www.jusletter.ch

Daniel Kettiger

Rechtliche Rahmenbedingungen für Location Sharing Systeme in der Schweiz

Der Raumbezug – insbesondere der Standort von Akteuren – erhält in den Internetanwendungen eine zunehmend grössere Bedeutung (standortbezogene Dienste; Location Based Services, LBS). Bei den so genannten Location Sharing Systemen wird der Raumbezug zum eigentlichen Inhalt des Dienstes: Drittpersonen können den Standort von Nutzerinnen und Nutzern abrufen. Der Aufsatz zeigt den rechtlichen Rahmen solcher Location Sharing Systeme in der Schweiz auf, welcher insbesondere durch das Fernmelde-, Datenschutz- und Geoinformationsrecht geprägt wird. Er befasst sich u.a. eingehend mit dem Rechtscharakter von IP-Adressen.

Rechtsgebiet(e): Datenschutz; Fernmeldewesen. Fernmeldenetze; Personenrecht; Informatikrecht

Zitiervorschlag: Daniel Kettiger, Rechtliche Rahmenbedingungen für Location Sharing Systeme in der Schweiz, in: Jusletter 9. August 2010

Inhaltsübersicht

1. Einleitung

[Rz 1] Die Zahl der Nutzerinnen und Nutzer von Mobiltelefonen nimmt auch in der Schweiz laufend zu. Je nach statistischer Erhebung bzw. Erhebungsmethodik gab es Ende 2008 rund 9 Mio.[1] bzw. 11 Mio.[2] Mobiltelefonkunden, davon rund 5 Mio. Kunden mit Zugang zu UMTS[3]. Es kann davon ausgegangen werden, dass in der Schweiz heute über 90 Prozent der Bevölkerung über ein Mobiltelefon verfügen.[4] Rund 60 Prozent der Schweizer Bevölkerung nutzten im April 2010 digitale Medien zu Zwecken der Kommunikation.[5] Gemäss neueren Erhebungsresultaten zur Informationsgesellschaft hat auch die Internetnutzung in den vergangenen Jahren stark zugenommen, scheint sich nun aber zu stabilisieren. Von April bis September 2008 benutzten 79 Prozent der Bevölkerung ab 14 Jahren das Internet (Weitester Nutzerkreis WNK). Täglich oder mehrmals pro Woche nutzten 71 Prozent der Befragten in besagtem Zeitraum das Internet (Engerer Nutzerkreis ENK).[6]

[Rz 2] Die technologische Entwicklung des letzten Jahrzehnts hat es ermöglicht in zunehmendem Mass von mobilen Endgeräten aus auf das Internet zuzugreifen. Gleichzeitig führt der technologische Fortschritt zusammen mit den wachsenden, immer dichteren digitalen Kommunikationsnetzen dazu, dass eine räumliche Ortung der Endgeräte möglich wird.[7] Parallel zur letztgenannten Entwicklung werden immer mehr Mobilfunktelefongeräte mit GPS-Systemen ausgerüstet, welche ebenfalls eine Ortung des Geräts ermöglichen. Diese Entwicklungen haben dazu geführt, dass digitale Dienstleistungen auf der Basis des Internets oder der Mobilfunktechnologie heute zunehmend als so genannte Location Based Services (LBS) raumbezogen bzw. ortsbezogen angeboten werden. Eine besondere Form der LBS stellen so genannte Location Sharing Systeme dar, bei denen die Dienstleistung direkt in der Vermittlung der Standortinformation besteht.[8] Mittlerweile bestehen rund 90 Angebote von Location Sharing Systemen.[9]

[Rz 3] Der vorliegende Aufsatz befasst sich mit der Frage, welchen rechtlichen Rahmenbedingungen Location Sharing Systeme in der Schweiz unterliegen. Die nachfolgenden Ausführungen reflektieren den heutigen Stand der Technologie einerseits und der Gesetzgebung, Lehre und Rechtspraxis andererseits. Sie bewegen sich auf rechtlichem Neuland, denn weder die Frage des Rechtsrahmens für Location Sharing Systeme in der Schweiz integral noch die meisten Teilfragen waren bisher Gegenstand von rechtlichen Abhandlungen oder von Gerichtsentscheiden.[10] Die nachfolgenden Ausführungen müssen allgemein gehalten werden; für jedes einzelne Location Sharing System muss auf der Grundlage der konkreten Architektur und der verwendeten Technologien im Einzelfall geprüft werden, ob die dargestellten rechtlichen Rahmenbedingungen eingehalten werden oder ob

---

1 Vgl. Amtliche Fernmeldestatistik 2008, Stand Februar 2010, Bundesamt für Kommunikation (BAKOM), S. 47, www.bakom.admin.ch/dokumentation/zahlen/00744/00746/index.html?lang=de (Stand: 20.07.2010).

2 Vgl. Indikatoren zur Informationsgesellschaft der Schweiz, Bundesamt für Statistik (BFS), Abonnementstyp in der Mobiltelefonie, www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30101.301.html?open=319#319 (Stand: 20.07.2010); zum algemeinen Trend bei Smartphones vgl. SonntagsZeitung vom 25. Juli 2010, S. 49.

3 Vgl. Indikatoren zur Informationsgesellschaft der Schweiz (Fn. 2); UMTS (Universal Mobile Telecommunications System) ist ein äusserst leistungsfähiges und komplexes digitales Mobilfunksystem der dritten Generation (3G), das im Vergleich zu GSM unter anderem höhere Übertragungsraten auf der Luftschnittestelle ermöglicht.

4 Die Schätzungen variieren je nach Erhebungsmethodik, vgl. Amtliche Fernmeldestatistik 2008 (Fn. 1), S. 50, mit Hinweisen; andere Quellen sprechen allerdings von 115 Abonnentinnen bzw. Abonnenten pro 100 Einwohnenden, vgl. Indikatoren zur Informationsgesellschaft (Fn. 2); in den USA verfügten im Jahr 2009 mindestens 87 Prozent der Bevölkerung über ein Mobiltelefon, vgl. Jacine Y. Tsai et al., Location-Sharing Technologies: Privacy Risks and Controls (revisted February 2010), CyLab, Carbegie Mellon University, S. 1, http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

5 Vgl. Digital Live Index Schweiz, Ausgabe 1/2010, www.digitallifeindex.ch/#Home (Stand: 20.07.2010).

6 Vgl. www.bakom.admin.ch/themen/infosociety/01692/index.html?lang=de (Stand: 24.04.2010).

7 In diesem Sinne auch Gerald Friedland/Robin Sommer, Cybercasing the Joint: On the Privacy Implications of Geo-Tagging, ICSI, Berrkeley 2010, S. 2, www.icir.org/robin/papers/hotsec10-geotube.pdf (Stand: 24.07.2010); ausführlich zur Lokalisationstechnik nachfolgend Ziffer 2.2.

8 Ausführlich zu Location Sharing Systemen nachfolgend Ziffer 2.1.

9 Siehe Übersicht bei Tsai et al. (Fn. 4), S. 22 f.

10 Selbst das Buch von Rolf H. Weber, E-Commerce und Recht, 2. Aufl., Zürich 2010, welches einen Aktualitätsstand von April 2010 aufweist, thematisiert die spezifische rechtliche Problematik von Location Sharing Systemen nicht.

auf Grund besonderer technischer Abweichungen allenfalls abweichende rechtliche Rahmenbedingungen bestehen.

2. Grundlagen zu Location Sharing Systemen

2.1 Begriff des Location Sharing Systems

[Rz 4] Bis heute besteht keine lexikografische oder allgemein gebräuchliche und anerkannte Definition des Location Sharing Systems.

[Rz 5] Location Sharing Systeme gehören zweifellos *als Unterkategorie zu den standortbezogenen Diensten*. Standortbezogene Dienste (engl. Location Based Services, LBS; auch: Location Dependent Services, LDS) sind «mobile Dienste, die unter Zuhilfenahme von positionsabhängigen Daten dem Endbenutzer selektive Informationen bereitstellen oder Dienste anderer Art erbringen».[11] LBS bewegen sich technologisch an der Schnittstelle zwischen Geoinformationssystemen (GIS), Internetanwendungen und Mobilfunktechnologie.[12] Ein LBS besteht minimal aus den folgenden Infrastrukturelementen:[13]

- *Mobiles Endgerät:* Mit dem mobilen Endgerät fragt die Nutzerin bzw. der Nutzer die benötigte Information ab. Mobile Endgeräte können insbesondere Mobiltelefone, PDA, Laptops oder Navigationsgeräte sein.
- *Mobiles Netzwerk:* Das mobile Netzwerk transportiert die Nutzerdaten und die Anfrage vom mobilen Endgerät zum Service Provider und die angefragte Information wieder zurück zur Nutzerin oder zum Nutzer.
- *Lokalisationstechnik:* Mit den Hard- und Software-Komponenten der Lokalisierungstechnik kann der aktuelle Standort des mobilen Endgeräts ermittelt werden.[14]
- *Service-Provider:* Der Service-Provider bietet der Nutzerin bzw. dem Nutzer verschiedene Dienstleistungen (Dienste, Anwendungen) an und ist verantwortlich für die Verarbeitung der Anfragen (request processing). Die angebotenen Dienste können z.B. in der Bestimmung des Standorts, im Auffinden einer bestimmten Strasse oder im Anbieten von besonderen Informationen bestehen, die sich unmittelbar auf den Standort des Endgeräts beziehen.
- *Data-Provider:* Der Service-Provider verfügt meist nicht selber über alle angefragten Informationen. Er bezieht diese Informationen bei einem Dritten, dem Data-Provider. Solche Daten sind beispielsweise Kartendaten, die bezogen auf den Standort des Endgeräts von staatlichen oder privaten Anbietern bezogen werden.

[Rz 6] Die *Location Sharing Systeme* unterscheiden sich von andern Arten der LBS dadurch, dass die Ermittlung des Standorts (engl. location) selber zum Hauptzweck und Hauptinhalt des Dienstes wird und nicht bloss als Parameter zum Anknüpfen ortsbezogener Dienstleistungen dient. Kern von Anwendungen des Location Sharings ist immer das Ermitteln, Auswerten, Darstellen (z.B. zusammen mit Darstellungen von Kartendaten[15] oder fotografischen Darstellungen der Topographie[16] oder des Standorts selbst[17]) und Weitergeben der Standortinformation. Im Übrigen müssen auch Location Sharing Systeme die vorstehend genannten notwendigen Infrastrukturmerkmale der LBS aufweisen. Mithin können Location Sharing Systeme wie folgt definiert werden:

> *Location Sharing Systeme sind Location Based Services (LBS), deren einziger Zweck oder deren Hauptzweck die Ermittlung, Auswertung, Darstellung und Weitergabe der Standortdaten des mobilen Endgeräts ist.*

2.2 Lokalisationstechnik

[Rz 7] Für die Ermittlung des Standorts eines bestimmten mobilen Endgeräts (Lokalisation, Ortung, engl. location) können je alleine für sich oder nebeneinander verschiedene Lokalisationstechniken angewendet werden.[18] Da die

---

[11] Wikipedia, http://de.wikipedia.org/wiki/Standortbezogene_Dienste (Stand 20.07.2010). Noch etwas präziser scheint dem Verfasser die Definition in der englischen Ausgabe von Wikipedia: «A location-based service (LBS) is an information and entertainment service, accessible with mobile devices through the mobile network and utilizing the ability to make use of the geographical position of the mobile device», http://en.wikipedia.org/wiki/Location-based_service (Stand 20.07.2010), welche sich an wissenschaftliche Publikationen anlehnt, vgl. z.B. Stefan Steiniger/Moritz Neun/Alistair Edwardes, Foundations of Location Based Services, ETHZ, Projekt CartouCHe (www.e-cartouche.ch), S. 2 ff., www.geo.unizh.ch/publications/cartouche/lbs_lecturenotes_steinigeretal2006.pdf (Stand 20.07.2010); vgl. auch Friedland/Sommer (Fn. 7), S. 1 f.

[12] Vgl. Steiniger/Neun/Edwardes (Fn. 11), S. 2.

[13] Nach Steiniger/Neun/Edwardes (Fn. 11), S. 3 f.

[14] Ausführlich dazu nachfolgend Ziffer 2.2.

[15] Z.B. mit Swiss Map Mobile des Bundesamtes für Landestopografie (swisstopo). Das Produkt Swiss Map Mobile bringt die Landeskarte aufs Handy. Mit dem im Mobiltelefon integrierten GPS-Empfänger kann die Karte auf den aktuellen Standort zentriert werden. Eine Markierung zeigt dem Anwender seine aktuelle Position. Vgl. www.swisstopo.admin.ch/internet/swisstopo/de/home/products/maps/mobile.html (Stand: 20.07.2010).

[16] Z.B. Google Earth, siehe http://earth.google.com/intl/de/ (Stand: 20.07.2010).

[17] Z.B. Google Street View, siehe http://maps.google.com/intl/en_us/help/maps/streetview/; vgl. Auch Weber (Fn. 10), S. 480 ff.

[18] Vgl. z.B. für die Anwendung PeopleFinder Norman Sadeh et al., Understanding and Capturing People's Privacy Policies in People Finder Application, undatiertes wiss. Papier, Carnegie Mellon University, S. 2, www.normsadeh.com/file_download/64/puc2008-peoplefinder+%281%29.pdf (Stand: 20.07.2010).

Lokalisationstechnik für die rechtliche Beurteilung von Bedeutung ist, werden die verschiedenen technischen Ansätze nachfolgend kurz dargestellt:[19]

- *Global Positioning System (GPS):* Zahlreiche mobile Endgeräte sind heute mit GPS ausgerüstet. Die Ortung mit GPS erfolgt durch den Datenaustausch des Endgeräts mit Satelliten in fixen Umlaufbahnen, deren Position zu einem bestimmten Zeitpunkt genau bestimmbar ist (die Bahndaten werden in Almanachen veröffentlicht). In der praktischen Anwendung erreicht heute ein handelsübliches GPS-Gerät bei der Messung mit 4 Satelliten Ortungsgenauigkeiten von rund 10 bis 20 Metern.[20] Die Genauigkeit des GPS lässt sich durch den Einbezug einer Referenzstation (GPS-Empfänger auf einem Punkt, dessen Koordinaten genau bekannt sind) weiter steigern (Differential GPS, D-GPS). Dieses differentielle Verfahren lässt sich auch in Echtzeit durchführen. Voraussetzung dazu ist allerdings eine Funkverbindung (Funk, GSM etc.) zwischen der Referenzstation und dem mobilen Endgerät.[21] Mit D-GPS werden Ortungsgenauigkeiten im Dezimeter- bzw. Zentimeterbereich erreicht.
- *Mobilfunk-Ortung:* Grundvoraussetzung für den Einsatz einer Mobilfunk-Ortung ist das Bestehen eines GSM-Netzes.[22] Grundsätzlich genügt schon ein Antennenstandort, um eine – allerdings ungenaue – Positionierung des Endgerätes vornehmen zu können.[23] Mit der Triangulation ausgehend von mindestens drei Antennenstandorten[24] und Zusatztechniken können Ortungsgenauigkeiten von bis zu 50 Meter erreicht werden.[25] Die Ortungsgenauigkeit hängt allerdings insbesondere auch von der Dichte des Antennennetzes ab. Während in den USA für die Lokalisierung bei Notrufen mit Mobilfunktelefonen eine Ortungsgenauigkeit von 125 Metern staatlich vorgeschrieben ist, verzichtet die Schweiz zurzeit darauf, die Ortungsgenauigkeit für die Standortidentifikation bei Notrufen festzulegen.[26]
- *Drahtlose Netzwerke:* Wireless Local Area Networks (WLAN) nehmen in urbanen Gebieten in der Zahl laufend zu. Sie haben Reichweiten von 10 bis 150 Metern (im Freien bis 300 Meter).[27] Endgeräte, welche sich im Netz befinden, können geortet werden. Wenn die Standorte der WLAN-Stationen bekannt sind, können auch die Endgeräte mit einer relativ hohen Genauigkeit geortet werden.[28]
- *IP-Adresse:* Geräte, die an ein Internet-Netzwerk angeschlossen sind, erhalten eine IP-Adresse. Auf der Grundlage der IP-Adresse kann in zahlreichen Fällen der Standort eines Endgerätes ebenfalls ermittelt werden.[29]

2.3 Rechtliche Relevanz der Lokalisationstechnik

[Rz 8] Location Sharing Systeme bewegen sich insbesondere in den Rechtsgebieten des Geoinformationsrechts, des Fernmelderechts und des Datenschutzrechts.

