schwierigkeiten:
  - Aufgrund der Dynamik des Mobile- bzw. E-Commerce-Marktes hätten sie ein ständiges »Hinterherlaufen« des Gesetzgebers hinter neuen technischen Entwicklungen zur Folge;
  - Symbole sind nicht zwingend selbsterklärend, so dass bei ihrer Einführung und Bekanntmachung eine auf Sprache basierte Erklärung unerlässlich erscheint;
  - Für international agierenden Unternehmen würden verschiedene optische Symbole für verschiedene Länder ein einheitliches Angebot faktisch unmöglich machen.
- Eine gesetzliche Verankerung der alternativen Nutzung von Symbolen wäre notwendig – die konkrete Ausgestaltung sollte aber durch Selbstregulierung erfolgen.

BITKOM

14

Bestätigung der Vertragsinhalte auf einem dauerhaften Datenträger bei digitalen Inhalten/1

- Art. 8 Abs. 7 VRRL (innerstaatlich umgesetzt in § 312f Abs. 2 n.F. BGB) fordert, dass spätestens bei der Lieferung der Ware oder bevor mit der Ausführung der Dienstleistung begonnen wird, die Informationen bezgl. des Vertragsschlusses auf einem dauerhaften Datenträger zur Verfügung zu stellen sind.
- Eine zu restriktive Auslegung des „Zur-Verfügung-Stellens“ birgt die Gefahr, dass wesentliche Vorteile des Geschäftsmodells des Bereitstellens von Downloads oder Streaming digitaler Inhalte durch diese Regelung erschwert oder gar gänzlich konterkariert werden. Der Verbraucher ist es bereits heute gewohnt und erwartet, dass die Übertragung digitaler Inhalte unmittelbar im Anschluss an seine entsprechende Vertragserklärung beginnt.
- Ein Absenden der Vertragsinhalte durch den Unternehmer sollte in der Praxis daher ausreichen.

BITKOM 15

Bestätigung der Vertragsinhalte auf einem dauerhaften Datenträger bei digitalen Inhalten/2

- Beim Mobile Commerce ist das Informieren des Verbrauchers in Textform über die herkömmlichen Wege (z.B. USB-Stick, CD-ROM, Speicherkarten, Festplatten und E-Mails) nicht praktikabel und oft auch technisch nicht möglich.
- Nach dem Stand der Technik sind bereits heute sogenannte fortgeschrittene Internet-Webseiten fähig, es dem Verbraucher zu ermöglichen, im Sinne der Definition des dauerhaften Datenträgers an ihn persönlich gerichtete Informationen jederzeit während eines zweckgerichteten Zeitraums unverändert wiederzugeben.
- Fortgeschrittene Internet-Webseiten sollten daher als dauerhaften Datenträger gelten.

BITKOM 16

4. Fazit

BITKOM

Eine weitere Vereinfachung der Informationspflichten ist notwendig

- E-Commerce und M-Commerce wachsen immer stärker zusammen. Aufgrund der begrenzten Displaygröße beim M-Commerce wird Unterscheidungs- oder Anpassungsbedarf weiterhin zur Erfüllung der Informationspflichten bestehen.
- Perspektivische Überlegungen für Änderungen der Bestimmungen im Anwendungsbereich der VRRL sollen auf EU-Ebene angeregt werden.
- Bei allen künftigen Lösungen soll die Rechtssicherheit für die Anbieter gewährleistet werden, indem eventuelle Vereinfachungen (z.B. mittels Symbolen) gesetzlich verankert werden, die gegenwärtigen gesetzlichen Anforderungen ersetzen können und nicht als zusätzliche Verpflichtungen eingeführt werden.
- In diesem Zusammenhang kann Selbstregulierung für die flexiblere und praxisnähere Konkretisierung der Informationspflichten ein sinnvolles Instrument darstellen, soweit dafür der Gesetzgeber klare Rahmenbedingungen und Anreize für die Beteiligung der Wirtschaftsakteure schafft.

BITKOM

18

Vielen Dank für Ihre Aufmerksamkeit.

Adél Holdampf-Wendel, LL.M.
Bereichsleiterin Medien- und Netzpolitik, Wettbewerbs- und Verbraucherrecht
00.49.30.27576-221
a. holdampf@bitkom.org

BITKOM

www.bitkom.org | www.digitalewelt.org | XING YouTube

RA Michael Neuber

Technikneutralität

1. Einleitung

Viele Diskussionen im Rahmen aktueller Gesetzgebungsvorhaben, speziell in technik- und/oder technologielastigen Regelungsbereichen sind heutzutage geprägt von Forderungen nach möglichst technikneutralen Formulierungen. Mit dem Begriff der Technikneutralität wird allerdings nicht etwa etwas grundsätzlich Neues in die gesetzgeberischen Debatten eingeführt. Es handelt sich lediglich um eine griffigere Beschreibung der Anforderung an ein jedes Gesetz, – im konkreten Falle eben unter Berücksichtigung möglicher technischer oder technologischer Besonderheiten der betroffenen Adressatenkreise – ausgewogene und nicht Einzelne belastende oder einschränkende, abstrakt-generelle Tatbestände zu enthalten. Technikneutralität ist dabei immer im Kontext der konkreten Gesetzesanwendung zu verstehen. Die zunehmende Diversität und stetige Neuerungen in Technik und Technologie stellen den Gesetzgeber vor große Herausforderungen an die Formulierung von Rechtssätzen welche weder durch eine zu große Anzahl unbestimmter Rechtsbegriffe geprägt, noch einzelne Adressaten durch eine zu einseitig auf eine bestimmte Technik oder Technologie abzielende Formulierung vom Regelungsgehalt ausnehmen und dadurch entweder unbillig belasten oder gar grundlos privilegieren sollen.

Fragen rund um die Technikneutralität bewegen sich also im Spannungsfeld zwischen der Notwendigkeit der Formulierung abstrakt-genereller Normen und dem Gebot der Normenklarheit und –bestimmtheit, um davor individuelle Einzelfälle verlässlich abbilden zu können. Technikneutrale Formulierungen knüpfen nicht an technische Merkmale oder Prozesse an. Als wichtigste Anforderung müssen gesetzliche Vorgaben unabhängig von dem konkret zur Geschäftsabwicklung genutztem technischem Gerät oder der verwendeten Technologie vor allen Dingen rechtssicher umsetzbar sein. In Zeiten zunehmender Medienkonvergenz kann es dabei zu höchst unterschiedlichen Anwendungsauswirkungen kommen je nachdem, ob eine Regelung technikneutral ausgestaltet ist, oder eben nicht. Ein hinzutretendes Erschwernis stellt der Befund dar, dass gerade technikneutrale Regelungen als Ausdruck abstrakt-genereller Regelungsbemühungen des Gesetzgebers in bestimmten Fällen nicht zu einem Weniger sondern zu einem Mehr an Belastungen für Teile des potentiellen Adressatenkreises führen können.

2. Anwendungsfall „Button-Lösung“

Für den Bereich des hier interessierenden „mobile shopping“ waren insbesondere die im Vorfeld der Umsetzung der bereits am 22.November 2011 verkündeten EU-Richtlinie 2011/83/EU über Rechte der Verbraucher (Verbraucherrechtsrichtlinie), welche zur Harmonisierung des in Europa geltenden Verbraucherrechts dienen soll, in Deutschland umgesetzten Regelungen zur Bekämpfung von Kostenfallen im Internet in der Diskussion, auch hinsichtlich geäußerter Forderungen nach technikneutralen Formulierungen[1].

Die geänderten gesetzlichen Regelungen sollen die Transparenz der einem Verbraucher vor deren Einführung bereits mitzuteilenden Informationen noch einmal erhöhen. Im Zuge der Neugestaltung wurde der bisherige § 312g in den Absätzen 2 bis 4 BGB um drei neue Absätze erweitert.

Die beabsichtigte Erhöhung der Transparenz bei Online-Geschäften zugunsten des Verbrauchers soll unter anderem durch Bereitstellung bestimmter Informationen unmittelbar vor Aufgabe der Bestellung in klar verständlicher und hervorgehobener Weise erreicht werden. Im Online-Bestellprozess muss nunmehr eine abschließende Informationen zur Zahlungspflichtigkeit zu entnehmen sein oder eine Schaltfläche („Button“), aus welcher die Zahlungspflichtigkeit hervorgeht, eingebunden werden.

Ebenso müssen gemäß § 312g Abs. 2 BGB die folgenden Verbraucherinformationen (Art. 246 § 1 EGBGB) vor Abschluss der Bestellung bereitgehalten werden:

- die wesentlichen Merkmale der Ware oder Dienstleistung
- die Mindestlaufzeit des Vertrags, wenn dieser eine dauernde oder regelmäßig wiederkehrende Leistung zum Inhalt hat

[1] vgl. Entschließungsantrag der GRÜNEN v. 29.02.2012, Drucksache 17/8806.

- den Gesamtpreis der Ware oder Dienstleistung einschließlich aller damit verbundenen Preisbestandteile sowie alle über den Unternehmer abgeführten Steuern oder, wenn kein genauer Preis angegeben werden kann, seine Berechnungsgrundlage, die dem Verbraucher eine Überprüfung des Preises ermöglicht
- gegebenenfalls zusätzlich anfallende Liefer- und Versandkosten sowie einen Hinweis auf mögliche weitere Steuern oder Kosten, die nicht über den Unternehmer abgeführt oder von ihm in Rechnung gestellt werden

Die Vorgaben gelten dabei für alle Online-Geschäfte zwischen Unternehmern und Verbrauchern (B2C) über Waren oder Dienstleistungen (mit Ausnahme von Finanzdienstleistungen) und betreffen Online-Shops ebenso wie geschlossene Verkaufsplattformen.

3. Technikneutrale Anforderungen an die Platzierung der Informationen

Die geforderten Informationen müssen dem Verbraucher unmittelbar vor Abgabe der Bestellung bereitgestellt werden. Noch im Zuge des Gesetzgebungsverfahrens wurde dabei ein gewichtiges Problem offenbar: Es sollen alle Angaben oberhalb des Bestell-Buttons und unmittelbar vor Abgabe der Bestellung angezeigt werden. Wann dieses recht unbestimmte Kriterium indes als erfüllt anzusehen ist, ist bislang nicht eindeutig entschieden.

Ausweislich der Gesetzesbegründung sah der Gesetzgeber die geforderte Unmittelbarkeit nur dann als gegeben an, wenn alle Angaben in räumlicher Nähe zum Bestell-Button und ausschließlich in sachlichem Zusammenhang mit Bestellung angezeigt werden. Ziel dieser Vorgaben soll die Möglichkeit für den Verbraucher sein, eine informierte Entscheidung bei Online-Erwerbsvorgängen treffen zu können. Der Verbraucher soll alle relevanten Informationen auf einen Blick erfassen können.

Die in § 312g Abs. 2 getroffenen Formulierungen knüpfen nicht an eine bestimmte Form der Nutzung – insbesondere stationär oder mobil - von Online-Inhalten an. Sie sind in bestem Sinne technikneutral. Eindeutige Vorgaben dazu, wann der geforderte Zusammenhang je nach praktizierter Nutzungsart durch eine bestimmte – möglicherweise technisch vorgegebene Gestaltungsmethode – entfallen kann, macht das Gesetz nicht.

Der insoweit unbestimmte Rechtsbegriff „unmittelbar bevor“ erfährt weder durch die Anknüpfung an eine bestimmte – technikabhängige – Verwendung noch in sonstiger Weise eine Konkretisierung im Gesetz selbst. Demgemäß könnten die erforderlichen Informationen bei einer Darstellung auf stationären Webseiten nicht nur zu spät, also jedenfalls nach Abschluss des Bestellvorgangs, sondern gegebenenfalls wohl auch „zu früh“, auf einer dem eigentlichen Bestellvorgang vorgeschalteten Webseite gegeben werden. Gerade bei umfangreichen Bestellvorgängen hätte es ohne weitere Begrenzung bereits im stationären Online-Bereich zu Problemen in der technischen Umsetzung der gesetzlichen Vorgaben kommen können. Ausweislich der ursprünglichen Begründung des Regierungsentwurfs[2] sollten die Informationen jedoch stets zusammen und auf der gleichen Webseite wie der Schaltfläche platziert werden.

> *“Die Aufmerksamkeit des Verbrauchers, der im Begriff ist, die Schaltfläche zu betätigen, soll sich auch auf diese Informationen richten, ohne dass trennende Gestaltungselemente davon ablenken oder den Eindruck erwecken, zwischen den Vertragsinformationen und der Bestellschaltfläche bestünde kein innerer sachlicher Zusammenhang. (...) Diese Anforderung ist nur dann erfüllt, wenn die Informationen und die Schaltfläche bei üblicher Bildschirmauflösung gleichzeitig zu sehen sind, ohne dass der Verbraucher scrollen muss. Keinesfalls genügt es, wenn die Informationen erst über einen gesonderten Link erreichbar oder nur einem gesondert herunterzuladenden Dokument entnehmbar sind.”*

Damit waren die entsprechend möglichen Rechtsunsicherheiten für den stationären Bereich zwar weitgehend beseitigt. Gleichzeitig schränkte diese enge Konkretisierung allerdings die Möglichkeiten der technischen Umsetzung zur Platzierung der Informationen stark ein und hob die zunächst technikneutrale Wirkung damit teilweise wieder auf. Denn faktisch wurde damit ein „Scrollverbot“ statuiert, ohne dass dies in Abhängigkeit möglicherweise unterschiedlicher Bildschirmauflösungen gesetzt wurde. Eine Vorgabe, welche insbesondere im Bereich des „mobile shopping“ auf kleinen Bildschirmen zur Unmöglichkeit einer rechtskonformen technischen Umsetzung geführt hätte. Dies

[2] vgl. Gesetzentwurf der Bundesregierung v. 16.11.2011, BT-Drucksache 17/7745.

wäre beispielsweise dann der Fall gewesen, wenn die erforderlichen Angaben so umfangreich wären, dass sie auf dem Bildschirm nicht dargestellt werden können – etwa wegen der Menge der bestellten Artikel oder der Informationen zur Versandabrechnung.

Auf diesen Einwand hin wurde der Gesetzesbegründung ein weiterer Nachtrag zugefügt:

> *“Eine Information des Verbrauchers, die unterhalb der Bestellschaltfläche angeordnet ist und erst durch Scrollen sichtbar wird, kann nicht sicherstellen, dass der Verbraucher die Informationen vor Abgabe der Bestellung erhält.”*

Aber selbst wenn durch diesen Nachtrag klargestellt wurde, dass ein Scrollen auf der Bestellwebseite grundsätzlich zulässig sei, finden sich keine weiteren Hinweise dazu, wann im Verlaufe eines – gegebenenfalls umfangreichen – Scrollvorgangs, der geforderte innere sachliche Zusammenhang möglicherweise trotzdem entfallen kann. Gemäß der Gesetzesbegründung haben die Anforderungen an die „Unmittelbarkeit“ nämlich sowohl einen zeitlichen wie auch einen räumlichen Aspekt. Insbesondere müssen die Informationen in räumlicher Nähe zu der Schaltfläche für die Bestellung angezeigt werden. Nimmt man dieses Erfordernis ernst, dass nicht nur ein sachlicher, sondern insbesondere auch ein räumlicher Zusammenhang aufrechterhalten bleiben muss, kann bei größeren Scrollvorgängen eben dieser Zusammenhang zwischen Erinnerung an die angebotenen Informationen und die Bestätigung der Bestellschaftfläche theoretisch entfallen.

Nichtbeachtung aber auch fehlerhafte Umsetzung der rechtlichen Vorgaben können indes gewichtige Konsequenzen haben. Ein Verstoß gegen die E-Commerce-Vorschriften des BGB stellt eine wettbewerbswidrige geschäftliche Handlung gemäß § 4 Nr. 11 UWG dar. Bei Verbraucherinformationsvorschriften handelt es sich nämlich nach Meinung der Gerichte um so genannte Marktverhaltensregeln[3]. Dies folgt aus der besonderen Bedeutung der Informationspflichten und deren Erfüllung seitens des Unternehmers beim Warenkauf im Fernabsatz auf das Marktgeschehen insgesamt. Mitbewerber können daher kostenpflichtige Abmahnungen gerichtet auf das Unterlassen (Nichtzurverfügungstellen) der gesetzlich geforderten Informationen aussprechen lassen.

Dieses Risiko besteht nicht nur bei vollständigem Unterlassen sondern auch dann, wenn die AGB nicht angepasst sind oder Bereitstellung der Informationen beispielsweise nicht wie gefordert „klar und verständlich“ und in „unmittelbarem räumlichen und zeitlichen Zusammenhang vor Abgabe der Bestellung“ erfolgt. Die insoweit technikneutrale Regelung schafft hier also ohne weitere eindeutige, technikbezogene Hinweise zu Anwendungsszenarien unnötige Rechtsunsicherheit. Letztlich werden hier die Gerichte für eine Eingrenzung und damit eine rechtssichere Herausbildung von „best-practise“-Standards sorgen müssen.

4. Technikneutrale Regelung zum Bestellvorgang

Gemäß § 312g Abs. 3 BGB ist weiterhin der Bestellvorgang so zu gestalten, dass der Verbraucher mit seiner Bestellung ausdrücklich bestätigt, sich zu einer Zahlung zu verpflichten. Weitere Vorgaben zur technischen Umsetzung macht das Gesetz nicht. Auch diese Regelung ist damit technikneutral ausgestaltet. Dies wird auch in § 312g Abs. 3 S. 2 konsequent weitergeführt. Der Gesetzgeber hatte hier erkannt, dass die Mehrzahl von Online-Bestellvorgänge durch den Klick auf einen entsprechenden „Button“ (daher „Button-Lösung“) ausgelöst werden dürften. Absatz 3 enthält daher eine weitergehende, praxisorientiere Konkretisierung hinsichtlich der Beschriftung entsprechender Klick-Buttons.

Bewusst verwendet das Gesetz hier jedoch den technikneutralen Begriff Schaltfläche, ohne sich auf eine bestimmte technische Ausgestaltung des den kostenpflichtigen Bestellvorgang auslösenden Schrittes zu beziehen. Damit sind neben dem klassischen Bestellbutton auch andere Bedienelemente erfasst, die eine ähnliche Funktion wie ein Button haben (z.B. Hyperlink oder Checkbox). Selbst ohne eine Schaltfläche sind die betreffenden Informationen gemäß Satz 1 bereitzuhalten.

Die teilweise geforderte Einführung einer Musterschaltfläche[4] dürfte vor diesem Hintergrund der gleichzeitigen Forderung nach technikneutralen Formulierungen widersprechen, zumindest aber als Einschränkung in der Gestaltung zu sehen sein. Da die Vorgaben der Button-Lösung in vollem Umfang auch für den Bereich des Mobile Commerce gelten, hätte die Gestaltung einer solchen Musterschaltfläche dann auch die

---

3 vgl. nur vgl. OLG Hamm v. 13.10.2011, MMR 2012, 29.
4 vgl. Entschließungsantrag der GRÜNEN v. 29.02.2012, Drucksache 17/8806.

unterschiedlichen Anwendungsszenarien berücksichtigen müssen. Technische Lösungsansätze sind im Vorhinein jedoch nicht planbar, weshalb eine entsprechende Umsetzung eine stetig zu erweiternde Differenzierung erfordert hätte und damit letztlich vollständig impraktikabel gewesen wäre.

5. Lösungsmöglichkeiten

Wie dargestellt sind technikneutrale Regelungen also grundsätzlich wünschenswert. In diesem Zusammenhang eingeführte unbestimmte Rechtsbegriffe bedürfen in Einzelfällen dann jedoch der bestmöglichen Konkretisierung im Gesetz selbst, je nach Maßgabe des intendierten Regelungserfolgs.

