# Kommunikation & Recht

## Betriebs-Berater für
## ● Medien ● Telekommunikation ● Multimedia

1
K&R



16. Jahrgang Januar 2013 Seiten 1 – 72

Deutscher Fachverlag GmbH · Frankfurt am Main

treiber von Funknetzwerken erstrecken. Zum anderen soll die Privilegierung auch auf Unterlassungsansprüche anwendbar sein. Im Gegensatz zum Vorschlag der Berliner Regierungskoalition werden keine technischen Schutzmaßnahmen normiert. Die Digitale Gesellschaft e. V. möchte mit diesem Gesetzentwurf Rechtssicherheit schaffen und die Teilhabemöglichkeiten insbesondere sozial schwächerer Erwachsener und Jugendlicher am Internet verbessern sowie insgesamt einen flächendeckenden Internetzugang für jedermann erreichen. Der Gesetzentwurf ist von der Bundestagsfraktion Die Linke übernommen und Ende Oktober 2012 in den Bundestag eingebracht worden.[46]

## IV. Fazit

Die Haftungsrisiken, die beim Betrieb des WLAN bestehen, sind nach der aktuellen Rechtslage überschaubar, soweit sichergestellt ist, dass geeignete Schutzmaßnahmen gegen eine unbefugte Nutzung des Netzwerkes getroffen werden. Die Gefahr, als WLAN-Betreiber wegen Urheberrechtsverletzungen, die von WLAN-Nutzern gegenüber Dritten begangen wurden, abgemahnt zu werden, bleibt in Anbetracht der unsicheren Rechtslage jedoch grundsätzlich bestehen. Da die zu diesen Haftungsfragen bisher ergangene Rechtsprechung nicht einheitlich ist, ist auch in Anbetracht der Ausprägungen, die das Abmahnwesen derzeit ausgebildet hat, eine klärende Regelung durch den Gesetzgeber geboten.

Es bleibt zu hoffen, dass die skizzierten sozial- und netzpolitischen Erwägungen der politischen Akteure in einem Gesetzgebungsprozess Berücksichtigung finden werden, um möglichst vielen Bürgern größtmögliche Teilhabe an Wissen und Demokratie zu ermöglichen und die Entwicklung innovativer Geschäftsmodelle am Standort zu fördern.

46 BT-Drs. 17/11137.

Dr. jur. Dipl.-Inf. Reto Mantz, Richter am LG, Frankfurt a. M.*

# Verwertung von Standortdaten und Bewegungsprofilen durch Telekommunikationsdiensteanbieter

## Der Fall Telefónica/$O_2$

*Während der Nutzung von mobilen Telekommunikationsdiensten fallen beim Telekommunikationsdiensteanbieter zwangsläufig Standortdaten an. Diese können ohne weiteres zu Bewegungsprofilen zusammengefasst werden. Kombiniert mit weiteren Daten lassen sich hieraus insbesondere geschäftlich wertvolle Erkenntnisse generieren. Der Beitrag beleuchtet die Zulässigkeit der geschäftlichen Verwertung von derlei entstandenen Bewegungsprofilen.*

## I. Einleitung

Die Monetarisierung von Kundendaten ist heutzutage mehr Regel- als Ausnahmefall. Gerade bei Internetdiensten beruhen die Geschäftsmodelle häufig darauf, möglichst viele, für Werbekunden aussagekräftige Daten über die Nutzer zu sammeln, ggf. auszuwerten und dann für gezielte Werbung zu verwenden oder insgesamt zu veräußern. Daten über Kunden, ihre Interessen und Vorlieben werden daher auch als „Währung des Internet" bezeichnet.[1]

Anbieter von mobilen Telekommunikationsdiensten („TK-Anbieter") generieren – unabhängig von Ortungsdiensten auf Smartphones, ja sogar unabhängig davon, ob ihre Kunden überhaupt ein Smartphone nutzen – bereits durch die Erbringung ihrer Dienste umfangreiche Daten über die Bewegungen ihrer Kunden. Diese Daten wecken Begehrlichkeiten, da sie – evtl. kombiniert mit anderen ebenfalls vorhandenen Daten – tiefe Einblicke in das Verhalten der Kunden ermöglichen. Dementsprechend wertvoll sind die Daten für Werbeanbieter, und damit auch für TK-Anbieter, die gewillt sind, die Daten über die reine Diensterbringung hinaus zu nutzen, auszuwerten und zu monetarisieren.

Der folgende Beitrag beleuchtet die Rechtmäßigkeit eines solchen Vorgehens durch TK-Anbieter, wobei nach einer Einleitung (II.) zunächst die betroffenen Datenarten charakterisiert werden sollen (III.). Anschließend soll anhand der Regelung des § 98 TKG die Rechtfertigung der geplanten Verwertung von Standortdaten (IV.), insbesondere im Hinblick auf eine eventuelle Anonymisierung (IV. 2) und/oder Einwilligung der Nutzer (IV. 3) untersucht werden.