[Rz 9] Das *Geoinformationsrecht* des Bundes und die entsprechende kantonale Gesetzgebung regeln das Erheben, Nachführen und Verwalten[30] von raumbezogenen Daten nur

---

[19] Vgl. auch die Darstellungen bei Tsai et al. (Fn. 4), S. 2 f.; Carsten Schulte/Christoffer Riemer, Handy-Ortung und GPS-Ortung, Nützliche Location Based Services und einfachste Überwachung für jedermann, Hausarbeit an der Universität Hannover, 10. März 2005, Ziff. III und IV, www.iwi.uni-hannover.de/lv/ucc_ws04_05/riemer/frame_haupt.htm (Stand: 20.07.2010); Steiniger/Neun/Edwardes (Fn. 11), S. 2 f.; die letztgenannten Publikationen unterscheiden im Wesentlichen nur zwischen GPS-Ortung und Mobilfunkortung, was nicht nur aus technischen, sondern auch aus rechtlichen Gründen zu kurz greift.

[20] Vgl. Schulte/Riemer (Fn. 19), Ziffer III; vgl. auch www.swisstopo.admin.ch/internet/swisstopo/de/home/topics/survey/procs/gps.html (Stand: 20.07.2010).

[21] Vgl. www.swisstopo.admin.ch/internet/swisstopo/de/home/topics/survey/procs/gps.html (Stand: 20.04.2010).

[22] Die Abkürzung GSM steht für «Global System for Mobile Communications», entstand ursprünglich aber aus der französischen Bezeichnung «Groupe Spécial Mobile» und bezeichnet einen Mobilfunkstandard der 2. Generation (Vgl. auch Weber [Fn. 10], S. LXXXVIII); HSCSD, GPRS und EDGE sind Erweiterungen des GSM-Standards mit höheren Übertragungsraten, UTMS (Universal Mobile Telecommunications System) ist demgegenüber ein eigener Mobilfunkstandard der 3. Generation; vgl. zum Ganzen auch BAKOM www.bakom.admin.ch/themen/technologie/01397/index.html?lang=de (Stand: 20.07.2010).

[23] So genannte Zellinfo (Cell of Origine-Technologie, COO), vgl. Schulte/Riemer (Fn. 19), Ziffer IV.2.

[24] Vgl. Schulte/Riemer (Fn. 19), Ziffer IV.2; Steiniger/Neun/Edwardes (Fn. 11), S. 18; Tsai et al. (Fn. 4), S. 2.

[25] Vgl. Steiniger/Neun/Edwardes (Fn. 11), S. 18; Schulte/Riemer (Fn. 19), Ziffer IV.2; bei Feldversuchen in Deutschland wurde diese Ortungsgenauigkeit aber nicht erreicht (Ziff. IV.4).

[26] Vgl. Bundesamt für Kommunikation (BAKOM), Technische und administrative Vorschriften betreffend die Leitweglenkung und die Standortidentifikation bei Notrufen, Ausgabe 11 vom 6. November 2009, SR 784.101.113 / 1.3, Ziffer 4.4.2, S. 19.

[27] Vgl. Steiniger/Neun/Edwardes (Fn. 11), S. 19.

[28] Vgl. Tsai et al. (Fn. 4), S. 2; ausführlich – bezogen auf die Aktivitäten von Skyhook Wireless – auch Markus Hofmann/Stefan Betschon, NZZ vom 18. Mai 2010, S. 11.

[29] In diesem Sinne Tsai et al. (Fn. 4), S. 2; zu den technischen Möglichkeiten und Grenzen vgl. Marit Köhntopp/Kristian Köhntopp, Datenspuren im Internet, leicht gekürzte Fassung des in Computer und Recht (CR) 4/200, S. 248 ff. erschienenen Aufsatzes, www.leetupload.com/database/Misc/Papers/eBooks/German!/Hacking/datenspuren_im_internet.pdf (Stand: 20.07.2010); Ralf Kornberger/Helmut Reiser, «Die Suche nach der Nadel im Heuhaufen» – Nyx – Ein System zur Lokalisierung von Rechnern in grossen Netzwerken anhand IP- oder MAC-Adressen, http://wwwmnm-team.informatik.uni-muenchen.de/pub/Publikationen/kore07/PDF-Version/kore07.pdf (Stand: 20.07.2010).

[30] Die Trilogie der Begriffe «Erheben, Nachführen und Verwalten» umfasst auch das Weitergeben, Veröffentlichen, Archivieren und Löschen von

insoweit, als diese Geodaten sich auf Verwaltungsrechtsnormen stützen bzw. durch die öffentliche Verwaltung im Rahmen des Vollzugs von öffentlichen Aufgaben bearbeitet werden. Das Geoinformationsgesetz (GeoIG[31]) des Bundes und seine Ausführungsverordnungen gelten für Geobasisdaten des Bundesrechts und weitere Geodaten der Bundesverwaltung (Art. 2 GeoIG). Gestützt auf Artikel 5 GeoIG hat der Bundesrat die Geobasisdaten des Bundesrechts in einem Katalog, dem so genannten Geobasisdatenkatalog (GBDK, Anhang 1 zur GeoIV[32]) in generell-konkreter Weise festgehalten.[33] Wenn Location Sharing Systeme Geobasisdaten dieses Katalogs benützen, kommt das Geoinformationsrecht zur Anwendung. Dies ist dann der Fall, wenn zu Navigationszwecken Kartendaten der Landesvermessung (Anhang 1 GeoIV, Identifikatoren 33 – 42 und 53), Kartendaten der amtlichen Vermessung (Anhang 1 GeoIV, Identifikatoren 52 – 64) sowie Orthofotos und Luftbilder (Anhang 1GeoIV, Identifikatoren 35 und 36) verwendet werden oder wenn für die Lokalisation mit einem D-GPS bzw. mit der Technologie der Real-time Kinematic (RTK) auf die Permanentnetzdaten (Anhang 1 GeoIV, Identifikator 34) zugegriffen wird. Ebenfalls unter die Geoinformationsgesetzgebung fällt die Lokalisation, wenn bei einer gerätebezogenen Positionierung (terminal-based positioning, device positioning[34]), z.B. bei einem A-GPS (Assisted GPS[35]), die Antennenstandorte (Basisstationen) von Mobilfunknetzen mit einbezogen werden, denn der Antennenkataster der öffentlichen Mobilfunknetze und der Rundfunkstationen gehört zu den Geobasisdaten des Bundesrechts (Anhang 1 GeoIV, Identifikator 111).

[Rz 10] Solange das Endgerät für die Lokalisierung nur die Technologie von GPS, D-GPS oder eine rein gerätebezogene Positionierungstechnologie auf der Grundlage der Antennenstandorte des Mobilfunknetzes verwendet[36], fällt ein Location Sharing System nur insoweit unter die *Fernmeldegesetzgebung*, als für die Datenübertragung das Fernmeldenetz benützt wird. Sowohl die Lokalisation als solche wie auch die Verarbeitung und Verwendung in einem Internet-Service stellen keine Fernmeldedienste oder andere in den Geltungsbereich der Fernmeldegesetzgebung fallenden Tätigkeiten dar (vgl. Art. 2 i.V.m. Art. 3 FMG[37]). Sobald für die Lokalisation Netzwerke von Fernmeldeanlagen (network-based positioning[38]) benützt werden, handelt es sich bei den Auswertungen um Standortdaten, die unter die Fernmeldegesetzgebung fallen (Art. 45b FMG). Auch die *Lokalisation mittels der IP-Adresse* fällt unter die Fernmeldegesetzgebung. Bei der IP-Adresse handelt es sich fernmelderechtlich um einen «numerischen Kommunikationsparameter, der die Identifikation einer insbesondere aus Netzrechnern oder -servern bestehenden Internet-Domain sowie der Benutzerrechner, die an den Verbindungen in diesem Netz beteiligt sind, ermöglicht». (vgl. Anhang zur AEFV[39]). Kommunikationsparameter (Art. 3 Bst. g FMG) sind Adressierungselemente im Sinne von Artikel 3 Buchstabe f FMG. Mit Hilfe der IP-Adressen lokalisierte Standorte von Endgeräten sind damit ebenfalls Standortdaten im Sinne von Artikel 45b FMG.

[Rz 11] Bei Location Sharing Systemen fallen einerseits Daten von (registrierten) Nutzerinnen und Nutzern des Services und andererseits Standortdaten von Geräten, die allenfalls (d.h. mit geeigneten Zusatzinformationen) bestimmten Personen zugeordnet werden können, an. Mithin stellen sich zahlreiche Rechtsfragen hinsichtlich des Datenschutzes, welche teilweise ebenfalls in Abhängigkeit von der verwendeten Technologie (u.a. der Lokalisierungstechnik) beantwortet werden müssen. Auf diese Fragen wird nachfolgend in Ziffer 3 eingegangen.

3. Kernproblem Datenschutz

3.1 Datenschutzbezüge bei Location Sharing Systemen

[Rz 12] Artikel 17 des UNO-Pakts II[40] statuiert einen *umfassenden Schutz der Privatheit*.[41] Dieser umfasst auch den Schutz personenbezogener Daten. Die Vertragsstaaten sind «verpflichtet, die Ermittlung, Verarbeitung, Verwendung und Weitergabe automationsgestützter personenbezogener Daten gesetzlich zu regeln und die Betroffenen gegen Missbräuche durch staatliche Organe wie Private zu schützen»[42]. Diese Bestimmung des UNO-Pakts II ist in der Schweiz

Geodaten und ist deshalb identisch mit dem im Datenschutzrecht gebräuchlichen Begriff des Bearbeitens von Daten.

[31] Bundesgesetz vom 5. Oktober 2007 über Geoinformation (Geoinformationsgesetz, GeoIG), SR 510.62.

[32] Verordnung vom 21. Mai 2008 über Geoinformation (Geoinformationsverordnung, GeoIV), SR 510.620

[33] Ausführlich zum Geobasisdatenkatalog Roman Frick/Daniel Kettiger, Geobasisdaten-Katalog nach Bundesrecht, Dokumentation der Finalisierungsarbeiten, INFRAS, Bern 2006; vgl. auch Bundesamt für Landestopografie (Hrsg.), Leitfaden für die Einführung des neuen Geoinformationsrechts durch die Kantone, Ausgabe vom 30. April 2010, S. 8 ff. und S. 40, Anhang A6, www.swisstopo.admin.ch/internet/swisstopo/de/home/swisstopo/legal_bases.parsysrelated1.61729.downloadList.3958.DownloadFile.tmp/leitfadende.pdf (Stand: 20.07.2010).

[34] Vgl. Steiniger/Neun/Edwardes (Fn. 11), S. 20.

[35] Vgl. http://en.wikipedia.org/wiki/Assisted_GPS (Stand: 20.07.2010).

[36] Vgl. Jason I Hong/J.D. Tygar, Privacy and Client-based Discovery of Location, University of California, Berkeley, S. 4, www.cs.cmu.edu/~jasonh/publications/puc2004-placelab.pdf (Stand: 20.07.2010).

[37] Fernmeldegesetz vom 30. April 1997 (FMG), SR 784.10.

[38] Vgl. Steiniger/Neun/Edwardes (Fn. 11), S. 20.

[39] Verordnung vom 6. Oktober 1997 über die Adressierungselemente im Fernmeldebereich (AEFV), SR 784.104.

[40] Internationaler Pakt vom 16. Dezember 1966 über bürgerliche und politische Rechte (UNO-Pakt II), SR 0.103.2.

[41] In diesem Sinne Manfred Nowak, UNO-Pakt über bürgerliche und politische Rechte. CCPR-Kommentar, Kehr/Strassburg/Arlington 1989, N. 15 f. zu Artikel 17.

[42] Nowak (Fn. 41), N. 21 zu Artikel 17.

direkt anwendbar (self-executing).[43] Auch Artikel 8 der Europäischen Menschenrechtskonvention (EMRK)[44] enthält einen umfassenden Schutz des Privat- und Familienlebens. Auch die EMRK-Bestimmung stellt direkt anwendbares Recht dar.[45] Das Bundesgericht hat – noch unter der alten Bundesverfassung – im Rahmen des Persönlichkeitsschutzes von Artikel 8 EMRK einen Anspruch auf informationelle Selbstbestimmung entwickelt.[46] Artikel 13 Absatz 2 der heutigen Bundesverfassung[47] bringt diese Praxis im Verfassungstext zum Ausdruck.[48] Der Datenschutz ist als *Grundrecht* in der Bundesverfassung verankert: Artikel 13 Absatz 2 BV gewährleistet explizit jeder Person den «Schutz vor Missbrauch ihrer persönlichen Daten». Die Formulierung im Verfassungstext ist allerdings missglückt, weil missverständlich.[49] Der Datenschutz reicht über den eigentlichen Bereich der Privatsphäre hinaus, umfasst alle Informationsbeziehungen und schützt nicht nur vor «Missbrauch» der Daten, sondern grundsätzlich vor Benachteiligungen der betroffenen natürlichen und juristischen Personen durch die Bearbeitung von Personendaten.[50] Dieser Schutzanspruch «gewährleistet dem Einzelnen, grundsätzlich selber darüber zu bestimmen, wem und wann er persönliche Lebenssachverhalte, Gedanken, Empfindungen oder Emotionen offenbart»[51].