Während die Vorgaben der „Button-Lösung“ hinsichtlich der Gestaltung der Bestellfläche hinreichend konkret aber dennoch technikneutral genug ausgestaltet sein dürften, stellen sich die aufgestellten Anforderungen an die ebenfalls einzuhaltenden Informationspflichten als weniger geglückt dar. Hier wäre es wünschenswert gewesen, die aus der Diskussion um die Formulierung des Gesetzestextes gewonnenen Erkenntnisse direkt in den Gesetzestext selbst mit einfließen zu lassen, anstatt erneute Rechtsunsicherheit für die Adressaten zu schaffen und die Konkretisierungsverantwortung einmal mehr den Gerichten zu überlassen.

Eine mögliche Konkretisierung könnte möglicherweise folgendermaßen lauten:

> *“Die Unmittelbarkeit ist im Sinne dieser Vorschrift gewahrt, soweit sämtliche Informationen entweder auf einen Blick ersichtlich oder in einem unterbrechungsfreien Anzeigevorgang (Scrollen) unabhängig von dessen Umfang nacheinander angezeigt werden und die so präsentierte Übersicht mit dem Bestellvorgang oder einer dafür bereitgehaltenen Schaltfläche abgeschlossen wird.”*

6. Fazit

Technikneutralität ist zunächst kein grundsätzliches, gesetzgeberisches Gebot sondern stellt einen besonderen Berücksichtigungsfaktor im Rahmen ausgewogener gesetzgeberischer Bemühungen dort dar, wo es um die Regelung technischer/technologischer Sachverhalte geht. Als weiteres Beispiel mag die Diskussion um einzelne Formulierungen des am 1. August 2013 in Kraft getretenen E-Government-Gesetzes dienen. Das Gesetz dient dem Ziel, die elektronische Kommunikation mit der Verwaltung zu erleichtern und Bund, Ländern und Kommunen zu ermöglichen, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten. Das Gesetz soll Behörden dazu zwingen, den Zugang via De-Mail zu eröffnen und damit zur breiten Durchsetzung dieser Technik beitragen. Diese offensichtliche Bevorzugung einer bestimmten Form der elektronischen Kommunikation stieß auf Kritik[5]. Namentlich wurde eine technikneutralere Regelung gefordert, welche auch andere Dienste, nämlich

> *„sonstige bundeseinheitliche Übermittlungswege, bei denen die Authentizität und Integrität der Daten gewährleistet werden und im Falle der Nutzung allgemein zugänglicher Netze ein Verschlüsselungsverfahren angewandt wird, das die Vertraulichkeit der übermittelten Daten sicherstellt”,*

erfasst oder zumindest keinen Zwang zur Einrichtung eines DE-Mail-Kontos enthält.

Während in vielen Fällen also technikneutrale Gesetzesformulierungen die Gefahr von Marktverzerrungen durch staatliche Maßnahmen minimieren und daher nicht nur wünschenswert, sondern aus rechtsstaatlicher Sicht notwendig sind, zeigen andere Anwendungsfälle, dass eine unbesehene Fokussierung auf technikneutrale Formulierungen möglicherweise unterschiedlich zu behandelnde Sachverhalte dort „über einen Kamm schert“ werden kann, soweit der Gesetzgeber die vor dem Hintergrund des eigentlichen Regelungszwecks möglicherweise auftretenden Güterbeeinträchtigungen nicht ausreichend berücksichtigt.

Diskutiert wurden entsprechende Folgen beispielsweise im Zusammenhang mit der Einführung des Gesetzes zur Neuregelung des Rechts der Erneuerbaren Energien im Strombereich und zur Änderung damit zusammenhängender Vorschriften (EEG), welches eine technikneutrale Differenzierung der Vergütungshöhen je nach Ertragskraft des Standorts vorsehen. Gefordert wurden hier differenzierendere Regelungen je nach Anbieter, wegen möglicher Nichtberücksichtigung der mit den verschiedenen Techniken verbundenen Investitionsunterschiede.

---

[5] vgl. Stellungnahme des Bundesrats v. 02.11.2012, BR-Drucksache 557/12 sowie Diskussionsentwurf des Bundesministeriums der Justiz zum Entwurf eines Gesetzes zur Förderung des elektronischen Rechtsverkehrs bei den Gerichten.

Allein die Technikbezogenheit möglicher Regelungsbereiche entfaltet also kein grundsätzlich zu forderndes Gebot der Technikneutralität. Sie materialisiert sich je nach Regelungsgegenstand lediglich als Ausdruck ausgewogener Gesetzgebung, wobei Besonderheiten und mögliche Unterschiede zwischen den verschiedenen Techniken oder Technologien stets mit zu beachten und gegebenenfalls gesondert zu regeln gilt.

Martin Schmidt-Kessel

Verträge über digitale Inhalte – Einordnung und Verbraucherschutz

Verträge über digitale Inhalte sind inzwischen ein eigener rechtspolitischer und rechtssystematischer Topos. Sie sind damit im Begriff, sich aus der – für den Alltagsjuristen immer noch schlecht erschlossenen – Welt des „Internet-Rechts“ hinaus zu entwickeln und Gegenstand allgemeiner rechtspolitischer wie rechtswissenschaftlicher Betrachtung zu werden. Mit der Umsetzung der Richtlinie 2011/83/EU über die Rechte des Verbrauchers wird der Vertrag über digitale Inhalte zum 13. Juni 2014 auch normativ Einzug in das deutsche Recht halten.

Die Etablierung als allgemein privatrechtlicher Topos bedeutet freilich nicht, dass im Bereich digitaler Inhalte nicht noch viel in Bewegung wäre. Das betrifft begriffliche Einordnungen und tatsächliche Eigenheiten ebenso wie die urheberrechtliche Determinierung und die Vertragstypenzuordnung. Diese Bewegung steht auch in Zusammenhang mit neuen Fragen nach Bedarfen für den Verbraucherschutz, von denen hier drei kurz angetippt werden sollen, nämlich das Widerrufsrecht, ferner die Qualität und schließlich Fragen von Nutzungsbeschränkungen und Weiterveräußerung.

I. Begriff digitaler Inhalte

Als neuen technischen Begriff definieren sowohl die Verbraucherrechterichtlinie 2011/83/EU als auch das deutsche Umsetzungsgesetz[1] den Begriff der digitalen Inhalte im Gesetz. Danach sind digitale Inhalte „Daten, die in digitaler Form hergestellt und bereitgestellt werden“ (Art. 2 lit. l VerbraucherrechteRL, § 312f. III BGB n.F.). Weitere materielle Voraussetzungen kennen die betreffenden Definitionen nicht. Was die Parteien im Einzelnen zum Gegenstand des Vertrages über digitale Inhalte machen, ist also ihnen überlassen, solange es sich eben um Daten in digitaler Form handelt. Trotz dieser formalen Offenheit des Begriffs digitaler Inhalte hat sich der europäische Gesetzgeber zusätzlich zu einer Klarstellung veranlasst gesehen: In Erwägungsgrund (19) der VerbraucherrechteRL werden beispielhaft genannt „Computerprogramme, Anwendungen (Apps), Spiele, Musik, Videos oder Texte“. Von den klassischen Inhalten fehlen in dieser Aufzeichnung vor allem Bilder.

Systematisch steht der Begriff digitale Inhalte damit auf einer Stufe etwa mit dem Sachbegriff des deutschen BGB (§ 90 BGB), der auch lediglich formal umschrieben ist.[2] Diese systematische Stellung als Rechtsobjekt wird zusätzlich durch einen Zusatz im Erwägungsgrund (19) VerbraucherrechteRL verdeutlicht: die Richtlinie stellt ausdrücklich klar, dass die Qualifikation als digitale Inhalte unabhängig davon ist, wie von den Parteien mit diesen unter dem Vertrag verfahren wird. Erwägungsgrund (19) nennt beispielhaft „Herunterladen oder Herunterladen in Echtzeit (Streaming)“ sowie die Zugriffsweisen „von einem körperlichen Datenträger oder in sonstiger Weise“. Für das Gemeinsame Europäische Kaufrecht hat die Kommission die Übernahme der Definition vorgeschlagen.[3]

Die dem europäischen wie auch dem deutschen Verständnis digitaler Inhalte eigene Unabhängigkeit von dem mit diesen verbundenen Verfahrensweisen lässt freilich von vornherein Zweifel daran aufkommen, ob der „Vertrag über digitale Inhalte“ tatsächlich als sinnvoll etabliert werden kann. Er wäre etwa ebenso spezifisch wie ein „Vertrag über Sachen“, der nicht nach Übertragung, Gebrauchsüberlassung oder Instrumentalität derselben differenziert.[4]

---

1 Zu diesem bereits Wendehorst, NJW 2014, 577 sowie die Beiträge von *Tonner, Schmidt/Brönneke, Leier, Tamm und Schomburg* in der VuR Hefte 12/2013 und 1/2014.

2 Dazu noch unten sub IV 3.

3 S. Schmidt-Kessel/*Schmidt-Kessel*, Art. 2 GEK-VO Rn. 44 ff.

4 Dazu noch unten sub IV.

II. Tatsächliche Eigenheiten digitaler Inhalte

Digitale Inhalte verfügen über eine Reihe technischer Eigenheiten, die sie auch für die Gestaltung vertraglicher Regeln als besonders erscheinen lassen: Zentrales Charakteristikum ist die verlustfreie Kopierbarkeit in dem Sinne, dass sich von digitalen Inhalten beliebig viele Kopien erstellen lassen, die hinsichtlich ihrer Qualität vom Original nicht zu unterscheiden sind und insbesondere keine Qualitätseinbußen gegenüber dem Original erleiden. Diese verlustfreie Kopierbarkeit führt dazu, dass im Rechtsverkehr (und außerhalb desselben) digitale Inhalte in der Regel nicht weitergegeben werden, sondern Gegenstand der Verbreitung sind: Der Verbreitende gibt seinen Zugriff auf seine Kopie der digitalen Inhalte in aller Regel nicht auf. Selbst wenn er dieses tut, ist dieser Aufgabeakt in aller Regel tatsächlich unabhängig vom Akt der Verbreitung, muss also gesondert geschehen.

Zweites Charakteristikum digitaler Inhalte ist ihre Hardware- und Systemabhängigkeit, welche regelmäßig erst die Nutzung ermöglicht, respektive die Nutzbarkeit sicherstellt. Das Gebrauchmachen von digitalen Inhalten setzt dementsprechend voraus, dass die Handelnden über die nötigen Hardware- und Systemvoraussetzungen verfügen.

III. Urheberrechtliche Determinierung rechtlicher Inhalte?

In juristischen Auseinandersetzungen um Verträge über digitale Inhalte spielen häufig Aspekte des Urheberrechts eine wesentliche Rolle. Das gilt sowohl dogmatisch für die Vertragstypenqualifizierung, als auch rechtspolitisch für die Frage, welche Rechte den Parteien standardmäßig zustehen und welche Vereinbarungen insbesondere zu Lasten von Verbrauchern getroffen werden können.

1. Ausgangspunkt: Keine Erschöpfung nach § 17 II UrhG

Der urheberrechtliche Erschöpfungsgrundsatz, wonach sich das Verbreitungsrecht des Urhebers hinsichtlich des einzelnen Werkstücks erschöpft, sobald der Urheber oder ein anderer von ihm dazu Berechtigter dieses Werkstück unter Eigentumsübertragung in Verkehr gebracht hat, gerät bei digitalen Inhalten an seine Grenzen. Die in ihm verschlüsselte Idee, dass der Urheber mit der einverständlichen Weitergabe seine angemessene Vergütung für das betreffende Werkstück bereits erhalten hat, funktioniert bei freier Kopierbarkeit nur eingeschränkt.

Es überrascht daher nicht, dass die Rechtsprechung klassischerweise den Erschöpfungsgrundsatz auf Fälle der Verbreitung körperlicher Werkexemplare beschränkt hat.[5] Dementsprechend kommt – nach der lange Zeit völlig überwiegenden Auffassung[6] – eine Erschöpfung bei digitalen Inhalten klassischerweise nicht in Betracht.[7] Der deutsche Gesetzgeber hat diese Abgrenzung nach dem Körperlichkeitskriterium 2003 partiell in § 19a UrhG festgeschrieben. Schwierigkeiten ergeben sich mit dieser Vorschrift freilich daraus, dass das Kriterium „zu Zeiten ihrer Wahl“ der öffentlichen Zugänglichkeit nicht alle Verbreitungswege digitaler Inhalte erfasst. Folglich zieht auch diese Festschreibung Unsicherheiten nach sich, insbesondere bei den sog. Push-Diensten mit Aufzeichnung beim Empfänger. Nach herrschender Auffassung soll hier keine Erschöpfung eintreten, während eine Mindermeinung hier die Anwendbarkeit von § 17 II UrhG für gegeben hält.

2. Sonderregeln für Software und Datenbanken

Für Software enthält § 69c Nr. 3 UrhG in Umsetzung von Art. 4 II RL 2009/24/EG (zuvor Art. 4 lit. c RL 91/250/EWG) eine Sonderregel zur Erschöpfung. Nach bislang herrschender Auffassung in Deutschland setzt freilich auch nach dieser Sonderregelung die Erschöpfung des Verbreitungsrechts ein körperliches Werkstück voraus, so dass die Erschöpfung des Urheberrechts an Software nur bei deren Übermittlung auf Datenträger eintreten soll. Hingegen ist die reine Online-Übermittlung nicht erfasst. Zudem ist § 69c Nr. 3 UrhG nach herrschender Auffassung hinsichtlich anderer Gegenstände als Software nicht analogiefähig. Ohnehin ermöglicht die Erschöpfung nach § 69c Nr. 3 UrhG dem Erwerber kein völlig freies Verfahren mit der erworbenen Software, weil die Erschöpfung die Möglichkeit einer Weitervermietung nicht erfasst.

---

5 Statt aller EuGH, C-456/06, 17. 4. 2008 – *Le Corbusier-Möbel II*.
6 Zur neueren Entwicklung siehe sogleich sub II.
7 Zu den Ausnahmen siehe sogleich sub. II.

Entsprechend ausgestaltet ist die erschöpfungsrechtliche Sonderregel für Datenbanken in §§ 87b II, 17 II UrhG, welche Art. 6 II lit. b RL 96/9/EG in das deutsche Recht umsetzt. Auch hier soll die Erschöpfung nach herrschender Auffassung nur bei Vorliegen körperlicher Vervielfältigungsstücke eintreten, so dass wiederum eine Übermittlung auf Datenträger erforderlich ist, während der reine Online-Vorgang für die Erschöpfung nicht ausreicht. Auch die Erschöpfung nach §§ 87b II, 17 II UrhG berechtigen den Erwerber nicht zur Weitervermietung.

Beide Sonderregeln ändern in ihrer Auslegung durch die bislang herrschende Meinung nichts an der Erforderlichkeit eines körperlichen Werkstücks für die Erschöpfung. Die herrschende Auffassung hat hier bis zuletzt die Ansicht vertreten, durch eine reine Online-Übermittlung könne Erschöpfung nicht eintreten.

3. Die UsedSoft-Entscheidung des Europäischen Gerichtshofs

Mit seiner am 3. Juli 2012 verkündeten Entscheidung in der Rechtssache UsedSoft GmbH gegen *Oracle International Corp.*[8] hat nun der Europäische Gerichtshof eine bahnbrechende Weiterentwicklung des Erschöpfungsgrundsatzes auch für digitale Inhalte vorgenommen.

Die im ursprünglichen Verfahren auf Unterlassung des Vertriebs gebrauchter Softwarelizenzen in Anspruch genommene UsedSoft GmbH handelt mit ebensolchen gebrauchten Softwarelizenzen. Für diesen Handel erwirbt sie bei Kunden von Oracle solche Nutzungslizenzen oder Teile davon, wenn dort Überkapazitäten vorliegen. Das ist vor allem dann der Fall, wenn die von diesem Kunden ursprünglich erworbenen Lizenzen für eine ihren Bedarf übersteigende Nutzerzahl gelten. Diese Kunden haben jeweils ihre Software als Ersterwerber durch Download von Oracle erworben; Übertragungen auf Datenträger finden regelmäßig nicht statt. Bei der nunmehr von Oracle vor den deutschen Gerichten angestrengten Unterlassungsklage kam es nun darauf an, ob UsedSoft zu der in seinem Geschäftsmodell eingeschlossenen Übertragung von Nutzungsrechten deshalb berechtigt war, weil durch den Download der Ersterwerber Erschöpfung an den jeweiligen Software-Kopien eingetreten war.

In Abweichung von der bislang – jedenfalls in Deutschland – herrschenden Auffassung hält der Gerichtshof den Eintritt von Erschöpfung nach Art. 4 II RL 2009/24/EG nunmehr bei Software grundsätzlich auch in reinen Download-Fällen für möglich. Voraussetzung dafür sei die Zustimmung des Inhabers zum Herunterladen der Kopie durch den Ersterwerber (auch soweit dieser Download selbst unentgeltlich ist), ferner die Zahlung eines Entgeltes (das bei unentgeltlichem Download für die nachträgliche Lizenzeinräumung zu entrichten ist) und schließlich die Einräumung eines Nutzungsrechts ohne zeitliche Begrenzung. Bei Vorliegen dieser drei Voraussetzungen sieht der EuGH im Ergebnis einen zweiten und auch jeden weiteren Erwerber durch die beim Ersterwerber eingetretene Erschöpfung geschützt.

4. Deutsche Reaktionen auf UsedSoft

Die Entscheidung des Europäischen Gerichtshofs ist gerade bei den Spezialisten des Urheberrechts als „Paukenschlag“ aufgenommen worden.[9] Die soeben veröffentlichte Folgeentscheidung des Bundesgerichtshofs,[10] auf dessen Vorlage hin der Europäische Gerichtshof entschied, muss sich dementsprechend mit ganz grundlegenden Angriffen auf die Bindungswirkung des Luxemburger Entscheids auseinandersetzen: Jedoch sieht der Erste Zivilsenat weder einen Verstoß gegen den WIPO-Urheberrechtsvertrag noch einen mit Art. 345 AEUV unvereinbaren Eingriff in die Eigentumsordnung der Mitgliedstaaten als gegeben an.

In der Sache weicht der Senat freilich in einem wichtigen Punkt von der Entscheidung des Europäischen Gerichtshofs ab und verlangt für die Erschöpfung zusätzlich, dass der Ersterwerber seine Kopie unbrauchbar gemacht hat.[11] Diese zusätzliche Voraussetzung ist in der EuGH-Entscheidung nicht enthalten und konterkariert – insbesondere unter Berücksichtigung der dem Nacherwerber auferlegten Beweislast – die Wirkungen

8 EuGH, Rs. C-128/11, 3. 7. 2012 – *UsedSoft/Oracle International*.
9 *Grützmacher*, ZGE 5 (2013), 46; die Formulierung übernehmend *Stieper*, NJW 2014, 270.
10 BGH GRUR 2014, 264.
11 BGH GRUR 2014, 264, Rn. 63 f.

der Entscheidung in signifikanter Weise. Ohne eine weitere Vorlage nach Luxemburg wird sich dieses zusätzliche Kriterium kaum halten lassen. Es ist auch nicht deckungsgleich mit dem – für das Geschäftsmodell von UsedSoft desaströsen – Verbot der Aufspaltung von Lizenzen.[12]

Hilfreich ist hingegen die zusätzliche Konkretisierung hinsichtlich Verbesserungen und Aktualisierungen der Software, für die der Senat darauf hinweist, dass auch insoweit eine urheberrechtliche Grundlage bestehen müsse.[13] Die vorgenommene Beschränkung auf einen Wartungsvertrag ist dabei freilich lediglich als beispielhaft anzusehen. Für einzeln „nachgekaufte“ Updates kann nichts anderes gelten. Umgekehrt ist die Formulierung des Senates zu weit geraten, wo sog. Patches der Mangelbeseitigung hinsichtlich der ursprünglichen Software dienen: Insoweit kann der Urheberrechtsinhaber durch nachträgliche Mangelbeseitigung die eingetretene Erschöpfung nicht wieder rückgängig machen, weil die Nachbesserungsleistungen gleichfalls an der Erschöpfung teilhaben.