## II. Hintergrund

Im Oktober 2012 gab der spanische Telekommunikations-Konzern Telefónica, in Deutschland durch seine Tochter $O_2$ vertreten, bekannt, dass er eine Geschäftseinheit namens „Dynamic Insight" eingerichtet habe.[2] Diese Geschäftseinheit solle Möglichkeiten erforschen, die bei Telefónica/$O_2$ anfallenden Daten, u. a. aufgrund des erheblichen Umfangs auch als „Big Data" bezeichnet, zu kommerzialisieren.[3] Das erste Produkt dieser Geschäftseinheit nennt sich „Smart Steps". Es sollte – unter Verwendung

* Mehr über den Autor erfahren Sie auf S. VIII.

1 *Kurz/Rieger*, Die Datenfresser, 2011, S. 12; vgl. Stellungnahme 5/2005 der Art. 29-Datenschutzgruppe, WP 115: „potenzielle Einnahmequelle", http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_de.pdf.

2 Pressemitteilung vom 9. 10. 2012, http://blog.digital.telefonica.com/?press-release=telefonica-launches-telefonica-dynamic-insights-a-new-global-big-data-business-unit.

3 Fn. 2.

„vollständig anonymisierter und aggregierter Daten" – z. B. Händlern und Kommunen[4] Informationen zu ihren Kunden bzw. Bürgern an die Hand geben, namentlich, dass und wie lang Kunden vor ihren Schaufenstern stehen geblieben sind bzw. in ihrem Geschäft verweilt haben, und aus welcher Richtung sie gekommen sind. Grundlage dieser Informationen sollten die von Telefónica/$O_2$ ausgewerteten Standort- und Bewegungsdaten seiner Kunden sein. Zusätzlich sollten die Daten um Alter und Geschlecht des Kunden angereichert werden.

Die Einführung von „Smart Steps" war zunächst für England geplant, später sollte der Dienst auch in Deutschland angeboten werden. Nach heftiger Kritik u. a. des Bundesdatenschutzbeauftragten *Schaar*[5] und der *Bundesregierung*[6] hat Telefónica/$O_2$ mittlerweile angekündigt, den Dienst in Deutschland nicht anbieten zu wollen.

Wie oben dargestellt, sind die bei TK-Anbietern gesammelten Daten geeignet, erhebliche Begehrlichkeiten zu wecken.[7] Daher bietet der Fall Telefónica/$O_2$ Anlass für eine Untersuchung der Rechtmäßigkeit bzw. Realisierbarkeit der Monetarisierung von Standortdaten durch TK-Anbieter.

## III. Grundlagen: Bestandsdaten, Verkehrsdaten, Standortdaten

Die von einem TK-Anbieter aufgrund der Erbringung seiner Dienstleistungen erhobenen Daten werden vom Gesetz unterschiedlich definiert und behandelt. Zunächst erhebt der TK-Anbieter Bestandsdaten nach § 3 Nr. 3 TKG, also Daten, die zur Begründung und Durchführung eines Vertragsverhältnisses erhoben werden, beispielsweise Name, Adresse, Alter und Geschlecht des Nutzers.[8] Hinzu kommen Verkehrsdaten nach § 3 Nr. 30 TKG, die bei der Erbringung eines TK-Dienstes entstehen, beispielsweise Zeitpunkt und Dauer der Nutzung sowie Absender und Empfänger einer Nachricht. Dritte Gruppe und zum Teil Untermenge der Verkehrsdaten sind gemäß § 3 Nr. 19 TKG Daten, die den Standort eines Endgeräts angeben (Standortdaten).[9]

Bereits Standortdaten für sich, erst recht aber gepaart mit Verkehrsdaten, erlauben die Zusammenstellung von aussagekräftigen Bewegungsprofilen.[10] Beispielhaft sei hier auf die mit dem Grimme Online Award ausgezeichnete Aufbereitung von Daten und Bewegungsprofilen des Politikers Spitz verwiesen, die auf sogenannten Vorratsdaten kombiniert mit öffentlich verfügbaren Daten basiert.[11] Einen nochmals gesteigerten Wert haben die Daten, wenn sie mit Bestandsdaten kombiniert werden, also wie im Fall Telefónica/$O_2$ beispielsweise mit Alter und Geschlecht des jeweiligen Nutzers.[12] Denn daraus lassen sich wiederum weitere geschäftlich nutzbare Erkenntnisse gewinnen.