[Rz 13] Artikel 13 Absatz 2 BV gewährleistet grundrechtlichen Datenschutz für jeden Umgang mit personenbezogenen Daten von natürlichen und juristischen Personen unabhängig von der Art und vom Verfahren der Datenbearbeitung.[52] Die *Definition des Begriffs der personenbezogenen Daten* ist somit für die Abgrenzung des Geltungsbereichs des Datenschutzes von entscheidender Bedeutung.[53] Die Bundesverfassung überlässt es aber Lehre und Rechtsprechung, den unbestimmten Rechtsbegriff der «persönlichen Daten» genauer zu bestimmen. Aus Artikel 8 EMRK und Artikel 17 UNO-Pakt II ergibt sich der grundrechtliche Datenschutz nur implizit; der Begriff der Personendaten findet sich in diesen internationalen Übereinkommen nicht. Demgegenüber enthält Artikel 2 Buchstabe a des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (ER-Konv-108)[54] eine Definition des Begriffs der personenbezogenen Daten. Artikel 3 Buchstabe a des Datenschutzgesetzes des Bundes (DSG)[55] übernimmt die Begriffsbestimmung von Artikel 2 Buchstabe a ER-Konv-108 fast wörtlich[56] und legt fest, Personendaten seien «alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen».

[Rz 14] Auch mit dem Begriffspaar «bestimmte oder bestimmbare Person» wurde ein unbestimmter Rechtsbegriff geschaffen.[57] Dieser wurde in der Schweiz durch die Lehre und Rechtsprechung primär als Anwendungsfall von Artikel 3 DSG (und gleich lautenden Bestimmungen in kantonalen Datenschutzgesetzen) ausgefüllt. Heute gilt eine Person als *bestimmt*, wenn sich aus der Information selbst ergibt, dass es sich um diese ganz bestimmte Person handelt (Adresse, Kundenkarteikarte, Personaldossier, Zeitungsartikel mit namentlicher Nennung bestimmter Personen). Wie der Bezug zur betroffenen Person hergestellt wird, ist ohne Bedeutung. Die Zuordnung kann auf verschiedene Arten erfolgen, indem z.B. ein Schlüssel (AHV-Nummer, Aktenzeichen, Kundennummer) verwendet wird.[58] *Bestimmbar* ist nach herrschender Lehre und Rechtsprechung eine Person dann, wenn eine Identifikation durch die Kombination verschiedener Informationen ohne einen unverhältnismässigen Aufwand möglich ist.[59] Der für die Bestimmung einer Person zu betreibende Aufwand ist dann nicht mehr vertretbar, «wenn nach den allgemeinen Lebenserfahrungen nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird (etwa durch eine komplizierte Analyse einer Statistik)...»[60]. Ob eine Person bestimmbar ist, muss daher anhand objektiver Kriterien im konkreten Fall beurteilt werden, wobei insbesondere auch die Möglichkeiten der Technik mit zu berücksichtigen sind. Entscheidend ist somit nicht, ob jene Person, welche die Daten bearbeitet, den für eine Identifizierung erforderlichen Aufwand treiben kann oder will, sondern ob damit gerechnet werden muss, dass eine Drittperson, die ein

[43] Vgl. Alexander R. Ziegler, Einführung in das Völkerrecht, Bern 2006, Rz. 279.

[44] Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), SR 0.101.

[45] Vgl. Ziegler (Fn. 43), Rz. 279.

[46] Vgl. z.B. BGE 113 Ia 1 ff.; Jörg Paul Müller/Markus Schefer, Grundrechte in der Schweiz; 4. Aufl.; Bern 2008, S. 164, mit Hinweisen.

[47] Bundesverfassung vom 18. April 1999 der Schweizerischen Eidgenossenschaft (BV), SR 101.

[48] In diesem Sinne Müller/Schefer (Fn. 46), S. 164.

[49] Vgl. Rainer J. Schweizer, St. Galler Kommentar, 2. Aufl., Artikel 13 Absatz 2 BV, Rz. 39.

[50] In diesem Sinne Rainer J. Schweizer, Verfassungsrechtlicher Persönlichkeitsschutz, in: Thürer, Daniel et al. (Hrsg.), Verfassungsrecht der Schweiz; Zürich 2001, Rz. 29, S. 704.

[51] Müller/Schefer (Fn. 46), S. 127, mit Hinweisen.

[52] Vgl. auch Schweizer (Fn. 49), Rz. 41.

[53] In diesem Sinne auch Weber (Fn. 10), S. 436.

[54] Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1.

[55] Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.

[56] In diesem Sinn auch Urs Belser, Basler Kommentar zum DSG, Artikel 3, Rz. 2.

[57] Die Lehre geht heute davon aus, dass sich das Kriterium der Bestimmtheit bzw. Bestimmbarkeit aus einem absoluten und einem relativen Element zusammensetzt: Als absolutes Element wird verlangt, dass sich die Personendaten auf eine bestimmte natürliche oder juristische Person beziehen (Individualisierbarkeit), als relatives Element kommt hinzu, dass diese Person identifiziert werden kann (Identifizierbarkeit), vgl. David Rosenthal, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 3 Bst. a, Rz. 18 ff.

[58] Vgl. Belser (Fn. 56), Artikel 3, Rz. 6.

[59] Vgl. Belser (Fn. 56), Artikel 3, Rz. 6.

[60] Vgl. Belser (Fn. 56), Artikel 3, Rz. 6, mit Hinweis auf BBl 1988 II 445.

Interesse an diesen Angaben hat, bereit ist, eine Identifizierung vorzunehmen.[61]

[Rz 15] Eine ähnliche, möglicherweise nicht ganz so enge Auslegung erfährt die Frage der Bestimmbarkeit übrigens auch im europäischen Gemeinschaftsrecht: «[A]ls bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.»[62] Bei der Entscheidung, ob eine Person bestimmbar ist, sollen «alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen»[63]. Damit wird zum Ausdruck gebracht, dass der Massstab nicht irgendwelche hypothetische Bedrohungen sein können, sondern dass von dem ausgegangen werden muss, was Menschen vernünftigerweise zu tun bereit sind, um zu gewissen für sie interessanten Informationen zu gelangen.

[Rz 16] Vom verfassungsrechtlichen Schutz vor dem Missbrauch persönlicher Daten (Art. 13 Abs. 2 BV) klar zu unterscheiden ist das ebenfalls als Grundrecht ausgestaltete *Fernmeldegeheimnis* (Art. 13 Abs. 1 BV). Das Post- und Fernmeldegeheimnis hat sich als besonderes Grundrecht aus der spezifischen Gefährdungslage der zunehmenden Organisation und Technologisierung der Kommunikation einerseits und der Monopolstellung des Staates bei den Kommunikationsträgern andererseits entwickelt.[64] Geschützt werden alle Formen der individualisierten Kommunikation[65], unabhängig vom verwendeten Übertragungsmedium.[66] Der Grundrechtsschutz umfasst nicht nur den Inhalt der Kommunikation, sondern auch Randdaten, z.B. Adressierungselemente oder Verkehrs- und Rechnungsdaten.[67] In der neueren Lehre und Rechtsprechung wird der Grundrechtsschutz von Artikel 13 Absatz 1 BV zunehmend auch auf elektronische Systeme zur Datenverarbeitung (bzw. deren Endgeräte wie Mobiltelefone) im globalen Kommunikationsnetz ausgeweitet.[68] Umstritten ist, ob das Fernmeldegeheimnis als solches eine Drittwirkung für Private hat[69] oder ob erst Artikel 35 BV den Gesetzgeber verpflichtet, für entsprechenden Schutz zu sorgen[70]. Das Fernmeldegeheimnis wird im FMG relativ ausführlich konkretisiert.[71]

[Rz 17] Eine klare dogmatische *Abgrenzung zwischen dem Datenschutz und dem Fernmeldegeheimnis* fehlt bis heute sowohl hinsichtlich der verfassungsmässigen Rechte wie auch hinsichtlich des Geltungs- und Anwendungsbereichs von DSG und FMG.[72] Der Grundsatz des Vorrangs des spezielleren Gesetzes (lex specialis) vor dem allgemeineren[73] sowie Hinweise in den Materialien zum FMG[74] führen zu einer Auslegung dahingehend, dass im gesamten Geltungsbereich des FMG das Fernmeldegeheimnis das Recht auf Persönlichkeitsschutz verdrängt und diesem vorgeht. Klarheit hat letztlich – für die Stufe des Verordnungsrechts – erst der Bundesrat mit der Kollisionsnorm von Artikel 89 FDV[75] geschaffen, welche festhält, dass das DSG insoweit Anwendung findet, als die FDV keine besonderen Regelungen zum Datenschutz enthält. Das Grundrecht auf Schutz vor Missbrauch persönlicher Daten und das allgemeine Datenschutzrecht kommen im Fernmeldebereich somit nur subsidiär zur Anwendung, insbesondere dann, wenn das Fernmeldegeheimnis weniger weit geht als der Personendatenschutz.

[Rz 18] Vor diesem Hintergrund werden nachfolgend verschiedene Personenbezüge zu untersuchen sein. Dabei

---

61 In diesem Sinne auch Jean-Philippe Walter, Der Datenschutz und die geographischen Informationssysteme, Newsletter e-geo.ch 5-3/2004, S. 4 f.

62 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, Artikel 2 Buchstabe a; zitiert aus BfD-Info 1, S. 112.

63 Richtlinie 95/46/EG, Erwägungsgründe, Ziffer 26; in diesem Sinne auch Urs Belser, Basler Kommentar zum DSG, Artikel 3, Rz. 6.

64 Vgl. Müller/Schefer (Fn. 46), S. 201.

65 Der Grundrechtsschutz umfasst nur die Kommunikation zwischen bzw. gegenüber individualisierbaren Einzelnen, nicht jedoch gegenüber einer nicht näher spezifizierten Allgemeinheit, vgl. Müller/Schefer (Fn. 46), S. 205.

66 Vgl. Müller/Schefer (Fn. 46), S. 203; Giovanni Biaggini, Bundesverfassung der Schweizerischen Eidgenossenschaft, Kommentar, Zürich 2007, Artikel 13, Rz. 10, je mit zahlreichen Hinweisen; geschützt werden damit gemäss der Lehre und Rechtsprechung etwa der Briefverkehr, Telefongespräche, Faxübermittlungen, SMS, MMS, eMails oder Signale des Pagers.

67 Vgl. Müller/Schefer (Fn. 46), S. 203; in Deutschland fallen diese Daten – anders als in der Schweiz – nach Abschluss des Übertragungsvorgangs nicht mehr unter den Schutz des Fernmeldegeheimnisses, sondern unter den Schutz der informationellen Selbstbestimmung, vgl. BVerfG, CR 2006, 383 = MR 2006, 217, Rz. 72, zitiert nach Volker Haug, Internetrecht, 2. Aufl., Stuttgart 2010, Rz. 87.

68 Vgl. Müller/Schefer (Fn. 46), S. 206 f.

69 Dieser Auffassung Müller/Schefer (Fn. 46), S. 207 ff.

70 Vgl. Biaggini (Fn. 66), Artikel 13, Rz. 10; in diesem Sinne offenbar auch die deutsche Lehre, vgl. Haug (Fn. 67), Rz. 85, mit Hinweisen.

71 In diesem Sinne auch Müller/Schefer (Fn. 46), S. 202.

72 Keines der Gesetze enthält im gegenseitigen Verhältnis ausdrückliche Kollisionsnormen.

73 Vgl. Ulrich Häfelin/Georg Müller/Felix Uhlmann, Allgemeines Verwaltungsrecht, 5. Aufl., Zürich 2006, Rz. 220.

74 Vgl. die Botschaft zum revidierten Fernmeldegesetz (FMG) vom 10. Juni 1996, BBl 1996 II 1405, S. 1415: «Ergänzend zum DSG regelt der Entwurf zum neuen Fernmeldegesetz Probleme des Datenschutzes, die spezifisch mit dem Erbringen von Telekommunikationsdienstleistungen im Zusammenhang stehen»; vgl. auch Botschaft zur Änderung des Fernmeldegesetzes (FMG) vom 12. November 2003, BBl 2003 7951, S. 7966, wo die ergänzten Regelungen im FMG als Verbesserung des Datenschutzes (und somit als spezialgesetzliche Datenschutzbestimmungen) bezeichnet werden; vgl. auch S. 7975, wo von Übereinstimmung mit dem DSG gesprochen wird (was nur dann Sinn macht, wenn man vom Vorrang der Regelung des FMG ausgeht).

75 Verordnung vom 9. März 2007 über Fernmeldedienste (FDV), SR 784.101.1.

können die Personenbezüge (und damit die allenfalls unter den Datenschutz und das Fernmeldegeheimnis fallenden Daten und Informationen) wie folgt unterschieden werden:

- *Personenbezug zu Dienstleistungen:* Personenbezüge zu Dienstleistungen (Services) entstehen dadurch, dass eine bestimmte Person diese Dienstleistung entgeltlich oder unentgeltlich nutzt. Durch die Registrierung als Nutzerin oder Nutzer bzw. durch eine vertragliche Abmachung[76] hinsichtlich der Nutzung entsteht eine Konsumentenstellung, die in der Regel individualisierbar ist und mit dem Austausch weiterer personenbezogener Daten verbunden ist (erweiterte Personalien, Rechnungsdaten etc.).[77]
- *Personenbezug zu Geräten und Anlagen:* Der Personenbezug zu Geräten und Anlagen in Kommunikationsnetzwerken besteht entweder (sachenrechtlich) im Eigentum oder (faktisch) in der Nutzung[78]. Über diese Bezüge ist es unter bestimmten Voraussetzungen ebenfalls möglich, eine Zuordnung von weiteren Daten und Informationen zu einer bestimmten Person zu machen.
- *Personenbezug zu Örtlichkeiten:* Im vorliegenden Kontext massgebliche Personenbezüge zu Örtlichkeiten entstehen durch einen räumlichen und zeitlichen Bezug zu einem bestimmten Ort, an dem sich eine bestimmte Person aufhält. Der Informationsgehalt der Daten besteht im Standort der bestimmten Person zu einem bestimmten Zeitpunkt. Zeitreihen von Daten über den Standort[79] einer bestimmten Person können zu Bewegungsbildern führen, welche unter bestimmten Umständen für sich alleine oder in Verbindung mit weiteren personenbezogenen Daten nicht mehr gewöhnliche Personendaten, sondern Persönlichkeitsprofile (Art. 3 Bst. d DSG) darstellen.[80]

3.2 Exkurs: Sind IP-Adressen Personendaten?

[Rz 19] Gemäss der neueren Rechtsprechung des in Datenschutzbelangen auf Bundesebene zuständigen Bundesverwaltungsgerichts (BVGer) handelt es sich bei den IP-Adressen um Personendaten.[81] Diese Auffassung findet sich teilweise auch in der Rechtslehre.[82] Sie soll nachfolgend untersucht werden.

[Rz 20] Vorab muss festgehalten werden, dass das Urteil des BVGer an einem grundlegenden Mangel leidet. Bei den IP-Adressen handelt es sich – wie bereits erwähnt[83] und wie auch vom BVGer richtig zitiert[84] – um numerische Kommunikationsparameter und damit um *Adressierungselemente im Sinne der Fernmeldegesetzgebung*. Mithin fallen die IP-Adressen primär unter das Fernmeldegeheimnis (Art. 13 Abs. 1 BV; Art. 43 FMG).[85] Als solche sind sie – solange sie Gegenstand individualisierbaren Fernmeldeverkehrs sind, wovon grundsätzlich auszugehen ist – geheim zu halten, unabhängig davon, ob sie Personendaten im Sinne der Datenschutzgesetzgebung darstellen. Die IP-Adressen gehören nicht zu jenen Adressierungselementen und damit verbundenen Daten im Bereich der Internet-Adressierung, die öffentlich bekannt gegeben werden müssen (e contrario Art. 14h ARFV). Somit dürfen IP-Adressen nur unter den besonderen in der Fernmeldegesetzgebung festgehaltenen Voraussetzungen bearbeitet und bekannt gegeben werden. Nach der hier vertretenen Auffassung liegt eine abschliessende Regelung durch die Fernmeldegesetzgebung vor, so dass das allgemeine Datenschutzrecht gar nicht zur Anwendung gelangen kann. Mithin ist die Frage, ob es sich bei IP-Adressen um Personendaten handelt, eigentlich entbehrlich.