In der instanzgerichtlichen Rechtsprechung sind weitere Klärungen teilweise bereits erfolgt, teilweise ist ein Diskussionsprozess angestoßen. So hat das Hanseatische OLG Hamburg darauf hingewiesen, dass als Folge der (zwingenden) Erschöpfungswirkung die Einschränkungen der Vereinbarkeit von Weitergabeverboten nunmehr auch für solche Software gelten, die lediglich online übermittelt worden ist, soweit nur die weiteren Voraussetzungen der Erschöpfung vorliegen.[14] Andererseits ist bereits unterinstanzlich entschieden worden, dass eine Übertragung der in der UsedSoft-Entscheidung für Software entwickelten Grundsätze zur Erschöpfung bei unkörperlichen Kopien auf andere digitale Inhalte nicht in Betracht komme.[15] Das ist um so bedeutsamer, als die Sonderregeln für Software solche digitalen Inhalte nicht erfassen, bei denen die Software lediglich der Kodierung einer anderweitig urheberrechtlich relevanten Schöpfung dienen – ein wichtiges Beispiel sind Videospiele.[16]

5. Folgerungen für Verbraucherverträge

Für Verbraucherverträge über digitale Inhalte hat die so geschilderte urheberrechtliche Rechtslage zunächst einmal die Konsequenz, dass auch der Verbraucher für digitale Inhalte des Erwerbs einer Nutzungsberechtigung (Lizenz) bedarf. Bei Software kann sich diese Nutzungsberechtigung aber auch schon qua Erschöpfung durch den Erwerb von (entgeltlichen) Ersterwerber ergeben; das ist die wesentliche Konsequenz der UsedSoft-Entscheidung des Europäischen Gerichtshofs. Ob und inwieweit sich diese Erschöpfungslösung – und damit die echte Verkehrsfähigkeit der digitalen Inhalte – auch auf andere Arten digitaler Inhalte übertragen lässt, ist bislang fraglich.[17] Aus verbraucherrechtlicher Sicht ist die Herstellung der Verkehrsfähigkeit jedoch zweifellos wünschenswert. Damit läge das Verbraucherrecht auch im Trend der allgemeinen Rechtsentwicklung, die dahin geht, Beschränkungen der Verkehrsfähigkeit digitaler Inhalte zurückzudrängen.

IV. Vertragstypenzuordnung

Angesichts der Besonderheiten digitaler Inhalte als Leistungsgegenstand und auch angesichts der ersten Regelungen stellt sich die Frage, welchen Vertragstypen solche Verträge zuzuordnen sind oder ob angesichts der Eigenheiten digitaler Inhalte die Entwicklung eigenständiger Vertragstypen erforderlich ist. Letzteres legt jedenfalls die Entwicklung der VerbraucherrechteRL – verstärkt durch den Vorschlag für das Gemeinsame Europäische Kaufrecht (GEKR) – nahe. Diese Frage ist keine rein akademische, weil auch im Unionsprivatrecht Sachfragen über dogmatische Zuordnungen (mit-)entschieden werden. Dabei stehen zwei Strukturfragen zur Beantwortung an: Welches ist der – vertragstypologisch zu erfassende – Leistungsgegenstand bei Verträgen über digitale Inhalte? Und: spielt die Frage der Entgeltlichkeit oder Unentgeltlichkeit eine wesentliche Rolle?

---

12 Dafür in der Tat EuGH, Rs. C-128/11, 3. 7. 2012 – *UsedSoft/Oracle International*, Rn. 86; ebenso nun OLG Frankfurt, GRUR 2013, 279; LG Frankfurt, MMR 2013, 125.
13 BGH GRUR 2014, 264, Rn. 62.
14 HOLG Hamburg, MMR 2014, 115. Zu Weitergabeklauseln s.u. sub. V 3.
15 In diesem Sinne LG Bielefeld, GRUR-RR 2013, 281.
16 Siehe zuletzt EuGH Rs. C-355/12, 23. 1. 2014 – *Nintendo/PC Box*, insbesondere Rn. 23.
17 S. o. sub. 4. und die Nachweise dort.

1. Entwicklung eigener Vertragstypen für die digitale Welt?

Auf den ersten Blick ergeben sich für die Vertragstypenzuordnung ganz erhebliche Besonderheiten durch die Abhängigkeit der Vertragsgestaltung von der urheberrechtlichen Nutzungsbefugnis. Auf den zweiten Blick finden sich je nach tatsächlicher Gestaltung Differenzierungen: Teilweise besteht eine offensichtliche Ähnlichkeit zu Waren, teilweise ähneln die Verträge Gebrauchsüberlassungsverträgen wie der Miete und teilweise geht es um Dienstleistungen.

Die nicht nur von interessierter Seite immer wieder ins Spiel gebrachte Abhängigkeit des Vertragstyps von der urheberrechtlichen Nutzungsbefugnis ist zumindest teilweise auch Ausdruck einer begrenzten Trennung respektive Abstraktion von dinglicher (urheberrechtlicher) Rechtslage und schuldrechtlichem Pflichtenprogramm. Durch die mit der UsedSoft-Entscheidung eingeleitete Entwicklung zu einer verstärkten Trennung beider Ebenen und die Herstellung der Verkehrsfähigkeit digitaler Inhalte ist diese Abhängigkeit deutlich gelockert worden. Das zeigt sich teilweise bis in die Urteilsbegründungen der deutschen Gerichte.

Durch die Verkehrsfähigkeit digitaler Inhalte wird aber auch die Ähnlichkeit von Verträgen über digitale Inhalte zu Warenverkehrsgeschäften deutlich. Das gilt insbesondere bei der vom EuGH in der UsedSoft-Entscheidung geforderten Dauerhaftigkeit der Rechteeinräumung gegenüber dem Ersterwerber (*permanent license*). Die Ähnlichkeit zum Warenverkehr wird dort besonders deutlich, wo die Bereitstellung digitaler Inhalte auf einem körperlichen Datenträger wie einer CD oder einer DVD erfolgt und das Unionsprivatrecht in Gestalt von Erwägungsgrund (19) RL 2011/83/EU von deren Behandlung als Waren ausgeht.

Zugleich ist die Verwandtschaft zu Gebrauchsüberlassungen von Sachen unverkennbar: An digitalen Inhalten wird eine Nutzungsbefugnis ohne volle eigene Rechtsinhaberschaft begründet. Diese Ähnlichkeit zur Gebrauchsüberlassung bereitet freilich schon deshalb Schwierigkeiten, weil das Unionsrecht traditionell Gebrauchsüberlassungsverträge vernachlässigt, wenn es in der Sprache des Binoms „Waren und Dienstleistungen” spricht. Bei Verwendung dieses Binoms wird nämlich nicht von vorn herein deutlich – und ist häufig auch sehr umstritten –, wie Gebrauchsüberlassungsverträge einzuordnen sind. Diese Undifferenziertheit des Unionsrechts wird nun auch für die Einordnung von Verträgen über digitale Inhalte zum Problem.

Schließlich ähneln Verträge über digitale Inhalte immer auch Dienstleistungen. Diese Ähnlichkeit ergibt sich primär aus der Immaterialität des Leistungsgegenstandes, wie er für digitale Inhalte selbstverständlich und für Dienstleistungen immerhin die Regel ist. Dieser Gleichlauf hat nicht selten dazu geführt, Verträge über digitale Inhalte in der bisher dualistischen Systematik „Waren und Dienstleistungen“ generell als Verträge über Dienstleistungen einzuordnen. Darüber hinaus haben Verträge über digitale Inhalte und über Dienstleistungen die Anknüpfung an die Funktionalität der erbrachten Leistung gemeinsam. Genau genommen ist dieser Anknüpfung jedoch nicht nur eine Eigenheit von Dienstleistungen und digitalen Inhalten, sondern wird auch bei Waren relevant, wie sich unschwer an der Anknüpfung an die Verwendungszwecke der Kaufzwecke zeigen lässt.

Die VerbraucherrechteRL tendiert unübersehbar zu einem weiten Verständnis und zu einer Zwischenstellung von Verträgen über digitale Inhalte. Dies zeigt sich bereits daran, dass die Einordnung nach Erwägungsgrund (19) RL 2011/83/EU „unabhängig davon“ sein soll, „ob sie durch Herunterladen oder Herunterladen in Echtzeit (streaming), von einem körperlichen Datenträger oder in sonstiger Weise zugegriffen wird“. Die Zwischenstellung macht die Richtlinie ebenfalls im Erwägungsgrund (19) deutlich: Verträge über digitale Inhalte seien „vergleichbar mit Verträgen über die Lieferung von Wasser, Gas oder Strom, wenn sie nicht in einem begrenzten Volumen oder in einer bestimmten Menge zum Verkauf angeboten werden oder über die Lieferung von Fernwärme“. Daher so die Schlussfolgerung des europäischen Gesetzgebers – „sollten Verträge über digitale Inhalte, die nicht auf einem körperlichen Datenträger bereitgestellt werden, für die Zwecke dieser Richtlinie weder als Kaufverträge noch als Dienstleistungsverträge betrachtet werden“. Mit diesen tertium datur scheint die Richtlinie nunmehr einen eigenen Vertragstyp etablieren zu wollen. Dem ist freilich entgegen zu treten.

2. Zu klärende Sachfragen

Die durch die Zuordnung von Verträgen über digitale Inhalte zu bestimmten Vertragstypen betroffenen Sachentscheidungen geraten vor dem Hintergrund dogmatischer Debatten nicht selten etwas in den Hintergrund. Dabei geht es zunächst um die Vertragsschlusssituation, bei der aus Sicht des Verbraucherschutzes vor allem Fragen des Schutzes vor dem nicht oder nicht so gewollten Vertrag im Mittelpunkt stehen. Das betrifft zunächst erschlichene Vertragsschlüsse (wie etwa in den Fällen des § 241a BGB oder der Kostenfallen), ferner Überrum-

pelungssituationen und mangelnde Kenntnis vom Leistungsgegenstand; das Vertragsrecht sucht diese Gefährdungssituationen durch Statuierung von Unwirksamkeiten, Widerrufsrechten und Informationspflichten zu entschärfen.

Der zweite zentrale Fragenkreis betrifft die Behandlung von Qualitätsdefiziten, also die herkömmlich sogenannte Sachmängelgewährleistung. Dabei kann es auch um Mängel der Daten selbst gehen, vor allem stehen jedoch Fragen der Funktionsfähigkeit im Mittelpunkt, die durch die Kompatibilitätsdebatte und die nachfolgend statuierten Anforderungen eine neue Facette erhalten haben: Die Kompatibilität digitaler Inhalte zählt wegen deren System- und Hardwareabhängigkeit zu den zentralen Qualitätsbestimmungsmechanismen des Rechts der digitalen Inhalte. Im Blick auf die wachsende Verkehrsfähigkeit digitaler Inhalte stellen zudem Kopierschutzmechanismen im Grundsatz legitime, in ihren Wirkungen häufig jedoch vertragswidrige Funktionsbeschränkungen dar. Auch an dieser Stelle muss das Zusammenspiel der neuen Welt digitaler Inhalte mit den klassischen Vertragsrechtsmechanismen erst noch optimiert werden.

Ein ganz eigenes Charakteristikum digitaler Inhalte bilden die besonderen Fragen der Nutzungsbeschränkungen und der Weiterveräußerungsbefugnis, die schuldrechtlich mit den Mitteln der Sach- oder Rechtsmängelhaftung bislang nicht hinreichend in den Griff zu bekommen sind. Grundsätzliche Schutzbedürfnisse der Urheber und anderen immateriell Berechtigten werden hier vermutlich immer einen gewissen Restbestand an Nutzungsbeschränkungen erhalten, zu denen nach dem Stand der Dinge Weiterveräußerungsverbote sicher nicht, dafür aber vermutlich Beschränkungen der Vermietbarkeit digitaler Inhalte, gehören werden.

3. Leistungsgegenstand digitale Inhalte?

Die RL 2011/83/EU über die Rechte der Verbraucher bildet nur einen allerersten Schritt zu einer befriedigenden vertragstypologischen Erfassung von Verträgen über digitale Inhalte. Zunächst ist die Richtlinie – und notgedrungen auch das Umsetzungsgesetz – zu undifferenziert, indem nicht nach der Art und Weise des Umgangs mit den digitalen Inhalten differenziert wird. Dies entspricht bereits im Blick auf die Anforderungen des Erschöpfungsgrundsatzes und der Nichterfassung der Weitervermietung durch denselben bereits nicht der immaterialgüterrechtlichen Rechtslage und ist daher zur Lösung der auftretenden schuldrechtlichen Sachfragen nicht hinreichend geeignet. Überdies hat die pauschale Erfassung sämtlicher Verträge über digitale Inhalte dazu geführt, dass der Schutz des Verbrauchers in einschlägigen Vertragskonstellationen häufig auf den kleinsten gemeinsamen Nenner reduziert wird und konsequenterweise reduziert werden muss. Eine einheitliche Behandlung sämtlicher Verträge über digitale Inhalte führt daher nicht zu einem angemessenen Verbraucherschutzniveau.

Digitale Inhalte sind Rechtsobjekte und als solche Funktionsäquivalente zu Sachen (im Sinne von § 90 BGB). Eine sachgerechte Regelung von Verträgen über digitale Inhalte muss daher zunächst einmal den Umstand berücksichtigen, dass das Rechtsobjekt selbst nicht Leistungsgegenstand ist, vielmehr eine Aktivität mit Bezug auf den digitalen Inhalt, etwa die dauerhafte Übertragung, Verschaffung und Belassung, die vorübergehende Nutzungsbefugnis oder die Instrumentalität bei Erbringung anderer Leistungen. Dem Regelungsansatz des europäischen Gesetzgebers fehlt daher eine Zwischenebene, wie es sie auch in der analogen Welt selbstverständlich gibt: Zum Leistungsgegenstand vertraglicher Ansprüche zählen nicht nur (und nicht einmal notwendig) Rechtsobjekte, vielmehr wird der Leistungsgegenstand maßgeblich dadurch bestimmt, was mit in Bezug genommenen Rechtsobjekten geschehen soll.

4. Ein differenziertes Vertragstypensystem für digitale Inhalte

Zieht man – dogmatisch oder legislativ – die soeben geforderte Zwischenebene der Aktivität mit Bezug auf digitale Inhalte ein, ergibt sich ein deutlich differenziertes Bild möglicher Vertragstypen:

An erster Stelle steht der Kauf digitaler Inhalte. Er ist auf die dauerhafte Übertragung und Verschaffung der Daten, der Nutzungsmöglichkeit und der Nutzungsberechtigung gerichtet. Dinglich ist er mit der Erschöpfung des Verbreitungsrechts verbunden. Schuldrechtlich finden die Regeln über Waren und Warenkäufe Anwendung, wobei die Anordnung der entsprechenden Anwendung durch § 453 I BGB die notwendigen Anpassungen an digitale Inhalte und ihre Besonderheiten ermöglicht. Nachlaufende Verpflichtungen des Verkäufers hinsichtlich der Funktionsfähigkeit digitaler Inhalte und deren Erhaltung sind hier gesondert begründungsbedürftig.

Verträge über die Gebrauchsüberlassung digitaler Inhalte im Wege von Miete oder Pacht sind auf die Verschaffung, Belassung und Erhaltung der Nutzungsmöglichkeit digitaler Inhalte gerichtet. Dies wird vielfach

auch eine Datenverschaffung beinhalten, welche bei Beendigung des Gebrauchsüberlassungsverhältnisses statt der Rückgabe eine Löschungspflicht entstehen lässt. Das ist freilich nicht notwendig der Fall, wie das Beispiel der Einräumung der Nutzungsmöglichkeit von Software as a Service (SaaS) etwa in Cloud-Systemen zeigt. Auch wenn die Abgrenzung zur Dienstleistung schon begrifflich in diesen Konstellationen nicht einfach ist, werden auch hier Konstellationen von Gebrauchsüberlassungen anzunehmen sein, insbesondere dort, wo das Ausmaß der Nutzung im Belieben des Leistungsempfängers steht. Die Miete oder Pacht digitaler Inhalte ist verbunden mit einer zeitlich beschränkten Nutzungsbefugnis für die Dauer der Überlassung oder Zugänglichkeit der digitalen Inhalte. Diese Nutzungsbefugnis kann und darf der Rechteinhaber wie auch der Vermieter auch urheberrechtlich absichern, wobei angesichts der Verkehrsfähigkeit digitaler Inhalte das gesetzliche Leitbild nicht dem Urhebervertragsrecht, sondern dem Recht der BGB-Gebrauchsüberlassungsverträge zu entnehmen ist. Insbesondere schuldet der Vermieter die Aufrechterhaltung der Funktionsfähigkeit der digitalen Inhalte.

Erbringt der Leistende eine Dienstleistung lediglich unter Einsatz digitaler Inhalte, beschränkt sich deren Funktion auf die Einordnung als Instrument der Leistungserbringung. Der Leistungsempfänger gerät dann regelmäßig nicht einmal in die Situation, selbst urheberrechtsrelevante Handlungen vorzunehmen. Unter den Voraussetzungen von § 631 II BGB wird hier häufig ein Werkvertrag vorliegen. Dies ist etwa der Fall bei Streaming-Leistungen, bei denen es sich letztlich um schlichte Ausführungsverträge handelt. Auch die Bereitstellung und Nutzung sozialer Netzwerke hat regelmäßig Werkvertragscharakter, wobei freilich die Besonderheit besteht, dass hier ein Dauerschuldverhältnis mit werkvertraglicher Ausgestaltung entsteht.

5. Entgeltlichkeit oder Unentgeltlichkeit

In der digitalen Welt spielt die (tatsächliche oder auch nur scheinbare) Unentgeltlichkeit von Leistungen eine ganz besondere Rolle. Dies hat offenbar vor allem zwei Gründe: Zum einen senkt die unbegrenzte Kopierbarkeit digitaler Inhalte deren Herstellungskosten derart, dass Geschäftsmodelle möglich werden, welche digitale Inhalte dauerhaft unentgeltlich zugänglich machen. Zum anderen entwickelt sich in den gewonnenen personenbezogenen Daten eine Art Parallelwährung, weil die Verwertung dieser Daten (der Empfänger unentgeltlicher digitaler Inhalte) mittelbar oder unmittelbar den eigentlichen Ertrag der neuen Geschäftsmodelle begründet.

Diese im Blick auf die Einordnung der Verträge bislang einigermaßen amorphe Entwicklung führt zu einer ganzen Reihe von Sachfragen, von denen hier lediglich drei kurz angesprochen werden sollen:

a) Personenbezogene Daten als Gegenleistung?

Eine erste Kernfrage zielt auf die Möglichkeit der Behandlung von Daten als Entgelte im Sinne des Vertragsrechts. Politisch besteht hier längst weitgehender Konsens, jedoch ist bislang die rechtstechnische Erfassung dieses Phänomens weitestgehend ungeklärt. Gesichert sollte immerhin sein, dass schon im Blick auf § 28 BDSG nicht jeder Erwerb von personenbezogenen Daten als Gegenleistung eingeordnet werden kann. Das dürfte sich freilich ändern, wenn der andere über die von § 28 BDSG erfassten Datenverwendungsmöglichkeiten hinaus Teil zusätzliche Befugnisse für den Datenumgang eingeräumt erhält. Lässt man diese Befugnis gegebenenfalls ergänzt um weitere Anforderungen ausreichen, um Daten als Entgelt einzuordnen, stellt sich weiter die Frage, ob diese tatsächlich als „Parallelwährung“ Geldcharakter haben sollen, und damit die gewöhnlichen Vertragstypen anwendbar bleiben oder ob über Tauschkonstellationen im weitesten Sinn nachzudenken ist.