## IV. Rechtfertigung der Erhebung, Verarbeitung und Nutzung von Standortdaten, § 98 TKG

Die Erhebung und Verarbeitung von Daten bedarf auch im Telekommunikationsrecht einer besonderen Rechtfertigung.[13] Eine solche kann § 98 TKG darstellen.[14] § 98 Abs. 1 TKG lautet (Ausschnitt, Hervorhebung durch Verfasser):

„Standortdaten … dürfen nur im zur Bereitstellung von *Diensten mit Zusatznutzen* erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, *wenn sie anonymisiert wurden* oder *wenn der Teilnehmer* dem Anbieter des Dienstes mit Zusatznutzen *seine Einwilligung erteilt hat*.… Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die *Übermittlung von Standortdaten* eines Mobilfunkendgerätes an … Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer abweichend von § 94 seine *Einwilligung ausdrücklich, gesondert und schriftlich* gegenüber dem Anbieter des Dienstes mit Zusatznutzen erteilen. …"

Die Verarbeitung von Standortdaten wurde in Umsetzung von Art. 9 der EU-Datenschutzrichtlinie[15] erstmals im TKG 2004 geregelt[16] und zuletzt im Mai 2012 geändert. Nach § 98 Abs. 1 TKG dürfen Standortdaten nur im zur Bereitstellung von Diensten mit Zusatznutzen (§ 3 Nr. 5 TKG) erforderlichen Umfang und unter engen Voraussetzungen verarbeitet werden. Dabei umfasst der aus der Richtlinie übernommene Begriff der Verarbeitung nach § 3 Abs. 4 BDSG auch den der Übermittlung, so dass nach § 98 TKG grundsätzlich auch eine Übermittlung an Dritte gerechtfertigt werden kann,[17] was auch § 98 Abs. 1 S. 4 TKG nahe legt.

### 1. Dienst mit Zusatznutzen?

Fraglich ist bereits, ob eine Rechtfertigung der Erhebung und Übermittlung von Standortdaten nach § 98 TKG vorliegend überhaupt in Betracht kommt, da schon unklar ist, ob es sich vorliegend um einen „Dienst mit Zusatznutzen" nach § 98 TKG handelt. Ein Dienst mit Zusatznutzen ist nach § 3 Nr. 5 TKG (u. a.) jeder Dienst, der die Erhebung und Verwendung von Standortdaten in einem Maße erfordert, das über die Übermittlung einer Nachricht hinausgeht. Allerdings gehen die Kommentatoren ausweislich der jeweils angeführten Beispiele davon aus, dass es sich um einen Dienst handelt, der *dem Kunden* einen Zusatznutzen bringt,[18] nicht aber dem TK-Anbieter oder dessen Geschäftskunden. Zu diesem Ergebnis ist laut Presseberichten bzgl. des Falls Telefónica/$O_2$ auch das Bundeswirtschaftsministerium gelangt.[19] Darüber hinaus dürfte

4 Die potentiellen Erwerber von Bewegungsprofilen und Standortdaten werden nachfolgend zusammenfassend als „Geschäftskunden" (der TK-Anbieter) bezeichnet.

5 Zeit Online v. 31. 10. 2012, http://www.zeit.de/digital/datenschutz/2012-10/schaar-handel-handy-daten; ebenso auch der rheinland-pfälzische Landesdatenschutzbeauftragte *Wagner*, Pressemitteilung v. 30. 10. 2012, http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2012103001.

6 Heise Online v. 31. 10. 2012, http://heise.de/-1740948.

7 Vgl. weiter zur Speicherung von Standortdaten durch Apple iPhones MMR-Aktuell 2011, 319493.

8 Im Folgenden werden die Betroffenen untechnisch als „Nutzer" bezeichnet. Auf die Unterscheidung zwischen den Begriffen „Teilnehmer", „Nutzer" und „Endnutzer" soll nicht eingegangen werden, s. dazu die Definitionen in § 3 Nr. 8, 14, 20 TKG.

9 Näher zur Abgrenzung nach Art. 6 Abs. 3 und Art. 9 der EU-Datenschutzrichtlinie *Steidle*, MMR 2009, 167, 168; *Eckhardt*, in: Spindler/Schuster, 2. Aufl. 2011, § 98 TKG Rn. 9.

10 BVerfG, 12. 3. 2003 – 1 BvR 330/96, 1 BvR 348/99, BVerfGE 107, 299, 320.

11 Zeit-Online, http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten.

12 Vgl. *Heckmann*, jurisPR-ITR 22/2012, Anm. 1.

13 Sog. Verbot mit Erlaubnisvorbehalt, *Eckhardt*, in: Heun, TK-Recht, 2. Aufl. 2007, Kap. L, Rn. 162; vgl. *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 2 Rn. 16.

14 Zur Nichtanwendbarkeit von § 96 Abs. 3 TKG auf Standortdaten und zur Anwendung von § 98 TKG auch auf die Erhebung von Daten *Jandt*, MMR 2007, 74, 75; *Wittern*, in: BeckTKG, 3. Aufl. 2006, § 98 Rn. 6 jew. m. w. N.

15 RL 2002/58/EG.

16 Näher *Löwnau*, in: Scheurle/Mayen, TKG, 2. Aufl. 2008, § 98 Rn. 1; *Ohlenburg*, MMR 2004, 431, 436.

17 Vgl. auch *Jandt*, MMR 2007, 74, 76.

18 *Graf*, in: BeckOK-StPO, 2012, § 98 TKG Rn. 2; *Wittern*, in: BeckTKG (Fn. 14), § 98 Rn. 2; *Löwnau*, in: Scheurle/Mayen (Fn. 16), § 98 Rn. 3-7, 11; *Ohlenburg*, MMR 2003, 82, 84: „dem Nutzer Dienste direkt an seinem Standort anzubieten."; vgl. auch BT-Drs. 15/2319, S. 20.