[Rz 21] Will man der Frage trotzdem nachgehen, muss man sich zuerst der Funktion der IP-Adresse bewusst werden:[86] Um eine Kommunikation zwischen zwei technischen Geräten aufzubauen, muss jedes der Geräte in der Lage sein, dem anderen Gerät Daten zu senden. Damit diese Daten bei der richtigen Gegenstelle ankommen, muss diese eindeutig benannt (adressiert) werden. Dies geschieht in IP-Netzen

---

[76] Im Bereich der Fernmeldegesetzgebung sind dies Abonnentinnen und Abonnenten im Sinne von Artikel 1 Buchstabe b FDV.

[77] Weber (Fn. 10), S. 434, verwendet den Begriff der Stammdaten; abweichend von Weber (Fn. 10), S. 435, werden die Abrechnungsdaten (Entgeltdaten) nicht als eigenständiger Personenbezug betrachtet sondern dem Bezug durch Dienstleistung zugerechnet.

[78] Im Bereich der Fernmeldegesetzgebung sind dies Benutzerinnen und Benutzer im Sinne von Artikel 1 Buchstabe a FDV; Weber (Fn. 10), S. 435, verwendet für den Begriff der Nutzungsdaten auch den Begriff «Verbindungsdaten».

[79] Der Begriff der «Standortdaten» ist bundesrechtlich anderweitig besetzt und meint – fernmeldetechnisch – den Standort des Endgerätes einer Kundin bzw. eines Kunden (Art. 45b FMG); die gleiche rechtstechnische Bedeutung hat der Begriff «Standortdaten» auch in Deutschland, vgl. Haug (Fn. 67), Anhang 2, S. 425.

[80] Das Vorliegen eines Persönlichkeitsprofils ist allerdings nicht leichthin anzunehmen, da die Gesamtheit der Daten eine Beurteilung wesentlicher Aspekte der Persönlichkeit ermöglichen muss, vgl. Belser (Fn. 56), Artikel 3, Rz. 21 f., sowie die Beispiele bei Yvonne Jöhri, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 3 Bst. d, Rz. 59.

[81] Urteil A-3144/2008 vom 27. Mai 2009, insbesondere E. 2.2.2 – 2.2.4.

[82] Vgl. Rosenthal (Fn. 57), Art. 3 Bst. a, Rz. 27; differenzierter Weber (Fn. 10), S. 470 f., der von keinen Personendaten ausgeht, wenn die Identifikation nur vom Access-Provider vorgenommen werden kann (S. 471), aber klar von Personendaten ausgeht, wenn Nutzerprofile unter Einbezug von IP-Adressen erstellt werden (S. 473).

[83] Vgl. vorstehend Ziffer 2.3.

[84] Vgl. Urteil A-3144/2008 vom 27. Mai 2009, E. 2.2.2.

[85] Damit ist auch fraglich, ob der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) als Vorinstanz überhaupt zuständig zur Abgabe einer Empfehlung gewesen ist und ob das BVGer die Beschwerde nicht schon wegen Unzuständigkeit der Vorinstanz (von Amtes wegen) hätte aufheben sollen.

[86] Vgl. http://de.wikipedia.org/wiki/IP-Adresse (Stand: 20.07.2010).

(insbesondere im Internet[87]) mit einer IP-Adresse. Die IP-Adresse gilt grundsätzlich als Adressierung eines Geräts in einem bestimmten Netzwerk; gehört das Gerät auch zu einem anderen Netzwerk, hat es dort allenfalls eine andere IP-Adresse.[88] Man muss zwischen statischen und dynamischen IP-Adressen unterscheiden. Eine *statische IP-Adresse* wird permanent oder für eine längere Dauer an ein bestimmtes Gerät (in der Regel ein Rechner) gebunden.[89] Bei statischen IP-Adressen ist mithin in aller Regel ein direkter und eindeutiger Bezug von der IP-Adresse auf das Gerät möglich. *Dynamische IP-Adressen* werden den Teilnehmern – genauer den an einer Punkt-Punkt-Verbindung eines Netzwerks teilnehmenden Geräten – erst bei der Nutzung zugewiesen und können pro Sitzung oder sogar während der laufenden Sitzung ändern.[90] Oft kennzeichnet eine IP-Adresse nicht unmittelbar den abrufenden Rechner, sondern einen vorgesetzten Proxy-Rechner, der stellvertretend für andere Geräte auftritt und die Abrufe vornimmt.[91] Bereits in grossen dynamischen lokalen Netzwerken ist es nach Auffassung von Fachpersonen keine triviale Aufgabe, den Standort eines bestimmten Endgeräts auf der Grundlage der IP-Adresse (allenfalls in Verbindung mit der fest einem Gerät zugeordneten MAC-Adresse) zu ermitteln.[92] Zudem gibt es heute zahlreiche neue Anonymitätstechniken, welche die Ermittlung des Endgerätes mittels der IP-Adresse weitgehend verhindern.[93] Bestimmte Anonymizer[94] und Remailer sind so wirksam, dass die Datenspur selbst für den Betreiber des betreffenden Dienstes nicht mehr nachvollziehbar ist.[95] Bereits aus technischen Gründen ist somit die Bestimmbarkeit eines Geräts im Internet auf der Grundlage der IP-Adresse oft nicht oder nur mit erheblichem Aufwand möglich.

[Rz 22] IP-Adressen – insbesondere dynamische IP-Adressen – können in der Regel nur über eine Auskunft des Access-Providers und ggf. weiterer Inhaber von an der Kommunikation beteiligten Webservern in Erfahrung gebracht werden.[96] Bezüglich der Anbieter in der Schweiz geschieht dies nach den Vorschriften betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜFP[97], VÜPF[98]). Jede Internet-Anbieterin muss gemäss Artikel 26 Absatz 1 VÜPF in der Lage sein, die Überwachungstypen nach Artikel 24 VÜPF auszuführen, die durch sie angebotene Dienste betreffen, und den zuständigen Behörden die vorgeschriebenen Auskünfte (Art. 27) zu erteilen (dazu gehören insbesondere IP-Adresse und E-Mail-Adresse). Die entsprechenden Auskünfte sind grundsätzlich nur im Rahmen der Strafverfolgung und nur unter den im BÜFP beschriebenen Voraussetzungen erhältlich.[99] Sobald sich ein Webserver im Ausland befindet, können die Informationen zur IP-Adresse nur noch auf dem Rechtshilfeweg in Erfahrung gebracht werden. Die Strafverfolgungsbehörden verschiedener ausländischer Staaten verweigern aber oft die entsprechenden Ermittlungen bei Delikten, welche nach ihrem Landesrecht als wenig schwer gewichtet werden (z.B. Ehrverletzungsdelikte, unlauterer Wettbewerb etc.). Zu diesen Staaten gehören insbesondere auch die Vereinigten Staaten von Amerika (USA)[100], wo eine Vielzahl von vielfrequentierten Internetanwendungen gehostet werden, insbesondere auch grosse Anbieter von E-Mail-Diensten.

[Rz 23] Soweit die oft aufwändigen Nachforschungen gelingen, lässt sich mit der IP-Adresse primär ein bestimmter Rechner identifizieren.[101] Auf der Grundlage dieser Information lässt sich – allenfalls ebenfalls mit erheblichem Aufwand – die Eigentümerin oder der Eigentümer des Geräts ermitteln. Auf diese Weise kann somit einer IP-Adresse in zahlreichen Fällen, aber immer nur nachträglich, die natürliche oder juristische Person zugeordnet werden, der das Gerät zum Zeitpunkt der Ermittlung (nicht zwangsläufig auch zu einem früheren Zeitpunkt) gehört.[102] Insoweit dieser Personenbezug herstellbar ist, ist die Person im Sinne von Artikel 3 Buchstabe a DSG grundsätzlich bestimmbar[103], und es müsste davon ausgegangen werden, dass es sich bei der IP-Adresse um Personendaten im Sinne der Datenschutzgesetzgebung

---

87 Das Kürzel IP steht für Internet-Protokoll.

88 Vgl. zum Datenfluss im Internet Köhntopp/Köhntopp (Fn. 29), S. 5 ff.

89 Vgl. Köhntopp/Köhntopp (Fn. 29), S. 1.

90 Vgl. Köhntopp/Köhntopp (Fn. 29), S. 1.

91 Vgl. Köhntopp/Köhntopp (Fn. 29), S. 2.

92 Vgl. Kornberger/Reiser (Fn. 29), Ziffer 1.2.

93 Vgl. Hannes Federrath/Andreas Pfitzmann, «Neue» Anonymitätstechniken, Datenschutz und Datensicherheit (DuD) 22 (1998), V2.6; Weber (Fn. 10), S. 489 f.; Craig Chatfield/René Hexel, Privacy and Security within Intelligent Environments, Griffith University, Brisbane, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.4348&rep=rep1&type=pdf (Stand: 20.07.2010).

94 Beschreibung vgl. Federrath/Pfitzmann (Fn. 93), S. 3.

95 Vgl. Burkhard Schröder, Rechtsextremismus im Internet, Aus Politik und Zeitgeschichte B 39/2000, S. 54.

96 In diesem Sinne auch Weber (Fn. 10), S. 471.

97 Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), SR 780.1.

98 Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF), SR 780.11.

99 Im Zivilprozess ist die Durchsetzung des Informationsanspruchs nicht möglich, vgl. Christian Schwarzenegger, Urheberstrafrecht und Filesharing in P2P-Netzwerken, in: Christian Schwarzenegger et al. (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, S. 249.

100 Dem Verfasser liegen aus seiner Anwaltstätigkeit mehrere solche Fälle vor, so auch das folgende Beispiel: Bei einem ehrverletzenden Beitrag auf einer Webseite mit einer Schweizer Domain (.ch) stellte sich heraus, dass diese auf dem in der Schweiz liegenden Server nur als Domain-Pointing gehostet wurde, während das eigentliche Hosting auf einem in den USA gelegenen Webserver vorgenommen wird. Die schweizerischen Strafverfolgungsbehörden stellten daraufhin die Ermittlungen ein wegen der mangelnden Erfolgsaussichten, die IP-Adresse des Geräts, von welchem aus der Inhalt aufgeschaltet wurde (content-management), von den US-Behörden rechtshilfeweise in Erfahrung zu bringen.

101 In diesem Sinne auch Urteil A-3144/2008 vom 27. Mai 2009, E. 2.2.4.

102 In diesem Sinne auch Rosenthal (Fn. 57), Art. 3 Bst. a, Rz. 27.

103 Vgl. vorstehend Ziffer 3.1.

handelt. Entgegen der Auffassung des BVGer wird hier die Auffassung vertreten, dass die Identifikation der Person nur mit einem unverhältnismässigen Aufwand möglich ist und dass deshalb keine Bestimmbarkeit im Sinne von Artikel 3 Buchstabe a DSG vorliegt.

[Rz 24] Die IP-Adresse kann – wie erwähnt – einem Gerät und damit allenfalls der am Gerät berechtigten Person zugeordnet werden. Entgegen der weit verbreiteten Auffassung[104] ist damit aber noch keine direkte Zuordnung zur Person möglich, welche das Gerät zu einem gegebenen Zeitpunkt wirklich nutzte (und sich – was vorliegend von Interesse ist – zu diesem Zeitpunkt am Gerätestandort befand).[105] Die Identifikation der Nutzerin bzw. des Nutzers muss über weitere prozessrechtliche Beweis- bzw. Zwangsmassnahmen (z.B. Zeugenbefragungen) oder an Hand von Indizienbeweisen (wenn sich die Rechner-Konsole in einem Raum befindet, zu dem nur eine bestimmte Person Zugang hat) vorgenommen werden.

[Rz 25] Die Frage, ob IP-Adressen tatsächlich Personendaten im Sinne der Datenschutzgesetzgebung sind, ist mit dem erwähnten Urteil des Bundesverwaltungsgerichts wohl kaum abschliessend geklärt und wird wohl noch längere Zeit kontrovers diskutiert werden. Offenbar ist auch in der Rechtspraxis anderer europäischer Staaten diese Frage noch nicht geklärt, so insbesondere in Deutschland[106]. Nach der hier vertretenen Auffassung stellen *IP-Adressen nicht generell Personendaten* dar; es ist vielmehr *im Einzelfall zu prüfen*, ob einer IP-Adresse im Bezug auf eine bestimmte Person die Qualität von Personendaten zukommt.

3.3 SIM-Karte

[Rz 26] Die SIM-Karte (Subscriber Identity Module) ist eine Chipkarte, die in ein Mobiltelefon bzw. ein anderes Endgerät der Mobilfunktechnologie eingesteckt wird und zur Identifikation der Nutzerin bzw. des Nutzers im Netz dient.[107] Mit ihr stellen Mobilfunkanbieter Teilnehmern mobile Telefonanschlüsse und Datenanschlüsse (z.B. Internetzugang) zur Verfügung. Über die SIM-Nummer lässt sich jede SIM-Karte identifizieren (Art. 2 Bst. m VÜPF). Zumindest bezüglich der Abonnentinnen und Abonnenten von Fernmeldeunternehmungen, die dem schweizerischen Fernmelderecht unterstehen, sowie bezüglich der Käuferinnen bzw. Käufer der in der Schweiz verkauften Prepaid-SIM-Karten[108] lässt sich die Identität jederzeit feststellen. Diese Person muss jedoch nicht identisch mit der Person sein, die ein mobiles Endgerät zu einem bestimmten Zeitpunkt auch wirklich nutzt, denn die SIM-Karte bzw. das entsprechende Endgerät kann sich – rechtmässig oder unrechtmässig – im Besitz einer anderen Person befinden.

[Rz 27] Die SIM-Karte lässt zudem auch keinen Bezug zu einem bestimmten Gerät zu, da sie in jedes beliebige Mobiltelefongerät eingesetzt und aus diesem auch wieder entfernt werden kann.