Ob Daten insoweit bereits eine Eignung als Universaltauschmittel erlangt haben, wie es dem Geld eigen ist, darf man freilich bezweifeln. Erforderlich ist die Entwicklung eines – dem Geldschuldrecht der §§ 244 ff. BGB vergleichbaren – Regelkanons eines Datenschuldrechts.[18]

b) Anwendbarkeit des besonderen Verbraucherschutzrechts

Die unklare Situation hinsichtlich der Grenzen der Entgeltlichkeit führt zu erheblichen Schwierigkeiten bei der Bestimmung des Anwendungsbereichs verbraucherschützender Vorschriften. Diese hat der deutsche

18 Hierzu demnächst *Langhanke*, Instrumente und Sanktionen im Kundendatenschutz in Österreich, der Schweiz und Deutschland.

Gesetzgeber durch das Umsetzungsgesetz zur VerbraucherrechteRL 2011/83/EU noch verstärkt, weil § 312 I BGB n.F. ab dem 13. 6. 2014 die Verbraucherverträge per definitionem auf entgeltliche Verträge begrenzt. Dieser Akt unsäglichen Beharrungsvermögens des deutschen Rechts wird – gerade in Bezug auf Verträge in der digitalen Welt – erneut die Frage aufwerfen, wie Verträge ohne Gegenleistung in Geld der Anwendungsbereich der besonderen Verbraucherschutzregeln der §§ 312 ff. BGB richtig zu bestimmen ist. Die alten und auch früher schon überflüssigen Debatten um den Anwendungsbereich des Haustürgeschäfterechts[19] werden so wieder aktuell. Die Art und Weise der Richtlinienumsetzung ist völlig unverständlich, weil insbesondere die VerbraucherrechteRL 2011/83/EU eine solche Beschränkung des Anwendungsbereichs auf entgeltliche Verträge nicht kennt. Hier besteht kurzfristig Handlungsbedarf – möglicherweise auch durch ein Vertragsverletzungsverfahren.

c) Anwendbarkeit zivilrechtlicher Haftungsprivilegierungen

Die verschiedenen Vertragstypen des BGB im Bereich unentgeltlicher Leistungen enthalten eine Reihe von Haftungsbeschränkungen zugunsten des Leistenden. Dieser haftet – immer mit Ausnahme des Auftrags – grundsätzlich nur für grobe Fahrlässigkeit (§§ 521, 599 BGB), und bei Sach- und Rechtsmängeln ist seine Haftung grundsätzlich auf Fälle der Arglist beschränkt (§§ 523, 524, 600 BGB), mit den bekannten Folgeproblemen bei Integritätsfolgeschäden.[20] Zudem wird die Haftung der unentgeltlichen Leistung durch erhebliche Beschränkungen der Naturalerfüllung bei Mängeln gekennzeichnet.

Für die digitale Welt mit ihrer nicht eindeutigen Entgeltlichkeit oder Unentgeltlichkeit stellt sich die Frage, ob der unentgeltlich Leistende in den Genuss dieser Privilegien kommen soll: Ist die Anwendbarkeit dieser Privilegien im geschäftlichen Verkehr, etwa bei Werbegeschenken, wegen der dahinter stehenden kommerziellen Zwecksetzung und der fehlenden Freigiebigkeit ohnehin schon zweifelhaft, so wird man jedenfalls für solche Fälle die Anwendbarkeit der einschlägigen Haftungsprivilegien zu verneinen haben, bei denen die Möglichkeit zur Datennutzung über gesetzliche Erlaubnistatbestände, insbesondere des § 28 BDSG, hinaus eingeräumt wird. Auch der an sich hilfreiche Art. 107 GEKR ist in dieser Hinsicht nicht das letzte Wort, weil er eine entsprechende Beschränkung nicht kennt.

V. Besondere Sachentscheidungen bei Verträgen über digitale Inhalte

Verträge über digitale Inhalte bedürfen aufgrund der tatsächlichen Besonderheiten ihrer Gegenstände wie auch im Blick auf die urheberrechtliche Rechtslage einer Reihe von Sonderregeln, die von den allgemeinen Grundlagen der – bislang – sachbezogenen Vertragstypen des BGB-Schuldrechts abweichen. Besonders augenscheinlich wird dies in den Punkten Widerrufsrecht, Leistungsqualität und schließlich Nutzungsbeschränkungen respektive Weiterveräußerung.

1. Widerrufsrechte bei digitalen Inhalten

Angesichts der Schwierigkeiten und der Missbrauchsanfälligkeit bei Rückabwicklung von Verträgen über digitale Inhalte lässt sich bereits die Eignung des Widerrufsrechts für Verträge über digitale Inhalte in Zweifel ziehen. Der europäische Gesetzgeber – und dementsprechend der deutsche Umsetzungsgesetzgeber – haben diese Eignung nicht generell verneint, jedoch einige wesentliche Beschränkungen eingezogen. Nicht zuletzt im Blick auf die UsedSoft-Entscheidung besteht hier jedoch weiterer rechtspolitischer Handlungsbedarf.

a) Eignung des Widerrufsrechts für digitale Inhalte?

Der verbraucherschützende Widerruf erfüllt eine Doppelfunktion als Verteidigungsrecht und als Basis für Rückabwicklungsansprüche. Vor Erbringung der geschuldeten Leistung erlaubt der Widerruf dem Verbraucher die Verteidigung gegen Erfüllungsansprüche des Unternehmers unabhängig davon, ob sie auf Zahlung oder auch auf Entgegennahme der Leistung gerichtet sind. Diese Funktion vermag das Widerrufsrecht ganz unabhängig von den Leistungsgegenständen zu erfüllen und jedenfalls insoweit ist das Widerrufsrecht auch für digitale Inhalte geeignet.

---

19 S. Entscheidung des EuGH, Rs. C-45/96, 17. 3. 1998 – *Bayerische Hypotheken und Wechselbank / Ditzinger*.

20 S. die berühmte Kartoffelpülpe-Entscheidung des Bundesgerichtshofs BGHZ 93, 23 sowie schon zuvor *Schlechtriem*, Vertragsordnung und außervertragliche Leistung.

Anders steht es mit der Auslösung von Rückabwicklungsansprüchen nach Beginn oder Vollendung der Vertragsdurchführung. Hier hängt die Funktion des Widerrufs an der Rückabwicklungsfähigkeit der erbrachten Leistung. Ohne eine solche Rückabwicklung oder zumindest deren Ersetzung durch Wertersatzansprüche drohen Überkompensationen des widerrufsberechtigten Verbrauchers. Für immaterielle Vorteile ist jedoch eine Rückabwicklung nahezu völlig ausgeschlossen. Das schränkt die Eignung des Widerrufsrechts für Dienstleistungen unter Einsatz von digitalen Inhalten ganz erheblich ein und auch für Gebrauchsüberlassungsgestaltungen steht die fehlende Rückabwicklungsfähigkeit der gezogenen Vorteile aus der Nutzung der Funktionsfähigkeit des Widerrufsrechts regelmäßig entgegen. Die drohende Überkompensation für den Verbraucher ergibt sich, wenn aufgrund mangelnder Rückabwicklungsfähigkeit die erbrachten Leistungen nicht ausgeglichen werden können. Das Widerrufsrecht droht dann die Funktion zu bekommen, die Unentgeltlichkeit der nicht rückabwicklungsfähigen Leistung nachträglich zu begründen. Wird dem Unternehmer umgekehrt ein Wertersatzanspruch gewährt, wird die Rückabwicklungsfunktion des Widerrufsrechts weitgehend entwertet; sie beschränkt sich dann auf Fälle überzogener Preise – sofern die Wertersatzberechnung entsprechend erfolgt.

Bei dauerhaften Übertragungen digitaler Inhalte eröffnet die UsedSoft-Entscheidung des europäischen Gerichtshofs hingegen neue Perspektiven: Verkehrsfähige digitale Inhalte lassen sich – eben weil sie verkehrsfähig sind – grundsätzlich auch rückabwickeln. Erfolgt nach Übertragung digitaler Inhalte ein wirksamer Widerruf, wäre auf der Rechtsfolgenseite zur Vermeidung der Überkompensation lediglich anstelle der – praktisch überflüssigen – Rückgewähr eine Löschung vorzunehmen. Dabei treten Missbrauchsgefahren auf, die nicht zu leugnen sind, die aber auch nicht umfänglicher sind als im Falle der schlichten Weiterveräußerung.

b) Ausgestaltung nach der künftigen lex lata

Das zum 13. 6. 2014 in Kraft tretende Umsetzungsrecht zur VerbraucherrechteRL enthält in Umsetzung dieser Richtlinie zahlreiche Sonderregeln für digitale Inhalte, die ohne körperlichen Datenträger übermittelt werden: Grundsätzlich wird auch in diesen Fällen ein Widerrufsrecht bestehen, wobei die Widerrufsfrist – wie im Regelfall nach § 355 II 2 BGB n.F. mit Vertragsschluss zu laufen beginnt, § 356 II Nr. 2 BGB n.F. Geschuldet ist dann – in der Sprache der analogen Welt – nach §§ 355 III, 357 BGB n.F. die Rückgewähr der erbrachten Leistung, woraus richtigerweise jedenfalls eine Pflicht zur Löschung der erhaltenen Daten abzuleiten ist. Ein Wertersatzanspruch wegen fehlender Rückabwicklungsfähigkeit schließt das Gesetz in § 357 IX BGB n.F. ebenso aus wie – nun ganz generell – Ansprüche auf Erstattung gezogener Nutzungen, § 361 I BGB n.F.

Allerdings enthält das Gesetz für digitale Inhalte neben dem Ablauf der Widerrufsfrist einen zweiten Erlöschensgrund, der an den Leistungsbeginn anknüpft. Danach erlischt das Widerrufsrecht, wenn der Verbraucher dem Leistungsbeginn in Kenntnis von dem damit einhergehenden Verlust des Widerrufsrechts zugestimmt hat, § 356 V BGB n.F. Eine Abschrift respektive Bestätigung des geschlossenen Vertrags müssen diese Zustimmung zum Leistungsbeginn und die Kenntnis vom Verlust des Widerrufsrechts dokumentieren, § 312 f. III BGB n.F.[21]

Bei Übermittlung der digitalen Inhalte auf einen körperlichen Datenträger finden hingegen auch weiterhin die Regeln des Widerrufs bei Verträgen über Waren Anwendung. Eine Sonderregel enthält insofern nach wie vor § 312g II Nr. 6 BGB n.F., der bei Entfernung der Versiegelung einer Verpackung des Datenträgers das Widerrufsrecht ausschließt. Insgesamt ergeben sich bei auf körperlichen Datenträgern gespeicherten digitalen Inhalten erhebliche Wertungswidersprüche zur Lieferung ohne körperlichen Datenträger. Insbesondere kann es in den Fällen des „Aufreißens“ auch ohne hinreichende Schwellen entsprechend § 356 V BGB n.F. (Kenntnis und Zustimmung) und Dokumentation nach § 312 f. III BGB n.F. zu einem Verlust des Widerrufsrechts kommen. Vor allem aber bildet die vorgenommene Differenzierung die überkommene urheberrechtliche Grundgestaltung ab, welche durch die UsedSoft-Entscheidung grundlegend ins Wanken geraten ist.

c) Rechtspolitischer Handlungsbedarf

Die Neuregelung verletzt ganz offensichtlich das Gebot der Medienneutralität. Nach diesem, die Innovationsoffenheit des Rechts sicherstellenden, Gebot dürfte die

[21] Die Folgen einer Verletzung dieser Dokumentationspflicht sind freilich unklar, in Betracht kommen Konsequenzen für den Nachweis der Voraussetzung von § 356 V BGB n.F. (vgl. §§ 312k II, 361 III BGB n.F.) oder auch eine Verschiebung des Fristbeginns nach § 356 III BGB n.F. i.V.m. Art. 246b § 1 I Nr. 12 EGBGB n.F.

Verwendung von Datenträgern für die Rechtsfolgenseite keine Rolle spielen. In Einzelfällen mag die im Gesetz vorgenommene Differenzierung dem Unternehmer sogar ein Wahlrecht über die Grenzen des Widerrufs verschaffen, was der grundsätzlichen Idee einer Zwingendstellung widerspräche.

Mit der UsedSoft-Entscheidung ist die Widerrufsregelung der VerbraucherrechteRL und damit auch des Umsetzungsgesetzes zudem überholt. Erforderlich ist daher die Anpassung der Widerrufsregelung an die vorgenommene und auch noch zu erwartende Ausweitung der Erschöpfungsregeln. Diese Anpassung sollte zu einer weitest gehenden Gleichstellung von digitalen Inhalten mit Waren dann führen, wenn vertraglich eine dauerhafte Rechteeinräumung zugesagt ist. Hingegen kann es beim Ausschluss des Wertersatzes bleiben, da der Verkäufer der digitalen Inhalte ein legitimes Interesse lediglich an der Löschung hat, während wegen der Vervielfältigungsmöglichkeit regelmäßig kein ersatzbarer Wertverlust eintritt.

2. Zur Leistungsqualität bei digitalen Inhalten

a) Mängel der Daten

Behandelt man Verträge über digitale Inhalte nach den – geringfügig anzupassenden – Regeln der klassischen Vertragstypen Kauf, Miete oder Dienstleistungen, bleiben deren Regeln selbstverständlich auch im Hinblick auf die Folgen vertragswidriger Leistungen anwendbar:

Das bedeutet im deutschen Recht zunächst die Anwendbarkeit der §§ 474 ff., 433 ff. BGB auf den Kauf digitaler Inhalte durch Verbraucher und damit auch der §§ 434 ff BGB. Dies ergibt sich aus § 453 I BGB. Dessen Verhältnis zu § 474 I BGB n.F. ist freilich unklar: Für eine Anwendung der Regeln über den Verbrauchsgüterkauf auf den Kauf digitaler Inhalte spricht zunächst der Wortlaut von § 453 I BGB und die darin verschlüsselte Grundidee, dass der Sachkauf lediglich das Paradigma für sämtliche Kaufgeschäfte sein soll. Gegen eine Anwendung spricht die abweichende Definition des Anwendungsbereichs in § 474 I BGB n.F.[22] Auch die Systematik, welche § 453 BGB bewusst an das Ende des allgemeine Kaufrechts gesetzt hat, deutet eher auf eine Unanwendbarkeit hin. Gleichwohl sollte es für das deutsche Recht bei einem breiten Verweis aus § 453 I BGB auf sämtliche kaufrechtlichen Vorschriften bleiben, was für den Kauf digitaler Inhalte durch Verbraucher eben auch §§ 474 ff. BGB einschließt. Der Regelungszweck des § 453 I BGB ist gerade darauf gerichtet, eine möglichst breite Anwendbarkeit kaufrechtlicher Vorschriften auch auf andere Gegenstände als auf Sachen sicherzustellen. Aus Sachgründen erforderliche Anpassungen ergeben sich daher nicht aus der Ausschlussfunktion dogmatischer Systembildung, sondern aus der in § 453 I BGB angelegten Anpassungsmöglichkeit an die sonstigen Vertragsgegenstände. Bereits nach der lex lata finden also auch die Sonderregeln über die Sachmängelgewährleistung beim Verbrauchsgüterkauf auf Verträge über digitale Inhalte Anwendung.

Hingegen verlangt die VerbrauchsgüterkaufRL 1999/44/EG nach ihrem Wortlaut ausdrücklich bewegliche körperliche Gegenstände als Kaufsachen, so dass digitale Inhalte jedenfalls dann aus dem Anwendungsbereich ausscheiden, wenn sie nicht auf einem dauerhaften Datenträger vorliegen. Das entspricht – jedenfalls für die Mängelrechte des Erwerbers – nicht der üblichen Praxis der Mitgliedstaaten, die die Regeln über Mängel beim Kauf typischerweise auch auf Mängel digitaler Inhalte anwenden. Für die Richtlinie stellt sich daher die Frage nach der Möglichkeit einer analogen Anwendung zur Erfassung digitaler Inhalte. Eine solche entspricht verbreiteter Praxis für das UN-Kaufrecht und hätte auch für sich, dass der reine Online-Handel von Software im Jahre 1999 noch nicht im Bewusstsein der gesetzgebenden Organe war. Auch die Erfassung digitaler Inhalte durch die auch an der Kaufrechtsrichtlinie orientierten Vorschläge im Kommissionsentwurf für ein gemeinsames europäisches Kaufrecht sprechen für eine derart erweiternde Auslegung.

Bei Anwendung deutschen Rechts ist nach alledem der in § 434 BGB niedergelegte Mängelbegriff für die Feststellung der Vertragswidrigkeit maßgebend. Dabei wird die gewöhnliche Beschaffenheit (Abs. I 2 Nr. 2) vielfach kleinere Programmierfehler mit einschließen, sofern diese die Funktionstauglichkeit der digitalen Inhalte nicht beeinträchtigen. Angesichts der Immaterialität digitaler Inhalte liegt zudem ein besonders Gewicht auf Fragen der Funktionstauglichkeit i.S.d. Eignung für den vereinbarten oder vertraglich vorausgesetzten Gebrauch. Dabei wird auch außerhalb von § 312d I 2 BGB n.F. der auf die Beschreibung der Funktionalität gerichteten Informationspflicht nach Art. 246 I Nr. 7 und 246a

[22] Zur entsprechenden Frage bei der Verbrauchsgüterkauf-RL 1999/44/EG s. sogleich.

§ 1 I Nr. 14 EGBGB n.F. bei der Bestimmung der maßgebenden Funktionalitätserwartungen eine wesentliche Bedeutung zukommen. Im Blick auf die Hardware- und Systemabhängigkeit digitaler Inhalte wird zudem der Kompatibilität und der Interoperabilität dieser Inhalte eine besondere Bedeutung zukommen.[23] Wie beim Sachkauf ergeben sich die Rechtsbehelfe bei Fehlerhaftigkeit der Daten dann vor allem aus der nicht abschließenden Liste des § 437 BGB und den dort in Bezug genommenen Anspruchs- respektive Rechtsgrundlagen. Grenzen der Abdingbarkeit schreiben – auch für digitale Inhalte – §§ 475, 309 Nr. 7, 8 BGB fest.

Bei der Miete digitaler Inhalte ergeben sich die vertraglichen Qualitätsanforderungen hingegen aus dem Mängelbegriff des § 536 I, II BGB, auf den die Rechtsbehelfe nach §§ 536, 536a, 539, 543 BGB Bezug nehmen. Sonderregeln für die Bewältigung von Verbraucherverträgen zur Gebrauchsüberlassung digitaler Inhalte finden sich nicht. Für die Bestimmung der Grenzen der Abdingbarkeit steht lediglich § 307 BGB zur Verfügung, der insoweit allerdings am Maßstab der AGB-RL 93/13/EWG zu konkretisieren ist.

Werden digitale Inhalte instrumental zum Erbringen von Dienstleistungen eingesetzt, ist der Rechtsanwender auf die begrenzte Struktur des deutschen Dienstleistungsvertragsrechts zurückgeworfen. Geschriebene Mechanismen zur Bestimmung der geschuldeten Qualität finden sich hier lediglich für den Fall der Qualifikation als Werkvertrag i.S.d. § 631 II BGB. In diesen Fällen ist der Mangelbegriff nach § 633 II BGB maßgebend, welcher im Verletzungsfalle auf die im § 634 BGB genannten Rechtsbehelfe und die dort in Bezug genommenen Anspruchs- und Rechtsgrundlagen verweist. Grenzen der Abdingbarkeit ergeben sich hier nach § 309 Nr. 7, 8 BGB und auch insoweit ist hier die KlauselRL 93/13/EWG zu beachten.

b) Insbesondere: Fehlende Kompatibilität und Interoperabilität

Ab 13. 6. 2014 enthalten BGB und EGBGB mehrere verbraucherschützende Informationspflichten im Hinblick auf die für digitale Inhalte besonders wichtige Interoperabilität.