19 Heise Online v. 31. 10. 2012, http://heise.de/-1740948; *Graf von Rex*, ZD-aktuell 2012, 03268.

die in § 98 Abs. 1 TKG und konkretisierend in § 98 Abs. 4 TKG vorgesehene Einschränkung auf die Erforderlichkeit ebenfalls darauf Bezug nehmen, inwieweit die Daten erforderlich sind, um *für den Kunden* den Dienst zu erbringen, da § 98 TKG die Rechtfertigung von Eingriffen in die Rechte des Kunden betrifft. Daten können daher für einen Dienst, der nur für einen unbekannten Dritten einen (Zusatz-)Nutzen darstellt, per se nicht erforderlich sein.

### 2. Anonymisierung

Nach § 98 Abs. 1 TKG kann eine Verarbeitung durch Anonymisierung der Daten gerechtfertigt werden. Für den Begriff der Anonymisierung ist zunächst der Schutzbereich des Datenschutzes zu umreißen: Nach § 91 Abs. 1 TKG i.V. m. § 3 Abs. 1 BDSG werden personenbezogene Daten unter Schutz gestellt. Personenbezogen sind nach § 3 Abs. 1 BDSG Angaben über eine bestimmte oder bestimmbare natürliche Person. Davon ausgehend ist Anonymisierung nach § 3 Abs. 6 BDSG das Verändern der personenbezogenen Daten derart, dass die Einzelangaben nicht mehr oder nur mit unverhältnismäßig großem Aufwand einer bestimmten oder bestimmbaren Person zugeordnet werden können. Es kommt also im Ergebnis darauf an, ob Daten personenbeziehbar sind.[20]

Vor diesem Hintergrund ist daher zu klären, ob die vom TK-Anbieter erhobenen und gespeicherten Daten (a) für den TK-Anbieter und (b) bei Übermittlung für den Empfänger anonym sind.[21]

#### *a) Erhebung, Speicherung und Nutzung der Daten durch den TK-Anbieter*

Will ein TK-Anbieter Bewegungsprofile veräußern, muss er zunächst eine Sammlung von Standortdaten (Standort plus Zeitpunkt) anlegen. Da dieses Profil im weiteren Zeitverlauf fortgeführt werden soll, müssen die Daten dauerhaft mit dem Kundenprofil, z. B. über seine Telefonnummer oder ein anderes Identifikationsmerkmal, verknüpft werden. Auch um das Bewegungsprofil um Bestandsdaten anzureichern, muss der TK-Anbieter einen Bezug der bisher gespeicherten Daten zur Person des Kunden herstellen können. Die Daten können folglich nicht anonym sein.[22]

Möglicherweise könnte der TK-Anbieter die Daten mittels eines speziellen Hash-Schlüssels separat speichern, sie also doppelt und um Namen und Anschrift bereinigt ablegen. Dies dürfte allerdings lediglich eine Pseudonymisierung nach § 3 Abs. 6 a BDSG und keine Anonymisierung darstellen.[23] Da dem TK-Anbieter die Hash-Funktion (zwangsläufig) bekannt ist, kann er den Personenbezug jederzeit mit vergleichsweise geringem Aufwand wiederherstellen. Auch derart abgelegte Daten sind daher nicht anonym.

Eine Anonymisierung könnte aber ggf. durch eine starke Aggregation der Daten erreicht werden. Dafür müsste der TK-Anbieter zu bestimmten Zeitpunkten die Daten seiner Kunden erheblich zusammenfassen. Nicht mehr datenschutzrechtlich relevant könnten beispielsweise Aussagen wie die folgende sein:

„Am 1. 1. 2013 haben sich im Zeitraum von 15:00h bis 15:05h in der Bahnhofstr. in Höhe der Hausnummern 20-30 durchschnittlich jeweils 5 Personen aufgehalten. Diese sind für durchschnittlich 45 Sekunden stehen geblieben. Das Alter der Personen lag zwischen 20 und 40 Jahren."

Es lässt sich leicht ersehen, dass diese Form der Aggregation (und Anonymisierung) den Wert der Daten erheblich mindert. Im Falle von Telefónica/$O_2$ sollten allein solche Angaben vermutlich nicht Gegenstand des Angebots „Smart Steps" sein.

Im Ergebnis dürfte eine Rechtfertigung durch Anonymisierung der Daten kaum greifen.

