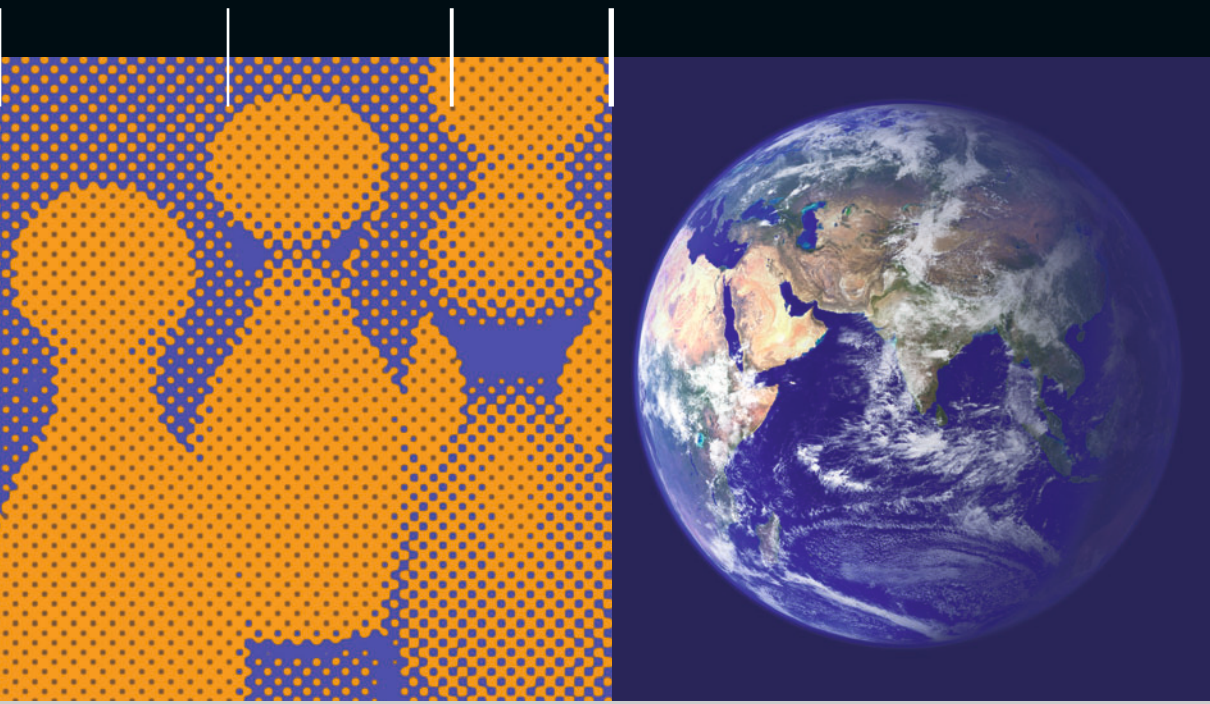
Lokalisiert und identifiziert

Wie Ortungstechnologien unser Leben verändern

Originally published in:
TA-SWISS / Zentrum für Technologiefolgen-Abschätzung 57/2012

Zentrum für Technologiefolgen-Abschätzung
Centre d'évaluation des choix technologiques
Centro per la valutazione delle scelte tecnologiche
Centre for Technology Assessment
TA SWISS



Lorenz Hilty, Britta Oertel,
Michaela Wölk, Kurt Pärli

Lokalisiert und identifiziert

Wie Ortungstechnologien unser Leben verändern

vdf

Zentrum für Technologiefolgen-Abschätzung
Centre d'évaluation des choix technologiques
Centro per la valutazione delle scelte tecnologiche
Centre for Technology Assessment

TA-SWISS 57/2012

Lorenz Hilty, Britta Oertel,
Michaela Wölk, Kurt Pärli

Lokalisiert und identifiziert

Wie Ortungstechnologien unser Leben verändern

v/dlf

Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Diese Studie wurde unterstützt vom Bundesamt für Landestopografie swisstopo, vom Bundesamt für Statistik BFS sowie vom Bundesamt für Strassen ASTRA.

ISBN 978-3-7281-3460-8 (Printausgabe)

Download open access:
ISBN 978-3-7281-3477-6 / DOI 10.3218/3477-6

www.vdf.ethz.ch
verlag@vdf.ethz.ch

Inhalt

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
ANPR	Automatic Number Plate Recognition (automatische Erkennung von Nummernschildern)
ARE	Bundesamt für Raumentwicklung
ArG	Arbeitsgesetz
ASTRA	Bundesamt für Strassen
BAKOM	Bundesamt für Kommunikation
BGE	Bundesgerichtsentscheid
BV	Bundesverfassung
BVGer	Bundesverwaltungsgericht
BVGE	Bundesverwaltungsgerichtsentscheid
BSV	Bundesamt für Sozialversicherungen
CBIR	Content-Based Image Retrieval (automatisches Auffinden von Bildern aufgrund ihres Inhalts)
CCTV	Closed Circuit Television (Überwachung durch Videokameras)
CeBIT	Centrum für Büroautomation, Informationstechnologie und Telekommunikation (weltweit grösste Messe für Informationstechnik)
DACH-Region	Deutschland, Österreich, Schweiz
DRSC	Dedicated Short Range Communication
DSG	Datenschutzgesetz
DSK	Europäische Datenschutzkonvention
DSRC	Dedicated Short Range Communication
DST	Digital Sky Technologies
EDK	Schweizerische Konferenz der kantonalen Erziehungsdirektoren
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EETS	European Electronic Toll Service
EGMR	Europäischer Gerichtshof für Menschenrechte
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Europäische Menschenrechtskonvention
EPC	Electronic Product Code
ERS	Emergency Response System

EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
EXIF	EXchangeable Image File Format
FMG	Fernmeldegesetz
GeoIG	Geoinformationsgesetz, Bundesgesetz über Geoinformation
GLONASS	Globalnaja Nawigazionnaja Sputnikowaja Sistema (von Russland betriebenes globales Satellitennavigationssystem)
GPS	Global Positioning System (von den USA betriebenes globales Satellitennavigationssystem)
GSM	Global System for Mobile Communications (Standard der zweiten Generation von Mobilfunknetzen)
HSPA(+)	High Speed Packet Access (Standard der vierten Generation von Mobilfunknetzen)
IETF	Internet Engineering Task Force
IKT	Informations- und Kommunikationstechnologie
IP-Adresse	Internet-Protocol-Adresse (Nummer, die einem am Internet teilnehmenden Gerät zugeordnet wird)
IPRG	Bundesgesetz über das Internationale Privatrecht
IPTC	International Press Telecommunications Council
IRNSS	Indian Regional Navigation Satellite System
ISP	Internet Service Provider
IT	Informationstechnik
ITB	Internationale Tourismus-Börse Berlin
KOBIK	Schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität
LAN	Local Area Network (Lokales Datennetz)
LBS	Location-Based Service, Standortbezogener Dienst
MAC-Adresse	Media-Access-Control-Adresse (Identifikationsmerkmal von Geräten, die in einem Netzwerk Daten austauschen)
NENA	National Emergency Number Association
NFC	Near Field Communication
NLBS	Near Location-Based Service
OBE	On-Board Equipment
OBU	On Board Unit
OR	Obligationenrecht
OTT	Over the top
PAM	Pluggable Authentication Module
PAYD	Pay As You Drive
PBG	Personenbeförderungsgesetz
PDA	Personal Digital Assistant
RFID	Radio Frequency IDentification
SBB	Schweizerische Bundesbahnen
SIM	Subscriber Identity Module

SIM-Card	Subscriber Identity Module Card
SKP	Schweizerische Kriminalprävention
SMM	Social Media Marketing
SWICO	Schweizerischer Wirtschaftsverband der Informations-, Kommunikations- und Organisationstechnik
TA	Technologiefolgen-Abschätzung, Technology Assessment
UGC	User Generated Content
UITP	International Association of Public Transport
UMTS	Universal Mobile Telecommunications System
UMU	Unique Mobile User
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
UWB	Ultra Wide Band
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
VBZ	Verkehrsbetriebe Zürich
VoIP	Voice over IP, Telefonieren via Internet
VZ-Netze	Verzeichnis-Netze
WLAN	Wireless Local Area Network
WWW	World Wide Web
ZGB	Schweizerisches Zivilgesetzbuch
ZPO	Zivilprozessordnung

Zusammenfassung

Heute sind zahlreiche technische Verfahren im Einsatz, die es erlauben, den Aufenthaltsort von Objekten oder Personen festzustellen. Neben der bekanntesten Technologie, der Satellitenortung durch GPS, werden heute mindestens 12 weitere Technologien verwendet, die es ermöglichen, den Standort von Geräten und damit indirekt ihrer Nutzer zu ermitteln. Dies kann je nach Technologie in Echtzeit oder auch nachträglich geschehen, von einigen Kilometern bis auf wenige Zentimeter genau, mit oder ohne Wissen der betroffenen Personen.

Weil die Ortung (auch: Positionsbestimmung, Geolokalisierung) technisch immer bequemer und kostengünstiger zu realisieren ist, werden im Alltag immer mehr Ortungsdaten erzeugt und gespeichert. Werden die Ergebnisse vieler Ortungsvorgänge kombiniert, können Bewegungsprofile oder auch Beziehungsprofile von Personen erstellt werden.

Neben der Navigation gibt es zahlreiche weitere Anwendungsbereiche von Ortungstechnologien: standortbezogene Dienste (location-based services), Mikromarketing, Berechnung von Gebühren und Versicherungsprämien, Überwachung von Einzelpersonen (im Gesundheitswesen oder im Strafvollzug), Diebstahlsicherung, Schwarmüberwachung (z.B. für Verkehrsprognosen), Notfalleinsätze, Dokumentation, Beweissicherung und in Zukunft möglicherweise noch andere Bereiche.

Die Ortung geschieht aus Sicht der georteten Personen häufig als Nebeneffekt einer anderen Funktion, die sie in Anspruch nehmen:

- Alle mobilen Geräte mit eingebautem GPS-Empfänger (darunter Smartphones) können ihren Standort mit hoher Genauigkeit feststellen; darauf aufbauend wird eine Vielzahl von Anwendungsprogrammen angeboten; den Nutzern ist nicht immer bewusst, ob bei der Verwendung einer App oder Dienstleistung ihre Ortungsdaten für Dritte sichtbar werden.
- Auch Mobiltelefone ohne GPS-Empfänger können von den Mobilfunk-Providern geortet werden. Die Kenntnis der Funkzelle, in welcher sich das

Gerät befindet, erlaubt schon eine grobe Ortung. Eine genauere Ortung von Mobiltelefonen ist auch ohne GPS durch Triangulationsverfahren möglich.

- Beim Zugriff auf Informationen über das Internet kann der Server aufgrund der IP-Adresse den Standort der Nutzerin grob eingrenzen. Erfolgt der Internet-Zugang über WLAN-Hotspots, ist auch eine genauere Ortung möglich.
- Beim Zugang zu Gebäuden oder gebührenpflichtigen Zonen mittels elektronischer Identifikation (z.B. durch RFID-Tags) und beim bargeldlosen Bezahlen werden ebenfalls Daten erzeugt, die die Aufenthaltsorte und Bewegungen von Personen dokumentieren.
- Auch Bilder, die Personen oder beispielsweise Fahrzeuge zeigen, können Aufenthaltsorte dokumentieren. Immer mehr Digitalkameras sind mit GPS-Empfängern ausgestattet und versehen digitale Bilddaten mit Geotags, die Zeit und Ort der Aufnahme angeben; Video-Überwachungskameras werden leistungsfähiger und unauffälliger. Parallel zu dieser Entwicklung verbessern sich durch den Fortschritt der Bildverarbeitungsverfahren die Möglichkeiten, Bildbestände automatisch nach Gesichtern oder Fahrzeugkennzeichen zu durchsuchen.

Ortungstechnologien sind dabei, in unserem Alltag eine ebenso selbstverständliche Stellung wie Telefon oder Internet zu erobern. Sie werden zu einem «externen Ortsgedächtnis», das für einen zunehmenden Anteil unserer Handlungen festhält, wann und wo wir sie vorgenommen haben.

Zukünftig wird die alltägliche Mobilität – sowohl mit privaten als auch mit öffentlichen Verkehrsträgern – nur schwer ohne Ortungssysteme vorstellbar sein. Aber auch das Agieren in sozialen Netzen auf Internet-Plattformen wird immer mehr mit dem physischen Aufenthaltsort der Nutzer verknüpft werden. Daraus werden neue, standortbasierte Geschäftsmodelle entstehen. Auf Ort, Zeit und Person fokussierte Werbung wird zum Normalfall werden. Ob dies langfristig zu Wirtschaftsprozessen führt, die sich besser an die Bedürfnisse der Menschen anpassen oder umgekehrt diese nur wirkungsvoller manipulieren, lässt sich nicht ohne weitreichende Annahmen und Bewertungen entscheiden.

Ortungstechnologien bieten vielfältige gesellschaftliche Chancen, etwa für die Förderung des öffentlichen Verkehrs (bequemere Nutzung des Angebots und einfachere Gebührenerhebung), für die Rettung im Notfall, für die persönliche

Sicherheit und Orientierung an unbekannten Orten, für das Treffen von Freunden und vielleicht auch für die Kontaktaufnahme unter Fremden.

Mit der Selbstverständlichkeit der Nutzung von Ortungsverfahren nimmt aber auch die Abhängigkeit von diesen Technologien zu. Sie werden zu neuen kritischen Infrastrukturen, deren Störung oder Ausfall weitreichende Folgen haben kann, vergleichbar etwa einem Ausfall der Telefonnetze. Verfälschte Ortungsinformation hat möglicherweise noch schwerere Folgen als fehlende Information, weil dadurch Verkehrsmittel, Personen und Frachtgüter in die Irre geführt werden können.

Die Kombination zweier Faktoren sorgt dafür, dass neben den Vorteilen und Chancen der Ortungstechnologien sich erhebliche gesellschaftliche Risiken entwickeln. Diese zwei Faktoren sind:

1. Die *abnehmende Freiwilligkeit der Nutzung der Ortungstechnologien*: Wer nicht geortet werden möchte, müsste bereits heute auf Mobiltelefonie und viele Internetfunktionen verzichten, im Extremfall auch auf elektronische Zugangs- und Zahlungssysteme, und wäre damit von vielen Aspekten des privaten und beruflichen Lebens ausgeschlossen.
2. Das *steigende Aufkommen an personenbezogenen Daten* aufgrund der zunehmenden Erzeugung, Übertragung, Speicherung und Verarbeitung von Ortungsdaten: Die privaten oder öffentlichen Stellen, die solche Daten bearbeiten, können sie zu Bewegungs- und auch Beziehungsprofilen zusammenfügen. Durch Kombination mit weiteren Daten, insbesondere Geodaten, können weitreichende Profilierungen von Personen und Gruppen vorgenommen werden.

Die Kombination dieser zwei Aspekte – Rückgang der Freiwilligkeit und Anstieg des Datenvolumens – birgt ein hohes gesellschaftliches Konfliktpotenzial, denn die schon bestehenden Schwierigkeiten des Einzelnen, sein Recht auf informationelle Selbstbestimmung durchzusetzen, könnten sich durch diese Entwicklung entscheidend verschärfen. Aufgrund der mangelnden Transparenz der eingesetzten Verarbeitungsprozesse, die häufig auch erst nachträglich einen Personenbezug herstellen, nimmt das Risiko von Persönlichkeits- und Datenschutzrechtsverletzungen zu.

In dieser interdisziplinären Studie werden die Technologien, Anwendungen und die in der Schweiz gegebenen rechtlichen Rahmenbedingungen der Ortungs-

technologien analysiert, wobei die Situation in der EU mitberücksichtigt wird. In einer vertiefenden Betrachtung der Schwerpunktthemen *Mobilität* und *soziale Netze* werden mögliche Auswirkungen (Chancen und Risiken) diskutiert und in Bezug auf ihre gesellschaftliche Relevanz beurteilt. Im Ergebnis zeigt sich politischer Handlungsbedarf in folgenden Bereichen:

- bei der technischen Überwachung von Personen in Abhängigkeitsverhältnissen, insbesondere von Mitarbeitenden, Schutzbedürftigen und Kindern;
- im Jugendschutz in Bezug auf die Teilnahme Minderjähriger an sozialen Netzen mit Ortungsfunktionen;
- bei der Durchsetzung der informationellen Selbstbestimmung des Einzelnen gegenüber dem Staat wie auch gegenüber Privatunternehmen; hier geht es um die Erhaltung der Kontrolle über die eigenen Ortungsdaten und die Vermeidung einer leichtfertigen Preisgabe von Grundrechten;
- bei der Begrenzung der Aufbewahrungsdauer von Ortungsdaten, insbesondere weil diese in vielen Fällen nachträglich Personen zugeordnet werden können und dann möglicherweise deren Persönlichkeitsrechte gefährden («Recht auf Vergessen»);
- bezüglich der Praxis der Allgemeinen Geschäftsbedingungen (AGB) der Anbieter von Softwareprodukten und Dienstleistungen mit Ortungsfunktionen, die zum Teil gegen geltendes Recht verstossen;
- im Hinblick auf die Vorbildfunktion staatlicher Stellen bei der Umsetzung von Datenschutzprinzipien, wenn sie selbst Ortungstechnologien zur effizienteren Wahrnehmung ihrer Aufgaben einsetzen;
- bezüglich der Sicherheit von Ortungssystemen als einer neuen kritischen Infrastruktur und dem Schutz gegen jene Formen der Cyberkriminalität, die durch Ortungstechnologien gefördert werden.

Aus diesem Handlungsbedarf leiten wir eine Reihe von Empfehlungen ab.

Die *allgemeinen Empfehlung*en zielen auf die Weiterentwicklung des Rechtsrahmens: Dringend geboten ist die Einführung effizienterer Sanktionsmöglichkeiten im Datenschutz, um den Missbrauch personenbezogener Daten (insbesondere Ortungsdaten von Personen), wirkungsvoll zu verhindern. Weiterhin sind Schritte erforderlich, um die Durchsetzbarkeit datenschutzrechtlicher Prinzipien im internationalen Raum zu verbessern. Ortungssysteme entwickeln sich

zu kritischen Infrastrukturen für die Schweizer Bevölkerung und müssen deshalb angemessen gegen Störung, Ausfall oder Zerstörung geschützt werden. Die Undurchschaubarkeit vieler Softwareprodukte und Dienstleistungen, welche Ortungsdaten von Schweizer Kunden verarbeiten, macht eine Zertifizierung für verlässliche und transparente Softwareprodukte und Dienstleistungen mit Ortungsfunktionen erforderlich. Das generell diskutierte «Recht auf Vergessen» von personenbezogenen Daten ist gerade bei Ortungsdaten von Bedeutung; deshalb sollte eine gesetzliche Verankerung dieses Rechts eingehend geprüft werden. Nicht zuletzt ist auch die empirische sozialwissenschaftliche Forschung gefordert, damit der tatsächliche Umgang mit Ortungstechnologien im Alltag und auch die soziale Entwicklungsdynamik der Austauschbeziehungen und Abhängigkeiten besser verstanden werden. Ein solches Verständnis ist die Grundlage für wirksame Regulierungen.

Neben diesen allgemeinen Empfehlungen, die auf die rechtlichen Leitplanken für eine grundrechtskonforme Weiterentwicklung und Anwendung der Ortungstechnologien abzielen, formulieren wir *spezielle Empfehlungen* für besondere Anwendungsbereiche: Informationsmassnahmen zu Allgemeinen Geschäftsbedingungen von sozialen Netzen; Handlungsanweisungen und eine klarere Regelung der Zulässigkeit der Ortung am Arbeitsplatz; Einbeziehung des Themas Ortung in Massnahmen zur Förderung der Medienkompetenz bei Jugendlichen; Einführung einer wirksamen Altersfeststellung der Nutzerinnen und Nutzer von Internetdiensten mit Ortungsfunktionen; Beitritt der Schweiz zur Europaratskonvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch; gezielte Nutzung des Vorbildcharakters staatlicher Anwendungen von Ortungstechnologien; die datenschutzgerechte Nutzung von Crowdsourcing (der Mitwirkung vieler Freiwilliger) im Verkehr; eine einheitliche Regelung der Video-Ortung; die Ausdehnung des Prinzips der sog. Robinsonliste («an meine Adresse bitte keine Werbung») auf digitale Medien, insbesondere standortbezogenes Marketing.

Die Empfehlungen dieser TA-Studie sollen die Nutzung von Ortungstechnologien und ihrer vielfältigen Vorteile nicht verhindern, sondern im Gegenteil dazu beitragen, dass die Risiken dieser faszinierenden Technik frühzeitig erkannt und minimiert werden – nur dann wird es auf Dauer gelingen, die Chancen der Ortungstechnologien zum Vorteil der Gesellschaft zu entfalten und *nachhaltigen Nutzen* daraus zu ziehen.

Summary

Today many technologies are being used that involve information on the location of objects or persons. In addition to the widely known geolocation by satellite via GPS, today at least 12 more technologies are being used that make it possible to determine the location of devices, and indirectly that of their users. This may happen in real time or after a delay depending on the technology; it may happen with a degree of precision ranging from a few kilometers to a few centimeters, and either with or without the knowledge of the persons affected.

Because localization or determination of position can be technically implemented with increasing convenience and decreasing cost, more and more localization data are being generated and stored all the time. When the results of many localization processes are combined, tracking profiles, or even relationship profiles, can be done on persons. In addition to navigation, there are numerous other application areas of localization technologies: location-based services, micromarketing, calculation of fees and insurance premiums, surveillance of individuals (for health reasons or in law enforcement), emergency missions, documentation, forensic evidence and in future perhaps other areas.

From the standpoint of the person being localized, localization is often done as a side-effect of another function that the person wants to use:

- All mobile devices with an integrated GPS receiver (such as smartphones) can determine their position with a high degree of precision; many apps build upon this; the user is not always conscious whether her localization data are visible to third parties when she uses an app or service.
- Mobile telephones that do not even feature a GPS receiver can also be localized by mobile providers. Just knowing in which cell the device is operating provides a rough localization. A more precise localization of mobile phones without GPS is also possible by triangulation.
- When a user is accessing information on the Internet, the server can roughly estimate the location of the user. Whenever Internet access is via a WLAN hotspot, an even more precise localization is possible.

- When buildings or fee-based zones are accessed using electronic identification (such as RFID tags) or when electronic payments are made, data are also generated that document the location and movement of persons.
- Images that show persons or vehicles may document locations. More and more digital cameras are equipped with GPS receivers and mark digital image data with geotags that specify time and location; video surveillance cameras are becoming more powerful and less conspicuous. Parallel to this development, image processing processes are being improved so as to enable authorities to mine collections of images automatically for faces or license plate numbers.

Localization technologies are in the process of taking a dominant position in our lives just as well-accepted as the telephone or the Internet. These devices are becoming an «external location memory» that records for more and more of our acts when and where we performed them.

In the future it will become difficult to imagine everyday mobility – both that in individual and that in public traffic – without localization systems. Likewise acting in social networks on Internet platforms will be associated increasingly with the physical location of the user. New location-based business models will result from that. Advertising focused on location, time and the individual will become normal. Whether this will lead to business processes that adapt better to people's needs, or inversely will manipulate persons, cannot be predicted without making far-reaching assumptions and evaluations.

Localization technologies offer many societal opportunities, e.g. for promoting public transportation (easier to find connections and to pay for them), for rescue operations, for personal security and orientation at unfamiliar locations, for meeting friends and perhaps even for making friends among strangers.

However, as localization technologies become more readily accepted, we are becoming more dependent on them. They are becoming new critical infrastructures the malfunctioning or collapse of which can have far-reaching consequences comparable with a breakdown of the telephone network. Manipulated localization information may have even more serious consequences than a lack of information, because it can misguide vehicles, persons and freight.

The combination of two factors can make considerable societal risks develop in addition to the ad-vantages and opportunities afforded by localization technologies. The factors are:

1. A drop in the voluntary nature of our use of localization technologies: If a person does not wish to be located even today, she has to do without a mobile phone and many Internet functions, in extreme cases even without electronic access and payment systems – thus becoming excluded from many aspects of personal and professional life.
2. The increasing amount of personal data in circulation due to the increasing generation, transmission, storage and processing of localization data: the private-sector and public offices that process such data can combine them into tracking and relationship profiles. Far-reaching profiles of persons and groups can be assembled by combining that with other data, in particular geographic data.

The combination of these two aspects – the drop in the voluntary nature and the increasing amount of data – holds a potential for societal conflict because the difficulties of the individual that exist today in getting her right to informational self-determination respected might later intensify to a critical mass. The lack of transparency in the processing steps used, which are frequently not associated with a person until after the fact, is increasing the risk of personal and data protection violations.

This interdisciplinary study examines the technologies, applications and Swiss legal framework conditions of localization technologies, including the situation in the EU whenever relevant. In keeping with the themes of Mobility and Social networks the possible impacts (both the opportunities and the risks) are discussed and evaluated as regards their societal relevance. The results show a need for political action in the following areas:

- For the technical surveillance of people in dependency relationships, especially employees, persons needing protection and children;
- In Child Protection Measures pertaining to the participation of adolescents in social networks with a localization function;
- In defending the informational self-determination of the individual vis-à-vis the state and private-sector enterprises; this is a matter of maintaining

control over one's own data and avoiding the thoughtless surrendering of basic rights;

- In limiting the retention of localization data, because in many cases it can be associated with persons after the fact, possibly jeopardizing their rights to privacy («right to be forgotten»);
- As regards the permissibility of the Terms of Service (ToS) used by the providers of software packages and services with localization functions, some of which violate current law;
- Taking seriously the model function of government offices in implementing data protection principles, whenever they use localization technologies to perform their own duties more efficiently;
- To recognize the security of localization systems as a new critical infrastructure and to protect the populace against those forms of cyber-criminality that are facilitated by localization technologies.

We derive a set of recommendations from the above list.

The general recommendations aim to develop further the legal framework: we urgently need to introduce more efficient ways to sanction violations in the data protection rules intended to effectively prevent the misuse of personally identifiable data (in particular, the localization data of persons). Furthermore, measures are needed to improve the enforcement of data protection principles in the international context. Localization systems are developing into critical infrastructures for the Swiss population and must therefore be protected from malfunctions, breakdown or destruction. Many people have difficulty understanding the operation of software products and services that process localization data; this inability makes a certification necessary, so that software products become more reliable and transparent. The widely discussed «right to be forgotten» for personal data is of special importance in the case of localization data; therefore a legal anchoring of this right should be investigated thoroughly. Empirical social science research is needed so that the real handling of localization technologies in everyday life and the social development dynamics of sharing relations and dependencies can be better understood. Such an understanding is the basis for effective regulation.

In addition to the general recommendations that aim to establish legal guideposts for the on-going development and use of localization technologies in compliance

with basic law, we next articulate special recommendations for special areas: improving the public's understanding of the Terms of Service of social networks; directions and a clearer regulation of the permissibility of localization at one's place of work; integration of the topic of localization in measures to promote the media literacy of adolescents; the introduction of effective ways to establish the legal age of users of Internet services with localization functions; the accession of Switzerland to the Council of Europe Convention on the Protection of Children from Sexual Exploitation and Abuse; exercising the model function that governments have in the application of localization technologies; bringing the use of crowd sourcing (cooperation of many volunteers) in road traffic into compliance with data protection principles; a uniform regulation of video localization; the extension of the principle of the so-called Robinson List («don't send me any advertising») to digital media, especially location-based marketing.

The recommendations of this TA study are not intended to hamper the use of localization technologies or to underplay their many advantages; instead we aim to help recognize and minimize the risks of these fascinating technologies at an early stage – only then will we succeed in the long run in exploiting the opportunities of localization technologies to the advantage of society and in deriving sustainable benefit from them.

Résumé

De nombreux procédés techniques permettent aujourd'hui de déceler le lieu où se trouvent des objets ou des personnes. La méthode la plus connue est la localisation par satellite au moyen du GPS ; mais au moins douze autres technologies sont utilisées aujourd'hui pour déterminer la position d'appareils, et donc indirectement aussi celle de leurs utilisateurs. Suivant la technologie choisie, la localisation se fait en temps réel ou après coup, avec une précision allant de quelques kilomètres à peu de centimètres, les personnes concernées le sachant ou non.

Etant donné que la localisation (appelée aussi positionnement ou géo-localisation) est techniquement de plus en plus aisée, et qu'elle est réalisable à un coût toujours plus avantageux, une quantité croissante de données de localisation sont produites et stockées dans la vie courante. La combinaison des résultats de nombreux processus de localisation permet d'établir des profils de déplacement ou des profils de relations entre personnes.

A part la navigation, il existe de nombreux autres domaines d'application de technologies de localisation : services géodépendants (location-based services), micromarketing, calcul de taxes et de primes d'assurance, surveillance de personnes (dans le système sanitaire ou pénal), protection contre le vol, surveillance d'essaims d'objets en mouvement (p.ex. pour les prévisions de trafic), interventions d'urgence, documentation, conservation de preuves, et peut-être encore d'autres domaines à l'avenir.

La localisation a lieu souvent en tant qu'effet collatéral d'une autre fonction à laquelle la personne repérée recourt:

- Tous les appareils mobiles avec récepteur GPS intégré (parmi eux les smartphones) peuvent déterminer leur position avec une très grande précision ; ce fait est à la base de nombreux programmes d'application proposés sur le marché ; les utilisateurs ne se préoccupent pas toujours de savoir si leurs données de localisation sont visibles par des tiers lorsqu'ils se servent d'une app ou d'un service.

- Les téléphones mobiles sans récepteur GPS peuvent aussi être localisés par les opérateurs. La connaissance de la cellule radio dans laquelle se trouve l'appareil permet déjà de déterminer sa position grossièrement. Une localisation plus précise est possible aussi sans GPS au moyen de processus de triangulation.
- Lors de la saisie d'informations par Internet, le serveur peut délimiter grossièrement la position de l'utilisatrice ou de l'utilisateur en se basant sur l'adresse IP. Si l'accès à Internet a lieu par une borne Wi-Fi, une localisation plus précise est également possible.
- Lors de l'accès à des bâtiments ou à des zones payantes par un moyen d'identification électronique (p.ex. étiquettes RFID), ou lors de paiements sans argent liquide, des données sont également produites qui fournissent des indications sur les positions et mouvements de personnes.
- Des images qui montrent des personnes ou par exemple des véhicules peuvent aussi renseigner sur la localisation. Toujours plus de caméras numériques sont dotées de récepteurs GPS et munissent les données d'images numériques de balises de géolocalisation qui indiquent l'heure et le lieu de la prise de vue. Les caméras de surveillance vidéo deviennent plus performantes et plus discrètes. Parallèlement à cette évolution, le progrès des méthodes de traitement d'images améliore les possibilités d'exploration automatique de stocks d'images en fonction des visages ou des plaques d'immatriculation.

Les technologies de localisation sont en voie de conquérir une place aussi habituelle dans notre quotidien que le téléphone ou Internet. Elles deviennent en quelque sorte une « mémoire des lieux externe » qui retient, pour une part croissante de nos actions, quand et où nous les avons accomplies.

Tant pour les transports privés que publics, il sera difficile à l'avenir d'imaginer la mobilité quotidienne sans systèmes de localisation. Les activités dans des réseaux sociaux sur des plates-formes Internet seront elles aussi toujours davantage associées à la localisation physique de l'utilisateur. Il en résultera de nouveaux modèles commerciaux basés sur la localisation. Il deviendra normal que la publicité soit axée sur le lieu, le moment et la personne. Cela conduira-t-il à long terme à des processus économiques mieux adaptés aux besoins des êtres humains, ou permettant au contraire de manipuler ces derniers plus

efficacement ? Il n'est pas possible de trancher sans partir d'hypothèses et d'appréciations de grande portée.

Les technologies de localisation procurent de multiples chances à la société, par exemple pour soutenir la promotion des transports publics (utilisation plus confortable de l'offre et perception plus simple des taxes), faciliter les sauvetages en situations d'urgence, assurer la sécurité de personnes et les aider à s'orienter en des lieux non connus, faciliter la rencontre d'amis ou la prise de contact entre personnes qui ne se connaissent pas.

L'utilisation de méthodes de localisation devenant toujours plus naturelle, il s'ensuit une dépendance à l'égard de ces technologies. Elles deviennent de nouvelles infrastructures critiques, dont les perturbations et les pannes ont des conséquences de grande portée, comparables à la défaillance de réseaux téléphoniques. Une fausse localisation peut avoir des suites encore plus graves que l'absence d'information, car des moyens de transports, des personnes ou des marchandises risquent alors de se fourvoyer.

La combinaison de deux facteurs fait qu'à part les avantages et les chances qu'elles offrent, les technologies de localisation impliquent des risques sociaux considérables. Ces deux facteurs sont:

1. Le fait que l'utilisation des technologies de localisation repose de moins en moins sur le libre choix : qui ne souhaite pas être localisé devrait aujourd'hui déjà renoncer à la téléphonie mobile et à de nombreuses fonctions Internet, voire même aux systèmes électroniques d'accès et de paiement, et serait exclu ainsi de nombreux aspects de la vie privée et professionnelle.
2. Le volume croissant de données se référant à des personnes, vu que toujours plus de données de localisation sont produites, transmises, stockées et traitées : les services privés ou publics qui procèdent au traitement de telles données peuvent les assembler en profils de déplacements et de relations. Leur combinaison avec d'autres données, en particulier des géodonnées, permet d'élaborer en profondeur des profils de personnes et de groupes.

La combinaison de ces deux aspects – l'érosion du libre choix et l'augmentation du volume de données – recèle un potentiel social élevé de conflit, car cette évolution pourrait aggraver de façon déterminante les difficultés auxquelles un

individu est déjà confronté pour faire valoir son droit à l'autodétermination informationnelle. Le manque de transparence des processus de traitement appliqués, qui n'établissent souvent qu'après coup un lien avec des personnes, accroît le risque de violation du droit de la personnalité et de la protection des données.

Les technologies de localisation, leurs applications et les conditions juridiques cadres qui leurs sont données en Suisse sont analysées dans cette étude interdisciplinaire en tenant compte aussi de la situation dans l'UE. Leurs effets possibles (chances et risques) sont discutés dans le contexte d'un examen en profondeur axé en priorité sur la mobilité et les réseaux sociaux et évalués quant à leur importance pour la société. Les résultats montrent que des mesures s'imposent au niveau politique à propos des domaines suivants:

- la surveillance technique de personnes en situation de dépendance, notamment de collaborateurs, de personnes ayant besoin de protection et d'enfants ;
- la protection de la jeunesse en ce qui concerne la participation de mineurs à des réseaux sociaux avec fonctions de localisation ;
- l'autodétermination informationnelle des individus à l'égard de l'Etat de même que d'entreprises privées ; à cet égard, il s'agit de garder le contrôle sur ses propres données de localisation et de ne pas abandonner à la légère des droits fondamentaux ;
- la limitation de la durée de conservation de données de localisation, notamment parce qu'elles peuvent être attribuées dans de nombreux cas après coup à des personnes et mettre alors éventuellement en danger leurs droits de la personnalité (« droit à l'oubli ») ;
- la pratique des conditions générales (CG) des fournisseurs de logiciels et de services avec fonctions de localisation, lesquelles transgressent en partie le droit en vigueur ;
- le rôle exemplaire de services de l'Etat dans la mise en œuvre de principes de protection des données, quand ces services utilisent eux-mêmes des technologies de localisation pour assumer leurs tâches de façon plus efficace ;

- la sécurité de systèmes de localisation en tant que nouvelle infrastructure critique et la protection contre les formes de cybercriminalité encouragées par des technologies de localisation.

Nous en tirons une série de recommandations.

Les recommandations générales visent le développement du cadre juridique : Des possibilités plus efficaces de sanctions en matière de protection des données s'imposent de toute urgence pour empêcher l'usage abusif de données liées à des personnes (en particulier de données de localisation de personnes). En outre, des démarches sont nécessaires pour améliorer l'applicabilité des principes du droit de la protection des données au niveau international. Les systèmes de localisation évoluent vers des infrastructures qui deviennent critiques pour la population suisse ; ils doivent donc être protégés contre les perturbations, les pannes ou leur destruction. La non-transparence de nombreux logiciels qui traitent des données de localisation de clients suisses rend nécessaire une procédure de certification garantissant la fiabilité et la transparence de tels logiciels et prestations. Le « droit à l'oubli » de données liées à des personnes, discuté de façon générale, est particulièrement important à propos des données de localisation ; c'est pourquoi il faudrait examiner en détail la possibilité d'inscrire ce droit dans la loi. La recherche empirique en sciences sociales est particulièrement concernée pour améliorer la compréhension de l'utilisation de technologies de localisation dans la vie de tous les jours et la dynamique du développement social des relations d'échange et des dépendances. Une telle compréhension constitue la base de réglementations efficaces.

Ces recommandations générales portent sur les grandes orientations juridiques devant garantir que les technologies de localisation se développent et soient appliquées dans le respect des droits fondamentaux. A part cela, nous formulons des recommandations spécifiques pour certains domaines d'application. Elles préconisent : des dispositions ayant trait à l'information sur les conditions générales de réseaux sociaux ; des instructions et une réglementation plus claire sur les conditions dans lesquelles la localisation est admissible au lieu de travail ; l'intégration du thème de la localisation dans les mesures d'encouragement de l'éducation aux médias ; la détermination efficace de l'âge des utilisatrices et utilisateurs de services Internet avec fonctions de localisation ; l'adhésion de la Suisse à la Convention du Conseil de l'Europe sur

la protection des enfants contre l'exploitation et les abus sexuels ; la mise en valeur du caractère exemplaire d'applications étatiques de technologies de localisation ; l'exploitation conforme à la protection des données de crowdsourcing (collaboration de nombreux volontaires) dans le trafic ; une règlementation homogène de la localisation par vidéo ; l'extension du principe de la liste Robinson (« pas de publicité à mon adresse ») aux médias numériques, en particulier au marketing localisé.

Les recommandations de cette étude TA n'ont pas pour objet d'empêcher l'utilisation de technologies de localisation et leurs multiples avantages, mais au contraire de contribuer à ce que les risques de cette technique fascinante soient reconnus et minimisés à temps – c'est alors seulement que l'on parviendra à la longue à développer à l'avantage de la société les chances offertes par ces technologies et d'en tirer une utilité durable.

Sintesi

Numerose tecnologie ci consentono oggi di accertare il luogo in cui si trovano oggetti o persone. La localizzazione satellitare tramite GPS è il sistema più conosciuto, ma ci sono almeno una dozzina di altri metodi che permettono di identificare l'ubicazione degli apparecchi e dunque indirettamente anche dei loro utilizzatori. A seconda della tecnologia utilizzata, la localizzazione può avvenire sia in tempo reale che a posteriori, con un grado di precisione che varia da alcuni chilometri fino a pochi centimetri, che gli interessati ne siano a conoscenza o meno.

Poiché a livello tecnico la localizzazione (chiamata anche individuazione della posizione, geolocalizzazione) è realizzabile in modo sempre più agevole ed economico, quotidianamente vengono generati e memorizzati sempre più dati al riguardo. Combinando i risultati di numerosi processi di localizzazione, è possibile quindi elaborare dei profili di movimento o anche ricostruire relazioni spaziali tra persone.

Esistono numerosi altri ambiti di applicazione delle tecnologie di localizzazione, oltre a quello della navigazione: servizi georeferenziati (location-based service), micromarketing, calcolo di spese e premi assicurativi, monitoraggio di singoli individui (nel sistema sanitario o penale), sistemi antifurto, monitoraggio di sciami (ad esempio ai fini dell'elaborazione di previsioni nel settore del traffico), interventi in caso di emergenza, documentazione, acquisizione di prove penali, e forse in futuro anche altri settori.

La localizzazione avviene spesso come effetto collaterale dell'utilizzo di un'altra funzione da parte delle persone:

- Tutti gli apparecchi mobili con ricevitore GPS integrato (tra cui gli smartphone) possono accertare la propria posizione con un alto grado di precisione; su queste basi viene proposta una molteplicità di applicazioni, ma gli utenti non sono sempre consapevoli del fatto che attraverso l'utilizzo di un'applicazione o di un servizio i loro dati di localizzazione diventano visibili anche a terzi.

- Anche i cellulari privi di ricevitore GPS possono essere localizzati dai provider di servizi di telefonia mobile. L'identificazione della cella telefonica in cui si trova l'apparecchio consente già una prima localizzazione di massima. Una localizzazione più precisa dei telefoni cellulari senza GPS è possibile anche attraverso processi di triangolazione.
- Durante l'accesso a informazioni via Internet, il server è in grado di circoscrivere grossolanamente l'ubicazione dell'utente sulla base dell' indirizzo IT. Se l'accesso a Internet avviene tramite un hotspot WLAN è possibile anche una determinazione più precisa.
- Durante l'accesso a edifici o zone soggette a pagamento mediante identificazione elettronica (ad es. mediante tag RFID – Identificazione a radio frequenza) o nel caso di pagamenti senza contanti vengono generati dati che documentano i luoghi di permanenza e i movimenti delle persone.
- Anche le immagini che mostrano persone o veicoli possono documentarne la posizione. Sempre più fotocamere digitali sono dotate di ricevitori GPS e associano ai dati delle immagini digitali dei geotag che indicano l'ora e il luogo della ripresa; le telecamere di videosorveglianza stanno diventando sempre più efficienti e sempre meno visibili. In parallelo a questa evoluzione, grazie al progresso compiuto dai processi di elaborazione delle immagini, migliorano inoltre le possibilità di esaminare automaticamente gli archivi di immagini per individuare volti o targhe di veicoli.

Le tecnologie di localizzazione sono destinate a occupare un posto abituale nella nostra vita di tutti i giorni, come il telefono o Internet. Esse si stanno trasformando in una «memoria locale esterna» per una percentuale sempre maggiore delle nostre azioni, indipendentemente dal momento in cui le abbiamo compiute.

In futuro sarà difficile immaginare la mobilità di tutti i giorni – con mezzi di trasporto sia privati che pubblici – senza sistemi di localizzazione. Ma anche l'utilizzo dei social network su piattaforme Internet verrà collegato sempre più spesso all'ubicazione fisica delle persone. Si avranno così nuovi modelli commerciali basati sulla localizzazione. Diverrà normale avere la pubblicità associata al luogo, al momento e alla persona. Tutto ciò porterà a processi economici che meglio si adegueranno alle esigenze delle persone o, al contrario, servirà unicamente a manipolare più efficacemente queste ultime?

Non è possibile dare dei giudizi senza partire da ipotesi e considerazioni molto generali.

Le tecnologie di localizzazione offrono molteplici opportunità sociali: nella promozione dei trasporti pubblici (maggiore comodità di utilizzo dell'offerta e semplificazione del rilevamento delle spese); negli interventi di salvataggio in caso di emergenza; per la sicurezza personale e per orientarsi in luoghi sconosciuti; per incontrare gli amici e magari anche per entrare in contatto con persone sconosciute.

Con il diffondersi di un utilizzo sempre più frequente di sistemi di localizzazione aumenta tuttavia anche la dipendenza da queste tecnologie. Esse diventano così nuove infrastrutture critiche, i cui guasti o interruzioni nel funzionamento possono avere conseguenze in ambito più ampio, paragonabili ad esempio a un'interruzione delle reti telefoniche. Inoltre un'informazione di localizzazione falsata può avere ripercussioni ancora più pesanti di un'informazione mancante, poiché mezzi di trasporto, persone e merci trasportate possono essere indotti in errore.

La combinazione di due fattori fa sì che, oltre ai vantaggi e alle opportunità offerti delle tecnologie di localizzazione, si abbiano anche dei rischi notevoli per la società. Si tratta dei seguenti due fattori:

1. Il fatto che le tecnologie di localizzazione siano sempre meno vincolate alla libertà di scelta: chi non desidera essere localizzato dovrebbe rinunciare già oggi ai telefoni cellulari nonché a numerose funzioni Internet e nei casi più estremi anche ai sistemi di accesso e di pagamento elettronici, venendo così escluso da molti aspetti della vita privata e professionale.
2. Il volume crescente di dati riferiti a persone in seguito alla produzione, al trasferimento, al salvataggio e all'elaborazione sempre più consistenti di dati di localizzazione: gli enti pubblici e privati che elaborano simili dati possono aggregarli all'interno di profili di movimento o di relazione. L'associazione di questi ultimi con altri dati, in particolare geodati, permette di definire in dettaglio profili di gruppi e di singole persone.

La combinazione dei due aspetti citati– la diminuzione della libertà di scelta e l'aumento del volume di dati – genera un elevato potenziale di conflitto sociale, poiché tale dinamica potrebbe aggravare in misura significativa le difficoltà che il

singolo individuo già incontra, nel far valere il proprio diritto all' autodeterminazione informativa. La mancanza di trasparenza nei processi di elaborazione impiegati, che spesso consentono di stabilire un riferimento personale anche a posteriori, aumenta anche il rischio di violazioni del diritto della personalità e del diritto alla protezione dei dati.

Le tecnologie di localizzazione, le loro applicazioni e le relative condizioni giuridiche quadro esistenti in Svizzera sono analizzate in questo studio interdisciplinare, tenendo anche conto della situazione esistente all'interno dell'UE. Le possibili conseguenze (rischi e opportunità) di queste tecnologie sono discusse nell'ambito di un'analisi approfondita, centrata primariamente sui temi della mobilità e dei social network, e sono esaminate alla luce della loro rilevanza sociale. I risultati dello studio mostrano che c'è bisogno di un intervento a livello politico nei seguenti settori:

- monitoraggio tecnico di persone in rapporti di dipendenza, in particolare di lavoratori dipendenti, persone che necessitano di protezione e bambini;
- protezione dei giovani, in particolare di minori che frequentano social network con funzioni di localizzazione;
- autodeterminazione informativa del singolo individuo nei confronti dello Stato nonché di aziende private; qui si tratta di mantenere il controllo sui propri dati di localizzazione e di non rinunciare a cuor leggero all' affermazione di diritti fondamentali;
- limitazione della durata di memorizzazione dei dati di localizzazione, soprattutto perché in molti casi questi dati possono essere attribuiti successivamente alle persone, minacciandone eventualmente il diritto della personalità («diritto all'oblio»);
- prassi delle Condizioni generali (CG) dei fornitori di prodotti software e servizi con funzioni di localizzazione che violano in parte il diritto vigente;
- ruolo esemplare svolto dai servizi statali nell'attuazione dei principi di protezione dei dati, allorché questi servizi impieghino essi stessi tecnologie di localizzazione al fine di svolgere in modo più efficiente i propri compiti;
- sicurezza dei sistemi di localizzazione in quanto nuova infrastruttura critica e tutela contro le forme di cybercriminalità favorite dalle tecnologie di localizzazione.

Sulla base di queste necessità di intervento possiamo definire una serie di raccomandazioni.

Le raccomandazioni generali mirano a favorire un ulteriore sviluppo del quadro giuridico. Si impone con urgenza l'introduzione della possibilità di sanzionare in modo più efficiente per meglio impedire l'utilizzo abusivo di dati relativi alle persone (in particolare di dati di localizzazione). Sono inoltre necessari dei provvedimenti atti a migliorare l'applicabilità dei principi di protezione dei dati a livello internazionale. Poiché i sistemi di localizzazione evolvono fino a diventare infrastrutture critiche per la popolazione svizzera, essi devono essere protetti adeguatamente contro i guasti, le interruzioni nel funzionamento e la distruzione. La scarsa trasparenza di molti prodotti software e servizi che elaborano dati di localizzazione di clienti svizzeri rende necessaria l'introduzione di una certificazione per i prodotti software e i servizi con funzioni di localizzazione affidabili. Il «diritto all'oblio» di dati relativi alle persone, discusso in termini generali, assume rilevanza proprio nel caso dei dati di localizzazione: per questo si impone un esame approfondito delle possibilità di regolare questo diritto a livello giuridico. La ricerca empirica delle scienze sociali è particolarmente interessata a comprendere meglio l'utilizzo effettivo delle tecnologie di localizzazione nella vita di tutti i giorni e anche la dinamica di sviluppo sociale dei rapporti di scambio e di dipendenza; tale conoscenza costituisce il punto di partenza per l'introduzione di una regolamentazione efficace.

Queste raccomandazioni di carattere generale sono orientate alle linee guida giuridiche per garantire che le tecnologie di localizzazione si sviluppino e vengano applicate nel rispetto dei diritti fondamentali. Qui formuliamo anche delle raccomandazioni specifiche per alcuni ambiti di applicazione: disposizioni relative all'informazione sulle condizioni generali dei social network; istruzioni operative e una regolamentazione più chiara sulle condizioni di ammissibilità della localizzazione sul posto di lavoro; l'introduzione del tema della localizzazione all'interno di misure volte a promuovere l'educazione ai media dei giovani; l'introduzione di un metodo di accertamento efficace dell'età degli utenti di servizi Internet con funzioni di localizzazione; l'adesione della Svizzera alla Convenzione del Consiglio d'Europa sulla protezione dei minori contro lo sfruttamento e gli abusi sessuali; la valorizzazione del carattere esemplare delle applicazioni delle tecnologie di localizzazione da parte dello Stato; l'utilizzo conforme alla legge sulla protezione dei dati del crowdsourcing (la co-

operazione di molti volontari) nel traffico; una regolamentazione unitaria della videolocalizzazione; l'estensione del principio della cosiddetta Lista Robinson («niente pubblicità al mio indirizzo») ai mezzi digitali, in particolare nel settore del marketing legato alla localizzazione.

Le raccomandazioni di questo studio di TA-SWISS non hanno lo scopo di impedire lo sfruttamento delle tecnologie di localizzazione e dei loro molteplici vantaggi, bensì, al contrario, di contribuire a riconoscere e minimizzare tempestivamente i rischi legati a questa affascinante tecnologia; solo allora sarà possibile sviluppare nel tempo le opportunità offerte dalle tecnologie di localizzazione nell'interesse della società e trarne vantaggio a lungo termine.

Danksagung

Dieses Buch hätte nicht entstehen können ohne die mehrfache kritische Begutachtung durch die Mitglieder der Begleitgruppe, denen wir hiermit herzlich für ihre ausführlichen Kommentare danken: Dr. Bruno Baeriswyl, Florence Bettschart, Dr. Erwan Bigan, Alain Buogo, Dr. Thomas Dübendorfer, Dr. Christine Giger, Prof. Dr. Gudela Grote, Dr. Jessica Heesen, Dr. Rainer Humbel, Thomas Kallweit, Dr. Francisco Klauser, Dr. Michael Kocheisen, Ulrich Lattmann, Urs Luther, Dr. Franziska Meister, Cyrill Osterwalder, Hans Kaspar Schiesser, Philipp Stüssi, Prof. Dr. Rolf H. Weber und Dr. Franz Zeller.

Ebenso danken wir Dr. Sergio Bellucci und Nadia Ben Zbir vom Schweizerischen Zentrum für Technologiefolgenabschätzung für die kooperative Projektleitung und den Bundesämtern für Statistik (BFS), für Strassen (ASTRA) und für Landestopographie (swisstopo) für die Unterstützung des Projekts.

Für ausführliche Fachgespräche, wertvolle Hinweise und schriftliche Ergänzungen bedanken wir uns ferner bei Martin Boess, Dr. Vlad Coroama, Nino Cozzio, Stefan Gerschwiler, Martin Hermida, Andreas Knöpfli, Renate Lang, Michael Laux, Thomas Ruddy, Simon Stöckli und Melanie Studer. Ein besonderer Dank geht an Patrizia Huber für Literaturrecherchen und umfangreiche redaktionelle Arbeiten am Manuskript.

1 Einleitung

Erstaunlich viele Alltagshandlungen hinterlassen Datenspuren, die darüber Auskunft geben, wo wir uns aufgehalten haben und mit wem wir in Verbindung stehen. Ob wir mobil telefonieren, auf das Internet zugreifen, von einer Videokamera erfasst werden, ein Foto auf eine Internetplattform hochladen, mit einem elektronischen Schlüssel eine Tür öffnen oder bargeldlos bezahlen: Fast immer entstehen dabei Daten, die Rückschlüsse auf unsere Aufenthaltsorte, unsere Bewegung im Raum und unsere Kontakte zulassen.

Immer mehr Geräte und damit indirekt ihre Nutzerinnen lassen sich auch in Echtzeit orten: Ein Beobachter kann «live» mitverfolgen, wo und in welche Richtung sich das geortete Gerät gerade bewegt und daraus Schlüsse ziehen.

Die Funkzellenortung von Handys, die GPS-Ortung (mit Weiterleitung der Daten über ein Funknetz) oder auch die Ortung WLAN-fähiger Laptops und Smartphones sind Verfahren, die technisch geeignet sind, Endgeräte und damit indirekt auch ihre Trägerinnen zu lokalisieren. Sie werden bereits für viele Anwendungen genutzt. Die Programme zeigen, wo sich der Verunfallte, das Schulkind, die Patientin, der Häftling, die Aussendienstmitarbeiterin, der Ehepartner, die Kundin, der verspätete Fluggast, der Frachtcontainer oder das gestohlene Fahrzeug gerade befindet. Hinzu kommt, dass Bilder aus Überwachungskameras oder die täglich 250 Millionen privaten Fotos, die allein auf Facebook hochgeladen werden, mit immer besseren Verfahren im Hinblick auf Gesichter oder Autokennzeichen ausgewertet werden können.

Technologien zur Ortung (auch: Positionsbestimmung, Geolokalisierung), können das Leben sicherer und komfortabler machen. Sie können im Notfall Hilfe herbeirufen, Gegenstände vor Diebstahl schützen, Reiserouten verkürzen, uns gezielt mit lokal relevanten Informationen versorgen, bei der Dokumentation unseres Lebens helfen und unsere Identität im Cyberspace, im virtuellen Raum, mit unserer physischen Identität verknüpfen. Treffen mit Freunden und Gleichgesinnten lassen sich leichter arrangieren, Arbeitsabläufe flexibilisieren und lokale Angebote besser mit der lokalen Nachfrage zur Deckung bringen.

Aufgrund der rasanten Ausbreitung solcher Technologien erscheint aber eine breite gesellschaftliche Diskussion auch der Risiken dieser Entwicklung drin-

gend erforderlich. Das gilt umso mehr angesichts unserer zunehmenden Abhängigkeit von diesen Technologien. Nur wenn erkennbare Risiken frühzeitig und auf sachlicher Grundlage diskutiert werden, können sie vermieden oder zumindest minimiert werden. Und nur dann wird es auf Dauer gelingen, auch die Chancen optimal nutzen.