Das gilt zunächst für die besonderen Vertriebsformen der Fernabsatz- und Außergeschäftsraumverträge, für welche die über § 312d I BGB n.F. anwendbare Art. 246a § 1 I Nr. 8 EGBGB n.F. vom Unternehmer verlangt, über solche Beschränkungen der Interoperabilität und der Kompatibilität digitaler Inhalte mit Hard- und Software zu informieren, soweit diese wesentlich sind und dem Unternehmer bekannt sind oder bekannt sein müssen. Die Erfüllung oder Nichterfüllung dieser Informationspflicht hat wegen § 312d I 2 BGB unmittelbare Auswirkungen auf den Vertragsinhalt und damit für die Maßstäbe zur Bestimmung der Vertragskonformität nach §§ 434, 536, 634 II BGB. Insbesondere haftet der Unternehmer auch für eine nicht mitgeteilte Kompatibilitäts- oder Interoperabilitätslücke, wenn diese wesentlich ist und daher die Mitteilung zu erwarten war. Die Informationspflicht des Art. 246a § 1 I Nr. 8 EGBGB n.F. konkretisiert damit auch die gewöhnliche Beschaffenheit nach § 434 I 2 Nr. 2 BGB. Dieser Mechanismus ist im Hinblick auf § 475 I BGB nicht abdingbar. Abweichungen von den Interoperabilitäts- und Kompatibilitätsstandards sind daher künftig nur ausdrücklich möglich. Erforderlich ist etwa der Hinweis „Funktioniert nicht für Betriebssystem X“.

Für die nicht in den Anwendungsbereich der Regeln über die besonderen Betriebsformen fallenden Verträge enthält der durch § 312a II BGB n.F. in Bezug genommene Art. 246 I Nr. 3 EGBGB n.F. eine ganz allgemeine Informationspflicht hinsichtlich Interoperabilität und Kompatibilität digitaler Inhalte, die der soeben besprochenen dem Wortlaut nach entspricht. Kompatibilität und Interoperabilität sind damit künftig ein ganz allgemeiner Qualitätsstandard für digitale Inhalte – jedenfalls für den Bereich der Verbraucherverträge. Mangels einer Parallelnorm zu § 312d I 2 BGB n.F. sind die Auswirkungen auf die Mechanismen zur Bestimmung der Vertragsgemäßheit in den §§ 434, 536, 634 II BGB jedoch unklar. Richtigerweise wird man die Informationspflicht als normative Determinierung des Empfängerhorizonts begreifen müssen, so dass man häufig zu identischen Ergebnissen wie im Anwendungsbereich von § 312d I 2 BGB n.F. kommen wird, was freilich Tatfrage ist. Dies zugrunde gelegt, läge der Unterschied zur ausdrücklichen Erhebung zum Vertragsinhalt durch § 312 I 2 BGB n.F. lediglich in der erleichterten Abdingbarkeit, weil in soweit für einen abweichenden Vertragsinhalt auch implizite Vereinbarungen oder solche durch schlüssiges Verhalten ausreichen können.

---

[23] Dazu noch unten b.

c) *Insbesondere: Kopierschutzmechanismen und Vertragswidrigkeiten*

Hinsichtlich Kopierschutzmechanismen bei digitalen Inhalten ist zunächst festzuhalten, dass diese nicht als solche mängelbegründend sind. Das ergibt sich schon daraus, dass sonst ein Widerspruch zur urheberrechtlichen Situation nach §§ 95a, 69a V UrhG eintreten würde.[24] Dass die urheberrechtlich privilegierten Kopierschutzmechanismen für Verbraucherverträge freilich nicht sakrosankt sind, zeigen die Informationspflichten nach Art. 246 Nr. 7, 246a § 1 Nr. 13 EGBGB n.F.: Da der Unternehmer verpflichtet ist, auf solche Kopierschutzmechanismen hinzuweisen, begründet das Schweigen über diese Tatsache im Blick auf § 312d I 2 BGB n.F. regelmäßig die Vertragswidrigkeit der digitalen Inhalte.

Ohne Anspruch auf Vollständigkeit wird man eine Mangelhaftigkeit dementsprechend jedenfalls dann annehmen dürfen, wenn das Verbreitungsrecht des Urhebers nach den Grundsätzen der UsedSoft-Entscheidung erschöpft ist. Auch ein *expiration date* führt bei Verträgen über die permanente Überlassung digitaler Inhalte, also Kaufverträgen, jedenfalls dann zur Mangelhaftigkeit, wenn der Vertrag nach Ablauf der Widerrufsfrist endgültig wirksam geworden ist.

Eine Mangelhaftigkeit digitaler Inhalte kann sich aber auch aus der Beeinträchtigung anderer Interessen des Verbrauchers ergeben. So sind datenschutzrelevante automatische Kontrollmitteilungen zu Kopierschutzzwecken nur mit Einwilligung der Betroffenen zulässig. Ohne eine solche Einwilligung begründen sie die Mangelhaftigkeit der übertragenen digitalen Inhalte.

3. Nutzungsbeschränkungen und Weiterveräußerung

Die mit der UsedSoft-Entscheidung eingeläutete Verkehrsfähigkeit digitaler Inhalte, jedenfalls für Software und vermutlich auch bald darüber hinaus, lässt das Urheberrecht als lediglich für die dingliche Rechtslage maßgebend in Kaufvertragskonstellationen hinter die schuldrechtlichen Regeln zurücktreten. Bei dauerhaften Übertragungen digitaler Inhalte sind dementsprechend mit Blick auf die Erschöpfungswirkungen nur noch wenige zulässige Nutzungsbeschränkungen denkbar. Zulässig ist insbesondere der Ausschluss der Befugnis, digitale Inhalte Dritten zum Gebrauch zu überlassen.[25] Außerdem ist es dem Urheber möglich, die Zahl gleichzeitiger Nutzer zu beschränken. Für Ausschlüsse der Netzwerknutzung, die als solche die berechtigten Interessen des Urhebers nicht tangiert, solange die Zahl der möglichen Nutzer nicht überschritten wird, ist die Zulässigkeit jedoch zweifelhaft; einer gesonderten Gestattung bedarf urheberrechtlich zudem die Aufspaltung von Lizenzen, welche nicht schon durch die Erschöpfungswirkung zulässig wird.[26] Möglich ist hingegen, dass sich der Rechteinhaber eine – unkomplizierte und dem Wert der digitalen Inhalte angemessene, mithin nicht prohibitive – Mitwirkung bei Weiterübertragungen vorbehält. Allerdings sind hierzu regelmäßig zusätzlich datenschutzrechtliche Einwilligungen der Drittempfänger erforderlich und die Übertragung darf nicht scheitern, wenn die Drittempfänger die Einwilligung verweigern.

Unzulässige Nutzungsbeschränkungen ergeben sich etwa beim Ausschluss von Kopien, welche Voraussetzung für das Funktionieren der digitalen Inhalte sind sowie für Sicherungskopien (§ 69d II UrhG) und Fälle des Testlaufs (§ 69d III UrhG). Im Blick auf die Möglichkeit nach Fristsetzung Mangelbeseitigungen selbst vorzunehmen, darf dem Käufer digitaler Inhalte auch die Fehlerbeseitigung urheberrechtlich nicht untersagt werden (§ 69d I UrhG). Weitere Verbote von Nutzungsbeschränkungen hat die Rechtsprechung bereits entwickelt und wird sie weiterhin entwickeln; dazu gehören etwa das Verbot von CPU-Klauseln[27] oder Anzeigepflichten bei neuen (erlaubten) Nutzungen.[28]

Im Blick auf die Verkehrsfähigkeit digitaler Inhalte sind auch Beschränkungen der Weiterveräußerungsbefugnis des Käufers – also in den Fällen einer die urheberrechtliche Erschöpfung bewirkenden dauerhaften Übertragung – unzulässig. Das gilt zunächst für die dingliche (urheberrechtliche) Ebene, weil die Regeln der Erschöpfung insoweit zwingend sind.[29] In Verbraucherverträ-

---

24 Vgl. BGB GRUR 2013, 1035 (EuGH-Vorlage).
25 Beim Verkauf von Software durch vom Lieferanten an den Leasinggeber wird die Berechtigung zur Gebrauchsüberlassung an den Leasingnehmer regelmäßig mit eingeräumt (OLG Hamm, MMR 2013, 438).
26 EuGH, Rs. C-128/11, 3. 7. 2012 – *UsedSoft/Oracle International*, Rn. 86; OLG Frankfurt, GRUR 2013, 279.
27 BGB NJW 2003, 2014, 2016.
28 LG Hamburg MMR 2014, 102.
29 OLG Frankfurt, GRUR 2013, 279; HOLG Hamburg, MMR 2014, 115, 116.

gen wird aber auch ein schuldrechtliches Weitergabeverbot regelmäßig scheitern, weil es gegen das für § 307 BGB maßgebliche gesetzliche Leitbild von Verträgen über die dauerhafte Übertragung von digitalen Inhalten verstößt.[30] Die Verkehrsfähigkeit hat insoweit den Weg auch schuldrechtlich geebnet.

VI. Zusammenfassung

Vertragsgegenstand von Verträgen über digitale Inhalte sind nicht die digitalen Inhalte selbst, sondern der Umgang mit diesen (dauerhafte Übertragung, vorübergehende Nutzbarkeit oder Instrument zur Erbringung von Dienstleistungen). Für Verträge über digitale Inhalte ist ganz grundsätzlich danach zu unterscheiden, ob diese dauerhaft oder nur vorübergehend oder gar nur als Mittel für Dienstleistungen zur Verfügung gestellt werden. Das geltende Recht ist insoweit zu undifferenziert. Die Unterscheidung ist nicht nur im Blick auf die schuldrechtliche Seite erforderlich, sondern im Hinblick auf die Voraussetzungen der Erschöpfung nach der UsedSoft-Entscheidung des EuGH auch für die urheberrechtliche. Nur bei dauerhafter Zurverfügungstellung sind die Verbreitungsbefugnisse des Urhebers (weitestgehend) nämlich als erschöpft anzusehen.

Die urheberrechtliche Determinierung von Verträgen mit Verbrauchern über digitale Inhalte befindet sich auf dem Rückzug, soweit diese die digitalen Inhalte dauerhaft zur Verfügung gestellt bekommen. Für dauerhaft zur Verfügung gestellte digitale Inhalte sollte die Erschöpfung über die Software hinaus gesetzlich klargestellt werden. Ferner sollten in diesen Fällen die Verbraucherschutzmechanismen soweit als möglich dem Warenkauf angeglichen werden; insbesondere sollten die Einschränkungen des Widerrufsrechts beseitigt werden. Der Unternehmer haftet für Mängel digitaler Inhalte in diesen Fällen nach den Regeln des Verbrauchsgüterkaufs. Dabei ist Interoperabilität eine Standardqualität digitaler Inhalte bei allen Vertragsgestaltungen.

Die Beschränkung von § 312 BGB auf entgeltliche Leistungen ist EU-rechtswidrig. Andererseits passen bei unentgeltlichen Leistungen digitaler Inhalte die klassischen Haftungserleichterungen wegen Unentgeltlichkeit vielfach nicht. Das gilt insbesondere, soweit vom Verbraucher Datennutzungen über gesetzliche Ermächtigungen des BDSG hinaus ermöglicht werden, und erst recht soweit die Unentgeltlichkeit der Erreichung geschäftlicher Zwecke dient.

30 HOLG Hamburg, MMR 2014, 115, 116; LG Hamburg MMR 2014, 102.

Arbeitsgruppe 3 „Mobile Payment“

Neue mobile Bezahlmethoden gewinnen in Deutschland zunehmend an Aufmerksamkeit und Bedeutung. Besonders hohe Erwartungen werden mit dem Einsatz der Kontaktlos-Technologie (Near Field Communication: NFC) verbunden. Zurzeit sind neue mobile Bezahlmethoden am deutschen Markt jedoch noch nicht flächendeckend verbreitet. Damit sich die neuen Bezahlverfahren neben den bestehenden Bezahlsystemen am Markt etablieren können, bedarf es eines hohen Vertrauens der Verbraucher in diese Systeme. Die Arbeitsgruppe „Mobile Payment“ wird sich inhaltlich auf das kontaktlose Bezahlen mittels Mobiltelefon und den Einsatz der NFC-Technik begrenzen. Dem Bezahlen unter Einsatz der NFC-Technik wird gegenwärtig ein großes Wachstumspotential zugesprochen, da Mobiltelefone heute das meistverbreitete digitale Endgerät der Welt darstellen. Vor diesem Hintergrund wollen wir in der Arbeitsgruppe „Mobile Payment“ mit den Teilnehmern verschiedene verbraucherrechtliche Fragen zu dieser Bezahlmethode erörtern. Folgende Themenschwerpunkte sollen behandelt werden:

- IT-Sicherheit
- Zahlungsverkehrsrecht
- Aufsichtsrecht

Dabei wird unter anderem die Frage zu diskutieren sein, ob die bestehenden gesetzlichen Regelungen zur Zahlungsverkehrssicherheit ausreichen oder für mobile Zahlungen geändert werden müssen. Ohne Vertrauen in die technische und rechtliche Sicherheit wird das kontaktlose Bezahlen keine hohe Akzeptanz bei Verbrauchern finden. Insbesondere möchten wir mit den Teilnehmern erörtern, ob der geltende Rechtsrahmen im Zahlungsverkehr im Falle einer missbräuchlichen Verwendung des Mobiltelefons mit einem implementierten NFC tauglichen Chip ausreichenden Schutz für den Verbraucher bietet oder um welche Aspekte er zu erweitern ist. Zudem wird zu beleuchten sein, ob das bestehende Widerspruchsrecht auch bei mobilen Zahlungen eine unkomplizierte Rückbuchung ermöglicht. Neben Fragen der technischen und prozeduralen Sicherheit sollen in der Arbeitsgruppe „Mobile Payment“ aber auch finanz aufsichtsrechtliche Fragen Diskussionsgegenstand sein.

PD Dr. Key Pousttchi

Mobile Payment und Verbraucherschutz

Das Leitthema der Bamberger Verbraucherrechtstage in diesem Jahr lautet Mobile Commerce. Was man in den nächsten Jahren unter Mobile Commerce verstehen wird, hat allerdings nur noch am Rande mit dem zu tun, was vor einigen Jahren darunter verstanden wurde.

Hinter dem Smartphone als nützlichem, allgegenwärtigen und vermeintlich harmlosem Gadget verbirgt sich ein Megatrend, der unser Leben in den nächsten zwei Dekaden dominieren und keinen Stein auf dem anderen lassen wird: das Verschmelzen der realen und der virtuellen Welt. Man kann das zu Recht den „Megatrend Mobile“ nennen. In der Öffentlichkeit wird diese Entwicklung weitgehend unterschätzt.

Die Anfänge des Mobile Payments in Deutschland

Mobile Payment, also *die Verwendung des Mobiltelefons des Endkunden für die Initiierung, Autorisierung oder Realisierung von Bezahlvorgängen*, steht im Zentrum dieser Entwicklung. Auch hier hat sich ein deutlicher Wandel vollzogen. Im Zuge des National Roundtable M-Payment der deutschen Banken und Mobilfunkanbieter im Auftrag des Bundeswirtschaftsministeriums in den Jahren 2004 und 2005 wurde schon damals versucht, die strategische Bedeutung dieser innovativen Bezahlverfahren für die deutsche Volkswirtschaft hervorzuheben und eine nationale Lösung anzustreben, die international wegweisend sein kann. Zu einem umfassenden Ansatz und zu der dazu erforderlichen Kooperation konnten sich die damals wichtigen Marktteilnehmer jedoch nicht durchringen. Als Folge dieser Entwicklung wurde Deutschland kein Vorreiter im M-Payment, sondern muss sich nun mit der Marktdominanz nordamerikanischer Kreditkarten- und Internetunternehmen auseinandersetzen.

Mobile Payment und Verbraucherschutz

Verbraucherschutz war für die Mobile-Payment-Verfahren alter Art ein Randthema. Es beschränkte sich weitgehend auf eine IT-Sicherheitsproblematik und Missbrauchsgefahr, die zum einen Teil analog zu klassischen kartenbasierten Bezahlverfahren und zum anderen Teil analog zu elektronischen Bezahlverfahren für das Internet bestanden. Beide Gefahren waren und sind heute noch relevant, mit den vorhandenen Mitteln jedoch gut beherrschbar. Sie sind nicht synergetisch und beinhalten damit prinzipiell keine neuartige Herausforderung.

Die Diskussion, die anlässlich der Einführung der kontaktlosen Geldkarte durch die Sparkassen in Teilen der Medien um die Sicherheit der NFC-Technologie geführt wurde, kann man zu Recht als etwas bizarr bezeichnen. Keines der vorgestellten Angriffsszenarien hatte realistisch das Potential zu einer ernsthaften Bedrohung für ein vernünftiges Bezahlverfahren zu werden.

Es handelt sich bei den gezeigten Beispielen um Probleme für IT-Administratoren und -Entwickler, die für Verbraucherschützer auf ministerieller Ebene keinen Grund zur Besorgnis darstellen sollten.

Ernsthafte Herausforderungen für den Verbraucherschutz

Die Herausforderungen für den Verbraucherschutz entstehen durch die andersartige Natur der kommenden, modernen Mobile-Payment-Verfahren und ihre Einbettung in den Mobile Commerce neuer Art, der das Verbraucherverhalten in der realen Welt durchziehen wird.

Wer das stationäre Internet nutzt, hinterlässt eine Datenspur. Auf dem Smartphone wird aus dieser Datenspur ein flächendeckender Datenteppich. Dazu tragen im Wesentlichen drei Dinge bei. Erstens wird das Betriebssystem des Smartphones von Playern kontrolliert, deren Kerngeschäft (und künftige Haupt-Einnahmequelle!) das Sammeln und Verwerten von Nutzerdaten ist und die diese an der Quelle mitschneiden, ohne dass der Nutzer faktisch eine Entscheidungsmöglichkeit hat. Zweitens sind heutige mobile Dienste und Anwendungen fast durchgängig absichtlich so konstruiert, dass alle Nutzungsdaten über die Server des Dienstanbieters geleitet werden, obwohl es objektiv auch für die Dienstperformance oft anders sinnvoller wäre. Mit einem Kalauer könnte man sagen: „Die Cloud heißt Cloud, weil sie Cloud“.

Und drittens wird das Smartphone künftig die Brücke zwischen der elektronischen und der realen Welt sein –

wir verknüpfen also 24 Stunden am Tag identifizierte, sehr detaillierte elektronische Nutzungsdaten mit Telekommunikationsdaten, Ortsdaten und zukünftig immer häufiger auch mit Bilddaten sowie Informationen aus lokalen Netzen, mit denen sich Ihr Gerät verbindet (z.B. in der Wohnung, im Einkaufszentrum oder Car-to-car im Straßenverkehr).

Dabei werden weit mehr Daten erhoben, als früher jemals vorstellbar oder sinnvoll analysierbar waren. Durch die neue Generation der In-Memory-Datenbanken wird es nun aber möglich, diese Daten automatisiert in Echtzeit auszuwerten. Dabei können durch Anwendung induktiver statistischer Methoden sehr treffsichere Prognosen der Nutzerbedürfnisse, des Nutzerverhaltens und geeigneter Methoden seiner Beeinflussung sowie der zukünftigen Kundenwertentwicklung erfolgen.

Ein Exkurs zur entsprechenden Analyse von Internet-Metadaten durch Geheimdienste würde den Rahmen dieses Beitrages sprengen. Aber der (sinngemäße) Filmtext von Tom Cruise aus „Minority Report“ ist bereits heute durchaus realistisch: „Pre-Crime Unit – ich verhafte Sie wegen eines Mordes, den Sie später begehen werden.“ Staatlicher Verbraucherschutz in den USA gegen die Art der derzeitigen Datensammlung durch Apple, Google, Facebook & Co. ist vor diesem Hintergrund Illusion, diese Sammlung wird im Gegenteil sehr begrüßt. Das wird auch beim Payment so sein.