#### *b) Übermittlung an den Geschäftskunden*

Auch die Übermittlung an den Geschäftskunden dürfte nicht den Anonymitätsanforderungen des § 98 Abs. 1 TKG genügen. Denn damit die Daten für den Geschäftskunden aussagekräftig und wertvoll sind, müssen sie so umfassend sein, dass dem Geschäftskunden in vielen Fällen wiederum eine Herstellung des Personenbezugs möglich sein dürfte. In diesem Fall wären die Daten aber nicht als anonym anzusehen.[24]

Dabei ist zu beachten, dass Geschäftskunden, die Bewegungsprofile beim TK-Anbieter erwerben, häufig zusätzlich auf eigene Datenbestände zurückgreifen können, beispielsweise EC- oder Kreditkartenabrechnungen, Daten aus Bonusprogrammen, Videoaufzeichnungen etc. Da sich aus dem Bewegungsprofil beispielsweise ermitteln lassen soll, wann und wie lange ein Kunde in einem Geschäft verweilte, aus welcher Richtung er kam, welchen Geschlechts und Alters er/sie ist, ist es nicht schwer sich vorzustellen, dass der Geschäftskunde auch ohne Mitteilung des Namens durch den TK-Anbieter in vielen Fällen ermitteln können wird, auf welchen seiner Kunden sich das erworbene Bewegungsprofil bezieht. In einem Extrembeispiel einer kleinen Boutique mit wenigen Stammkunden muss der Inhaber des Geschäfts im Grunde nur die Kreditkartenabrechnung (Zeitpunkt eines Einkaufs) mit dem Bewegungsprofil (wann hat der Kunde das Geschäft verlassen?) abgleichen. Ist der Kunde gleichzeitig Teilnehmer eines der vielen Bonusprogramme, können durch die Verwendung von Alter (oder sogar Geburtsdatum), Geschlecht und Zeitpunkt des Einkaufs einzelne Kunden unproblematisch auch aus einer größeren Gruppe von Kunden heraus identifiziert werden.

Vor diesem Hintergrund geht auch die Art. 29-Datenschutzgruppe bei Standortdaten und Bewegungsprofilen praktisch zwangsläufig von personenbezogenen – und damit nicht anonymen – Daten aus.[25]

### 3. Einwilligung

Als weiteren Rechtfertigungsgrund sieht § 98 Abs. 1 TKG die Einwilligung des Kunden vor. Auch hier ist zu unterscheiden zwischen der Einwilligung in (a) die Erhebung, Verarbeitung und Nutzung durch den TK-Anbieter und (b)

20 *Klesczewski*, in: BerlinTKG, 2. Aufl. 2009, § 91 Rn. 21; *Dammann*, in: Simitis (Fn. 13), § 3 Rn. 23, 196; *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 3 Rn. 10.

21 Auf den insbesondere zu IP-Adressen geführten Streit, ob auf einen absoluten oder relativen Personenbezug abzustellen ist, soll hier nicht näher eingegangen werden, s. dazu *Dammann*, in: Simitis (Fn. 13), § 3 Rn. 23 ff.; *Gola/Schomerus* (Fn. 20), § 3 Rn. 10 jew. m. w. N.

22 Vgl. auch Stellungnahme 13/2011 der Art. 29-Datenschutzgruppe, WP185, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, S. 8 f.; dazu *Spies*, MMR-Aktuell 2011, 318376.

23 Näher *Scholz*, in: Simitis (Fn. 13), § 3 Rn. 212 ff.; *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 3 Rn. 51.

24 Selbst bei Anwendung des Begriffs des relativen Personenbezugs (s. o. Fn. 21) liegt eine rechtfertigungsbedürftige Übermittlung vor, wenn der Empfänger der Daten – hier der Geschäftskunde – den Personenbezug mittels eigener Daten herstellen kann, *Gola/Schomerus* (Fn. 21), § 3 Rn. 44 a; *Dammann*, in: Simitis (Fn. 13), § 3 Rn. 34.

25 Stellungnahme 13/2011 der Art. 29-Datenschutzgruppe (Fn. 22), S. 10.

in die Übermittlung an und die anschließende Verarbeitung durch den Geschäftskunden des TK-Anbieters.

*a) Einwilligung in Erhebung, Verarbeitung und Nutzung durch den TK-Anbieter*

Die Voraussetzungen für die Einwilligung in die Datenverwendung ergeben sich aus §§ 94 TKG, 4 a Abs. 1 BDSG.[26] Danach muss der Nutzer vor Erteilung der Einwilligung insbesondere klar und verständlich über den vorgesehenen Zweck und den Umfang der Erhebung, Verarbeitung und Nutzung informiert werden.[27] Die Einwilligungserklärung muss, wenn sie nicht sogar separat eingeholt wird, deutlich hervorgehoben sein, ggf. ohne Verstoß gegen das Kopplungsverbot (§ 95 Abs. 5 TKG[28]) eingeholt werden und die Art der Daten und den Zweck der Erhebung, Verarbeitung und Nutzung sowie den Empfänger einer Übermittlung bezeichnen.[29] Im vorliegenden Fall hatte Telefónica/$O_2$ offenbar beim Bestellvorgang eine Einwilligung des Nutzers zu einer Verwendung seiner Standortdaten „im Rahmen des Erforderlichen" auch für „Vermarktung" und „Meinungsforschung" vorgesehen.[30] Eine solch pauschale Formulierung, ohne Hinweis auf den konkreten Zweck und die spätere Übermittlung an Dritte, dürfte – unabhängig von der erforderlichen deutlichen Hervorhebung – die dargestellten Voraussetzungen nicht erfüllen.