3.4 Anonymes Location Sharing System: die Ausnahme

[Rz 28] Nach der hier vertretenen Auffassung ist es grundsätzlich möglich, ein Location Sharing System (allerdings mit teilweise eingeschränkten Funktionen und kostenlos) zu betreiben, bei welchem die Nutzerin bzw. der Nutzer vollständig anonym bleiben könnte, dies solange zur Lokalisation ausschliesslich die reine GPS-Technologie eingesetzt wird und die Informationsübertragung ausschliesslich mittels der Telefonie erfolgt: Die Nutzerin oder der Nutzer kann sich von irgendeinem beliebigen Rechner aus beim entsprechenden Internetservice anonym mit einem Pseudonym (nick-name) registrieren und erhält eine numerische Benutzeridentifikation (Benutzer-ID). Die notwendige Software für das mobile Endgerät kann die Person ohne Registrierung direkt vom Internet auf das Endgerät herunterladen. Das mobile Endgerät sendet dann die mittels GPS ermittelten Vektordaten des Standorts zusammen mit der kryptografisch verschlüsselten Benutzer-ID periodisch über eine Telefonverbindung an den Service. Der Service nimmt die Anrufe entgegen, ohne die Teilnehmernummern aufzuzeichnen, entschlüsselt die Benutzer-ID und rechnet den Standort aus. In einem Darstellungsdienst (Geodaten-Viewer) kann dann durch Eingabe des Pseudonyms der Standort raumbezogen (d.h. auf einem Kartenhintergrund) dargestellt werden. Zugriff im Internet zu den Informationen über den Standort der betreffenden

[104] Vgl. Rosenthal (Fn. 57), Art. 3 Bst. a, Rz. 27; Urteil A-3144/2008 vom 27. Mai 2009, E. 2.2.4.

[105] Vgl. Hong/Tygar (Fn. 36), S. 5: «It should also be noted that even if a web service can correlate IP addresses to physical locations, it may not be a significant threat to individual privacy if no personally identifiable information is transmitted. The web service might be able to infer that someone is there, but not necessarily who.»

[106] Das Amtsgericht Berlin hat mit Urteil vom 27. März 2007 (Az. 5 C 314/06) befunden, bei der IP-Adresse handle es sich um Personendaten im Sinne der Datenschutzgesetzgebung, das Amtsgericht München kam mit Urteil vom 30. September 2008 (Az. 133 C 5677/08) zum gegenteiligen Schluss; mit Urteil vom 2. März 2010 (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08) geht das BverfG implizit davon aus, dass es sich bei der IP-Adresse um Personendaten handelt, stuft aber deren Schutzwürdigkeit erheblich herab, vgl. Haug (Fn. 67), Rz. 405; Christoph Ohrmann, Der Schutz der Persönlichkeit in Online-Medien, Frankfurt a.M. 2009, S. 89, vertritt die Auffassung, dynamische IP-Adressen seien *im Zweifelsfall* als Personendaten zu betrachten.

[107] Vgl. http://de.wikipedia.org/wiki/SIM-Karte (Stand: 20.07.2010).

[108] Die Anbieterinnen und Anbieter von Fernmeldediensten müssen sicherstellen, dass beim Verkauf von Prepaid-SIM-Karten die Personalien der Kundinnen und Kunden (Name, Vorname, Adresse, Geburtsdatum) anhand eines gültigen Reisepasses, einer Identitätskarte oder eines anderen für den Grenzübertritt in die Schweiz zulässigen Reisedokumentes erfasst werden; ausserdem sind die Art des Ausweises und die Ausweisnummer zu erfassen (Art. 19a VÜPF).

Nutzerinnen und Nutzer hätten dann nur diese Person selbst sowie Personen, denen das Pseudonym mitgeteilt wird. Ein solches System lässt weder einen Personenbezug zum Service noch einen Personenbezug zum Gerät und damit auch keinen Personenbezug zum Standort zu.

3.5 Einwilligung (informed consent)

[Rz 29] Gemäss Artikel 45b FMG ist die Bearbeitung von Standortdaten auch über Abrechnungszwecke hinaus – d.h. auch für Mehrwertdienste und Services – zulässig, wenn eine entsprechende Einwilligung der Kundin bzw. des Kunden vorliegt. Auch das Datenschutzgesetz lässt eine Bearbeitung von Personendaten in jedem Fall zu, wenn die betroffene Person in die Bearbeitung ausdrücklich eingewilligt hat (vgl. Art. 6 Abs. 2 Bst. c, Art. 13 Abs. 1, Art. 17 Abs. 2 Bst. c, Art. 19 Abs. 1 Bst. b DSG). In zahlreichen Fällen ist allerdings keine Einwilligung notwendig, der betroffenen Person steht aber die Möglichkeit zum Widerspruch offen (Art. 12 Abs. 2 und Art. 20 DSG)[109]; in diesen Fällen wird mit der ausdrücklichen Einwilligung aber ein Widerspruch zum Vornherein ausgeschlossen. In der Praxis können bei komplexen Datenflüssen, wie sie bei Location Sharing Systemen bestehen, Abgrenzungsprobleme entstehen, ob eine Einwilligung notwendig ist[110]; diese Abgrenzungsprobleme und die damit allenfalls verbundenen Beweisschwierigkeiten können vermieden werden, wenn eine Einwilligung (freiwillig) eingeholt wird. Der Schlüssel zu einem Location Sharing Service, der in jedem Fall zweifelsfrei den Erfordernissen der Datenschutzgesetzgebung entspricht, heisst somit Einwilligung durch die Abonnentin bzw. den Abonnenten des Services.

[Rz 30] Der Gesetzgeber hat sich hinsichtlich der Einwilligung beim Datenschutz (Art. 4 Abs. 5 DSG) an den Anforderungen der Einwilligung des aufgeklärten Patienten bei medizinischen Eingriffen orientiert.[111] Die betroffene Person muss somit über alle Informationen verfügen, die erforderlich sind, damit sie eine *freie Entscheidung* treffen kann (informed consent).[112] Dies entspricht im Übrigen auch den Empfehlungen von Branchenverbänden.[113]

[Rz 31] Eine Einwilligung in die Bearbeitung von eigenen Personendaten kann erteilen, wer in dieser Sache urteilsfähig ist, d.h. wer fähig ist, die Folgen der Datenbearbeitung in einem Location Sharing System abzuschätzen; eine Zustimmung der gesetzlichen Vertretung ist bei urteilsfähigen, aber unmündigen (z.B. Kinder unter 18 Jahre) oder entmündigten Personen nicht notwendig.[114] Die Frage, ob umgekehrt Eltern für ihre unmündigen Kinder eine Einwilligung erteilen können, wird nachfolgend noch zu diskutieren sein.[115]

[Rz 32] Die Einwilligung muss immer *im Voraus*, d.h. vor Inbetriebnahme des Services für die betreffende Person und vor dem Beginn der Bearbeitung von Daten, erteilt werden (Art. 4 Abs. 5 DSG); eine nachträgliche Einwilligung ist als solche unwirksam.[116] Die Einwilligung ist jederzeit und *frei widerrufbar*.[117] Dies ergibt sich insbesondere auch aus dem Verbot der übermässigen Selbstbindung (Art. 27 Abs. 2 ZGB[118]).[119] Der Widerruf gilt allerdings nur für die Zukunft, d.h. hinsichtlich der künftigen Bearbeitung von Daten; auf die seit dem Zeitpunkt der Erteilung der Einwilligung bearbeiteten Daten hat er keinen Einfluss mehr (diese Bearbeitung bleibt rechtmässig).[120] Das Recht zum Widerruf besteht auch dann, wenn dieser im Widerspruch zu vertraglichen Vereinbarungen steht, er kann aber allenfalls einen Vertragsbruch darstellen, der zu Schadenersatz führen kann.[121]

[Rz 33] Die Einwilligung in die Bearbeitung von Personendaten ist nicht an eine bestimmte Form gebunden und kann grundsätzlich stillschweigend bzw. durch konkludentes Handeln erfolgen.[122] Untätigkeit (Nichthandeln) oder Schweigen gilt üblicherweise aber nicht als Willenserklärung und kann deshalb grundsätzlich nicht als Einwilligung im Sinne von Artikel 4 Absatz 5 DSG verstanden werden.[123] Der Gesetzgeber geht davon aus, dass – als Ausfluss des Verhältnismässigkeitsgrundsatzes und des Grundsatzes von Treu und Glauben – die Zustimmung umso klarer zu erfolgen hat, je sensibler die fraglichen Personendaten sind.[124] Hinsichtlich

---

[109] Vgl. David Rosenthal, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 4 Abs. 5, Rz. 66.

[110] In diesem Sinne auch Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 99.

[111] In diesem Sinne auch Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 67.

[112] Vgl. Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 67 ff.; zum Informed Consent im Datenschutz auch Marc Langheinrich/Günter Karjoth, Einwilligung und ihre technische Umsetzung, digma 2009.4, S. 139 f.; grundsätzlich zur Aufklärungspflicht Claudia Fink, Aufklärungspflicht von Medizinalpersonen, Bern 2008.

[113] Vgl. z.B. Best Practices and Guidelines for Location-Based Services (Version 3.18.08), The Wireless Association (CTIA), S. 5, www.ctia.org/business_resources/wic/index.cfm/AID/11300 (Stand: 20.07.2010).

[114] Vgl. Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 70.

[115] Vgl. nachfolgend Ziffer 3.7.2.

[116] In diesem Sinne auch Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 113.

[117] Vgl. Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 104.

[118] Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210.

[119] Vgl. Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 93.

[120] In diesem Sinne auch Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 104.

[121] Vgl. Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 105 f.

[122] Vgl. Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003 (Botschaft Änderung DSG), BBl 2003 2101, S. 2127; vgl. auch Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 79.

[123] Auch Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 80, ist grundsätzlich dieser Auffassung; die von ihm angeführten Beispiele, in welchen auch Schweigen einer Einwilligung gleichkommt (Rz. 81), sind nach der hier vertretenen Auffassung nicht zutreffend; vgl. zur elektronischen Einwilligung Langheinrich/Karjoth (Fn. 112), S. 138 f.

[124] Vgl. Botschaft Änderung DSG, BBl 2003 2101, S. 2128, mit Hinweisen; vgl. auch Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 89.

der Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen muss deshalb die Einwilligung *ausdrücklich* erfolgen (Art. 4 Abs. 5, 2. Satz DSG).[125] Ausdrücklich muss der Inhalt der Willenserklärung (d.h. der erkennbare Willen, dass und in welcher Weise bestimmte Personendaten, die besonders schützenswert sind oder die zusammen ein Persönlichkeitsprofil ergeben, bearbeitet werden dürfen), nicht aber die Form der Willenserklärung sein.[126] Die sich bereits über eine kurze Zeitdauer in einem Location Sharing System ansammelnden Daten über den Standort eines bestimmten mobilen Geräts, das grundsätzlich einer Abonnentin bzw. einem Abonnenten des Services zugeordnet werden kann, und die damit verbundene Möglichkeit der Erstellung von Bewegungsbildern führen zusammen mit weiteren Zugangs- und Verbindungsdaten, den Daten über den Personenkreis, der berechtigt ist, die Standorte abzufragen, und den für die Abonnementsverwaltung erhobenen Stammdaten dazu, dass eine Zusammenstellung von Daten vorliegt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Mithin ist wohl davon auszugehen, dass es sich bei der Gesamtheit der in einem Location Sharing System bezüglich einer bestimmten Person verarbeiteten Daten um ein *Persönlichkeitsprofil* (Art. 3 Bst. d DSG) handelt, dies auch deshalb, weil dadurch ein Längsprofil (biografisches Bild) entstehen kann und solche Längsprofile aus datenschutzrechtlicher Sicht als besonders heikel beurteilt werden.[127] Mithin sollte von den Nutzerinnen und Nutzern eines Location Sharing Systems *immer eine ausdrückliche Einwilligung zur Datenbearbeitung* eingeholt werden. Grundsätzlich könnte eine solche Einwilligung auch in Allgemeinen Geschäftsbedingungen (AGB) oder einer allgemeinen Datenschutzerklärung vorgesehen sein, die mit der Abonnierung eines Location Sharing Services angenommen wird.[128] Aus Beweisgründen wird den Anbietern von Location Sharing Services allerdings empfohlen, eine ausdrückliche Einwilligungserklärung auf der Registrierungsseite aufzuschalten (am besten als PDF-File, das man auch ausdrucken kann), der die Nutzerinnen und Nutzer dann durch aktives Setzen eines Häkchens ins entsprechende Feld und durch Anklicken eines Buttons mit der Beschriftung «Ich habe die Einwilligungserklärung gelesen und stimme der Datenbearbeitung gemäss der Erklärung ausdrücklich zu» zustimmen müssen.[129] Auf diese Weise lässt sich über die Logfile-Daten das Vorliegen einer Einwilligung nachweisen.

[Rz 34] Location Sharing impliziert, dass die Daten nicht nur durch den Service-Anbieter bearbeitet, sondern auch an Dritte weitergegeben werden, denn die Information von Dritten über den eigenen Standort ist ja gerade der Zweck von solchen Systemen. Das Abrufen von Personendaten über das Internet stellt nach schweizerischer Rechtsauffassung immer eine Bekanntgabe von Daten (und damit eine Bearbeitung) dar.[130] Da auf das Internet weltweit zugegriffen werden kann, handelt es sich bei einem Internet-Abrufverfahren immer um eine *Bekanntgabe ins Ausland* im Sinne von Artikel 6 DSG, darunter auch in Staaten, in denen ein der Schweiz gleichwertiger Datenschutz fehlt.[131] Da die anderen gesetzlichen Gründe (Art. 6 Abs. 2 Bst. a sowie c – g DSG) für eine Bekanntgabe ins Ausland bei Location Sharing Systemen üblicherweise fehlen dürften, ist auch diesbezüglich eine Einwilligung der betroffenen Person (Art. 6 Abs. 2 Bst. b DSG) notwendig.

3.6 Datenschutzrechtlicher Rahmen für den Betrieb

[Rz 35] Wer in der Schweiz bzw. von der Schweiz aus ein Location Sharing System betreiben will, hat den vorstehend dargestellten datenschutzrechtlichen Gegebenheiten Rechnung zu tragen, dies insbesondere dadurch, dass bei den Nutzerinnen und Nutzern eine rechtsgenügende Einwilligung (informed consent) im beschriebenen Sinn[132] eingeholt wird.

[Rz 36] In der Fachwelt wird heute darüber hinausgehend diskutiert, dass den Nutzerinnen und Nutzern die Möglichkeit eingeräumt werden sollte, die *Bekanntgabe ihrer Standorte an Dritte einzuschränken*.[133] Als hinsichtlich des Persönlichkeitsschutzes wirksam werden insbesondere die folgenden Beschränkungen erachtet:[134]

- *Personenbezogene Beschränkungen:* Bei den personenbezogenen Beschränkungen stehen «schwarze Listen» (black lists), bei denen bestimmten anderen Nutzerinnen und Nutzern des Service der Zugang ausdrücklich verwehrt wird, sowie gruppenbezogene

[125] Vgl. Botschaft Änderung DSG, BBl 2003 2101, S. 2127; vgl. auch Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 83.

[126] Vgl. Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 83.

[127] Vgl. Belser (Fn. 56), Artikel 3, Rz. 21 f., unter Hinweis auf die Rechtsprechung der vormaligen Eidgenössischen Datenschutzkommission, VPB 65.48.

[128] Vgl. Rosenthal (Fn. 109), Art. 4 Abs. 5, Rz. 90; in der deutschen Praxis zum Datenschutzrecht muss eine vorformulierte Einwilligung allenfalls nicht einmal die Form einer Opt-in-Klausel haben, oft genügt die Form einer Opt-out-Klausel, vgl. Haug (Fn. 67), Rz. 107; kritisch zu Einwilligungsklauseln in AGB Weber (Fn. 10), S. 457 f.