Bedeutung von Bezahldaten

Das Ziel eines groß angelegten Mobile-Payment-Verfahrens im Jahr 2013 ist nicht mehr primär die Erzielung von Transaktionsgebühren, wie es früher der Fall war. Damit ist derzeit auch kein Geld zu verdienen. Das Hauptziel eines modernen M-Payment-Verfahrens ist Mobile Marketing, ist die Generierung von Transaktionsdaten in dem Sinne, wie zuvor bereits ausführlich geschildert wurde.

Bezahldaten gehören zu den mächtigsten Daten überhaupt. Kreditkartenfirmen können anhand von Bezahldaten in den USA bereits heute besser prognostizieren, wer sich in den nächsten fünf Jahren scheiden lassen wird, als es die Leute selbst können.

Es gibt es nur eine Handvoll Player, die perspektivisch über eine hinreichende Menge Kundendaten verfügen, um das zuvor Beschriebene in absehbarer Zeit zu realisieren. Kriterium ist hierbei die Querschnittlichkeit ihrer Dienste im Leben des Kunden, beispielsweise gemessen an der Nutzungszeit pro Tag. Man kann diese Frage letztendlich auch mit „Wem gehört der Kunde?“ übersetzen und der Kampf darum ist voll entbrannt. Derzeit gibt es fünf realistische Kandidaten: In der ersten Reihe Apple, Google, Facebook, in der zweiten Reihe eBay/PayPal und Amazon. Alle haben sehr unterschiedliche Stärken und Schwächen. Unter Forschern wird diese Gruppe nach ihren Anfangsbuchstaben als AGFEA bezeichnet.

Alle haben gemeinsam, dass Bezahldaten aus der realen Welt das wichtigste Puzzlestück sind, das Ihnen für die vollständige Nutzerprofilierung fehlt (im Falle der beiden ersten Player könnte man auch sagen: das letzte Puzzlestück), um ihre Dominanz in die reale Welt zu übertragen. Alle haben gemeinsam, dass sie seit Jahren Payment-Entwicklungen vornehmen und/oder Patente aufkaufen.

Als relevante Player zu beachten sind zudem noch die Kreditkartenunternehmen – nicht weil sie das Beschriebene selbst könnten, sondern weil sie prinzipiell mit jedem Player bündnisfähig sind, zuletzt haben ja auch die deutschen Mobilfunkanbieter die eigenen Strategien wegen Erfolglosigkeit eingestellt und sich Visa und MasterCard angedient. Die aktuellen EU-Regulierungsvorschläge zu Kreditkartengebühren noch außer Betracht gelassen, könnte das 2-3 % Kaufkraftverlust beim deutschen Verbraucher nach sich ziehen, der an diese Player abgeführt wird.

Gesamtbewertung und Handlungsempfehlung.

Als Ausgangspunkt für die Gesamtbewertung noch ein kurzer Blick auf den Nutzer, den Endkunden. Die Forschungsgruppe wi-mobile hat sich länger und tiefer mit dem Endkunden befasst als irgendjemand sonst im Bereich mobiler Dienste und M-Payment: *Die Botschaft dieses Beitrages ist nicht, dass das Sammeln von Nutzerdaten verboten oder willkürlich erschwert werden sollte.*

Die Dienste der Zukunft werden alle auf der Auswertung von Nutzerdaten beruhen, zahlreiche neue Geschäftsmodelle werden entstehen und Deutschland kann und sollte sich dem nicht entziehen. Die Nutzer wollen die modernen und innovativen Dienste. Auf unreflektierte Verbote würden sie mit unreflektierten Einwilligungen reagieren, die erteilen sie ja jetzt schon, wenn auch ungern. *Entsprechende Lösungen wären also nur Scheinlösungen.*

Drei Dinge sind zentral:

(1) Die Auswertung von Nutzerdaten ist wichtig und wird der zentrale Innovationsfaktor der nächsten zwei Dekaden sein. Aber der Manchester-Kapitalismus beim Sammeln von Nutzerdaten muss aufhören. Es sind durchweg nordamerikanische Player, die a) ein sehr anderes Datenschutzverständnis haben als die Europäer und die b) die EU-Datenschützer bislang am Nasenring durch die Arena führen (ebenso wie übrigens die Steuerbehörden).

Dazu gehört auch und vor allem die Unterbindung des dramatischen Missbrauchs von Marktmacht. Ein 16-jähriges Mädchen hat heute keine Wahl, ob sie die Nutzungsbedingungen des De-Facto-Monopolisten Facebook akzeptiert – die Alternative ist der soziale Ausschluss.

Das gleiche gilt für das massenhafte „Abgreifen“ der Smartphone-Daten durch die Besitzer der Betriebssysteme. Wer heute ein modernes Telefon will, egal von welchem Anbieter, gibt seine Datenhoheit ab. Auch das ist ein dramatischer Missbrauch von Marktmacht.

Pauschale, abgepresste (weil realistisch alternativlose) Einwilligungen müssen unterbunden werden. Der Nutzer muss detailliert entscheiden können, welche seiner Daten verwendet werden dürfen. Dazu muss er zunächst einmal genau wissen, wer was mit seinen Daten vorhat. Das muss im gesamten Bereich mobiler Dienste so sein, aber insbesondere im M-Payment.

(2) Der deutsche stationäre Einzelhandel – wie auch verschiedene andere Branchen – muss aus seinem Dornröschenschlaf aufwachen und erkennen, dass er dieses Spiel mit seinem bisherigen Verhalten zwar spielen (siehe etwa das M-Payment bei Edeka und Rewe), aber nicht gewinnen kann, weil ihm die Querschnittlichkeit fehlt. Der Effekt von querschnittlichen Marktteilnehmern ist, dass sie eine vollständige Empfehlungsmacht entwickeln und den Nutzer mit hoher Trefferquote zu einem Online- oder Offline-Händler lenken können. Im nächsten Schritt werden Händler dafür zahlen müssen, bei diesen Empfehlungen berücksichtigt zu werden. Dem 1x1 der Mikroökonomie folgend wird dabei im Wettbewerb die Rendite des Einzelhändlers abgeschöpft. Darüber hinaus folgt für große Teile des Einzelhandels ein ruinöser Preiswettbewerb gegen den Online-Handel, den diese nicht gewinnen können. Die Allgegenwärtigkeit der Empfehlungsmacht moderner Mobile-Marketing-Systeme, die auf M-Payment basieren, wird dabei nicht viele Nischen übrig lassen. Die Wirkung auf die Arbeitsplätze ist nicht Thema der Veranstaltung, aber auf die makroökonomischen Auswirkungen sei zumindest nachdrücklich hingewiesen.

(3) Die Lösung kann nur intelligente Regulierung plus eigene Innovation lauten. Einerseits müssen die Auswüchse der Datenenteignung – im M-Payment, aber sinnvollerweise für alle mobilen Dienste – so unterbunden werden, dass der Nutzer keine wesentlichen Einschränkungen wahrnimmt. Dies ist zum jetzigen Zeitpunkt noch problemlos möglich.

Andererseits – und das ist entscheidend – müssen Systeme entwickelt werden, die Nutzerdatenauswertung nicht gegen den Verbraucher und verborgen vor ihm so wie heute, sondern mit ihm zusammen und transparent vornehmen.

Abseits vom unmittelbaren Verbraucherschutz sei dabei noch gesagt: Will man für die deutsche und europäische Volkswirtschaft handeln, sollte dabei sowohl die mögliche Abschöpfung der Handelsmargen durch Inhaber zentraler Empfehlungsmacht als auch die Wettbewerbssituation zwischen Online- und Offline-Handel ins Kalkül gezogen werden und dazu überlegt werden, inwieweit eine agnostische Position hier noch vertretbar ist.

Eine mögliche Lösung könnte eine neutrale Instanz beinhalten, die Kundendaten klassischer Offline-Unternehmen treuhänderisch sammelt, aggregiert, Auswertungen bereitstellt und Mobile-Marketing-Kampagnen ermöglicht, bei denen der Kunde seine Datenhoheit behält und der stationäre Handel nicht übervorteilt, sondern gestärkt wird.

Apropos Innovation: Wenn Europa in der elektronischen Welt nicht auf Dauer nur hinterherlaufen will, wäre auch die Debatte um den elektronischen Euro, die die EZB sich bisher weigert zu führen, dringend angezeigt.

Die neuen Dienste werden kommen und Mobile Payment wird dabei eine zentrale Rolle spielen. Dies kann aktiv im Sinne des Verbrauchers mitgestaltet werden.

Annick Fuchs

Mobile Zahlungen – Zahlungsverkehrsrecht

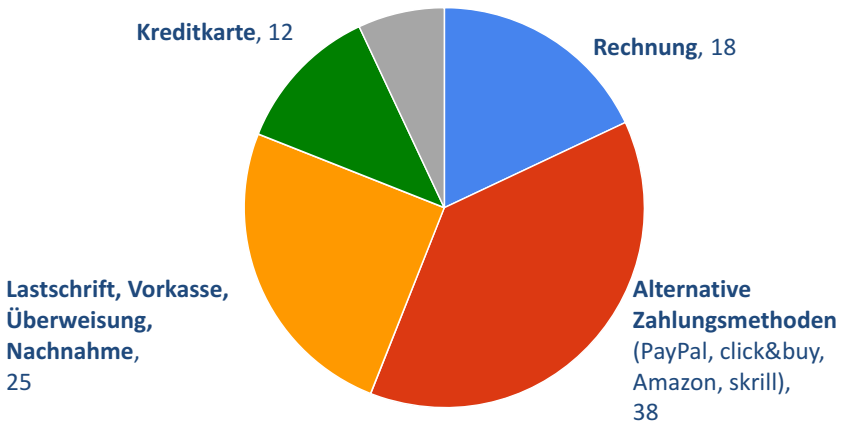
MOBILE ZAHLUNGEN – ZAHLUNGSVERKEHRSRECHT

Annick Fuchs
Leiterin Recht - PayPal Deutschland/Österreich/Schweiz
Rechtsanwältin, Attorney-of-law (California)

Nov 2013

PayPal Mit Sicherheit mehr Umsatz.

Präferenz Zahlungsweisen im Online Handel – Deutschland



Quelle: ECC des Instituts Für Handelsforschung, Köln, Studie “Zahlungsverkehr” Dez. 2012, www.ecckoeln.de

PayPal Mit Sicherheit mehr Umsatz.

Mobile Zahlungen — Seziert

Gemeinsamer Nenner

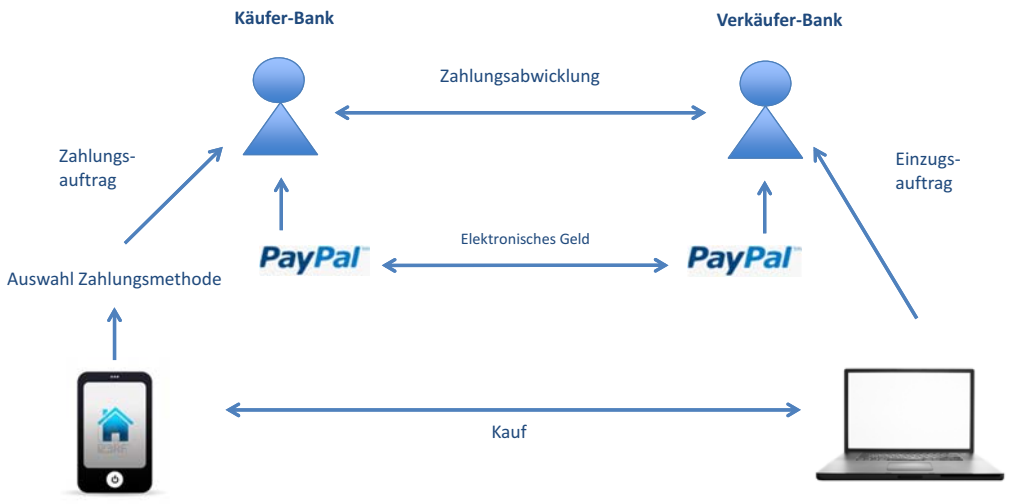
- Lastschrift (direkt oder als Zahlungsquelle)
- Kreditkarte (direkt oder als Zahlungsquelle)
- Online Überweisung (EFT)

- Auslöser:
  - Smartphone
  - Tablet
  - Computer
- Zahlung einstufig (Kreditkarte oder Lastschrift direkt)
- Zahlung mehrstufig (Einbindung eines oder mehrer Payment Service Provider — PSP)

3 Confidential and Proprietary

PayPal Mit Sicherheit mehr Umsatz.

Mobile Zahlungen* — Seziert

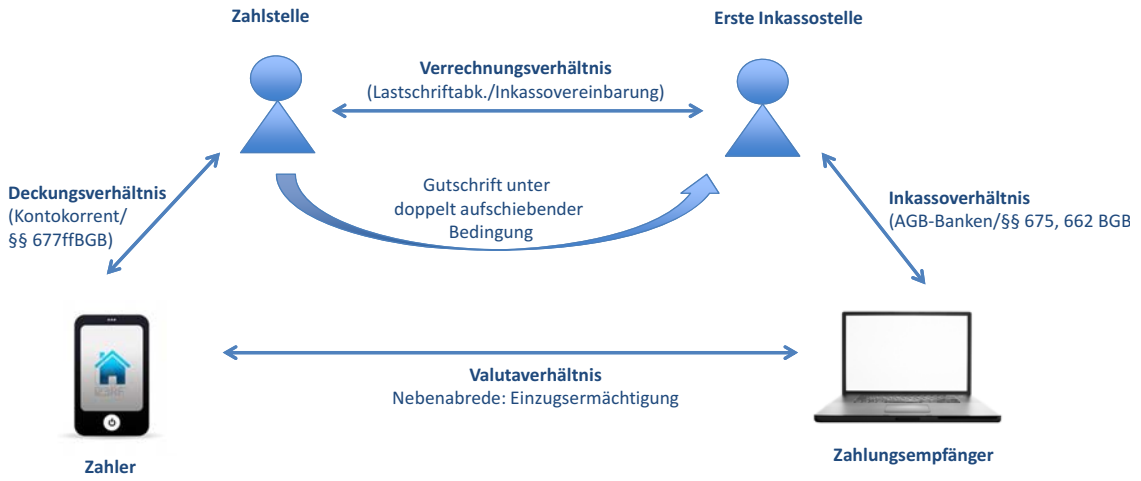


* Reduzierung auf Lastschrift, Kreditkarte, alternative Zahlungsmethoden

4 Confidential and Proprietary

PayPal Mit Sicherheit mehr Umsatz.

Rechtsverhältnisse bei Lastschrift*

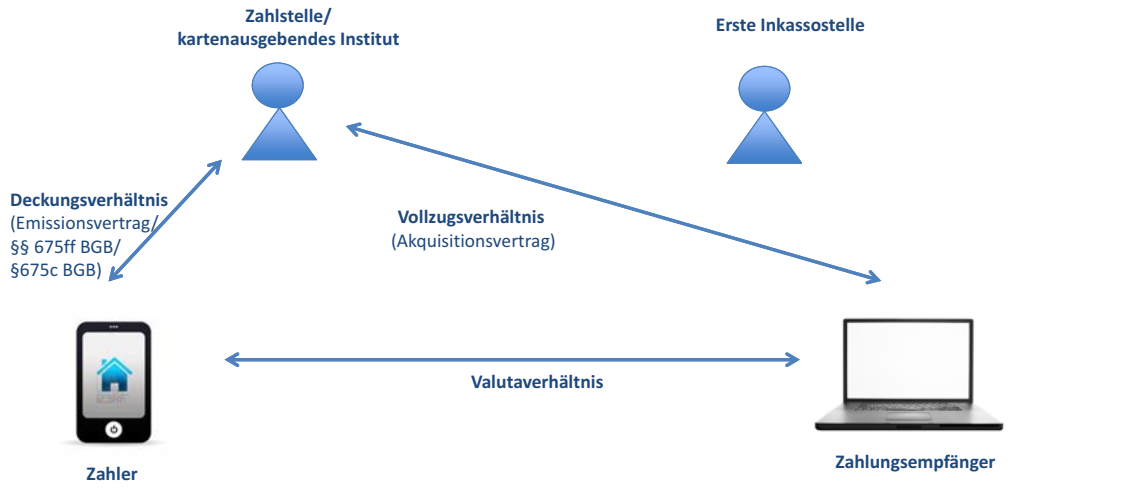


* Vor Inkrafttreten der Gesetzesänderungen durch SEPA (Single European Payment Area)

5 Confidential and Proprietary

PayPal Mit Sicherheit mehr Umsatz.

Rechtsverhältnisse bei Kreditkarte*

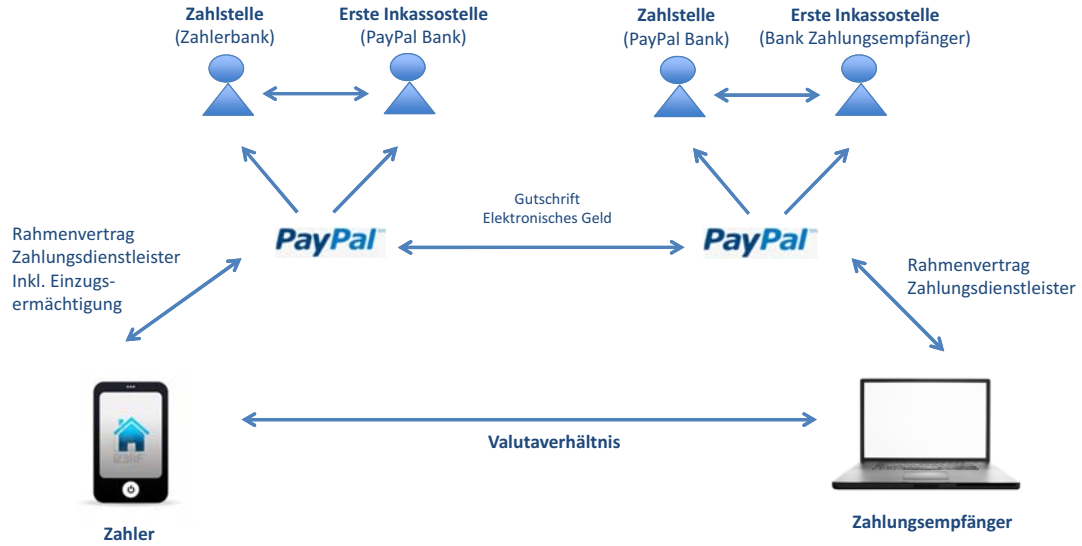


* Vor Inkrafttreten der Gesetzesänderungen durch SEPA (Single European Payment Area)

6 Confidential and Proprietary

PayPal Mit Sicherheit mehr Umsatz.

Rechtsverhältnisse bei alternativen Zahlmethoden



PayPal Mit Sicherheit mehr Umsatz.

Haftung bei online Zahlungen*

Lastschrift

- Lastschrift gilt als **unautorisierte Zahlung** nach § 675u BGB
- **Rückgabe** innerhalb von ca 6 Wochen möglich
- **Haftung**: Zahlungsempfänger = **Händler** auf vollen Betrag
- **Rechtsbehelf**: Vorgehen aus Valuta-verhältnis/Bereicherungsrecht

Kreditkarte

- **Garantie/Factoring** - Zahlungsstelle übernimmt Haftung für NSF und garantiert grds Zahlung
- **Haftung**: Zahlungsempfänger = **Händler** wenn kein Nachweis Autorisierung oder Verlust Kreditkarte plus Meldung durch Inhaber (je nach Akquisitionsvertrag), evtl: Nichtlieferung der Ware

Unauthorisierte Zahlungen

- Unautorisierte Zahlungen: § 675u BGB - ohne Zustimmung oder Genehmigung
- **Haftung**:
  - **Zahler** bei Vorsatz, grober Fahrlässigkeit und/oder Nichtmeldung des Verlusts von Zahlungsinstrumenten,§ 675v BGB
  - **Zahlungsdienstleister** in sonstigen Fällen
  - **Händler** bei Vereinbarung mit ZDL

Sicherheit durch alternative Zahlmethoden

- Intermediär Lastschriften/ Kartenzahlungen
- Käufer-/ Verkäuferschutzprogramme/ Zahlungsgarantie

* Vor Inkrafttreten der Gesetzesänderungen durch SEPA (Single European Payment Area)

PayPal Mit Sicherheit mehr Umsatz.