Als Folge wäre bereits die Erhebung der Standortdaten durch den TK-Anbieter nicht gerechtfertigt, was sich zwangsläufig auf die weitere Verwendung auswirkt. Daten, die rechtswidrig erhoben wurden, müssen nach § 35 Abs. 2 S. 2 BDSG unverzüglich gelöscht werden. Dementsprechend kann der TK-Anbieter in einem solchen Fall Bewegungsprofile gar nicht erst rechtmäßig anlegen. Die Grundlage für einen späteren Verkauf der Daten fehlt dann ebenfalls.

*b) Einwilligung in die Übermittlung an Geschäftskunden*

An die Einwilligung in die Übermittlung von Standortdaten sind zunächst die selben Anforderungen zu stellen. Auch hier ist eine informierte Einwilligung des Kunden zu verlangen, dem Kunden müssen daher Umfang und Art der Daten, Zweck der Übermittlung und Empfänger mitgeteilt werden. Darüber hinaus muss die Einwilligungserklärung deutlich hervorgehoben sein.[31] Weiter ist ggf. das Kopplungsverbot des § 95 Abs. 5 TKG zu beachten. Diese Anforderungen dürften im Hinblick auf die Sensitivität von Standortdaten im Kleingedruckten von AGB kaum wirksam erfüllt werden können, zumal die Einwilligung in die Übermittlung von solchen Daten an Dritte in AGB als überraschend anzusehen sein dürfte.

Nach § 98 Abs. 1 S. 4 TKG werden darüber hinaus an die Einwilligung in die Übermittlung von Standortdaten, die von Mobilfunkgeräten erhoben werden,[32] an Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen (hier: der TK-Anbieter) sind, erhebliche darüber hinaus gehende Anforderungen gestellt. Der Nutzer muss in solchen Fällen seine Einwilligung ausdrücklich, gesondert und schriftlich gegenüber dem TK-Anbieter erteilen. § 98 Abs. 1 S. 4 TKG geht damit noch einmal deutlich über die Voraussetzungen des § 4 a BDSG hinaus. Eine Einholung der Einwilligung im Kleingedruckten der AGB oder überhaupt bei einem Online-Bestellvorgang ist damit ausgeschlossen.[33]

Das öffentliche Echo bei Bekanntwerden der Pläne von Telefónica/$O_2$ zeigt zudem, dass TK-Anbieter eine den Anforderungen genügende Einwilligung (insbesondere von Altkunden) vermutlich nicht in nennenswertem Umfang erhalten dürften, da die Bereitschaft zur Preisgabe und Gestattung der Verwendung dieser Daten offenbar nicht generell besteht.

### 4. Allgemeine datenschutzrechtliche Rechtfertigung?

Eine Rechtfertigung nach den allgemeinen datenschutzrechtlichen Regelungen, insbesondere nach § 28 Abs. 1 BDSG, scheidet im Übrigen ebenfalls aus, da dessen Anwendung durch § 98 TKG gesperrt ist.[34] Im Übrigen dürfte das Anlegen von Bewegungsprofilen kaum im Sinne von § 28 Abs. 1 S. 1 Nr. 1 BDSG für die Vertragsdurchführung, oder nach § 28 Abs. 1 S. 1 Nr. 2 BDSG für berechtigte Interessen des TK-Anbieters ohne Überwiegen der schutzwürdigen Interessen des Betroffenen erforderlich sein. Schließlich handelt es sich bei Bewegungsprofilen nach der Ratio des § 98 TKG um sensitive Daten, wenn auch grundsätzlich nicht solche mit dem erheblichen Rang der Daten nach § 3 Abs. 9 BDSG.

### 5. Verletzung des Fernmeldegeheimnisses, § 206 StGB

Wenn, wie hier, die durch den TK-Anbieter übermittelten Standortdaten weder anonym sind, noch die Übermittlung auf Basis einer wirksamen Einwilligung erfolgt, und keine andere Rechtfertigung greift, ist die Weitergabe der Daten für die Verantwortlichen gleichzeitig eine strafbare Verletzung des Fernmeldegeheimnisses nach § 206 Abs. 1 StGB durch unbefugte Mitteilung der näheren Umstände von Telekommunikation an eine andere Person,[35] denn auch Standortdaten eines Telekommunikationsdienstes unterfallen dem Fernmeldegeheimnis.[36]

## V. Fazit und Ausblick

Die Monetarisierung von Standortdaten, zumal in Kombination mit Bestandsdaten, ist nach derzeitigem Stand telekommunikations- und datenschutzrechtlich praktisch nur über eine klare, deutliche und ggf. schriftliche Einwilligung zu rechtfertigen. Diese Lösung dürfte für TK-Anbieter aber vermutlich eher unattraktiv sein. Ohne Einwilligung ist das Vorgehen allerdings rechtswidrig und zudem nach § 206 StGB strafbar.