Eine solche Diskussion anzuregen und dazu die Grundlagen bereitzustellen, ist das Ziel der vorliegenden Studie, die vom TA-Swiss in Auftrag gegeben und von einem interdisziplinären Projektteam durchgeführt wurde (Institut für Informatik der Universität Zürich; Abteilung Technologie und Gesellschaft der Empa, St.Gallen; Institut für Zukunftsstudien und Technlogiebewertung, Berlin; Zentrum für Sozialrecht, Zürcher Hochschule für Angewandte Wissenschaften, Winterthur). Konkret waren die folgenden Fragen zu beantworten:

- Welche Ortungstechnologien stehen derzeit zur Verfügung – in der Schweiz und im Ausland?
- Welche Entwicklungen sind in naher Zukunft zu erwarten?
- Bergen die Ortungstechnologien Konfliktpotenzial? Welche Konflikte könnten sich ergeben?
- Welches sind die Hauptakteure im Bereich Ortungstechnologien und welches sind ihre Beweggründe?
- Welcher gesetzliche Rahmen regelt die Anwendung der verschiedenen Ortungstechnologien?
- Welche wirtschaftlichen Interessen und Auswirkungen sind mit den Ortungstechnologien verbunden?
- Welche Entwicklungen im Bereich Ortungstechnologien sind aus Sicht der Bevölkerung wünschenswert?

Technologiefolgen-Abschätzung (TA) hat das generelle Ziel, einen reflektierten Umgang der Gesellschaft mit neuen technischen Möglichkeiten zu fördern und politische Entscheidungsträger dabei zu unterstützen, Chancen und Risiken frühzeitig zu erkennen und die Entwicklung aktiv zu gestalten.

Die Weiterentwicklung und Verbreitung von Ortungstechnologien ist von einer hohen Dynamik gekennzeichnet. Das haben wir auch als Projektteam erfahren, wurden wir doch im Laufe der Erarbeitung dieser Studie (Juli 2010 – Januar

2012) mehrfach von der Entwicklung eingeholt. Das gilt nicht nur für die Entstehung und Einstellung von Angeboten (wie Google Buzz), sondern auch für Skandale wie die Aufzeichnung von Ortungsdaten durch die iPhones von Apple oder politische Schritte wie die Evaluation des Datenschutzgesetzes. Wir hoffen, dass es uns – wie in einer wissenschaftlichen Arbeit geboten – durch ausreichende Abstraktion gelungen ist, die *prinzipiellen* Aspekte unseres Gegenstandes herauszuarbeiten, die vom Wandel der konkreten Produkte, medialen Ereignisse und Konfliktauslöser unabhängig sind. Zugleich hoffen wir, dass der Bericht allgemein verständlich geblieben ist. Um die Verständlichkeit zu unterstützen, haben wir ein Glossar hinzugefügt und an vielen Stellen illustrierende Beispiele angeführt. Die Beispiele haben den Nachteil, dass sie in kurzer Zeit veralten – wir gehen jedoch davon aus, dass unsere prinzipiellen Schlussfolgerungen mit der weiteren Ausbreitung von Ortungstechnologien nicht an Aktualität verlieren werden.

Diese Studie gibt den Stand vom 1. Januar 2012 wieder.

Aufbau der Studie:

Das anschliessende Kapitel 2 führt in die technischen Grundlagen ein. Es gibt einen Überblick über die Verfahren und Technologien, die geeignet sind, den Standort von Gegenständen oder Personen festzustellen. Dabei werden auch Technologien berücksichtigt, die nicht primär zu diesem Zweck entwickelt wurden, heute aber dazu eingesetzt werden.

Kapitel 3 führt in die rechtlichen Grundlagen ein. Es beschreibt den rechtlichen Rahmen, der für die Nutzung von Ortungstechnologien und die Verarbeitung der durch sie gewonnen Daten in der Schweiz massgeblich ist. Zusätzlich gibt es einen Einblick in die Rechtslage in der Europäischen Union und deren Auswirkungen auf die Schweiz.

Kapitel 4 skizziert die gesellschaftlichen Konfliktlinien, die sich um die Nutzung von Ortungstechnologien bereits abzeichnen, und führt Kriterien zur Beurteilung der gesellschaftlichen Relevanz von Anwendungen ein. Auf dieser Grundlage werden zwei Anwendungsgebiete ausgewählt, die im Anschluss vertieft behandelt werden: *Mobilität* und *Soziale Netze.* Die beiden daran anschliessenden Kapitel sind diesen beiden Vertiefungsgebieten gewidmet.

Kapitel 5 behandelt das Vertiefungsgebiet *Mobilität*. Es beschreibt den Stand der Anwendung von Ortungstechnologien auf dem Gebiet der Mobilität in der Schweiz und identifiziert ihre gesellschaftlich relevantesten Auswirkungen.

Kapitel 6 behandelt analog das Vertiefungsgebiet *Soziale Netze*. Es beschreibt die Entwicklung der sozialen Netzplattformen und die zunehmende Integration von Ortungsfunktionen in diese Plattformen. Auch hier werden die gesellschaftlich relevantesten Auswirkungen identifiziert.

Kapitel 7 strukturiert die gesellschaftlichen Chancen und Risiken der Ortungstechnologien, die sich als Ergebnis unserer Analyse herauskristallisiert haben. Auswirkungen, die sich nicht eindeutig als Chance oder Risiko beurteilen lassen, werden als ambivalente Auswirkungen eingeordnet, bei denen besonderer gesellschaftlicher Diskussionsbedarf gegeben ist.

Kapitel 8 bewertet die Auswirkungen nach ihrer gesellschaftlichen Relevanz und leitet daraus politischen Handlungsbedarf und konkrete Empfehlungen ab.

2 Technische Grundlagen

2.1 Historische Entwicklung der Ortungstechnologien

Die frühesten technischen Hilfsmittel zur Ortung wurden für die Schiffsnavigation entwickelt. Neben dem Kompass war der *Sextant* über Jahrhunderte das wichtigste Werkzeug zur Navigation. Er diente dazu, den Winkelabstand zwischen dem Horizont und der Sonne (oder einem anderen Himmelskörper) möglichst genau zu messen. Um die Position zu berechnen, benötigte man allerdings auch die aktuelle Uhrzeit. Die Präzision der Zeitmessung war deshalb der begrenzende Faktor für die astronomische Navigation auf den Weltmeeren. Erst die Schiffs-Chronometer des Uhrmachers John Harrison ermöglichten ab 1759 die Bestimmung der Längengrad-Position mit einer Genauigkeit von wenigen Seemeilen – eine Technologie, die Menschenleben und Güter auf Ost-West-Passagen sicherte und dem Schiffsverkehr einen weiteren Aufschwung brachte. Der Sextant verlor seine Bedeutung für die nautische Navigation erst zwei Jahrhunderte später mit dem Aufkommen der Satellitennavigation (Sobel, 2005; Dodel & Häupler, 2010).

Basierend auf der *Funktechnik* sind im 20. Jahrhundert verschiedene Ortungstechnologien entstanden. Diese nutzen die Richtung, die Laufzeit oder die Feldstärke von Radiowellen, um eine Position zu bestimmen. Leuchttürme und Leuchtschiffe wurden ab 1913 mit so genannten Funkfeuern ausgerüstet. Im Ersten Weltkrieg verwendete die US Navy erstmals den von Frederick A. Kolster erfundenen Funkkompass (Dodel & Häupler, 2010).

Im Zweiten Weltkrieg gelangte mit dem *Radar* eine weitere funkbasierte Ortungstechnologie zum Durchbruch. Das Radar-Verfahren beruht darauf, dass Radiowellen von metallischen Objekten reflektiert werden. Es wurde bereits 1904 von seinem deutschen Erfinder Christian Hülsmeier zum Patent angemeldet. Wahrscheinlich unbeeinflusst davon wurde die Technologie in den 1930er Jahren in mehreren Ländern zur Praxisreife entwickelt. Die Radartechnik spielte in der Luftschlacht um England (Battle of Britain) 1940 eine entscheidende Rolle (Buderi, 1996).

In der weiteren Entwicklung des Radars wurden Ortungs- und Identifikationstechnologien miteinander verknüpft. Bereits zum Ende des Zweiten Weltkrieges wurden Flugzeuge mit sog. Transpondern zur Freund-Feind-Erkennung ausgestattet. Das sind Geräte, die auf ein Funksignal mit einem eigenen Signal antworten (auch Sekundärradar genannt) und sich dadurch identifizieren. Seit 1950 sind Transponder in der Zivilluftfahrt Standard (Honold, 1971).

Nach dem Ende des Zweiten Weltkrieges wurden für andere Anwendungen *passive Transponder* entwickelt, die ein Funksignal bei der Reflexion modulieren und dadurch Information übertragen können, ohne dass sie eine eigene Energiequelle benötigen. Der älteste passive Transponder ist der so genannte Hohlraumresonator. Berühmt wurde das darauf beruhende Abhörgerät des russischen Erfinders Léon Theremin, mit dessen Hilfe von 1945 bis 1952 die US-Botschaft in Moskau belauscht wurde. Eine Membran, die durch Schallwellen in Schwingung versetzt wurde, modulierte das zurückgestrahlte Funksignal und machte dadurch Gespräche abhörbar. Seit den 1960er Jahren wurden Hohlraumresonatoren auch zur Identifikation von Eisenbahnwagen und von Autoteilen in der Industrie eingesetzt. Ein identifizierender Code wurde hier durch das Eindrehen von Schrauben eingestellt, welche das Volumen verschiedener Hohlräume veränderten.

Hohlraumresonatoren gelten als Vorläufer der heutigen RFID-Transponder[1], die auf digitaler Elektronik beruhen und deshalb trotz ihrer viel kleineren Abmessungen wesentlich mehr Information abgeben können. Die grösste Verbreitung haben einfache, passive RFID-Transponder, die vor allem in der Logistik und im Einzelhandel, aber auch zur Personen- und Tieridentifikation eingesetzt werden. Die jährlichen Verkaufszahlen weltweit liegen in der Grössenordnung von einer Milliarde (RFID, 2011). Datenschutzbedenken haben im vergangenen Jahrzehnt eine breite Diskussion zu den Chancen und Risiken von RFID ausgelöst (siehe z.B. Oertel et al., 2005). Die Europäische Kommission hat im Jahr 2009 eine Empfehlung für die Umsetzung von Datenschutzprinzipien bei RFID-Anwendungen herausgegeben, die in Form des «Privacy and Data Protection Impact Assessment Frameworks» (PIA) konkretisiert wurde (European Commission, 2001).

[1] RFID: Radio Frequency IDentification. Identifikation durch Funkwellen im Bereich der Radiofrequenz. Passive RFID-Transponder sind heute auch als «Intelligente Etiketten» und «Chipschlüssel» bekannt.

Als Ortungstechnologie betrachtet, ermöglichen passive RFID-Transponder lediglich eine so genannte *Engpassortung:* Objekte können nur geortet werden, wenn sie sich an einem Lesegerät (z.B. in der Form eines Gates) vorbei bewegen, wie das bei der Artikelsicherung im Einzelhandel oder bei Zugangskontrollen der Fall ist. Die maximal mögliche Auslesedistanz beträgt einige Meter oder auch nur Zentimeter, je nach Typ des Transponders. Aktive Transponder können aber auch grössere Entfernungen überbrücken und Sensorinformation verarbeiten, z.B. um festzustellen, ob ein Container geöffnet wurde.

Als *typische Ortungstechnologie* gilt heute die Satellitenortung, die nach ihrer militärischen Entwicklung in die zivile Nutzung überging. Am weitesten fortgeschritten ist das US-amerikanische GPS-System. Dessen Aufbau wurde 1973 begonnen; 20 Jahre später wurde GPS mit zunächst 24 Satelliten in Betrieb genommen. Im Jahr 2000 wurde die künstliche Verschlechterung der Genauigkeit für Nutzer, die nicht über einen geheimen Schlüssel verfügen, abgeschaltet. Dies hat zu einer raschen Diffusion von GPS-Empfängern, z.B. als Bestandteil von Auto-Navigationsgeräten, geführt. Seit 2008 ist das russische System GLONASS in Betrieb. Das europäische System Galileo wird voraussichtlich 2015 einsatzfähig sein. Neben diesen globalen Systemen sind Satellitennavigationssysteme für den regionalen Einsatz in China (BeiDou/ Compass) und Indien (IRNSS) im Aufbau (Dodel & Häupler, 2010).

Der letzte und für unser Thema entscheidende Schritt in der Entwicklung der Ortungstechnologien war aber die *Digitalisierung der Kommunikation*. Bis in die 1980er Jahre hinein war der digitale Computer primär eine Maschine zur *Verarbeitung* und *Speicherung*, nur ausnahmsweise auch zur *Übertragung* von Daten. Fortschritte in der Digitaltechnik ermöglichten dann den Aufbau breitbandiger digitaler Kommunikationsnetze und damit die Verschmelzung von Informations- mit Kommunikationstechnologien. Durch Digitalisierung wird grundsätzlich jeder Kommunikationsvorgang der Speicherung und Verarbeitung zugänglich und jedes von Sensoren aufgenommene Datum ohne Qualitätsverlust übertragbar.

Diese noch nicht abgeschlossene Entwicklung hat unter anderem die Konsequenz, dass ganz neue Formen der Ortung möglich werden. Wesentlich sind hier vor allem folgende Entwicklungen:

- Mobilfunknetze: Das GSM[2] als erster Standard für volldigitale Mobilfunknetze setzte sich in den 1990er Jahren durch und hat zu einer raschen Verbreitung der Mobiltelefonie geführt. Diese Entwicklung war nicht nur für die Industrieländer, sondern parallel dazu auch für Entwicklungs- und Schwellenländer relevant, weil die Infrastruktur im Verhältnis zu einem traditionellen Festnetz relativ leicht aufzubauen ist. Im Jahr 2002 überholte die Zahl der weltweiten Mobilfunk-Subscriber die Zahl der Festnetz-Telefonanschlüsse, die bei rund einer Milliarde stagniert. Im Jahr 2011 gab es weltweit bereits 5 Milliarden Mobilfunk-Subscriber (ITU, 2009; ITU, 2010). GSM, auch als Mobilfunk der 2. Generation bezeichnet, koexistiert heute in der Schweiz mit Mobilfunktechnologien der 3. Generation wie UMTS[3] und HSPA(+)[4]. Multifunktionale Smartphones lösen die einfachen Mobiltelefone ab und werden zunehmend für mobilen Internetzugang genutzt.
- Das Internet: Der weltweite Zusammenschluss von Computernetzen machte den Computer in den 1980er Jahren vom Rechner zum Kommunikationsmedium, zunächst vor allem durch die Anwendung E-Mail. Der eigentliche Durchbruch des Internet kam ab 1993 mit seiner Nutzung als World Wide Web[5] (WWW) und der Verbreitung entsprechender Browser, Server und später auch Suchmaschinen. Inzwischen wurden zahlreiche weitere Internet-Dienste wie Telefonie (z.B. Skype) und Internet-Radio realisiert. Mit der Zunahme der nutzergenerierten Inhalte und Dienste wurde das WWW nach dem Jahr 2000 allmählich zu einer Plattform für soziale Interaktion unter Millionen Nutzern, für die sich die – unter Fachleuten umstrittene, weil unbegründete – Bezeichnung «Web 2.0» durchgesetzt hat. Unter dem Aspekt der Ortung besonders interessant ist der mobile Zugang zum Internet. Dabei wird ein mobiles Endgerät entweder über ein Mobilfunknetz (GSM, UMTS, siehe oben) oder über einen WLAN[6]-Zugangspunkt mit dem Internet verbunden.

---

2 GSM: Global System for Mobile Communications (früher Groupe Spécial Mobile, GSM)

3 UMTS: Universal Mobile Telecommunications System

4 HSPA(+): High Speed Packet Access, eine Erweiterung des UMTS, die höhere Datenübertragungsraten ermöglicht.

5 WWW: Das World Wide Web (WWW) ist eine Anwendung des Internet, die häufig irrtümlich mit dem Internet gleichgesetzt wird. Das Internet ist die Infrastruktur für den Datentransport, auf der das WWW, E-Mail-Dienste und viele weitere Anwendungen realisiert sind.

6 WLAN: Wireless Local Area Network. Der am weitesten verbreitete Standard für drahtlose lokale Computernetze. WLAN-Zugangspunkte (Basisstationen) werden für den mobilen Zugang

- Endgeräte: Die Miniaturisierung und rasche Diffusion digitaler Endgeräte (z.B. Laptops, Smartphones, digitale Foto- und Videokameras, Navigationssysteme, RFID-Leser usw.) mit zunehmender Leistungsfähigkeit und Interoperabilität schafft neue Zugänge zu digitalen Infrastrukturen. Immer mehr Alltagsgegenstände verbinden sich ohne Zutun ihres Nutzers mit dem Internet und tragen dazu bei, die Vision vom «Internet der Dinge» (ITU, 2005; Mattern, 2005) zu verwirklichen.
- Standards für die *drahtlose Kommunikation im Nahbereich:* Bluetooth, NFC[7], UWB[8] und weitere Funkstandards schaffen zusätzliche technische Möglichkeiten zum Datenaustausch auf kürzere Distanzen und damit indirekt auch zur Ortung von Objekten in ausreichend dichten Netzen.

Diese Entwicklungen führen zum Teil einzeln, vor allem aber in Kombination miteinander zu neuen Formen und Verfahren der Ortung, die aus der Sicht des Nutzers nicht als Hauptzwecke seines technischen Handelns, sondern als Nebeneffekt der digitalen Kommunikation auftreten.

Die Allgegenwart der Endgeräte und Netzzugänge, verbunden mit ihrer fortschreitenden Miniaturisierung und Einbettung in Alltagsgegenstände, machen es für den Einzelnen immer schwerer durchschaubar, welche Folgen seine Handlungen auslösen. Diese als «Ubiquitous Computing», «Pervasive Computing» oder «Ambient Intelligence» diskutierte Entwicklung wurde in ihrem Frühstadium bereits in einem Projekt des TA-SWISS behandelt (Hilty et al., 2003; Som et al., 2004). Eine weitere Studie des TA-SWISS befasste sich mit dem Dilemma zwischen Freiheit und Abhängigkeit durch die zunehmende digitale Automatisierung und Autonomisierung (Kündig & Bütschi, 2008). Beide Zukunftstrends werden heute greifbar in einem speziellen Segment der Entwicklung: die Ausstattung von Objekten mit einem «Sinn für den geographischen Raum» durch Ortungstechnologien.

Die vorliegende Studie konzentriert sich auf diesen speziellen Bereich und ihre gesellschaftlichen Auswirkungen. Dabei erscheint es uns wichtig, den Begriff

---

zu Firmennetzen und zum Internet eingerichtet. Wenn es sich um öffentliche Zugangspunkte zum Internet hadelt, werden sie auch als «Hotspots» bezeichnet.

7 NFC: Near Field Communication. Standard zur Übertragung von Daten zwischen Geräten über sehr kurze Distanz (typischerweise 10 cm oder weniger). Dazu werden die Geräte kurzzeitig aneinandergehalten, etwa um einen Bezahlvorgang auszulösen.

8 UWB: Ultra Wide Band, Ultrabreitband. Robuste Technologie zur Übertragung von Daten mit einer Reichweite von 10 m – 50 m, auch durch Wände hindurch.

der Ortung relativ weit zu fassen und auch die indirekten und asynchronen Formen der Ortung zu berücksichtigen, die erst durch die Digitalisierung ermöglicht wurden. Das breite Spektrum der Ortungsverfahren wird im folgenden Abschnitt dargestellt.

2.2 Kategorisierung von Ortungsverfahren

Ortungsdaten (auch: Standortdaten, Positionsdaten, Lokalisierungsdaten) können durch unterschiedliche Verfahren gewonnen werden, die wir im Folgenden grob kategorisieren. Ortungs*verfahren* jeder Kategorie können prinzipiell mit verschiedenen *Technologien* oder auch unterschiedlichen Kombinationen von Technologien realisiert werden. Abbildung 1 (S. 13) zeigt die hier beschriebenen Verfahren im Überblick.

2.2.1 Selbstortung vs. Fremdortung

Von *Selbstortung* spricht man, wenn die Positionsdaten dort entstehen, wo sich das geortete Objekt selbst befindet. Ein Beispiel ist die klassische Schiffsnavigation.

Bei der *Fremdortung* dagegen fallen die Daten an einem anderen Ort an, und zwar in der Regel dort, wo sich ein Beobachter befindet, der sich für die Position des Objekts interessiert. Beispiele sind das Bodenradarverfahren, das die Position bewegter Objekte feststellt, oder die Ortung eines Mobiltelefons nach einem Diebstahl. Aber auch die Eingrenzung des geographischen Raumes, in dem eine bestimmte Internetadresse (IP-Adresse)[9] zu einem bestimmten Zeitpunkt zum Zugriff auf das Internet verwendet wurde, kann als Fremdortung betrachtet werden. Beispielsweise könnte die Tatsache, dass auf ein E-Mail-Konto zeitnah von zwei weit auseinanderliegenden Orten aus zugegriffen wird, als Hinweis auf missbräuchliche Nutzung interpretiert werden.

Einige Autoren reservieren die Bezeichnung «Ortung» für die Fremdortung und bezeichnen die Selbstortung dagegen als «Positionsbestimmung». Heute

[9] IP: Internet Protocol. Siehe auch Abschnitt 2.3.9.

scheint sich «Ortung» als Oberbegriff jedoch durchgesetzt zu haben. Gelegentlich werden «Lokalisierung» oder auch «Geolokalisierung» als Synonyme verwendet.

Die Fremdortung unterscheidet sich in einem wesentlichen Aspekt von der Selbstortung: Sie ist in der Regel nur dann von Nutzen, wenn auch eine Möglichkeit zur *Identifikation* des georteten Objekts gegeben ist. Ein Punkt auf dem Radarschirm sagt wenig aus, wenn nicht wenigstens bekannt ist, ob es sich um Freund oder Feind handelt. Ein verlorener oder gestohlener Gegenstand kann nur sinnvoll geortet werden, wenn er eindeutig identifizierbar ist. Durch Auswertung von Videoaufzeichnungen verschiedener Kameras kann man eine Person nur orten, wenn man sie auf dem Bild identifizieren kann. Dass eine dynamisch vergebene IP-Adresse in einer bestimmten Region benutzt wurde, um im Internet eine strafbare Handlung zu begehen, führt auf die naheliegende Frage, *wer* diese Adresse zur Tatzeit benutzt hat.

Fremdortungsverfahren sind also aus prinzipiellen Gründen eng mit Identifikationsverfahren verbunden. Auch dies ist ein Grund, weshalb die Digitalisierung der Kommunikation (wie oben in Abschnitt 2.1 beschrieben) für die Ausweitung der Ortungsverfahren von zentraler Bedeutung war und ist, denn die Identifikation des Nutzers eines Endgeräts (Authentifizierung) ist in vielen Anwendungen zum Zweck der Autorisierung[10] und Leistungsabrechnung vorgesehen.

2.2.2 Direkte vs. indirekte Ortung

Mit Hilfe der digitalen Mobilfunkinfrastruktur ist es heute mit geringem Aufwand möglich, die von einem mobilen Objekt durch Selbstortung gewonnenen Positionsdaten weiterzugeben. Ein typisches Beispiel sind die GPS-Tracker, die heute u.a. zur Überwachung[11] von Kindern angeboten werden (z.B. «iNanny», Scheffel, 2009). Diese Geräte bestimmen die eigene Position durch Satellitenortung (GPS) und leiten die Positionsdaten über Mobilfunk (z.B. als SMS) an die Eltern oder andere Aufsichtspersonen weiter. Dadurch wird faktisch der

[10] Autorisierung bedeutet in diesem Zusammenhang das Einräumen von Rechten zum Zugriff auf Daten und Dienste.

[11] Wir verwenden einen wertneutralen Begriff der Überwachung. «Überwachung» ist in diesem Text gleichbedeutend mit dem englischen Wort «Monitoring».

gleiche Effekt wie bei einer Fremdortung erreicht, zumal die Details des technischen Vorgangs (Selbstortung plus Versenden der Daten) dem Benutzer verborgen bleiben. Wir bezeichnen diesen Fall deshalb als *indirekte Fremdortung*.

Ähnliche Verfahren finden im motorisierten Individualverkehr Anwendung. Das von der EU eingeführte Notrufsystem für Kraftfahrzeuge «eCall», das für Neuwagen in der EU Pflicht werden soll, sendet im Notfall die aktuellen GPS-Koordinaten über das Mobilfunknetz an eine Notrufzentrale.

Die Grenzen zwischen direkter und indirekter Fremdortung verwischen, wenn beide Seiten (das ortende und das geortete Gerät) an der Bestimmung der Position mitwirken. Das ist der Fall bei WLAN-basierten Technologien, wie sie beispielsweise zur Ortung von Mitarbeitern auf einem Betriebsgelände angeboten werden. Hier misst das mobile Endgerät nur die Feldstärken der WLAN-Basisstationen und übermittelt sie an eine zentrale Stelle, die daraus die Position berechnet (Zenz & Fritsche, 2009). Ähnliches gilt für neue Formen der akustischen Ortung von Mobiltelefonen (siehe Abschnitt 2.3.2).[12]

Es gibt auch den umgekehrten Fall, die *indirekte Selbstortung*. Dabei veranlasst ein mobiles Objekt eine Fremdortung und lässt sich das Ergebnis (also die eigene Position) von der ortenden Instanz mitteilen. Beispielsweise bieten einige Mobilfunk-Provider die Dienstleistung an, die Position eines Mobiltelefons zu bestimmen, um sie dann an eben dieses zu senden. Dieser Dienst ist ein Ersatz für eine «echte» Selbstortung (typischerweise über GPS) in Fällen, in denen das Endgerät dazu nicht in der Lage ist (T-Mobile, 2011).

Ähnliches leistet Googles Anwendung «My Location». Hier werden die vom Handy empfangenen Signale von Mobilfunk-Basisstationen zentral ausgewertet und die Positionsdaten an den Nutzer zurückgesendet, damit er sie in Google Maps verwenden kann.

[12] Wir kategorisieren solche Fälle im Zweifel als *indirekte* Fremdortung, weil sie ohne die Übertragung gemessener Daten vom georteten Objekt zur zentralen Stelle nicht funktionieren würden.

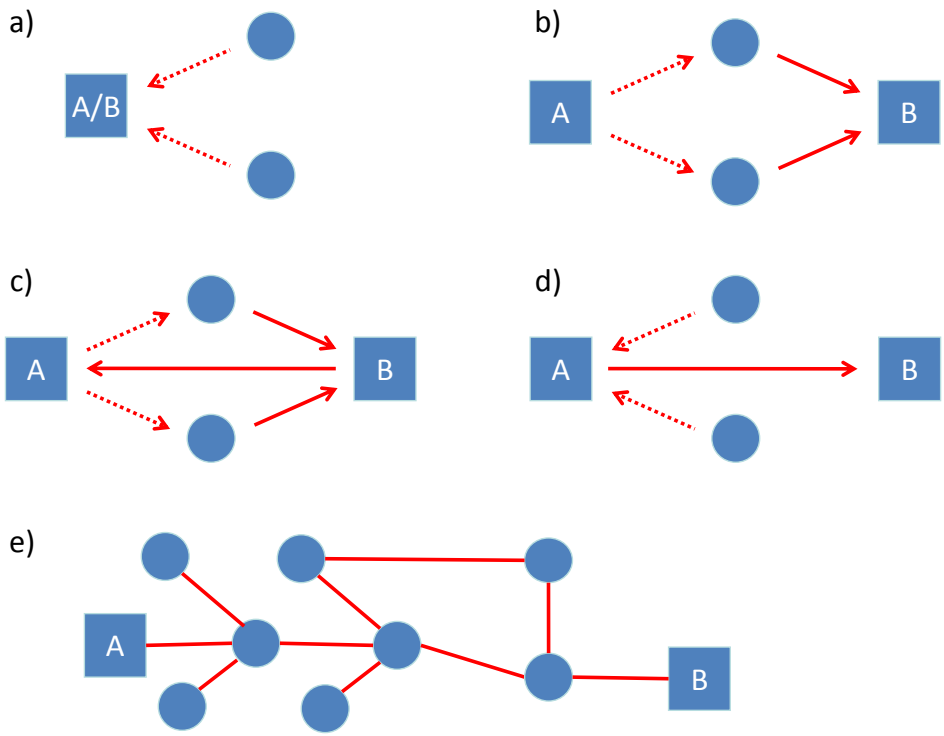


Abbildung 1: *Klassifikation von Ortungsverfahren*
Gestrichelte Linien: zur Ortung verwendete Signale; durchgezogene Linien: Datenfluss; A: geortete Instanz: B: ortende Instanz; Kreise: Sende-/Empfangsanlagen oder Netzknoten. Erläuterung der fünf Fälle siehe Text.

Abbildung 1 zeigt die grundlegenden Ortungsverfahren in schematischer Darstellung: a) direkte Selbstortung, b) direkte Fremdortung, c) indirekte Selbstortung, d) indirekte Fremdortung und e) die Netzwerkortung, die wir als Spezialfall der Fremdortung betrachten.

2.2.3 Synchrone vs. asynchrone Ortung

Im Fall der indirekten Ortung lässt sich weiter unterscheiden, ob die Positionsdaten zeitnah («in Echtzeit») oder erst nach einer Zwischenspeicherung an ihren Nutzer übermittelt werden. Soll beispielsweise die Fahrtroute eines Dienstwagens dokumentiert werden, so kann die aktuelle Position des Fahrzeugs entweder sofort via Mobilfunk an eine Zentrale übermittelt oder aber im Fahrzeug aufgezeichnet und erst später ausgelesen werden. Auch die als «Pay as you drive» bekannten Angebote von Autohaftpflichtversicherungen stützen sich auf die Aufzeichnung der gefahrenen Routen, die dann z.B. monatlich an den Versicherer zur Auswertung übertragen werden. Hierfür wird eine sog. Telematikbox oder Onboard-Unit in die Fahrzeuge eingebaut.

Die Unterscheidung zwischen synchronen und asynchronen Verfahren kann unter Aspekten des Datenschutzes relevant sein (vgl. Kapitel 3).

Tabelle 1: Kategorisierung von Ortungsverfahren und Beispiele

	Selbstortung	**Fremdortung**
direkt	Satellitenortung Selbstortung durch WLAN	Radar Handyortung durch Provider Ortung von IP-Adressen
indirekt, synchron	Handyortung durch Provider plus SMS an Subscriber Google «My Location»	Tracking von Fahrzeugen oder Personen durch GPS plus Mobilfunk in Echtzeit Ortung von Mitarbeitern durch WLAN
indirekt, asynchron	(keine relevanten Beispiele bekannt)	Telematikbox für Pay-as-you-drive-Versicherung Nebeneffekt digitaler Fotoarchive

Die asynchrone indirekte Ortung ist für diese Studie aus einem weiteren Grund von Bedeutung: Mit heutigen Technologien kann leicht eine unbeabsichtigte Ortung im Nachhinein stattfinden. Wenn jemand beispielsweise ein digitales Fotoarchiv anlegt, so ist ihm möglicherweise nicht bekannt, ob die Fotos von der Kamera mit einem sog. Geotag versehen wurden. Ist dies der Fall, gibt der Zugriff auf das Foto einem Betrachter die Möglichkeit, auf den exakten Aufenthaltsort der Kamera und folglich der gezeigten Personen zum Zeitpunkt der Aufnahme zurückzuschliessen. Es handelt sich in unserer Systematik um eine asynchrone, indirekte Fremdortung.

Tabelle 1 fasst die Ausführungen zur Kategorisierung von Ortungsverfahren zusammen.

2.3 Stand der Technik

Tabelle 2 gibt einen Überblick über aktuelle Technologien, mit denen die oben beschriebenen Ortungsverfahren realisiert werden können. Jede Technologie entspricht einer Zeile der Tabelle und ist in einem eigenen Abschnitt näher beschrieben (Abschnitte 2.3.1 bis 2.3.9). Wir beschränken uns hier auf Technologien, die im Zuge der Digitalisierung und Konvergenz von Informationsverarbeitung und Telekommunikation neu entstanden sind. Klassische Ortungstechnologien wie Radar, analoge Funknetze, Ultraschall- oder Infrarot-Ortung bleiben damit ausgespart.

Es ist zu beachten, dass nur wenige der in Tabelle 2 aufgeführten Technologien zum Zweck der Ortung von Objekten entwickelt wurden. In vielen Fällen tritt die Möglichkeit zur Ortung nur als Nebeneffekt der Kommunikation auf, so im Mobilfunk, bei der Nutzung von WiFi (WLAN), oder bei der stationären Internetnutzung.

Jede Ortungstechnologie arbeitet nach dem Prinzip, die *relative Lage* des zu ortenden Objekts zu einem oder mehreren *Referenzobjekten* zu ermitteln. Weil die Position des Referenzobjekts bekannt ist, kann daraus die absolute Position des zu ortenden Objekts im gemeinsamen Bezugssystem errechnet werden. Die Spalten «Gegebene Position» und «Ermittelte Position» in Tabelle 2 charakterisieren jede Technologie anhand dieser Merkmale.

Die angegebenen Genauigkeiten und Einschränkungen (vierte und fünfte Spalte) können sich mit der weiteren technischen Entwicklung verändern. Auch lassen sich durch *Kombination* mehrerer Ortungstechnologien oft höhere Genauigkeiten erzielen bzw. Einschränkungen überwinden.

Wie oben in Abschnitt 2.2.1 erläutert, stellt sich bei der Fremdortung unmittelbar die Frage der *Identifikation* der georteten Objekte. Die letzte Spalte von Tabelle 2 zeigt die jeweils aus technischer Sicht naheliegende Möglichkeit zur Identifikation des georteten Objekts. Die Nutzung weiterer Identifikationsmöglichkeiten ist aber nicht ausgeschlossen.

Die folgenden Abschnitte erläutern jede der aufgeführten Ortungstechnologien.

Tabelle 2: Aktuelle Ortungstechnologien und ihre Eigenschaften (Fortsetzung siehe nächste Seite)

Technologie	**gegebene Position**	**ermittelte Position**	**Genauigkeit**	**Einschränkungen**	**Identifikation**
Satellitenortung (GPS, Galileo)	Geostationäre Satelliten	Empfänger	ca. 10 m	Abschattung (Tunnels und Gebäude)	keine
Mobilfunk (GSM, UMTS)	Mobilfunk-Basisstationen (Sendemasten)	Mobilfunkgerät (Handy, GSM-Modul)	von 100 m in Ballungsräumen bis zu mehreren km auf d. Land	Abschattung, Funklöcher	SIM[13]-Karte
WLAN, Wireless Local Area Network	WLAN-Basisstationen	WLAN-fähiges Endgerät	theoretisch bis zu 1 m	Reichweite 40 m – 300 m	MAC[14]-Adresse

[13] SIM: Subscriber Identity Module. Die SIM-Karte dient zur Identifikation des Nutzers (Subscribers) eines Mobilfunkgeräts.

[14] MAC: Media Access Control. Die MAC-Adresse dient zur Identifikation eines Geräts in einem Computernetzwerk. MAC-Adressen können mit einfachen Mitteln manipuliert werden. Das Gerät bzw. sein Nutzer kann also gegenüber dem Netz eine falsche Identität vortäuschen.

UWB, Ultra Wide Band	UWB-fähige Geräte	UWB-fähiges Gerät	25 cm	Reichweite 10 m – 50 m	
Bluetooth	Bluetooth-fähige Geräte	Bluetooth-fähiges Gerät	entspricht Reichweite	Reichweite 1 m – 100 m	Bluetooth-Geräte-adresse
RFID, Radio Frequency Identification	RFID-Leser	RFID-Tag (Trans-ponder)	entspricht Lesedistanz (Engpass-ortung)	Lesedistanz 15 cm – 50 m für passive Tags	Seriennum mer des Chips oder ggf. EPC[15]
Akustische Ortung von Mobil-telefonen	Mobil-telefone oder Laut-sprecher	Mobiltelefon	1 cm – 2 cm	Reichweite 4 m – 10 m	SIM-Karte
Foto- und Video-kameras	Kamera	aufgenom-menes Objekt	begrenzt durch Genauigkeit der Kamera-position	Grenzen der inhalts-basierten Bildersuche (CBIR[16])	z.B. Erkennung von Gesich-tern und Nummern-schildern
Stationäre Internet-nutzung	Anschlüsse für Internet-zugang	dynamische IP-Adresse	Region; mit Verbin-dungsdaten bis Strasse/ Haus-nummer	genaue Ortung setzt Zugriff auf Verbin-dungsdaten voraus	z.B. ISP[17]-Kunden-nummer

2.3.1 Satellitenortung

Das heute weltweit am häufigsten eingesetzte Ortungssystem ist das Global Positioning System (GPS, offiziell: NAVSTAR GPS), das vom US-Verteidigungsministerium betrieben wird. Seit dem Jahr 2000 ist damit die Selbstortung durch GPS-Empfänger mit Genauigkeiten bis unter 10 m möglich. Die so

[15] EPC: Electronic Product Code. Standard zur weltweit eindeutigen Kennzeichnung von Produktexemplaren durch RFID.

[16] CBIR: Content-Based Image Retrieval. Bildbestände werden automatisch nach einem gegebenen Inhalt durchsucht, z.B. dem Gesicht einer bestimmten Person.

[17] ISP: Internet Service Provider. Anbieter von Internetdienstleistungen, insbesondere Internetzugang.

gewonnenen Positionsdaten kennt nur der GPS-Empfänger selbst, solange er sie nicht weiterleitet.

Neben der Selbstortung ist auch die indirekte Fremdortung durch Kombination mit Mobilfunk immer häufiger anzutreffen. Ein Mobiltelefon mit GPS-Empfänger oder ein spezielles Tracking-Gerät (bestehend aus GPS-Empfänger und GSM-Modul) kann die durch Satellitenortung ermittelte Position über das Mobilfunknetz weitergeben. Weil es sich um einen automatischen Vorgang handelt, kann dies grundsätzlich auch ohne Wissen des Trägers des Geräts erfolgen.

GPS-Empfänger sind wie zahlreiche andere Module stark miniaturisiert worden. Es gibt bereits SIM-Karten mit integriertem GPS-Empfänger (BlueSky Positioning, 2010). Dadurch werden Anwendungen mit indirekter Fremdortung in GPS-Genauigkeit auch für Handys ohne eingebauten GPS-Empfänger nachrüstbar.

Navigationssysteme mit GPS-Empfänger dienen in der Regel zur reinen Selbstortung. Einige Produkte können ihre aktuelle Position aber auch mittels GSM-Modul an eine zentrale Stelle melden, um Dienste wie Stauwarnung zu ermöglichen (TomTom, 2010).

Das europäische Galileo-Projekt dient zum Aufbau eines Systems ähnlich GPS und wird voraussichtlich 2015 in Betrieb gehen. Auch das russische System GLONASS, das wie GPS zivil nutzbar ist, könnte für kommerzielle Anwendungen an Bedeutung gewinnen. Ein wichtiger Vorteil von GLONASS und Galileo könnte in Zukunft darin bestehen, *in Kombination* mit GPS die Genauigkeit und Zuverlässigkeit der Ortung zu verbessern. Durch die dann insgesamt grössere Zahl von Satelliten lässt sich ein genaueres und verlässlicheres Ergebnis erzielen.

GPS-Empfänger lassen sich durch imitierte Satellitensignale täuschen. Mit entsprechender Ausrüstung kann ein «Spoofer» also Personen und Fahrzeuge, die sich auf Satellitenortung verlassen, in die Irre führen (Capkun, 2011).

2.3.2 Mobilfunk

Mobilfunknetze ermöglichen die Fremdortung der Endgeräte (z.B. Handys) aufgrund der Funkzelle, in der sie sich befinden. Ein Mobilfunk-Provider kann auf diese Weise jedes mit einer SIM-Karte versehene und eingeschaltete

Endgerät orten und darauf aufbauende Dienstleistungen anbieten. Weil die Ausdehnung einer Funkzelle bei GSM zwischen 100 m im Stadtgebiet und 35 km auf dem Land betragen kann, ist auch die Genauigkeit der Ortung sehr uneinheitlich. Wird die Laufzeit des Funksignals mitberücksichtigt, lässt sich die Genauigkeit grundsätzlich verbessern, jedoch gibt es Probleme mit reflektierten Signalen (Zogg, 2007; Bosien, 2008).

Verfeinerte Verfahren nutzen aus, dass sich ein Endgerät meist in Funkreichweite von mehreren Sendemasten befindet. Auch wenn nur ein Sendemast ausreichend nahe ist, um Telefongespräche in ausreichender Qualität zu ermöglichen, so können die Signalstärken mehrerer Masten ausreichen, um durch Triangulation die Position genauer zu bestimmen: «At any given time, a mobile phone is likely in signal range of upwards of three cell phone towers, allowing a location to be triangulated if the locations of the cell towers are known» (Tsai et al., 2010, S. 2).

Die Mobilfunk-Ortung kann prinzipiell als Fremd- oder Selbstortung durchgeführt werden, d.h. sowohl der Provider als auch das Mobilfunkgerät selbst können die Position bestimmen. Selbstortung setzt allerdings geeignete Software und den Zugriff auf ein Antennenkataster voraus, also eine Datenbank, die die Positionen der Antennenmasten verzeichnet (Bosien, 2008; Kettiger, 2010).

2.3.3 WLAN, Wireless Local Area Network

Wireless Local Area Networks (WLANs) dienen zur drahtlosen Verbindung von Computern und Peripheriegeräten. Dabei ermöglicht eine WLAN-Basisstation den drahtlosen Zugang zu einem lokalen Netzwerk (LAN). Eine immer dichtere Abdeckung mit solchen Basisstationen ermöglicht eine Sekundärnutzung dieser Technologie zur Ortung von Endgeräten. Die verwendeten Zugangspunkte müssen dabei nicht notwendigerweise zum öffentlichen Internetzugang dienen (sog. Hotspots); gerade die viel zahlreicheren privaten WLAN-Basisstationen sind für die Ortung nützlich, sofern ihre Standorte in entsprechenden Datenbanken verzeichnet und zugänglich sind. Eine WLAN-Basisstation kann auch zur Ortung verwendet werden, ohne dem Endgerät Netzzugang zu gewähren.

Ähnlich wie bei den Mobilfunknetzen kann hier durch Auswertung von Signalstärken oder -laufzeiten sowohl Selbst- als auch Fremdortung durchgeführt

werden. Ortbar sind alle WLAN-fähigen Geräte wie Laptops, Tablets oder Smartphones. Die Positionen der WLAN-Basisstationen müssen bekannt sein, damit die Position des mobilen Endgeräts relativ dazu bestimmt werden kann. Theoretisch kann damit eine Genauigkeit von 1–3 m erreicht werden (Retscher and Kealy, 2005). Praktisch stellt sich das Problem, dass die komplexe Feldstärkeverteilung durch Abschirmung, Reflexion und Beugung der Strahlung durch Wände und metallische Gegenstände beeinflusst wird, was die Genauigkeit stark herabsetzt. In Gebieten mit einer sehr hohen Dichte an WLAN-Basisstationen wird dieser Nachteil durch Redundanz wiederum ausgeglichen (Bosien, 2008).

Wie die GPS-Ortung so ist auch die WLAN-Ortung anfällig für technische Manipulation (Spoofing) (Capkun, 2011).

2.3.4 UWB, Ultra Wide Band

Ultra-Wide Band ist ein Funkstandard, der im Gegensatz zur herkömmlichen Nutzung von Funksignalen nicht auf der Modulation eines Trägersignals auf einer bestimmten Frequenz, sondern im Aussenden von Pulsen über ein breites Frequenzspektrum beruht. Diese Technologie ermöglicht eine Bestimmung der Position von UWB-Geräten mit einer Genauigkeit von ca. 25 cm auch unter erschwerten Bedingungen, z.B. durch Wände hindurch (Saeed et al., 2006).

Typische Anwendungen wie z.B. die Ortung von Feuerwehrleuten im Einsatz nutzen die entfernungsabhängigen Laufzeiten der Signale zwischen UWB-Geräten. Die Geräte bestimmen die Entfernungen zueinander und können diese einander mitteilen, so dass ihre Positionen durch Triangulation bestimmbar werden. Kennt eines der Geräte, z.B. dasjenige der Einsatzleitung, seine absolute Position (z.B. aus einem GPS-Empfänger), kann die Position aller Geräte berechnet werden.

2.3.5 Bluetooth

Bluetooth ist ein Standard für die Funkübertragung zwischen Geräten über kurze Distanzen. Die Verwendung als Ortungstechnologie beruht darauf, dass Bluetooth-fähige Geräte einander entdecken können, wenn diese sich in

Funkreichweite (typischerweise 10 m, je nach Geräteklasse) befinden. Durch den Aufbau eines zellularen Netzwerks mit Funkzellen von nur 20 m Durchmesser (auch «Piconet» genannt) mit Bluetooth-Geräten als Basisstationen kann die Bewegung anderer Geräte durch das Netz von Zelle zu Zelle verfolgt werden, was als «Bluetooth Tracking» bezeichnet wird. Die Identifikation ist anhand der Bluetooth-Geräteadresse möglich, die jedes Gerät weltweit eindeutig kennzeichnet (Herfurt & Mulliner, 2004; Hallberg et al., 2008).

Diese Technologie ist insofern von Bedeutung, als zahlreiche Geräte wie Handys und Laptops standardmässig über eine Bluetooth-Schnittstelle verfügen, teilweise ohne dass die Nutzer sich dessen bewusst sind. Diese Geräte sind in Piconetzen ortbar, sofern Bluetooth nicht ausgeschaltet wird. Die Bewegungen der Geräte können somit verfolgt werden, wo entsprechende Netze installiert sind. Dies wird auch als «Bluetooth Surveillance» bezeichnet (Fuller, 2008).

2.3.6 RFID, Radio Frequency Identification

Die Technologie der *Radio Frequency Identification* kann grob in Systeme mit aktiven und solche mit passiven Transpondern eingeteilt werden. Aktive Transponder verfügen über eine eigene Energiequelle und können über Distanzen geortet werden, die je nach Sendeleistung bis in die Grössenordnung von Kilometern reichen können. Dagegen werden passive Transponder vom Versorgungsfeld des Lesegeräts mit Energie versorgt, was nur über relativ kurze Distanzen möglich ist (siehe auch Oertel et al., 2005).

Aktive Transponder werden aufgrund ihres hohen Preises nicht für die Identifikation von Massengütern eingesetzt und sind deshalb nur für die Ortung von hochwertigen Objekten (Container, Geräte auf einem Fabrikgelände) und von Personen von Bedeutung. Die Australische Firma Electro-Com bietet ein entsprechendes «Asset and Personnel Tracking System» namens AXCESS an, das unter anderem in Krankenhäusern und in Gefängnissen eingesetzt wird.[18]

Die folgenden Ausführungen beziehen sich auf Systeme mit passiven RFID-Transpondern, die bereits milliardenfach im Einsatz sind. Sofern sie Konsum-

[18] http://www.ferret.com.au/c/Electro-Com-Australia/Asset-and-personnel-tracking-system-from-Electro-Com-n674030

güter kennzeichnen, werden sie in den publizistischen Medien teilweise als «Funkchips» oder «intelligente Etiketten» bezeichnet. In diesen Fällen werden die zu identifizierenden Objekte mit einem billigen passiven Transponder (auch Tag genannt) ausgestattet und können dann von einem RFID-Lesegerät berührungslos und ohne Sichtverbindung identifiziert werden. Letzteres ist der Vorteil gegenüber dem Barcode. Ausserdem können beim Auslesevorgang mehr Daten übermittelt werden als beim Ablesen eines Barcodes. Dadurch wird eine weltweit eindeutige Identifizierung der Tags möglich (Oertel et al., 2005).

Passive RFID-Systeme können nur für eine eingeschränkte Form der Fremdortung genutzt werden. Ein Lesegerät kann nur feststellen, ob sich ein Tag überhaupt in Lesereichweite befindet. Praktisch muss der Tag dazu ein entsprechendes Gate passieren oder auch mit einem tragbaren Leser auf relativ kurze Distanz ausgelesen werden. Wenn die Position des Lesegeräts bekannt ist, ist dann – wegen der geringen Lesedistanz – auch die Position des identifizierten Tags bekannt. Um die Bewegung von Objekten mithilfe eines passiven RFID-Systems zu verfolgen, müssen Lesegeräte an Stellen aufgebaut werden (z.B. an Eingängen), die einen räumlichen Engpass für den Fluss von Objekten oder Personen bilden, also nicht umgangen werden können. Diese Form der Fremdortung wird deshalb auch als «Engpassortung» bezeichnet.

Ein zusätzlicher Aspekt ist die Möglichkeit, Lesevorgänge auf grössere Distanz mittels besonders empfindlicher Antennen *abzuhören*. Dieses «Belauschen» von RFID-Datenaustausch ist aus Entfernungen möglich, die ein Vielfaches der eigentlichen Lesedistanz betragen (Finke & Kelter, 2004). Dabei wird jedoch weiterhin vorausgesetzt, dass ein Lesegerät den Transponder aus der (kürzeren) Lesedistanz aktiviert. Auch unter der Annahme, dass jemand den Inhalt eines passiven RFID-Transponders mit hohem technischem Aufwand aus Distanz auszulesen versucht, bleibt es also beim Prinzip der Engpassortung.

RFID-basierte Zugangs- oder auch Zahlungssysteme können als Nebeneffekt die Erstellung von Bewegungsprofilen ermöglichen. Diese Profile sind umso detaillierter, je engmaschiger das Netz von Lesegeräten (installiert an überwachten Durchgängen, Automaten, Bezahlstationen usw.) geknüpft ist.

Umgekehrt können passive RFID-Transponder auch zur Selbstortung eines mobilen Lesegerätes eingesetzt werden. Dazu werden zahlreiche passive Transponder fest in die Infrastruktur integriert (z.B. in Boden, Wände oder Fahrwege). Das mobile Objekt (z.B. ein Roboter) ist mit einem mobilen RFID-

Leser ausgestattet, der nun aufgrund der Transponder, die er in seiner näheren Umgebung identifiziert, die eigene Position bestimmen kann.

2.3.7 Akustische Ortung von Mobiltelefonen

Mit der Verbreitung von Mobiltelefonen kommt auch die Nutzung akustischer Signale im hörbaren Frequenzbereich zur Ortung der Geräte in Betracht. Die akustische Ortungstechnologie setzt die Installation spezieller Anwendungsprogramme (Apps) auf den Handys voraus, die auf das Mikrofon zugreifen, auch wenn nicht telefoniert wird. Zwei Verfahren werden bisher diskutiert.

Das erste Verfahren beruht auf der relativen Ortung der Handys zueinander und lässt sich als reine Softwarelösung ohne zusätzliche Hardware oder Infrastruktur realisieren. Die Geräte tauschen untereinander Tonsignale (ähnlich Klingeltönen) aus. Aufgrund von Laufzeitdifferenzen kann die Entfernung berechnet werden. Mit einer «BeepBeep» genannten Anwendung können handelsübliche Handys nach Angaben seiner Entwickler ihren Abstand Position mit einer Genauigkeit von unter 2 cm bestimmen (Peng et al., 2007). Bei mehr als zwei Geräten lässt sich das Verfahren so erweitern, dass durch Datenübertragung und Triangulation relative Koordinaten berechnet werden können.

Das zweite Verfahren ist nur in einer kontrollierten Umgebung (wie einer Fabrikhalle oder einem Einkaufszentrum) realisierbar. Fest installierte Lautsprecher mit bekannter Position senden spezielle akustische Signale aus, die für die Software im Handy eindeutige Codes darstellen. Abhängig davon, welche dieser Signale mit welcher Laufzeitverzögerung das Mikrofon des Handys erreichen, kann das Handy seine Position berechnen und ohne Zutun seines Besitzers über das Mobilfunknetz weitermelden. Das «krypto-akustische» Signal kann so gestaltet werden, dass es vom menschlichen Zuhörer nicht bewusst wahrgenommen wird, obwohl es hörbar ist. Die in den USA bereits verbreitete Anwendung Shopkick[19] beruht auf dieser Technologie. Als Anreiz für das Installieren der Shopkick-App dient ein ausgefeiltes Rabattsystem (Hamann, 2010).

Aus technischer Sicht wäre es grundsätzlich möglich, derartige Software zum Belauschen von Gesprächen (auch in der Umgebung von unbenutzten Handys)

[19] http://www.shopkick.com

zu missbrauchen, da die Mikrofone der Handys ständig offen sind, d.h. ihr Signal laufend von der App verarbeitet wird.

2.3.8 Foto- und Videokameras

Die rasche Ausbreitung digitaler Foto- und Videokameras (u.a. als Bestandteil von Mobiltelefonen, als Webcams oder auch in Form von Überwachungskameras) zusammen mit der Verfügbarkeit von Bilddaten im Internet erhöht die Wahrscheinlichkeit, dass dadurch Aufenthaltsdaten von identifizierbaren Objekten und Personen erzeugt und verarbeitet werden.

Entscheidend hierfür sind gleichzeitige Fortschritte in zwei Technologiebereichen:

- Das sog. *Geotagging* von Foto- und Videoaufnahmen: Immer mehr Kameras statten digitale Aufnahmen direkt mit einem *Geotag* aus. Dies ist ein Metadatum, das die Position der Kamera zum Zeitpunkt der Aufnahme festhält. Sie wird i.d.R. mit einem eingebauten GPS-Empfänger festgestellt. Wenn das Foto oder Video anschliessend im Internet zugänglich gemacht wird, sind auch Ort und Zeit der Aufnahme öffentlich bekannt.
- Fortschritte in der *inhaltsbasierten Bildersuche (Content-Based Image Retrieval, CBIR):* Damit werden Verfahren bezeichnet, um Bildbestände mit Suchkriterien zu durchkämmen, die sich auf den Inhalt der Bilder beziehen, beispielsweise Gesichter bestimmter Personen oder Nummernschilder von Autos (Dimov et al., 2008).

Aufgrund der Kombination dieser beiden Entwicklungen werden auch private Fotosammlungen nachträglich zu Quellen von Positionsdaten. Sofern Objekte und Personen auf dem Bild identifiziert werden können, lässt sich anhand der Metadaten feststellen, wann sie sich wo aufgehalten haben.

Die beiden Technologiebereiche werden im Folgenden näher beschrieben.

Geotagging

Digitale Bilder enthalten mehr als Bilddaten. In den Metadaten sind zahlreiche weitere Informationen zum Bild abgelegt. Im EXIF-Bereich (Exchangeable

Image File Format) befinden sich technische Aufnahmedaten (z.B. Belichtungszeit, Blende, genutzte Kamera, Uhrzeit und Datum der Aufnahme). Im IPTC-Bereich (International Press Telecommunications Council) werden zudem Daten zum Bildinhalt untergebracht (z.B. Stichwörter, Daten des Urhebers und Kategorien). Als Geotag bezeichnet man die geographische Position des Aufnahmeorts, die ebenfalls als Metadatum abgespeichert werden kann. In den EXIF-Daten geschieht dies über Koordinaten, in den IPTC-Daten über den Ortsnamen.