Verbraucherschutz

- **Lastschrift**
  - Kontokorrentvertrag/III Nr. 1 Lastschriftabkommen:
    - **Zahler-Verbraucher** kann innerhalb von 6 Wochen Lastschrift zurückgeben ohne Angaben von Gründen (post Sepa 8 Wochen)
    - **Empfänger-Verbraucher:** ungeschützt
- **Kreditkarte**
  - Je nach Akquisitionsvertrag:
    - **Zahler-Verbraucher**: ungeschützt es sei denn
      - Sittenwidriges Geschäft
      - PSP kann nicht beweisen, dass Zahlungsauftrag vorliegt oder
      - Zahler kann Verlust Karte plus Meldung geltend machen
    - **Empfänger-Verbraucher**:
      - grds. geschützt wenn ordnungswidriger Auftrag nachweisbar
      - bei NSF
      - ungeschützt bei unmögl. Nachweis Autorisierung und Verlust Karte plus Meldung und ggf. INR
- **Alternative Zahlungsmethoden**
  - Je nach Angebot:
    - **Zahler-Verbraucher**: SNAD und INR auch bei Kreditkarte, außerdem Lastschrift nicht überall angeboten
    - **Empfänger-Verbraucher**: Schutz bei Lastschriftrückgabe, NSF, Betrug

PayPal
Mit Sicherheit mehr Umsatz.

Prof. Dr. Robert Freitag

Aufsichtsrechtliche Aspekte von mobile payments

I. Einleitung

Der Markt für Bezahlsysteme ist in den letzten Jahren durch die starke Verbreitung mobiler Endgeräte mit Internetzugang (insbes. smartphones, tablets, laptops, ultrabooks etc.) erheblich in Bewegung geraten. Zahlreiche Anbieter haben unterschiedliche Systeme entwickelt, die Zahlungen mittels der genannten Endgeräte ermöglichen und die in Konkurrenz zu den etablierten mobilen Bezahlsystemen mit Bargeld oder Zahlungskarten treten bzw. treten sollen. Einen weiteren Schub hat diese Entwicklung mit der Einführung neuer Funkstandards wie Near Field Communication (NFC) und Bluetooth 3.0 sowie die optische Quick Response-Technologie (QR) erfahren, die die berührungslose Kommunikation mobiler Endgeräte mit stationären oder ebenfalls mobilen Transaktionsterminals gewerblich tätiger Zahlungsempfänger ermöglichen. In diesem Kontext stellt sich die Frage nach den aufsichtsrechtlichen Anforderungen an die Zulässigkeit derartiger innovativer Bezahlsysteme, die den Kreditinstituten das Geschäft mit dem bargeldlosen Zahlungsverkehr streitig machen.

II. Begriff der „mobile payments“ im weiteren Sinne

Die (aufsichts-)rechtliche Betrachtung der geschilderten Systeme setzt notwendig eine Definition des Begriffs des „mobilen Bezahlsystems“ voraus. Allerdings enthalten weder das deutsche noch das europäische Aufsichts- oder Zivilrecht in Form des Zahlungsdiensteaufsichtsgesetzes (ZAG),[1] der Zahlungsdiensterichtlinie[2] oder der E-Geld-Richtlinien[3] eine Legaldefinitionen mobiler Bezahlsysteme. Indes hat sich in der Praxis ein weitgehend konsentiertes Verständnis der mobilen Bezahlsystemen im weiteren Sinne etabliert: Danach handelt es sich um Bezahlsysteme, die die Auslösung, Bestätigung oder Übermittlung eines elektronischen[4] Bezahlvorgangs durch oder über[5] ein internettaugliches Telephon (smartphone), tablet oder ein vergleichbares mobiles Endgerät[6] ermöglichen.[7]

Derartige mobile Bezahlsysteme lassen sich weiter in vielfältigster Weise unterscheiden, etwa danach, ob sich der Zahler oder der Zahlungsempfänger des mobilen Endgerätes bedient, ob das verwendete mobile Endgerät zum Datentransfer über das Internet verwendet wird oder ob es ausschließlich Zahlungsdaten an das Händlerterminal übermittelt, ob die Kommunikation zwischen dem mobilen Endgerät und dem Terminal des Zahlungsempfängers drahtlos, optisch oder über das Internet erfolgt, ob das mobile Gerät dazu dient, Zahlungsdaten „klassischer“ Bezahlmittel (Daten von Zahlungskarten oder Kontoinformationen) zu übermitteln oder ob vorausbezahlte Guthaben zwischen Zahler und Zahlungsempfänger transferiert werden etc. Da die unterschiedlichen Ausgestaltungen derartiger Bezahlsysteme aus Sicht des Bankaufsichtsrechts je nach ihrer Ausgestaltung unterschiedlich zu beurteilen sein können, wird für die Zwecke der nachfolgenden Betrachtung differenziert.

---

1 Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz - ZAG), eingeführt als Art. 1 des Gesetzes zur Umsetzung der aufsichtsrechtlichen Vorschriften der Zahlungsdiensterichtlinie vom 25. 6. 2009, BGBl. I S. 1506.

2 Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG, ABl. L 319/1.

3 Richtlinie 2000/46/EG des Europäischen Parlaments und des Rates vom 18. September 2000 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, ABl. L 275/39, sowie Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG, ABl. 2009 L 267/7.

4 Die Zahlung mit baren Geldmitteln (Geldscheinen und/oder -münzen) ist damit nicht erfasst.

5 Es lässt sich danach differenzieren, ob der Bezahlvorgang im Einzelfall der Freigabe durch den jeweiligen Inhaber des mobilen Endgeräts bedarf oder ob er infolge der Installation eines entsprechenden Programms (einer app) „automatisch“ ausgelöst wird, wenn das Gerät Kontakt mit einem Bezahlterminal aufnimmt.

6 Nicht erfasst werden daher kartengestützte Bezahlvorgänge, die an einem stationären Terminal getätigt werden.

7 So die Definition in Ziffer 2.4 des Grünbuchs der Kommission „Ein integrierter europäischer Markt für Karten-, Internet- und mobile Zahlungen“, KOM(2011) 941 endgültig. Vgl. auch Deutsche Bundesbank, Monatsbericht September 2012, S. 51 f.; BITKOM, Positionspapier Mobile Payments vom 11.02.2013, http://www.bitkom.org/files/documents/Positionspapier_Mobile_Payments.pdf (abgerufen am 09.01.2014), S. 4; Bauer, Vertrauen in Mobile Payment Dienste (2012), 2.2.1.

Nicht zu analysieren sind an dieser Stelle die aufsichtsrechtlichen Aspekte des Einsatzes von Funktechniken wie NFC und Bluetooth, die den mobilen Endgeräten die Kommunikation mit händlerseitig eingesetzten stationären oder mobilen Bezahlterminals ermöglichen. Insoweit genügt an dieser Stelle der Hinweis, dass die Bundesnetzagentur gem. § 55 TKG bestimmte Frequenzbänder im Rahmen von Allgemeinzuteilungen für die Nutzung derartiger Drahtlostechniken freigegeben hat.

III. Bankaufsichtsrechtliche Aspekte mobiler Bezahlsysteme

1. Allgemeines

Den bankaufsichtsrechtlichen Erläuterungen zu den einzelnen Systemen voranzustellen ist die allgemeine Feststellung, dass die Anbieter solcher Bezahlsysteme, bei denen ein unmittelbarer Zugriff auf eine Konto erfolgt, Zahlungsdienste im Sinne des Zahlungsdiensteaufsichtsgesetzes (ZAG) erbringen.[8] Zahlungsdiensteanbieter[9] unterliegen im Interesse ihrer Kunden sowie der Allgemeinheit der Beaufsichtigung durch die BaFin[10] und bedürfen daher je nach Art des angebotenen mobilen Bezahlsystems gem. § 8 Abs. 1 bzw. § 8a ZAG[11] für die Aufnahme und Ausübung ihrer Tätigkeit grundsätzlich der Erlaubnis. Hinzu kommen umfangreiche Anforderungen an die Eigenkapitalausstattung der Zahlungsdiensteanbieter (§ 12, § 12a ZAG), an die Absicherung der zu Zahlungszwecken vereinnahmten Kundengelder (§ 13, § 13a ZAG), die Zuverlässigkeit der Geschäftsleitung, spezielle Bilanzierungsregeln etc. (§§ 14 ff. ZAG).

Die genannten Anforderungen des ZAG gelten nicht für Kreditinstitute, die das Einlagen- und Kreditgeschäft betreiben und zusätzlich mobile Bezahldienste anbieten, da die § 8 Abs. 1, § 8a Abs. 1 ZAG die Erlaubnispflicht auf „Zahlungsinstitute“ iSd § 1 Abs. 1 Nr. 5 bzw. § 1a Abs. 1 Nr. 5 ZAG beschränken, zu denen solche Kreditinstitute nicht zählen, die im Sinne des Art. 4 lit. a der Bankenrichtlinie 2006/48/EG[12] (umgesetzt in § 1 Abs. 1 Nr. 1, Nr. 2 KWG) das Einlagen- und Kreditgeschäft betreiben. Hinter dieser Befreiung steht die Erwägung, dass die Erlaubnis zur Ausübung des riskanteren Einlagen- und Kreditgeschäfts iSd KWG die Erlaubnis zum weniger gefährlichen Angebot von Zahlungsdiensten nach dem ZAG umfasst, zumal der Betrieb des Einlagen- und Kreditgeschäfts fast notwendigerweise mit dem Angebot von Zahlungsverkehrsgeschäften verbunden wird.[13]

2. Einsatz mobiler Endgeräte durch den Zahler im Rahmen des „mobile banking“

Keine aufsichtsrechtlichen Besonderheiten bestehen in Bezug auf Bezahlvorgänge, bei denen der Zahler das mobile Endgerät lediglich wie einen stationärer Computer einsetzt, um ohne unmittelbare Kontaktaufnahme mit einem Gerät des Zahlungsempfängers Zahlungen im Rahmen des kontobasierten Internetbankings zu veranlassen (sog. „mobile banking“). Derartige Transaktionen unterscheiden sich in keiner Weise vom sonstigen Internetbanking über einen stationären Computer, d.h. das kontoführende Institut erbringt dem Zahler gegenüber einen Zahlungsdienst im Sinne des § 1 Abs. 2 Nr. 2 ZAG, wobei es vom Einzelfall abhängt, ob die Erteilung eines Überweisungsauftrags, die Autorisierung einer Lastschrift oder der online-Einsatz einer Zahlungskarte vorliegt. Die Erlaubnispflicht für die vom kontoführenden bzw. kartenemittierenden Kreditinstitut ausgeübte Tätigkeit beruht in diesem Fall auf den bereits unter 1. erwähnten § 8, § 8a ZAG.[14]

3. Einsatz mobiler Endgeräte durch den Zahlungsempfänger (mobile point of sale)

Ebenfalls weithin unproblematisch ist der Einsatz mobiler Bezahlsysteme durch den Zahlungsempfänger. Hier werden ganz überwiegend mobile Kartenlesegeräte verwendet, die drahtlos (per bluetooth) oder über

---

8 Zur Definition des Zahlungsverkehrsgeschäfts vgl. § 1 Abs. 2 ZAG; zu den Einzelheiten der jeweils ausgeübten Tätigkeiten sogleich.
9 Zum Begriff vgl. § 1 Abs. 1 ZAG.
10 Zur Zuständigkeit der BaFin für die Beaufsichtigung von Zahlungsdienstleistungsunternehmen vgl. § 3 ZAG.
11 Maßgeblich ist, ob die Zahlung über ein Bankkonto (§ 8 ZAG) oder über ein Konto bei einem E-Geld-Anbieter (§ 8a ZAG) abgewickelt wird. Auf die Abgrenzung ist an dieser Stelle noch nicht einzugehen.
12 Richtlinie 2006/48/EG vom 14. Juni 2006 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute (Neufassung), ABl. L 177/1.
13 Vgl. Erwägungsgrund (8) zur Zahlungsdiensterichtlinie (Nachw. oben Fn. 2).
14 § 8 ZAG gelangt beim Zugriff auf ein online-Konto bei einer Bank zur Anwendung, während § 8a ZAG den Fall regelt, dass über ein E-Geld-Guthaben verfügt wird. Auf diese Differenzierung ist an dieser Stelle nicht näher einzugehen.

eine Kabelverbindung an das mobile Endgerät des Zahlungsempfängers angeschlossen werden. Das Lesegerät liest die Daten der von den Zahlern verwendeten Zahlungskarten aus, die mittels einer auf dem mobilen Endgerät installierten Software (app) verarbeitet und anschließend über dessen Internetverbindung an einen Zahlungsdienstleister des Zahlungsempfängers transferiert werden. Spezielle bankaufsichtsrechtliche Probleme, die eine vom Einsatz stationärer Kartenterminals abweichende rechtliche Betrachtung erforderten, bestehen nicht. Insbesondere spielt es bankaufsichtsrechtlich weder eine Rolle, ob die Daten der vom Zahler eingesetzten Zahlungskarten an den Zahlungsdienstleister des Händlers über ein festes Datenkabel transferiert oder drahtlos über ein Mobiltelephon an den nächsten Sendemast übertragen und anschließend in das Festnetz eingespeist werden.

4. Verwendung mobiler Endgeräte durch den Zahler im Rahmen von mobile payments im engeren Sinne

Unter den Bezahlsystemen, die es dem Zahler ermöglichen, über sein mobiles Endgerät Transaktionen abzuwickeln oder anzustoßen, ist zu unterscheiden:

a) mobile payments mit E-Geld

Zu den neueren Entwicklungen im Bereich mobiler Bezahlsysteme zählt der Transfer von E-Geld (e-money) mittels mobiler Endgeräte vom Zahler an den Zahlungsempfänger. Nach der Legaldefinition des § 1a Abs. 3 ZAG handelt es sich bei E-Geld um „jeden elektronisch, darunter auch magnetisch, gespeicherten monetären Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um damit Zahlungsvorgänge im Sinne des § 675f Ab satz 3 Satz 1 des Bürgerlichen Gesetzbuchs durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem Emittenten angenommen wird.“

Die betreffenden mobilen Bezahlsysteme unterscheiden sich von Zahlungen über herkömmliche Bankkonten iSd mobile banking (dazu oben 2.) wirtschaftlich im Wesentlichen dadurch, dass die Zahlung nicht über die jeweiligen (häufig nicht identischen) Kreditinstitute von Zahler und Zahlungsempfänger abgewickelt wird, sondern über einen speziellen Zahlungsdienstleister, mit dem beide Parteien des Bezahlvorgangs jeweils eine Kontobeziehung[15] unterhalten. Im Ergebnis entspricht die Situation bei der Bezahlung mittels E-Geld daher im Wesentlichen der Hausüberweisung, die den Vorteil hat, sofort ausgeführt werden zu können. Aufgrund des Umstands, dass E-Geld stets vorausbezahlt sein muss (dazu sogleich) und E-Geld-Konten folglich stets auf Guthabenbasis geführt werden, hat der Zahlungsempfänger unmittelbar im Anschluss an die Autorisierung der Zahlung durch den Zahler Gewissheit darüber, dass die Zahlung erfolgreich irreversibel zu seinen Gunsten ausgeführt worden ist.

Es versteht sich von selbst, dass E-Geld die von den Marktteilnehmern intendierte Werttransferfunktion nur erfüllen kann, wenn die emittierten Werteinheiten iSd § 1a Abs. 3 ZAG auch von anderen Personen als dem Emittenten zu Zahlungszwecken akzeptiert werden. Bezahlsysteme im Rahmen von „Insellösungen“, bei denen gegen Leistung gesetzlicher Zahlungsmittel ausgegebene elektronische Guthaben ausschließlich vom Emittenten selbst akzeptiert werden (z.B. Kantinenkarten, Gutscheinsysteme eines Anbieters etc.), fallen daher nicht in den Anwendungsbereich der Bestimmungen für das E-Geld-Geschäft, wobei die Abgrenzung im Einzelfall erhebliche Schwierigkeiten bereiten kann.

An die Emission von E-Geld und die Durchführung des E-Geldgeschäfts stellt das Aufsichtsrecht besonders strenge Anforderungen. So darf E-Geld gem. § 1a Abs. 3 ZAG nur gegen Zahlung mit gesetzlichen Zahlungsmitteln ausgegeben werden, d.h. E-Geld ist stets vorauszubezahlen,[16] wobei indes auch die Zur-Verfügung-Stellung von E-Geld gegen Erteilung einer Lastschriftermächtigung durch den Zahler gestattet ist.[17] E-Geld-Instituten ist es im Übrigen untersagt, das Einlagengeschäft zu betreiben, d.h. E-Geld-Guthaben dürfen nicht verzinst werden (§ 2 Abs. 1a S. 3 ZAG) und können von

15 E-Geld kann nach der Legaldefinition des § 1a Abs. 3 ZAG auch „kontenbasiert“ gespeichert werden, vgl. Regierungsbegründung zum ZAG, BT-Drucks. 17/3023, S. 40.

16 Dabei hat der Umtausch „unverzüglich“ zu erfolgen, § 2 Abs. 1a S. 1 ZAG, und muss der Nennwert des erworbenen E-Geld-Guthabens gem. § 23b Abs. 1 S. 1 ZAG zwingend dem Nennwert des eingesetzten gesetzlichen Bar- oder Buchgelds entsprechen.

17 § 2 Abs. 3 S. 2 ZAG gestattet den kreditfinanzierten Erwerb von E-Geld.

den Kunden gem. § 23b Abs. 1 S. 2 ZAG jederzeit wieder gebührenfrei in gesetzliche Zahlungsmittel zurückgetauscht werden. Ebenso wenig dürfen E-Geld-Guthaben zur Kreditvergabe verwendet werden, soweit die Kreditvergabe nicht der Durchführung von E-Geld-Zahlungen dient, § 2 Abs. 3 S. 2 ZAG.

Im Ergebnis ist die Rentabilität des E-Geld-Geschäfts daher einschränkt, was dazu geführt hat, dass ehemalige Anbieter von E-Geld zwischenzeitlich die Zulassung als Kreditinstitute beantragt haben, um auch das Einlagen- und Kreditgeschäft anbieten zu können.

b) Wallet-Lösungen (digitale Brieftaschen)

Erheblicher Beliebtheit bei den mobilen Bezahlsystemen erfreuen sich auch sog. „wallet-Lösungen“. Diese sind dadurch charakterisiert, dass der Kunde auf seinem mobilen Endgerät (oder auf einem über das Endgerät aufrufbaren Server) – in der Regel kennwortgeschützt – die erforderlichen Informationen über Bankkonten, E-Geld-Konten und Zahlungskarten speichert. Der Zahler kann sodann bei jedem Bezahlvorgang über das mobile Endgerät auswählen, über welchen Zahlungsweg die Transaktion abzuwickeln ist, regelmäßig ist er dabei zugleich dazu in der Lage, die betreffende Transaktion zu initiieren. Auf diesem Weg kann sich der Zahler die mühsame händische Eingabe von Kontoinformationen in entsprechende Felder von online-Bestellformularen ersparen, da die relevanten Zahlungsdaten unmittelbar an den Zahlungsempfänger oder den einschlägigen Zahlungsdienstleister übermittelt werden.