Bemerkenswert ist letztlich die öffentliche Aufmerksamkeit, die der Fall hervorgerufen hat. Das Thema wurde kurzfristig von praktisch allen Medien aufgegriffen. Im

26 *Klesczewski*, in: BerlinTKG (Fn. 20), § 94 Rn. 5; *Büttgen*, in: BeckTKG (Fn. 14), § 94 Rn. 4.
27 *Eckhardt*, in: Spindler/Schuster (Fn. 9), § 98 TKG Rn. 6 f.
28 Dazu *Eckhardt*, in: Heun (Fn. 13), Kap. L Rn. 191.
29 *Klesczewski*, in: BerlinTKG (Fn. 20), § 94 Rn. 5 f., § 98 Rn. 10; vgl. *Simitis*, in: Simitis (Fn. 13), § 4 a Rn. 40 f.; *Wittern*, in: BeckTKG (Fn. 14), § 98 Rn. 10; s. zu Einwilligungserklärungen in AGB auch BGH, 16. 7. 2008 – VIII ZR 348/06, K&R 2008, 678 – Payback; BGH, 11. 11. 2009 – VIII ZR 12/08, K&R 2010, 116 – Happy Digits.
30 *Dugge*, Tagesschau.de v. 30. 10. 2012, http://tagesschau.de/wirtschaft/telefonica106.html.
31 S.o. Fn. 29.
32 *Eckhardt*, in: Spindler/Schuster (Fn. 9), § 98 TKG Rn. 17.
33 Vgl. auch Stellungnahme 13/2011 der Art. 29-Datenschutzgruppe (Fn. 22), S. 14.
34 *Jandt*, MMR 2007, 74, 76; *Eckhardt*, in: Heun (Fn. 13), Kap. L Rn. 196; *Klesczweski*, BerlinTKG (Fn. 20), § 91 Rn. 15; *Robert*, in: BeckTKG (Fn. 14), § 91 Rn. 4.
35 Vgl. *Fischer*, StGB, 59. Aufl. 2012, § 206 Rn. 7; *Lenckner/Eisele*, in: Schönke/Schröder, StGB, 28. Aufl. 2010, § 206 Rn. 6 a; *Weidemann*, in: BeckOK-StGB, § 206 Rn. 3.
36 BGH, 21. 2. 2001 – 2 BGs 42/2001, MMR 2001, 442, 443 m. Anm. *Bär*; *Bock*, in: BeckTKG (Fn. 14), § 88 Rn. 5, 15; *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 35), § 206 Rn. 6 a; *Weidemann*, in: BeckOK-StGB, § 206 Rn. 3; zur Rechtslage bei IMSI-Catchern s. BVerfG, 22. 8. 2006 – 2 BvR 1345/03, MMR 2006, 805, 807 – IMSI-Catcher; zum Streitstand *Günther*, NStZ 2005, 485; *Nachbaur*, NJW 2007, 335 jew. m. w. N.

Ergebnis dürfte dies zu der schnellen und entschiedenen Äußerung durch die Bundesregierung geführt haben.

Offenbar ist die Öffentlichkeit im Hinblick auf das Thema Datenschutz stärker sensibilisiert als bisher gedacht. Es kann davon ausgegangen werden, dass dies auch ein Verdienst derjenigen ist, die sich in den letzten Jahren intensiv, öffentlichkeitswirksam und erfolgreich um die Aufhebung der Regelungen zur Vorratsdatenspeicherung bemüht haben,[37] ein Thema, das seither – auch durch die entsprechenden Unstimmigkeiten in der Regierungskoalition – wiederholt Gegenstand öffentlichen Diskurses war. Mit den Debatten um die Volkszählung in den 1980er Jahren[38] ist das öffentliche Aufsehen des vorliegenden Falls zwar noch nicht zu vergleichen. Aber es ist doch eine positive Tendenz zu erkennen, dass die Betroffenen sich mit Themen des Datenschutzes zunehmend intensiver auseinandersetzen, was mehr und mehr auch von den politischen Entscheidungsträgern erkannt wird.

37 S. dazu BVerfG, 2. 3. 2010 – 1 BvR 256/08, NJW 2010, 833.

38 Vgl. dazu *Reymann*, FAZ v. 7. 5. 2011, http://www.faz.net/-gq3-z2tt; zur Volkszählung 1983 und dem Recht auf informationelle Selbstbestimmung BVerfG, 15. 12. 1983 – 1 BvR 209/83, BVerfGE 65, 1; dazu *Simitis*, NJW 1984, 394.