[129] Vgl. dazu auch Langheinrich/Karjoth (Fn. 112), S. 138 f.

[130] Vgl. Belser (Fn. 56), Artikel 3, Rz. 21 f., unter Hinweis auf die Rechtsprechung der vormaligen Eidgenössischen Datenschutzkommission, VPB 68.92.

[131] Vgl. Urs Maurer-Lambrou/Andrea Steiner, Basler Kommentar zum DSG, Artikel 6, Rz. 15, mit Hinweis auf VPB 68.92; David Rosenthal, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 6, Rz. 4.

[132] Vgl. vorstehend Ziffer 3.5.

[133] Vgl. Tsai et al. (Fn. 4), S. 20.

[134] Vgl. Tsai et al. (Fn. 4), S. 19 f.; Michael Benisch et al., The Impact of Expressiveness on the Effectiveness of Privacy Mechanisms for Location Sharing, Carnegie Mellon University, CMU-ISR-08-141, Dezember 2008, 12, www.normsadeh.com/file_download/111/CMU-ISR-08-141R.pdf.

Zugangsregeln (group-based rules, closed user groups), die nur einer definierten Nutzergruppe den Zugang ermöglichen, im Vordergrund.

- *Ortsbezogene Beschränkungen:* Mit ortsbezogenen Beschränkungen wird der Nutzerin bzw. dem Nutzer ermöglicht, die Übermittlung des Standorts jeweils automatisch zu unterdrücken, wenn sie oder er sich an einem vorbestimmten Standort bzw. in dessen Umgebung (z.B. in und in der Nähe der Wohnung) befindet. Diese Funktion hilft beispielsweise bei der Prävention von Stalking.[135]
- *Zeitbezogene Beschränkungen:* Mit zeitbezogenen Beschränkungen kann der Zugriff auf den Standort auf bestimmte Tageszeiten bzw. Zeiten in der Woche eingeschränkt oder zu diesen Zeiten untersagt werden. Ebenfalls zeitbezogen sind Funktionen, die den Zugriff auf die Daten des Standorts während einer vorbestimmten Zeit (z.B. während der nächsten drei Tage, an welchen sich die Person auf einer Bergwanderung befindet) einschränkt.

[Rz 37] Angesichts des gemäss ausländischen Studien zu beobachtenden steigenden Datenschutzbedürfnisses von Nutzerinnen und Nutzern von Location Sharing Services[136] sollte ein datenschutzkonformes schweizerisches Location Sharing System die Kombination der drei dargestellten Arten von Beschränkungen des Zugangs durch die betroffene Person ermöglichen. Das sich in Anwendung befindende Angebot von Loccacino[137] erlaubt diese Kombination[138] und beweist damit, dass solche Beschränkungen technisch ohne weiteres machbar sind. Ebenfalls ziemlich ausgebaute (aber weniger differenzierte) Beschränkungsmöglichkeiten sieht Google Latitude[139] vor.

[Rz 38] Wenn eine Nutzerin oder ein Nutzer einer Drittperson im System ausdrücklich den Zugriff auf die Daten ihres bzw. seines Standorts ermöglicht, so stellt diese Information *Personendaten bezogen auf die Drittperson* dar (ähnlich wie wenn eine Person auf ihrer Seite in einem sozialen Internet-Netzwerk eine andere Person als ihren «Freund» bezeichnet). Die betroffene Drittperson könnte diesen Bezug zur Nutzerin bzw. zum Nutzer nicht wollen und sollte deshalb – sofern mit der Teilnahme im Location Sharing System nicht auch bereits die implizite Zustimmung erteilt wurde, Informationsempfänger zu sein und bestimmten Nutzergruppen gegen eigenen Willen zugeteilt zu werden – über die eingeräumten Abfragerechte informiert werden und die Möglichkeit haben, die erhaltenen Zugangsrechte abzulehnen. Das Interesse an Letzterem kann aus anderen als datenschutzrechtlichen Gründen bestehen. So könnte eine Person, der Zugriffsrechte eingeräumt wurden, aus diesen Rechten eine Garantenpflicht zur Beobachtung der Standorte erwachsen, was allenfalls zu unerwünschten Haftungsfragen führen kann.

[Rz 39] Anbieter von Location Sharing Systemen, die dem schweizerischen Datenschutzrecht unterstehen, müssen weiter ihre Datensammlung beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) *anmelden* (Art. 1a Abs. 3 DSG), da es sich um Persönlichkeitsprofile handelt[140] und die Daten regelmässig bekannt gegeben werden. Dieser Pflicht können sich die Anbieter dadurch entledigen, dass sie entweder über eine *datenschutzverantwortliche Person* verfügen, welche mit der nötigen Unabhängigkeit die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt (Art. 11a Abs. 5 Bst. e DSG)[141], oder dass sie aufgrund eines *Zertifizierungsverfahrens* nach Artikel 11 ein Datenschutz-Qualitätszeichen erworben haben und dass das Ergebnis der Bewertung dem Beauftragten mitgeteilt wurde (Art. 11a As. 5 Bst. f DSG)[142].

[Rz 40] Wenn der Schweizer Anbieter eines Location Sharing Services hinsichtlich der Datenbearbeitung *mit einer Unternehmung im Ausland zusammenarbeitet* bzw. einer solchen allenfalls die Datenbearbeitung (z.B. das Hosting) überträgt (IT-Outsourcing), dann stellt dies ebenfalls eine grenzüberschreitende Bekanntgabe von Personendaten (Art. 6 DSG) dar.[143] Dieser Fall ist klar zu unterscheiden von der grenzüberschreitenden Bekanntgabe bei der Abfrage der Lokalisation durch die Nutzerinnen und Nutzer selbst.[144] Der Vorgang des Datenabrufs durch die Nutzerinnen und Nutzer selbst oder durch von diesen autorisierten Personen von einem Gerät im Ausland ist ein Vorgang, der genügend konkret und abgegrenzt ist, damit bezogen auf alle künftigen Abfragen noch eine Einwilligung «im Einzelfall» (Art. 6 Abs. 2 Bst. b DSG) zulässig ist.[145] Demgegenüber kann zu einer generellen Übertragung der Datenbearbeitung an einen Betrieb im Ausland und der damit verbundenen grenzüberschreitenden Bekanntgabe keine gültige Einwilligung erteilt werden.[146] Somit kann die Datenbearbeitung nur dann problemlos an eine Unternehmung im Ausland übertragen werden, wenn sich

[135] Vgl. Tsai et al. (Fn. 4), S. 19.

[136] Vgl. Benisch et al. (Fn. 134), S. 16.

[137] www.loccaccino.com (Stand: 20.07.2010).

[138] Vgl. Tsai et al. (Fn. 4), S. 20.

[139] www.google.com/intl/en_us/mobile/latitude/ (Stand: 20.07.2010); dafür stellt sich bei dieser Anwendung das Problem der kommerziellen Datenauswertung durch Google (Google Analytics), Vgl. Weber (Fn. 10), S. 473 f. sowie Sven Thomsen/Markus Hansen/Marit Hansen, Verwischte Sicht auf Datenbearbeitung, digma 2009.3, S. 94 ff.

[140] Vgl. vorstehend Ziffer 3.5, Rz 33.

[141] Ausführlich dazu die Website des EDÖB: www.edoeb.admin.ch/themen/00794/01609/01611/index.html?lang=de (Stand: 20.07.2010).

[142] Zur Datenschutzzertifizierung Caroline Gloor Scheidegger/Karin Koç, Datenschutzzertifizierung: Stand der Dinge, digma 2010.2, S. 74 f.

[143] Vgl. Rosenthal (Fn. 131), Art. 6, Rz. 7.

[144] Vgl. vorstehend Ziffer 3.5, in fine.

[145] Der Gesetzgeber wollte die Einwilligung im Einzelfall weit fassen, vgl. Rosenthal (Fn. 131), Art. 6, Rz. 53, mit Hinweisen.

[146] Vgl. Rosenthal (Fn. 131), Art. 6, Rz. 53.

diese in einem Staat befindet, dessen Datenschutzrecht den Anforderungen von Artikel 6 Absatz 1 DSG entspricht. Darüber, ob dies voraussichtlich der Fall ist, gibt eine Liste des EDÖB Auskunft.[147] Bei einer Zusammenarbeit mit Unternehmen mit Standorten in nichtsicheren Staaten, muss der angemessene Datenschutz vertraglich gesichert werden (Art. 6 Abs. 2 Bst. a DSG).[148] Der EDÖB stellt hierfür einen Mustervertrag zur Verfügung.[149] Darüber hinaus ist der EDÖB über die Verträge zu informieren (Art. 6 Abs. 3 DSG).[150]

[Rz 41] Besonders zu beachten ist die Frage einer Zusammenarbeit mit *Unternehmen in den USA*. Da die Gesetzgebung der USA aus Sicht der Schweiz keinen angemessenen Datenschutz gewährleistet, mussten bis vor kurzem Unternehmen in der Schweiz mit ihren Partnern in den USA einen Vertrag abschliessen (Art. 6 Abs. 2 bst. a DSG), der einen angemessenen Datenschutz gewährleistet, und diesen dem EDÖB zur Prüfung vorlegen. Im Rahmen des Kooperationsforums Schweiz-USA für Handel und Investitionen wurde am 9. Dezember 2008 vom EDÖB ein Briefwechsel zur Schaffung eines «U.S.-Swiss *Safe Harbor Framework*» unterzeichnet. Dieses bilaterale Datenschutzrahmenwerk vereinfacht die Übermittlung von personenbezogenen Daten von Unternehmen in der Schweiz zu Unternehmen in den USA.[151] Gestützt auf dieses Abkommen können sich U.S. Unternehmen beim Handelsministerium der USA zur Einhaltung der im «U.S.-Swiss Safe Harbor Framework» festgehaltenen Datenschutzgrundsätze verpflichten und sich zertifizieren. Für Unternehmen in der Schweiz hat dies den Vorteil, dass sie mit zertifizierten Unternehmen in den USA weder einen Vertrag aushandeln (Art. 6 Abs. 2 Bst. a DSG), noch den EDÖB informieren müssen (Art. 6 Abs. 3 DSG), weil hinsichtlich dieser Unternehmen von einem angemessenen Datenschutz (Art. 6 Abs. 1 DSG) ausgegangen wird.

3.7 Datenschutzrechtlicher Rahmen für die Benutzung

3.7.1 Allgemeines

[Rz 42] In Location Sharing Systemen werden Daten über den Standort von Endgeräten und damit mutmasslich auch über den Standort der entsprechenden registrierten Nutzerinnen und Nutzer des Systems ausgetauscht. Hinsichtlich der eigenen Daten ist eine bestimmte Nutzerin bzw. ein bestimmter Nutzer des Systems primär Subjekt bzw. Nutzniesser des Datenschutzes. Hinsichtlich des gegenseitigen Austausches von Daten erwachsen jeder Nutzerin bzw. jedem Nutzer eines Location Sharing Systems auch Pflichten. Wenn ein Location Sharing System es ermöglicht, den Zugriff auf bzw. die Bekanntgabe von Daten über den Standort auf bestimmte Personen oder Personengruppen zu beschränken, und jemand von dieser Beschränkungsmöglichkeit Gebrauch macht, dann muss davon ausgegangen werden, dass diese Person damit gleichzeitig den Willen geäussert hat, dass keine Bekanntgabe der Daten des Standorts an Dritte ausserhalb des bezeichneten Nutzerkreises erfolgen soll. Wer somit Zugriff auf solche Daten über den Standort einer Person hat und diese ohne ausdrückliche Ermächtigung dieser Person bzw. ausserhalb von Notfallsituationen weitergibt (an aussenstehende Dritte bekannt gibt), begeht eine Persönlichkeitsverletzung (Art. 12 DSG) und muss allenfalls die Rechtsfolgen tragen.

[Rz 43] Heute besteht bereits ein erhebliches Angebot von Anwendungen und Services im Internet, mit welchen der Datenaustausch mit und die Standorte von Mobiltelefonen (mobilen Endgeräten) ausspioniert werden kann.[152] Wer einen derartigen Dienst auf einem fremden Endgerät ohne die Einwilligung der Eigentümerin bzw. des Eigentümers abonniert oder ohne die entsprechende Einwilligung heimlich Software installiert, erfüllt allenfalls den objektiven und subjektiven Tatbestand des unbefugten Eindringens in ein Datenverarbeitungssystem (Art. 143bis StGB[153]). Das Bundesgericht hat in seiner Rechtsprechung festgehalten, dass die heutigen Mobiltelefone bzw. Mobiltelefonsysteme als Datenverarbeitungsanlage im Sinne der Strafgesetzgebung zu gelten haben.[154] Wer zudem die Daten über die Standorte der betroffenen Personen auswertet, erfüllt auch den objektiven Straftatbestand des unbefugten Beschaffens von Personendaten (Art. 179novies StGB), da es sich bei einer Ansammlung von Daten über den Standort einer Person sehr rasch einmal um ein Persönlichkeitsprofil handelt.

3.7.2 Besondere Fragen im familienrechtlichen Kontext

[Rz 44] Die heute angebotenen Location Sharing Services eignen sich teilweise zur *Überwachung der Standorte von Kindern* und werden damit auch beworben. Untersuchungen aus dem anglo-amerikanischen Raum zeigen auf, dass Befragte mit eigenen Kindern gerade darin den hauptsächlichen Nutzen von Location Sharing Systemen sehen.[155] In diesem

[147] Siehe unter www.edoeb.admin.ch/themen/00794/00827/index.html?lang=de (Stand: 20.07.2010); nach Rosenthal (Fn. 131), Art. 6, Rz. 30, stellt die entsprechende Bezeichnung des Staates auf der Liste allerdings nur eine Vermutung dar, dass ein angemessener Schutz besteht.

[148] Vgl. auch Rosenthal (Fn. 131), Art. 6, Rz. 38 ff.

[149] Mustervertrag für das Outsourcing von Datenbearbeitungen ins Ausland, www.edoeb.admin.ch/dienstleistungen/00587/00966/00968/index.html?lang=de (Stand: 20.07.2010).

[150] Ausführlich dazu Rosenthal (Fn. 131), Art. 6, Rz. 88.

[151] Vgl. Jürg Schneider, Personendaten-Transfer in die USA, digma 2009.3, S. 126 f.; vgl. auch Medienmitteilung vom 9. Dezember 2008, www.news.admin.ch/message/index.html?lang=de&msg-id=23809 (Stand: 20.07.2010).

[152] Siehe statt vieler z.B. die Angebote bei www.flexispy.com/de/ oder www.catchmee.com/deutsch_3_58_58.html (Stand: 20.07.2010).

[153] Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 310.

[154] Vgl. BGE 129 IV 315, E. 2.2.3, S. 320 ff.

[155] Vgl. Tsai et al. (Fn. 4), S. 16 und 18.