Bankaufsichtsrechtlich bedürfen derartige wallet-Lösungen solange keiner speziellen Erlaubnis, als allein die Zahlungsdaten elektronisch übermittelt werden. Anders liegt es, wenn mit einem auf dem mobilen Endgerät installierten Programm (app) unmittelbar ein Zugriff des Zahlers auf ein in der digitalen Brieftasche hinterlegtes Bank- oder E-Geld-Konto erfolgt. In diesem Fall sind die Anforderungen an das mobile banking zu beachten, das wiederum keinen spezifischen Anforderungen im Hinblick auf das verwendete mobile Endgerät unterliegt (dazu oben unter 2.).

IV. Schlussbemerkung

Im Bereich der mobile payments ist innerhalb Europas eine erhebliche regulatorische arbitrage zu beobachten: Aufsichtsrechtliche Unterschiede im Hinblick auf E-Geld-Institute bestehen innerhalb der Europäischen Union a priori nicht, da das Zahlungsverkehrsrecht durch die Zahlungsdiensterichtlinie sowie die E-Geld-Richtlinien – vorbehaltlich einzelner explizit gewährter Umsetzungsspielräume abschließend unionsrechtlich harmonisiert ist. Auch grundsätzlich einheitliche Aufsichtsregeln können allerdings uneinheitlich implementiert werden: Hierzu kann es nicht allein durch eine mehr oder minder strenge Anwendung der einheitlichen Normen kommen, sondern auch unterschiedliche (In-)Flexibilität im Umgang mit den (potentiellen) Anbietern. Beispielhaft genannt seien die vergleichsweise knappen Erläuterungen der deutschen BaFin zum ZAG[18] sowie die wesentlich umfassendere online-Dokumentation der englischen Financial Conduct Authority zu e-money[19]. Insbesondere E-Geld-Systeme, die von mobilen Endgeräten aus bedient werden können, werden jedenfalls ganz überwiegend von Großbritannien, Irland oder Luxemburg aus angeboten, nicht hingegen von Deutschland aus,[20] was selbstverständlich auch steuerliche und sonstige, nicht aufsichtsrechtlich bedingte wirtschaftliche Gründe haben kann.

Ob sich im Übrigen mobile Bezahlsysteme in der Praxis durchsetzen werden, hängt auch und vor allem von wirtschaftlichen Erwägungen ab. Insbesondre bewirkt die starke Fragmentierung des Marktes der mobilen Bezahlsysteme, d.h. die geringe Marktdurchdringung der bereits vorhandenen Angebote, sowohl auf Seiten der Händler wie der Verbraucher große Zurückhaltung. Denn derzeit ist noch nicht vorhersehbar, welche(s) System(e) sich letztlich in der Praxis durchsetzen wird bzw. werden. Darüber hinaus bestehen aus Sicht der potentiellen Nutzer noch immer erhebliche Vorbehalte gegenüber mobilen Bezahlsystemen und dem Aspekt der Datensicherheit.

---

18 Abrufbar unter http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html (zuletzt aufgerufen am 10.01.2014).

19 Abrufbar unter http://www.fca.org.uk/firms/firm-types/emoney-institutions mit zahlreichen weiteren links (abgerufen am 10.01.2014).

20 Die BaFin listet derzeit unter Verstoß gegen § 30a ZAG, der die Einrichtung eines eigenen Registers für E-Geld-Institute vorschreibt, das nicht existiert im allgemeinen Register der Kreditinstitute insgesamt 4 E-Geld-Institute auf (abrufbar unter http://www.bafin.de/SharedDocs/Downloads/DE/Liste/Unternehmensdatenbank/dl_li_ki_gesamt.html?nn=2814084, abgerufen am 10.01.2014). Demgegenüber finden sich etwa im speziellen Register der e-money institutions der FSA (abrufbar unter http://www.fsa.gov.uk/register/2EMD/2EMD_MasterRegister.html, abgerufen am 10.01.2014) über 40 Einträge.

Impressionen der Veranstaltung


Bundesministerium für
Ernährung, Landwirtschaft
und Verbraucherschutz
Bamberger Verbraucherrechtstage

Lebensläufe der Autorinnen und Autoren

Arbeitsgruppe 1

Patrick von Braunmühl

Geschäftsführer
Selbstregulierung Informationswirtschaft e. V.

Patrick von Braunmühl ist Geschäftsführer des gemeinnützigen Vereins Selbstregulierung Informationswirtschaft (SRIW), dessen Ziel die Förderung von Datenschutz und Verbraucherschutz durch Instrumente der Selbstregulierung ist. Gründungsmitglieder sind der ITK-Verband BITKOM sowie führende Unternehmen der Internetbranche.

Vorher war Herr von Braunmühl unter anderem als stellvertretender Vorstand beim Bundesverband der Verbraucherzentralen (vzbv), als Projektleiter für die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) in Indien, als Mitglied der Geschäftsleitung von Cisco Systems und als Leiter der Rechtsabteilung der Bertelsmann Tochter Lycos Europe tätig. Herr von Braunmühl ist Volljurist und als Rechtsanwalt niedergelassen.

Arbeitsgruppe 1

Prof. Dr. Gerald Spindler

Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Multimedia- und Telekommunikationsrecht
Universität Göttingen

Prof. Dr. Gerald Spindler, Dipl.-Ökonom, geboren 1960, hat Rechtswissenschaften und Wirtschaftswissenschaften in Frankfurt am Main, Hagen, Genf und Lausanne studiert und beide Staatsexamina absolviert. Nach einer Assistentenzeit bei Prof. Dr. Mertens, Frankfurt, sowie am Institut für Internationales und Ausländisches Wirtschaftsrecht, Frankfurt, promovierte er 1993 mit einer rechtsvergleichenden Arbeit über das Thema „Recht und Konzern".

Die Habilitation erfolgte 1996 mit einer Arbeit über „Unternehmensorganisationspflichten", wobei ihm die Lehrbefugnis für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Internationales Privatrecht, Rechtsvergleichung und Arbeitsrecht verliehen wurde.

Prof. Dr. Gerald Spindler ist seit 1997 nach Ablehnung von Rufen an die Universitäten zu Köln, Bielefeld, Frankfurt sowie die ETH Zürich Ordinarius für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Rechtsvergleichung, Multimedia- und Telekommunikationsrecht an der Universität Göttingen und beschäftigt sich schwerpunktmäßig einerseits mit Rechtsfragen des E-Commerce bzw. Internet- sowie Telekommunikationsrechts, des Urheber- und Immaterialgüterrechts, andererseits mit Problemen des Gesellschafts- und Kapitalmarktrechts.

Arbeitsgruppe 1

Prof. Niko Härting

Härting Rechtsanwälte

Niko Härting ist Gründungspartner von HÄRTING Rechtsanwälte (www.haerting.de).

Der Fokus der Beratung liegt auf dem Medien- und Internetrecht.

Niko Härting ist Autor des Werkes „Internetrecht“, das soeben in der 5. Auflage erschienen ist.

Er ist zudem Herausgeber der Zeitschrift „Privacy in Germany“ (PinG), Honorarprofessor an der Hochschule für Wirtschaft und Recht (HWR Berlin) und Lehrbeauftragter an der Freien Universität Berlin.

Arbeitsgruppe 1

Dr. Thilo Weichert

Landesbeauftragter für den Datenschutz Schleswig-Holstein

Jurist u. Politologe, Studium in Freiburg und Genf/Schweiz

1984 bis 1986 Landtagsabgeordneter in Baden-Württemberg

Von 1982 an Tätigkeiten als Rechtsanwalt, Politiker, Publizist, Dozent in Freiburg, Stuttgart, Dresden und Hannover

1991 Justiziar beim Sächsischen Landtag, zugleich juristischer Berater des Bürgerkomitees zur Auflösung der Staatssicherheit

1990 bis 2004 Vorsitzender der Deutschen Vereinigung für Datenschutz (DVD)

1992 bis 1998 Referent beim Landesbeauftragten für den Datenschutz in Niedersachsen

Von 1998 an Stellvertretender Landesbeauftragter für Datenschutz Schleswig-Holstein in Kiel

Seit 2004 Landesbeauftragter und damit Leiter des Unabhängigen Landeszentrums für Datenschutz in Kiel (ULD)

Arbeitsgruppe 2

Jutta Gurkmann

Leiterin Team Recht & Internationales
Verbraucherzentrale Bundesverband e.V. (vzbv)

Nach dem Studium der Rechtswissenschaften in Heidelberg und der Referendarszeit, die sie u.a. am Gerichtshof für Menschenrechte in Straßburg absolvierte, begann Jutta Gurkmann 2002 als Juristin bei EURO-INFO-VERBRAUCHER e.V., einem deutsch-französischen Verein, dessen Aufgabe die Information und Beratung europäischer Verbraucher in grenzüberschreitenden Angelegenheiten ist. 2006 übernahm sie die Leitung des dort angesiedelten Europäischen Verbraucherzentrums Deutschland. Tätigkeitsschwerpunkte waren hier das deutsche und europäische Zivilrecht sowie das Internationale Privatrecht.

Ab Oktober 2009 war Frau Gurkmann als Referentin für Wirtschaftsrecht für den Verbraucherzentrale Bundesverband e.V. tätig, wo sie sich vor allem um Fragen des europäischen Verbraucher- und Vertragsrechts, des Kartellrechts, des Verbraucherinformationsrechts sowie der Sammelklagen und der Schlichtung kümmert. Seit Juli 2013 ist sie dort Leiterin des Teams Recht & Internationales.

Arbeitsgruppe 2

Adél Holdampf-Wendel

Bereichsleiterin Medien- und Netzpolitik,
Wettbewerbs- und Verbraucherrecht
Bundesverband Informationswirtschaft, Telekommunikation
und neue Medien (BITKOM)

Adél Holdampf-Wendel ist Bereichsleiterin beim Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) in Berlin. Sie betreut die Themenfelder Medien- und Netzpolitik sowie Wettbewerbs- und Verbraucherrecht. Schwerpunkte Ihrer Tätigkeit bilden derzeit insbesondere die Rundfunk- und Plattformregulierung, der Jugendmedienschutz sowie Rechtsfragen des elektronischen Geschäftsverkehrs und des unlauteren Wettbewerbs.

Vor ihrer Tätigkeit bei BITKOM arbeitete Frau Holdampf-Wendel drei Jahre lang in der Europäischen Kommission in Brüssel als Referentin („Case Handler“) im Bereich der Telekommunikationsmarktregulierung der Generaldirektion Informationsgesellschaft und Medien (jetzt GD CONNECT).

Überdies war sie als Fachreferentin für Informationsgesellschaft und Telekommunikation im Generalsekretariat des Europäischen Parlaments, ebenfalls in Brüssel, tätig.

Frau Holdampf-Wendel studierte Rechtwissenschaften und erwarb Studienabschlüsse an der Eötvös Lóránt Universität (ELTE) in Budapest sowie an der Humboldt Universität zu Berlin.

Sie ist Autorin im Berliner Kommentar zum Telekommunikationsgesetz.

Arbeitsgruppe 2

Michael Neuber

Justiziar im Bundesverband Digitale Wirtschaft (BVDW) e.V.

Michael Neuber ist Rechtsanwalt und berät als Justiziar den Bundesverband Digitale Wirtschaft (BVDW) e.V. und dessen Mitglieder in Rechtsfragen vor allem in den Bereichen Datenschutz, Urheber- und Medienrecht.

Neben dem Forum Recht unterstützt er außerdem maßgeblich die Arbeit des Forums Medien- und Netzpolitik.

Seit 2009 ist er Lehrbeauftragter an der Hochschule für Wirtschaft und Recht (HWR) sowie an der German open Business School (GoBS) Hochschule für Wirtschaft und Verwaltung.

Arbeitsgruppe 2

Prof. Dr. Martin Schmidt-Kessel

Lehrstuhl für Deutsches und Europäisches Verbraucherrecht und Privatrecht sowie Rechtsvergleichung
Universität Bayreuth

Prof. Dr. Martin Schmidt-Kessel studierte von 1988 bis 1993 Rechtswissenschaften an den Universitäten Freiburg, München und Köln.

Von 1993 bis 1998 war er wissenschaftlicher Angestellter am Institut für ausländisches und Internationales Privatrecht der Albert-Ludwigs-Universität Freiburg. Von 1998 bis 2003 war er Wissenschaftlicher Assistent der Universität Freiburg, zunächst am Institut für ausländisches und internationales Privatrecht und dann am Institut für Wirtschaftsrecht, Arbeits- und Sozialversicherungsrecht. 2001 wurde Prof. Dr. Martin Schmidt-Kessel promoviert. 2003 erfolgte die Habilitation durch die Rechtswissenschaftliche Fakultät der Universität Freiburg.

Im selben Jahr erhielt er einen Ruf auf einen Lehrstuhl für Bürgerliches Recht, Europäisches Privat- und Wirtschaftsrecht an der Universität Osnabrück. 2004 bis 2010 hatte er eine Professur im European Legal Studies Institute der Universität Osnabrück inne und war dort zuletzt Direktor der zivilrechtlichen Abteilung des Instituts.

Seit 2007 hat er regelmäßig Forschungs- und Lehraufenthalte an der Università degli Studi di Verona. 2010 nahm Prof. Dr. Martin Schmidt-Kessel einen Ruf an die Universität Bayreuth an. Dort ist er Inhaber des vom BMEL finanzierten Stiftungslehrstuhls für Verbraucherrecht sowie Direktor der Forschungsstelle für Verbraucherrecht sowie Mitglied in den Forschungsstellen für Familienunternehmen, Deutsches und Europäisches Lebensmittelrecht sowie für Deutsches und Europäisches Energierecht. Seit 2011 ist er Mitglied im Wissenschaftlichen Beirat „Verbraucher- und Ernährungspolitik“ des Bundesministeriums für Ernährung und Landwirtschaft.

Arbeitsgruppe 3

PD Dr. Key Pousttchi

Forschungsgruppe wi-mobile
Universität Augsburg

Key Pousttchi ist einer der international führenden Mobile-Business-Experten.

Er baute ab 2001 die Forschungsgruppe wi-mobile an der Universität Augsburg auf und ist bislang der einzige deutschsprachige Wirtschaftsinformatiker, der zum Mobile Business promoviert (2004 zu M-Payment) und habilitiert (2009 zum Einsatz von Mobile Business in Unternehmen und Angeboten für Endkunden) wurde.

Vortragstätigkeit und Projekte führten ihn nach Nordamerika, Asien und Afrika, seine Arbeiten wurden vielfach ausgezeichnet.

Er ist Inhaber der wi-mobile Dr. Pousttchi GmbH, in der Praxis als Strategieberater, Keynote-Speaker und Aufsichtsrat tätig sowie gefragter Gesprächspartner der Medien, von Deutschlandfunk und ZDF bis zur “New York Times”.

2013 holte er die International Conference on Mobile Business im zwölften Jahr ihres Bestehens erstmals nach Deutschland.

Arbeitsgruppe 3

Annick Fuchs

Leiterin Rechtsabteilung D/A/CH
PayPal Deutschland GmbH

Annick Fuchs ist seit Februar 2010 in der Rechtsabteilung von PayPal, Region Deutschland, Österreich, Schweiz bei der PayPal Deutschland GmbH.

Sie studierte Jura in Freiburg im Breisgau, Baden-Württemberg und im italienischen Verona. Neben dem Erwerb des ersten deutschen Staatsexamens in Freiburg setzte sie Schwerpunkte auf internationales Recht. Ihr Rechtsreferendariat absolvierte sie in Nordrhein-Westfalen.

Die gebürtige Pariserin startete ihre Karriere in Los Angeles, USA, bei White & Case LLP, einer internationalen Großkanzlei mit Schwerpunkt im Intellectual Property und internationalen Wirtschaftsrecht. Zusätzlich qualifizierte sie sich im US-Amerikanischen Recht und ist seitdem zugelassene Anwältin (Attorney-at-law) im amerikanischen Bundestaat Kalifornien.

Im Anschluss arbeitete sie vier Jahre in der internationalen Großkanzlei Freshfields Bruckhaus Deringer LLP in Frankfurt am Main mit Schwerpunkten im Gesellschafts- und im Bankenrecht. Zu ihren betreuten Mandaten gehören großvolumige Übernahmen in der Automobil-/Banken- und Industriegüterbranche sowie der anwaltlichen Beratung durch Gutachten im Bankaufsichtsrecht.

Bei der PayPal Deutschland GmbH liegt ihr Schwerpunkt in der rechtlichen Beratung und Begleitung sämtlicher Rechtsfragen in Deutschland, Österreich und der Schweiz, insbesondere im internationalen Bankenaufsichtsrecht, im e-commerce und im Urheber- und Medienrecht. Bei PayPal leitet Annick Fuchs seit 2011 nun die Rechtsabteilung, die mittlerweile aus einem Team von 4 Volljuristen besteht.

Annick Fuchs ist in Frankfurt am Main aufgewachsen.

Mit den Hobbies Laufen, Yoga, Tennis, Bergsteigen zeigt sich Annick Fuchs auch als passionierter Sportlerin.

Annick Fuchs spricht neben der Muttersprache Deutsch zusätzlich Englisch, Französisch und Italienisch fließend und hat Grundkenntnisse in Schwedisch.

Arbeitsgruppe 3

Prof. Dr. Robert Markus Freitag

Lehrstuhl für Deutsches, Europäisches und Internationales Privat- und Wirtschaftsrecht an der Friedricht-Alexander-Universität Erlangen-Nürnberg (FAU)

Prof. Dr. Robert Markus Freitag, Maître en droit (Bordeaux), geboren 1968 in Göttingen. Studium der Rechtswissenschaften in Göttingen, Bordeaux und Bayreuth, 1991 Maîtrise en droit (Bordeaux), 1993 Erste Juristische Staatsprüfung (Bayreuth), 1996 Zweite Juristische Staatsprüfung (Bayreuth). 1996-1999 Wissenschaftlicher Mitarbeiter/Assistent am Lehrstuhl von Prof. Dr. Ulrich Spellenberg (Universität Bayreuth), 1999-2000 Wissenschaftlicher Mitarbeiter/Assistent am Lehrstuhl von Prof. Dr. Thomas Pfeiffer (Universität Bielefeld). 2000 Promotion an der Universität Bayreuth, Titel der Doktorarbeit: „Der Einfluss des Europäischen Gemeinschaftsrechts auf das Internationale Produkthaftungsrecht". 2002-2002 Tätigkeit als Syndikusanwalt bei einer Großbank in München. Von 2002-2005 Wissenschaftlicher Assistent am Lehrstuhl von Prof. Dr. Ulrich Spellenberg (Bayreuth), 2005 Habilitation in Bayreuth, Titel der Habilitationsschrift:
„Der Darlehensvertrag im System des Schuldrechts". 2006-2011 zunächst Vertreter, später Inhaber des Lehrstuhls für Bürgerliches Recht, Deutsches und Europäisches Handels- und Gesellschaftsrecht an der Fakultät für Rechtswissenschaft der Universität Hamburg und Gründer sowie Direktor der Forschungsstelle für Bank- und Kapitalmarktrecht an der Universität Hamburg. Seit 2011 Inhaber des Lehrstuhls für Deutsches, europäisches und inter-nationales Privat- und Wirtschaftsrecht an der Friedricht-Alexander-Universität Erlangen-Nürnberg (FAU), seit 2013 Gründer sowie Direktor der Forschungsstelle für Bank- und Kapitalmarktrecht in Nordbayern an der FAU.

Herausgeber
Bundesministerium für Ernährung
und Landwirtschaft (BMEL)
Wilhelmstraße 54
10117 Berlin

Stand
März 2014

Autoren
Patrick von Braunmühl, Prof. Dr. Robert Freitag, Annick Fuchs, Jutta Gurkmann,
Adél Holdampf-Wendel, Prof. Niko Härting, Michael Neuber, PD Dr. Key Pousttchi,
Prof. Dr. Martin Schmidt-Kessel, Prof. Dr. Gerald Spindler, Thilo Weichert

Gestaltung
BMEL

Druck
BMEL

Fotos
fotolia; Charlotte Moser

Weitere Informationen finden Sie im Internet unter
www.bmel.de