Sollen nur wenige Bilder mit diesen Metadaten ausgestattet werden, ist auch eine manuelle Zuweisung des Aufnahmeortes per Karte möglich. Dies kann beispielsweise auf Online-Fotoseiten wie Locr, Flickr oder Panoramio erfolgen, oder aber mittels der Freeware GeoSetter vom eigenen PC aus. Effizienter ist die Bestimmung der Aufnahmeposition mittels GPS, sofern die Kamera über einen GPS-Empfänger verfügt. Firmen wie Sony, Panasonic und Samsung statten zunehmend nicht nur Profikameras, sondern auch Kompaktkameras für den Massenmarkt mit GPS aus (Schwindt, 2009).

Durch Geotags ist die Kameraposition in der digitalen Bilddatei festgehalten und bleibt zugänglich, sofern nicht aktiv Massnahmen dagegen ergriffen werden.

Inhaltsbasierte Bildersuche

Das Auffinden von Bildern nach Merkmalen der abgebildeten Inhalte zählt zu den schwierigen Problemen in der Informatik. Für das Thema der vorliegenden Studie ist primär die Suche nach bestimmten Gesichtern oder Nummernschildern relevant.

Wer seinen Namen in die Bildersuche von Google eingibt, bekommt jene Bilder zurück, in deren Kontext der Name als Text vorkommt, unabhängig davon, ob das eigene Gesicht auf dem Bild erscheint. Die Suche erfolgt also nicht *by content* (nach dem Inhalt), sondern *by context* (nach dem Zusammenhang). Deshalb werden auch Namensvettern gefunden oder Bilder, die keine Personen zeigen.

Obwohl grundlegende Probleme der inhaltsbasierten Bildersuche in der Informatik noch nicht gelöst sind, werden seit 1995 kommerzielle Softwareprodukte angeboten. Zu den ersten gehörte QBIR von IBM. Seither sind sowohl

die Forschung als auch die Zahl der kommerziellen Anwendungen im Bereich CBIR explodiert.

Suche nach Gesichtern

Die häufigste Form der Anfrage für die Bildersuche ist die Suche durch Beispiel (Query by Example). So kann man z.B. Fotoverwaltungs-Programmen wie iPhoto von Apple oder Picasa von Google ein Foto mit dem Namen einer darauf abgebildeten Person versehen. Das Programm versucht dann, andere Bilder der gleichen Person zu finden. Das Verfahren beruht auf Ähnlichkeitsmassen für Gesichter. Dass das Verfahren nur begrenzt funktioniert, ist daran zu erkennen, dass es häufig Fotos falscher Personen vorschlägt. Je mehr korrekte Fotos man aber dem System bestätigt hat, desto besser wird die Trefferquote, da die Menge der Beispiele zunimmt. Je grösser andererseits der zu durchsuchende Bildbestand ist, desto schlechter wird wiederum die erreichbare Trennschärfe. Dies ist ein prinzipielles Problem solcher Verfahren. Dennoch sollten die Möglichkeiten von CBIR zur Personenortung nicht unterschätzt werden (EDÖB, 2010).

Von CBIR zu unterscheiden ist die eigentliche *Gesichtserkennung (Face Recognition)*. Solche Verfahren dienen zur möglichst zuverlässigen Identifikation einzelner Personen und gehören zu den biometrischen Authentifizierungsverfahren wie z.B. die Fingerabdruck- oder Iriserkennung. Dazu wird die zu identifizierende Person unter möglichst kontrollierten Bedingungen mit einer hochauflösenden Kamera oder sogar einem speziellen, laserbasierten Gesichtsscanner aufgenommen. Die Zuverlässigkeit der besten Verfahren liegt heute über derjenigen der menschlichen Gesichtserkennung.

Biometrische Gesichtserkennungsverfahren sind nicht dazu gedacht, unter Tausenden oder Millionen von Bildern diejenigen aufzufinden, auf denen eine bestimmte Person abgebildet ist. Deshalb kann aus Fortschritten in der Gesichtserkennung nicht gefolgert werden, dass auch die Suche in Foto- oder Videobeständen mit ähnlich hoher Zuverlässigkeit möglich ist. Dennoch haben Verfahren der Gesichtserkennung auch die CBIR-Verfahren beeinflusst, insbesondere im Bereich der Auswertung von Videobildern von CCTV-Überwachungskameras. Im Projekt Pam-Face-Authentication wird die Entwicklung

eines «Pluggable Authentication Module (PAM)» zur Authentifizierung von Personen über einfache Webcams verfolgt.[20]

China setzt in Grossstädten wie Shenzhen auf flächendeckende Videoüberwachung in Kombination mit einer US-amerikanischen Software, die gesuchte Personen oder auch ungewöhnliches Verhalten automatisch erkennen soll (Bradsher, 2007).

Suche nach Fahrzeugnummern

Neben der Erkennung bestimmter Personen auf Bildern ist das automatische Lesen von Fahrzeugkennzeichen eine wichtige bildbasierte Ortungstechnologie. Die automatische Nummernschilderkennung (engl. Automatic Number Plate Recognition, ANPR) hat in den vergangenen Jahren Fortschritte gemacht, jedoch ist der Einsatz in der Verkehrsüberwachung nur dann ausreichend zuverlässig, wenn speziell zu diesem Zweck installierte Kameras verwendet werden, wie z.B. an Mautbrücken[21].

Auch bei der Erkennung von Nummernschildern ist die nachträgliche Durchforstung gegebener Bildbestände, die zu anderen Zwecken erstellt wurden (z.B. Urlaubsfotos), technisch gesehen die wesentlich grössere Herausforderung und stösst hinsichtlich der erreichbaren Trennschärfe an prinzipielle Grenzen.

2.3.9 Internetnutzung

Zur Nutzung des Internet benötigt das jeweilige Endgerät (z.B. ein privater PC) eine IP-Adresse. Statische IP-Adressen sind einem Gerät fest zugeteilt, dynamische Adressen werden abwechselnd den gerade aktiven Endgeräten zugeteilt. Jeder Internet Service Provider (ISP) hat einen festen Bereich von Adressen, die er vergeben darf. Deshalb lässt sich bei bekannter IP-Adresse das geographische Gebiet, in dem sich das Endgerät befinden muss, auf mehr oder weniger grosse Gebiete einschränken (etwa auf der Ebene von urbanen Regionen oder manchmal auch Stadtteilen).[22]

[20] http://pam-face-authentication.org/index.php
[21] Kontrollstellen, die zur automatischen Abrechnung von Verkehrsabgaben dienen.
[22] Beispielsweise mit Hilfe der IP-to-Country Database: http://ip-to-country.webhosting.info/

Um aber das Endgerät eindeutig zu ermitteln, über das die Internetnutzung stattgefunden hat, sind Verbindungsdaten notwendig, die nur der ISP kennt. In den meisten Ländern sind die ISPs verpflichtet, diese Daten für einen bestimmten Zeitraum (einige Monate) aufzubewahren und im Rahmen strafrechtlicher Ermittlungen entsprechende Auskünfte zu erteilen.

Weil Internet-Provider oder Netzwerk-Administratoren (bzw. die Strafverfolgungsbehörden) in der Regel das Endgerät identifizieren können, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war und weil damit indirekt der Nutzer oder zumindest Inhaber des Geräts bestimmt werden kann, gelten IP-Adressen nach EU-Recht als Personendaten (Weber & Schnyder, 2009). Zum Personenbezug von IP-Adresse vgl. auch Abschnitt 3.5.2.

2.3.10 Weitere Technologien

NFC, Near Field Communication

Near Field Communication ist ein Standard zum drahtlosen Datenaustausch über sehr kurze Entfernungen (unter 20 cm), der auf RFID-Standards aufbaut. Praktisch werden zwei NFC-fähige Geräte aneinandergehalten (gepaart) und können dann Daten austauschen. Im Gegensatz etwa zu Chipkarten mit RFID-Schnittstelle ist hier eine Zwei-Wege-Kommunikation möglich. Durch die guten Verschlüsselungsmöglichkeiten ist das bargeldlose Bezahlen eine wichtige Anwendung von NFC. Für viele Anwendungen ist NFC eine hinsichtlich der Datenübertragung leistungsfähigere und sicherere Alternative zu RFID.

Hinsichtlich Ortung verhält sich NFC ähnlich wie RFID: Es ist ausschliesslich eine Engpassortung möglich.

ZigBee

ZigBee ist ein Standard für Funknetze, mit dem sich Geräte über Entfernungen von 10 m – 100 m verbinden können. Er ist gedacht für Sensornetze, drahtlose Schalter und andere Anwendungen, wo batteriebetriebene Geräte in ein Netz eingebunden werden müssen und die Häufigkeit des Batteriewechsels so gering wie möglich gehalten werden muss. Zum Einsatz von ZigBee als

Ortungstechnologie gibt es Anwendungen, die den Einsatz von Geräten in einer kontrollierten Umgebung (z.B. in einem Krankenhaus) überwachen.

DSRC, Dedicated Short Range Communication

DSRC ist ein Funkstandard, der für die drahtlose Kommunikation im Bereich von 200 m – 1000 m gedacht ist und besonders im Strassenverkehr den Mobilfunk ergänzen soll, etwa zur Datenübertrage zwischen Strasse und Fahrzeug oder zwischen Fahrzeugen. DSRC unterstützt u.a. die Bildung von mobilen Ad-hoc-Netzen: Einander zuvor unbekannte «On-board Units» verschiedener Fahrzeuge können sich spontan zu Netzen zusammenschliessen, z.B. um Verkehrsinformationen weiterzugeben, ohne dass (wie im Mobilfunk) ein Netz von Basisstationen installiert sein muss. In Österreich und Norwegen ist DRSC für die Maut-Erfassung im Einsatz (Wessel, 2006).

Proprietäre Sensornetze

Proprietäre, also von ihrem Hersteller ohne Bezugnahme auf offene Standards definierte Sensornetze, werden für viele technische Anwendungen eingesetzt. Ein wichtiges Beispiel sind die drahtlosen Reifendrucksensoren, die in Autos zunehmend zur Überwachung des Reifendrucks eingesetzt werden. Die spezielle Technik überträgt die Daten über ein Funksignal vom rotierenden Reifen zu einem Empfänger im Auto. Als unbeabsichtigter Nebeneffekt ist dieses Signal bis zu einer Entfernung von 10 m – 40 m abhörbar und identifiziert das Fahrzeug eindeutig (Rouf et al., 2010).

2.4 Anwendungen

In diesem Abschnitt unternehmen wir einen Versuch, die vielfältigen Anwendungen der oben beschriebenen Ortungstechnologien grob zu charakterisieren. Jeder Anwendung werden wir jene Ortungsverfahren (aus Abschnitt 2.2) und Technologien (aus Abschnitt 2.3) zuordnen, die für die Realisierung der Anwendung geeignet sind. Wir hoffen, dass dadurch die Technologien anschaulicher und in ihrer gesellschaftlichen Bedeutung verständlicher werden.

Konkreter werden wir aber in den beiden Vertiefungsfeldern dieser Studie (*Mobilität* und *Soziale Netze*) auf Anwendungen eingehen (Kapitel 5 und 6).

Tabelle 3 zeigt die Eignung der Technologien für die verschiedenen Anwendungen, wie sie sich aufgrund der Fachliteratur heute darstellt. Jede Zeile der Tabelle entspricht einer Anwendung und wird in einem der folgenden Abschnitte näher erläutert.

Tabelle 3: *Eignung der Ortungstechnologien für die wichtigsten Anwendungen von Ortung.*
«X» bedeutet Eignung, «(X)» bedingte Eignung.

	Satelliten	Mobilfunk	WLAN	UWB	Bluetooth	RFID aktiv	RFID passiv	akustisch	Foto/Video	IP-Adressen	NFC	ZigBee	DRSC
Navigation	X		X										
Standortbezogene Dienste	X	X	X		(X)		(X)	X		X	X		
Mikromarketing	(X)		(X)		(X)		(X)	X	(X)	X	X		
Gebührenerhebung	X					X	X				(X)		X
Einzelüberwachung	X	(X)	X	X	(X)	X	X		(X)			(X)	
Massenüberwachung		X					X		(X)				X
Emergency Response	X	(X)	(X)	X									X
Dokumentation/ Beweissicherung	X	(X)	(X)						X	X			

2.4.1 Navigation

Navigation ist die klassische Anwendung von Ortungstechnologien. Durch die Satellitenortung hat sich die Zugänglichkeit der Navigationsdienste stark verändert. Die heutigen Navigationssysteme (meist für Fahrzeuge) beruhen auf der Selbstortung durch einen GPS-Empfänger und digitalen Karten, die entweder schon beim Kauf im Gerät gespeichert sind oder zu einem späteren Zeitpunkt erworben werden. Das Navigationssystem bestimmt laufend seine eigene geographische Position und kann diese dank der lokal vorhandenen Karten in einen für den Nutzer sinnvollen Kontext einbetten; insbesondere kann es die aktuelle Position und Bewegungsrichtung auf der Karte anzeigen und eine optimale Route zur gewünschten Destination errechnen.

Es handelt sich um eine reine Selbstortung, d.h. die durch Satellitenortung ermittelte Position kann nicht von einem Dritten eingesehen werden. Ausnahmen bilden Geräte, die beispielsweise zur Stauwarnung über Mobilfunk die eigene Position an eine Zentrale senden können, wie das bei den Navigationsgeräten des europäischen Marktführers TomTom der Fall ist (vgl. Abschnitt 2.3.1).

2.4.2 Standortbezogene Dienste

Standortbezogene Dienste (Location-Based Services, LBS) sind Dienste, die sich auf die aktuelle geographische Position ihres Nutzers beziehen. Typischerweise besteht der Dienst in der Bereitstellung einer ortsabhängigen Information über ein Mobiltelefon oder ein anderes Gerät (z.B. Laptop), das jeweils vom Dienstanbieter geortet werden kann.

Reaktive Dienste werden nur nach Aufforderung durch den Nutzer angeboten, *proaktive* Dienste reagieren auf Ereignisse wie z.B. das Betreten oder Verlassen einer bestimmten Zone.

Typische Beispiele für reaktive Dienste sind Informationsangebote wie Kinoprogramme, Hinweise auf Restaurants, Sehenswürdigkeiten oder auch Fahrpläne des öffentlichen Verkehrs, die entsprechend der aktuellen Position des Nutzers ausgewählt werden. In der Smartphone-App der Schweizerischen Bundesbahnen (SBB) gibt es beispielsweise die Funktion «Take me home», die ausgehend vom aktuellen Standort den schnellsten Weg zur Heimadresse ermittelt.

Zu den proaktiven Diensten gehören Werbehinweise auf Angebote in der aktuellen Umgebung, aber auch beispielsweise Notfalldienste. Ein mit einem entsprechenden Modul (GPS plus GSM) ausgestattetes Fahrzeug kann bei einem Unfall automatisch einen Notruf mit einer exakten Positionsangabe absetzen. Hierfür benötigen die Fahrzeuge Sensoren, um einen Notfall festzustellen (im Auto z.B. einen Beschleunigungssensor oder eine Verbindung zum Airbag-System), einen GPS-Empfänger und ein Kommunikationsmodul, um den Notruf über Mobilfunk abzusetzen. Gemäss der E-Call-Initiative der EU müssen Neuwagen demnächst mit einem einheitlichen Notrufsystem angeboten werden (s.a. Abschnitt 5.3.1).

Ein klar festzustellender Trend ist ferner die Erweiterung von Social-Network-Plattformen um standortbezogene Dienste. Facebook ermöglicht seinen mobilen Nutzern mit dem Dienst «Places», den eigenen Standort mit Freunden auszutauschen und gerade in der Nähe befindliche Freunde zu kontaktieren. Ausserdem werden ortsbezogene Informationen (z.B. Sonderangebote in den Läden der näheren Umgebung) an die Nutzer gesendet. Microsoft entwickelt den Dienst «Vine», mit dem man seine Kontakte dynamisch, d.h. abhängig vom eigenen Aufenthaltsort und dem seiner Kontaktpartner, organisieren kann und der in Notfällen Freunde in der Nähe alarmiert (McCarthy, 2009). Ortungsfunktionen im Kontext sozialer Netze werden in Kapitel 6 ausführlich behandelt.

Von «Near LBS» (NLBS) spricht man, wenn statt Mobilfunk Ortungstechnologien mit geringerer Reichweite eingesetzt werden. Dazu zählen z.B. WLAN, Bluetooth, RFID und die akustische Handyortung (vgl. Abschnitt 2.3).

Ein Spezialfall eines LBS liegt vor, wenn der Dienst hauptsächlich darin besteht, die Positionsdaten eines mobilen Endgeräts zu ermitteln und weiterzugeben. Ein Beispiel ist die Anwendung PeopleFinder, die dazu dient, den eigenen Standort einem ausgewählten Kreis automatisch mitzuteilen (Sadeh et al., 2008). Man spricht in diesem Fall auch von Location Sharing Systemen: «Location Sharing Systeme sind Location Based Services (LBS), deren ... Hauptzweck die Ermittlung, Auswertung, Darstellung und Weitergabe der Standortdaten des mobilen Endgeräts ist.» (Kettiger, 2010, S. 3).

2.4.3 Mikromarketing

Mikromarketing ist eine Form des Marketings, die sich auf sehr fein gegliederte Kundensegmente (bis hin zum einzelnen Kunden) bezieht. Beispielsweise werden Angebote nicht nur gezielt auf bestimmte demographische oder regionale Faktoren, sondern auf einzelne Kunden zugeschnitten. Im Extremfall wird das Verhalten des Kunden so detailliert analysiert, dass seine nächste Kaufentscheidung mit hoher Wahrscheinlichkeit vorhergesagt werden kann («behavioral targeting»; Hamann, 2010).

Mikromarketing ist durch die Beobachtung des Online-Verhaltens von Internetnutzern im grossen Stil praktikabel geworden und erlebt heute durch die standortbezogenen Dienste (siehe Abschnitt 2.4.2) einen weiteren Boom. Neu ist also die wechselseitige Verknüpfung von Mikromarketing mit LBS und weiteren Anwendungen von Ortungstechnologien. Wenn beispielsweise die akustische Handy-Ortung in Verkaufsräumen eingesetzt wird, so kann das Einkaufsverhalten auf den Zentimeter genau beobachtet werden, auch wenn keine Transaktionen erfolgen.

Grosse Unternehmen wie Adidas und Kraft planen nach einem Medienbericht in der New York Times *beobachtende Werbung*, bei der in digitalen Werbeplakaten Anwendungen zur sog. Publikumsanalyse integriert sind. Im November 2011 sollen Anwendungen in mehreren grossen US-amerikanischen Städten eine Anwendung der Firma «Immersive Labs» zum Einsatz kommen, die es dem Einzelhandel ermöglicht, Kunden vor einem Schaufenster nach Geschlecht, ungefährem Alter, Verweildauer und Aufmerksamkeit einzuschätzen und so eine Publikumsstatistik aufzubauen. NEC bietet eine Software an, mit der anhand von Videoaufzeichnungen ausgewertet werden kann, wann sich welche Zielgruppen beispielsweise in einem Einkaufszentrum aufhalten. In Deutschland entwickelte das Fraunhofer-Institut für Integrierte Schaltungen (IIS) das Softwareprodukt «Shore», das von Aufnahmen nicht nur auf Geschlecht und Alter, sondern durch Erkennung des Gesichtsausdrucks auch auf die Stimmung schliessen soll. Als Hinweise auf die Aufmerksamkeit der Personen werden beispielsweise Kopfhaltung oder Blickrichtung gedeutet. Die Anbieter von Anwendungen zur Publikumsanalyse verweisen darauf, dass mit derartigen Software-Lösungen keine Individuen identifiziert werden sollen. Sie bezeichnen die Verfahren daher nicht als Gesichtserkennung, sondern als Gesichtsdetektion (Lischka, 2011; Singer, 2011).

2.4.4 Gebührenerhebung

Überall, wo für den Aufenthalt in einem abgrenzbaren Gebiet oder für die Nutzung eines Verkehrsweges eine Gebühr erhoben wird, kann dies durch Ortungstechnologien automatisiert werden. Hierzu gehören Strassenbenutzungsgebühren (Road Pricing, Maut oder auch die Abrechnung von Leistungen im öffentlichen Verkehr).[23] Die technische Realisierung ist von den konkreten Anforderungen abhängig und reicht von RFID bis GPS.

In allen Fällen wäre aus rein technischer Sicht eine Selbstortung und eine Berechnung der gebührenrelevanten Kennzahlen beim Nutzer selbst möglich, sodass diese Systeme betrieben werden könnten, ohne dass der Nutzer seine Positionsdaten weitergibt. Die datenschutzrechtlich problematischere Realisierung als direkte Fremdortung (z.B. als Engpass-Ortung mit RFID) oder als indirekte Fremdortung (z.B. durch GPS plus Mobilfunk) ist dagegen besser gegen Manipulation durch den Nutzer gesichert und ermöglicht Sekundärnutzungen der Daten, z.B. für Statistiken. Die Fremdortung kann grundsätzlich auch durch eine *Trusted Third Party* geschehen, welche die Daten nur im Konfliktfall und nur mit Einwilligung des Nutzers an den Anbieter weitergibt.

Die technisch anspruchsvollste Anwendung ist die Autoversicherung mit dynamischen Prämien, die sich teils an dem vom Fahrer eingegangenen individuellen Risiko orientieren. Dieses Angebot ist auch als «Pay As You Drive (PAYD)» bekannt. Technisch basieren PAYD-Versicherungen auf der Erfassung und Auswertung der GPS-Koordinaten und der Daten weiterer Sensoren, die Aufschluss über Fahrleistung oder Fahrstil geben. Typischerweise werden die Daten in einer «On-Board Unit» (OBU) gespeichert, auch «Telematikbox» genannt, die im Fahrzeug installiert ist, und asynchron weitergegeben.

2.4.5 Einzelüberwachung

Direkte und indirekte Formen der synchronen Fremdortung ermöglichen die Verfolgung von Objekten im Raum und auch die Auslösung eines Alarms, wenn ein Objekt räumlich definierte Grenzen überschreitet.

[23] Die generelle Vision des «pay per use» («zahle nach Nutzung») lässt sich duch allgegenwärtige Informationsverarbeitung in vielen Gebieten verwirklichen, wo dies bisher nicht praktikabel war (vgl. Langheinrich et al., 2002).

Man spricht in solchen Fällen von einem *virtuellen Schutzzaun (engl. Geofence*). Sobald das ortbare Gerät die Grenze überschreitet, wird an zentraler Stelle ein Alarm ausgelöst. Will man bewegliche Objekte oder Personen überwachen, muss die Zuordnung zwischen dem ortbaren Gerät und dem zu überwachenden Objekt bzw. der Person sichergestellt werden. Im Falle der «elektronischen Fussfessel» geschieht dies, indem die Entfernung der Fessel auf mechanische Weise stark erschwert bzw. mit Sanktionen bedroht wird.

Elektronische Fussfesseln werden im Strafvollzug eingesetzt oder dienen auch zur Durchsetzung von Unterlassungsbefehlen, z.B. wenn ein Stalker verurteilt wurde, sich vom Wohnort einer Person fernzuhalten. Im ersten Fall umzäunt der *Geofence* ein Gebiet, das nicht verlassen werden darf, im zweiten Fall eines, das nicht betreten werden darf.

Ein virtueller Schutzzaun kann aber auch eingesetzt werden, um einen Alarm auszulösen, wenn Kinder oder Patienten ein definiertes Gebiet verlassen (Entführung, Verlaufen). Besonders bei Alzheimer-Patienten werden ortbare Armbänder eingesetzt, die das für die Patienten gefährliche «Wandern» verhindern sollen (Kuhn & Wilson, 2002).

Die Einführung von RFID-Tags für Schüler an einzelnen US-amerikanischen und britischen Schulen[24] hat eine öffentliche Diskussion ausgelöst, weil die Schulen nicht nur die Kontrolle der Anwesenheit im Unterricht, sondern auch Vorbeugung gegen Vandalismus und nicht offengelegte Zwecke damit verfolgten. Als in einem Fall bekannt wurde, dass die Schule ein Abkommen mit dem Anbieter des RFID-Systems geschlossen hatte, der das Projekt zur Werbung für seine Produkte nutzen und die Schule am Erfolg zukünftiger Verkäufe beteiligen wollte, protestierten die Eltern (Zetter, 2005; Roberti, 2010).

Wenn ein zu überwachendes Gebiet auch physisch umzäunt ist, so genügt eine Engpassortung (z.B. mit passiven RFID-Transpondern), um den gewünschten Überwachungseffekt zu erreichen. Der Vorteil der Technologien mit grösseren Reichweiten besteht indessen gerade darin, dass kein physisches Einsperren nötig ist und die Grenzen des erlaubten Gebietes flexibel und individuell definiert werden können.

[24] Die Tags müssen um den Hals getragen werden oder sind in die Schuluniform integriert.

In Shenzen, China, werden die Zugezogenen mit einer Kombination aus biometrischen RFID-Pässen, einem Netz von Lesegeräten und 20 000 Videokameras mit Gesichtserkennung überwacht (Theissen, 2009).

Im Rahmen eines von der EU geförderten Modellprojekts wird auf dem ungarischen Flughafen Debrecen jeder einzelne Fluggast mittels einer Kombination aus aktiver RFID-Technik und hochauflösenden Videokameras überwacht. Dieses «opTag» genannte System soll Verspätungen reduzieren, aber auch verhindern, dass Fluggäste unbemerkt ihre Bordkarten tauschen (Theissen, 2009).

2.4.6 Schwarmüberwachung

Eine andere Ebene der Anwendung von Ortungstechnologien wird betreten, wenn nicht mehr einzelne Objekte oder Personen, sondern grössere Ansammlungen beispielsweise von Konsumgütern, Fahrzeugen oder Menschen überwacht werden. Dies erfordert nicht die Identifikation der georteten Personen, da das Interesse nur dem «Schwarmverhalten» gilt. Die biologische Metapher des Schwarms ist in diesem Kontext allgemein üblich.

Beispielsweise kann allein aufgrund der Tatsache, dass sich viele Mobiltelefone mit einer sehr geringen Geschwindigkeit in eine Richtung bewegen, ein Verkehrsstau vermutet werden. Die Bewegungen von Personen können in 93% der Zeit zutreffend vorhergesagt werden (Johnston, 2010).

Navigationsgeräte eignen sich ebenfalls zur Schwarmüberwachung, wenn sie mit einem GSM-Modul ausgestattet sind. Die verbreiteten TomTom-Navigationsgeräte verfügen über diese Funktion, die z.B. bei der Erkennung von Verkehrsstaus hilft. Auf Protest stiess in Holland der Verkauf von Verkehrsdaten aus TomTom-Navigationsgeräten an die Polizei, die damit die Aufstellung von Radarfallen optimierte (ZEIT, 2011). G. Karjoth weist darauf hin, dass hier nur anonymisierte Daten verwendet wurden (Auswertung des Schwarmverhaltens), sich die unerwartete Sekundärnutzung aber dennoch gegen das subjektive Interesse des Einzelnen richten kann (Karjoth, 2011).

Grundsätzlich kann die direkte Fremdortung von Mobiltelefonen (Funkzellenabfrage) auch bei Grossveranstaltungen wie z.B. Sportveranstaltungen oder Demonstrationen[25] genutzt werden. Allerdings setzt diese Form der Überwachung die Kooperation der Betroffenen voraus, denn ausgeschaltete Mobiltelefone existieren für die Sendemasten nicht.

2.4.7 Emergency Response

Naturkatastrophen und Krisen erfordern die lokale Koordination von Rettungsmassnahmen. Zu diesem Zweck werden vermehrt «Emergency Response Systems» (ERS) eingesetzt, die Entscheidungsträger unterstützen, um die Folgen einer Katastrophe zu minimieren (Wex et al., 2010).

Ein Aspekt der ERS ist die Ortung der Rettungskräfte, die sich oft nicht auf funktionsfähige Infrastrukturen stützen kann. Deshalb sind hier Technologien wie UWB und DRSC, die kein Netzwerk von Basisstationen erfordern, in Verbindung mit GPS besonders geeignet.

2.4.8 Dokumentation und Beweissicherung

Firmen und Privatpersonen verwenden aufgezeichnete Positionsdaten häufig zu Dokumentationszwecken. Mit GPS aufgezeichnete Routen dienen zur Abrechnung von Reisespesen und als Beleg für die Ausführung von Aufträgen (hierfür gibt es z.B. sog. *Tracksticks* mit USB-Anschluss).

Technische Aufnahmen (z.B. im Baugewerbe) und auch private Fotos werden immer häufiger mit Geotags versehen und ermöglichen dadurch die zuverlässige Dokumentation von mobilen Einsätzen bzw. von Reiserouten.

Der Übergang von der asynchronen Selbst- zur Fremdortung ist leicht möglich. Werden private Aufnahmen Dritten zugänglich, lassen sie Sekundärnutzungen im Mikromarketing zu. Sie können auch als Grundlage für kriminelle Handlungen missbraucht werden (Einbruch, Erpressung oder Identitätsdiebstahl).

[25] Wie in Deutschland geschehen (Die Wochenzeitung, 2011)

Auf der anderen Seite dient die asynchrone Fremdortung aber auch zur Beweissicherung in der Strafverfolgung. Grosse Datenmengen mit Ortsbezug werden aus Video-Überwachungskameras sowie in Form von Mobilfunk- oder Internet-Verbindungsdaten aufbewahrt, um im Rahmen eines Ermittlungsverfahrens Hinweise auf Tat oder Täter zu liefern.

Unfreiwillig haben iPhone-Nutzer ihre Aufenthaltsorte unverschlüsselt auf dem Gerät gespeichert, so dass ein Dritter leicht darauf zugreifen könnte (Alasdair & Warden, 2011; vgl. auch Abschnitt 4.1.1).

2.5 Auswertung im Kontext vorhandener Geodaten

Als Geodaten bezeichnet man «raumbezogene Daten, die mit einem bestimmten Zeitbezug die Ausdehnung und Eigenschaften bestimmter Räume und Objekte beschreiben, insbesondere deren Lage, Beschaffenheit, Nutzung und Rechtsverhältnisse» (Art. 3 Abs. 1 lit. a GeoIG). Karten sind Sammlungen von Geodaten, da sie die Standorte zahlreicher Objekte und die Lage von Gebieten kennzeichnen.

Die Daten, die als Ergebnis einer Ortung (Lokalisierung) entstehen und die üblicherweise als Positionsdaten oder Standortdaten bezeichnet werden, sind ebenfalls Geodaten. Sie unterschieden sich von den kartographischen Geodaten nur dadurch, dass sie sich in der Regel auf bewegliche Objekte beziehen und deshalb in kürzeren Zeitabständen aktualisiert werden müssen.

Erst durch die Verknüpfung der Positionsdaten mit kartographischen Geodaten in einem gemeinsamen Bezugssystem entsteht eine nutzbare Information. Beispielsweise muss ein Navigationsgerät die eigene Position mit einer digitalen Karte verknüpfen, um seine Funktion erfüllen zu können. Die eigene Position ohne Karte oder die Karte ohne Möglichkeit zur Selbstortung würde offensichtlich keine Navigation ermöglichen.

Generell werden durch Ortung gewonnene Daten erst dann nutzbar, wenn sie im Kontext vorhandener Geodaten ausgewertet werden. Die Auswertungsmöglichkeiten nehmen durch zwei Entwicklungen laufend zu:

1. Die Weiterentwicklung der Ortungstechnologien selbst und die Diffusion ihrer vielfältigen Anwendungen, wie in den vorausgegangenen Abschnitten beschrieben.
2. Die zunehmende Verfügbarkeit von Geodaten in Form digitaler Karten. Dabei kann es sich um topographische oder – was weitere Auswertungsmöglichkeiten eröffnet – auch um thematische Karten handeln.

Schätzungen besagen, dass etwa 80% aller Daten einen Raumbezug besitzen und sich potenziell in Form von Karten darstellen lassen (Teege, 2001). Durch die immer bessere Zugänglichkeit auch thematischer Karten wird eine Auswertung von Standorten und Bewegungsprofilen immer interessanter, sei es für wirtschaftliche Zwecke oder im Zusammenhang mit der Überwachung von Personen.

Erst im entsprechenden Kontext wird eine Taxifahrt zu einem Klinikbesuch, eine Wohnadresse zu einem Hinweis auf die Einkommensklasse, eine Liegenschaft zu einem überschwemmungsgefährdeten Objekt, ein nächtlicher Aufenthalt zu einem Besuch im Rotlichtviertel. Der subjektiven Intepretation solcher Datenverknüpfungen sind keine Grenzen gesetzt. Wenn man sich vorstellt, dass solche Auswertungen regelmässig zu Entscheidungen führen, die für die Betroffenen nicht transparent sind (etwa bei einer Anstellung, der Gewährung eines Kreditrahmens, dem Abschluss einer Versicherung), lässt sich das Konfliktpotenzial dieser Entwicklung erahnen.

Die Grenze zwischen Sach- und Personendaten ist im Bereich der Geodaten fliessend. Es handelt sich zwar um Sachdaten, aber durch Kombination mit anderen Daten können häufig Personen bestimmt werden (NRC, 2010b). Beispielsweise enthalten Sachdaten über Gebäude indirekt auch Angaben über Eigentümer, Halter oder Nutzer (Weichert, 2009).

Für viele Anwendungen von Ortungstechnologien ist die Qualität des grundlegenden Kartenmaterials entscheidend für die Zuverlässigkeit der Dienste. Eine veraltete Karte in einem Navigationssystem verlängert die Wegedauer im Verkehr. Die Erstellung und Pflege digitaler Karten ist sehr aufwändig.

Wenn Standortdaten nicht in Form von Koordinaten vorliegen (sondern z.B. als Strassenadressen oder IP-Adressen), müssen sie geokodiert werden, damit sie mit anderen Geodaten verknüpfbar werden.

Lizensierbare digitale Karten für Geokodierungen sind MultiNet von TeleAtlas sowie NAVSTREETS von Navtech. Sie sind die konkurrierenden Systeme für High-End-Navigation, Verkehrstelematik, GIS/Online Mapping, Location Based Services und weisen deutliche Parallelen auf.

Google Maps oder Bing Maps (von Microsoft) haben sich als hochwertige und für viele Zwecke kostenlose Karten- und Navigationsanwendungen für Smartphones und andere Internetzugänge verbreitet. Das Kartenmaterial bildet die Plattform für Anwendungen zahlreicher Anbieter. Ebenfalls beruhen darauf Google Street View und Google Latitude mit der Möglichkeit, eine Historie der eigenen Positionsdaten zu erfassen («Google Standortverlauf»). Die Datenschutzbestimmungen von Google beinhalten dabei das Recht, dass standortbezogene Daten zur Bereitstellung und Verbesserung der Google-Services einschliesslich der Werbeprogramme gespeichert und verwendet werden können (Google, 2010).

OpenStreetMap ist ein Projekt mit dem Ziel, eine «freie Weltkarte» zu erstellen. Die Unterstützenden erarbeiten die Kartenbasis u.a. durch das Sammeln von GPS-Daten und durch Qualitätskontrolle. Die Daten werden sowohl als Karten als auch als Rohdaten bereitgestellt und können für beliebige Zwecke genutzt werden. Die Nutzung ist nach der Creative-Commons-Lizenz möglich. Aktuell (Herbst 2011) sind 500 000 Unterstützende registriert.[26]

[26] http://www.openstreetmap.de/

3 Rechtlicher Rahmen

3.1 Einleitung

Die Ortung von Personen, erfolge sie durch Private oder durch den Staat, wirft grundsätzliche datenschutzrechtliche Fragen auf, die im Folgenden erörtert werden. Dabei wird vorerst die grundlegende Bedeutung des Datenschutzes in der verfassungsrechtlichen Wertung dargelegt. Mit Blick auf mögliche künftige gesetzliche Restriktionen der Verwendung von Ortungstechnologien werden datenschutzrechtliche Wertungen mit verfassungsrechtlichen Ansprüchen auf Informations-, Kommunikations- und Wirtschaftsfreiheit kontrastiert.

Der Schutz vor Persönlichkeits- und Grundrechtsverletzung durch den Einsatz von Ortungstechnologien findet sich grundlegend in den Datenschutzerlassen des Bundes und der Kantone. Je nach angewendeter Technik und Einsatzbereich gelangen auch Datenschutzbestimmungen in anderen Gesetzen zur Anwendung. So regelt das Fernmeldegesetz (FMG) die fernmeldetechnische Übertragung von Informationen umfassend, insbesondere ist auch der Mobilfunk umfasst. Nach Art. 45 Abs. 2 FMG ist die Bearbeitung von Standortdaten über Abrechnungszwecke hinaus nur zulässig, wenn die betroffene Person in die Bearbeitung ausdrücklich einwilligt (Für Einzelheiten siehe Bondallaz, 2007, Rz 1435 ff.). Bezüglich Geodaten ist das Bundesgesetz über Geoinformation (GeoIG) zu beachten, das in Art. 11 GeoIG explizit auf die Anwendung des Bundesgesetzes über den Datenschutz (DSG) verweist.

Der Fokus wird im Folgenden auf das DSG gelegt. Anhand dessen wichtigster Prinzipien wird eine Art Folie entwickelt, die danach auf ausgewählte Anwendungsfelder von Ortungstechnologien gelegt werden kann. So kann geprüft werden, ob und inwieweit die heutigen gesetzlichen Regelungen des DSG erlauben, Persönlichkeits- und Grundrechtsverletzungen durch Ortungstechnologien angemessen zu bekämpfen oder, ob sich ergänzende Vorschriften aufdrängen. Bei dieser Würdigung sind die ebenfalls durch die Rechtsordnung geschützten Interessen am (möglichst ungehinderten) Einsatz der Ortungstechnologien einzubeziehen.

3.2 Die verfassungsrechtliche Ausgangslage

Der Schutz der Persönlichkeit und der Grundrechte bei der Datenbearbeitung hat einen hohen Stellenwert: Art. 13 Abs. 2 der Bundesverfassung (BV) gewährt ausdrücklich einen Anspruch auf Schutz vor Missbrauch persönlicher Daten[27] und einen Anspruch auf informationelle Selbstbestimmung[28]. Zudem verpflichtet sich die Schweiz auch im Rahmen von Art. 8 EMRK und des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarates (Europaratskonvention 108) zum Schutz der Persönlichkeit des Einzelnen vor missbräuchlicher Datenbearbeitung.

Das Recht auf informationelle Selbstbestimmung gewährt einer Person den Anspruch, selber zu bestimmen, wem und weshalb sie persönliche Lebenssachverhalte, Gedanken, Empfindungen oder Emotionen offenbart. Die informationelle Selbstbestimmung als Teil des verfassungsrechtlichen und privatrechtlichen Persönlichkeitsschutzes ist eine zentrale Voraussetzung einer liberalen Gesellschaft auf der Grundlage personaler Autonomie. Der demokratische Rechtsstaat ist auf Bürgerinnen und Bürger angewiesen, die ihren Anspruch auf informationelle Selbstbestimmung sowohl in horizontalen Verhältnissen als auch gegenüber dem Staat einfordern können (Aebi-Müller, 2005).

Der Anspruch auf informationelle Selbstbestimmung gilt deshalb nicht nur im Verhältnis der Privaten zum Staat; dem Staat kommt im Rahmen grundrechtlicher Schutzpflichten vielmehr die Verpflichtung zu, mit geeigneten Mitteln den Datenschutz auch in privatrechtlichen Verhältnissen zu verwirklichen (Schweizer, 2008, S. 326). Die missbräuchliche Bearbeitung von Personendaten im Zusammenhang mit den in Art. 8 Abs. 2 BV aufgeführten Merkmalen wie Rasse, soziale Stellung, Behinderung, Weltanschauung, politische Überzeugung kann für die betroffenen Personen zu Stigmatisierung und Diskrimi-

[27] Der Wortlaut der Bestimmung ist zu eng. Es geht nicht nur um Missbrauchsschutz sondern ganz generell um den Anspruch, darüber informiert zu sein, wer wann und mit welcher Legitimation über die eigene Person Daten bearbeitet, siehe dazu Schweizer, N 39 ff. zur Art. 13 BV, in: Rosenthal/Yöri, N 4 zu Art. 1 DSG.

[28] Zur bundesgerichtlichen Rechtsprechung zum Recht auf informationelle Selbstbestimmung siehe BGE 113 Ia, 5; BGE 120 II 118, Erw. 3a; BGE 130 III, Erw. 4.2.

nierung führen. Dem Datenschutz kommt auch eine Diskriminierungsschutzfunktion zu (Pärli, 2009, 117; 543). [29]

Im Zusammenhang mit der (technisch) zunehmend einfacheren Ortung von Personen stellt sich die Frage nach einem grundrechtlichen Anspruch auf Anonymität. Für ein eigenständiges, ungeschriebenes Grundrecht auf Anonymität besteht keine Notwendigkeit. Das Recht auf Anonymität, auf Selbstbestimmung bezüglich der eigenen Personendaten, lässt sich aus dem Grundrecht auf informationelle Selbstbestimmung ableiten (Rudin, 2008).

Die Ortung von Personen berührt auch den grundrechtlichen Anspruch auf persönliche Freiheit (Art. 10 BV) und den Anspruch auf Achtung des Privatlebens und – in gewissen Konstellationen – den Schutz des Fernmeldegeheimnisses (Art. 13 Abs. 1 BV). Die Ungewissheit um die jederzeit mögliche Ortung und ungehinderte Verbreitung dieser Information an nicht abschliessend bekannte Empfänger beeinträchtigt die freie Entfaltung. Persönliche und telefonische Überwachungsmassnahmen stellen Eingriffe in das Privatleben dar (BGE 125 I 46).

Eine weitere Grundrechtsgefährdung erfolgt durch die zeitlich unbeschränkte Veröffentlichung von z.B. durch Personenortung gewonnener Daten im Internet. Bruno Baeriswyl, der Datenschutzbeauftragte des Kantons Zürich, fasst die Problematik prägnant unter dem Titel «Das Internet vergisst nicht» zusammen (DSB Kanton Zürich, 2008, S. 6). Selbst Informationen, die mit der Einwilligung der betroffenen Person publik gemacht wurden, können zu einem späteren Zeitpunkt «informationsunwürdig» werden. Das Interesse der Öffentlichkeit an diesen Informationen besteht nicht mehr und eine erneute (oder weiterhin bestehende) Veröffentlichung kann die Person stark beeinträchtigen. Im Kern des Problems liegt dabei die Bestimmung der Tragweite einer Einwilligung nach Art. 13 Abs 1 DSG.[30] Das aktuelle Datenschutzrecht scheint in Anbetracht dieser Herausforderungen lückenhaft (Weber, 2011, S. 103). Der Eidgenössische Daten- und Öffentlichkeitsschutzbeauftragte und die EU-Kommission fordern

[29] Das zeigt sich auch dadurch, dass im Bundesgesetz über den Datenschutz (DSG) bestimmte Daten wie solche über die Intimsphäre, die Gesundheit, die Religion oder Rasse als besonders schützenswert eingestuft werden (Art. 3 lit. c, Ziff. 1-4 DSG).

[30] Erwähnt wird das «Stacy Snyder Beispiel»: Stacy Snyder stellt ein Bild von sich auf ihre MySpace Seite, welches sie mit einem Piratenhut und alkoholtrinkend an einer Party zeigte. Bei einer späteren Bewerbung wird sie nicht berücksichtigt, da der potenzielle Arbeitgeber dieses Bild gesehen hat. Es stellte sich danach die Frage, ob Stacy die Einwilligung zur Verwendung in einem Bewerbungsgespräch gegeben hatte.

daher gestützt auf einen grundrechtlich begründbaren Anspruch auf Vergessen mehr Rechte für die Internetbenutzer/innen auf Löschung ihrer Personendaten (Thür, 2006; EU-Kommission, 2010). Weber (2011) fügt an, dass ein neues Grundrecht lediglich einen datenschutzrechtlichen Gewinn bringt, falls dessen Umsetzung in einem konkreten (individuellen) Anspruchssystem gelingt. Er kritisiert die bisherigen Bestrebungen auf EU-Ebene als vage und als Beschränkung auf ein moralisches Postulat. Den Betroffenen soll also eine Art «digital eraser» in die Hand gelegt werden (Weber, 2011).

Aufschlussreich zur Aufbewahrungsdauer von Personendaten ist auch das Urteil des Bundesgerichts vom 14. Dezember 2006 (BGE 133 I 77) zur Frage der zulässigen Dauer der Aufbewahrung von Vidoeaufnahmen aus der Überwachung von öffentlichen Plätzen und Strassen. Eine längere Aufbewahrungsdauer stelle bereits per se einen schwerwiegenden Eingriff in das nach Art. 13 Abs. 2 BV geschützte informationelle Selbstbestimmungsrecht dar und erhöhe die Gefahr einer missbräuchlichen Verwendung der Videoaufzeichnung (BGE 133 I 77, Erw. 5.3)[31]. Keinen Raum für ein «Recht auf Vergessen» sieht indes das Bundesverwaltungsgericht im Bereich der öffentlichen Handelsregisterdaten. Privaten Anbietern ist es demzufolge erlaubt, diese Daten unbeschränkt für eigene Plattformen zu verwenden (BVGE 2008/16)[32].

Sofern sich für bereits in der Verfassung niedergeschriebene Grundrechte durch technologische Innovation wie vorliegend im Bereich Ortungstechnologie neue Gefährdungspotenziale abzeichnen, sind die staatlichen Behörden gestützt auf die Pflicht zur Verwirklichung der (bestehenden) Grundrechte (Art. 35 BV) je in ihrem Kompetenzbereich (Gesetzgebung, Verwaltung, Gerichte) aufgerufen, *wirksam* für den Schutz der Personen vor missbräuchlicher Datenbearbeitung und vor ungerechtfertigten Eingriffen in die persönliche Freiheit und in das Privatleben zu sorgen. Soweit die Gefährdungen durch Private erfolgen, erfordert dies insbesondere Regelungen auf Gesetzesstufe, da die Grundrechte in ihrer *justiziablen* Schicht nur gegenüber staatlichen Eingriffen Wirkung entfalten. Nach Art. 35 Abs. 3 BV haben die Behörden dafür zu sorgen, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden. Der Gesetzgeber hat das Grundrecht auf Datenschutz und den grundrechtlichen Anspruch auf Schutz des Fernmeldeverkehrs im Datenschutzgesetz

[31] In casu erachtete das Bundesgericht indes die im Polizeireglement der Stadt Sankt Gallen vorgesehene Aufbewahrungsdauer von 100 Tagen als gerade noch zulässig.

[32] Zur Kritik an dieser Entscheidung siehe Baeriswyl (2009b).

(DSG) und im Fernmeldegesetz (FMG) konkretisiert (Schweizer, 2010, Rz 37 zu Art. 13 Abs. 2 BV; Kettiger, 2010, Rz 16).

Zu beachten ist, dass bestehende wie allfällige neue gesetzliche Regelungen zur Einschränkung des Einsatzes von Ortungstechnologien die ebenfalls grundrechtlich garantierten Freiheiten der Wirtschaftsteilnehmer/innen – sowohl der Produzenten/innen wie der Konsumenten/innen – tangieren. Wirtschaftsakteure haben gestützt auf die in Art. 27 BV verankerte Wirtschaftsfreiheit einen grundrechtlichen Anspruch auf Freiheit ökonomischer Entscheidungen (Hangartner, 1987, S. 127). Die mit Ortungstechnologien gewonnenen Informationen berühren weiter die Kommunikationsgrundrechte. So gewährt Art. 16 Abs. 3 BV das Recht, Informationen frei zu empfangen, aus allgemein zugänglichen Quellen zu beschaffen und zu verbreiten.[33]

Sowohl Entwicklung als auch Vermarktung, Verbreitung von Ortungstechnologien und die Nutzung der entsprechend gewonnenen Informationen sind grundrechtlich erfasst. Einschränkungen der Grundrechte haben folglich dem Eingriffsprogramm nach Art. 36 BV zu genügen: Einschränkungen müssen auf einer ausreichenden gesetzlichen Grundlage beruhen, im öffentlichen Interesse liegen oder den Schutz der Grundrechte Dritter bezwecken (Grundrechtskollision), verhältnismässig sein und dürfen den Kerngehalt des Grundrechts nicht verletzen.

Auch das in Art. 8 EMRK verankerte Recht auf Privatsphäre gilt nicht schrankenlos. Für den Europäischen Gerichtshof für Menschenrechte (EGMR) ist bzw. eine staatlich angeordnete GPS-Überwachung im Rahmen eines strafrechtlichen Ermittlungsverfahrens wegen schwerer Delikte zulässig. Die GPS-Überwachung ist nach Auffassung des EGMR im konkreten Fall durch legitime Ziele gerechtfertigt (Strafverfolgung) und im Sinne von Art. 8 Abs. 2 («in einer demokratischen Gesellschaft notwendig») auch verhältnismässig.[34]

[33] Im Kontext gesetzgeberischer Initiativen für Beschränkungen der Internetdienste im Interesse des Jugend-, Urheber-und Datenschutzes wird in einschlägigen Kreisen vermehrt ein Grundrecht «Freiheit der Internetdienste» gefordert, siehe dazu etwa die entsprechende Initiative der Professoren Holznagel und Schumacher (Holznagel & Schumacher, o.J.).

[34] EGMR, Urteil vom 2. September 2010, Beschwerde Nr. 35623/05, Bernhard Uzun gegen Deutschland. Einen Überblick über weitere Urteile des EGMR mit Bezug zum Datenschutz gibt das Themenblatt «Protection des données personelles» (EGMR, 2011).

3.3 Hintergrund und wichtigste Grundsätze des Bundesgesetzes über den Datenschutz (DSG)

Die Befürchtung über negative Auswirkungen der elektronischen Datenverarbeitung förderte die Entstehung des Bundesgesetzes über den Datenschutz (DSG)[35], das 1992 verabschiedet wurde, seit dem 01.07.1993 in Kraft ist und 2004, 2006 und 2010 teilrevidiert wurde.[36] Das DSG bezweckt den Schutz der Persönlichkeit und der Grundrechte der Personen, über die Daten bearbeitet werden (Art. 1 DSG). Bereits damit wird deutlich, dass das DSG sowohl die Datenbearbeitung im öffentlich-rechtlichen (Grundrechtsschutz) wie im privatrechtlichen Bereich (Persönlichkeitsschutz) regelt (Rosental & Jöhri, 2008, N 1 zu Art. 1 DSG).

Das DSG hält im 2. Abschnitt allgemeine Bestimmungen (Datenbearbeitungsgrundsätze) fest, die sowohl für Private wie Bundesorgane gelten (Art. 4 bis 11 DSG). Auf einzelne, im Zusammenhang mit Ortungstechnologien besonders wichtige Grundsätze wird nachfolgend näher eingegangen:

- Personendaten, d.h. Daten über eine bestimmte oder bestimmbare Person, dürfen vorab nur rechtmässig bearbeitet werden (Art. 4 Abs. 1 DSG) und diese Bearbeitung hat nach Treu und Glauben zu erfolgen (Art. 4 Abs. 2 DSG). Unrechtmässig ist eine Datenbeschaffung dann, wenn sie unter Verletzung von Rechtsnormen erfolgt. Eine Beschaffung wider Treu und Glauben liegt z.B. bei einer heimlichen Datenbeschaffung vor, ohne dass gegen eine Rechtsnorm verstossen wird.
- Zentral ist das Verhältnismässigkeitsgebot (Art. 4 Abs. 2 DSG): Personendaten dürfen nur soweit bearbeitet werden, wie dies für einen bestimmten Zweck objektiv betrachtet geeignet und tatsächlich erforderlich ist. Zudem muss die Datenbearbeitung mit Blick auf den Bearbeitungszweck und die Persönlichkeitsbeeinträchtigung in einem vernünftigen Verhältnis stehen (Maurer-Lambrou & Steiner, 2008, N 11 zu Art. 4 DSG). Daraus folgt auch

[35] Zur Entstehung des Datenschutzgesetzes siehe ausführlich: Seethaler (2008).

[36] Die Teilrevision vom 24. März 2006 steht im Zusammenhang mit der Ratifizierung des Zusatzprotokolls vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung. Die Änderungen vom 19. März 2010 stehen im Zusammenhang mit der Umsetzung des Rahmenbeschlusses 2008/977 über den Schutz von Personendaten der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.

der Grundsatz der Personendatenvermeidung: Es ist z.B. bei geokodierten Daten zu prüfen, ob der Datenbearbeitungszweck auch durch anonymisierte Daten zu realisieren ist (5. Tätigkeitsbericht EDÖB, S. 49 ff.). Unter Bezugnahme auf das Prüfschema der Verhältnismässigkeit setzte das Bundesgericht klare Schranken für den Einsatz eines GPS-Systems zur Überwachung der Einsätze von Mitarbeitenden. Im konkreten Fall erachtet das Bundesgericht den GPS-Einsatz einzig zum Zwecke der Qualitätskontrolle als verhältnismässig (BGE 130 II 245, Erw. 5).

- Der Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSG) besagt, dass Personendaten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde oder aus den Umständen ersichtlich ist. Im Bereich der Geodaten stellt diese Bestimmung eine besonders grosse Herausforderung dar. Die zunehmend einfachere Verknüpfung und Verkettung verändert den Bearbeitungszweck und verstärkt häufig die Bedrohung der Persönlichkeitsrechte (Weichert, 2009, S. 350). Die Verletzung des Zweckbindungsgebots macht eine Datenbearbeitung Privater widerrechtlich, soweit nicht ein Rechtfertigungsgrund nach Art. 13 DSG geltend gemacht werden kann.[37]
- Die in Art. 4 Abs. 4 DSG geforderte Erkennbarkeit der Datenbeschaffung bezweckt die Erhöhung der Transparenz für die betroffene Person; sie soll damit entscheiden können, ob sie sich der fraglichen Datenbearbeitung widersetzen will. Das Transparenzprinzip erfordert etwa bei den Street-View-Aktivitäten von Google sowohl eine Information der betroffenen Gebiete eine Woche vor den Aufnahmen als auch eine Information bevor die Bilder aufgeschaltet werden. Dabei genügt eine Information auf der Webseite von Google Maps nicht. Die Hinweise auf die geplanten Aufnahmeorte müssen auch in der lokalen Presse erfolgen (BVGer, A-7040/2009, E. 8.3.3 und Erw. 11). Google argumentierte gegen dieses Erfordernis, dass die Datenbeschaffung nur «erkennbar» sein müsse und heute «jeder der sich in er Öffentlichkeit bewege, mit Aufnahmen durch Behörden und Private»

[37] Mit der ersten DSG-Revision wurde in Art. 12 Abs. 2 lit. a der Vorbehalt der Rechtfertigungsmöglichkeit bei einer Datenbearbeitung entgegen den Grundsätzen der Art. 4 ff. DSG gestrichen. In der Literatur ist die Bedeutung dieser Streichung umstritten und die Materialien ergeben kein eindeutiges Ergebnis. Das Bundesgericht kommt in seinem Urteil vom 8. September 2010 zum Schluss, die Bestimmung sei so auszulegen, dass eine Rechtfertigung der Bearbeitung von Personendaten entgegen der Datenbearbeitungsgrundsätze zwar nicht generell ausgeschlossen sei, aber nur mit grosser Zurückhaltung angenommen werden dürfe (Bger v.8.9.2010, Urteil IC_285/2009, Erw. 5.2.4).

rechnen müsse (BVGer, A-7040/2009, E. 8.3.1; die Firma Google hat das Urteil an das Bundesgericht weitergezogen).