Zusammenhang stellen sich heikle Fragen des *innerfamiliären Persönlichkeitsschutzes*.[156]

[Rz 45] Informationelle Privatheit[157] dient jeder Person zum Schutz von Identität und Gefühlswelt, dem Schutz der Menschenwürde und ist für das menschliche Dasein existenziell.[158] Es geht u.a. darum, einen autonomen Bereich der Lebens- und Beziehungsgestaltung zu schützen, in dem die einzelne Person ihre Individualität entwickeln, entfalten und erhalten kann. Zu den wesentlichen Bereichen der von Artikel 27 ff. ZGB geschützten Persönlichkeit gehört mithin die Freiheit der persönlichen Lebensgestaltung, welche durch Fremdbeobachtung wesentlich beeinträchtigt wird.[159] Ebenfalls zu schützen ist die Möglichkeit jeder Person, ihre sozialen Bindungen (insbesondere auch Freundschafts- und Intimbeziehungen) autonom zu gestalten.[160] Die autonome Lebens- und Beziehungsgestaltung wird bei unmündigen Kindern und Jugendlichen durch die elterliche Sorge von Gesetzes wegen eingeschränkt. So darf das Kind namentlich ohne Einwilligung der Eltern die häusliche Gemeinschaft nicht verlassen und es darf ihnen auch nicht widerrechtlich entzogen werden (Art. 301 Abs. 3 ZGB). Dies schliesst mit ein, dass die Eltern grundsätzlich über den Aufenthalt ihres Kindes bestimmen dürfen und damit auch ein berechtigtes Interesse haben, zu wissen, wo sich ihr Kind aufhält.[161] Die Eltern müssen sich allerdings – ebenfalls von Gesetzes wegen – bei der Erziehung ihres Kinds und bei allen Entscheiden, die sie mit Bezug auf dieses treffen, vom Kindeswohl leiten lassen (Art. 301 Abs. 1 ZGB) – ihre elterliche Sorge endet dort, wo das Kindeswohl verletzt wird.[162] Zudem müssen die Eltern dem Kind die seiner Reife entsprechende Freiheit der Lebensgestaltung gewähren und müssen in wichtigen Angelegenheiten, soweit tunlich, auf die Meinung des Kinds Rücksicht nehmen (Art. 301 Abs. 2 ZGB). Letzteres gilt auch für die dem Kind ausserhalb des elterlichen Haushalts zu gewährende Bewegungs- und Kontaktfreiheit ohne Beobachtung.

[Rz 46] Hinsichtlich der für die Abonnierung bzw. Nutzung eines Location Sharing Services notwendigen Einwilligung[163] sind die Eltern bzw. die gesetzlichen Vertreter grundsätzlich in Anwendung von Artikel 304 Absatz 1 ZGB befugt, das Kind zu vertreten, d.h. an dessen Stelle die notwendige Einwilligung vorzunehmen, allerdings nur so weit, wie dies im Interesse des Kindes ist[164], d.h. für dieses aus objektiver Sicht nutzbringend ist und den Interessen der betroffenen Person nicht zuwiderläuft[165]. Weil die Einwilligung zu einer Persönlichkeitsverletzung ein höchstpersönliches Recht ist und für die gültige Einwilligung damit die Urteilsfähigkeit des Kindes unabhängig von dessen Mündigkeit genügt (Art. 19 Abs. 2 ZGB), ist die gesetzliche Vertretung nur so weit bzw. so lange zulässig, als die betroffene Person *habituell urteilsunfähig* ist.[166] Gesetzliche Vertreterinnen und Vertreter dürfen deshalb nicht für urteilsfähige Unmündige oder Entmündigte vertretungsweise eine Einwilligung in eine Persönlichkeitsverletzung abgeben.[167] Letztlich sind Fälle denkbar, wo der Reifegrad eines Kindes zwar nicht der Urteilsfähigkeit zur Einwilligung in eine Persönlichkeitsverletzung, aber der Urteilfähigkeit zur Verweigerung des Eingriffs entspricht; in diesen Fällen geht die Verweigerung der betroffenen Person der Einwilligung der gesetzlichen Vertretung in der Regel vor.[168]

[Rz 47] Bei Kindern muss spätestens ab einem Alter von 14 Jahren davon ausgegangen werden, dass sie zu ihrer notwendigen, altersgemässen, physisch und psychisch gesunden Entwicklung auf ein zunehmend erhöhtes Mass an Freiheit in ihrer Lebensgestaltung und ihrer Beziehungspflege angewiesen sind. Spätestens ab diesem Alter dürfen daher nach der hier vertretenen Auffassung die Eltern bzw. die gesetzlichen Vertreter weder stellvertretend für die unmündigen Kinder die Einwilligung zur Nutzung eines Location Sharing Systems (und damit wohl immer implizit zum Zugriff auf die Daten der aktuellen Standorte) geben noch das Kind gegen seinen Willen dazu zwingen, ihnen Zugriff auf die Standorte in einem von diesem abonnierten bzw. genutzten Location Sharing System zu bewilligen.

[Rz 48] Wenn Eltern ohne die entsprechende Einwilligung des Kinds auf einem Endgerät, das in dessen Eigentum steht, heimlich Software installieren, erfüllt dies in der Regel den objektiven und subjektiven Tatbestand des unbefugten Eindringens in ein Datenverarbeitungssystem (Art. 143bis StGB).

[Rz 49] Letztlich gilt es zu beachten, dass bei Kindern und Jugendlichen, welche eine Berufslehre absolvieren, die Bekanntgabe von Daten über deren Standort an die Eltern (auch die allenfalls einvernehmliche Bekanntgabe) während

---

[156] Die von Regina E. Aebi-Müller, Personenbezogene Information im System des zivilrechtlichen Persönlichkeitsschutzes, Bern 2005, S. 363 f. aufgezeigte und als bedenklich bezeichnete Entwicklung nimmt somit ihren Fortgang.

[157] Die herrschende Lehre geht noch von der *Sphärentheorie* (Intimsphäre, Privatspäre, Gemeinsphäre) aus, vgl. Raphaël Haas, Die Einwilligung in Persönlichkeitsverletzung nach Art. 28 Abs. 2 ZGB, Zürich 2007, S. 12 ff., welche aber gemäss neuerer Lehrmeinungen nur schlecht auszudrücken vermag, worum es beim Recht auf Privatheit geht (vgl. Aebi-Müller [Fn. 156], S. 621; Haas, S. 13 f.); vorliegend wird deshalb von der von Aebi-Müller (Fn. 156), S. 303 ff. entwickelten Konzeption des *Schutzes der informationellen Privatheit* ausgegangen.

[158] Vgl. Aebi-Müller (Fn. 156), Rz. 650.

[159] In diesem Sinne Aebi-Müller (Fn. 156), Rz. 652 und 654.

[160] In diesem Sinne Aebi-Müller (Fn. 156), Rz. 665.

[161] Ein Bedürfnis nach Beaufsichtigung ergibt sich auch aus Artikel 333 Absatz 1 ZGB.

[162] In diesem Sinne auch Haas (Fn. 157), S. 116.

[163] Vgl. vorstehend Ziffer 3.5.

[164] Vgl. Aebi-Müller (Fn. 156), Rz. 235; Haas (Fn. 157), S. 116.

[165] Vgl. Aebi-Müller (Fn. 156), Rz. 240.

[166] Vgl. Aebi-Müller (Fn. 156), Rz. 239; Haas (Fn. 157), S. 114 f.

[167] Vgl. Haas (Fn. 157), S. 104.

[168] Vgl. Haas (Fn. 157), S. 115.

der Arbeitszeit das Fabrikations- und Geschäftsgeheimnis des Lehrbetriebes verletzen kann.

3.7.3 Besondere Fragen im arbeitsrechtlichen Kontext

[Rz 50] Artikel 328 des Obligationenrechts (OR)[169] verpflichtet die Arbeitgeberin bzw. den Arbeitgeber privatrechtlich, die Persönlichkeit der Arbeitnehmerinnen und Arbeitnehmer zu achten und zu schützen; dies betrifft insbesondere auch die Zulässigkeit von Überwachungsmassnahmen am Arbeitsplatz[170]. Zudem regelt im öffentlichen Arbeitsrecht Artikel 26 der Verordnung 3 zum Arbeitsgesetz (ArGV 3)[171] die Überwachung am Arbeitsplatz. Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, dürfen demnach nicht eingesetzt werden (Art. 26 Abs. 1 ArGV 3). Sind Überwachungs- oder Kontrollsysteme aus andern Gründen erforderlich, sind sie so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmerinnen bzw. Arbeitnehmer dadurch nicht beeinträchtigt werden (Art. 26 Abs. 2 ArGV 3). Das Bundesgericht hat diesbezüglich entschieden, dass der Einsatz von Lokalisierungssystemen zur Überwachung von Aussendienstmitarbeitenden dann zulässig ist, wenn diese zur Sicherheit der Arbeitnehmenden oder zu organisatorischen Zwecken, d.h. beispielsweise einem effizienteren Einsatz, dienen.[172] Der Einsatz von Lokalisierungssystemen zur Überwachung der Mitarbeitenden ist demgegenüber verboten.[173]

[Rz 51] Der Einsatz von Lokalisierungssystemen zur Überwachung von Mitarbeitenden im öffentlichen Dienst bedarf zudem einer ausdrücklichen Grundlage in einem Rechtserlass, in der Regel wohl auf Gesetzesstufe (Art. 5 Abs. 1 BV).

3.8 «Data Security Breaches» bei Location Sharing Systemen

[Rz 52] Angesichts der Mobilität der Nutzerinnen und Nutzer sowie zugriffsberechtigter Dritter besteht bei Location Sharing Systemen eine erhöhte Wahrscheinlichkeit, dass es zu unrechtmässigen Zugriffen oder zur unrechtmässigen Bekanntgabe (Art. 3 Bst. f DSG; Bekanntgabe: zugänglich machen, Einsicht gewähren, weitergeben, veröffentlichen) von Personendaten – so genannten «Data Security Breaches»[174] – kommt, insbesondere bezüglich der Standorte von Personen. Solche Standortdaten können in der Zeitreihe Bewegungsbilder von Personen und damit Persönlichkeitsprofile (Art. 3 Bst. d DSG) darstellen. Selbst bei nur kurzfristigen unrechtmässigen Zugriffen erhalten aber Dritte Kenntnis gegen den Willen der betroffenen Person vom deren aktuellem Standort. Dies ermöglicht unberechtigten Dritten, die Person allenfalls örtlich aufzuspüren und physisch zu beeinträchtigen. Ein «Data Security Breach» kann bei Loccation Sharing Systemen somit für die betroffenen Nutzerinnen und Nutzer im Einzelfall ein hohes Gefährdungspotenzial aufweisen. In Extremfällen führt ein «Data Security Breach» zu Stalking, häuslicher Gewalt oder Ehrenmord.

[Rz 53] Anders als das Recht in Deutschland[175] oder in den USA[176] sieht das schweizerische Datenschutzrecht eine Informationspflicht bei «Data Security Breaches» nicht explizit vor.[177] Die neuere Lehre geht aber davon aus, dass sich eine solche Informationspflicht aus dem Grundsatz ergeben kann, dass die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen hat (Art. 4 Abs. 2 DSG).[178] Dieser Auffassung ist zuzustimmen. Weiter wird etwa die Auffassung vertreten, eine Informationspflicht könne sich in bestimmten Fällen auch als Massnahme der Datensicherheit (Art. 7 Abs. 1 DSG) zwingend ergeben.[179] Jedenfalls kann eine Nichtinformation in Fällen eines «Data Security Breach» Haftungsfolgen haben, wenn eine Person (in adäquater Kausalität) als Folge des «Data Security Breach» *und* der anschliessenden Nichtinformation zu Schaden kommt.[180]

[Rz 54] Betreibern von Location Sharing Systemen in der Schweiz muss deshalb empfohlen werden, in ihrem System eine Funktionalität einzubauen, welche es ermöglicht, die Nutzerinnen und Nutzer des Services im Falle eines «Data Security Breach» in adäquater Weise zu informieren (d.h. wohl auf das mobile Endgerät).

---

[169] Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht), SR 220.

[170] Vgl. Rolf A. Tobler et al., Arbeitsrecht, Kommentierte Gesetzesausgabe, Lausanne 2006, Artikel 328, Rz. 1.8.

[171] Verordnung 3 vom 18. August 1993 zum Arbeitsgesetz (Gesundheitsvorsorge, ArGV 3), SR 822.113.

[172] Vgl. BGE 130 II 425, E. 4.; für das deutsche Arbeitsrecht vgl. Peter Gola, Datenschutz und Multimedia am Arbeitsplatz, 3. Aufl., Frechen 2010, S. 30 ff, insbesondere Rz. 91.

[173] Vgl. BGE 130 II 425, E. 4.4.; für Deutschland vgl. Gola (Fn. 172), S. 32 f., Rz. 92 f.

[174] Ausführlich Matthias Ebneter, Informationspflichten im Zusammenhang mit «Data Security Breaches», Jusletter vom 7. Juni 2010; vgl. auch Jürgen Bonfert, Sicherheit auf mobilen Endgeräten, digma 2007.1, S. 16 ff.; nach einer Schätzung der US Federal Trade Commission (FTC) aus dem Jahr 2010 sind 5 bis 10 Mio. Amerikaner jährlich Opfer von Datendiebstahl, www.ftc.gov/opa/2003/09/idtheft.shtm (UStand: 24.07.2010).

[175] Vgl. Ebneter (Fn. 174), Rz. 6 ff.

[176] Vgl. Ebneter (Fn. 174), Rz. 4 f.

[177] Vgl. Ebneter (Fn. 174), Rz. 11.

[178] Vgl. David Rosenthal, in: David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 4, Rz. 16; Ebneter (Fn. 174), Rz. 16.

[179] Vgl. Rosenthal (Fn. 178), Rz. 16; Ebneter (Fn. 174), Rz. 12 f.

[180] In diesem Sinne Ebneter (Fn. 174), Rz. 13 ff.

4. Voraussetzungen für den Betrieb in der Schweiz

4.1 Betrieb durch Private

[Rz 55] Die Voraussetzung für den Betrieb eines Location Sharing Systems in der Schweiz bzw. von der Schweiz aus besteht primär in der Einhaltung der datenschutzrechtlichen Rahmenbedingungen[181] bzw. in der Gewährleistung des Fernmeldegeheimnisses. Mit der *Einholung einer ausdrücklichen Einwilligung der Nutzerin bzw. des Nutzers* des Location Sharing Systems über alle wesentlichen Formen der Bearbeitung der personenbezogenen Daten (informed consent)[182] einerseits und der Ermöglichung eines selektiven Zugriffs auf die standortbezogenen Daten einer Nutzerin bzw. eines Nutzers andererseits kann den datenschutzrechtlichen Rahmenbedingungen weitestgehend Rechnung getragen werden. Allenfalls sollte die Einwilligung auch die Bearbeitung im Ausland umfassen. Wer ein Location Sharing System betreibt, tut zudem gut daran, bei den Einwilligungen auch den besonderen familienrechtlichen[183] und arbeitsrechtlichen[184] Kontext zu berücksichtigen. Weiter sind allenfalls zusätzlich die datenschutzrechtlichen Vorschriften für den *grenzüberschreitenden Datenaustausch* (Art. 6 DSG) zu beachten.[185]

[Rz 56] Es stellt sich weiter die Frage, ob ein Location Sharing System für sich alleine einen meldepflichtigen Fernmeldedienst (Art. 4 FMG) darstellt. Der Begriff des Fernmeldedienstes (Art. 3 Bst. b FMG) umfasst nur die eigentliche Datenübertragung. Er ist identisch mit dem im europäischen Recht verankerten Begriff des elektronischen Kommunikationsdienstes.[186] Dieser Begriff umfasst ganz eng nur die «gewöhnlich gegen Entgelt erbrachten Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschliesslich Telekommunikations- und Übertragungsdienste in Rundfunknetzen»[187], ausdrücklich nicht aber die so genannten Dienste der Kommunikationsgesellschaft[188]. Zu den Letzteren zählt das Gros der Dienste im Internet (Online-Dienste). Mithin fallen die Location Sharing Services als solche nicht unter den Begriff der Fernmeldedienste und sind *nicht meldepflichtig*.