RA Dr. Florian Deusch, Ravensburg*

# Compliance-Vorgaben für den Einsatz von Smartphones im Unternehmen

*Kann ein Unternehmen die Vorteile des „Mobile Computing" z. B. durch die schlichte Ausgabe von Smartphones an seine Mitarbeiter nutzen? Sind neben der Geräteausgabe zusätzliche Maßnahmen für einen effizienten und sicheren IT-Einsatz notwendig? Der folgende Beitrag untersucht, ob und falls ja welche Rechtspflichten ein Unternehmen bzw. die Unternehmensleitung treffen, wenn den Mitarbeitern Smartphones zur betrieblichen Nutzung zur Verfügung gestellt werden.*

## I. Einleitung

Die Nutzung mobiler Endgeräte im Berufsleben ermöglicht die Erreichbarkeit der verantwortlichen Personen und den Zugriff auf unternehmensinterne IT-Systeme – unabhängig von Zeit und Ort. Aktuelle Studien erwarten eine deutliche Verstärkung dieses Anwendungstrends.[1]

Gegenstand dieser Untersuchung ist die Frage, ob und falls ja welche Compliance-Vorgaben für den Einsatz mobiler Endgeräte am Beispiel sogenannter Smartphones zu beachten sind.[2] Zunächst wird dargestellt, wie Smartphones derzeit in Unternehmen eingesetzt werden und welche Risiken hierbei bestehen (siehe Abschnitt II). Sodann befasst sich der Beitrag damit, ob und falls ja aus welchen Rechtsgrundlagen sich Pflichten des Unternehmens und der dort verantwortlichen Personen für einen sicheren Einsatz der Smartphones ergeben und wie diese umzusetzen sind (siehe die Abschnitte III und IV). Hieraus werden Thesen abgeleitet, die sich aus rechtlicher Sicht für den Einsatz von Smartphones in Unternehmen ergeben (siehe Abschnitt V).

## II. Einsatz von Smartphones in Unternehmen

### 1. Begriff und Anwendungsbereiche

Bislang existiert weder eine gesetzliche noch eine sonstige allgemeingültige Definition des Begriffs Smartphone. Verschiedenen Definitionsansätzen gemeinsam ist die Beschreibung des Smartphones als ein mobiles, handtellergroßes Hardware-Gerät, das sowohl zum Telefonieren als auch für weitere Datenanwendungen (Datenerfassung, -bearbeitung und -kommunikation) eingerichtet ist.[3]

Ein Smartphone verfügt unter anderem über einen Prozessor zur Ausübung von Rechenoperationen, einen lokalen Speicher (derzeit bis zu 64 Gigabyte[4]), einen Bildschirm und je nach Hersteller eine Tastatur.

Über diverse Schnittstellen kann das Smartphone mit anderen Hardware-Geräten und Servern in verschiedenen Netzen Daten austauschen. Zur Datenkommunikation wer-

* Der Autor ist als Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter (Ravensburg) tätig. Mehr über den Autor erfahren Sie auf S. VII. Der Beitrag geht auf einen Vortrag bei der DSRI-Herbstakademie 2012 zurück, die im Tagungsband Jürgen Taeger (Hrsg.), IT und Internet – mit Recht gestalten, DSRI-Herbstakademie 2012, Edewecht 2012 dokumentiert wurde. Der Beitrag ist jedoch aktualisiert um die bis zum November 2012 erschienene Rechtsprechung und Literatur.

1 Nach einer Studie der SYMANTEC Corporation (State of Mobility Survey 2012, S. 8) beabsichtigen 71 % aller befragten Unternehmen, ihren Mitarbeitern maßgeschneiderte mobile Applikationen bereitzustellen (http://www.symantec.com/content/en/us/about/media/pdfs/b-state_of_mobility_survey_2012.en-us.pdf, abgerufen am 10. 12. 2012); laut einer Studie von *Gartner* werden bis zum Jahr 2014 90 % aller Unternehmen mobile IT-Anwendungen einsetzen, siehe hierzu *Conrad*, CR 2011, 797.

2 Dargestellt wird die Konstellation, in der das Unternehmen dem Mitarbeiter ein Smartphone zur ausschließlichen betrieblichen Nutzung überlässt. Die Nutzung privater Geräte zu betrieblichen Zwecken („Bring your own Device") bleibt einer gesonderten Darstellung vorbehalten. Auch spezifische Themen des Arbeitsrechts (etwa das Erfordernis betrieblicher Mitbestimmung gemäß § 87 BetrVG oder Fragen des Arbeitszeitrechts) wären gesondert zu prüfen.

3 European Network and Information Security Agency (kurz: ENISA), Smartphones: Information security risks, opportunities and recommendations for users, December 2010 (https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users, abgerufen 10. 12. 2012), S. 9; ähnlich die Definitionen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (http://www.bfdi.bund.de/DE/Themen/TechnologischerDatenschutz/TechnologischeNeuerungen/Artikel/Miniaturisierung.html) und des Bundesamtes für Sicherheit in der Informationstechnik (kurz: BSI, siehe IT-Grundschutzkatalog B 3405 unter https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b03/b03405.html, abgerufen 10. 12. 2012).

4 http://store.apple.com/de/browse/home/shop_iphone/family/iphone/iphone4s?afid=p228|GBDE&cid=AOS-EMEA-SHOPIP-GoogleBase-DE, abgerufen 10. 12. 2012.