- Für die Bearbeitung von Persönlichkeitsprofilen und von besonders schützenswerten Personendaten gelten erhöhte Anforderungen an den Datenschutz.[38] So ist die Bekanntgabe an Dritte – z.B. die Publikation im Internet – nur bei Einwilligung der betroffenen Person erlaubt (Art. 12 Abs. 2 lit. c DSG). Art. 4 Abs. 5 DSG verlangt, dass die Einwilligung bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen ausdrücklich erfolgen muss. Art. 14 DSG verankert für den Inhaber einer Datensammlung[39] eine Informationspflicht beim Beschaffen besonders schützenswerter Personendaten. Private Datenbearbeiter müssen zudem Ihre Datensammlungen beim EDÖB anmelden, sofern sie regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten.[40]

  Ein *Persönlichkeitsprofil* liegt gemäss Art. 3 lit. d DSG vor, wenn die Zusammenstellung von Daten eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (siehe auch Kasten auf S. 49). Die Ortung von Personen bzw. das Zusammenführen von Sachdaten und Personendaten kann dazu führen, dass ein Persönlichkeitsprofil vorliegt (Probst, 2010, S. 6). Mit höheren Anforderungen an die Rechtmässigkeit der Bearbeitung von Persönlichkeitsprofilen und besonders schützenswerten Daten will der Gesetzgeber unterstreichen, dass gewisse Personendaten bzw. die Verdichtung von Personendaten zu einem Persönlichkeitsprofil offensichtlich geeignet sind, die Persönlichkeit und die Grundrechte mehr zu gefährden als eine Bearbeitung «gewöhnlicher» Personendaten. Zu ergänzen ist: Ob die Bearbeitung von Personendaten die Persönlichkeitsrechte beeinträchtigt, ist regelmässig nicht bloss von der Art der Personendaten sondern ebenso vom Bearbeitungskontext abhängig (Belser, 2006, N 10 zu Art. 3 DSG; Probst, 2010, S. 9). Wird der Aufenthaltsort einer Person geortet, z.B. der (zufällige) Aufenthalt einer bestimmten oder bestimmbaren Person in unmittelbarer Nähe einer Demonstration, handelt

[38] Besonders schützenswerte Personendaten sind gemäss Definition in Art. 3 lit. c Ziff. 1-4 DSG u.a. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, über die Gesundheit oder die Intimsphäre.

[39] Art. 3 lit. g DSG d

[40] Nach Art. 11a Abs. 5 lit. e und f DSG können sich die Inhaber von Datensammlungen entweder durch Bezeichnung eines betrieblichen Datenschutzbeauftragten oder durch den Erwerb eines Datenschutzzertifikats (Vorschriften dazu in Art. 11 DSG) von der Registrierungspflicht befreien lassen.

es sich um besonders schützenswerte Personendaten (es sind Daten über die – tatsächliche oder vermeintliche – politische Gesinnung bzw. Aktivität).

Persönlichkeitsprofile

Ein Persönlichkeitsprofil ist eine Zusammenstellung von Daten über eine Person, die zusammen eine Beurteilung wesentlicher Aspekte der Persönlichkeit erlauben.

Beispiel 1: Einkaufsdaten, die mit Kundenkarten gesammelt werden, bilden ein Persönlichkeitsprofil. Obwohl ein einzelner Einkauf nicht viel über eine Person aussagt, lassen Daten über ihre regelmässigen Einkäufe Rückschlüsse auf die Lebenssituation zu (Singlehaushalt oder Partnerschaft? Hobbies? Vorlieben? Krankheiten? ...).

Beispiel 2: Das von der Firma Bodymedia angebotene Sensoren-Armband speichert 5000 Messwerte pro Minute auf einem Server zu dem Zweck, eine gesündere Lebensführung zu unterstützen. Auch diese Daten bilden Persönlichkeitsprofile (siehe Abbildung; Bildquelle: www.bodymedia.com).

- Art. 5 DSG verankert den Grundsatz der Datenrichtigkeit; wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Diese Bestimmung kann eine Rolle spielen, wenn durch Ortung gewonnene und verbundene Personendaten ein Bild vermitteln, das den tatsächlichen Verhältnissen nicht entspricht (z.B. werden Daten einer falschen Person zugeordnet). Art. 5 Abs. 1 verlangt vom Datenbearbeiter angemessene Massnahmen zur Berichtigung oder Vernichtung solcher Daten. Nach Art. 5 Abs. 2 DSG hat die betroffene Person überdies einen Anspruch auf Berichtigung unrichtiger Daten.
- Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSG). Zweck dieser in der Verordnung zum DSG konkretisierten[41] Norm ist die Verhinderung der unbefugten Datenbearbeitung (Rosenthal & Jöhri, 2008, Rz 7 zu Art. 7 DSG).

Während die Datenbearbeitungsgrundsätze sowohl für Private wie für Bundesorgane gelten, beurteilt sich die weitere Rechtsmässigkeit einer Datenbearbeitung unterschiedlich. *Für Private* ist die Datenbearbeitung zulässig, soweit sie im Rahmen der Datenbearbeitungsgrundsätze erfolgt bzw. ein Rechtfertigungsgrund geltend gemacht werden kann. Als Rechtfertigungsgründe nennt Art. 13 DSG die Einwilligung der Person, über die Daten bearbeitet werden, ein überwiegendes privates oder öffentliches Interesse oder ein Gesetz. Der Gesetzgeber hat mit der Revision des Datenschutzgesetzes im Jahre 2008 die Anforderungen an die Einwilligung erhöht (Art. 4 Abs. 5 DSG). Zu beachten gilt es insbesondere das Erfordernis der ausdrücklichen Einwilligung bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen. Die Datenbearbeitung *durch Organe des Bundes* ist nur zulässig, wenn dafür eine gesetzliche Grundlage besteht (Art. 17 DSG). Als Beispiel dafür kann die Videoüberwachung im öffentlichen Verkehr angeführt werden. Der Gesetzgeber hat hier in Art. 55 des Personenbeförderungsgesetzes die gesetzliche Grundlage für die Überwachung geschaffen und deren Inhalt und Grenzen in den Grundzügen festgelegt.[42]

[41] Art. 8 ff. Verordnung zum Datenschutzgesetz (VDSG).

[42] Vorgesehen ist u.a., dass die Videodaten zwar aufbewahrt werden dürfen, jedoch vor Missbrauch zu schützen und spätestens nach 100 Tagen zu vernichten sind (Art. 55 Abs. 3 und 4 Personenförderungsgesetz). Weiter ist die Bekanntgabe des Datenmaterials nur an strafverfolgenden Behörden oder Behörden, bei denen die Unternehmen Anzeige erstatten oder Rechtsansprüche geltend machen, zulässig (Art. 55 Abs. 5 Personenförderungsgesetz).

3.4 Durchsetzung der datenschutzrechtlichen Ansprüche

In Art. 15 DSG sind die Rechtsansprüche betroffener Personen im Falle von Datenschutzverletzungen durch Private geregelt. Es wird dabei auf die Art. 28, 28a und 28 1 ZGB verwiesen und konkretisiert, die Ansprüche würden insbesondere die Sperrung der Bekanntgabe an Dritte, Vernichtung oder Berichtigung von Personendaten (Art. 15 Abs. 1 DSG), das Anbringen eines Bestreitungsvermerks (Art. 15 Abs. 2 DSG) und die Bekanntgabe der erwähnten Ansprüche (Art. 15 Abs. 3 DSG) betreffen. Mit dem Verweis auf Art. 28 ZGB wird deutlich, dass auch Schadenersatz- und Genugtuungsansprüche (letzteres bei Vorliegen einer schweren Persönlichkeitsverletzung) geltend gemacht werden können. In datenschutzrechtlichen Verfahren gegenüber Bundesbehörden räumt Art. 25 DSG den betroffenen Personen im Ergebnis gleiche Ansprüche ein.

Soweit ersichtlich werden die genannten Rechtsbehelfe kaum je in Anspruch genommen. Die spärlichen datenschutzrechtlichen Urteile weisen auf eine ganz grundsätzliche Problematik des Datenschutzes hin: Wer durch eine Datenbearbeitung widerrechtlich in seinen Persönlichkeitsrechten verletzt wird und eine entsprechende Klage einreichen will, riskiert, dass eine lieber geheim zu haltende Information erst recht weiteren Personen zugänglich wird. Die Wirksamkeit der datenschutzrechtlichen Rechtsbehelfe bilden Gegenstand der Evaluation des DSG, die vom Bundesamt für Justiz in Auftrag gegeben und im Dezember 2011 veröffentlicht wurde (EJPD, 2011b; Bundesrat, 2011).

Der Durchsetzung des DSG dienen indes nicht nur die individualrechtlichen Klagemöglichkeiten nach den Art. 15 und 25 DSG. Flankiert wird die Durchsetzung des Datenschutzes einerseits durch die Strafandrohungen in den Art. 34 und 35 DSG – die Tatbestände sind einerseits als Antragsdelikte (Art. 34 Abs. 1 und Art. 35 Abs. 1 DSG) und andererseits als Offizialdelikte (Art. 34 Abs. 2 und Art. 35 Abs. 2 DSG) ausgestaltet – und durch die Aufsichtstätigkeit des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Dieser kann Private in Datenschutzfragen beraten (Art. 28 DSG) und er kann von sich aus oder auf Meldung Privater nach Art. 29 DSG unter den dort aufgeführten Voraussetzungen Sachverhaltsabklärungen bezüglich möglicher Datenschutzverletzungen vornehmen. Gestützt auf seine Erkenntnisse kann er den Daten-

bearbeitern/innen Empfehlungen abgeben und wenn diese nicht akzeptiert werden, die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen. Dieses Vorgehen hat der EDÖB beispielsweise gegenüber Google bezüglich derer Street-View-Aktivitäten (vorerst) erfolgreich gewählt (BVGer. A-7040/2009; der Fall ist vor Bundesgericht hängig).[43]

Ein wichtiger Zusammenhang zu den Durchsetzungsrechten besteht im Auskunftsrecht, das in Art. 8 DSG verankert ist. Jede Person hat grundsätzlich das Recht zu erfahren, ob und welche Personendaten über sie angelegt und zu welchem Zweck verwendet werden. Zudem steht den Auskunftsberechtigten das Recht zu, ihre Angaben zu berichtigen oder löschen zu lassen. Das Auskunftsrecht soll gemäss dem Willen des Gesetzgebers die betroffenen Personen überhaupt erst in die Lage versetzen, die (weiteren) Durchsetzungsrechte nach DSG wahrnehmen zu können.[44] Über Klagen zur Durchsetzung des Aufsichtsrechts wird seit dem Inkrafttreten der eidgenössischen Zivilprozessordnung (ZPO) im vereinfachten Verfahren entschieden (Art. 15 Abs. 4 DSG).

Zur Durchsetzung des DSG innerhalb der Bundesorgane dient Art. 27 DSG. Diese Vorschrift erlaubt es dem EDÖB von sich aus oder auf Meldung Dritter hin einen Sachverhalt näher abzuklären (Art. 27 Abs. 2 DSG). Dem EDÖB ist erlaubt, Akten herauszuverlangen und Auskünfte einzuholen (Art. 27 Abs. 3 DSG). Aufgrund dieser Abklärungen kann er Empfehlungen herausgeben und eine Änderung oder Unterlassung der Praxis fordern oder vorsorgliche Massnahmen beantragen. Entscheidet sich das gerügte Bundesorgan, eine Empfehlung nicht zu befolgen oder abzulehnen, so kann die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorgelegt werden (Art. 27 Abs. 5 DSG). Das Departement bzw. die Bundeskanzlei entscheidet in Form einer Verfügung, gegen welche der EDÖB ein Beschwerderecht hat (Art. 27 Abs. 6 DSG).

Obwohl die Rechtsdurchsetzung auf mehreren Ebenen vorgesehen ist (Auskunftsrecht, individuelle Klagemöglichkeiten nach Zivil- oder Verwaltungsrecht, strafrechtliche Sanktionen, Interventionsmöglichkeiten des EDÖB), leidet das DSG an einem Durchsetzungsdefizit. Vorschläge zur Verbesserung liegen vor: Stärkung der datenschutzrechtlichen Aufsicht (u.a. mit härteren Sanktionsmöglichkeiten) und Verbesserung der individualrechtlichen Durchsetzungs-

[43] Zur Klage des EDÖB vom 11.11.2009 gegen Google siehe Geiser und Uttinger (2010).
[44] Botschaft zum DSG, BBl 1988 II 413 ff.

möglichkeiten durch Verbandsklagerechte (Brunner, 2011). Postuliert wird ferner, dass im Datenschutzrecht nicht nur ein Ausbau sondern auch und vor allem eine Verwesentlichung der Datenschutzrechte ansteht (Tinnefeld, 2010). Die Rede ist von einem «Post Privacy-Zeitalter» und davon, dass sich der Charakter der Privatsphäre im Lichte der omnipräsenten online-Dienste wandle (Brunner, 2011). Ob allerdings künftiges Datenschutzrecht einem behaupteten oder herbeigeredeten grundlegend neuen Verständnis von Privatsphäre entsprechen muss, bedarf fundierter Analyse und einer breiten gesellschaftlichen Diskussion (Pärli, 2011).

3.5 Ausgewählte Fragen des DSG mit Blick auf Ortungstechnologien

3.5.1 Datenbearbeitung als umfassender Begriff

Das DSG definiert in Art. 3 Abs. e den Begriff der «Datenbearbeitung». Darunter ist «jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Archivieren oder Vernichten von Daten» zu verstehen. Der Gesetzgeber bringt mit dieser Definition die Technikneutralität des DSG zum Ausdruck. Das Gesetz soll auch Bearbeitungsvorgänge und -methoden erfassen, die im Erlasszeitpunkt noch gar nicht bekannt waren (Belser, 2008, N 26 zu Art. 3 DSG). Auch in der ersten Revision des DSG (2008) wurde an der Technikneutralität des Gesetzes festgehalten. Der Gesetzgeber erkannte, dass durch die technischen Innovationen Daten, auch Personendaten, wesentlich einfacher zu speichern, flexibler auszuwerten und leichter weiterzugeben seien. Aus diesem Grund wurden im Rahmen der DSG-Revision die Informationspflicht bei der Beschaffung besonders schützenswerter Personendaten und von Persönlichkeitsprofilen verstärkt (Leupold & Wüger, 2008, S. 181).

Die heute (und künftig) technisch möglichen Ortungsverfahren sind, soweit Personendaten betroffen sind, vom Datenschutzrecht erfasst. Es ist jedoch fraglich, ob die im Datenschutzrecht enthaltenen Grundsätze der Datenbearbeitung sowie die Rechtsbehelfe zur Durchsetzung datenschutzrechtlicher Ansprüche und die Tätigkeit des EDÖB die vom Verfassungs- und Gesetzgeber ge-

wünschte Wirkung – Schutz der Grundrechte und der Persönlichkeit der Personen, über die Daten bearbeitet werden – auch tatsächlich ermöglichen.

3.5.2 Was sind Personendaten?

Das DSG definiert in Art. 3 zentrale Begriffe. In lit. a und b wird festgehalten, dass nur Personendaten im Sinne des DSG relevant sind. Personendaten sind Angaben über eine bestimmte oder bestimmbare Person (Art. 3 lit. a DSG). Bereits in dieser Definition kommt ein wichtiger Teil des Schutzkonzeptes des DSG zum Ausdruck; nicht die Daten sollen geschützt werden, sondern die Personen vor missbräuchlicher Bearbeitung ihrer Personendaten (Maurer-Lambrou & Kunz, N 3 zu Art. 1 DSG).

Werden Geräte geortet, welche einer Person gehören, entstehen dadurch ebenfalls personenbezogene Daten, es ist fraglos ein Personenbezug gegeben. Schwieriger wird es, wenn nicht direkt eine Person geortet wird, sondern der Personenbezug erst durch Verbindung zwischen Sach- und Personendaten oder durch Verknüpfung verschiedener Sachdaten geschaffen wird. Geodaten sind Sachdaten[45]; ein Personenbezug wird jedoch angenommen, wenn zwischen den Daten und einer natürlichen oder juristischen Person eine Verknüpfung besteht oder mit vernünftigem Aufwand hergestellt werden kann (Botschaft Geoinformationsgesetz, 7852)[46]. Als unverhältnismässig gilt ein Aufwand dann, wenn «nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen Aufwand auf sich nehmen wird (etwa durch komplizierte Analyse einer Statistik)» (Botschaft zum Datenschutzgesetz, 1988)[47]. In der juristischen Literatur wird kritisch vermerkt, dass bei Geodaten angesichts deren raumbezogener Referenzinformationen und der Möglichkeit, diese Informationen mit Adressen und diese wiederum mit Personen zu verknüpfen, praktisch immer Personendaten vorliegen würden. Alle diese Daten dem Datenschutzregime zu unterstellen, sei nicht sachgerecht (Forgo & Krügel, 2010, S. 19ff.; vgl. auch Abschnitt 2.5). Im Geoinformationsgesetz des Bundes wird in Art. 11 auf die Anwendbarkeit des DSG für Geodaten des Bundes hinge-

[45] Art. 3 Nr 2 der Richtlinie 2007/2/EG (Inspire-Richtlinie) definiert Geodaten als «Daten mit einem direkten oder indirekten Bezug zu einem bestimmten Standort oder geografischen Gebiet.» Sie sind also grundsätzlich nicht personenbezogen, sondern sachbezogen.

[46] Botschaft zu GeoIG, BBl 2006.

[47] Botschaft zum DSG, BBl 1988 II 445.

wiesen. Die Frage, wann Geodaten Personendaten im Sinne des DSG sind, wird indes weder vom DSG noch vom GeoIG ausdrücklich beantwortet, und auch in Lehre und Praxis findet sich noch keine präzise Darlegung (Kettiger, 2010). In der «Google Street View»-Angelegenheit hat das Bundesverwaltungsgericht bejaht, dass die Rohbilder von Personen klar als Personendaten zu qualifizieren sind. Dasselbe gelte auch für Fahrzeugkennzeichen und Abbildungen von Häusern, Gärten und Höfen, da sich auch bei diesen Daten problemlos ein Personenbezug herstellen lasse (BVGer, A-7040/2009, E. 7.6.3).

Eine weitere umstrittene Frage ist der Personenbezug einer IP-Adresse (Weber & Fercsik Schnyder, 2009). Die Frage, ob eine IP-Adresse ebenfalls einen Personenbezug aufweist, wurde vom Bundegericht in einem Urteil vom 8. September 2010 (BGE 136 II 508, Erw. 3.5) teilweise offengelassen. So sei eine abstrakte Feststellung zu dieser Frage nicht möglich. Im konkreten Fall wurde jedoch bejaht, dass die IP-Adressen (und die Weiterleitung dieser und weiterer Daten an die Rechtsinhaber) der Downloader urheberrechtlich geschützter Werke Personendaten darstellen. Aufschlussreich – gerade auch für die Frage, wann Ortungsdaten ein Personenbezug zukommt – sind die Ausführungen des Bundesgerichts in Erw. 3.2: «Eine Person ist dann bestimmt, wenn (...) aufgrund zusätzlicher Informationen auf sie geschlossen werden kann. Für die Bestimmbarkeit (...) insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat.» Dieselbe Information kann somit aus der Sicht des einen Empfängers einen Personenbezug aufweisen und aus der Sicht einer anderen Person nicht (Rosenthal, 2011, S. 40; siehe zum Urteil auch: Glarner & Ruefenacht, 2010, und Weber, 2011, S. 28–29).

3.5.3 Datenverknüpfungen: Auswirkungen auf Transparenz, Einwilligung und Informationspflicht

Die durch Ortungsverfahren gewonnenen Informationen berühren in besonderem Masse das Problem der Datenverknüpfung. Aus reinen Sachdaten – z.B. der Angabe des Standortes – können durch entsprechende Verknüpfung Personendaten entstehen, gegebenenfalls sogar besonders schützenswerte Perso-

nendaten oder Persönlichkeitsprofile. Besonders problematisch ist, wenn die Person, über die durch Datenverknüpfung (besonders schützenswerte) Personendaten oder Persönlichkeitsprofile bearbeitet werden, dies gar nicht ausreichend zu erkennen vermag. Wer seine Personendaten gegenüber Privaten offenbart (z.B. Bekanntgabe des aktuellen Standortes an Apple durch entsprechende Bestätigung beim iPhone), erteilt dem Empfänger keinen Freipass für eine x-beliebige Weiterverwendung dieser Daten. Vielmehr ist der Datenempfänger hier an die allgemeinen Grundsätze der Datenbearbeitung (Treu und Glauben, Verhältnismässigkeit, Zweckbindung, siehe oben) gebunden. Eine Einwilligung für eine Verknüpfung der Personendaten ist bei der Datenbekanntgabe nicht per se anzunehmen (Probst, 2010, S. 35). Die Datenverknüpfung hat für die betroffene Person vielmehr hinreichend erkennbar zu sein und muss durch den Zweck der Datenbeschaffung gedeckt sein. Soweit besonders schützenswerte Personendaten oder Persönlichkeitsprofile betroffen sind, muss eine *ausdrückliche* Einwilligung vorliegen (Art. 4 Abs. 5 DSG).

Wenn durch Datenverknüpfungen Persönlichkeitsprofile entstehen oder besonders schützenswerte Personendaten generiert werden, ist der Inhaber einer Datensammlung verpflichtet, die betroffene Person über die Beschaffung dieser Daten zu informieren; diese Informationspflicht gilt auch dann, wenn die Daten bei Dritten beschafft werden (Art. 14 Abs. 1 DSG).

3.5.4 Erfordernis der ausreichenden gesetzlichen Grundlage für die Datenbearbeitung

Der Einsatz von Ortungsverfahren durch die öffentliche Verwaltung (Bund, Kantone, Gemeinden, öffentlich-rechtliche Anstalten usw.) ist nur zulässig, sofern dafür eine ausreichende gesetzliche Grundlage vorhanden ist (Kettiger, 2010, Rz 58). Das DSG hält in Art. 17 Abs. 2 DSG für Bundesorgane fest, dass besonders schützenswerte Personendaten und Persönlichkeitsprofile nur bearbeitet werden dürfen, wenn ein Gesetz im formellen Sinne es ausdrücklich vorsieht oder einer der Ausnahmetatbestände in Art. 17 Abs. 2 lit. a. bis c vorliegt. Eine gesetzliche Grundlage ist z.B. für die Videoüberwachung öffentlicher Räume notwendig, sofern mit der eingesetzten Technik Personendaten nach DSG bearbeitet werden. Eine Grundlage in einem formellen Gesetz ist immer dann notwendig, wenn die Videobilder besonders schützenswerte Personendaten enthalten oder zu Persönlichkeitsprofilen verarbeitet werden. Die Videoüber-

wachung muss überdies einem öffentlichen Interesse entsprechend und verhältnismässig sein.[48]

3.5.5 Überwiegendes privates oder öffentliches Interesse an der Datenbearbeitung

Die Widerrechtlichkeit einer persönlichkeitsverletzenden Bearbeitung von Personendaten durch Private entfällt bei Vorliegen eines Rechtfertigungsgrundes (Art. 13 DSG), namentlich bei einem überwiegenden privaten oder öffentlichen Interesse des Datenbearbeiters.

Kein überwiegendes Interesse Privater (und auch kein öffentliches Interesse) anerkennt das Bundesgericht im wirtschaftlichen Interesse der Firma Logistep am Einsatz ihrer Software zur Suche in P2P-Netzwerken nach urheberrechtlich geschützten Werken. Daran ändere auch das Interesse der Auftraggeber nichts. Die wirksame Bekämpfung der Urheberrechtsverletzung vermöge die Persönlichkeitsverletzung und die mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen. Ein überwiegendes privates oder öffentliches Interesse sei umso mehr zu verneinen, als dieses nur zurückhaltend bejaht werden dürfe (Bger 1C_285/2009, Erw. 6.3.3).

Auch in der Google Street View Streitsache stellt sich die Frage der Rechtfertigung der Datenbearbeitung durch überwiegende private oder öffentliche Interessen. Wie schon im Vorfeld von einigen Stimmen aus der Lehre angenommen wurde (Baeriswyl, 2009a, S. 100; Geiser & Uttinger, 2010, S. 127) können nach dem Urteil des Bundesverwaltungsgerichts die Persönlichkeitsverletzungen durch Google nicht gerechtfertigt werden. Das öffentliche Interesse, welches an der Dienstleistung von Google bestehe, sei kein öffentliches Interesse im rechtlichen Sinne. Der Wettbewerbsdruck, der durch das Angebot entstehe, wie auch die Interessen zahlreicher Unternehmen an dieser Dienstleistung, wurden vom Gericht lediglich als private Interessen mitberücksichtigt, nicht jedoch als öffentliche (BVGer, A-7040/2009, E. 10.4.4). Diese Ansicht stiess auf Kritik. So sei nicht ersichtlich, wieso das BVGer allgemeine Interessen wie z.B., dass der Service kostenlos und einfach ist und dadurch das

[48] Zur ganzen Problematik siehe den Bericht des EJPD zur Videoüberwachung zu Sicherheitszwecken in Bahnhöfen, Flughäfen und an anderen öffentlichen Orten (EJPD, 2007).

schnelle Auffinden verschiedener Orte ermögliche, nicht als öffentliches Interesse berücksichtigt habe, um eine allenfalls ungenügende Anonymisierung zu rechtfertigen (Meier, 2011, S. 70). Auch Blonski (2011, S. 842) kommt zum Schluss, dass ein gewisses öffentliches Interesse an der Dienstleistung bestehe. Google brachte als überwiegende private Interessen vor allem rein wirtschaftliche Interessen vor. Diese sind zwar dazu geeignet eine Datenbearbeitung zu rechtfertigen, da grundsätzlich jedes Interesse von einem allgemein anerkannten Wert mitberücksichtigt werden kann (BVGer, A-7040/2009, E. 10.4.1). Diesen Interessen stellte das BVGer die Interessen der von der Datenbearbeitung Betroffenen gegenüber. Die Persönlichkeit der Betroffenen sei immer ein schützenswertes Interesse (BVGer, A-7040/2009, E. 10.4.5). In diesem Zusammenhang argumentierte Google, die Beeinträchtigungen der Datenschutzinteressen der Betroffenen hätten erstens auf ein Minimum reduziert werden können, da nur noch vereinzelte Personen bestimmbar seien, und zweitens handle es sich um Aufnahmen von «harmlosen Alltagssituationen». Der Zweck, der von Google Street View verfolgt werde, rechtfertige den Eingriff in die Interessen der betroffenen (BVGer, A-7040/2009, E. 10.1). Im Rahmen der Interessensabwägung stellte das BVGer fest, dass die von Google angeführten wirtschaftlichen Interessen nicht genügen, um die Datenbearbeitung zu rechtfertigen. Die Persönlichkeitsverletzungen seien vermeidbar. Zwar erfordert die, allenfalls auch manuelle, Anonymisierung der Daten einen finanziellen Mehraufwand, welcher die Existenz der Beklagten jedoch nicht gefährden würde. Zudem liege in der Kostenlosigkeit von Google Street View weder ein öffentliches noch ein privates Interesse (BVGer, A-7040/2009, E. 10.4.6.). Es bleibt abzuwarten, wie weitgehend das Bundesgericht den Entscheid des Bundesverwaltungsgerichts stützen wird. Google hat am 11. Mai 2011 seine Beschwerde gegen diesen Entscheid beim Bundesgericht eingereicht (Meier, 2011, S. 71).

3.5.6 Anwendbarkeit des DSG in internationalen Sachverhalten

Insbesondere mit Blick auf die in diesem Bericht vertieft behandelten Datenschutzfragen der sozialen Netzwerke (siehe Kapitel 6) stellt sich die Frage, wie weit das DSG überhaupt anwendbar ist, wenn der Anbieter der Dienstleistung vom Ausland aus operiert und somit ein internationaler Sachverhalt vorliegt.

Bezüglich der Interventionsmöglichkeiten des EDÖB ist davon auszugehen, dass Art. 29 DSG grundsätzlich anwendbar ist, wenn in der Schweiz eine Datenbearbeitung stattfindet (Rosenthal, Handkommentar DSG, Rz 6 zu Art. 29 DSG). Das Beschaffen von Daten in der Schweiz durch eine Unternehmung aus dem Ausland erfüllt diesen Tatbestand (Zum Ganzen: Thalmann, 2007, S. 341 ff.). Ob diese Voraussetzungen bei sozialen Netzwerken, die vom Ausland aus operieren, gegeben sind, ist zweifelhaft.

Bei einem privatrechtlichen internationalen Sachverhalt (wenn z.B. ein Nutzer eines Social-Media-Angebotes gegenüber der fraglichen Unternehmung eine Klage auf Schadenersatz als Folge einer Datenschutzverletzung geltend machen will) stellt sich zum einen die Frage der gerichtlichen Zuständigkeit und zum anderen diejenige nach dem anwendbaren Recht. Die gerichtliche Zuständigkeit bestimmt nach einschlägigen völkerrechtlichen Verträgen oder nach dem Bundesgesetz über das Internationale Privatrecht (IPRG). Möglich ist eine Klage nach Art. 129 Abs. 1 IPRG am Wohnsitz oder Sitz des Beklagten, am Ort des gewöhnlichen Aufenthaltes oder am Ort der Niederlassung[49]. Art. 129 Abs. 2 IPRG sieht ferner eine alternative Zuständigkeit am Handlungs- oder Erfolgsort (der Persönlichkeitsverletzung) vor. Das soziale Netz Facebook hat in Irland eine Niederlassung. Vor diesem Hintergrund ist das für eurointernationale Sachverhalte geschaffene Lugano-Übereinkommen (LugÜ) einschlägig (SR 0.275.12). In einer allfälligen Klage gegen Facebook kommt sowohl eine deliktische wie auch eine vertragliche Anspruchsgrundlage in Frage. Für einen deliktischen Anspruch dürfte eine Zuständigkeit gemäss Art. 5 Ziff. 3 LugÜ – Zuständigkeit am Handlungs- oder Erfolgsort – gegeben sein (sofern der Erfolgsort am Wohnsitz des Geschädigten in der Schweiz liegt). Für vertragliche Ansprüche besteht, da es sich eine Verbrauchersache iSv Art. 15 LugÜ handelt, ebenfalls ein Gerichtsstand am Wohnsitz des Klägers, gestützt auf Art. 16 Abs. 1 LugÜ. Eine Gerichtsstandsvereinbarung ist in den Schranken von Art. 23 LugÜ zulässig, das bedeutet, dass z.B. die Vereinbarung eines Gerichtsstands ausserhalb eines LugÜ-Staates nicht zulässig ist. Zur Frage des anwendbaren Rechts sieht Art. 139 IPRG vor, dass bei Persönlichkeits- und Datenschutzverletzungen der geschädigten Person weitgehend ein Wahlrecht zukommt. Im Ergebnis ist die Anwendbarkeit des schweizerischen Datenschutzrechts in praktisch allen Konstellationen internationaler (Datenbearbeitungs-)Sachverhalte

[49] Nach dem ausdrücklichen Wortlaut in Art. 129 Abs. 1 IPRG sind Klagen am Sitz der Niederlassung nur zulässig, sofern die Klage aufgrund der Tätigkeit dieser Niederlassung erfolgt.

möglich (Dasser, 2007, N 39 zu Art. 139 IPRG; siehe auch Erw. 5.5.1 bis 5.5.6 des «Street-View-Urteils», BVGer. A-7040/2009). Zu relativieren ist, dass in der Praxis Art. 139 IPRG nicht zuletzt aufgrund fehlender Kenntnis wenig angewendet wird (Rosenthal, 2008, N 2 zu Art. 139 IPRG), jedoch lieferte auch der oben diskutierte Street-View-Entscheid des BVGer ein Anwendungsbeispiel von Art. 139 IPRG (BVGer, A-7040/2009, E. 5.5.1 ff.). Soweit vertragliche Ansprüche geltend gemacht werden, untersteht das Vertragsverhältnis gemäss Art. 120 Abs. 1 IPRG dem Recht des gewöhnlichen Aufenthalts des Konsumenten; eine Rechtswahl ist nach Art. 120 Abs. 2 IPRG ausgeschlossen. I.d.R. dürfte dies dasselbe Recht sein, dass sich bei deliktischen Ansprüchen aus Persönlichkeitsverletzung gemäss Art. 139 IPRG ergibt.

3.6 Zwischenfazit aus rechtlicher Sicht

Das DSG ist technikneutral ausgestaltet, das heisst, alte wie neue und künftige (Ortungs-)Technologien sind grundsätzlich vom DSG erfasst. Das DSG findet sowohl auf die Datenbearbeitung der Bundesbehörden wie auf diejenige von Privaten Anwendung. Für die Datenbearbeitung der Kantone gilt kantonales Datenschutzrecht.

Von hoher Relevanz ist die Frage, ob die durch Ortung gewonnenen Informationen einen ausreichenden Personenbezug aufweisen. Sofern die Daten allein oder durch Verkettung oder Verknüpfung zu Angaben über eine bestimmte oder bestimmbare Person führen, liegen Personendaten im Sinne des DSG vor. Die Bearbeitung von Personendaten mittels Ortungsverfahren ist in den Schranken der im zweiten Abschnitt des DSG enthaltenen Bearbeitungsgrundsätze zulässig: Personendaten müssen rechtmässig beschafft werden, die Bearbeitung hat verhältnismässig zu erfolgen und darf den Prinzipien der Zweckbindung, Datenrichtigkeit, Datensicherheit und Transparenz nicht widersprechen. Für besonders schützenswerte Personendaten und Persönlichkeitsprofile gelten erhöhte Bearbeitungshürden, namentlich was die informierte Einwilligung betrifft.

Die Bearbeitung von Personendaten durch Behörden erfordert eine ausreichende gesetzliche Grundlage. Sofern Persönlichkeitsprofile und besonders schützenswerte Personendaten bearbeitet werden, ist dafür eine Grundlage in einem formellen Gesetz notwendig. In privatrechtlicher Hinsicht ist die persönlichkeits-

verletzende Bearbeitung von Personendaten (nach allerdings umstrittener Lehre und Rechtsprechung) rechtfertigungsfähig, namentlich durch eine Einwilligung sowie durch überwiegende private oder öffentliche Interessen. Nach Lehre und Rechtspraxis kommt den Persönlichkeitsrechten in unserer Rechtsordnung eine zentrale Bedeutung zu; ein rechtfertigendes überwiegendes Interesse der Datenbearbeiter darf deshalb nicht leichthin und nicht primär unter Berufung auf wirtschaftliche Interessen erfolgen.

Die Durchsetzung der datenschutzrechtlichen Grundprinzipien erweist sich in der Praxis oft – nicht nur, aber auch bei der Bearbeitung von Ortungsdaten – als utopisch. Die mit der Personenortung einhergehenden Datenschutzprobleme werden regelmässig als Indikator für eine eigentliche Datenschutzkrise wahrgenommen. Als Ausweg werden Konzepte «regulierter Selbstregulierung», eine Stärkung der datenschutzrechtlichen Aufsicht und die Verbesserung der individualrechtlichen Durchsetzungsrechte gefordert (Brunner, 2011). Besonders notwendig ist die Verbesserung des Persönlichkeitsschutzes im Bereich der Arbeit. Hier kann die Missachtung der Datenbearbeitungsgrundsätze für die Betroffenen existenziell bedrohende Auswirkungen haben (Pärli, 2011).

3.7 Die Rechtslage in der EU – Auswirkungen auf die Schweiz

3.7.1 Die EU-Datenschutzrichtlinien

In der EU-Datenschutzrichtlinie 95/46/EG kommen wesentliche Ziele des europäischen Intergrationsprozesses zum Ausdruck. Nach Art. 1 Abs. 1 RI 95/46/EG haben die Mitgliedstaaten einerseits den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten. Andererseits wird in Abs. 2 der gleichen Bestimmung der Grundsatz festgehalten, dass der freie Verkehr personenbezogener Daten zwischen den Mitgliedstaaten nicht beschränkt werden darf. Damit erfüllt die Richtlinie eine Binnenmarktfunktion.

Im Einzelnen sieht die Richtlinie strenge Beschränkungen für die Erhebung und Verwertung personenbezogener Daten vor. Die Mitgliedstaaten müssen zudem eine unabhängige nationale Datenschutzbehörde einrichten. Ergänzt wird der Datenschutz innerhalb der Europäischen Union durch eine spezifische Datenschutzrichtlinie für elektronische Kommunikation. Die Richtlinie 2002/58/EG – geändert durch die Richtlinie 2009/136/EG[50] – verpflichtet die EU-Mitgliedstaaten zum Erlass telekommunikationsspezifischer Regelungen zum Datenschutz. Die Richtlinie bildet Teil eines allgemeinen unionsrechtlichen Rechtsrahmens für elektronische Kommunikationsnetze[51]. Sie beinhaltet u.a. Vorschriften über die Vertraulichkeit der Kommunikation, die Datenaufzeichnung, «Spam» und «Cookies» sowie über öffentliche Verzeichnisse.

Der Anwendungsbereich der Datenschutzrichtlinie 95/46/EG ist gemäss Art. 3 Abs. 2 erster Spiegelstrich beschränkt: Die Bereiche öffentliche Sicherheit, Landesverteidigung, Sicherheit des Staates und Tätigkeiten des Staates im strafrechtlichen Bereich sind ausgeschlossen (Epiney, 2011, S. 649). In den genannten Bereichen sind die EU-Mitgliedstaaten und die durch die Dublin/ Schengen-Abkommen integrierten Nicht-EU-Staaten indes an die unionsrechtlichen Rahmenbeschlüsse 2006/960[52] und 2008/977[53] gebunden.[54]

[50] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

[51] Richtlinie 2009/140/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste.

[52] Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union.

[53] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.

[54] Siehe zum Ganzen: Epiney (2011).

3.7.2 Reform des EU-Datenschutzrechts

Die EU-Kommission veröffentlichte im November 2010 ein Gesamtkonzept für den Datenschutz der Europäischen Union[55]. Als Hauptziele der Reform des geltenden EU-Datenschutzrechts werden die Stärkung der Rechte des Individuums und die Stärkung der Binnenmarktdimension des Datenschutzes genannt. Diese Ziele sind bereits in der RI 95/46/EG angelegt (siehe oben).

Verstärkung des Schutzes der Persönlichkeit

Die Notwendigkeit der Stärkung der Rechte des Individuums ergibt sich für die EU-Kommission auch auf dem Hintergrund der EU-Charta der Grundrechte, die mit dem Inkrafttreten des Lissabonvertrages für die Union und die EU-Mitgliedstaaten bei der Anwendung von EU-Recht rechtsverbindlich wurde. Art. 8 der EU-Grundrechscharta garantiert jeder Person das Recht auf Schutz der sie betreffenden Daten. Im Vertrag über die Arbeitsweise der Union (AEUV) wurde zudem eine Rechtsgrundlage für eine umfassende, kohärente Datenschutzregelung geschaffen (Art. 16 Abs. 2 AEUV)[56].

Ein besserer Individualrechtsschutz erfordert gemäss dem Kommissionsbericht die Erhöhung der Transparenz für die von der Datenbearbeitung betroffenen Personen. Bemängelt werden die heute in der Online-Umgebung oft unklaren, schwierig zu findenden und wenig transparenten *Datenschutzhinweise*. Abhilfe könne die Erstellung eines oder mehrerer EU-Standardmuster für Datenschutzhinweise schaffen.[57] Weiter sollen die von der Datenbearbeitung betroffenen Personen bessere Kontrollrechte erhalten, u.a. solle das «Recht auf Vergessen» präzisiert werden, was besonders im Zusammenhang mit sozialen Online-Netzwerken in der Praxis Probleme bereite.[58] Die Kommission wird zudem prüfen, ob die heutigen Bestimmungen für den Schutz sensibler Daten ausreichen. Angestrebt wird eine Präzisierung der Kategorie der sensiblen Daten. Auf der Ebene der Rechtsdurchsetzung will die Kommission klären, ob bestehende Sanktionsregelungen verschärft werden sollen, beispielsweise

[55] Gesamtkonzept für den Datenschutz in der Europäischen Union – Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, KOM (2010) 609 endgültig.
[56] Gesamtkonzept (Fn 55), S. 2.
[57] Gesamtkonzept (Fn 55), S. 7.
[58] Gesamtkonzept (Fn 55), S. 8.

durch strafrechtliche Sanktionen bei schwerwiegenden Datenschutzverstössen.[59] Gefördert werden sollen auch Initiativen zur Selbstregulierung und die Einführung von EU-Zertifizierungsregelungen.[60]

Harmonisierung des EU-Datenschutzrechts – Auswirkungen auf Drittstaaten

Die Binnenmarktdimension des EU-Datenschutzes erfordert nach der Einschätzung der Kommission eine weitgehende Harmonisierung der einzelstaatlichen Datenschutzvorschriften. Dabei bleiben auch Nicht-EU-Mitgliedstaaten nicht verschont. Nach Ansicht der Kommission ist bei der Datenbearbeitung durch in Drittstaaten ansässige Datenbearbeiter darauf hinzuwirken, dass den von dieser Bearbeitung Betroffenen das EU-Schutzniveau gewährt wird, was eine Überprüfung der geltenden Vorschriften über das anwendbare Recht bei internationalen Sachverhalten notwendig mache.[61]

Angesichts der globalen Dimension des Datenschutzes sollen die bestehenden Verfahren für den internationalen Transfer personenbezogener Daten verbessert werden. Es soll sichergestellt werden, dass die personenbezogenen Daten beim Transfer und bei der Verarbeitung ausserhalb der EU und des EWR angemessen geschützt werden.[62]

Vorschläge der «Artikel 29»-Gruppe zur Regelung der Ortungstechnologie

Die «Artikel 29»-Gruppe (ein gestützt auf Art. 29 RI 95/46/EG eingesetztes unabhängiges Beratungsgremium der EU-Kommission zu Fragen des Datenschutzes) hat im Mai 2011 eine Stellungnahme zur Nutzung von Ortungsdaten im Zusammenhang mit Handys und anderen mobilen Geräten erlassen.[63] Die Gruppe kommt zum Schluss, die Nutzung von Geodaten von Smartphones falle in den Anwendungsbereich der RI 95/46/EG und die Ortungsdaten stellten Personendaten im Sinne dieser Richtlinie dar.

59 Gesamtkonzept (Fn 55), S. 10.
60 Gesamtkonzept (Fn 55), S. 14.
61 Gesamtkonzept (Fn 55), S. 12.
62 Gesamtkonzept (Fn 55), S. 18 f.
63 Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, adopted on 16 May 2011, 881/11/EN WP 185.

Die Arbeitsgruppe «Artikel 29» fordert, dass Ortungsdienste standardmässig (d.h. als Voreinstellung) deaktiviert sein müssen. Für die Zustimmung zur Verwendung der georteten Daten durch die Anbieter der Dienstleistung seien wesentlich klarere Einwilligungen erforderlich, als diese praxisgemäss von den Nutzern erfragt würden. Die Einwilligung soll nur für ein Jahr gültig sein und müsse jederzeit und sehr einfach widerrufen werden können. Zur Vermeidung einer dem Nutzer nicht bewussten Ortung sollten die Anbieter zum Aufschalten eines permanenten Warn-Icons verpflichtet werden.[64]

Besondere Aufmerksamkeit widmet die Stellungnahme der Einwilligung in die Bearbeitung ortungstechnologisch gewonnener Daten im Arbeitskontext. Mit Bezug auf eine frühere spezifische Stellungnahme[65] fordert die Arbeitsgruppe «Artikel 29», die Ortung von Arbeitnehmenden nur in engen Grenzen zuzulassen. Namentlich müsse die gegebenenfalls zulässige Ortung der Arbeitnehmenden auf die Arbeitszeit beschränkt bleiben.[66]

3.7.3 Auswirkungen auf die Schweiz

Bei den Auswirkungen des EU-Datenschutzrechts auf die Schweiz gilt es, zwischen staatsvertraglichen Verpflichtungen zur Übernahme von EU-Recht und faktischer Notwendigkeit zur EU-rechtskonformen Anpassung des schweizerischen Datenschutzrechts zu unterscheiden.

Im Zusammenhang mit der sogenannten «Schengenassozierung»[67] und der «Dublinassozierung»[68] hat sich die Schweiz zur Anwendung verschiedener datenschutzrechtlich relevanter EU-Rechtsakte verpflichtet. Insbesondere muss die Schweiz die Weiterentwicklung des einschlägigen EU-Rechts übernehmen.[69] Vor diesem Hintergrund wurde in der Schweiz das «Bundesgesetz

64 Opinion 13/2011 (Fn 63), S. 16.
65 Article 29 Date Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context.
66 Opinion 13/2011 (Fn 63), S. 14.
67 Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assozierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes, SR 0.362.31.
68 Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrages, SR 0.142.392.68.
69 Art. 2 Abs. 3 in Verb. mit Art. 7 Schengen-Assozierung (Fn 67).

über die Umsetzung des Rahmenbeschlusses 2008/077 über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen» erlassen. Im Rahmen dieses Gesetzes wurde eine Reihe von Bestimmungen des DSG geändert (siehe dazu: Epiney, 2011, S. 646 f.).

Die Datenschutzrichtlinie 95/46/EG ist für die Schweiz als Nicht-EU-Mitgliedstaat nicht unmittelbar rechtsverbindlich (Brunner, 2009, S. 140).[70] Gleiches gilt für die Rl 2002/58/EG bzw. die Rl 2009/136/EG (Richtlinie über die elektronische Kommunikation). Zu beachten ist indes die faktische Notwendigkeit der Anpassung des schweizerischen Datenschutzrechtes an dasjenige der Europäischen Union. Nach Art. 25 Rl 95/46/EG müssen die EU-Mitgliedstaaten vorsehen, dass die Übermittlung personenbezogener Daten in ein Drittland nur zulässig ist, wenn dieses Drittland über ein angemessenes datenschutzrechtliches Schutzniveau verfügt. Die EU-Kommission hat mit Entscheid vom 26. Juli 2000 der Schweiz zugebilligt, dass sie diese Voraussetzungen erfülle.[71] Eine vollständige Kompatibilität des schweizerischen Datenschutzrechts mit der Rl 95/46/EG besteht jedoch nicht und wurde vom Gesetzgeber bei den jüngsten Revisionen[72] auch nicht angestrebt (Epiney, 2009, S. 3 ff.).

Die Europäische Kommission bereitet gegenwärtig einen umfassenden Rechtsrahmen für das Datenschutzrecht vor. Namentlich ist eine Anpassung der Rl 95/46/EG an die neuen technologischen Entwicklungen geplant (siehe oben). Aus schweizerischer Sicht sind dabei allfällige «Schengen/Dublin» betreffende Änderungen gestützt auf die schweizerische Assoziierung, automatisch zu übernehmen. Weitergehender Anpassungsbedarf kann sich aus praktischer Sicht (und mit Blick auf Art. 25 Rl 95/46/EG, siehe vorherigen Abschnitt) ergeben, wenn bspw. der Begriff der besonders schützenswerten Daten konkretisiert oder die Anforderungen an die Einwilligung bei Datenverknüpfungen erhöht würden.

---

70 Zu beachten ist die Rl 95/46/EG indes in den Bereichen der Schengen/Dublin-Assozierung. Epiney (2011) plädiert für die Annahme, die Rl 95/46/EG sei für die Schweiz integral verbindlich.

71 Entscheidung der Kommission vom 26. Juli 2000 gemäss der Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, Amtsblatt Nr. L 215 vom 25/8/2000, S. 0001-0003.

72 Siehe dazu Fn 36.

3.8 Datenschutzrechtliche Entwicklungen im Europarat

Die Konvention Nr. 108 zum Schutz des Einzelnen im Hinblick auf die automatische Verarbeitung personenbezogener Daten (Europäische Datenschutzkonvention, DSK) des Europarates ist die wichtigste völkerrechtliche Regelung im Bereich des Datenschutzes und formuliert in allen Vertragsstaaten einen datenschutzrechtlichen Mindeststandard (Epiney & Schleiss, 2011, S. 78 ff.). Die DSK wurde am 8.11.2001 durch das Zusatzprotokoll Nr. 181 ergänzt. Die Schweiz hat sowohl die DSK wie das Zusatzprotokoll ratifiziert.

Zurzeit sind im Europarat Bestrebungen im Gange, die DSK zu überarbeiten.[73] Auch hier steht die Frage im Zentrum, wie durch das Übereinkommen die Persönlichkeitsrechte des Individuums besser vor Datenschutzverletzungen geschützt werden können.

[73] Die «roadmap» des Europarates sieht vor, dass bis zum Trimester des Jahres 2012 dem Ministerkomitee des Europarates ein Entwurf vorgelegt wird, siehe zum Ganzen: http://www.coe.int/t/dghl/standardsetting/dataprotection/Modernisation_en.asp (13.09.2011)

4 Konfliktlinien und gesellschaftliche Relevanz

Technische Entwicklungen können bis anhin bewährte Vorstellungen in Frage stellen und deshalb zu gesellschaftlichen Konflikten führen. Die Gültigkeit von Werten und Normen, aber auch austarierte Interessengleichgewichte müssen unter den durch Technik veränderten Bedingungen neu ausgehandelt werden. Die heute bereits erkennbaren Konfliktlinien im Kontext von Ortungstechnologien werden – basierend auf den bisherigen Kapiteln und einer Literaturrecherche – im Folgenden kurz dargestellt (Abschnitt 4.1).

Das Konfliktpotenzial ist jedoch nicht das einzige Kriterium, das die gesellschaftliche Relevanz technischer Entwicklungen anzeigt. Um gezielt die Anwendungsbereiche zu identifizieren, mit der sich die Politik vorausschauend befassen sollte, entwickeln wir eine Kriterienkatalog für gesellschaftliche Relevanz. Dieser baut auf den Erfahrungen früherer Arbeiten zur Technologiefolgenabschätzung auf (Hilty et al., 2003; Som et al. 2004; Som et al., 2009). Diesen Kriterienkatalog verwenden wir zunächst für ein erstes Screening der Anwendungsbereiche von Ortungstechnologien, um die Vertiefungsfelder für diese Studie auszuwählen (Abschnitt 4.2) und die Ergebnisse aus den Vertiefungsfeldern zu beurteilen (Kapitel 5 und 6). Die gleichen Kriterien werden wir später in Kapitel 8 erneut einsetzen, um die gesellschaftliche Relevanz der identifizierten Auswirkungen zu beurteilen.

4.1 Aktuelle Konfliktlinien

Dieser Abschnitt widmet sich den Konfliktlinien, die sich heute im Umgang mit Ortungstechnologien abzeichnen und sich in den kommenden Jahren möglicherweise verstärken werden. Als «Konfliktlinie» bezeichnet man in der Politikwissenschaft eine gesellschaftliche Furchung, die auf anhaltenden Konflikten in Bezug auf Werte und Interessen beruht.

Die folgende Auswahl von Konfliktlinien stützt sich auf die Literatur, die wir für die Recherche der Technologien, Anwendungen und rechtlichen Grundlagen für

die vorausgegangenen Kapitel bearbeitet und dort zitiert haben, sowie auf weitere Fach- und Medienberichte, die bei Bedarf in diesem Kapitel zitiert werden.

4.1.1 Kontrolle über die eigenen Ortungsdaten – ein aussichtsloses Unterfangen?

Das Internet hat einen virtuellen Raum geschaffen, in dem die Freiheit des Nutzers zunächst scheinbar nur zunehmen konnte. Besonders die Informations- und Meinungsfreiheit hat im Internet einen mächtigen Unterstützer gefunden. Als gegenläufiger Trend entstanden Technologien, die das Verhalten der Nutzerin im Cyberspace überwachen und im Extremfall jeden Mausklick auswerten, etwa um Massnahmen des Marketings zu perfektionieren.

Durch die aktuell beginnende Rückbindung des Cyberspace an die Geographie scheint nun eine Grenze überschritten zu werden, die vielen Nutzern Unbehagen verursacht. Dies belegen beispielsweise die Reaktionen auf die verdeckte Speicherung von Ortungsdaten in Smartphones. Als im April 2011 bekannt wurde, dass Apples iPhones und iPads seit der Betriebssystemversion iOS 4 Standortdaten der Geräte in einem lokalen File aufzeichnen, so dass anhand dieser Daten jede Bewegung des Trägers des jeweiligen Geräts nachverfolgt werden konnte, wurden Proteste laut (Alasdair & Warden, 2011; Karjoth, 2011). Bemerkenswert ist, dass gerade in Südkorea, dessen Bevölkerung u.a. aufgrund der Breitbandversorgung und dem hohen Stellenwert von Computerspielen als besonders technikaffin gilt, über 26 000 Betroffene eine Sammelklage gegen Apple einreichten.

Eine Befragung kanadischer Bürger hat ergeben, dass diese grosses Unbehagen empfinden, wenn Daten über ihren Aufenthaltsort ohne ihre Kontrolle weitergegeben und verarbeitet werden. Wenn sie jedoch die Kontrolle über die Daten und deren Verwendungskontext behalten, empfinden sie die Weitergabe der Positionsdaten als unproblematisch. Die zentrale Schlussfolgerung aus der Untersuchung lautet: «Die Kontrolle über die Information, die weitergegeben wird, und der Kontext (im Wesentlichen der Verwendungszweck) sind entscheidend dafür, ob sich jemand mit der Weitergabe persönlicher und ortsbezogener Information wohlfühlt.» (NRC, 2009, S. ii; Übers. durch die Autoren).

Das Bedürfnis nach Kontrolle über die eigenen Ortungsdaten wird indessen durch technische Entwicklungen grundlegend in Frage gestellt. Es ist bekannt, das selbst anonymisierte oder pseudonymisierte Daten durch Verknüpfung mit Geodaten nachträglich Rückschlüsse auf Personen zulassen können (Emam et al., 2008). Die ebenfalls kanadische Studie «International Comparative Analysis of Geospatial Information Privacy» spricht von «neuen Herausforderungen infolge der möglichen Re-Identifizierung von Personen durch Kombination von öffentlich erhältlichen mit Privatfirmen gehörenden Geodaten.» (NRC, 2010a, S. 2; Übers. durch die Autoren).

Aus wiederholt erfassten Ortungsdaten lassen sich, auch wenn sie nur in pseudonymisierter oder gar anonymisierter Form vorliegen, zahlreiche Informationen gewinnen: häufig besuchte Orte, Prognosen von Routen und Zielen, der Transportmodus (mit welchem Verkehrsmittel bewegt sich das Objekt?), daraus abgeleitet wahrscheinliche Wohn- oder Arbeitsadressen und schlussendlich die Identität von Personen. Einen Überblick über die bekannten Verfahren gibt Grossenbacher (2011).