[Rz 57] Soweit für die Darstellung der Standorte in einem Darstellungsdienst als Georeferenzdaten bzw. Kartenhintergrund *Geobasisdaten des Bundesrechts* verwendet werden, muss die Betreiberin bzw. der Betreiber des Location Sharing Systems auch über die entsprechenden Einwilligungen der zuständigen Stelle zur gewerblichen Nutzung der Geodaten (Art. 25 Abs. 2 GeoIV) verfügen und die entsprechenden Quellenangaben (Art. 30 GeoIV) anbringen.

4.2 Betrieb durch Stellen der öffentlichen Verwaltung

[Rz 58] Soweit Stellen der öffentlichen Verwaltung (Bund, Kantone, Gemeinden etc.) ein Location Sharing System zur Erfüllung einer öffentlichen (allenfalls sogar hoheitlichen) Aufgabe (z.B. Überwachung von polizeilichen Wegweisungen, elektronische Fussfesseln) oder zur Überwachung des Personals im öffentlichen Dienst (z.B. Personal der Forstdienste zu allfälligen Rettungszwecken im Wald) betreiben wollen, ist – *zusätzlich zu den für private Betreiber bestehenden Voraussetzungen* – eine genügende gesetzliche Grundlage notwendig (Art. 5 Abs. 1 BV).

[Rz 59] Ob Stellen der öffentlichen Verwaltung über den Bereich der eigentlichen öffentlichen Aufgaben hinaus in Konkurrenz zu Privaten Location Sharing Systeme anbieten dürfen, bestimmt das jeweils anwendbare Verfassungs- und Gesetzesrecht hinsichtlich der privatwirtschaftlichen (gewerblichen) Tätigkeit des Staates. Für die Bundesverwaltung gilt als Voraussetzung, dass dazu eine gesetzliche Ermächtigung besteht (Art. 41 FHG[189]). Eine solche Ermächtigung besteht heute in einem beschränkten Umfang bereits für das Bundesamt für Landestopografie. Der Bundesrat kann Stellen der Bundesverwaltung ermächtigen, zur Erfüllung besonderer Kundenwünsche Geodaten und weitere Leistungen im Bereich der Geoinformation gewerblich anzubieten (Art. 19 Abs. 1 GeoIG). Dies hat der Bundesrat in der Landesvermessungsverordnung (LVV)[190] hinsichtlich der gewerblichen Leistungen der Landesvermessung getan (Art. 24 LVV). Allerdings besteht eine genügende Rechtsgrundlage nur im Umfang der in der Verordnung umschriebenen Tätigkeitsbereiche. Dazu gehört auch, Daten und Leistungen der Landesvermessung in einer besonderen Form anzubieten (Art. 24 Abs. 1 Bst. c LVV) und im Bereich der Geomatik und Kartografie Aufträge von anderen Stellen der Bundesverwaltung und von Dritten auszuführen (Art. 24 Abs. 1 Bst. a LVV). Das Bundesamt für Landestopografie kann somit legal von sich aus Location Sharing Systeme anbieten oder solche – massgeschneidert

[181] Vgl. vorstehend Ziffer 3.

[182] Vgl. vorstehend Ziffer 3.5.

[183] Vgl. vorstehend Ziffer 3.7.2.

[184] Vgl. vorstehend Ziffer 3.7.3.

[185] Vgl. vorstehend Ziffer 3.6.

[186] Vgl. Botschaft Änderung FMG, BBl 2003 7951, S. 7967.

[187] Artikel 1 Ziffer 1 der Richtlinie 2002/77/EG der Kommission vom 16. September 2002 über den Wettbewerb auf den Märkten für elektronische Kommunikationsnetze und -dienste, ABl Nr. L 249 vom 17. September 2002.

[188] «Jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung», vgl. Artikel 1 Ziffer 2 der Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG.

[189] Bundesgesetz vom 7. Oktober 2005 über den eidgenössischen Finanzhaushalt (Finanzhaushaltgesetz, FHG), SR 611.0.

[190] Verordnung vom 21. Mai 2008 über die Landesvermessung (Landesvermessungsverordnung, LVV), SR 510.626.

für bestimmte Kundenbedürfnisse – Dritten im Auftrag anbieten. Für andere Bundesämter besteht zurzeit keine entsprechende Rechtsgrundlage.

5. Betreiber im Ausland

[Rz 60] Wenn sich Personen und die ihnen gehörenden Endgeräte im Hoheitsgebiet der Schweiz befinden, gilt für die Nutzung der schweizerischen Fernmeldenetze und hinsichtlich des Personendatenschutzes uneingeschränkt das schweizerische Landesrecht, unabhängig davon, ob die Personen Kundinnen bzw. Kunden ausländischer Mobiltelefonanbieter sind und Location Sharing Systeme ausländischer Dienstleister nutzen, welche auf Servern im Ausland betrieben werden. Hinsichtlich der Verwendung von Standortdaten aus dem schweizerischen Fernmeldenetz (d.h. von Fernmeldeeinrichtungen in der Schweiz) gilt somit die Beschränkung gemäss Artikel 45b FMG. Solange sich diese Personen in der Schweiz aufhalten, dürfen die Daten über ihre Standorte – soweit sie nicht ausschliesslich mit GPS-Technologie ermittelt wurden – in irgendeinem Location Sharing System auf der Welt nur dann bearbeitet und bekannt gegeben werden, wenn eine Einwilligung vorliegt, die den Anforderungen des schweizerischen Rechts genügt[191]. Ausländische Anbieter von Location Sharing Systemen riskieren allenfalls, wegen Verletzung des schweizerischen Fernmeldegeheimnisses belangt zu werden – nicht primär strafrechtlich, aber ggf. in einem Haftungsfall, wenn durch die Verletzung des schweizerischen Rechts ein Schaden entsteht.

6. Schluss: «Cyber-Location» als neue Herausforderung für den Persönlichkeitsschutz

[Rz 61] Der Nutzen von Location Sharing Systemen ist heute – insbesondere wegen der Beschränkung auf den Freizeit- und Familienbereich – im Vergleich zum technischen Potenzial eher beschränkt. Künftig sind sowohl für die öffentliche Verwaltung wie für den privaten Gebrauch zahlreiche nutzbringende und allenfalls auch kommerziell interessante Anwendungen denkbar. Der Raumbezug von Endgeräten und damit der *voraussichtliche Standort von Personen aus einer bestimmten Zielgruppe* ist ökonomisch interessant – so interessant, dass das Unternehmen Google zur Gewinnung entsprechender Information auch Verletzungen des Datenschutzrechts auf sich nimmt[192], was zuerst in Europa[193] und nun auch in den USA[194] zur Kritik von Seiten von Datenschutzaufsichtsbehörden führte, und dass das Unternehmen Apple über das iPhone ebenfalls problematische Formen der Datengewinnung vornimmt[195]. Das Interesse am Raumbezug von Endgeräten und damit die Anwendungen von standortbezogenen kommerziellen Diensten und Location Sharing Systemen werden in den nächsten Jahren zunehmen.

[Rz 62] Die Nutzung von standortbezogenen Diensten, insbesondere von Location Sharing Systemen birgt ein hohes Risiko hinsichtlich des Persönlichkeitsschutzes; so entstehen durch die Möglichkeit der Mitverfolgung von Personenbewegungen neue Probleme im Bereich des Datenschutzes.[196] Bei konsequenter Beachtung der datenschutzrechtlichen Rahmenbedingungen[197] und der Gewährleistung des Persönlichkeitsschutzes mittels entsprechender technischer Massnahmen kann dieses Risiko minimalisiert werden. Darüber hinaus muss allerdings beachtet werden, dass es Bereiche des wirtschaftlichen und gesellschaftlichen Lebens gibt, die hinsichtlich einer Nutzung von Location Sharing Systemen besonders sensibel sind (Familie, Arbeitsplatz, Gesundheitswesen etc.). Hinsichtlich solcher Bereiche muss sich eine klare Rechtspraxis erst noch herausbilden. Die zuständigen Behörden stehen vor der Herausforderung, einerseits das geltende Recht im Interesse der Betroffenen durchzusetzen (ohne sich der Marktmacht bestimmter technologischer Grossunternehmen zu beugen) und andererseits die technologische und gesellschaftliche Entwicklung mit zu berücksichtigen. Dies erfordert gleichzeitig ein sorgfältiges juristisches Arbeiten und die Fähigkeit zum interdisziplinären Denken, das über die Bereiche Technik und Recht (insb. Personen-, Datenschutz-, Fernmelde- und Geoinformationsrecht) in gesellschaftswissenschaftliche Bereiche (Sozialwissenschaften, Ethik etc.) hineinreicht. Denn die Haltung der

[191] Vgl. dazu Ziffer 3.5, insbesondere muss die einmal erteilte Einwilligung die Verwendung von Standortdaten der Mobiltelefonie sowie – wegen der Publikation im Internet – die Bekanntgabe ins Ausland, d.h. die Möglichkeit der Abfrage im Internet von jedem Territorium jedes beliebigen Staates aus, umfassen.

[192] Vgl. Raffael Schuppisser, Lauschangriff von Google, NZZ am Sonntag vom 23. Mai 2010, S. 54; Beat Rudin, «Strassenansichten» fordern heraus, digma 2009.3, S. 92 f.; Weber (Fn. 10), S. 480 ff.

[193] Rudin (Fn. 192), S. 92 f.; Bruno Bariswyl, Die Anwendbarkeit des Datenschutzgesetzes, digma 2009.3, S. 98 ff.; Thilo Weichert, Der Fall «Street View» in Deutschland, digma 2009.3, S. 102 ff.; Bruno Baeriswyl, Vom Selbstverständnis der Beauftragten, digma 2009.3, S. 108 f.; Empfehlung des EDÖB vom 9. November 2009 (nicht rechtskräftig).

[194] 38 US-Bundesstaaten schliessen sich dem Generalstaatsanwalt von Connecticut an, der gegen Google wegen der Aufzeichnung ungesicherter WLAN-Verbindungen vorgeht, vgl. NZZ am Sonntag vom 25. Juli 2010, S. 50; vgl. auch www.20min.ch/digital/dossier/google/story/38-US-Staaten-wollen-gegen-Google-vorgehen-21197676.

[195] Vgl. NZZ am Sonntag vom 25. Juli 2010, S. 21; vgl. auch www.computerworld.ch/aktuell/news/51850/.

[196] In diesem Sinne auch Weber (Fn. 10), S. 485; Beat Rudin, Datenschutz in der Schweiz – Herausforderungen und Perspektiven in Wirtschaft und Verwaltung, in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Herausforderung Datenschutz, Zürich 2005, S. 78 f., hat schon vor fünf Jahren auf die fehlende Risikodiskussion hingewiesen.

[197] Vgl. vorstehend Ziffer 3.

Bevölkerung – oder deren verschiedenen gesellschaftlichen Gruppen – scheint hinsichtlich Privatsphäre und Datenschutz ambivalent zu sein: Eine repräsentative Umfrage in der Schweiz im Januar 2009 zeigt einerseits auf, dass die Bevölkerung einen starken Datenschutz will.[198] Andererseits zeigt eine neue deutsche Studie auf, dass die Bevölkerung nicht bereit ist, für Datenschutz zu bezahlen und beim Einkaufen über das Internet ihre Bedenken hinsichtlich der Privatsphäre wegen Preisvorteilen über Bord wirft.[199]

[Rz 63] Bereits warten allerdings im Bereich der «Cyber-Location», d.h. der Möglichkeit der Lokalisation im Internet neue Herausforderungen. Amerikanische Forscher haben kürzlich herausgefunden, dass eine Lokalisation nicht nur jeweils aktuell mit den erwähnten Techniken (GPS, Mobilfunk-Ortung, WLAN, IP-Adresse)[200] möglich ist, sondern auch *nachträglich auf der Grundlage von Metadaten von digitalen Fotografien und Videoaufzeichnungen*.[201] Solche georeferenzierten Metadaten finden sich primär in EXIF-Dateien von Aufnahmen in den Formaten JPEG, TIFF und WAV.[202] Internet-Netzwerke wie Flickr, YouTube und Twitter erlauben eine ortsbezogene Suche; bei Craiglist ist eine ortsbezogene Suche indirekt mit wenig technischem Aufwand möglich.[203]

[Rz 64] Die voraussichtlich grösste Herausforderung für den Persönlichkeitsschutz wird angesichts der aufgezeigten technischen Entwicklungen und der globalen (d.h. die Staatengrenzen und damit den Geltungsbereich des nationalen Rechts überschreitenden) Ausdehnung von entsprechenden Internet-Anwendungen in den nächsten Jahren der *Schutz ortsbezogener individueller Informationen (Local Privacy)* sein.[204] Von zentraler Bedeutung wird es dabei sein, international einen Konsens über einen adäquaten Datenschutz bei standortbezogenen Diensten zu finden.[205]

Mag. rer. publ. Daniel Kettiger ist Rechtsanwalt und Berater in Bern. Der vorliegende Aufsatz ist eine überarbeitete und aktualisierte Fassung eines Rechtsgutachtens zuhanden des Bundesamtes für Landestopografie (swisstopo).

Soweit keine besonderen Aktualitätsangaben bestehen, gibt der Aufsatz den Stand der Literatur und der Internet-Publikationen von Mitte Juli 2010 wieder.

---

* * *

---

[198] Vgl. Andrea Ruf, Bevölkerung fordert Datenschutz, digma 2009.1, S. 44 f.

[199] Vgl. Alstair R. Beresford/Dorothea Kübler/Sören Preibusch, Unwillingness to Pay for Privacy: A Field Experiment, WZB-Paper SP II 2010 – 03, Berlin 2010.

[200] Vgl. Ziffer 2.2.

[201] Vgl. Friedland/Sommer (Fn. 7), S. 2 f.

[202] Vgl. Friedland/Sommer (Fn. 7), S. 3.

[203] Vgl. Friedland/Sommer (Fn. 7), S. 3 ff.

[204] Vgl. Friedland/Sommer (Fn. 7), S. 5; Weber (Fn. 10), S. 485; Rudin (Fn. 196); Andrew J. Blumberg/Peter Eckersley, On Location Privacy, and How to Avoid Losing it Forerver, Electronic Frontier Foundation (EFF), www.eff.org/files/eff-locational-privacy.pdf (Stand: 24.07.2010).

[205] Vgl. Friedland/Sommer (Fn. 7), S. 5.