Abbildung 2: *Indoor-Bewegungsprofil eines Mitarbeiters (Bildquelle: Beresford, 2005, S. 62)*

Abbildung 2 zeigt an einem Beispiel von Innenraumortung, wie aus den Aufenthaltszeiten einer zunächst nicht identifizierten Person leicht auf den Standort ihres Schreibtisches (H) und damit auf ihre Identität geschlossen werden kann (Beresford, 2005).

Auch die zunehmende Verbreitung von mit Geotags versehenen Digitalfotos, auf denen Personen abgebildet sind (bei gleichzeitigen Fortschritten in der Gesichtserkennung) trägt dazu bei, dass Personen nachträglich durch die Verarbeitung vorhandener Datenbestände identifiziert werden können, wodurch ihnen die Kontrolle über die eigenen Ortungsdaten entgleitet.

Es erscheint deshalb prinzipiell unmöglich, eine eindeutige Schwelle für den Personenbezug von Geodaten zu definieren (vgl. auch Abschnitte 3.5.2 und 3.5.3). Dies ist darin begründet, dass es sich auch aus technisch-statistischer Sicht um einen fliessenden Übergang handelt und ein Personenbezug durch Anwendung entsprechender Verfahren «schleichend» entstehen kann: «...es erscheint offensichtlich, dass es keine klar definierte Regel oder einen Standard gibt, um auf einfache Weise zu entscheiden, an welchem Punkt Geodaten zu Personendaten werden.» (NRC, 2010b, S. 31; Übers. durch die Autoren).

Aus Sicht des Individuums, das die Kontrolle über seine Ortungsdaten zum Schutz seiner Persönlichkeit nicht preisgeben will, bleiben prinzipiell drei Möglichkeiten:

- *Resignation/Anpassung:* Das Bedürfnis nach Kontrolle über die eigenen Ortungsdaten wird aufgegeben oder in seiner Wichtigkeit zurückgestuft; die damit verbundenen Risiken werden in Kauf genommen.

- *Verstärktes Engagement:* Einsatz für einen Ausbau der Regulierung der Bearbeitung von Ortungsdaten und/oder für eine wirksamere Durchsetzung des geltenden Rechts.

- *Abstinenz:* Verzicht auf die Nutzung bestimmter Technologien, um die Entstehung von Ortungsdaten über die eigene Person möglichst zu vermeiden.

Entlang dieser Reaktionsmöglichkeiten könnten auch die zukünftigen gesellschaftlichen Konfliktlinien verlaufen. Dies ist auch im Zusammenhang mit der abnehmenden Freiwilligkeit der Nutzung von Ortungstechnologien zu sehen (siehe Abschnitt 4.1.3), die das Konfliktpotenzial verschärft.

4.1.2 Sicherheit oder Freiheit – was hat Priorität?

Ortungstechnologien, die zur *Fremdortung* genutzt werden (wie in Abschnitt 2.2.1 definiert) sind Überwachungstechnologien. Eine Person zu überwachen, kann stets ihrer eigenen Sicherheit (oder auch der Sicherheit anderer) dienen, aber auch ihre Freiheit einschränken.

Dass die Menschen hier eine implizite Güterabwägung vornehmen, zeigt sich beispielsweise bei der unterschiedlichen Bewertung von Überwachungskameras. Je nach räumlich-sachlichem Zusammenhang wird Videoüberwachung von den Betroffenen in unterschiedlichem Masse akzeptiert. Im öffentlichen Raum, wie beispielsweise in U- und S-Bahnhöfen oder auf öffentlichen Plätzen, besteht laut Petri (2010) eine relativ hohe Akzeptanz. Demgegenüber weist die hohe Zahl an Eingaben bei den Datenschutzbehörden darauf hin, dass die Videoüberwachung im private(re)n Rahmen, etwa in der eigenen Strasse oder am Arbeitsplatz, grosse Ablehnung erfährt. Die Ursachen für die unterschiedliche Bewertung der Überwachung werden dadurch erklärt, dass sich die Bevölkerung von Überwachungskameras im öffentlichen Raum eine erhöhte Sicherheit verspricht. Petri weist auf einen weiteren Aspekt hin, dessen Voraussetzungen sich durch die technische Entwicklung aber ändern könnten: «Möglicherweise besteht … auch die Einschätzung, dass man als Betroffener im öffentlichen Raum zwar bildlich erfasst wird, aber in der Anonymität der Masse unbehelligt bleibt, solange man sich ‹normgerecht› verhält. Einmal abgesehen davon, dass gerade dieser Effekt von Videoüberwachung hinsichtlich ihrer Ausgrenzungseffekte gesellschaftspolitisch problematisch ist, trifft diese Annahme angesichts der heutigen technischen Möglichkeiten nicht mehr uneingeschränkt zu.» (Petri, 2010, S. 28).

Je mehr Lebensbereiche der Überwachung mit technischen Mitteln zugänglich werden, desto stärker werden auch individuelle Unterschiede bezüglich dieser Güterabwägung hervortreten. Besonders sensible Bereiche sind hier die Überwachung von desorientierten Personen (Demenzkranken) und von Kindern.

Im Zusammenhang mit der Überwachung von Schulkindern verweisen wir auf die bereits erwähnten Kontroversen um den Einsatz von RFID-Tags für Schüler an US-amerikanischen und britischen Schulen (Abschnitt 2.4.5).

Die elektronische Überwachung desorientierter Personen …

1. soll dem desorientierten Menschen das Leben in seiner gewohnten Umgebung ermöglichen.
2. soll dem desorientierten Menschen möglichst grosse Freiheit gewähren bzw. bewahren.
3. soll die Beziehungen des desorientierten Menschen zu seiner Umgebung verbessern oder erhalten.
4. soll vom desorientierten Menschen und seiner Umgebung bedingungslos akzeptiert werden. Eine Entscheidung kann in jedem Fall rückgängig gemacht werden.
5. soll die Würde des desorientierten Menschen wahren.

Abbildung 3: Charta der Stiftung für elektronische Hilfsmittel (FST, 2000, S. 8)

4.1.3 Wie freiwillig wird Ortung bleiben?

Die digitalen Technologien schaffen allgegenwärtige und nahezu unbeschränkte Möglichkeiten zur Kommunikation. Internetplattformen und soziale Netzwerke bieten die Möglichkeit, scheinbar ohne Regeln und Schranken Kontakte zu knüpfen, zu pflegen oder sich selbst darzustellen. Aufenthaltsorte, Bilddaten, Informationen der verschiedensten Art zur eigenen Person, einem Arbeitskollegen oder einer Mitschülerin werden zu allgemein oder auch eingeschränkt zugänglichen Daten. Ob diese persönlichen Informationen ihres ursprünglichen Zusammenhangs enthoben werden, lässt sich genauso wenig kontrollieren wie die Möglichkeit, dass die entsprechenden Daten zu späteren Zeitpunkten irgendwo im Internet wieder auftauchen (Petri, 2010; Cheng, 2012), solange die Aufbewahrungsdauer persönlicher Daten nicht wirksam begrenzt werden kann (Baeriswyl, 2011: vgl. auch Abschnitte 3.2 und 3.7.2).

Diese Situation hat einen paradoxen Effekt, der in der Kommunikationspsychologie seit langem bekannt ist: Der Versuch, Kommunikation zu verweigern, wenn die Möglichkeit zur Kommunikation gegeben ist, ist selbst ein Akt der Kommunikation. Es ist deshalb unmöglich, *nicht* zu kommunizieren (oder jedenfalls: nicht interpretiert zu werden), wenn ein Kommunikationskanal erst einmal zur Verfügung steht. Dieses sog. metakommunikative Axiom (Watzlawick,

1996) entfaltet heute, angesichts der immer zahlreicher verfügbaren Kommunikationskanäle, eine mächtige Wirkung: Je mehr Kommunikationskanäle zur Verfügung stehen, desto mehr wird man (implizit) kommunizieren bzw. interpretiert werden, weil man eben auch durch den eingeschränkten Gebrauch oder den Nichtgebrauch eines Kanals etwas mitteilt. In der Welt der Ortungstechnologien gilt das nun auch für die Kanäle, auf denen man den eigenen Aufenthaltsort bekannt gibt.

Heesen spricht in einem ähnlichen Zusammenhang vom «Subtext» der Einstellungen, die man z.B. auf den persönlichen Seiten in sozialen Netzen vornimmt, um zu regeln, wem man wie viel vom eigenen Datenbestand kommuniziert. «Durch das Gewähren beziehungsweise Verweigern von personenbezogenen Daten wie etwa Lokationsanfragen hinterlassen die Beteiligten eines interaktiven Netzwerkes jedoch indirekt eine Darstellung ihrer persönlichen Beziehungsnetzwerke – den sozialen Subtext ihrer Nutzungseinstellungen – der selbst wieder in Wechselwirkung steht zur Entstehung oder Festigung von Beziehungen.» (Heesen, 2008, S. 241).

Selbst Techniken zur Anonymisierung oder Pseudonymisierung von Identitäten verhindern laut Heesen nicht, dass eben diese Strategien der persönlichen Datenverwaltung zu einem Bestandteil der Fremd- und Eigenwahrnehmung werden, mit der paradoxen Konsequenz: «In sozialen Netzwerken … kann der Selbstdatenschutz insofern problematisch werden, als er *ex negativo* über das Verhalten und die Präferenzen der jeweiligen Nutzerinnen und Nutzer berichtet.» (Heesen, 2008, S. 241).

Die Konfliktlinie verläuft hier zwischen den Verteidigern der klassischen Privacy im Sinn von «The right to be let alone» (Warren & Brandeis, 1890) und jenen Nutzerinnen, die die zunehmende Verfügbarkeit von Kommunikationskanälen (einschliesslich Fremdortung) begrüssen oder zumindest akzeptieren.

4.2 Kriterienkatalog für gesellschaftliche Relevanz

Wie wir in Kapitel 2 gezeigt haben, bieten Ortungstechnologien vielfältige Anwendungsmöglichkeiten, die sich möglicherweise in naher Zukunft ausweiten werden. Nicht alle Anwendungen haben aber die gleiche gesellschaftliche Relevanz. Nachfolgend versuchen wir deshalb zunächst, *generelle* Kriterien für die gesellschaftliche Relevanz neuer Anwendungsmöglichkeiten von (beliebigen) Technologien zu definieren. Im Anschluss daran beschreiben wir *spezielle* Kriterien, die sich auf Ortungstechnologien im Besonderen beziehen.

Der Kriterienkatalog wird für die Auswahl der beiden Vertiefungsfelder für diese Studie eingesetzt. Sinngemäss werden wir ihn für die spätere Gewichtung von Auswirkungen einsetzen.

4.2.1 Generelle Kriterien für die gesellschaftliche Relevanz neuer Technikanwendungen

Die generellen Kriterien für die gesellschaftliche Relevanz neu entstehender Technikanwendungen sind in Tabelle 4 zusammengefasst und werden nachfolgend erläutert.

Veränderungspotenzial

Das erste Kriterium ist das *Veränderungspotenzial*. Um im betrachteten Zeitraum[74] gesellschaftliche Veränderungen auslösen zu können, muss eine Anwendung erstens in diesem Zeitraum technisch und ökonomisch machbar sein (Unterkriterium *Machbarkeit*). Zweitens muss die Anwendung entweder grosse Chancen oder grosse Risiken[75] (oder beides) mit sich bringen (Unterkriterien *Grosse Chancen* bzw. *Grosse Risiken*), und die erwarteten Veränderungen müssen die breite Bevölkerung betreffen, also nicht auf spezialisierte Nutzergruppen beschränkt bleiben (Unterkriterium *Breitenwirkung*).

[74] Bei der Anwendung aller hier genannten Kriterien muss ein Zeithorizont angenommen werden Diese Studie betrachtet (wie in der Einleitung angegeben) den Zeitraum von 2010–2020.

[75] Ein Risiko ist ein möglicherweise eintretender Schaden, eine Chance (dazu spiegelbildlich) ein möglicherweise eintretender Nutzen.

Tabelle 4: Generelle Kriterien für die gesellschaftliche Relevanz neu entstehender Technikanwendungen

1. Veränderungspotenzial:
a. Machbarkeit: Die Anwendung ist im betrachteten Zeitraum technisch und ökonomisch realisierbar.
b. Grosse Chancen: Die Anwendung hat einen hohen potenziellen Nutzen
c. Grosse Risiken: Die Wahrscheinlichkeit, dass ein hoher Schaden eintritt, ist nicht zu vernachlässigen.
d. Breitenwirkung: Die erwarteten Wirkungen betreffen die breite Bevölkerung im täglichen Leben.
2. Ambivalenz:
a. Hauptwirkungen: Es besteht im Voraus kein gesellschaftlicher Konsens, welche der erwarteten Wirkungen als positiv (d.h. als Chance) oder negativ (d.h. als Risiko) zu bewerten sind.
b. Nebenwirkungen: Es ist möglich, dass unerwartete Nebenwirkungen (wie z.B. Missbrauch) auftreten, über deren Gewichtung im Voraus kein Konsens besteht.
3. Konfliktpotenzial
a. Freiwilligkeit: Die Nutzung der Anwendungen ist für eine relevante Zahl von Personen nicht oder nur teilweise freiwillig, weil die Vermeidung der Nutzung mit relevanten Nachteilen verbunden wäre oder weil die Nutzung auch unbewusst erfolgen kann. Je geringer die Freiwilligkeit, desto höher das Konfliktpotenzial.
b. Gerechtigkeit: Wahrgenommene Chancen und Risiken sind nicht gleich auf gesellschaftliche Gruppen verteilt, d.h. eine Gruppe nutzt hauptsächlich die Chancen, eine andere trägt hauptsächlich die Risiken. Je geringer die Gerechtigkeit, desto höher das Konfliktpotenzial.

4.	Klärungsbedarf Es bestehen Unklarheiten in den von der Politik gesetzten Rahmenbedingungen (insbesondere in rechtlichen Hinsicht) in Bezug auf die neuen technischen Möglichkeiten.
5.	Mangelnde Resilienz Es sind Risiken mit der Anwendung von Technologien verbunden, für deren Abwehr keine geeigneten gesellschaftlichen Strukturen und Institutionen vorhanden sind.

Ambivalenz

Das zweite generelle Kriterium ist die *Ambivalenz* der Anwendung hinsichtlich gesellschaftlicher Werte. Technologien entstehen nicht durch einen vorgegebenen Prozess «ausserhalb» der Gesellschaft, sondern sind sozial eingebettet, d.h. sie werden stets vor dem Hintergrund von Werthaltungen entwickelt, interpretiert und genutzt. Allein die Unterscheidung zwischen Nutzen und Schaden bzw. Chancen und Risiken ist nicht ohne impliziten Bezug auf ein Wertesystem, einen normativen Rahmen möglich. Ein Teil der für unser Thema relevanten Werthaltungen ist in die Gesetzgebung eingeflossen und bildet den rechtlichen Rahmen, wie er in Kapitel 3 beschrieben wurde. Ein grosser Teil der Werthaltungen drückt sich aber auch in *ungeschriebenen* sozialen Normen aus, die zwischen sozialen Gruppen variieren können.

Wir bezeichnen eine Anwendung dann als ambivalent, wenn nicht a priori klar ist, wie sie auf der Grundlage allgemein akzeptierter Wertvorstellungen zu bewerten ist. Dies kann der Fall sein, weil die erwarteten Veränderungen (*Hauptwirkungen* der Anwendungen) unterschiedlich bewertet werden oder weil es *Nebenwirkungen* gibt, über die keine Einigkeit besteht. Gerade im Bereich der Informations- und Kommunikationstechnologien sind unintendierte Konsequenzen keine Ausnahme (Hilty et al. 2006; Hilty, 2007). Nebenwirkungen neuer Technologien können unterschiedlich bewertet werden; aber selbst wenn Konsens darin bestehen sollte, dass sie unerwünscht sind, kann die Abwägung mit den intendierten Konsequenzen (Hauptwirkungen) unterschiedlich ausgehen.

Ein Beispiel soll den letzgenannten Fall verdeutlichen: Würde heute die Technik des Automobils eingeführt, so würde wohl niemand die zu erwartende Zahl der Verkehrsunfälle als erwünschte Konsequenz betrachten; dennoch könnte es unterschiedliche Meinungen geben, ob die Nebenwirkungen so schwerwiegend sind, dass sie starke Einschränkungen der Entwicklung der Technologie rechtfertigen (oder verlangen) würden oder nicht.

Konfliktpotenzial

Ein zentrales Element gesellschaftlicher Entwicklung ist der Umgang mit Konflikten, die durch das Spannungsverhältnis zwischen grundlegenden Werten und Normen entstehen, wie oben schon beschrieben. Als drittes Kriterium wählen wir deshalb das Kriterium *Konfliktpotenzial* mit den zwei Unterkriterien *Freiwilligkeit* und *Gerechtigkeit* (Hilty et al., 2003).

- Das Unterkriterium *Freiwilligkeit* leitet sich aus dem Autonomieprinzip der traditionellen Ethik ab. Bei der alltäglichen Techniknutzung gibt es selten eine harte Grenze zwischen Freiwilligkeit und Unfreiwilligkeit, sondern eher ein Kontinuum von «Teilfreiwilligkeit». Entscheidend ist der Umfang der Nachteile, die eine Person in Kauf nehmen muss, wenn sie die – aus ihrer Sicht unerwünschten – Folgen zu vermeiden versucht, die die neue Technikanwendung mit sich bringt. Es besteht hier ein Zielkonflikt mit dem technischen Entwicklungsziel der Unaufdringlichkeit (unobtrusiveness), die Bestandteil von Technikvisionen wie Pervasive Computing oder Ambient Intelligence ist: Wenn sich der Nutzer nicht bewusst ist, dass er eine Funktion nutzt, ist die Freiwilligkeit in Frage gestellt.
- Das zweite Unterkriterium des Konfliktpotenzials ist die *Gerechtigkeit* in der Techniknutzung. Sie ist dann gefährdet, wenn die Chancen und Risiken ungleich verteilt sind. Im gedachten Extremfall kommt ein Teil der Gesellschaft in den Genuss aller Chancen, während ein anderer Teil alle Risiken trägt. Wird ein Mangel an Gerechtigkeit wahrgenommen, entstehen Kontroversen und Konflikte.

Klärungsbedarf

Eine technische Entwicklung ist auch dann gesellschaftlich relevant, wenn die bestehenden *Rahmenbedingungen* aufgrund der neuen technischen Möglichkeiten nicht mehr eindeutig erscheinen. Das gilt besonders für die rechtlichen Rahmenbedingungen, die von der technischen Entwicklung überholt werden können, z.B. weil der Gesetzgeber bestimmte Kategorien von Handlungen, die technisch möglich werden, nicht vorhersehen konnte. Definitionsprobleme und Fragen der Anwendbarkeit von Regelungen bzw. der Zuständigkeit von Institutionen müssen dann geklärt werden.

Mangelnde Resilienz

Mangelnde Resilienz ist gegeben, wenn eine technische Anwendung erhebliche Risiken mit sich bringt, für deren Kontrolle und Abwehr noch keine geeigneten gesellschaftlichen Strukturen und Institutionen existieren.

4.2.2 Spezielle Relevanzkriterien in Bezug auf Ortungstechnologien

Neben den generellen Kriterien für die gesellschaftliche Relevanz technischer Anwendungen gibt es naheliegende spezielle Kriterien, die nur im Kontext der vorliegenden Studie gelten. Diese sind:

1. Die Anwendungen beruhen entscheidend auf der *Erzeugung und Verarbeitung von Positionsdaten (Standortdaten, Ortungsdaten)* und fallen damit in den Themenbereich dieser Studie.
2. Die Anwendungen sollen bezüglich des *rechtlichen Rahmens* oder der bereits erkennbaren *Konfliktlinien* im Bereich der Ortungstechnologien relevant sein (Abschnitt 4.1).
3. Die Anwendungen sollen hinsichtlich der tangierten Werte und Interessen *exemplarischen Charakter* für eine breitere Gruppe von Anwendungen haben, damit die Ergebnisse möglichst auch auf andere Anwendungen übertragbar sind.
4. Die Anwendungen sollen möglichst *unterschiedliche Funktionen der Ortung* (z.B. Komfort, Sicherheit, soziale Vernetzung) und verschiedene Nutzer-

gruppen abdecken, damit die Studie für verschiedene Zielgruppen von Nutzen sein kann.

4.2.3 Auswahl der Vertiefungsfelder der Studie

Als Anwendungsfelder, mit denen sich diese Studie vertieft beschäftigt (Vertiefungsfelder) wurden in einer ersten Phase zunächst betrachtet:

1. Georeferenzierte Online-Bilddatenbanken: Georeferenzierte Bildpanoramen (z.B. Google Street View, Rundumzug) und georeferenzierte Bildverbände (z.B. Microsoft Photosynth) und die Folgen für die Ortung von Personen und Fahrzeugen auf Fotos mit zunehmen automatisierten Verfahren;
2. Personenortung durch Handys: Ortung von Partnern und Kindern, Ortung bei Notfall oder Diebstahl und der potenzielle Missbrauch; Ortungsdaten als Nebenprodukt von standortbasierten Diensten (Location-Based Services) und Smartphone-Apps;
3. Ortung und Auto: Navigation, Flottenmanagement, Notruf bei Unfällen und Pay-as-you-Drive Versicherungen mit dem Fokus auf der Überwachung von Fahrzeugen, besonders im Kontext Arbeit (Überwachung der Fahrer durch Arbeitgeber);
4. Personenortung in Gebäuden: Indoor-Ortung für standortbasierte Dienste (wie z.B. Shopkick: Handelsketten wie Best Buy in USA geben Rabattpunkte, wenn der Kunde sich in den Einkaufsräumen akustisch orten lässt) und Indoor-Ortung im Kontext Arbeit;
5. Nutzung von Geodaten zur Auswertung von Ortsangaben: Auswertung der durch Ortung gewonnenen Daten im Kontext vorhandener Geodaten (v.a. thematischen Karten), besonders als Sekundärnutzung von Daten (secondary use, dual use), Vermischung staatlicher Aufgaben und kommerzieller Interessen (Beispiel Solarkataster); welche Kombinationen von Ortung und Auswertungskontexten bergen Konfliktpotenzial?
6. Soziale Netze und Ortung: Verbindung von Social-Networking-Plattformen mit Location-Based Services, Matching von Profilen mit Personen, die sich in der Nähe befinden, mit Möglichkeit zur nachträglichen Kontaktaufnahme (Smartphone-App Aka-Aki), laufende Information über den Aufenthaltsort

von Freunden (Facebook Places, Google Latitude u.a.); Chancen und Risiken für Sozialkontakte bis hin zu Missbrauch für Stalking.

Die Begleitgruppe des Projekts hat beschlossen, die Anwendungsfelder *Mobilität* (alle Verkehrsarten) und *Soziale Netze* zu fokussieren. Mit Mobilität sind die Punkte 3 und Teilaspekte von 1 und 2 (soweit es dabei um Verkehrsvorgänge oder den öffentlichen Raum geht) abgedeckt. Das Anwendungsfeld Soziale Netzt entspricht Punkt 6.

Diese Auswahl berücksichtigt das hohe Veränderungspotenzial, das auf diesen beiden Gebieten zu erkennen ist, und ebenso das hohe Konfliktpotenzial aufgrund eingeschränkter Freiwilligkeit: Die Notwendigkeit, öffentliche Infrastrukturen für die eigene Mobilität zu nutzen, oder auch der soziale Druck zur Präsenz auf Plattformen der sozialen Netze machen es dem Einzelnen schwer bis unmöglich, den Entwicklungen auszuweichen.

Trotz dieser Auswahl von zwei Vertiefungsfeldern werden wir bei der Strukturierung der Auswirkungen (Kapitel 7) und bei der Ableitung von Handlungsbedarf (Kapitel 8) Chancen und Risiken berücksichtigen, die auch auf anderen Anwendungsgebieten auftreten. Die Vertiefungsfelder sind also exemplarisch zu verstehen; wir untersuchen sie vertieft, um durch anschliessende Abstraktion die prinzipiellen Wirkungen von Ortung herauszuarbeiten und vorsorglichen Handlungsbedarf zu erkennen.

Die beiden nachfolgenden Kapitel präsentieren die Analysen der Vertiefungsfelder.

5 Vertiefungsfeld «Mobilität»

5.1 Mobilität und Ortungstechnologien

5.1.1 Mobilität und Verkehr

Zunehmende Mobilität ist ein Kennzeichen moderner Gesellschaften. Häufig wird Mobilität mit *Verkehr* gleichgesetzt, obwohl es überzeugende Argumente gibt, Mobilität als den *Nutzen des Verkehrs* zu verstehen. Es wird dann beispielsweise erkennbar, dass die gleiche Mobilität mit unterschiedlichem Aufwand an Verkehr erreicht werden kann (Monheim & Monheim-Dandorfer, 1990).

Mobilität kann aber auch als Herausforderung unserer modernen Gesellschaft verstanden werden: Mit der Digitalisierung und Globalisierung haben viele Aktivitäten eine Flexibilisierung und Beschleunigung erfahren. Diese Dynamik wirkt sich auf Einzelne ebenso aus wie auf Unternehmen oder staatliche Organisationen und erfordert neue Strategien und Gestaltungsansätze zu ihrer Bewältigung.

In den Verkehrsstatistiken ist ein Wachstum an Verkehr zu verzeichnen. Diese Entwicklung basiert nicht auf der Anzahl der Ziele, die eine Person pro Tag aufsucht, sondern in der Zunahme der Entfernungen: Obwohl sich die Anzahl der Wege pro Tag im Personenverkehr wenig verändert hat, nehmen die zurückgelegten Distanzen und – damit zusammenhängend – die Zahl der motorisierten Fahrzeuge stetig zu. Dies hat u.a. dazu geführt, dass sich die gesamte Personenverkehrsleistung (gemessen in Personenkilometern, pkm) in der Schweiz zwischen 1970 und 2008 mehr als verdoppelt hat. Im Jahr 2009 waren 5,4 Millionen Motorfahrzeuge, davon 4 Millionen Personenwagen, in der Schweiz gemeldet. 80% der Schweizer Haushalte verfügten über mindestens einen Personenwagen, 30% hatten zwei und mehr Autos. Auch der Güterverkehr hat sich aufgrund der zunehmenden Globalisierung und internationalen Arbeitsteilung im gleichen Zeitraum verdreifacht (BFS, 2010).

Vor allem in Agglomerationsräumen führt dies zu Problemen beim Verkehrsfluss, aber auch zu Lärm- und Luftbelastungen, Unfällen und in der Folge zu steigenden externen Kosten. Die Kapazitäten der Verkehrswege stossen an

Grenzen, da ein weiterer Ausbau mit steigenden Grenzkosten verbunden ist. Das Staurisiko ist in den grossen Agglomerationen sowie auf den diese verbindenden Hauptachsen am höchsten, besonders wenn gleichwertige Ausweichrouten fehlen (UVEK, 2010).

5.1.2 Relevante Entwicklungen

Im Vertiefungsfeld Mobilität untersuchen wir die Rolle von Ortungstechnologien in Anwendungen, die Mobilität unterstützen bzw. den Verkehr im öffentlichen oder für die Öffentlichkeit zugänglichen Raum betreffen. Dabei sind folgende Entwicklungen relevant:

Technologische Entwicklungen:

- Die Zahl der ortungsfähigen Endgeräte steigt, ebenso wird das Spektrum der eingesetzten Ortungstechnologien breiter. Dabei ist die zunehmende Vernetzung verschiedener Technologien von Bedeutung (beispielsweise WLAN, RFID, Mobilfunk, vgl. auch Kapitel 2). Experten schätzen, dass die Zahl von SIM-Cards, wie sie in Handys und anderen Mobilfunk-Endgeräten eingesetzt werden, in der Schweiz bis zum Jahr 2015 auf 100 Mio. ansteigen wird. Damit kämen rechnerisch auf einen Schweizer Bürger ca. 12 Mobilfunkkarten. Die hohe Zahl der SIM-Cards verdeutlicht, dass damit auch Anwendungen der Maschine-zu-Maschine-Kommunikation realisiert werden.[76] Kommunikationsvorgänge werden also in vielen Fällen nicht mehr direkt von einer Person veranlasst, sondern von Geräten automatisch ausgelöst, wobei die mobile Kommunikation als Nebeneffekt immer auch eine (zumindest grobe) Ortung ermöglicht (vgl. auch Mattern, 2005).
- Die Leistungsfähigkeit von Ortungstechnologien steigt, während gleichzeitig die äusseren Abmessungen der Endgeräte sinken. Beispielsweise werden Videoüberwachungssysteme im öffentlichen Raum kleiner. Gleichzeitig liefern die Systeme jedoch immer detailreicheres Bildmaterial, das durch Fortschritte in der Bildverarbeitung die Möglichkeiten verbessert, Personen automatisch zu erkennen. Durch die immer höhere Speicherdichte und die

[76] Persönliche Kommunikation mit Andreas Knöpfli, Präsident des Schweizerischen Wirtschaftsverbandes der Anbieter von Informations-, Kommunikations- und Organisationstechnik (SWICO).

sinkenden Preise für Speicherplatz werden längere Aufbewahrungszeiten der Videodaten möglich.

- Navigationsgeräte unterstützen die Routenplanung, sogenannte Onboard-Units ermöglichen das schnelle Passieren von Mautstellen und Fahrerassistenzsysteme unterstützen Fahrzeuglenker und ihr Verhalten im Verkehr (Mühlethaler et al., 2003). Bei diesen Prozessen fallen nicht nur immer mehr Daten an, sie werden auch immer häufiger über Mobilfunknetze übertragen sowie an zentralen Stellen gespeichert und ausgewertet.

Entwicklung des Einsatzes und der Einsatzzwecke:

- Die Überwachung des öffentlichen Raums mit Videokameras und Kontrollstellen für den Verkehr nimmt zu, ebenso die Nutzung von Auswertungsmöglichkeiten für die dabei gewonnenen Daten.
- Mobile Endgeräte, insbesondere Smartphones, entwickeln sich zu Plattformen, die die individuelle Mobilität unabhängig vom Verkehrsmittel unterstützen.
- Ortungstechnologien werden genutzt, um kundenorientierte Informationsangebote (beispielsweise die aktuellen Ankunftszeiten von Verkehrsmitteln an Haltestellen) bereitzustellen. Aus Betreibersicht sollen vernetzte und integrierte Systeme Verkehrsflüsse optimieren (Friedewald, 2011). Informations-Dienstleistungen dienen auch dazu, die Akzeptanz neuer Technologien (beispielsweise von Elektrofahrzeugen mit ihren geringeren Reichweiten und noch unzureichenden Infrastrukturen) zu steigern oder umweltorientierte Verhaltensänderungen (beispielsweise den Umstieg auf den öffentlichen Verkehr) zu fördern, um den Verbrauch fossiler Energie und Stauzeiten zu reduzieren (Palma & Lindsey, in Press).
- Ortungstechnologien werden für den Schutz, die Sicherheit bzw. für Kontrollzwecke nicht nur von Personen, sondern auch von beweglichen Gütern genutzt. Dazu zählen Anwendungen wie der Diebstahlschutz oder der Schutz vor Vandalismus. Assistance-Funktionen wie elektronische Fahrtenbücher oder die Ortung von Fahrzeugen in Echtzeit beispielsweise unterstützen das Flottenmanagement.

Neue Märkte, neue Wettbewerber und neue Geschäftsmodelle:

- Ortungstechnologien gelten als Wachstumsbereich, mit denen sich neue Märkte national und international erschliessen lassen. Sie bieten damit ein Wachstumspotenzial für die Schweizer digitale Wirtschaft.
- Viele Telekommunikationsunternehmen sowie Anbieter von Endgeräten und Anwendungen (beispielsweise Apple) oder Navigationsdienstleistungen (beispielsweise TomTom) erfassen kontinuierlich Standorte der Nutzer, sofern die diesbezüglichen Funktionen im Endgerät verfügbar sind und nicht deaktiviert werden. Diese Daten werden zu anonymisierten Bewegungsprofilen kombiniert und bilden die Basis für neue Geschäftsmodelle: Vodafone beispielsweise erfasst Bewegungsprofile aus dem Mobilfunknetz und übermittelt sie an den Anbieter von Navigationsdiensten. Der Navigationssystem-Anbieter TomTom erfasst Daten für den Stauprognose-Dienst «HD Traffic» und verkauft anonymisierte Bewegungsprofile seiner Kunden an Dritte (Lischka, 2010; siehe auch Abschnitt 2.4.6).
- Weitere Geschäftsmodelle beziehen sich auf personalisierte und standortbezogene Nutzerinformationen oder sogenannte «Unique Mobile Users (UMUs)»[77]. Apple beispielsweise plant, mit einem neuen Angebot «iAd» in den Markt für lokalisierte Werbung einzusteigen. (Lischka, 2010) Facebook-Nutzer, die das soziale Netzwerk auf ihrem Mobiltelefon nutzen und ihren Standort preisgeben, können bereits in vier europäischen Ländern von Unternehmen mit lokalisierter Werbung kontaktiert werden.[78] Derartige Geschäftsmodelle fussen nicht nur auf mobilen Endgeräten: Nach Presseberichten soll Google im Jahr 2011 bereits mehr als eine Milliarde Dollar verdienen, indem die Suchmaschine «Ergebnisse abhängig vom jeweiligen Aufenthaltsort des Nutzers anzeigt und damit auch die Werbung an den Ort anpasst.» (Schmidt, 2011).

Am Beispiel von Assistance-Leistungen von Versicherungsunternehmen wird deutlich, dass auch neue Wettbewerber mittels Ortungstechnologien neue

[77] Der Begriff «Unique Mobile Users (UMU)» wird in der Werbung verwendet, um die Zahl der Personen zu beziffern, die mit Seiten im mobilen Internet oder personalisierten Werbebotschaften im Mobilfunk erreicht werden («Nutzer-Tracking» einschliesslich von Analysen zur Beschreibung der Nutzergruppen). Diese Herangehensweise ergänzt die Reichweiten- und Strukturanalysen, wie sie bereits vom E-Commerce im Internet bekannt sind und überträgt sie auf M-Commerce und auf standortbezogenes Marketing.

[78] In Deutschland, Grossbritannien, Spanien, Frankreich Italien nutzen Unternehmen wie Douglas, Benetton, Esprit oder H&M das Facebook-Merkmal für Werbung. (Rungg, 2011)

Geschäftsfelder erschliessen wollen. Die Mobilfunk-Ortung von Personen beispielsweise nach einer automatisierten Meldung über einen möglichen Sturz oder das Angebot von Armbanduhren mit Ortungstechnologie für Demenzkranke weisen darauf hin, dass Versicherungen neue Dienstleistungsmärkte erschliessen. Das Versicherungsunternehmen Allianz hat eine Tochtergesellschaft gegründet, um in Rettungsleitstellen europaweit die IT-Infrastruktur für die Lokalisierung von Notrufen per Handy bereitzustellen (Müller, 2011).

5.1.3 Fokus Personenverkehr im öffentlichen Raum

Die folgenden Überlegungen vertiefen diese Analyse mit einem Schwerpunkt auf Anwendungen im *Personenverkehr* im *öffentlichen Raum,* wobei der geographische Fokus auf der Schweiz liegt. Wichtige internationale und insbesondere europäische Entwicklungen werden ergänzend berücksichtigt. Konkret werden die folgenden Forschungsfragen untersucht:

- Welche Ortungssysteme sind im Bereich «Mobilität im öffentlichen Raum» derzeit in der Schweiz im Einsatz, welche sind geplant oder werden diskutiert?
- Welche Aufgaben erfüllen die Systeme heute, welche technischen und organisatorischen Leistungsmerkmale und Funktionalitäten weisen sie auf?
- Welche Daten werden von wem für welche Zwecke erhoben, gespeichert oder weitergegeben?
- Liegen Erkenntnisse vor, wie die Systeme von Nutzern bewertet bzw. akzeptiert werden?
- Welche «Push-Faktoren» ergeben sich für die Schweiz aus Entwicklungen in der Europäischen Union, beispielsweise durch die grenzübergreifende Zusammenarbeit?
- Zeichnen sich gesellschaftliche Konflikte in Bezug auf spezielle Anwendungen ab, insbesondere mit Bezug auf die in den Abschnitten 3.1 bis 3.3 angesprochenen Themen?

Öffentlicher Raum und Infrastrukturen

Verkehr findet in der Regel im öffentlichen Raum bzw. im öffentlich zugänglichen Raum statt. Zum *öffentlichen Raum* zählt laut Definition des Eidgenössischen Justiz- und Polizeidepartements (EJPD) einerseits der im Eigentum des Gemeinwesens stehende und grundsätzlich für jede Person zugängliche Raum (z.B. Strassen und Plätze) sowie andererseits der Raum, an dem niemand Eigentum haben kann, für deren Schutz oder Unterhalt der Staat aber zu sorgen hat (z.B. Gewässer). Der *öffentlich zugängliche Raum* umfasst Privateigentum, das der Erfüllung einer öffentlichen Aufgabe dient. Diese Räume sind für jede Person zugänglich und werden regelmässig von vielen Personen genutzt (beispielsweise Flughäfen, Bahnhöfe, Transportmittel) (EJPD, 2007).

Infrastrukturnetze sind laut Definition des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation (UVEK) «langlebige physische Einrichtungen, die der Versorgung von Bevölkerung und Wirtschaft mit grundlegenden Gütern wie Mobilität, Energie oder Kommunikation dienen.» Sie dienen nicht nur Privatpersonen, sondern bilden auch die Basis für gesellschaftliche Wohlfahrt und die Leistungsfähigkeit der Volkswirtschaft. Damit sind sie «entsprechend oft Gegenstand einer politisch definierten Grundversorgung» (UVEK, 2010, S. 9).

Die Finanzierung der staatlichen Infrastrukturnetze «Strasse» und «Schiene» erfolgt über die öffentlichen Haushalte: Bau-, Unterhalts- und Betriebskosten des Nationalstrassennetzes werden über zweckgebundene Abgaben wie die Mineralölsteuer oder die Autobahnvignette von den Strassennutzern getragen, die Infrastrukturkosten des Schienennetzes von den Netzbenutzern (Trassenpreise), den Steuerzahlern (Betriebs- und Investitionsbeiträge) und Strassennutzern (Beiträge aus Spezialfinanzierungen, Infrastrukturfonds und zweckgebundene Zuweisungen).

In der Schweiz wird diskutiert, wie das Gleichgewicht zwischen Ausgaben und Einnahmen erhalten werden kann. Verkehrsnetze werden älter und komplexer, Verkehrsbelastungen steigen und führen zu neuen Herausforderungen bezüglich Sicherheit, Umwelt und Management von Verkehrsflüssen. Experten gehen davon aus, dass der «durchschnittliche jährliche Finanzierungsbedarf bis 2030 um 22% bis 33%» steigen wird (UVEK 2010, S. 64). Gleichzeitig sinken die Einnahmen beispielsweise durch das Absinken des Treibstoffverbrauchs moderner Fahrzeuge mit effizienten Antriebstechnologien (UVEK 2010, S. 64).

Vor diesem Hintergrund werden auch neue Management- und Finanzierungsmodelle thematisiert, bei denen Ortungstechnologien eine zentrale Rolle spielen oder einen massgeblichen Beitrag leisten können. Das Spektrum umfasst höhere und verursachergerechte Beiträge der Verkehrsteilnehmer auf Strasse und Schiene beispielsweise durch gebührenpflichtige Strecken, aber auch die schnelle Abwicklung beispielsweise von Bezahlvorgängen durch die Ortung von Verkehrsteilnehmern im Schienenverkehr. Auch für die Finanzierung von Verkehrsinfrastrukturprojekten im Rahmen von Public-Private Partnerships werden Strassenbenutzungsgebühren diskutiert (UVEK 2010, S. 65).

Die Strasseninfrastruktur der Schweiz ist ein staatliches Monopol. Nur der Tunnel am Grossen St. Bernhard ist eine private Strecke, für die eine Sondergebühr erhoben wird (UVEK, 2010).

Kennzahlen zu Mobilität und Personenverkehr in der Schweiz

Laut Mikrozensus haben die in der Schweiz wohnhaften Personen im Jahr 2005[79] ab 6 Jahren pro Tag durchschnittlich 37 Kilometer zurückgelegt und waren rund 88 Minuten unterwegs. Distanzmässig erreicht der motorisierte Individualverkehr einen Anteil von fast 70%, weitere 20% fallen auf den öffentlichen Verkehr. Allerdings wird rund die Hälfte aller Inland-Etappen zu Fuss oder per Velo zurückgelegt. Diese Etappen sind aber meist sehr kurz. Die Verkehrsmittelwahl wird wesentlich durch den Verkehrszweck bestimmt. Wichtigstes Mobilitätsmotiv ist der Freizeitverkehr, gefolgt vom Pendlerverkehr für Ausbildung und Beruf (BFS, 2007; ARE, 2009).

Die Zahl der geleisteten Personenkilometer in Millionen ist im Zeitraum zwischen 1990 und 2009 auf Schienen und Strassen deutlich gestiegen. Auf der Schiene stieg die Zahl der Personenkilometer im genannten Zeitraum von ca. 12 500 auf 18 500. Auf der Strasse stieg der private motorisierte Verkehr von knapp 78 000 auf knapp 90 000, der öffentliche Verkehr von knapp 4700 auf knapp 5400 Personenkilometer in Millionen (BFS, 2011b).

Das Strassennetz ist die meist genutzte Verkehrsinfrastruktur: Über das Strassennetz werden 83% des Personenverkehrs und 61% des Güterverkehrs

[79] Die Ergebnisse der Mikrozensus-Erhebung 2010 waren zum Zeitpunkt der Drucklegung noch nicht veröffentlicht.

abgewickelt. Allein über die Nationalstrassen, die nur etwa 2,5% der Streckenlänge ausmachen, werden ca. 40% des gesamten Motorfahrzeugverkehrs abgewickelt. Die Jahresfahrleistung auf den Nationalstrassen steigt derzeit um 3,1%[80] pro Jahr. (UVEK, 2010, ASTRA, 2010) «Der Bund investiert 2011 rund 1,9 Milliarden Franken in das Nationalstrassennetz. 740 Millionen davon fliessen in den Bau von neuen Abschnitten, mehr als 1,1 Milliarden werden für den Ausbau und Unterhalt des bestehenden Netzes eingesetzt.» (ASTRA, 2011).

Das Bundesamt für Strassen (ASTRA) errechnete für Jahr 2009 ca. 11 800 Staustunden auf dem Nationalstrassennetz und damit 18% mehr als im Vorjahr. Verkehrsüberlastungen verursachen ca. zwei Drittel der Staustunden, Baustellen und Unfälle ein weiteres Drittel. (ASTRA, 2010) Der deutliche Anstieg zwischen 2008 und 2009 ist nicht typisch, in den Jahren zuvor betrug die Steigerungsrate 1–2% (BFS, 2010).

Im Jahr 2010 wurden auf Schweizer Strassen ca. 19 600 Strassenunfälle mit Personenschaden von der Polizei registriert, an denen mindestens ein motorisiertes oder unmotorisiertes Fahrzeug beteiligt war. Dabei wurden mehr als 4000 Menschen schwer verletzt und mehr als 300 Menschen getötet[81] (BFS, 2011c). Die Zahl der Verkehrstoten ist, wie auch in anderen westlichen Ländern, rückläufig. Dazu haben Sicherheitsvorschriften, aber auch technische und organisatorische Verbesserungen in der Fahrzeug- und Verkehrstechnik, im Rettungswesen sowie regulatorische und erzieherische Massnahmen beigetragen (BFS, 2010). Diese Verbesserungen erfolgen zunehmend in enger Anlehnung an die Entwicklungen im Bereich Ortungstechnologien.

Für die Zukunft ist von einer weiteren Zunahme des Personenverkehrs auszugehen: «Je nach Szenario wird diese für den Zeitraum 2010–2030 zwischen 15% und 29% liegen. Im Gegensatz zum vorangegangenen Zeitraum rechnet man beim öffentlichen Verkehr mit einer stärkeren Zuwachsrate als beim motorisierten Individualverkehr, dessen Anteil bis 2030 auf 70% zurückfallen könnte. Der Freizeitverkehr, der bereits heute fast zur Hälfte zur Verkehrsleistung des Personenverkehrs beiträgt, wird in Zukunft weiterhin überproportional wachsen.» (Rapp, 2007, S. 5).

[80] ohne Berücksichtigung von Netzverlängerungen

[81] Als schwer verletzt gelten laut ASTRA Personen, die schwere sichtbare Beeinträchtigungen aufweisen, welche normale Aktivitäten zu Hause für mindestens 24 Stunden verhindert. Als getötet sind Personen anzuführen, die an der Unfallstelle ihr Leben verloren oder innert 30 Tagen nach der Kollision an den Unfallfolgen gestorben sind.

5.2 Übersicht über Anwendungen im Bereich Mobilität

Die folgende Übersicht kategorisiert die Anwendungen von Ortungstechnologien im Bereich Mobilität. Die Aufzählung erhebt keinen Anspruch auf Vollständigkeit.

Öffentliche Aufgaben

Die öffentliche Hand und Betreiber von Verkehrssystemen nehmen Aufgaben wie die Prognose, Steuerung und Regelung von Verkehrsflüssen, die Finanzierung von Verkehrsinfrastrukturen oder die Gewährleistung von Sicherheit und Gesundheitsversorgung im öffentlichen Raum wahr. Ziel ist es einerseits, die Mobilität des Einzelnen und damit verbunden die Teilnahme am Erwerbsleben, am Konsum sowie die Lebensqualität insgesamt zu unterstützen. Andererseits sollen die negativen Folgen der räumlichen Mobilität gemildert werden.

Ortungssysteme können dabei folgende Funktionen unterstützen:

- Mittel- und langfristige Verkehrsplanung, beispielsweise durch eine verfeinerte Statistik auf der Basis von verbesserter Verkehrsüberwachung und Auswertung von Bewegungsmustern;
- Kurzfristige Verkehrssteuerung, beispielsweise durch Routenhinweise auf freie Parkplätze oder Alternativstrecken oder standortbezogene Hinweise auf Verkehrsstörungen;
- Verkehrskontrolle, beispielsweise im Hinblick auf Geschwindigkeitsübertretungen oder unberechtigte Zufahrt zu gebührenpflichtigen Gebieten;
- Abwicklung von Zahlungsvorgängen, beispielsweise beim mobile Ticketing im öffentlichen Verkehr oder zur Erhebung von Strassenbenutzungsgebühren;
- Ortung von Personen oder Fahrzeugen bei Notrufsystemen.

Als weitere mögliche Einsatzfelder werden in der Literatur die Koordination und Dokumentation des Winterdienstes, die Ortung von Bundesfahrzeugen bzw. die

Ortung von Polizei- und Einsatzfahrzeugen oder sogar von VIP-Personen aufgeführt (iDynamics, 2010).

Dienstleistungen von Unternehmen:

Private und öffentlich-rechtliche Unternehmen bieten zahlreiche Dienste für Verkehrsteilnehmer an, die auf Ortungstechnologien basieren. Zwei grosse Gruppen von Anwendungen können grundsätzlich unterschieden werden:

1. Dienstleistungen im Zusammenhang mit dem Verkehrsvorgang selbst:

   - Informationsangebote, beispielsweise zur stets aktuellen Planung von Fahrten im öffentlichen Nah- und Fernverkehr: Sie fördern das schnelle Erreichen des Ziels oder eine verkehrsträgerübergreifende Navigation.
   - Pay-per-Use-Modelle, bei denen Nutzer in der Regel für die eigentliche Verkehrsleistung bezahlen: Sie können sich jedoch auch auf die Infrastruktur, deren Qualität und Ausstattung beziehen (beispielsweise die Nutzung von Fahrzeugen, Fahrspuren, Erste-Klasse-Waggons).
   - Pay-per-Risk-Modelle, neue Prämienmodelle von Versicherungen, richten sich an Risikofaktoren aus und berücksichtigen das Fahrverhalten, Zeit und Ort der Fahrt (Stadtteil, Strassentyp) und weitere mittels Ortungstechnologien gewonnene Daten.
   - Dienstleistungen zur Verfolgung («Tracking») von Geräten und Fahrzeugen ermöglichen das Auffinden beispielsweise von Fahrzeugen nach einem Diebstahl oder die Lokalisierung, beispielsweise bei Car-Sharing. Selten werden auch Personen, beispielsweise im Personenschutz oder im Strafvollzug («elektronische Fussfesseln») überwacht.
   - Dienstleistung zur Steuerung oder zur Optimierung von Verkehrsflüssen. Dazu zählen beispielsweise elektronische Staumelder, die sowohl im Fahrzeug als auch im öffentlichen Strassenraum installiert sein können oder Hinweise zu verfügbaren Parkplätzen.
   - Unterstützungsleistungen ermöglichen schnelle Hilfe bei Notfällen unterwegs. Typisch sind Anwendungen für die schnelle Antwort auf Notrufe von Personen, die gesundheitliche Probleme oder die Orientierung verloren haben. Weitere Dienstleitungen richten sich an Autofahrer, die nach einem Unfall oder bei einer Panne Hilfe benötigen.

2. Dienstleistungen im Zusammenhang mit dem Verkehrszweck, wobei hier die Zwecke «Einkaufen» und «Freizeit» im Vordergrund stehen:

   - Mobile Advertising umfasst Informationsangebote, die sich am Standort und am diesbezüglichen Informationsinteresse von Mobilfunknutzern orientieren, bis hin zum Mikromarketing (siehe Abschnitt 2.4.3). Dazu zählen beispielsweise Restauranthinweise zur Mittagszeit.
   - Mobile Couponing bezeichnet Gewinnspiele, Rabattaktionen oder Gutscheincodes, die mögliche Kunden im öffentlichen Raum in der Nähe von Restaurants oder Geschäften dazu bewegen sollen, das entsprechende Angebot wahrzunehmen. Es handelt sich hier um eine Kombination aus LBS (Abschnitt 2.4.2) und Mikromarketing (Abschnitt 2.4.3).
   - Reiseinformationen für Touristen: Laut einer Erhebung des World Travel Trends Report im Auftrag der Berliner Tourismusmesse ITB im Jahr 2011 besitzen 40 von 100 Personen, die international reisen, ein Smartphone, davon nehmen 12 Buchungen vor und 16 recherchieren Reiseinformationen. Nur 2% reisen ohne Handy (Allmaier 2011). Neben der Navigation und den Hinweisen auf Sehenswürdigkeiten zählen hierzu z.B. auch Anwendungen, die Übersetzungen von Redewendungen unterstützen, die mit dem Smartphone aufgenommen und an den Dienstleister versandt werden. Ein weiteres Beispiel ist das Erkennen von Bauwerken mit «Google Goggles».

Weitere Anwendungen sind denjenigen für soziale Netze verwandt, die wir in Kapitel 6 behandeln werden, sind aber nicht in soziale Netze eingebunden, sondern als Einzelanwendungen verfügbar. Dazu zählen mehrere Angebote von Google, beispielsweise für das Erfassen des eigenen Standortverlaufs in Google Maps. Google bietet auch die Möglichkeit, den eigenen Standort stets im Blog oder auf der eigenen Webseite zu veröffentlichen oder bei Nutzung von Google Chat und Google Talk mitzuversenden.

5.3 Stand der Anwendungen in der Schweiz

Die folgende Auswahl stellt Anwendungen und Systeme vor, die in der Schweiz Standorte oder Routen ermitteln, georeferenzieren oder auch Personen oder Fahrzeuge im öffentlichen Raum identifizieren. Das Umfeld der jeweiligen Anwendung und die wichtigsten Akteure werden benannt. Einige Anwendungen sind bereits realisiert, andere sind in der Einführungsphase bzw. in Diskussion.

Geokodierung und Routenerfassung für planerische Aufgaben im Verkehrsbereich

Der Mikrozensus zum Verkehrsverhalten der ständigen Wohnbevölkerung der Schweiz bildet die Grundlage für planerische Aufgaben im Verkehrsbereich. Beim aktuellen Mikrozensus 2010 zum Verkehrsverhalten werden neben den Wegen auch Routen berechnet. Dabei werden für einen typischen Tag alle Etappen und Routen von mehr als 25 Metern erfasst und statistisch ausgewertet (Rebmann & Marconi, 2009).

Mittels einer computergestützten Telefonbefragung werden alle fünf Jahre mehr als 30 000 Personen befragt. Bereits 2005 wurde dabei ein Geokodierungs-Tool für die adressgenaue Lokalisierung der einzelnen Etappenpunkte und erweiterte Analysemöglichkeiten genutzt.

Die Geokodierung der Etappen und das Erfassen der Routen bedeutet, dass den Start- und Zielorten der Etappen sowie den Routenpunkten räumliche Koordinaten zugewiesen werden. Durch das auf unterschiedlichen Geodatenbanken basierende Erhebungsinstrument werden einzelne Aufenthaltsorte entweder über eine Adresse, eine Haltestelle, einen sogenannten Point of Interest oder eine Karte erfasst (Abbildung 4). In 89% der Fälle konnte die genaue Wohnadresse ermittelt und damit der Wohnort «adressscharf» geokodiert werden. Von den aufgesuchten Start- und Zielorten der Etappen wurden 78% adressscharf georeferenziert (Rebmann & Marconi, 2009, S. 16).

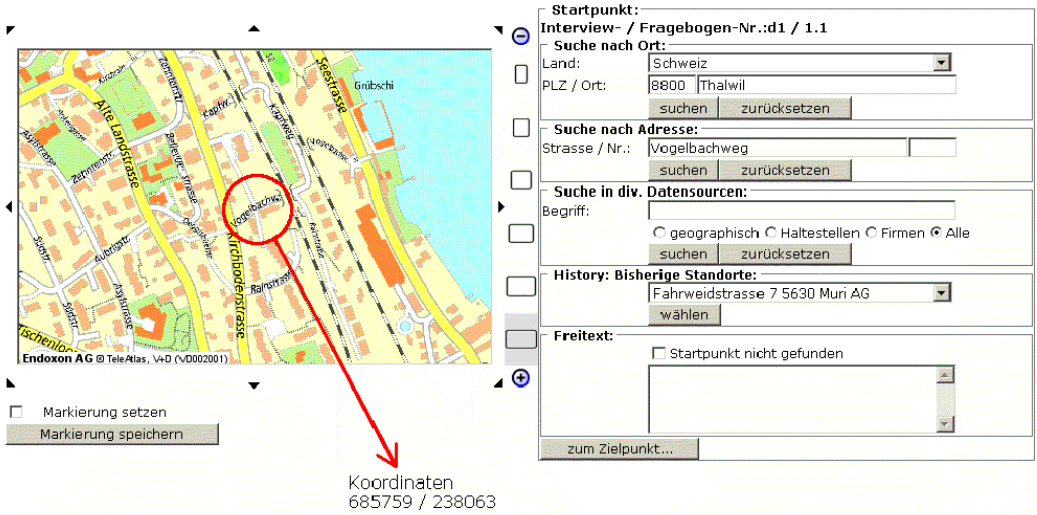


Abbildung 4: Geokodierungstool des Mikrozensus Verkehr 2005 (Zanetti et al., 2008,8)

Standortidentifikation für alle Notrufnummern

Bereits im Jahr 2007 kamen zwei Drittel der ca. 200 000 Notrufe pro Jahr in der Schweiz von mobilen Endgeräten. Häufig können die mobilen Anrufer ihren Standort nur ungenau beschreiben. Diese Information ist jedoch für einen effizienten Rettungseinsatz entscheidend. Die Verordnung über Fernmeldedienste regelt daher, dass die Schweizer Mobilfunkunternehmen einen Dienst zur Standortidentifikation für alle Notrufnummern ermöglichen, der von allen Alarmzentralen genutzt werden kann. Seit dem 1. Juli 2006 unterstützen die GSM-Netze und seit dem 1. Juli 2007 die UMTS-Netze aller Telekommunikationsanbieter in der Schweiz die Standortidentifikation bei Anrufen auf Notrufnummern (Zogg, 2007). Die Lokalisierung bei Anrufen über das Festnetz ist ebenfalls gewährleistet, da zu jedem Anschluss Geodaten und Adresse gespeichert sind.

Rund 70 Rettungsdienste und 20 Sanitätsnotrufzentralen sind in der Schweiz für das Notfallmanagement verantwortlich. Bei Unfällen oder lebensbedrohlichen Erkrankungen ist es das Ziel der Rettungsdienste, innerhalb von15 Minuten vor Ort zu sein. In Zeiten von hohem Verkehrsaufkommen und

bei ungenauen Positionsdaten ist dies laut Interverband für Rettungswesen «keine leichte Aufgabe» (Interverband für Rettungswesen, 2011).

Für Notrufe über Mobiltelefone muss die Lokalisierung über die Mobilfunkzellen erfolgen (siehe Abschnitt 2.3.2). Dieses Verfahren weist in seiner heutigen Form deutliche Defizite auf, einmal durch geographische Faktoren wie Reflexionen in Gebirgen, aber auch durch beträchtliche Qualitätsunterschiede der für den Rettungsdienst bereit gestellten Daten je nach Mobilfunkanbieter. Die Grösse des identifizierten Aufenthaltsraumes schwankt zwischen 1 und 100 Quadratkilometern (Zogg, 2007).

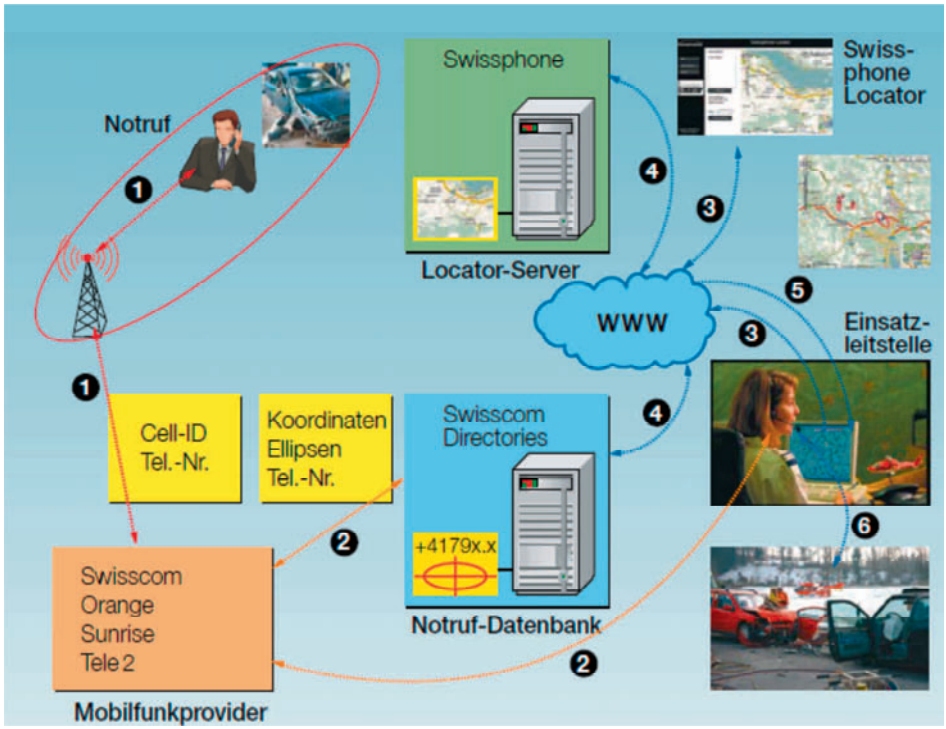


Abbildung 5: Ablauf einer Standortidentifikation (Zogg, 2007, 19)

Die Ortung bei Internettelefonie (beispielsweise über die VoIP-Software Skype), die allein als Anwendung im Netz und nicht als Angebot von «klassischen» Netzbetreibern realisiert wird, ist heute (Anfang 2012) nicht möglich. Diese Anwendungen werden als «over the top» (OTT)[82] bezeichnet. Grundsätzlich können die OTT-Anbieter eine Lokalisierung im Internet aufgrund der IP-Adresse durchführen. Die Qualität dieser Daten ist jedoch für den Notfalleinsatz sehr ungenau. Ebenfalls könnten die OTTs die GPS-Daten erfassen, sofern diese vom Endgerät erhoben und mit übermittelt werden.[83] Tschofeniga et al. verweisen darauf, dass Standardisierungseinrichtungen wie die Internet Engineering Task Force (IETF), die National Emergency Number Association (NENA) und die 3rd Generation Partnership Lösungen für die Ortung von Anrufern für Notfallsysteme auf «nomadische, mobile» Voice-over-IP ausweiten wollen. Die Herausforderungen dafür sind hoch, da bei VoIP die Aufgaben des Internetzugangs- und des Internettelefonie-Anbieters auf zwei Betreiber aufgeteilt sein können. Die Anbieter müssen über keine Geschäftsbeziehungen verfügen. Mittlerweile wurden erste Architekturen entwickelt, die auf der Annahme basieren, dass Endgeräte über eine neue Funktionalität verfügen, die die Erkennung des Internetanbieters bei Notfallanrufen auf den Anbieter der Internettelefonie überträgt (Tschofeniga et al., 2010).

Elektronisches Ticketing im öffentlichen Nah- und Fernverkehr[84]

Die rund 135 Schweizer Transportunternehmungen arbeiten seit über zehn Jahren an einem elektronischen Ticketing-System. Unter Federführung der SBB entwickelten sie in den neunziger Jahren das System «EasyRide», das auch im Ausland die Weiterentwicklung der sogenannten Be-in-Be-out-Systeme (BiBo) beeinflusst hat. BiBo funktioniert unabhängig von Touchpoints, an denen zum Beispiel eine Chipkarte ein- oder vorbeigeführt werden muss; es handelt sich um eine sogenannte Raumerfassung, die im Speichermedium (Karte, Mobiltelefon) eine Stromquelle notwendig macht. Feldversuche im ÖV der Städte Genf und Basel wiesen nach, dass EasyRide fälschungssicher war und eine

[82] «Over the top» (OTT) ist eine Bezeichnung für Telekommunikationsanwendungen, die einen Mehrwert für Kunden bieten, ohne dass der Anbieter dieser Anwendungen bzw. Dienste selbst ein Telekommunikationsnetzwerk betreibt bzw. Festnetz- oder Mobilfunkzugänge «aus einer Hand» vertreibt. (LTC International, 2007)

[83] Persönliche Kommunikation mit Dr. Erwan Bigan, Swisscom

[84] Die Angaben in diesem Abschnitt stammen vom «Verband öffentlicher Verkehr», dem Dachverband der schweizerischen Transportunternehmen des öffentlichen Verkehrs. Die Autoren danken Herrn Hans Kaspar Schiesser für die Mitarbeit an diesem Text.

Präzision von mindestens 98 Prozent aufwies. In Dresden wurde der Versuch unter dem Namen Allfa und unter Langzeitbedingungen weiter differenziert. Die Probleme mit der Kapazität des Akkus und den Kosten der Raumerfassungs-Geräte in jedem Fahrzeug sowie die Komplexität des verbundenen ÖV in der Schweiz (Fachbegriff «Direkter Verkehr») führten dann aber zum Abbruch des Projekts EasyRide.

2011 wurde eine Neuauflage des Projektes unter dem Namen «ETIK» gestartet. Auch jetzt sucht der ÖV Schweiz nach Lösungen, die ebenso komfortabel sind wie das hierzulande weit verbreitete Generalabonnement (GA). Damit sind System nach dem Muster Check-in-Check-out (CiCo) ausgeschlossen. Denn dabei muss – im noch bequemsten Fall wie bei Octopus in Hong Kong, bei der Deutschen Bahn oder dem ÖV in den Niederlanden – das Speichermedium, in der Regel eine Chipkarte, zur Registrierung aktiv und nahe an einem Sensor vorbeigeführt werden. Bei BiBo-Systemen (und damit auch bei ETIK) genügt es dagegen, die Karte irgendwo mit sich zu führen, z.B. im Portemonnaie, in der Hand- oder der Manteltasche. Die stichprobenartige Kontrolle wird jedoch nicht überflüssig. So wird zum Beispiel entdeckt, ob versucht wurde, die Registrierung im Fahrzeug mit einer metallischen Hülle zu vereiteln.

ETIK beruht aus einer Kombination von RFID und WLAN-Techniken, wie sie aus der Güterlogistik bekannt sind. Weil das die Menge der für ETIK nötigen technischen Neuentwicklungen drastisch herabsetzt, hat ETIK aus heutiger Sicht bei rund 25 000 Transportgefässen des ÖV Schweiz deutlich kleinere Kostenfolgen als seinerzeit EasyRide. Grundsätzlich könnten sich auch die zahlreichen touristischen Unternehmen wie Seilbahnen, sofern sie zum Beispiel zum Gültigkeitsbereich der Halbpreis- oder Generalabonnemente gehören wollen, anschliessen. Voraussetzung ist, dass es ein handliches, preiswertes Kontrollgerät gibt, mit dem auch kleine Transportunternehmen prüfen können, ob der Fahrt eine Bezahlung hinterlegt ist.

Die Daten werden bei ETIK nicht mehr auf der Karte der Kunden kumuliert. Die Karte enthält – wie eine Identitätskarte – nur noch die persönlichen Angaben der Inhaberin. Die Daten, Einsteigeort, Aussteigeort, Zeitpunkt, Wagenklasse und ähnliches, werden im Fahrzeug, also zum Beispiel im Zug gespeichert und am Tagesende an einen zentralen Server übermittelt. Für Echtzeit-Fahndungen nach Personen (ob mit oder ohne rechtliche Grundlage) eignet sich das System somit nicht. Die Daten werden für praktisch alle Zwecke anonymisiert und nach

gesetzlich fixierter Frist gelöscht. Als Bezahlmodus sind sowohl Vorauszahlung (pre-paid) als auch nachträgliche Abrechnung (post-paid) möglich. ETIK setzt voraus, dass das Fahrzeug (z.B. Bus, Eisenbahnwagen) per GPS feststellen kann, wo es sich aktuell befindet.

Das System hat aus Sicht des Verbandes öffentlicher Verkehr folgende Vorteile:

- Die Distributionskosten sinken: ETIK ist pro Ticketverkauf preiswerter als der Ticketautomat.
- Schwarzfahren wird schwieriger, da die Bewegungsdaten auf dem zentralen Server und nicht auf der Karte gespeichert sind.
- Der ÖV bekommt präzise und umfassende Bewegungsdaten in erster Linie zur gerechten und bisher in der Schweiz sehr komplizierten und teuren Aufteilung der Erträge unter den beteiligten Transportunternehmen.
- ETIK ermöglicht die Realisierung flexibler Rabattsysteme, etwa niedrigere Fahrpreise in Nebenverkehrszeiten oder spontane Klassenwechsel ohne Aufwand.

ETIK wird erstmals in Form einer ÖV-Karte, welche das Halbpreis- und das Generalabonnement abdeckt, ab ca. 2014 getestet werden. Diese Karte enthält wie die spätere ETIK-Karte nur die – von den Kunden einsehbaren – identifizierenden Personendaten. Der flächendeckende Einsatz als BiBo-System dürfte ab 2018 oder 2019 realistisch werden.

Überwachung «neuralgischer Orte» im öffentlichen Raum

Videoüberwachungsanlagen finden sich zunehmend in öffentlichen oder öffentlich zugänglichen Räumen. Ihre Präsenz soll Straftaten verhindern, zur Aufklärung von Straftaten beitragen und das subjektive Sicherheitsempfinden verbessern.

Unter Videoüberwachung wird die Beobachtung von Zuständen oder Vorgängen durch optisch-elektronische Anlagen (Kameras) verstanden (EJPD, 2007, S. 9). Zur Überwachung «neuralgischer Orte» werden heute primär fest installierte Videokameras eingesetzt.

Das Eidgenössische Justiz- und Polizeidepartement unterscheidet u.a. die folgenden Typen von Videoüberwachung:

- Die *dissuasive Videoüberwachung* zur präventiven Verhinderung von Gefährdungen und Straftaten durch Abschreckung. Sie ist nach aussen hin deutlich erkennbar. Eingesetzt werden Technologien, die die Bildsignale aufzeichnen und die ggf. die Identifikation von Personen ermöglichen. Wenn die Daten aufgezeichnet werden, können nachträglich ausgewertet werden, insbesondere im Rahmen der Strafverfolgung.
- Die *invasive Videoüberwachung* verfügt über vergleichbare technische Leistungen, Ziel ist jedoch die gezielte Beschattung einer Person. Dazu können bestimmte Orte wie z.B. Hauseingänge überwacht werden. Die invasive Videoüberwachung erfolgt vorübergehend und verdeckt.
- Die *observative Videoüberwachung* unterstützt den reibungslosen Ablauf von Verkehrs- oder Personenströmen und soll auf etwaige technische Störungen verweisen. Hierbei werden die Identifikation und damit die Ortung von Personen nicht unterstützt (EJPD, 2007, S. 9).

Zahlen darüber, wie viele Videoüberwachungskameras in der Schweiz installiert wurden, liegen nicht vor. Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich und Präsident des Verbandes der schweizerischen Datenschutzbeauftragten, beobachtet in seinem Kanton «die Tendenz eines starken Anstiegs», die auch für das ganze Land zu vermuten sei. In den letzten zwei, drei Jahren habe die Zahl der Beratungen und Beurteilungen, die er Zürcher Behördenstellen in Bezug auf Videoüberwachung anbiete, stark zugenommen (zit. nach Kuenzi, 2011). Die gesetzlichen Vorschriften lassen Videoüberwachung nur dann zu, wenn andere Massnahmen nicht greifen. Eine flächendeckende Überwachung ist ausgeschlossen und Videoüberwachung müsse dem Schutz vor Attacken auf Personen oder Einrichtungen dienen. Der Erfolg der Massnahme muss geprüft werden.[85]

Mit der dissuasiven Videoüberwachung ist eine Abschreckungshypothese verbunden. Demnach erweitert Videoüberwachung die Kontrollmöglichkeiten und als Folge die Produktivität und die Effizienz der Polizeiarbeit. Dazu tragen ein erhöhtes Entdeckungsrisiko, die Nutzung von Aufzeichnungen als Beweismaterial und der effektivere Einsatz von Sicherheitspersonal bei. Auch die Zivil-

[85] NZZ Online, 2008. Erläuterung von Beda Harb, Stellvertreter des Datenschutzbeauftragten des Kantons Zürich, zur Videoüberwachung in Tram, Bus und S-Bahn.

courage kann in überwachten Räumen ggf. gesteigert werden. Eine gegenläufige Hypothese vermutet eine Verschiebung von Straftaten in andere Zonen und sorgloses Verhalten bei möglichen Opfern (Stutzer & Zehnder, zitiert nach Kantonsrat Basel-Stadt, 2011).

Als erste Schweizer Stadt entschied sich St. Gallen Ende 2007, die Überwachung ausgewählter Punkte im öffentlichen Raum auf eine kommunale Rechtsgrundlage zu stellen. In der Volksabstimmung vom 25. November 2007 hat die Bürgerschaft einem Kredit über insgesamt CHF 2,48 Mio. zur Ausstattung der Umgebung der AFG-Arena in St. Gallen sowie vier «neuralgischer Orte» in der Innenstadt mit Überwachungseinrichtungen (Videokameras und Notrufsäulen) mit 63% zugestimmt. Nach Auskunft des zuständigen Stadtrats Nino Cozzio ist der primäre Zweck der Ende 2008 realisierten Videoüberwachung auf öffentlichem Grund (23 Kameras und 10 Notrufsäulen), das subjektive Sicherheitsempfinden zu verbessern und auch die objektive Kriminalitätsbelastung in den überwachten Zonen zu senken. Ausserdem dient das Bildmaterial, das vom Untersuchungsrichter herausverlangt werden kann, als Ermittlungs- und Beweismaterial im Rahmen von Strafermittlungen. Die Bilder werden aufgezeichnet und 100 Tage lang aufbewahrt. Der Zugang zu den Daten und deren Nutzung ist strikt geregelt; eine kontinuierliche Kontrolle der Videobilder durch die Stadtpolizei erfolgt nicht. Nur bei Eingang eines Notrufs und in den vom Gesetz geregelten Fällen werden die aktuellen Videobilder in der Einsatzzentrale aufgeschaltet.

Nach repräsentativen Umfragen, die die Stadt regelmässig durchführt, hat sich das subjektive Sicherheitsempfinden in den Unterführungen verbessert, während es in den anderen Bereichen unverändert geblieben ist. Es habe sich gezeigt, dass die Kameras – anders als von den Gegnern befürchtet – nicht dazu führen, dass Menschen diese Zonen meiden oder sich befangen fühlen. Ein signifikanter objektiver Rückgang der Kriminalität als Folge der Videoüberwachung kann indessen nicht nachgewiesen werden.[86]

Eine relativ hohe Akzeptanz in der Bevölkerung wurde auch in internationalen Studien zur Videoüberwachung festgestellt: Das «Urbaneye»-Projekt der Technischen Universität Berlin kommt zu ähnlichen Ergebnissen (Kantonsrat Basel-Stadt, 2011).

[86] Persönliche Kommunikation mit Stadtrat Nino Cozzio, Direktor Soziales und Sicherheit, Stadt St. Gallen.

In der Regel ist eine kontinuierliche Kontrolle aller Videobilder aufgrund des hohen Zeitaufwandes nicht leistbar. Typischerweise werden Bilder nur dann an eine Zentrale geleitet, wenn ein Alarm ausgelöst wurde. Verlässliche Verfahren, die eine automatische Identifizierung von Personen anhand ihrer Gesichtsmerkmale und den unmittelbaren Abgleich mit den Daten einer Bilddatenbank ermöglichen, stehen derzeit nicht zur Verfügung (vgl. Abschnitt 2.3.8). Pilotversuche in London und Mainz bestätigen jedoch das grundsätzliche Interesse an der videogestützten Gesichtserkennung zur Identifikation von vorher bekannten Personen im Rahmen der Fotofahndung (Bundesministerium des Innern, o.D.).

Bruno Baeriswyl formulierte jüngst die Gefahr von Verhaltenskontrollen mittels Videoüberwachung als Folge der fortschreitenden technologischen Entwicklung: «Heute registriere eine Videokamera Bilder. In Zukunft werde sie aber auch versuchen, ein bestimmtes Verhalten zu eruieren […]. Wer beispielsweise auf einem Parkplatz direkt auf ein Auto zugeht, wird nicht näher erfasst. Wer aber hin- und hergeht, wird erfasst und allenfalls mit einer Datenbank abgeglichen, denn er könnte ein potenzieller Autodieb sein.» Laut Baeriswyl sind in Grossbritannien bereits Systeme im Einsatz, die Menschen auf ein bestimmtes Verhalten hin beobachten (zit. nach Kuenzi, 2011).

Die Bearbeitung von Daten der Videoüberwachung, auf denen Personen erkennbar sind, greift in die in Art. 8 EMRK geschützte Recht auf Achtung des Privatlebens und in den grundrechtlich geschützten Anspruch auf Schutz vor Missbrauch der persönlichen Daten ein (BGE 133 I 77 Erw. 3.2). Sowohl die Videoüberwachung in Echtzeit[87] wie die Aufbewahrung der Personendaten stellen einen schwerwiegenden Grundrechtseingriff dar und erfordern eine gesetzliche Grundlage und ein öffentliches Interesse oder den Schutz der Grundrechte Dritter an der Überwachung. Überdies muss die Überwachung dem Grundsatz der Verhältnismässigkeit genügen (BGE 133 I 77 Erw. 4.1).

«Jede Videoüberwachung ist auf die datenschutzrechtlichen Anforderungen individuell zu überprüfen» (DSB Kanton Zürich, 2010, S. 1). Zur Beurteilung der Verhältnismässigkeit der Videoüberwachung sind die öffentlichen Interessen

[87] Siehe dazu den Entscheid des Bundesgerichts vom 13. Oktober 2010, 1C_315/2009. Das Bundesgericht kommt zum Schluss, für die Videoverordnung des bernischen Regierungsrates bestehe im bernischen Polizeigesetz eine ausreichende gesetzliche Grundlage (Bger 1C_315/2009, Erw. 3.4.)

und die privaten Interessen gegeneinander abzuwägen. Beispielsweise rechtfertigen geringfügige einmalige Verstösse wie kleine Sachbeschädigungen oder Ruhestörungen keine Videoüberwachung (DSB Kanton Zürich, 2010).

Die Verhältnismässigkeit des Einsatzes kann durch technische und organisatorische Massnahmen erreicht werden. Dazu zählen der Einsatz von Privacy-Filtern, die Verschlüsselung von Bildmaterial, kurze Aufbewahrungszeiten oder die Beschränkung des Aufnahmebereichs der Videokamera nur für den verfolgten Zweck (Datenschutzbeauftragter des Kantons Zürich 2010, S. 5). Insbesondere Privacy-Filter werden von Datenschützern zur Gewährleistung der Verhältnismässigkeit befürwortet. Dabei werden die von der Kamera aufgenommen Objekte und Personen vor der Speicherung des Bildes automatisch unkenntlich gemacht, während unbewegliche Räume und Gegenstände scharf bleiben. «Mit einem Software-Schlüssel können berechtigte Personen die unkenntlichen Bereiche nachträglich, z.B. im Rahmen einer Strafermittlung, wiederherstellen» (EJPD, 2007, S. 10).

Videoüberwachung in öffentlichen Verkehrsmitteln

Auch in öffentlichen Verkehrsmitteln, an Bahnhöfen und in Haltestellen sowie an Ticket-Automaten wird die dissuasive Videoüberwachung eingesetzt. Unternehmen können nach den aktuellen gesetzlichen Regelungen zum Schutz der Reisenden, des Betriebes und der Infrastruktur eine Videoüberwachung einrichten. Videosignale können aufgezeichnet werden. Sie müssen grundsätzlich am nächsten Werktag ausgewertet werden. Aufbewahrte Videosignale sind vor Missbrauch zu schützen und spätestens nach 100 Tagen zu vernichten. Nur strafverfolgende Behörden oder Behörden, bei denen die Unternehmen Anzeige erstatten oder Rechtsansprüche geltend machen, dürfen die Daten für weitere Zwecke verwenden (PBG, 2009).

Der Zürcher Verkehrsverbund (ZVV)[88] beispielsweise nutzt Videoüberwachung sowohl in den Fahrzeugen als auch an den Haltestellen. Die Auswahl der Einsatzorte orientiert sich an der Zahl der Vorfälle, ein «flächendeckender Einsatz» erfolgt nicht und ist rechtlich auch nicht möglich. Zusätzlich zu den Videodaten werden die Uhrzeit und das IBIS Signal aufgezeichnet, das in Tram und Bus zur Steuerung der Anzeigen verwendet wird (Linie, Kurs, Haltestation).

[88] Persönliche Kommunikation mit Michael Laux, Zürcher Verkehrsverbund.

Im ZVV sind drei Mitarbeiterinnen und Mitarbeiter des ZVV mit der Auswertung betraut. Die Auswertung ist in einer Rahmenvereinbarung geregelt: Wann muss ausgewertet werden, wann darf nicht ausgewertet werden und wann kann im Einzelfall ausgewertet werden? (siehe Abbildung 6). Die Auswertung erfolgt nach schriftlichem Antrag der Polizei, der Staatsanwaltschaft oder bei dringendem Interesse der Verkehrsbetriebe Zürich (VBZ). Ein Eigeninteresse der Verkehrsbetriebe liegt bei Sachbeschädigungen mit Flusssäure[89] und beim Zerkratzen mehrerer Scheiben vor. Insgesamt steigt die Zahl der Anfragen von der Polizei, auch bei Handtaschendiebstählen.

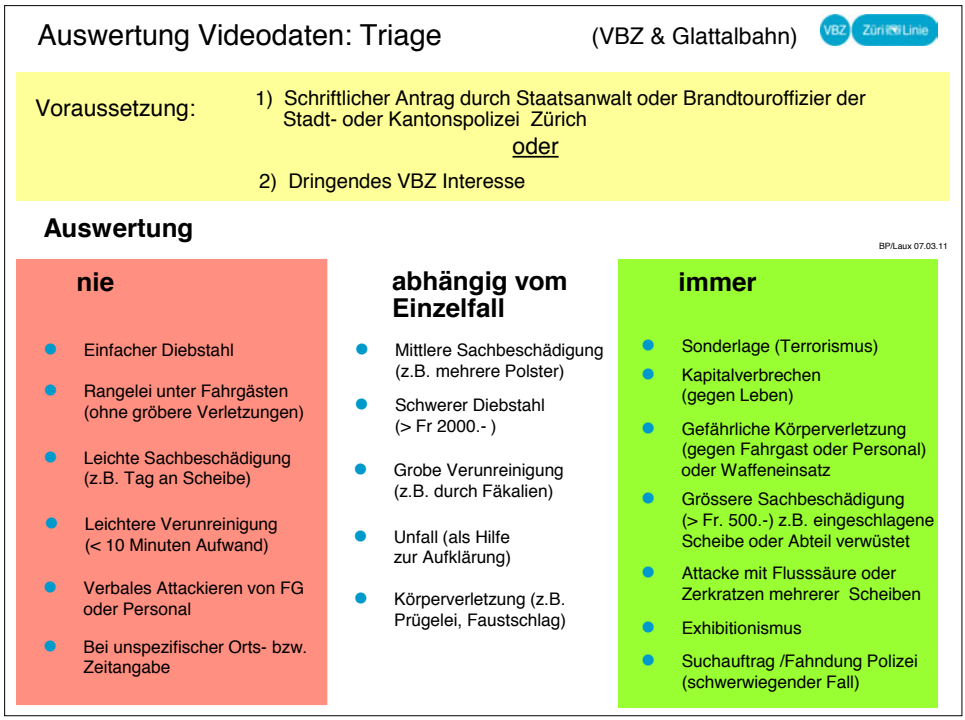


Abbildung 6: Kategorien zur Aufzeichnung von Videoauswertungen (Bildquelle: Verkehrsverbund Zürich, 2011)

[89] Flusssäure ist eine Verbindung aus Wasserstoff und Fluor, die in der gewerblichen Ätzung von Glas eingesetzt wird. Sie kann erhebliche Gesundheits- und Sachschäden verursachen.

Nach Angaben des Zürcher Verkehrsverbundes werden pro Woche 1 bis 2 Fälle ausgewertet. Im Vordergrund des Einsatzes von Videoüberwachung steht demnach die abschreckende Wirkung. Diese kann im direkten Vergleich von baugleichen Fahrzeugen mit und ohne Videoüberwachung belegt werden. Die Kunden des ZVV akzeptieren Videoüberwachung und haben sich daran gewöhnt. Die Videoanlagen sind klar gekennzeichnet. Beim Einstieg sind in jedem Fahrzeug Sticker angebracht, die auch eine Kontaktnummer für Anfragen beinhalten. Bisher ist noch keine Informationsanfrage von Kunden eingegangen.

Die Fahrer sind nicht im Fokus der Kamera, wie auch von Datenschützern gefordert. Grundsätzlich ist eher eine gegenläufige Tendenz der Einstellungen von Fahrzeugführern zur Videoüberwachung zu verzeichnen: Viele Fahrer hätten nichts gegen eine Videoüberwachung einzuwenden, um bei etwaigen Vorfällen wie Schlägereien abgesichert zu sein.[90]

Von weiteren Verkehrsunternehmen werden die Erfahrungen, insbesondere bei der Prävention von Gewalt- oder Vandalenakten, als sehr gut bezeichnet. «Die Zahl der Vandalenakte sei um bis zu 90% zurückgegangen.

Auch international wird argumentiert, dass sich die Videoüberwachung auf die Sicherheit und Schadensbekämpfung in öffentlichen Verkehrsmitteln positiv auswirkt. Laut Untersuchungen der International Association of Public Transport (UITP) berichten 75% der Verkehrsunternehmen von Rückgängen bei Vandalismus und Graffiti-Schäden.» (Kantonsrat Basel-Stadt 2011, S. 9). Detailliertere Analysen belegen Unterschiede zwischen Bahnhofsbereich und Verkehrsmitteln. Der Rückgang beträgt auf Bahngebiet über 20%, in überwachten Zugskompositionen bis zu 80% (EJPD, 2007).

Seit Beginn des Einsatzes von Videoüberwachung wurden die Datenschutzvorgaben gelockert. Vor ca. 5 Jahren durften nur Kameras mit offenem Objektiv eingesetzt werden, bei denen die Fahrgäste wussten, ob sie im Bild waren. Heute werden kleine Kuppe-/Dome-Kameras eingesetzt. Vor ca. 8 Jahren wurden Aufbewahrungsfristen auf ca. 24 Stunden befristet. Bis 2009 betrug die *maximale* Aufbewahrungszeit 48 bis 72 Stunden, seit 2009 regelt das Bundesrecht eine *minimale* Aufbewahrungsfrist von 72 Stunden und erlaubt maximal 100 Tage (Videoüberwachungsverordnung ÖV, 2009). Hintergrund für der Beschränkung auf maximal 100 Tage bildet der Leitentscheid des Bundesgerichts

[90] Persönliche Kommunikation mit Michael Laux, Zürcher Verkehrsverbund.

vom 14. Dezember 2006 (BGE 133 I 77). Gemäss Bundesgericht steigt bei längerer Aufbewahrungsdauer das Missbrauchspotenzial. Das Bundesgericht hielt jedoch fest, dass von Straftaten betroffene Personen oft aus nachvollziehbaren Gründen ein Delikt nicht sofort anzeigen würden und deshalb lasse sich die 100 Tage Aufbewahrungsfrist im streitigen Polizeireglement der Stadt St. Gallen rechtfertigen. Die Verhältnismässigkeit der Aufbewahrung Datenmaterial bestimme sich indes nicht ausschliesslich nach deren Dauer, wichtig sei vielmehr auch «wie und von wem dieses verwendet wird und in welchem Ausmass die Personen, deren Daten aufgezeichnet sind, vor einem nicht sachgerechten Zugriff auf die Aufzeichnungen und einer missbräuchlichen Verwendung der Daten geschützt werden» (BGE 133 I 77, Erw. 5.4).

Für die Verlängerung der Aufbewahrungsfristen war u.a. ausschlaggebend, dass Anzeigen nicht immer direkt nach einem Vorfall erfolgen, sondern häufig einige Tage später. Auch unterschieden die ersten Regelungen nicht zwischen Werk- und Wochentagen. Aber auch technische Faktoren spielen eine Rolle: Die Schwelle zur Aufzeichnung und Aufbewahrung grösserer und genauerer Datenmengen ist durch höhere Speicherdichten und sinkende Preise für Speicherplatz deutlich niedriger geworden.

Road Pricing oder Mobility Pricing

Die Zunahme des motorisierten Strassenverkehrs und die steigenden Ausgaben der öffentlichen Hand für den Verkehr führen auch in der Schweiz zu Überlegungen, ob das Verkehrswachstum durch preisliche Mittel reduziert werden kann oder ob die bestehende Kostenteilung zwischen Verkehrsteilnehmern und öffentlicher Hand verändert werden sollte (Rapp et al., 2007).

«Mobility Pricing» ist definiert als benutzungsbezogene Abgabe für Infrastrukturnutzung und Dienstleistungen im Individualverkehr und im öffentlichen Verkehr mit dem Ziel der Beeinflussung der Mobilitätsnachfrage. Road Pricing umfasst als Teilaspekt nur die benutzungsbezogenen Abgaben für den fahrenden motorisierten Individualverkehr (Rapp, 2007). Erfassungs- bzw. Ortungstechnologien sollen die Einführung und Abwicklung massgeblich befördern. Die technologischen Lösungen werden typischerweise entweder im öffentlichen Raum (Kennzeichenerfassung oder Radiofrequenz-Identifikation) oder im Fahrzeug installiert (mittels Positionserkennung über Satellit und Datenübertragung in Mobilfunknetzen) (Palma & Lindsey, in Press).

Benutzungsbezogene Abgaben basieren auf dem Prinzip der Nutzniesserfinanzierung bzw. des «pay per use», also gebrauchsabhängiger Entgelte. Bei Systemen auf Basis von Ortungstechnologien sind sehr differenzierte Abrechnungsmodelle technisch möglich, die die Gebühr beispielsweise abhängig von Fahrzeugtyp, Fahrspur, Region, Verkehrsdichte oder Tageszeit berechnen. Diese Systeme werden international erprobt bzw. befinden sich in vielen Ländern bereits im Regelbetrieb. Als technische Lösungen für entsprechende elektronische Systeme in der Schweiz werden Kennzeichenerfassung (vgl. Abschnitt 2.3.8), Nahbereichskommunikation (engl. Dedicated Short Range Communication, DSRC; vgl. Abschnitt 2.3.10) und satellitenbasierte Systeme diskutiert (Rapp et al., 2007).

Langfristig fasst der Bundesrat die Ersetzung aller bisherigen Infrastrukturabgaben durch eine flächendeckende, verkehrsträgerübergreifende, leistungsabhängige Mobilitätsabgabe («Mobility Pricing») ins Auge. Eine solche Abgabe würde die Finanzierung auf eine tragfähige Grundlage stellen und dank verursachergerechter Anreize eine sinnvolle und nachhaltige Nutzung der verschiedenen Verkehrsträger fördern (SF, 2010; UVEK, 2010). Als Gründe hierfür werden sinkende Einnahmen aus den Treibstoffabgaben und die fehlende Lenkungswirkung des heutigen Finanzierungssystems benannt.

Mobility Pricing soll also nach dem Prinzip «pay as you drive/ride» die bisherigen Finanzierungssysteme ersetzen und sich dabei an der tatsächlichen Fahrleistung bzw. Strecke orientieren. Dabei sollen alle Verkehrssysteme einbezogen und auch ökologische Kriterien berücksichtigt werden. Die vollautomatische Erhebung ohne Behinderung des Zugangs zu den Verkehrsnetzen ist dabei ein gleichwertiges Kriterium. Der Bundesrat will die möglichen Optionen «im Rahmen eines breit angelegten, wissenschaftlich fundierten und international vernetzten Meinungsbildungsprozesses eingehend evaluieren und die Ergebnisse zum gegebenen Zeitpunkt zur Diskussion stellen». (Generalsekretariat, UVEK 2010, S. 5) Das Thema «Ortungstechnologien und Mobility Pricing» ist folglich derzeit in der Schweiz nicht aktuell, könnte aber aufgrund des gestiegenen Problemdrucks, steigender Akzeptanz in der Bevölkerung und positiven Erfahrungen im Ausland zukünftig an Bedeutung gewinnen[91] (Rapp et al., 2007).

[91] In der Schweiz verbietet die Verfassung derzeit die Erhebung von Strassenbenutzungsabgaben. Die Einführung von Mobility Pricing oder Road Pricing bedarf also einer Verfassungs-

Bereits 2004 hat das TA-SWISS gemeinsam mit dem Bundesamt für Strassen (ASTRA) und dem Bundesamt für Raumentwicklung (ARE) Diskussionsrunden mit Bürgern zu diesem Thema durchgeführt, um sie in den technologiepolitischen Entscheidungsprozess einzubinden und das Meinungsspektrum in der Bevölkerung einzufangen. Demnach birgt Road Pricing erhebliches Konfliktpotenzial: «Teilnehmende mit Wohnsitz in der Stadt beurteilen die neue Abgabe tendenziell positiver als BewohnerInnen aus der Agglomeration. Und in den Gruppen aus der Romandie stösst das Instrument des Road Pricing auf deutlich mehr Vorbehalte als in jenen aus der deutschen Schweiz.» (Rey, 2004, S. 5). Die Teilnehmenden machten ihre Bereitschaft zur Akzeptanz des Instrumentes auch von den damit verbundenen Zielen und der Transparenz des Umsetzungsprozesses abhängig.

Pay as you drive

«Pay as you drive» (PAYD, deutsch: «Bezahle, wie Du fährst») erweitert typische Prämienmodelle von Autoversicherungen um nutzungs- bzw. risikobezogene Parameter, die auf der lückenlosen Erfassung von Strecke, Uhrzeit und Fahrverhalten basieren. Sie werden einerseits als «massgeschneiderte» Lösungen mit Potenzial zur Kostenreduktion für Wenigfahrerinnen beworben, andererseits mit dem Anreiz für junge Fahrer vermarktet, durch risikobewussten und umsichtigen Fahrstil die hohen Gebühren für Fahranfänger zu reduzieren (Progressive, 2004; Aviva, 2006).

Das Konzept wurde vor ca. fünf Jahren in der Schweiz als Angebot für Privatkundinnen und Unternehmen diskutiert,[92] jedoch noch nicht eingeführt. Die Diskussion wurde durch Pilotprojekte von Versicherungsunternehmen in anderen europäischen Ländern und in den USA initiiert.

Technologisch basieren PAYD-Versicherungen im Wesentlichen auf der kontinuierlichen Beobachtung und Auswertung der GPS-Koordinaten des Fahr-

änderung und damit der Zustimmung der Mehrheit der Stimmbürger (Rapp 2007, S. 11). Die Ergebnisse einer Bevölkerungsumfrage zeigten vor einigen Jahren keine Mehrheit für die Einführung von Strassenbenutzungsgebühren in der Schweiz. Der Lösungsansatz «Mobility Pricing» ist auch bei zivilgesellschaftlichen Akteuren umstritten. Der Touring Club Schweiz (TCS) kritisiert, dass die bisherigen Konzeptionen nur die Vorteile von Strassenzöllen aufführten und somit nicht darlegten, «unter welchen Bedingungen und in welcher Form die Einführung eines Road Pricing in der Schweiz sinnvoll wäre.» (TCS, 2007).

92 http://www.privacy-security.ch/interface/2007/

zeugs, die Aufschluss über Fahrleistung, Uhrzeit, gefahrene Routen (Rush Hour oder «risikoreiche» Gebiete) oder Fahrstil geben. Hierzu wird im Fahrzeug eine «On-Board Unit» (OBU) installiert, die die Strecken nach Zeit und Geokoordinaten erfasst und über eine Mobilfunkverbindung an die Kostenstelle leitet. So können u.a. auch Geschwindigkeitsübertretungen registriert werden.

5.3.1 Ergänzende internationale Beispiele

ECall-Initiative der Europäischen Union

ECall ist ein auf europäischer Ebene standardisiertes Rettungssystem auf Initiative der Europäischen Kommission. Die Schweiz hat die diesbezügliche Absichtserklärung unterschrieben. Die Zuständigkeit für eCall liegt auf der kantonalen Ebene. (Rapp et al., 2009)

Bei einem schweren Unfall bzw. wenn mehrere vorgegebene Sensoren im Fahrzeug einen Grenzwert überschreiten, sendet eCall eine Nachricht an die einheitliche europäische Notrufnummer 112 und übermittelt Fahrzeugdaten («Minimum set of data») und Position zum Unfall an die nächstgelegene Einsatzzentrale. Die erforderlichen Daten, Protokolle, die Ortung und die Abwicklung sind standardisiert (Rapp et al. 2009, S. 11). Neben der Übermittlung von Daten initiiert eCall auch die Sprachkommunikation zwischen dem Fahrer und der Notrufzentrale. Ziel ist es, eine schnellere Ortung durchzuführen und das Eintreffen der Rettungskräfte am Unfallort zu beschleunigen (Rapp et al. 2009, S. 5). Die Anwendung soll dem Problem entgegen wirken, dass bei schweren Verkehrsunfällen, insbesondere auf wenig befahrenen Strassen, wertvolle Zeit verstreichen kann, bis die Rettungsdienste alarmiert sind. Von 2015 an sollen Neuwagen mit dem automatischen Notrufsystem eCall ausgerüstet werden, auch eine Nachrüstung wird möglich sein. Das Basissystem soll ca. 200 Euro kosten (Europäische Union, 2010).

ECall hat insbesondere dann Vorteile, wenn Unfallopfer nicht mehr in der Lage sind, per Mobiltelefon selbst Hilfe anzufordern, wenn sie ihre genaue Position nicht kennen und kein Beobachter vor Ort ist. Auch kennen Touristen oft nicht die Notrufnummer oder können sich aufgrund von Sprachbarrieren nicht ausreichend verständigen. Durch eCall werden vor allem in diesen Fällen die Reaktionszeiten verkürzt (Rapp et al. 2009, S. 11).

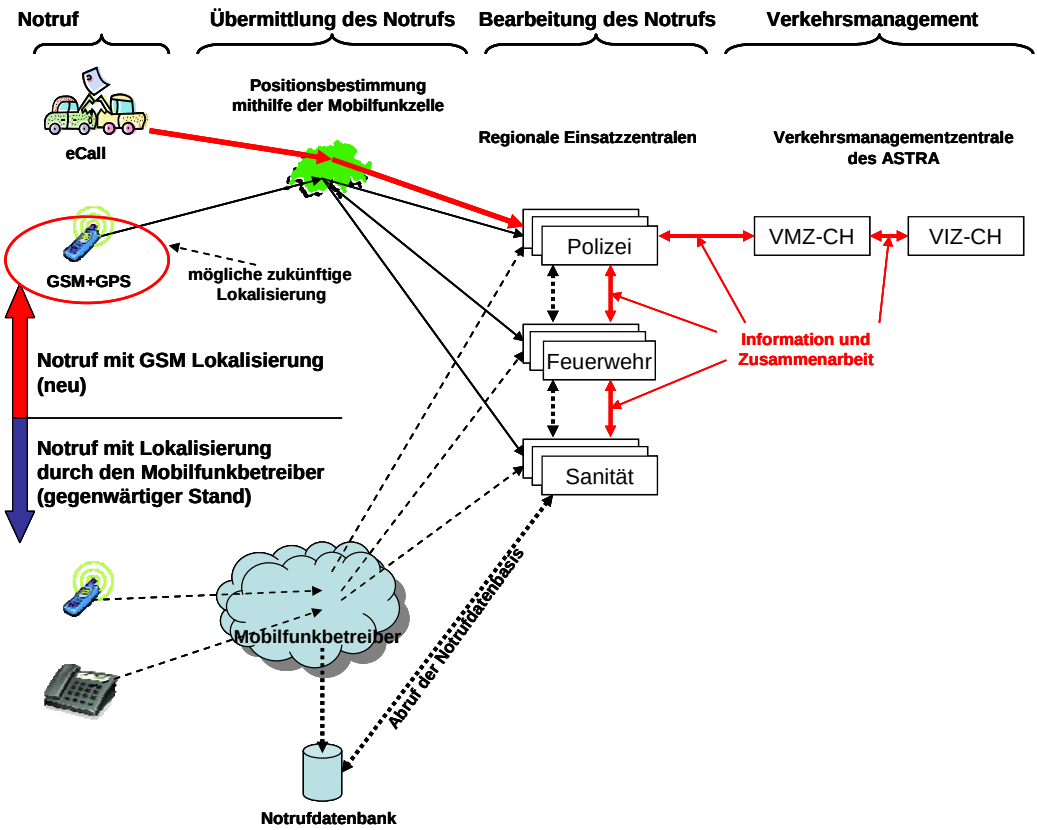


Abbildung 7: *Schema der Behandlung von Notrufen und möglicher eCalls in der Schweiz (Bildquelle: Rapp et al. 2009, S. 46)*

ECall ist auch ein Beispiel für die informationstechnische Aufrüstung der Fahrzeuge. Zahl und Empfindlichkeit der Sensoren haben allein in den letzten fünf Jahren, seitdem eCall diskutiert wird, deutlich zugenommen. Das GPS-Signal ist genauer als die Ortung in einer Mobilfunkzelle, neben den exakten Koordinaten des Unfallortes wird auf Autobahnen auch die Fahrtrichtung einbezogen, die Zahl der eingerasteten Sicherheitsgurte erlaubt Hinweise auf die Zahl der möglichen Verletzten, die ausgelösten Sensoren lassen Art und Schwere des Unfalls erkennen. Die Übermittlung einer Fahrzeug-Identifikationsnummer ermöglicht es den Rettungshelfern, bereits auf der Fahrt zum Einsatz

die Rettungsblätter des betreffenden Fahrzeugtyps zu studieren. ECall nutzt die in Europa fast flächendeckend einheitliche Notrufnummer 112.

ECall stellt höhere Anforderungen an die Leitstellen und an das Zusammenwirken von Akteuren: Zur flächendeckenden Einführung von eCall müssen alle Notrufzentralen über die für die Annahme und Bearbeitung von eCall-Notrufen erforderliche Ausrüstung verfügen (Europäische Union, 2009). In der Schweiz müssten dazu rund 70 Notrufzentralen aufgerüstet werden (Rapp et al. 2009, S. 31). Entscheidend für das Funktionieren von eCall ist eine ausreichende Mobilfunknetzabdeckung, auch in Gebieten mit schlechtem Mobilfunkempfang (wie in Garagen, Tunnels und Gebieten mit schwacher Netzabdeckung). Dazu zählt auch die Lokalisierung des Standortes in der Mobilfunkzelle. Notruforganisationen müssen über die eCall-Technologie und geschultes Personal verfügen, Behörden die Massnahmen koordinieren. Von Versicherungsunternehmen wird erhofft, dass sie ihre Prämien für Fahrzeuge mit eCall reduzieren (Rapp et al., 2009).

Basierend auf der Kosten-Nutzen Analyse der EU wurde für die Schweiz errechnet, dass mit eCall die Zahl der Verkehrstoten jährlich um 10–20 Personen gesenkt würde und damit Einsparungen von 20–50 Mio. CHF möglich wären (Rapp et al., 2009, S. 5).

Derzeit zeichnen sich technische Entwicklungen ab, die die eCall-Technologie substituieren könnten. Hierzu zählt beispielsweise die Notruffunktion von Mobiltelefonen. «Die rasche Entwicklung und ein kommerzieller Erfolg von solchen neuartigen Technologien könnten einen wesentlichen Bestandteil des heutigen eCall Konzeptes in Frage stellen und dadurch seine Implementierung stark beeinflussen.» (Rapp et al. 2009, S. 50).

Auch mit GPS-fähigen Smartphones kann eine Übermittlung der Unfallposition erfolgen. Die schweizerische Luftrettung Rega bietet eine iPhone-Applikation an, die bei einem Handynotruf auch die Standortangaben des Anrufers übermittelt und den Ortungsvorgang verkürzt. Bis heute wurde die Anwendung in fünf Notfällen erfolgreich eingesetzt. «iRega» kann bei Notfällen in der Schweiz und im Ausland genutzt werden. Zwei Tastatureingaben genügen, um Alarm auszulösen. Dabei werden sogleich die Koordinaten und zuvor abgespeicherte Personalien des Anwenders an die Rega übermittelt und eine Telefonverbindung mit der Einsatzzentrale hergestellt. Nach telefonischer Rücksprache mit dem Alarmierenden leitet die Rega dann die Rettung ein.» Voraussetzung

für iRega ist die Aktivierung von Ortungsdiensten im iPhone. Die App stellt auch eine Testfunktion für Anwender und Anwenderinnen bereit (Klöpper, 2011).

Europäischer elektronischer Mautdienst

Der europäische elektronische Mautdienst (EETS[93]) hat das Ziel, Autofahrern den Zugang zu gebührenpflichtigen Infrastrukturen in der Europäischen Union zu erleichtern. Ein einziger Vertrag mit einem EETS-Anbieter soll es ermöglichen, Maut in allen EETS-Gebieten des europäischen Strassennetzes zu bezahlen. Basis ist ein Bordgerät (OBE – On-board equipment), das in allen EETS-Gebieten verwendet werden kann (EETS, 2009). Der EETS ist in der Richtlinie 2004/52/EG geregelt.

Die EETS-Provider entrichten an die Mauterheber (die sog. Toll Charger) die in Rechnung gestellten Mautgebühren und stellen diese wiederum ihren Kunden in Rechnung. Die rechtliche Grundlage bilden die Richtlinie 2004/52/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über die Interoperabilität elektronischer Mautsysteme in der Gemeinschaft und die Entscheidung 2009/750/EG der Kommission vom 6. Oktober 2009 über die Festlegung der Merkmale des europäischen elektronischen Mautdienstes und seiner technischen Komponenten (Europäische Kommission, 2009).

Congestion-Charging-Systeme

In London, Singapur, Oslo und in Stockholm wurden sog. Congestion-Charging-Systeme aufgebaut, also Systeme, die Staugebühren (Knappheitspreise für Strassenkapazitäten) erheben. Das schwedische System ist eines der aktuellsten Beispiele. Es fusst auf einem Maut-System für den Innenstadtbereich. Das System funktioniert auf einer Kombination aus RFID und Kennzeichenerfassung an Kontrollpunkten und einem automatischem Bankeinzugsverfahren. Die Gebühren sind zu den Hauptverkehrszeiten am höchsten und auf einen Maximalbetrag begrenzt.

Ziel des Congestion-Charging-Systems ist jedoch nicht nur die Verringerung des Verkehrsaufkommens in der Innenstadt, sondern auch die stärkere Nutzung öffentlicher Verkehrsmittel, eine geringere Umweltbelastung und die

[93] EETS: European Electronic Toll Service

Finanzierung einer Umgehungsstrasse. Durch das System reduzierte sich die Verkehrsbelastung in der Innenstadt um 25%. Die Fahrzeiten im strassengebundenen öffentlichen Nahverkehr konnten verkürzt werden und trugen so zur Attraktivität der öffentlichen Verkehrsmittel bei (IBM Deutschland, o.J.).

Crowdsourcing zur Instandhaltung von Infrastrukturen

In Städten werden Bürgerinnen und Bürger heute aufgefordert, Mängel wie defekte Strassenlaternen oder Graffiti via Internet oder Smartphone-Anwendungen zu melden. Dies kann beispielsweise bereits per SMS oder durch die Übersendung einer Bilddatei mit einer ergänzenden Textnachricht geschehen (Hagenacker, 2011). Beispiele hierfür sind *fixmystreet* oder *fixmytransport* in Grossbritannien, der *Maerker* im deutschen Bundesland Brandenburg oder Schadensmeldungen in deutschen Städten; die Stadt Wolfsburg stellt eine MeldeApp für iPhone Nutzer bereit, die auch anonyme Schadensmeldungen akzeptiert.[94] Die britischen Seiten sind auch für Nutzer des mobilen Internets optimiert und bieten eine Funktion an, den jeweiligen Standort des Nutzers zu lokalisieren.[95]

Einen Schritt weiter geht eine Smartphone-Applikation, die von der Verwaltung der Stadt Boston initiiert wurde. Die Anwendung erkennt Schlaglöcher in den Strassen durch den Beschleunigungssensor des Smartphone und meldet dann die GPS-Position an die Verwaltung. Sofern von mehreren Smartphones bzw. mehrfach Hinweise auf Schlaglöcher gesendet werden, ist von einem Instandsetzungsbedarf ausgegangen (Brandon, 2011).

5.3.2 Exkurs: Entwicklungen im Bereich «intelligente Fahrzeuge»

Fahrer-Assistenz-Systeme

Systeme zur Fahrerassistenz steigern die Sicherheit im Strassenverkehr. Sie tragen dazu bei, Unfälle zu vermeiden, indem sie den Fahrer warnen, wenn er seine eigene Leistungsfähigkeit überschätzt, wenn diese absinkt oder beispielsweise bei einem Herzinfarkt nicht mehr gegeben ist. Ortungstechnologien

94 http://www.wolfsburg.de/irj/portal/anonymous?NavigationTarget=imperiafully://de/townhall/49c0f8b2.xml/Rathaus/Rathaus/Kommunikation/Nachrichten/Schadensmeldung

95 http://www.fixmystreet.com/ oder http://www.fixmytransport.com

wirken hier entweder allein oder mit spezieller Sensorik und Aktorik zusammen. Solche Systeme gibt es heute auch als Smartphone-Apps (Grifantini, 2011).

Eingreifende Fahrüberwachungssysteme

So genannte eingreifende Fahrüberwachungssysteme sollen dazu beitragen, Diebstähle oder Kollisionen zu vermeiden. Als Diebstahlsicherung können sie beispielsweise einen Neustart des Autos unterbinden. Autoverleiher diskutieren eine Lösung, bei der das Fahrzeug nach einem unzulässigen Grenzübertritt stillgelegt wird.

Automatisierte Fahrsysteme

Im Oktober 2010 meldeten die Nachrichtenagenturen zwei Pilotversuche mit führerlosen Personenwagen im Strassenverkehr. Ein mit Laserscannern und Radarsensoren ausgerüsteter VW Passat der Technischen Universität Braunschweig mit dem Namen «Leonie» fuhr führerlos drei Kilometer durch die Stadt (Roboterauto «Leonie» rollt durch Braunschweig, 2010).

In den USA wurde ein führerloser Wagen vom Softwarekonzern Google getestet. Nach Unternehmensangaben wurden mit sieben Testfahrzeugen bereits 225 000 Kilometer ohne Eingreifen des Fahrzeugführers zurückgelegt (Auch Google testet Roboterautos, 2010). Zur Orientierung greifen die Roboterwagen nach Pressemitteilungen unter anderem auf die Daten von Google Street View zurück (dpa, 2010).

Smartphone-Anwendungen mit Fahrer-Assistenz-Funktionen

Typischerweise werden unter Fahrerassistenz-Systemen Lösungen verstanden, die fest im Fahrzeug installiert werden. Mittlerweise sind jedoch auch Anwendungen für Smartphones verfügbar, die Autofahrer unterstützen sollen. Beispielsweise berechnet die Anwendung «iOnRoad» mittels GPS, Beschleunigungssensor und Kreiselinstrument die Entfernung zu anderen Fahrzeugen und die Geschwindigkeit, mit der diese unterwegs sind. In Gefahrensituationen ertönt ein Warnton, gleichzeitig wird ein Warnsignal auf dem Display ausgegeben (Grifantini, 2011).

Tracking von Fahrzeugen als (unerwünschter) Nebeneffekt von Bordnetzen

In heutigen Autos werden zum Teil drahtlose Bordnetze zur Datenübertragung eingesetzt. Durch das Auffangen der Funksignale lässt sich u.U. das Fahrzeug eindeutig identifizieren, was unter Aspekten des Datenschutzes von Bedeutung sein kann (vgl. Abschnitt 2.3.10, Proprietäre Sensornetze).

5.4 Gesellschaftliche Relevanz von Ortungstechnologien für Mobilität

Im Folgenden beurteilen wir die im Bereich der Mobilität diskutierten Anwendungen von Ortungstechnologien nach ihrer gesellschaftlichen Relevanz und verwenden dabei die in Abschnitt 4.2.1 eingeführten generellen Kriterien. Zur Erläuterung der Kriterien, die hier als Zwischentitel eingesetzt sind, vgl. S. 76ff und dort Tabelle 4.

Dieser Abschnitt wird durch illustrierende, anschauliche Beispiele ergänzt, die durch Kästen vom Text abgehoben sind.

Veränderungspotenzial, Machbarkeit

Die alltägliche Anwendung von Ortungstechnologien im Anwendungsfeld Mobilität ist bereits Realität, wie die vorausgegangen Abschnitte gezeigt haben. Die Machbarkeit muss also nicht speziell begründet werden.

Veränderungspotenzial, grosse Chancen

Grosse und schon teilweise genutzte Chancen bestehen bei der Navigation und Routenplanung im Verkehr (in Zukunft auch vermehrt über verschiedene Verkehrsträger hinweg) in der Effizienz und Bequemlichkeit bei Zugangskontrollen und elektronischen Zahlungsvorgängen (z.B. im öffentlichen Verkehr) und in Sicherheitsaspekten, beispielweise für die Notrettung nach Unfällen.

Veränderungspotenzial, grosse Risiken

Ein generelles Risiko besteht darin, dass der mobile Nutzer die *Kontrolle über die eigenen Daten* verliert, falls die zunehmende Erzeugung und Verarbeitung von Ortungsdaten nicht nach den Prinzipien des Datenschutzes erfolgt. Im mobilen Internet wird der Kunde möglicherweise immer mehr durch die Preisgabe persönlicher Daten – einschliesslich seines Standorts – bezahlen und dadurch Rückschlüsse auf sein Verhalten seine sozialen Gewohnheiten und Präferenzen ermöglichen. Der Einzelne überblickt bereits heute nicht mehr, wann und in welchen Zusammenhängen personenbezogene Daten erfasst und gespeichert werden, insbesondere wenn im Ausland operierende Anbieter involviert sind. Vor diesem Hintergrund wachsen mit allgegenwärtigen Ortungstechnologien die Bedrohungen für die informationelle Selbstbestimmung. Ist es erwünscht, dass ausländische Privatfirmen die Bewegungen der Smartphones von Schweizer Politikern verfolgen können?

Veränderungspotenzial, Breitenwirkung

Weil jeder Mensch das Bedürfnis nach Mobilität hat und entsprechende Infrastrukturen nutzt, betrifft die Anwendung von Ortungstechnologien in diesem Bereich die gesamte Bevölkerung; wer nicht selbst Ortungstechnologien einsetzt, ist zumindest indirekt davon betroffen.

Ambivalenz, Hauptwirkungen

Eine intendierte Wirkung des Einsatzes von Ortungstechnologien im Mobilitätsbereich ist die verbesserte *Überwachung* von Vorgängen, Fahrzeugen und Personen. Vom Tracking von Fahrzeugen und Personen bis zur Videoüberwachung öffentlicher Plätze dienen viele Anwendungen dazu, die Bewegung im Raum und den Aufenthalt an Orten durch automatisierte Überwachung effizienter und sicherer zu machen.

Die Auswirkungen zunehmender Überwachung sind jedoch ambivalent. Den Chancen einer erhöhten Sicherheit und Effizienz steht dabei das Risiko entgegen, dass mit der Überwachung Grundsätze der informationellen Selbstbestimmung verletzt werden, ohne dass die Betroffenen dies bemerken (Rossnagel, 2007). Dadurch kann sich auch das Verständnis von öffentlichem

Raum und der Kommunikation im öffentlichen Raum verändern. Die Debatte um die Überwachung ist dabei nur ein Teil einer umfassenderen Debatte über die Nutzung des öffentlichen Raums in der Schweiz, die auch Themen umfasst wie Wegweisungsverbote, kommerzielle Nutzung öffentlicher Plätze und Konflikte um Nachtleben/Nachtruhestörung.

In die gleiche Kategorie fällt die Verhaltensbeobachtung von Kunden durch Anbieter von Produkten und Dienstleistungen, die der Optimierung des Marketings dient. Auch hier sind die Wirkungen ambivalent. Standortbezogene Dienstleistungen ermöglichen grundsätzlich neue Qualitätsmerkmale, von denen Kunden und Anbieter profitieren können, wenn die Interessen beider Seiten berücksichtigt werden (Zibuschka & Kosta, 2011). Der Kunde wird aufgrund seines Verhaltensprofils gezielt angesprochen. Die Möglichkeiten der Ortungstechnologie erlauben es insbesondere, diese Ansprache auf einen kleinen Raum (wenige Quadratmeter) zu fokussieren. Wie weitgehend diese Veränderungen sein können, zeigen die Erwartungen von Analysten, dass mobiles Marketing zunehmend die Werbung im Rundfunk oder im Internet ersetzen wird (TNS Emnid & Radiozentrale, 2011). Zugleich kann diese Entwicklung zum oben erwähnten Kontrollverlust über die eigenen Ortungsdaten beitragen.

Besonders deutlich wird die Ambivalenz von Ortungstechnologien, wenn das Ziel einer Anwendung direkt in der Überwachung einzelner Personen besteht. Einerseits kann so Schaden von Personen abgewendet bzw. Hilfe geleistet werden, andererseits können Personen in Privat- oder Arbeitsleben – auch missbräuchlich – kontrolliert werden. Wichtige Bereiche sind:

- Überwachung von Minderjährigen: Die «Ortung via Handy» eröffnet die Möglichkeit, die Bewegungsmuster von Kindern beispielsweise auf dem Schulweg zu kontrollieren. Eltern, die sich um ihre Kinder sorgen, möchten sie bei Verspätungen oder für den Fall, dass sie vermisst werden, lokalisieren können. Die Ortung von Minderjährigen wird in Expertengesprächen als mögliches Geschäftsfeld und auch als nachgefragtes Einsatzfeld benannt. Auch im Rahmen der Videoüberwachung wird die Kontrolle von Schulhäusern auch zum Schutz von Kindern und Jugendlichen thematisiert. Das Thema wirft ethische Fragen auf, die auch laut den Ergebnissen der Experteninterviews einer gesellschaftlichen Diskussion bedürfen.
- Unterstützung von Demenzkranken: Nicht alle älteren Menschen können sich bewusst für ein Notrufsystem entscheiden. Demenzkranke Menschen

und ihre Pflegerinnen und Pfleger bzw. pflegende Angehörige gelten als Gruppe, die von Ortungstechnologien profitieren können, sei es um die Autonomie zu erhöhen, die Sicherheit zu gewährleisten oder die Pflegebelastung zu reduzieren. Vor allem vor dem Hintergrund des demographischen Wandels werden derartige Assistance-Leistungen diskutiert. Entsprechende Anwendungen verbergen sich beispielsweise in Armbanduhren. Die Ortung von Demenzkranken bedarf deren Einwilligung oder bei fehlender Einwilligungsfähigkeit die Einwilligung des gesetzlichen Vertreters.

- Ortung von Arbeitnehmenden: Nach schweizerischem Arbeitsrecht ist eine Ortung einzig zum Zwecke der Überwachung des Verhaltens von Arbeitnehmenden nicht erlaubt. Zulässig ist eine Überwachung nur aus überwiegenden Sicherheitsinteressen oder zur Leistungskontrolle. Dabei müssen die Verhältnismässigkeit gewahrt und Datenschutzgrundsätze eingehalten werden. Zudem sind die Mitwirkungsrechte der Arbeitnehmenden zu beachten. Der Einsatz von Ortungssystemen ist heute in der Arbeitswelt üblich, z.B. wird beim Flottenmanagement die Echtzeit-Ortung via GPS von Fahrzeugen praktiziert. Für die Ortung von Firmenfahrzeugen bzw. der das Fahrzeug lenkenden Arbeitnehmenden setzt das Bundesgericht in BGE 130 II 425 hohe Anforderungen an die Verhältnismässigkeit (vgl. Abschnitt 3.3). In der Lehre wird zudem kritisch vermerkt, GPS-Überwachungssysteme würden stets nur eine geographische und keine inhaltliche Aussage erlauben und seien deshalb in vielen Fällen gar nicht geeignet, den beabsichtigten Zweck zu erfüllen (Wermelinger, 2004). Bekannt sind Fälle von Missbrauch von Videoüberwachung zur Verhaltenskontrolle beispielsweise im Einzelhandel in Deutschland. Für die Schweiz gehen die im Rahmen der Studie befragten Expertinnen und Experten von der Einhaltung der rechtlichen Vorgaben vor allem in grossen Unternehmen aus.
  - Die Basler Versicherung will ihre Mitarbeiter im technischen Dienst im Schichtdienst vor allem nachts durch zusätzliche Massnahmen schützen. Dazu gehört die standortübergreifende Lokalisierung des Mitarbeitenden nach einem Vorfall (nextiraone, 2011).
  - Im Rahmen der Videoüberwachung im öffentlichen Nahverkehr werden Mitarbeitende nicht erfasst. Allerdings haben einzelne Erwerbstätige den Wunsch geäussert, in die Videoaufzeichnung einbezogen zu werden, um ihr korrektes Verhalten im Konfliktfall belegen zu können.

Insgesamt ist festzuhalten, dass der Einsatz von Ortungstechnologien zur gezielten Überwachung von Personen ein sensibles und vielschichtiges Thema ist, das dringend einer offenen Diskussion bedarf.

Ambivalenz, Nebenwirkungen

Viele Anwendungen von Ortungstechnologien haben die Nebenwirkung, dass sie langfristig gespeicherte Datenspuren hinterlassen. Mit immer geringerem technischem Aufwand lassen sich frühere Aufenthaltsorte von Objekten zurückverfolgen, und zwar auch dann, wenn – wie beim mobilen Internetzugriff oder beim Fotografieren – der primäre Zweck nicht darin bestand, Ort und Zeitpunkt der Handlung zu dokumentieren oder gar Dritten offenzulegen.

Diese Auswirkung kann sowohl positiv als auch negativ bewertet werden, je nachdem ob man die damit verbundenen Vorteile höher bewertet als den drohenden Verlust von *Location Privacy*[96].

Vorteile bestehen u.a. in den verbesserten Möglichkeiten für Stadtplaner und Verkehrsforscher, wenn Bewegungsprofile von Personen ausgewertet werden können (Lischka, 2010). Im öffentlichen Bereich verbessern solche Daten die Planungssicherheit für den Ausbau von Strassen und Schienen. Dieser Nutzen ist auch dann gegeben, wenn die Daten anonymisiert vorliegen, also keine Personendaten geschaffen werden.

Ein Beispiel für die Entstehung persönlicher Datenspuren als Nebeneffekt einer anderen Anwendung sind die Datenbus-Schnittstellen in Fahrzeugen. Dadurch können GPS-Boxen Fahrzeugdaten wie Kilometerstand, Tankfüllung, Treibstoffverbrauch, Betriebsstunden, Gas- und Bremspedalstellung, Kühlwassertemperatur, Fahrerkarte und Status, Batteriespannung und Drehzahl an einen zentralen Server übertragen. Diese Daten können ausgewertet werden und erlauben vielfältige Rückschlüsse auf den Fahrer (iDynamics AG, 2010).

[96] Darunter versteht man «… the ability to prevent other parties from learning one's current or past location.» (Beresford & Stajano, 2003, zitiert nach Krumm, 2009). Die Rückverfolgbarkeit spielt dabei eine besondere Rolle: «It's not about where you are... It's where you have been!» (Gary Gale, Head of UK Engineering for Yahoo! Geo Technologies, zitiert nach Langheinrich, 2010). Für eine Einführung in die Geschichte und Bedeutung von «privacy» und die Unterscheidung zwischen «data privacy» und «location privacy» siehe Langheinrich (2009).

Zwei Koffer im gleichen Hotelzimmer

«Verfügen Gegenstände über miniaturisierte Lokalisierungstechniken, können für sie ‹Fahrtenschreiber› entwickelt werden, die immer wissen, wo sich der Gegenstand befindet. Werden diese Daten zusammen mit der momentanen Uhrzeit oder einem Zeitstempel abgespeichert, kann für jeden beliebigen Zeitpunkt die ‹Lebensspur› des Gegenstands rekonstruiert werden. Durch den Abgleich verschiedener solcher Lebensspuren kann der gemeinsame Kontext verschiedener Dinge ermittelt werden. Waren etwa zwei Koffer zur gleichen Zeit im gleichen Hotelzimmer, kann mit einer gewissen Wahrscheinlichkeit auf ein bestimmtes Verhältnis ihrer damaligen Besitzer geschlossen werden.» (Rossnagel 2007, S. 35–36).

Konfliktpotenzial, Freiwilligkeit

Datenschutz steht im Spannungsverhältnis zwischen Freiheit und Sicherheit. Spätestens seit dem 11. September 2001 ist das Interesse staatlicher Stellen hoch, aufgrund von gestiegenen Bedrohungen im öffentlichen Raum zur Gefahrenabwehr auf Daten aus Informations- und Kommunikationsnetzen sowie Ortungssystemen zuzugreifen. Ob dieses höhere Kontrollniveau zu einer höheren Sicherheit führt, die die Beschränkungen für die Privatsphäre rechtfertigen und die mangelnde Transparenz der Verwendung von personenbezogenen Daten rechtfertigen, ist in der öffentlichen Diskussion umstritten.

Nach unserem Kriterium der Freiwilligkeit zählen alle vom Staat eingesetzten Überwachungstechnologien für die Betroffenen – notwendigerweise – zu den unfreiwillig genutzten Anwendungen und sind allein schon deshalb konflliktträchtig.

Klauser verweist auf einen Effekt, der bei Konflikten zum Tragen kommen kann: Durch die Technisierung von Ordnungs- und Sicherheitsaufgaben (z.B. durch Videoüberwachung) nimmt der persönliche Kontakt zwischen Ordnungshütern auf der einen und Bürgern auf der anderen Seite ab. Es entsteht eine Zweiteilung zwischen «Kontrollraum» und «kontrolliertem Raum», die das «Miteinander» von Akteuren in ein «Nebeneinander» wandelt (Klauser, 2007).

Konfliktpotenzial, Gerechtigkeit

Generell kann ein durch Überwachung erreichter Zuwachs an Sicherheit an einem Ort auch ein Mehr an Belastungen oder Bedrohung an anderen Orten oder für andere Gruppen bedeuten (Verlagerung von Problemen, siehe die beiden Kästen), was auf lange Sicht gesellschaftliche Konflikte verstärkt.

Dürfen private Dienstleister den Verkehrsmanagement-Auftrag des Bundes unterlaufen?

Der Bund verfügt seit der Neugestaltung des Finanzausgleichs und der Aufgabenverteilung zwischen Bund und Kantonen von 2008 über die Kompetenz, auf den Nationalstrassen Massnahmen zur Lenkung des Verkehrs anzuordnen (Strassenverkehrsgesetz Art. 57c). Dabei sind neben harten Massnahmen wie zwingenden Umleitungen und Tempobegrenzungen auch blosse Umfahrungs-Empfehlungen möglich. Solche Empfehlungen geben gleichzeitig – unabhängig von den Zielen und Analysen des Bundes – auch private Anbieter von Navigationsdiensten ab.

Navigationsdienstleister werten zunehmend Daten aus Fahrzeugen im Verkehr in Echtzeit aus (sog. Floating Car Data), um Staus oder noch wenig belastete Umfahrungsmöglichkeiten zu detektieren. Fahrzeugseitig setzt das einen GPS-Empfänger (im Navigationsgerät enthalten) und ein Mobilfunkmodul voraus.

Während der Bund seine Lenkungsmassnahmen oder Empfehlungen dabei auf die Interessen der Kantone oder allenfalls der Gemeinden, durch welche wahrscheinliche Umwegrouten führen könnten, abstützen muss, haben private Anbieter keinen Grund zu solcherlei Rücksichtnahme. So könnte der Fall eintreten, dass bei einem Unfall auf einer Autobahn der Bund auf eine Umfahrungsempfehlung verzichtet, um nicht Kantonsstrassen oder Dorf-Durchfahrungen zu blockieren, während private Navigationsdienstleister genau dies empfehlen würden. Der Verkehrsmanagement-Auftrag des Bundes würde so unterlaufen oder konterkariert werden. Ein Übergewicht der Befolgung der Navigationsdienstleister-Empfehlungen könnte rasch zu massiven Konflikten mit Gemeinden, Kantonen und dem Bund führen. Eine Regelung dieser Frage ist vorderhand nicht in Sicht.

Räumliche Verlagerung von Kriminalität

Die Stadt Olten setzte früh Videoüberwachung für die Stadtentwicklung in einem städtischen Problembezirk ein. Damit waren drei unterschiedliche Ziele verbunden: Erstens sollte die Sicherheit auf den Strassen beispielsweise für die hier tätigen Prostituierten gegeben sein. Zweitens sollte das Sicherheitsgefühl von Passanten subjektiv erhöht und das Stadtgebiet so revitalisiert werden. Drittens sollte das aufgrund von Presseberichten negative Image der Stadt Olten verbessert werden (Klauser, 2007).

Klauser argumentiert, dass das Beziehungsgefüge zwischen der Technisierung des Alltags und den Erwartungen an gestiegene Sicherheit und das Sicherheitsempfinden der Bürger komplexer sei, als es in den Argumentationen der Befürworter dargestellt werde. Vor allem werden erste Erfolge häufig im Zeithorizont durch Gewöhnungseffekte überlagert. Auch müssten etwaige Verlagerungen beispielsweise von Strassenkriminalität in der Evaluation stärker berücksichtigt werden. Klauser vertritt die These, dass durch Videoüberwachung nicht die Kriminalität an sich reduziert werde. Es werde nur das «optimale Funktionieren von separierten, hierarchisch organisierten Teilen der städtischen Umgebung» unterstützt (Klauser, 2007, S. 339).

Klärungsbedarf

Die rechtlichen Anforderungen an die Transparenz bei der Bearbeitung personenbezogener Daten werden heute im Bereich von Ortungstechnologien weitgehend ausgehöhlt. Für den Einzelnen ist vielfach nicht transparent, ob, wann und durch wen seine Bewegungs- und Verhaltensprofile erfasst, ausgewertet bzw. an Dritte weitergegen werden. Den Nutzerinnen ist nach kurzer Zeit auch nicht bewusst, dass personenbezogene oder personenbeziehbare Daten erfasst werden. Der Einzelne kann deshalb die rechtmässige Verwendung von individuellen und ortsbezogenen Daten in der alltäglichen Praxis nicht mehr kontrollieren und durchsetzen. Dies gilt besonders für Auswertungen, die Ortungsdaten nachträglich analysieren.

Klärungsbedarf besteht auch beim Umgang mit Bildern von Personen. Weil sich die technischen Möglichkeiten laufend verbessern, Personen auf Fotos, Videos

oder Aufnahmen von Webcams zu identifizieren, können in Kombination mit Geotagging (einschliesslich Zeitstempeln) sowohl der Ortsbezug als auch Beziehungsmuster und Zeitpunkte ausgewertet werden (Rudin, 2011; siehe auch Abschnitt 2.3.8). Es ist deshalb anzunehmen, dass die aktuelle Diskussion um Google Street View (siehe Kasten) wohl nur ein erstes Beispiel für das Konfliktpotenzial des Umgangs mit Bildern liefert. Videoüberwachung im öffentlichen und öffentlich zugänglichen Raum wird heute nicht nur von öffentlichen Stellen, sondern auch von Unternehmen oder Privatpersonen durchgeführt. Diese Daten werden zukünftig noch umfassender ausgewertet werden können. Derzeit ist ungeklärt, welche politischen Einflussmöglichkeiten zur Gewährleistung von Datenschutz und informationeller Selbstbestimmung bestehen bleiben, wenn standortbezogene Datenauswertungen durch ausländische Unternehmen im grossen Massstab erfolgen werden.

Aktuell bestehen in der Schweiz uneinheitliche Regelungen im Bereich Videoüberwachung auf kantonaler und auf kommunaler Ebene. Im Sinne der Transparenz und der Gewährleistung von Medienkompetenz erscheinen einheitliche Regelungen oder ein einheitlicher Mindeststandard sinnvoll (EJPD, 2007). Videoüberwachung durch staatliche Behörden stellt einen Grundrechtseingriff dar und ist nur zulässig, wenn für die Überwachung eine ausreichende gesetzliche Grundlage und ein öffentliches Interesse vorliegen und der Grundsatz der Verhältnismässigkeit gewahrt ist. Laut EJPD (2007) waren Umfang und Modalitäten der Videoüberwachung in der Schweiz uneinheitlich geregelt. Inzwischen wurde beispielsweise für alle Schweizer Unternehmen, die Personen regelmässig und gewerbsmässig befördern, mit dem Bundesgesetz über die Personenbeförderung (kurz: Personenbeförderungsgesetz, PBG) vom 20. März 2009 eine einheitliche Regelung geschaffen. Diverse bundesrechtliche Vorschriften regeln Videoüberwachung staatlicher Verwaltungs-, Parlaments- und Regierungsgebäude und orientieren sich an den unterschiedlichen Anforderungen. Das EJPD wies 2007 auf ungenügende Regelungen hinsichtlich Existenz und Qualität der rechtlichen Grundlagen hin: «Diejenigen Kantone und Gemeinden, die über keine oder nur ungenügend bestimmte formellgesetzliche Grundlagen für die Videoüberwachung mit Personenerkennbarkeit verfügen, erfüllen die verfassungsmässigen Voraussetzungen für die Einschränkung von Grundrechten nicht.» (EJPD, 2007, S. 2).

Die Kontroverse um Google Street View

Am Beispiel von «Google Street View» wird deutlich, wie ein neues Phänomen gesellschaftlichen und rechtlichen Klärungsbedarf auslöst. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hatte in dieser Angelegenheit das Bundesverwaltungsgericht angerufen, um die Persönlichkeitsrechte betroffener Personen zu schützen. Google war zuvor Empfehlungen des EDÖB «zur datenschutzkonformen Ausgestaltung von Street View» nicht gefolgt. Dazu zählte u.a. die Forderung, «sämtliche aufgenommenen Gesichter und Kontrollschilder vor der Veröffentlichung unkenntlich zu machen» (EDÖB, 2011). In seinem Urteil vom 30. März 2011 folgte das Gericht dem Antrag des EDÖB (BVGer, A-7040/2009; vgl. Abschnitte 3.3 und 3.5.2).

Der EDÖB betont in seinem 18. Tätigkeitsbericht die Alleinstellungsmerkmale von Google Street View auch im Vergleich zu ähnlichen privatwirtschaftlichen Initiativen. Hier würden Daten des neuen Medienformates automatisch und flächendeckend für privatwirtschaftliche Zwecke erfasst. Die Verbände ICTswitzerland und SWICO wiesen in ihrer Stellungnahme auf unterschiedliche Regelungen zu Bildmaterial von Strassenansichten hin – je nachdem, ob die Daten für öffentliche Zwecke, durch die Presse oder durch privatwirtschaftliche Unternehmen erfasst wurden. Das Urteil werfe demnach auch rechtliche Fragen bei öffentlichen Webcams und Newsportalen auf (ICTswitzerland, 2011).

Klärungsbedarf besteht auch bei Anwendungen im Rettungswesen. Die Chancen für den Erhalt von Menschenleben durch die schnelle und genaue Ortung von Personen stehen zwar ausser Frage. Dazu sind aber hohe Investitionen in Infrastrukturen erforderlich, die ggf. auch von der schnellen technischen Entwicklung überholt und teilweise entwertet werden können (wie das Beispiel der eCall-Initiative zeigt). In diesem wichtigen Handlungsfeld sind nicht nur öffentliche Akteure aktiv. Viele Unternehmen haben Assistance-Dienstleistungen auf Basis von Ortungstechnologien als zukünftiges Geschäftsfeld erkannt. Hier zeichnet sich ein Diskussionsbedarf ab, welche Leistungen im Sinne des Gemeinwohls durch öffentliche Akteure abgesichert werden müssen.

Wem gehören integrierte Verkehrsdaten?

Ortungstechnologien ermöglichen etwa im öffentlichen Verkehr zahlreiche Anwendungen wie Verkehrszählungen und Ticketing-Funktionen. Voraussetzung in integrierten Systemen wie dem ÖV Schweiz ist dabei, dass die Daten unternehmensübergreifend erhoben, gesammelt und ausgewertet werden. Somit laufen etwa Daten von Wettbewerbern wie z.B. den Schweizerischen Bundesbahnen (SBB) und regionalen Verkehrsunternehmen in einem Server zusammen. Die Nutzung der (auch anonymisierten) Daten zu Marketingzwecken, beispielsweise zum Verkauf von Verbundabonnementen in Konkurrenz zum Generalabonnement, ist für verschiedene Anbieter attraktiv. Die Frage, wie die Verfügungsmacht über die wertvollen Daten geregelt wird, damit keine Datenmonopole mit entsprechender Marktmacht entstehen, ist offen.

Mangelnde Resilienz

In dem Masse, in dem Ortungssysteme aufgrund von Abhängigkeiten zu kritischen Infrastrukturen werden, müssen auch entsprechende Schutzkonzepte vorliegen. Soweit nicht die Schutzkonzepte für die Telekommunikation auch die Ortungssysteme abdecken, besteht hier ein Mangel an Resilienz: Die Gesellschaft würde bei einer Sabotage oder einem Ausfall beispielsweise des GPS-Systems nicht über Strukturen und Institutionen verfügen, um mit dieser Situation umzugehen.

Als kritische Infrastrukturen werden Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen bezeichnet, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere Folgen eintreten würden. Dies gilt sowohl für die Verkehrsnetze als auch für die Telekommunikationsnetze.

Laut UVEK ist die Integration innovativer IKT-Systeme – und hierzu zählen wir die Ortungstechnologien – in traditionelle Infrastrukturnetze eine anspruchsvolle Aufgabe, bei der alte und neue Technologien zusammenwirken müssen. «Um die technischen und wirtschaftlichen Risiken beherrschbar zu halten, sollte die technische Aufrüstung der Infrastrukturnetze wenn immer möglich graduell

erfolgen, wobei die herkömmliche Technik im Rahmen der wirtschaftlichen Verhältnismässigkeit als redundante Rückfallebene weiterhin zur Verfügung steht» (UVEK, 2010, 61).

Es wäre abzuklären, wie weit diese Anforderung für die wichtigsten heute bereits eingesetzten Ortungstechnologien erfüllt ist; in jedem Fall erscheint es geboten, Ortungssysteme (schon aufgrund ihrer Bedeutung für die kritische Infrastruktur Verkehr) in das Programm zum Schutz Kritischer Infrastrukturen aufzunehmen und die Notwendigkeit spezifischer Schutzkonzepte abzuklären.

6 Vertiefungsfeld «Soziale Netze»

6.1 Soziale Netze und Ortung

In den vergangenen Jahren sind Plattformen im Web entstanden, die Nutzerinnen und Nutzer dabei unterstützen, ihr soziales Netz zu pflegen bzw. aufzubauen. Diese Web-Plattformen werden heute kurz als «soziale Netze»[97] (engl. «social networks») bezeichnet, obwohl diese Bezeichnung etwas ungenau das technische Mittel mit seiner intendierten Funktion gleichsetzt.

Einige dieser sozialen Netze verbinden Menschen mit ähnlichen Interessen oder Vorlieben, während andere im Wesentlichen die Bekanntenkreise der realen Sphäre nachbilden. Neuere Anwendungen integrieren verstärkt mobile Technologien, Anwendungen und Dienstleistungen. Durch die Nutzung von Ortungstechnologien wie GPS und WLAN können sich die Mitglieder «moderner» sozialer Netze damit auch zu jeder Zeit orten lassen bzw. interessante Menschen, Sehenswürdigkeiten, Geschäfte und Einrichtungen in ihrer Nähe orten.

Im Rahmen des Vertiefungsfeldes «Soziale Netze» werden gesellschaftliche Chancen und Risiken dieser Plattformen und ihren Anwendungen mit Ortungsbezug untersucht. Ziel der Untersuchung ist die Beantwortung der folgenden Forschungsfragen:

- Welche sozialen Netze gibt es und welche von ihnen bieten Ortungsfunktionen an?
- Wie sieht die Nutzung sozialer Netze mit Ortungsbezug aus? Welche Nutzergruppen sind erkennbar?
- Welche Geschäftsmodelle liegen den sozialen Netzen mit Ortungsbezug zugrunde?

[97] Wir verzichten bewusst auf den Anglizismus «Netzwerk». «Netz» ist die korrekte Übersetzung von «network».

- Welche Daten werden von den Anbietern sozialer Netze erhoben, gespeichert und verwertet? Was sagen die allgemeinen Geschäftsbedingungen bzw. Datenschutzrichtlinien darüber aus?
- Welche gesellschaftlichen Nebenwirkungen sind bei der Nutzung von sozialen Netzen mit Ortungsbezug erkennbar? Sind alle gesellschaftlichen Nutzergruppen gleichermassen betroffen?

Zur Untersuchung dieser Fragen wird zunächst eine *Umfeldanalyse* vorgenommen, die die wesentlichen Entwicklungslinien und Akteure im Kontext sozialer Netze mit Ortungsbezug darlegt. Da soziale Netze mit Ortungsbezug auch eine Weiterentwicklung der sozialen Netze insgesamt sind, ist es dabei notwendig, die Entwicklungsbedingungen von sozialen Netzen insgesamt zu beleuchten.

Anschliessend werden auf der Grundlage der in Kapitel 3.4 dargelegten Kriterien Schlussfolgerungen für die gesellschaftliche Relevanz sozialer Netze mit Ortungsbezug gezogen.

Was ist ein soziales Netz?

In der Wissenschaft beschäftigen sich vielfältige Disziplinen mit dem Thema der sozialen Netze, beispielsweise die Ökonomie, die Psychologie, die Kommunikationswissenschaften, die Rechtswissenschaften oder auch die Soziologie. Hieraus ergeben sich in der Literatur verschiedenste Quellen, die zur Definition des Begriffes «soziales Netz» herangezogen werden können. Allgemein lässt sich ein soziales Netz als System sozialer Beziehungen zwischen Individuen beschreiben. Durch die auf Barnes (in: Paulus, 1997) zurückgehende Metapher eines Fischernetzes soll menschliches Miteinander durch Knotenpunkte, welche die einzelnen Personen darstellen, und Verbindungen untereinander, die die sozialen Beziehungen ausdrücken, charakterisiert werden. Soziale Netze repräsentieren nach Trojan und Hildebrandt (in: Paulus, 1997) als primäre, sekundäre oder auch tertiäre Netze mehr oder weniger stark organisierte Gebilde. Als primäre Netze gelten nicht organisierte Netze wie Partnerschaften, Familien, Verwandte oder auch enge Freundeskreise. Sekundäre Netze sind beispielsweise Beziehungen zu Bekannten, Nachbarn oder Kollegen. Tertiäre Netze beinhalten die Vernetzung der Mitglieder von Organisationen, z.B. Arbeitskreise oder Nachbarschaftszentren.

Im Kontext des WWW versteht man unter einem sozialen Netz elektronische Plattformen zur Pflege von Beziehungsgeflechten, über die die Teilnehmer persönliche Daten austauschen und Beziehungen zueinander herstellen und vertiefen. Diese elektronisch gestützten sozialen Netze gehören in die Gruppe der sozialen Medien (englisch: social media). Soziale Medien sind dabei der Überbegriff für Medien, «die auf den ideologischen und technologischen Grundlagen des Web 2.0 aufbauen und die Herstellung und den Austausch von User Generated Content (UGC) ermöglichen.» (Kaplan & Haenlein, 2010). Als «Ideologie» des Web 2.0 ist dabei primär die Idee zu verstehen, dass die Nutzer selbst die Inhalte bestimmen. Neben den sozialen Netzen gehören in die Gruppe der sozialen Medien auch Foren, Weblogs, Media-Sharing-Plattformen, Wikis, Crowdsourcing-Angebote und Micro-Blogs. Die sozialen Medien führen zur Bildung von Gruppen und Gemeinschaften um Produkte, Unternehmen und/oder bestimmte Interessen. Die aktive Beteiligung der Nutzerinnen kann ein Wir-Gefühl unter den Mitgliedern erzeugen und soziale Beziehungen zwischen ihnen festigen bzw. aufbauen.

Es gibt breit angelegte soziale Netze wie Facebook oder MySpace, aber auch solche für spezifische private oder berufliche Interessen. Mittlerweile gibt es nahezu für jede Alters-, Religions-, Berufs- oder Personengruppe soziale Netze, für Studierende oder Schüler, für die Kleinkindererziehung oder für ältere Personen, für Jäger oder Hundebesitzer.

Mit der Mitgliedschaft in einem sozialen Netz können die Mitglieder – je nach Anbieter – eine Reihe von Funktionen nutzen. Zu den wichtigsten Funktionen zählen:

- Suche nach Menschen, die aus dem echten Leben bekannt sind: Freunde, ehemalige Arbeitskollegen, Schulfreunde, Verwandte etc. Hierfür ist es notwendig, dass diese Menschen ebenfalls Mitglied im gleichen Netz oder in einem angeschlossenen Netz sind. Um gefunden werden zu können, müssen die Mitglieder ein Mindestmass an persönlichen Daten von sich hinterlegt haben.
- Suche nach neuen, bislang unbekannten Kontakten: Über die Profile anderer Mitglieder lassen sich neue Menschen kennenlernen.

- Benachrichtigungen: Über ein integriertes Nachrichtensystem können die Mitglieder eines sozialen Netzes mit anderen Mitgliedern im Kontakt bleiben bzw. in Kontakt treten.
- Multimedialer Austausch: Über das soziale Netz lassen sich multimediale Daten (Bilder, Videos, Links zu weiteren Dokumenten, etc.) austauschen.
- Statusinformationen: Die Mitglieder können sich anzeigen lassen, wer gerade online ist, wer mit wem gemeinsame Freunde hat oder wer wen über eine andere Person kennt.
- Blogs: Zu einem Mitglied-Account gehört häufig ein Blog, der es ermöglicht, aktuelle Informationen über sich bekannt zu geben.
- Gruppen: Innerhalb eines sozialen Netzes gibt es Gruppen oder Foren, in denen sich Mitglieder zu einem Thema zusammen finden können.
- Kalender: Jeder kann Termine in seinem Mitglieds-Account verwalten, die andere Mitglieder einsehen können.
- Ortung: die Mitglieder können ihre eigene Position auf einer geographischen Karte bestimmen und nachsehen, welche Freunde oder Bekannte sich in der Nähe aufhalten bzw. welche interessanten Lokalitäten sich in der Nähe befinden.

Weltweit gibt es rund 7 Mrd. Menschen (Deutsche Stiftung Weltbevölkerung).[98] 31% oder 2,2 Mrd. nutzen das Internet (Worldometer, 2011).[99] In der Schweiz lag die Zahl der Internet-Nutzer ab 14 Jahren im Jahr 2010 bei knapp 84%. Bei den 14–29jährigen in der Schweiz ist der prozentuale Anteil mit 95% am höchsten (MA-net, 2011).[100]

Mit dem Einsatz des Internets allgemein ist auch die Nutzung von sozialen Medien im Aufschwung. Statistiken zeigen, dass die Nutzerzahlen weltweit kontinuierlich steigen. Im März 2010 nutzten über 313 Millionen Personen soziale Netze von zu Hause oder am Arbeitsplatz (Nielsen, 2010b). Eine Erhebung zum Nutzungsverhalten von sozialen Medien durch Nielsen ermittelt dabei eine weitgehende Übereinstimmung der Nutzerpräferenzen über die Ländergrenzen hinweg. In den befragten Ländern befreunden sich die Men-

98 http://www.weltbevoelkerung.de/index.php?id=45
99 http://www.worldometers.info/
100 http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html?open=5,1#1

schen mit Vorliebe auf Facebook, teilen Videos auf YouTube und informieren sich besonders gern auf Wikipedia, so die Ergebnisse aus den USA sowie sechs europäischen Ländern, darunter auch die Schweiz. Der internationale Vergleich durch Nielsen zeigt, dass Facebook in den untersuchten Ländern oftmals das soziale Netz mit den meisten Nutzerinnen und Nutzern ist, so beispielsweise in den USA, UK und Italien (Nielsen, 2010a).

Eine von der Europäischen Kommission in Auftrag gegebene Umfrage ergab, dass bereits heute europaweit ein Grossteil der Heranwachsenden in sozialen Netzen aktiv ist. Bereits 77% der 13–16-Jährigen und 38% der 9–12-Jährigen sollen über ein eigenes Profil in einem sozialen Netz verfügen und einen Grossteil ihrer Freizeit in sozialen Netzen verbringen, um hier mit Freunden zu chatten, Fotos, Filmclips und Musikvideos zu tauschen oder virtuelle Grüsse zu hinterlassen (EU, 2011). Zwar sind die Jüngeren erwartungsgemäss deutlich häufiger in sozialen Netzen anzutreffen, die Zuwachsraten bei den Nutzern ab 50 Jahren sind jedoch in den letzten Jahren auch signifikant gestiegen (Lenhart et. al., 2010; Madden, 2010; Purcell, 2010).

Die Idee der elektronischen sozialen Netze besteht mittlerweile seit mehr als einem Jahrzehnt: Das erste, auch heute noch bekannte soziale Netz «Friendster» ging im Jahr 2002 online. MySpace, OpenBC/XING, LinkedIn folgten im Jahr 2003; 2004 starteten Orkut und Facebook.

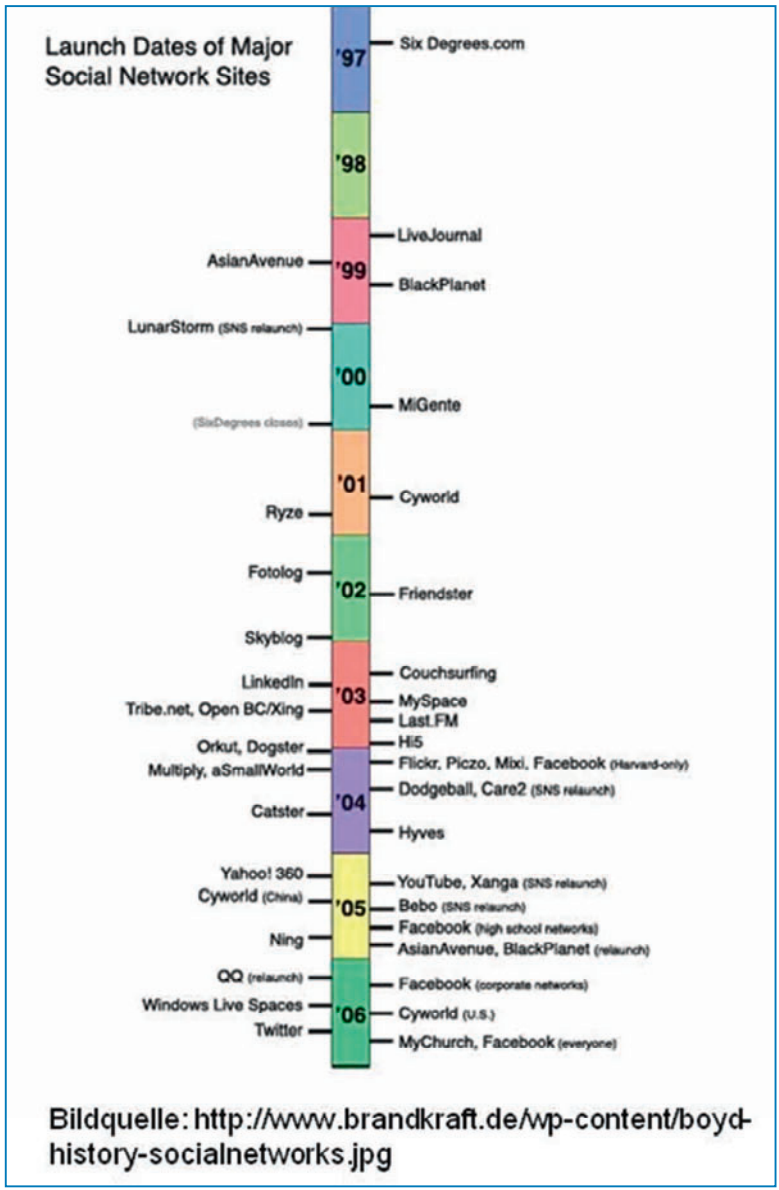


Abbildung 8: Historie von Angebot und Nutzung sozialer Netze 1997–2006

Im Folgenden sind exemplarisch Nutzungsinformationen zu ausgewählten sozialen Netzen genannt.

- **Facebook** ist weltweit die grösste und bekannteste Community – sie ist in mehr als 70 Sprachen verfügbar. Facebook hat eigenen Angaben zufolge derzeit über 800 Milionen Mitglieder (Stand: November 2011). Das Netz steht allen Interessierten offen, nachdem es sich anfangs nur an Studenten richtete. Im Oktober 2007 kaufte Microsoft einen Anteil von 1,6% an der Firma und zahlte dafür 240 Millionen Dollar.

  Jedes Profil bei Facebook hat eine sogenannte «Wall» (Pinnwand), auf der andere Nutzerinnen Kommentare hinterlassen können und die ein Protokoll der Handlungen des Facebook-Mitglieds ist. Dort finden sich Informationen darüber, mit wem sich das Mitglied angefreundet und wie sich der Status verändert hat. Zusätzlich sind dort Beiträge zu finden, die andere dort hinterlassen haben. Ausserdem können Informationen darüber, welche Veranstaltungen das Mitglied besuchen möchte und weitere Neuigkeiten vorgefunden werden. Bei Facebook können die Mitglieder Gruppen beitreten, Fan von Etwas werden, sich für Events anmelden, andere darüber informieren oder selbst Events organisieren und persönliche Fotoalben gestalten, in die Angebote anderer Facebook-Mitglieder verlinkt werden können.

- **Orkut** ist ein seit dem 24. Januar 2004 angebotenes soziales Netz von Google. Das Netz wurde nach dem Google-Techniker benannt, der es entwickelt hat: Orkut Büyükkökten. Es dient wie die anderen sozialen Netze hauptsächlich dazu, Bekanntschaften zu schliessen und zu pflegen. Orkut hat sich vor allem in Brasilien schnell verbreitet. Voraussetzung für die Erstellung eines Orkut-Profils ist ein Google-Konto. In Orkut können Communities gebildet, Fotoalben eingerichtet und Anwendungen (Apps) zum Profil hinzugefügt werden. Zudem können die Mitglieder des sozialen Netzes (video-)chatten.

- **LinkedIn** ist eine Online-Plattform zur Pflege und zum Knüpfen von Geschäftskontakten. Die am 5. Mai 2003 offiziell gegründete Website hat nach eigenen Angaben weltweit mehr als 100 Millionen Mitglieder in mehr als 200 Ländern und Regionen, davon über eine Millionen in der DACH-Region (Deutschland, Österreich, Schweiz) (Stand: März 2011). LinkedIn ist derzeit in sechs Sprachversionen verfügbar: Englisch, Französisch, Deutsch, Italienisch, Portugiesisch und Spanisch. LinkedIn bezeichnet sich

als «Wissensnetzwerk für Entscheider». Vor allem Fach- und Führungskräfte sowie Experten sollen sich hier vernetzen.

- **Xing** – das deutsche Pendant zu LinkedIn – berichtet von über 10,8 Millionen Mitgliedern weltweit, die die Plattform für Geschäft, Job und Karriere nutzen (Stand: März 2011). Die Zahl der Nutzer in Deutschland, Österreich und der Schweiz wird mit rund 4,7 Millionen beziffert. Die 2003 in Hamburg gegründete Plattform hiess ursprünglich OpenBC und ist seit 2006 unter neuem Namen börsennotiert.
- **Netlog** ist ein soziales Netz speziell für Jugendliche. Ähnlich wie bei anderen sozialen Netzen können sich die Nutzerinnen und Nutzer dort anmelden und eine so genannte Nickpage mit Blogs, Bildern, Videos, Events und vielem mehr erstellen und mit Freunden teilen. Der Anbieter *Massive Media NV* hat eine Lokalisierungs-Technologie entwickelt, über die alle Inhalte für jedes Mitglied geografisch abgestimmt und personalisiert werden. Netlog ist eigenen Angaben zufolge zur Zeit in 34 Sprachen verfügbar und hat mehr als 77 Millionen Mitglieder in Europa.
- **Twitter** (engl. für zwitschern) hat eigenen Angaben zufolge weltweit 200 Millionen Mitglieder, davon sind 45% 18–34 Jahre alt.[101] Twitter ist eine Anwendung zum Mikroblogging, einer Form des Bloggens, bei der die Benutzer SMS-ähnliche Kurznachrichten von maximal 140 Zeichen veröffentlichen. Privatpersonen nutzen Twitter u.a. als öffentliches Tagebuch im Internet, Organisationen hauptsächlich als Plattform zur Verbreitung von Pressemitteilungen oder Unternehmensnachrichten. Auch bei Diskussionen beispielsweise von Teilnehmenden einer Veranstaltung oder zur spontanen Verabredung von Gruppen (sog. «flash mobs») findet Twitter Anwendung. Der US-Schauspieler Charlie Sheen hatte bereits zwei Tage nach der Einrichtung seines Kontos bei Twitter 1,3 Millionen sogenannte Followers, die seine Einträge bei Twitter verfolgen. Popstar Lady Gaga hat rund 8,5 Millionen Followers (o. V., 2011a).

[101] http://www.twitter-welt.ch/2011/05/ein-paar-zahlen-zu-twitter/

Tabelle 5: Nutzung sozialer Netze nach Ländern in Millionen Nutzern (ohne Doppelzählungen) und Stunden pro Monat

Country	Unique Audience (000)	Time per Person (hh:mm:ss)
United States	142,052	6:09:13
Japan	46,558	2:50:21
Brazil	31,345	4:33:10
United Kingdom	29,129	6:07:54
Germany	28,057	4:11:45
France	26,786	4:04:39
Spain	19,456	5:30:55
Italy	18,256	6:00:07
Australia	9,895	6:52:28
Switzerland	2,451	3:54:34
Source: The Nielsen Company		

Aber nicht nur die Reichweite in Anzahl der Nutzerinnen und Nutzer, sondern auch die Zeit, die sie in sozialen Netzen verbringen, ist von grosser Bedeutung, unter anderem für die Platzierung von Werbeanzeigen. Laut einer Studie der Nielsen Company verbringen «globale Nutzer»[102] durchschnittlich mehr als 5,5 Stunden pro Monat in sozialen Netzen. Spitzenreiter sind die Australier, die knapp sieben Stunden in sozialen Netzen verbringen; die Schweizer Internetnutzer halten sich durchschnittlich 3 Stunden und 54 Minuten pro Monat in sozialen Netzen auf.

Der Aufstieg des Internet zum Hauptmedium für viele Menschen bedeutet, dass nicht nur Privatpersonen, sondern zunehmend auch Organisiationen bzw. Unternehmen in sozialen Medien präsent sind bzw. sein müssen. In sozialen Netzen werden häufig die wichtigsten Informationen zu Produkten und Dienstleistungen vor einem Kauf gesucht und/oder zwischen Individuen ausgetauscht (Raddatz, 2010). Die Gespräche vieler Millionen Internet-Nutzer beeinflussen die Meinungsbildung breiter Massen gegenüber Unternehmen und deren Angeboten (Schmiegelow & Milan, 2010). Daher gilt: Die Glaubwürdigkeit

[102] In der Studie wurden Daten der folgenden Länder erfasst: U.S., Grossbritannien, Australien, Brasilien, Japan, Schweiz, Deutschland, Frankreich, Spanien und Italien.

von Marken, Angeboten und Unternehmen wird mittlerweile auch durch die Transparenz und Authentizität ihrer Kommunikation in den sozialen Medien, insbesondere sozialen Netzen beeinflusst.

Für Unternehmen spielt – unabhängig von ihrer Grösse – zum einen das «Social Media Marketing (SMM)» eine Rolle, das verschiedene Formen der sozialen Medien nutzt, um mit den Kunden oder potenziellen Kunden in Kontakt zu treten. Kernelemente und Voraussetzung eines erfolgreichen SMM sind der Dialog mit den Nutzern, Transparenz in der Kommunikation und die Fähigkeit, Kritik von Kunden anzunehmen und angemessen darauf zu reagieren (Raddatz, 2010). Die Gemeinschaft der Internet-Nutzer selbst steht dabei im Mittelpunkt: Das Ziel besteht darin, durch Interaktion mit den Nutzerinnen eine langfristige Beziehung auf Basis von Loyalität und Vertrauen aufzubauen (Weinberg, 2010). SMM macht sich bei der Erreichung von Marketing-Zielen die Beteiligung der Anwender zunutze: Engagierte Kunden und Fans fügen im Positivfall den Online-Inhalten der Unternehmen ihre eigenen Videos, Fotos, Präsentationen hinzu und ergänzen diese im Sinne des anbietenden Unternehmens (Schmiegelow & Milan, 2010). Im Negativfall können Fehler und Versäumnisse in diesen Medien allerdings auch zu unerwünschten viralen Effekten führen, wenn Kritik, schlechte Erfahrungen oder nicht eingehaltene Versprechungen Gegenstand des Austauschs sind.

Zum anderen spielen für Organisationen bzw. Unternehmen die sozialen Netze zunehmend im Bereich der Personalrekrutierung eine bedeutende Rolle. Vor allem Grossunternehmen setzen hier zunehmend auf Facebook, Xing und LinkedIN. Die Personalabteilungen treten in den sozialen Netzen meist mit eigenen Profilen auf und veröffentlichen neben Stellenausschreibungen auch karriererelevante Informationen, Veranstaltungshinweise oder Informationen zum Arbeitgeber. Sie recherchieren gleichzeitig auch Informationen über Bewerberinnen und Bewerber im Hinblick auf deren Präsenz und Reputation in sozialen Netzen.

Eine aktuelle Untersuchung von Bernet_PR und Barbara Kunert (2011)[103] zeigt für die Schweiz, dass 62% der grossen Unternehmen aktiv Auftritte auf Facebook, YouTube, Twitter, Blog oder anderen Kanälen pflegen; 38% der befragten Unternehmen in der Schweiz engagieren sich bislang nicht in den sozialen Medien. Am stärksten ist der Einsatz der Unternehmen mit Abstand

[103] http://www.bernet.ch/socialmediastudie

auf Facebook. Im internationalen Vergleich liegt das Schweizer Social-Media-Engagement etwa gleich hoch wie in Deutschland (Studie Social Media Governance), jedoch deutlich unter den weltweiten Zahlen (Burton-Marsteller, 2010). Der Einsatz auf diesen Kanälen erfolgt bislang noch eher spontan: Erst 22% der Unternehmen haben eine Strategie im Hinblick auf ihre Aktivitäten in den sozialen Medien formuliert. Nur 30% verfügen über Mitarbeiter-Richtlinien für den Einsatz dieser Instrumente. Die wichtigsten drei Ziele sind mehr Dialog (64% der Nennungen), Markenpflege als Arbeitgeber (59%) und generelle Image- und Reputationspflege (52%). Als grösste Schwächen der sozialen Medien werden befürchtet: Kontrollverlust (62%), hoher Aufwand (57%), Gefahr von Indiskretionen und öffentliche Kritik (je 12%).

Angebot und Nutzung sozialer Netze mit Ortsbezug

Der Ortsbezug in sozialen Netzen ist eng mit der zunehmenden mobilen Nutzung des Internet verbunden: Immer mehr Nutzer greifen mit Endgeräten wie Handy, PDA oder Netbook auf die sozialen Netze zu. Bereits 2012 sollen 134 Millionen Nutzerinnen weltweit vom Handy aus soziale Netze besuchen, so eine aktuelle Studie der «Cyber Security»-Agentur der Europäischen Union, Enisa (Enisa, 2010).

Viele der sozialen Netze bieten mittlerweile den mobilen Zugriff an:

- Twitter bietet ein Miniprogramm für Apple iOS (iPhone, iPad) und Smartphones mit Google Android-Betriebssystem. Das grundlegende Konzept von Twitter, Informationen von maximal 140 Zeichen auszutauschen, lebt sehr stark vom mobilen Bezug: Viele Nutzerinnen und Nutzer twittern beispielsweise, wenn sie einen Zug oder ein Flugzeug betreten oder in einem Restaurant sitzen. Im Gegensatz zu der Twitter-Webseite kann direkt aus der App heraus ein Bild oder ein Geotag (vgl. Abschnitt 2.3.8), das den Ort des Benutzers anzeigt, an einen neuen Tweet angehängt werden.
- Auch Facebook setzt stark auf den mobilen Zugang und bietet Apps für Apple iOS und Google Android. Die Lösung ist genauso gestaltet wie die Twitter-Lösung: Auf der Startseite gibt es verschiedene Symbole, von denen jeweils eines für eine integrale Funktion des sozialen Netzes steht. So erreichen die Nutzerinnen und Nutzer ihre «Freunde» über eine Liste mit allen persönlichen Kontakten, die im Stil des iPhone- beziehungsweise

Android-Adressbuchs einschliesslich der Profilfotos angezeigt wird. Aus der App können auch Fotos direkt hochgeladen werden (Netzwelt, 2011).

- Auch das soziale Netz Orkut kann über ein mobiles, internetfähiges Endgerät (z.B. Handy) genutzt werden. Im März 2010 wurde eine App für Android-Telefone freigeschaltet. Damit können auch unterwegs Informationen über die Aktivitäten von Freunden abgerufen bzw. Nachrichten und Fotos für Freunde freigegeben werden.

Im Bereich der beruflichen sozialen Netze gibt es jedoch auch Gegenbeispiele. So hat XING sein Mobilangebot zunächst weiter ausgebaut und neben der mobilen Version seiner Plattform auch Apps für iPhone, Android- und Blackberry-Telefone bereitgestellt. Ab Juni 2011 wurden die Apps jedoch wieder abgeschaltet: «Die Nachfrage nach Web-Apps im Social-Business-Kontext hat sich nicht so entwickelt, wie erwartet. Deshalb haben wir uns entschlossen, die Weiterentwicklung nicht mehr voranzutreiben und die Applikationen auf XING Anfang Juni abzuschalten» (Xing, 2011).

Mit der mobilen Nutzung der sozialen Netze, die nicht zuletzt durch populäre mobile Geräte wie das iPhone und dafür entwickelte Apps sehr schnell an Bedeutung gewonnen hat, erfährt auch die Integration und Akzeptanz standortbezogener Dienste (vgl. Abschnitt 2.4.2) einen Aufschwung. Dabei eröffnet die Verknüpfung von GPS-Funktionen mit sozialen Netzen den Betreibern neue Möglichkeiten für standort- und kontextsensitives Marketing bzw. Vertrieb.

Während die klassischen sozialen Netze in erster Linie auf realen Bekanntschaften aufbauen und vom Engagement der Nutzerinnen und Nutzer auf der Plattform abhängig sind, greift die neue Generation der sozialen Netze verstärkt auf Ortungstechnologien wie GPS, WLAN oder Mobilfunk zurück (vgl. Abschnitt 2.3) und erlaubt damit auch ad-hoc organisierte, standortbezogene Information und Kommunikation. Die neuen, mobilen sozialen Netze knüpfen ihre Verbindungen damit nicht nur um Personen, sondern auch um Orte herum.

Die Nutzung der entsprechenden Dienste von sozialen Netzen auf GPS-fähigen Mobiltelefonen ermöglicht es, dass automatisch Freunde lokalisiert und kontaktiert werden können, die sich gerade in der Nähe befinden. Aber auch Fotos, Videos und andere Daten können mittels Geotagging einem bestimmten Ort zugeordnet und über diese lokale Angabe wieder von anderen Netzteilnehmern gefunden werden. Neben dem von Mitgliedern erzeugten Content sind die

neuen sozialen Netze darüber hinaus auch für standortbasierte Werbung und Mikromarketing interessant (vgl. Abschnitt 2.4.3).

Mittlerweile sind zahlreiche Dienste für die Kombination aus Handyortung (vgl. Abschnitt 2.3.2) und mobilem sozialem Netz verfügbar. Das Grundprinzip ist einfach: auf der Basis der via GPS, WLAN oder Mobilfunk ermittelten Position kann das genutzte mobile Endgerät erkennen, ob sich die Person z.B. gerade in einem Restaurant oder an einer Strassenkreuzung befindet. Mit einem Klick können sich die Mitglieder sodann – den entsprechenden Wunsch vorausgesetzt – «einchecken» und sehen, wer sonst noch da ist, wer sich oft an diesem Ort aufhält oder wer kürzlich noch dagewesen ist.

Grundsätzlich können soziale Netze, die explizit für die ortungsbezogene Nutzung konzipiert worden sind und solche, die schon längere Zeit als «klassische» soziale Netze bestehen und um eine Ortungsfunktionalität erweitert wurden, unterschieden werden:

- Klassische soziale Netze mit einer Zusatzfunktionalität «Ortsbezug»: z.B. Facebook Places/Orte, Twitter mit entsprechender Zusatzsoftware, Google Latitude.
- Soziale Netze, die eigens für die ortungsbezogene Nutzung konzipiert wurden: z.B. Foursquare, Friendticker, Brightkite, Gowalla, Aka-Aki, Yelp.

Die Gründungswelle der sozialen Netze mit Ortsbezug liegt in den Jahren 2008 bis 2010: So startete Aka-Aki im Jahr 2008 seinen Dienst, 2009 kamen Foursquare, Friendticker, Brightkite und Gowalla sowie Google Latitude hinzu. Im Jahr 2010 startete Facebook Places (USA) bzw. Orte und im Jahr 2011 erweiterte Twitter seinen Dienst um die Lokalisierungsfunktion (USA). Das Ende Juni 2011 im Feldtest online geschaltete und seit Mitte September 2011 öffentlich verfügbare soziale Netz Google+ (Google Plus) integriert von Beginn an eine Ortungsfunktionalität: Wer zulässt, dass Google plus auf den eigenen Standort zugreift, kann den Nachrichten-Stream auch unter dem Aspekt «Nearby», also nach räumlicher Nähe, anordnen.

Foursquare hat in den USA bereits für viel Aufsehen gesorgt und ist nun auch zunehmend in Europa verbreitet. Foursquare hat eigenen Angaben zufolge weltweit über zehn Millionen Nutzer, täglich sollen ca. 35 000 neue Mitglieder hinzu kommen. Die Händler-Plattform wird den Unternehmensangaben zufolge derzeit von 500 000 Unternehmen genutzt (Stand: November 2011). Der primär

über Handy-Apps genutzte Dienst verknüpft einen interaktiven Fremdenführer und ein Tool für spontane Verabredungen mit spielerischen Komponenten. Foursquare-Mitglieder verwenden die zugehörigen Smartphone-Apps (für iPhone, Android und Blackberry) oder die mobile Website, um anderen Mitgliedern ihre aktuelle Position in Form von «Check-Ins» mitzuteilen. Den Angaben von Foursquare zufolge finden täglich über eine Milliarden Check-Ins statt (Stand: November 2011). Mit Hilfe des aktuell genutzten Funknetzknotens oder auch mit Hilfe eines integrierten GPS-Moduls können die Apps die Position des Nutzers ermitteln und anzeigen, welche Restaurants, Sehenswürdigkeiten oder sonstigen interessanten Örtlichkeiten sich in der Nähe des Mitglieds befinden. Sobald ein Mitglied sich an einem Ort aufhält, den es anderen mitteilen möchte, kann es sich dort einchecken. Falls die besuchte «Location» noch nicht bei Foursquare eingetragen ist, kann sie neu angelegt werden. Sollten sich Freunde des Mitglieds in der Nähe aufhalten, informiert Foursquare die Mitglieder darüber und ermöglicht so spontane Treffen. Wer die Position eines bestimmten Standorts meldet, erhält darüber hinaus «Punkte» und kann in einer Rangliste aufsteigen. Dieses Verfahren hat zu einem Wettbewerb mit grosser Beteiligung geführt – auch beispielsweise bei Bars und Kneipen. Wirte nutzen den Wettkampf als Eigenwerbung und verteilen an den Gast mit den meisten Foursquare-Punkten beispielsweise Freigetränke. Der Couponing-Anbieter[104] Groupon will künftig im Bereich Vertrieb mit Foursquare kooperieren, berichtet *AllThingsDigital* im Mai 2011.[105]

[104] Aufgrund von späteren gesetzlichen Regelungen ist das Couponing, also die Rabattkultur in Europa, im Gegensatz zu den USA, bisher noch nicht so stark ausgeprägt. Seit 2009 sorgen jedoch zahlreiche Anbieter für Aufsehen, die Coupons im Internet auf ihren Plattformen anbieten und weltweit Millionen von Coupons verkaufen. Die sogenannten Couponanbieter, also spezielle Dienstleister, schliessen dabei mit den Gutscheinverkäufern einen Vertrag ab, in dem sie die Bedingungen für die Gutscheine festlegen. Die Gutscheinverkäufer haben oft grosse E-Mail-Empfängerlisten, die sie mit jedem lukrativen Angebot erweitern können.

[105] http://allthingsd.com/20110523/foursquare-and-groupon-planning-distribution-deal/

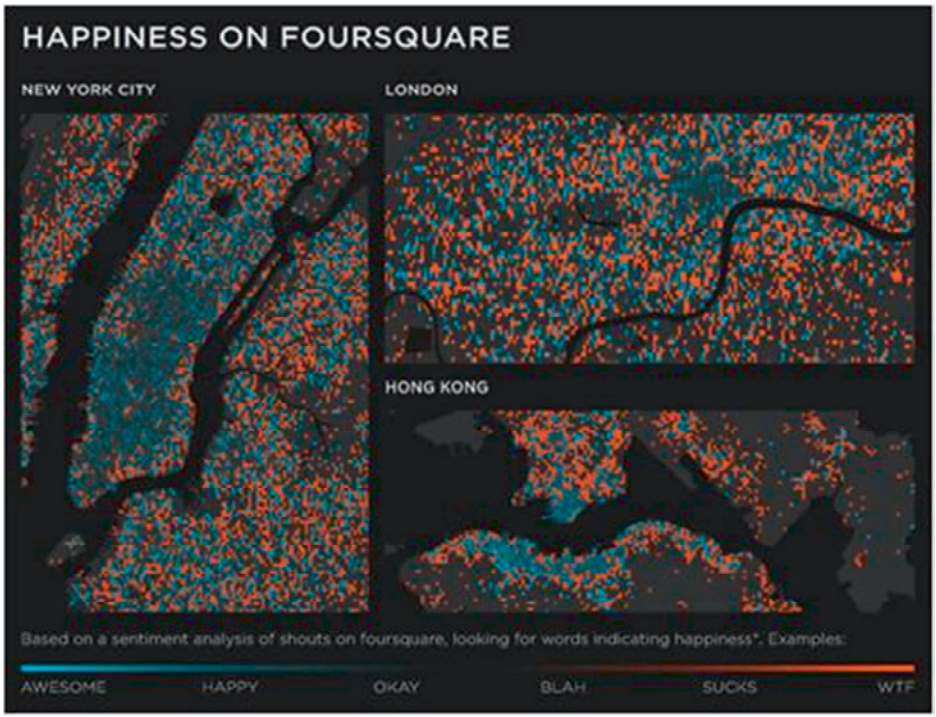


Abbildung 9: «Happiness on Foursquare»

Abbildung 9 zeigt eine ortsbezogene Auswertung von auf Foursquare geäusserten Gefühlseindrücken für die drei Orte New York City, London und Hongkong. Basis der Auswertung sind sogenannte Shouts (Nutzung der Shout-Funktion). Die Skala reicht von Blau (Begeisterung) bis Rot («Wtf» für «what the fuck»). Es zeigt sich, dass Manhatten die Foursquare-Gemeinde offensichtlich zu den meisten emphatischen Äusserungen anregt.

Friendticker wurde erstmals auf der CeBIT 2009 vorgestellt. Mit Friendticker wird dem Netz-Mitglied von seinen Freunden mitgeteilt, was diese gerade machen. Dazu zeigt der Dienst gleichzeitig auch interessante Orte wie Bars oder Cafés in der Nähe an und teilt mit, ob sich dort gerade Freunde oder andere Mitglieder befinden. Die Anwendung basiert auf einer mobilen Internet-Lösung für internetfähige Handys. Angaben zu aktuellen Mitgliederzahlen werden auf der Friendticker-Site nicht gemacht. Friendticker bietet Schnittstellen zu Twitter bzw. ist mit einer Fan-Seite dort vertreten. Friendticker ist für den

privaten Nutzer kostenlos, Firmen müssen dagegen eine Aufnahmegebühr und weitere Gebühren für jeden erfolgreichen Check-In der Mitglieder zahlen. Integraler Bestandteil der Nutzungsvoraussetzungen, formuliert in den Allgemeinen Geschäftsbedingungen, ist jedoch:

> «Mit der Inanspruchnahme von friendticker erklärt sich der Nutzer zum Erhalt von auf friendticker befindlicher Werbung auf seinem Endgerät bereit.»

Im April 2011 hat der Dienst eine enge Kooperation mit den deutschen VZ-Netzwerken (StudiVZ, MeinVZ, SchülerVZ) bekannt gegeben. Friendticker integriert dafür seine Check-In-Funktion sowie seine Informationen über Läden, Restaurants, Sehenswürdigkeiten etc. in die iPhone-App der VZ-Netzwerke. Für die nahe Zukunft ist auch eine Integration von friendticker in die Android-Applikation der VZ-Netzwerke geplant. Zudem soll es demnächst möglich sein, für Check-Ins über die VZ-App die friendticker-typischen Rabatte und Gutscheine in Anspruch nehmen zu können (Weigert, 2011).

Brightkite ist nach Angaben des Anbieters die einfache Möglichkeit, mit Freunden und Orten in Verbindung zu bleiben. Der Dienst ist in der Lage, gleichzeitig 25 Teilnehmer miteinander zu verbinden. Die Anmeldung bei Brightkite ist obligatorisch, um den Dienst nutzen zu können (Brightkite, 2011).[106] Brightkite zeigt auf Wunsch laufend geographische Positionsdaten und weitere Informationen zur Person an. Es ist möglich, die Positionen anderer Teilnehmer zu verfolgen, wenn diese sich dazu bereit erklärt haben. Wie bei fast allen Diensten können die Mitglieder den Kreis der Personen für die Bekanntgabe des Standortes eingrenzen. (Jüngling, 2009) Der Dienst bietet Schnittstellen beispielsweise zu den sozialen Netzen Twitter, Flickr oder Facebook. Brightkite ist derzeit kostenlos für die Mitglieder und wird über möglichst zielgruppen- bzw. ortsspezifische Werbung finanziert:

> «Um dies zu ermöglichen, verkaufen wir Werbung, um den Service zu unterstützen. Wir bemühen uns, die Werbung so relevant wie möglich zu gestalten, aber wir versuchen ständig, uns zu verbessern.» (brightkite, 2011; Übers. durch die Autoren).[107]

[106] http://brightkite.com/learn_more
[107] http://brightkite.com/pages/bk_terms_of_service.html

Auch **Gowalla** ist auf die mobile Kommunikation ausgerichtet. Schon zum Start gab es eine App für das iPhone, mit dem per GPS der Standort des Nutzers bzw. der Nutzerin bestimmt wird und Orte (Spots) hinzugefügt werden können, bei denen dann «eingecheckt» wird. Automatische Querinformationen zu Twitter und Facebook sind optional verfügbar. Zudem ist ein Feature Push-Nachrichten integriert: Eine Nachricht wird gesendet, wenn ein anderer «Gowalla-Freund» am gleichen Ort eincheckt. Auch die Spielefunktionen sind bei diesem Dienst relevant: Sobald die Mitglieder eingecheckt sind, können per Zufall Gegenstände (Items) «gefunden» werden. Darüber hinaus können auch Abzeichen (Pins) gesammelt werden: Im Laufe des Spiels können so verschiedenste Ränge (Spaziergänger, Wanderer, Entdecker etc.) und Auszeichnungen für selbst erstellte Orte erreicht werden. Der Dienst ist für das iPhone, Android und Blackberry sowie blackOS nutzbar. Aktuelle Mitgliederzahlen werden auf der Website von Gowalla nicht veröffentlicht. In Zürich befinden sich derzeit beispielsweise 141 Spots (Stand: Juni 2011).

Aka-Aki zeigt neben dem Standort auf Wunsch auch persönliche Vorlieben des Nutzers an. Darüber hinaus können Teilnehmer Gleichgesinnte – zum Beispiel andere Personen mit einer Vorliebe für exotische Speisen – finden und sich zum gemeinsamen, spontanen Restaurantbesuch verabreden. Aka-Aki hat seit Kurzem eine Schnittstelle zu Facebook, so dass die Anmeldung vereinfacht wird und der Facebook-Status direkt über Aka-Aki aktualisiert werden kann. Im Mai 2010 hatte Aka-Aki eigenen Angaben zufolge mehr als 700 000 Mitglieder, vor allem in Deutschland, Frankreich und Grossbritannien. Ähnliche Funktionen wie Aka-Aki bieten Dienste wie **Zyb, Picos, Loopt** oder **Qiro**.

Auch **Twitter** will künftig den momentanen Aufenthaltsort der Autoren speichern, die einen Tweet veröffentlichen. Damit soll man künftig Informationen von Twitterern ausfiltern können, die sich vor Ort befinden. Noch brauchen die Nutzerinnen und Nutzer dafür spezielle Software wie Twitroid, Twibble oder Twinkle. Der Anbieter hat jedoch bereits angekündigt, dass er die Lokalisierungsfunktion demnächst technisch unterstützen wird.

Im Jahr 2010 hat **Facebook** den Dienst **Places** (im deutschsprachigen Raum unter dem Namen **Orte**) vorgestellt. Die Nutzung setzt voraus, dass man bei Facebook registriert ist. Damit kann das grundsätzliche Potenzial der Nutzerinnen und Nutzer von Places/Orte mit über 800 Millionen beziffert werden (Stand: November 2011). Facebook-Places/Orte muss vor der ersten Nutzung aktiviert

werden. Erst nachdem der Dienst aktiviert ist, können Facebook-Mitglieder alleine oder mit ihren Freunden an verschiedenen Orten wie Restaurants, Shops oder Cafés «einchecken» und dort auch Kommentare hinterlassen. Places/Orte soll drei Zwecke erfüllen: Es hilft Mitgliedern dabei, ihren Freunden mitzuteilen, wo sie sind, wer sich in der Nähe aufhält und was in der unmittelbaren Umgebung geschieht. Erreicht werden soll dies durch eine eigene Check-In-Funktionalität innerhalb von Facebook sowie durch eine neue Schnittstelle für andere standortbasierte Dienste, um deren Nutzeraktivitäten bei Facebook integrieren zu können. Facebook Places/Orte offenbart zunächst nur Angaben über öffentliche Orte, die eindeutig beschrieben sind, Privatwohnungen werden nicht angezeigt. Allerdings ist es den Mitgliedern möglich, neue Orte hinzuzufügen. Derzeit steht der Dienst Facebook-Mitgliedern in ausgewählten Ländern mit mobilem Zugang für das iPhone, Android, Blackberry oder touch.facebook.com zur Verfügung (Sander, 2010).

Yelp wurde 2004 gegründet, um Menschen dabei zu unterstützen, lokale Anbieter wie Ärzte, Friseure oder Werkstätten ausfindig zu machen. Yelp gibt es derzeit in acht Ländern: USA, Kanada, Vereinigtes Königreich, Irland, Frankreich, Deutschland, Österreich und Niederlande.

Google hat den Dienst **Latitude** entwickelt, der die hauseigene Navigationssoftware Google Maps um die Darstellung des Aufenthalts von Personen erweitert. Um Google Latitude verwenden zu können, müssen die Interessenten ein allgemeines Google-Konto einrichten bzw. darüber verfügen (und damit auch den allgemeinen Nutzungsbedingungen von Google zustimmen). Der Dienst erlaubt auch, die eigene Position manuell anzugeben. Latitude läuft auf den meisten Smartphone-Plattformen. Bei Andoid-, Blackberry-, Symbian-S60 und Windows-Mobile-Smartphones ist Latitude ein Teil von Google Maps und oft schon vorinstalliert. Latitude nutzt zur Positionsbestimmung eine Kombination aus Mobilfunkzellen- und WLAN-Ortung sowie GPS (Janssen, 2011).

Zusätzlich hat Google im Februar 2010 **Google Buzz** lanciert, aber im Oktober 2011 wieder geschlossen. Dieser Dienst erweiterte Google Mail um einen Menüpunkt, hinter dem sich ein Nachrichten-Stream verbarg. Ähnlich wie bei Facebook und Twitter erschienen hier die abonnierten Nachrichten von Freunden sowie Kommentare zu diesen Nachrichten. Google warb noch im Juli 2011: «Entdecken Sie, was in Ihrer Nähe los ist, posten Sie eine Nachricht mit Standortkennzeichnung und zeigen Sie die Standorte Ihrer Freunde an».

Google Buzz führte einerseits zu erheblichem Unmut unter den US-Datenschützern, da zunächst automatisch die meist frequentierten – und nicht explizit freigegebenen – Kontakte eines Nutzers zum Mitlesen vorgeschlagen wurden. Andererseits will sich Google nunmehr auf «Google+» als zentrale Netzwerkplattform des Konzerns konzentrieren.

Google+ ist seit dem 28. Juni 2011 erreichbar und besteht aus mehreren Elementen, die ineinander greifen: Circles steht für die verschiedenen Freundes-, Kollegen- und Bekanntenkreise, denen die Mitglieder angehören. Sparks soll den Nutzerinnen als eine Art personalisierter News-Aggregator Inhalte zu jeweils interessierenden Themen liefern. Huddle lädt zum Textchat ein, Hangouts zum Videochat. Dazu gibt es eine Mobil-App für Android-Geräte, mit der Mitglieder Handy-Fotos hochladen und ihren Standort mitteilen können. Mit der «Nearby»-Funktion wird es hierbei möglich, einen schnellen Überblick über die Vorgänge in der Umgebung zu erhalten. Angezeigt werden beispielsweise Beiträge von Circle-Kontakten oder öffentliche Beiträge von Personen aus der Umgebung.

Erfassung, Nutzung und Weitergabe ortsbezogener Daten

Die Integration von ortsbezogenen Diensten in soziale Netze führt zu neuen Nutzungsmöglichkeiten sowohl für die Betreiber der sozialen Netze als auch für die unternehmerischen und privaten Nutzer. Sie führt aber auch zu neuen Anforderungen für die Privatsphäre ihrer einzelnen Anwender. So sind nicht nur die vielen und sensiblen privaten Daten besonders zu schützen, sondern auch die ortsbezogenen Daten in Form vom Positionsdaten und Aufenthaltsinformationen, die das (physische) Auffinden von Nutzerinnen ermöglichen bzw. erleichtern. Hinzu kommt, dass ortungsbezogene Daten von den Betreibern der sozialen Netze bzw. Anbietern dort integrierter Dienste in Datenbanken gespeichert werden können, um bessere Produkte anzubieten oder um die Lokalisation von Hot Spots für Smartphones, Tablets oder WLAN-Notebooks bereitstellen zu können. Damit stellt sich auch grundsätzlich die Frage, für wen diese Datenbanken geöffnet und nutzbar sind.

Ortungsdaten sind vor allem für Werbekunden interessant, die so Anzeigen gezielter schalten und mehr über potenzielle Kunden erfahren können. Aber auch für Strafverfolgungsbehörden sind Ortungsdaten von Nutzen.

Während Daten, die beim Surfen im Internet hinterlassen werden, vor allem Vorlieben und Interessen offenlegen, erlauben ortsbezogene Daten auch Einblicke in das tatsächliche Handeln der Menschen. Sie zeigen beispielsweise eine besuchte Arztpraxis, häufig genutzte Einkaufspassagen und Restaurants oder den Wohnstandort.

Einen Anhaltspunkt dafür, ob die Ortsinformationen durch die Anbieter der sozialen Dienste vertrauenswürdig behandelt werden, geben die Aussagen in den jeweils gültigen Geschäftsbedingungen und Datenschutzrichtlinien. Im Folgenden werden exemplarisch Angaben über die Erhebung, Nutzung und Weitergabe von Daten von Foursquare, Aka-Aki, Facebook Orte, Friendticker und Google+ dargestellt.

In den Datenschutzrichtlinien formuliert **Foursquare** unter dem Punkt «Welche personenbezogenen Daten sammelt Foursquare?»:

> «Personenbezogene Daten, die Du an uns übermittelst: Wir empfangen und speichern jegliche Informationen, die Du mittels unseres Service eingibst oder uns auf jegliche andere Art zur Verfügung stellst. Persönliche Informationen, die gesammelt werden, beinhalten unter anderem Deinen Namen, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Nutzernamen für Twitter und Facebook, Nutzungsdaten bezüglich der Benutzung unseres Service und Browser-Informationen. Wir erhalten automatisch Deinen Standort, wenn Du unseren Service benutzt. Die persönlichen Daten, die Du bereitstellst, werden für verschiedene Zwecke genutzt; zum Beispiel, um es Dir zu ermöglichen, ein Nutzerkonto und Profil zu erstellen, mit dem Du mittels unseres Service mit anderen Nutzern interagieren kannst, aber auch um den Inhalt des Service zu verbessern, Werbung und Inhalt, den Du siehst, kundengerecht zu gestalten und um Dir Mitteilungen über Sonderangebote und neue Funktionen zu schicken. Wir nutzen diese persönlichen Informationen eventuell auch, um die Services unserer Commun [Anmerkung der Autoren: der Satz bricht im Original unvermittelt ab] Daten, die automatisch gesammelt werden: Wenn Du den Service benutzt, erhält und speichert foursquare automatisch Informationen von Deinem Browser oder Deiner Handy-Plattform auf unseren Server Logs, einschliesslich Deines Standorts, IP-Adresse, Cookie-Informationen und die Seite, die Du aufgerufen hast. Wir behandeln diese Daten als nicht-persönlich, es sei denn es ist uns gesetzlich anders vorgeschrieben. foursquare nutzt diese Informationen nur als Sammeldaten. Wir übermitteln diese Sammeldaten darüber, wie unsere Kunden, kollektiv, unsere Webseite benutzen, gelegent-

> lich auch an unsere Partner, damit diese verstehen können, wie oft Leute ihre Dienstleistungen und unseren Service in Anspruch nehmen.»[108]

Zu den Datenschutzrichtlinien hat Foursquare ergänzend Informationen zum so genannten «Datenschutz 1x1» bereitgestellt. Hier heisst es:

> «Dein Standort wird NUR dann für andere sichtbar, wenn Du Dich aktiv dazu entscheidest, auf foursquare an einem bestimmten Ort einzuchecken. Jeder Deiner Check-ins auf foursquare wird auf der Seite Check-in-*Verlauf* gespeichert, damit Du sehen kannst, an welchen Orten Du seit der Erstellung Deines foursquare-Kontos überall eingecheckt hast. Du kannst einzelne oder alle Check-ins von der Verlaufsseite auf der foursquare-Webseite löschen.»

> «Um die Check-in-Informationen eines anderen Nutzers sehen zu können, musst Du mit dieser Person befreundet sein. (…) Nur Deine foursquare-*Freunde* können Deinen Check-in-Verlauf mit den einzelnen Check-ins sehen.»

Die Standortermittlung kann bei Foursquare nicht generell unterbunden werden. Allerdings bietet Foursquare ausgewählte Möglichkeiten, sich der Weitergabe von Ortsinformationen an andere Foursquare-Mitglieder zu entziehen. So hat Foursquare zum einen die Möglichkeit des «unsichtbaren Einchecken» entwickelt. Dabei können die Mitglieder an einem «Venue» einchecken, ohne dabei den spezifischen Standort mit Freunden oder anderen Mitgliedern zu teilen. Um «unsichtbar» einzuchecken, müssen die Mitglieder auf allen Check-In-Seiten der Handy-Anwendungen auf die Frage «Dieses Check-in mit Freunden teilen?» mit «Nein» antworten. Zum anderen können sich die Mitglieder unter den Einstellungen aus der so genannten «Wer-ist-hier»-Liste ausklinken, über die üblicherweise Einblick gewährt wird, welche anderen Mitglieder aktuell in der Nähe eingecheckt haben.

Foursquare räumt seinen Mitgliedern die Möglichkeit ein, ihr Konto zu schliessen. Hierbei sollen alle Daten gelöscht werden, wobei Foursquare aufgrund von Sicherheitsspeicherungen eine endgültige Löschung der Daten nach 90 Tagen zusagt.

Der Anbieter des sozialen Netzes **Aka-Aki** verweist darauf, dass der Schutz der Nutzerdaten ein zentrales Thema für das Unternehmen sei, bei einem auf

[108] Quelle: https://de.foursquare.com/legal/privacy (03.08.2011)

räumlicher Nähe basierten Dienst allerdings grundsätzlich einige Besonderheiten zu beachten seien. Dabei wird darauf verwiesen, dass Aka-Aki auf praxistauglichen, die Privatsphäre der Mitglieder respektierenden, relativen und unscharfen Kategorien von Nähe basiere. Die Mitglieder können beispielsweise sehen, wer «in der Nähe» ist oder «in Laufweite». Dabei können andere Mitglieder standardmässig nicht erkennen, in welcher Strasse sich das andere Mitglied befindet – es sei denn, diese Information wird ausdrücklich selbst mitgeteilt. Andere Mitglieder erfahren also, wie weit ein Mitglied von ihnen entfernt ist, aber nicht genau, wo es sich aufhält.

Grundsätzlich kann eine solche absichtlich ungenaue Ortsangabe durch Kombination mehrerer Angaben (u.a. durch Triangulation) zu einer genaueren verrechnet werden. Es könnten sich also mehrere Mitglieder verabreden, um ein weiteres Mitglied zu orten.

In Hinblick auf die Weitergabe von Daten an Dritte steht in den Datenschutzbestimmungen von Aka-Aki unter Punkt 12:

> «aka-aki gibt Nutzerdaten nicht an Dritte weiter, es sei denn, der Nutzer hat vorher seine ausdrückliche Einwilligung dazu erklärt oder es besteht eine rechtlichen Verpflichtung dazu. Ein Ausnahme sind bestimmte, von uns sorgfältig ausgewählte und uns insoweit weisungsgebundene technische Dienstleister, die für uns bestimmte Aufgaben übernehmen. Diese Aufgaben sind zum Beispiel das Versenden unseres Newsletters (Auftragsdatenverarbeitung) oder die Erhebung und Verarbeitung anonymisierter Daten zum Nutzungsverhalten bzw. die Erfassung von Informationen zu aufgetretenen Software-Fehlern zur Verbesserung von aka-aki.»

Ähnlich wie Foursquare bietet Aka-Aki seinen Mitgliedern die so genannte Tarnkappenfunktion: Wenn andere Mitgliedern nicht über eine Nähe informiert werden sollen, kann die Option «macht mich sichtbar: für niemanden» (Einstellungen im Handyprogramm) aktiviert werden. Auch können die Mitglieder jederzeit ihre Mitgliedschaft ohne Angabe von Gründen kündigen. Mit der Abmeldung wird den Angaben von Aka-Aki zufolge der gesamte unter dem Profil des Nutzers gespeicherte Datensatz vollständig gelöscht.

Die Funktionalität **Facebook Orte** kann genutzt werden, wenn ein Konto bei Facebook eingerichtet wurde. Sobald der Dienst «Orte» dann über eine App oder einen Browser aufgerufen wird, erfragt Facebook die Erlaubnis, den

Standort zu übermitteln. Gleichzeitig wird erfragt, ob auch Freunde den eigenen Standort eingeben können.

In den Datenschutzrichtlinien verweist Facebook auf die automatische Sammlung von Ortsinformationen:

> «Zugriff auf Informationen von Zugangsgeräten und Browsern. Wenn du über einen Computer, ein Handy oder ein anderes Gerät auf Facebook zugreifst, sammeln wir u.U. von diesem Gerät Informationen über deinen Browsertyp, deinen Standort, deine IP-Adresse und die Seiten, die du besuchst.»[109]

Auch wird unter dem Punkt «Informationen, die Du mit anderen teilst» auf eine mögliche Weitergabe von Ortsinformationen an Dritte verwiesen:

> «Wir können zudem Informationen über den Standort deines Computers oder Zugangsgeräts und dein Alter Anwendungen und Webseiten zur Verfügung stellen, damit sie angemessene Sicherheitsmassnahmen einführen und die Verbreitung von altersgemässen Inhalten kontrollieren können.»

Die Datenschutzrichtlinien enthalten keinen Hinweis auf die Verwendung bzw. Weiterleitung der Standortinformationen an werbetreibende Unternehmen, ggf. für ortsabhängige Werbung. Die Zusatzfunktion «Orte» kann über die Privacy-Einstellungen abgeschaltet werden. Dabei ist darauf zu achten, dass sowohl die besuchten Orte auf «nur ich» gestellt als auch die Möglichkeit deaktiviert wird, dass Freunde den Standort angeben können.

Friendticker verweist in der Datenschutzerklärung darauf, dass personenbezogene Daten erhoben, genutzt und verarbeitet werden. Dabei wird die Standortinformation als personenbezogenes Datum klassifiziert:

> «Servtag erhebt personenbezogene Daten auf verschiedene Arten bei der Nutzung von friendticker. (…)
>
> c) Wenn der Nutzer die automatisierte Lokalisierungsfunktion der App verwendet, werden die hierfür + erforderlichen Standortdaten ermittelt und für den Zeitraum der Verbindung gespeichert. Verwendet der Nutzer die manuelle Check-in Funktion von friendticker oder erstellt er Locations

[109] http://www.facebook.com/policy.php

> wird der Benutzernamen im Zusammenhang mit dem jeweiligen Ort gespeichert.»[110]

Die erhobenen personenbezogenen Daten werden nach Auskunft von Friendticker zur Erfüllung der Leistungen aus dem abgeschlossenen Vertrag gegenüber dem Mitglied genutzt und verarbeitet. Dabei wird klargestellt, dass der Betreiber des sozialen Netzes, die Servtag GmbH, berechtigt ist, diejenigen personenbezogenen Daten des Nutzers an Dritte weiterzugeben, die die Daten benötigen, um von Servtag gegenüber dem Mitglied erbrachte Leistungen abzurechnen. Ob und inwieweit die Standortinformationen für ortsbasierte Werbung genutzt werden, ist der Datenschutzerklärung nicht zu entnehmen.

Die Mitglieder von Friendticker können ihre unentgeltliche Mitgliedschaft jederzeit ohne Angabe von Gründen schriftlich oder per E-Mail beenden. Mit erfolgter Kündigung werden das Nutzerkonto und die Inhalte des Nutzers den Angaben des Anbieters zufolge gelöscht. Der Betreiber Servtag behält sich dabei allerdings das Recht vor, in Friendticker eingestellte Inhalte nicht zu löschen, sondern lediglich den Nutzernamen zu entfernen.

Google+ verweist in den Datenschutzbestimungen zunächst auf die Erfassung von Standortdaten:

> «Wenn Sie Google+ auf Ihrem Mobiltelefon verwenden, erfasst Google Ihren Standort, um entsprechende Dienste anbieten zu können, z.B. die Anzeige von Beiträgen von Nutzern in der Nähe, wie bei Ihrer Anmeldung bei der mobilen Version von Google+ beschrieben. Wenn Sie über Ihr Mobilgerät Inhalte auf Google+ posten, können Sie die Standorterfassung deaktivieren und Ihren Standort für jeden Beitrag einzeln anzeigen lassen oder den Standort aus allen Beiträgen entfernen. Wenn Sie nicht über ein Mobilgerät posten, können Sie Ihren Standort für jeden Beitrag einzeln hinzufügen.
>
> Beiträge, die Ihren Standort enthalten, sind für Nutzer sichtbar, die Google+ Beiträge ‹in der Nähe› des Standorts suchen, an dem Sie Ihren Beitrag gepostet haben. Diese Beiträge sind nur für Nutzer sichtbar, mit denen diese Inhalte geteilt wurden.»

[110] http://de.friendticker.com/home_page/show_agb. Das Pluszeichen steht im Original mitten im Satz und ist möglicherweise Ergebnis einer vorgenommenen Löschung

Im Hinblick auf die Verwendung der Daten wird zudem auf die Google-Datenschutzbestimmungen verwiesen. Hier sind dann die folgenden Passagen zu finden:

> «Standortbezogene Daten – Google bietet standortbezogene Services wie Google Maps oder Latitude an. Wenn Sie diese Services nutzen, erhält Google möglicherweise Informationen zu Ihrem tatsächlichen Standort (beispielsweise von einem Mobilgerät übermittelte GPS-Signale) oder Informationen, über die Ihr ungefährer Standort ermittelt werden kann (z.B. die Zellen-ID). (…)
>
> Darüber hinaus verwenden wir die gesammelten Daten zu folgenden Zwecken:
>
> Bereitstellung, Aufrechterhaltung, Schutz und Verbesserung unserer Services, einschliesslich der Werbeprogramme und der Entwicklung neuer Services. (…)
>
> Google verarbeitet personenbezogene Daten auf seinen Servern in den USA und in anderen Ländern. In manchen Fällen werden personenbezogene Daten ausserhalb Ihres Landes verarbeitet.»

Im Fazit kann festgehalten werden, dass die Anbieter sozialer Netze sich in der Regel pauschal ein Nutzungs- und Weitergaberecht im Hinblick auf die standortbezogenen Daten einholen und in der Regel keine Möglichkeiten bieten, dies zu beschränken oder dem zu widersprechen. Die Erklärungen sind zudem schwer nachvollziehbar, da (immer wieder) Verweise auf andere, weiterführende Seiten angegeben werden und die Regelungen exemplarisch formuliert bzw. mit Ausnahmen ausgestattet sind.

Digitale Hinterlassenschaft

Ein besonderes Problem zeigt sich bei Tod eines Mitglieds von sozialen Netzen. Das Datenschutzgesetz schützt Persönlichkeits- und Grundrechte von lebenden Personen. Digitale Daten gehen entsprechend in den normalen Nachlass einer verstorbenen Person ein, wenn sie auf Datenträgern abgespeichert sind, die dem Verstorbenen gehörten. Sind die Daten nun aber auf Datenträgern von Dritten gespeichert, wie den Servern von Dienstleistungsanbietern im Internet, so erlischt der Auftrag (Zenger 2010). Es ist jedoch möglich, zu Lebzeiten mit dem Provider Extra-Regelungen abzuschliessen – sei das

für Zugriffe auf Material, für den Verbleib der Inhalte als Vermächtnis oder auch deren Löschung. Zur Regelung des digitalen Nachlasses gibt es zudem immer mehr Datendienste wie die Site www.mywebwill.de oder www.deathswitch.com. Auf diesen Seiten kann jeder schon zu Lebzeiten entscheiden, was nach seinem Tod passieren soll: auf Facebook ein letztes Update schreiben oder per Google-Mail noch eine Nachricht an Freunde verschicken. Auch kann eine E-Mail verfasst werden, die zum Beispiel Passwörter oder wichtige Dateien enthält. Wenn sich die Nutzer nicht in bestimmten Zeiträumen auf der Webseite einloggen und auch nach mehreren Erinnerungen nicht reagieren, wird die E-Mail automatisch versendet. Eine Tradition der digitalen Nachbearbeitung eines Todesfalls im Internet hat sich insgesamt bislang noch nicht entwickelt. Es gibt kaum Hilfestellung für die Hinterbliebenen, die meist nicht wissen, was sie mit ihrem digitalen Erbe anfangen sollten – falls sie überhaupt wissen, dass es existiert und worin es besteht.

Finanzierung der sozialen Netze

Eine der zentralen Herausforderungen für die Gründer und Betreiber von sozialen Netzen (mit Ortsbezug) ist die Sicherstellung der wirtschaftlichen Existenz. Die Finanzierungsmodelle von sozialen Netzen basieren bislang im Wesentlichen auf verschiedenen Formen von Werbung und Sponsoring sowie (seltener) auf Mitgliedsbeiträgen. Die Geschäfts- und Finanzierungsmodelle unterliegen einer nach wie vor hohen Dynamik und sind in ihrer Grundstruktur und strategischen Ausrichtung nicht immer transparent. Einige der Unternehmen beziehen Wagniskapital (z.B. Foursquare) und befinden sich in ersten Finanzierungsrunden (z.B. Friendticker).

Wirtschaftlichen Erfolg erzielen die sozialen Netze, indem sie aufgrund ihrer Popularität zunehmend Werbetreibende anziehen. Mehr als 80 der grössten 100 Unternehmen der Vereinigten Staaten werben inzwischen auf Facebook; in Grossbritannien sei die Quote mit 40 der Top-50-Unternehmen ähnlich hoch, so der Unternehmensvertreter Chandlee von Facebook (Schmidt, 2009).

Die USA spielen bei Werbung in sozialen Netzen noch immer die Vorreiterrolle. Rund 1,68 Milliarden US-Dollar sollen 2010 in den USA in Werbung in sozialen Netzen geflossen sein, so eine Mitte 2010 veröffentlichte Studie von eMarketer. Im Vergleich zum Vorjahr entspricht das einer Zunahme von 20% (Emarketer, 2010).

Im Folgenden werden die Finanzierungsmodelle der sozialen Netze Facebook und Twitter exemplarisch vorgestellt.

Das weltweit grösste Netzwerk Facebook hat den Angaben des Gründers und Vorstandsvorsitzenden Mark Zuckerberg zufolge rund fünf Jahre nach seiner Gründung und 700 Millionen Dollar Investition im zweiten Quartal 2009 erstmals einen positiven Cash-Flow erreicht. In den ersten neun Monaten 2010 hat Facebook – den Unterlagen der Investmentbank Goldman Sachs zufolge – einen Umsatz von 1,2 Milliarden Euro und einen Netto-Gewinn in Höhe von 355 Millionen US-Dollar erzielt, berichtet die Nachrichtenagentur Reuters. Die Umsatzrendite liegt damit bei rund 30%. Hochgerechnet auf das Gesamtjahr könnte sich der Umsatz von Facebook im Jahr 2010 damit im Vergleich zum Vorjahr nahezu verdoppelt haben. 2009 hatte das Unternehmen 770 Millionen Dollar Umsatz und 200 Millionen Dollar Gewinn erzielt (o.V., 2011b). Die bislang noch ausserbörslich gehandelten Anteile von Facebook sind begehrt: zu den Investoren zählen beispielsweise die Investment-Bank Goldman Sachs sowie Digital Sky Technologies (DST) aus Russland. Experten vermuten, dass der Börsengang von Facebook zu einem der grössten in der Geschichte werden könnte.[111]

Für die Finanzierung von Facebook ist Werbung eine der zentralen Säulen. Mit der Werbevermarktung hat Facebook im Jahr 2010 1,86 Milliarden Dollar erlöst (Weigert, 2011). Die Anzahl der Nutzerinnen und Nutzer und die Intensität der Nutzerinteraktion sind in dieser Hinsicht bedeutende Faktoren der Leistungserstellung. Je mehr Mitglieder Facebook hat und je höher die Interaktion auf Facebook ist, desto attraktiver ist das soziale Netz für werbetreibende Unternehmen. Dabei wendet Facebook – wie viele andere soziale Netze – das sogenannte Symbiose-Prinzip an: Während die Teilnahme an der Community, also die Kernleistung von Facebook, kostenlos angeboten wird, sind Nebenleistungen wie Werbeflächen und Data Mining kostenpflichtig. Dabei ist die Kernleistung Mittel zum Zweck, wobei diese ohne die Einnahmen aus der Nebenleistung nicht aufrechterhalten werden kann und umgekehrt die Nebenleistung ohne die Kernleistung gar nicht existieren würde (Kollmann, 2009). Aufgrund dieser gegenseitigen Abhängigkeit von Kern- und Nebenleistung spricht man von Symbiose.

[111] http://www.spiegel.de/wirtschaft/unternehmen/0,1518,749119,00.html

Die ortsspezifischen Profilseiten von Facebook können genau wie personenbezogene Profilseiten am rechten Seitenrand des Profils beworben werden. Bei der Preisgestaltung haben die Werbetreibenden die Möglichkeit, entweder einen Preis pro Klick auf die Anzeige oder einen Preis für 1000 Impressionen zu wählen. Bei beiden Varianten können die Werbetreibenden selbst bestimmen, welches Budget sie ausgeben möchten. Die Werbetreibenden haben die Möglichkeit, zu bestimmen, bei welcher Zielgruppe die Werbung eingeblendet wird. So können sie beispielsweise festlegen, dass Anzeigen nur bei Männern zwischen 18 und 35 Jahren, die aus einem bestimmten Land kommen, erscheinen. Zudem lässt sich die Zielgruppe nach den Parametern Schulabschluss, Arbeitsplatz, oder auch Beziehungsstatus einschränken.

Neben der Werbevermarktung sind die *Credits* als webweite eigene virtuelle Währung von Facebook ein zweites wichtiges wirtschaftliches Standbein für die Finanzierung. Seit November 2008 treibt Facebook sein Credits-Programm langsam, aber zielstrebig voran. Statt von den Mitgliedern zu erwarten, dass sie beispielsweise bei jedem Spiel aufs Neue ihr Guthaben per Kreditkarte, PayPal oder auf anderen Wegen aufladen, können diese zentral im Prepaid-Verfahren erworbene Credits für sämtliche Zahlungsvorgänge innerhalb der Plattform verwenden. Von den generierten Umsätzen verbucht Facebook eine Provision für sich: Genau wie in Apples App Store oder im Android-Markt gehen 70% der mit Credits erzielten Umsätze an die App-Anbieter, 30% werden als Provision einbehalten (Weigert, 2011).

Kostentreibender Faktor für Facebook sind die hohen Kosten für das Photo-Hosting. Facebook ist mittlerweile zu einem der grössten Foto-Archive des Web angewachsen – die Möglichkeit, (private) Bilder mit befreundeten Mitgliedern austauschen zu können, gilt als Killerapplikation von Facebook. Den Angaben von allfacebook.de zufolge werden derzeit 6 Milliarden Fotos – und damit oft auch die zugehörigen Ortsinformationen – jeden Monat hochgeladen.[112]

Der Kurznachrichtendienst **Twitter** ist nach wie vor auf der Suche nach einer geeigneten Erlösquelle. Neben dem Ansatz, Werbeflächen zu vermarkten, verdient das Unternehmen Geld, indem die Betreiber den Zugriff auf ihre Datenbank verkaufen. Im November 2010 schloss Twitter einen Vertrag mit dem Social Media-Datenlieferanten Gnip ab. Der sammelt bereits seit 2008 Informa-

[112] http://allfacebook.de/zahlen_fakten/infografik-facebook-photo-nutzung-6-000-000-000-photos-auf-facebook-pro-monat

tionen von YouTube, Facebook und anderen populären Plattformen und verkauft sie dann an Marketing- und andere interessierte Firmen weiter. Nützlich kann dies sein, wenn ein Kundenservice-Unternehmen über Gnip nach Feedback zu von ihm betreuten Produkten sucht oder eine Werbeagentur den Erfolg einer Kampagne in sozialen Netzen auswerten will. Wer beispielsweise über den so genannten «Gardenhose»-Zugang die Hälfte aller getwitterten Botschaften sehen und auswerten will, muss dafür 360 000 Dollar an Gnip zahlen. Mehr Daten als dieses Paket erhalten nur die beiden Twitter-Partner Microsoft und Google, die den Kurznachrichtendienst für ihre Suchmaschinen direkt nutzen und Analysten zufolge mehr zahlen. (Schwan, 2010) Wem für statistische Zwecke 5% aller Tweets der Twitter-Mitglieder ausreichen, der bezahlt nach einem US-Medienbericht 60 000 Dollar im Jahr («Decahose»; Crum 2010).

Im April 2011 hat Twitter eine weitere Vereinbarung mit dem Unternehmen Mediasift (Online-Plattform: DataSift.net) getroffen. Demnach verkauft Mediasift den Zugriff auf grundsätzlich alle verfügbaren Daten: Die Kunden erhalten die Auswertungen nach einer eigenständig formulierten Anfrage, der Preis richtet sich dann nach den jeweiligen Such- bzw. Auswertungskriterien (z.B. Stichwörter, Länder; Biermann, 2011).

Insgesamt zeigt sich, dass die Anbieter sozialer Netze seit geraumer Zeit versuchen, auch unter dem Blickwinkel der Investoren verbesserte Geschäftszahlen zu produzieren. In wiederkehrenden Abständen werden neue Funktionen veröffentlicht und es wird in den Medien spekuliert, inwieweit diese darauf ausgerichtet sind, den Nutzerinnen und Nutzern weitere Daten zu entziehen, die dann an externe Werber und Marketingabteilungen verkauft werden können.

Fest steht, dass Werbeagenturen grosses Interesse daran haben, wo sich welche Individuen bzw. Nutzergruppen häufig aufhalten, um möglichst zielgruppen- und ortsspezifisch Werbung platzieren zu können. So werden den Besuchern bestimmter Orte spezielle Preise angeboten. Stammkunden erhalten Gutscheine oder auch virtuelle Coupons (Rabattmarken). Zudem kann den Mitgliedsunternehmen von sozialen Netzen mit Ortungsfunktion ein weiterer Dienst angeboten werden: Sie erhalten detaillierte Statistiken darüber, welche Netzmitglieder wann wie oft kommen, wer schon länger nicht da war und zu welchen Zeiten die Mitglieder am häufigsten da sind (Barczok, 2011).

6.2 Gesellschaftliche Relevanz sozialer Netze mit Ortungsbezug

Im Folgenden beurteilen wir die im Bereich der sozialen Netze diskutierten Anwendungen von Ortungstechnologien nach ihrer gesellschaftlichen Relevanz und verwenden dabei die in Abschnitt 4.2.1 eingeführten generellen Kriterien. (Zur Erläuterung der Kriterien, die im Folgenden als Zwischentitel eingesetzt sind, vgl. S. 76ff und dort Tabelle 4.)

Dieser Abschnitt wird durch illustrierende Beispiele ergänzt, die durch Kästen vom Text abgehoben sind.

Veränderungspotenzial, Machbarkeit

Die technische und ökonomische Machbarkeit sozialer Medien mit Ortungsbezug ist dadurch belegt, dass weit verbreitete soziale Netze bereits heute Ortung als Dienst integriert haben (z.B. Facebook Places/Orte, Google+) und sich ausserdem neue Plattformen etablieren, die im Kern auf der Verwaltung von Ortsangaben beruhen (z.B. Foursquare, Friendticker).

Veränderungspotenzial, grosse Chancen

Grosse gesellschaftliche *Chancen* erkennen wir vor allem für die heranwachsende Generation, die soziale Netze selbstverständlich und in der Regel für die Bewältigung altersbedingter Entwicklungsaufgaben produktiv nutzt: Jugendliche haben in der Regel ein grosses Interesse daran, sich selbst darzustellen. Interessen und soziales Umfeld repräsentieren die Persönlichkeit, und das wiederum verschafft Anerkennung durch andere Jugendliche. Soziale Netze mit Ortsbezug machen es noch einfacher, Personen mit ähnlichen Interessen zu finden und zu treffen.

Veränderungspotenzial, grosse Risiken

Gesellschaftliche Risiken sehen wir in den extrem dynamischen, nicht immer transparenten Geschäftsmodellen (Motto: «Try it out»), bei denen in der Regel verschiedene Spezialdienstleister eingebunden werden (z.B. Twitter mit Gnip/

Mediasift). Hieraus wird die Nutzung und Weitergabe von personen- oder standortbezogenen Daten für die Mitglieder intransparent, so dass die Teilnahme schwer einschätzbare Auswirkungen haben kann. Hier besteht also wie im Bereich Mobilität das Risiko eines Kontrollverlusts über die eigenen Ortungsdaten und damit eine faktische Aushöhlung des Rechts auf informationelle Selbstbestimmung.

Veränderungspotenzial, Breitenwirkung

Die Breitenwirkung von sozialen Netzen im Internet ist durch die hohen und auch weiterhin steigenden Mitgliederzahlen offensichtlich, wie oben dargestellt. Wie sich die Teilnahme an den sozialen Netzen mit Ortsbezug langfristig entwickeln wird, ist noch offen. Wenn die heute zu beobachtende Entwicklung anhält, also keine Gegenbewegung eintritt, könnte es in wenigen Jahren zum Normalfall werden, dass die Präsenz von Personen im Internet und ihre Präsenz im geographischen Raum gekoppelt sind.

Allein das Hochladen von Fotos mit Geotags (mit dem Potenzial zur nachträglichen Fremdortung) hat eine enorme Breitenwirkung. Auf Facebook werden täglich rund 250 Millionen Fotos hochgeladen und rund 100 Millionen Markierungen – meist von Gesichtern – auf Fotos vorgenommen (Hutter, 2011).

Ambivalenz, Hauptwirkungen

Als ambivalent sehen wir die folgenden (intendierten) Auswirkungen sozialer Netze mit Ortungsbezug:

- Soziale Netze leisten für viele ihrer Mitglieder einen Beitrag zur Verwirklichung eines Ideals: der universellen und unbegrenzten Freiheit der Information und Kommunikation. Diese Mitglieder halten die Preisgabe persönlicher und ortsbezogener Daten sowie deren Verarbeitung durch Dritte deshalb nicht für problematisch (zumindest solange nicht, wie sie nicht persönlich von einer Datenschutzproblematik betroffen sind). Im Kontrast dazu drücken sich im Datenschutzrecht gesellschaftlich verbindliche Normen aus, die zum genannten Ideal im Widerspruch stehen, sich aber ebenfalls aus grundlegenden Freiheitsrechten ableiten. Soziale Netze dürften laut Baeriswyl (2010) gar nicht betrieben werden, wenn die Mitglieder beim

Beitritt nicht durch Zustimmung zu den allgemeinen Geschäftsbedingungen (AGB) praktisch vollständig auf den Schutz ihrer Persönlichkeits- und Datenschutzrechte verzichten würden. In rechtlicher und rechtspolitischer Hinsicht stellt sich die Frage, wie weit dieser «Datenschutzverzicht» sich mit der Vertragsfreiheit (innerhalb der ihr gesetzten Schranken) überhaupt rechtfertigen lässt.

- Sogenannte Flashmobs (in der Regel kurze Menschensammlungen auf öffentlichen oder halböffentlichen Plätzen) lassen sich sehr wirkungsvoll organisieren. Dies bietet Chancen im Hinblick auf die Erhöhung des gesellschaftlichen Handlungsvermögens. Andererseits besteht ein Risiko von Gewaltexzessen.

Ambivalenz, Nebenwirkungen

Eine Nebenwirkung sozialer Netze ist die Tatsache, dass die Profile nicht nur Informationen über das betreffende Mitglied, sondern auch Beziehungsinformationen über die jeweiligen «Freunde» oder andere indirekt betroffene Personen enthalten (Egli, 2011). Beziehungsinformation kann erst recht bei einem Ortsbezug der Daten relevant werden (Wer war gleichzeitig am gleichen Ort?) und geht möglicherweise über die Informationen hinaus, die der Einzelne über sich selbst freiwillig offenbaren will. Eine solch weitreichende Bekanntgabe von Personendaten muss den Geboten der Transparenz und der Einwilligung genügen. Wie bereits an anderer Stelle dargelegt, ist die Um- und Durchsetzung der Datenbearbeitungsgrundsätze in der Praxis oft kaum wirksam möglich (vgl. Abschnitt 3.4).

Als ambivalent erweist sich zuweilen die zunehmende Nutzung der sozialen Netze durch Arbeitgeber. So nutzen die Arbeitgeber soziale Netze oftmals im Bewerbungsprozess, um Informationen über potenzielle Mitarbeiter zu recherchieren. Die Verfügbarkeit von Ortsinformationen erweitert das Spektrum: Freizügige Fotos, aber eben auch die Präsenz zur «falschen» Zeit am «falschen» Ort können schnell zum Ausschlussargument für einen Bewerbungskandidaten werden. Die rechtliche Zulässigkeit des «Screening von Stellenbewerbern» im Netz ist umstritten (Egli, 2011).

Konfliktpotenzial, Freiwilligkeit

In folgenden Bereichen sehen wir Einschränkungen der Freiwilligkeit in der Nutzung sozialer Medien mit Ortsbezug:

- Der zunehmende Einsatz sozialer Medien mit Ortsbezug ist eng verbunden mit der informationsethischen Diskussion, ob die Menschen *nicht mehr frei in ihrer Nutzungsentscheidung* sind. Im privaten Bereich verbleibt – abgesehen von einem möglichen sozialen Druck – grundsätzlich die Möglichkeit, den sozialen Netzen aus dem Weg zu gehen und auf eine Mitgliedschaft zu verzichten. Im beruflichen Zusammenhang wird solche «Abstinenz» aber zunehmend schwierig, weil sich z.B. die Werbung und Kontaktpflege von Unternehmen in immer mehr Branchen in den sozialen Medien abspielt. Hierbei spielt auch die Verfügbarkeit von Ortsinformationen zur betrieblichen Prozessoptimierung und Nachweiserbringung eine Rolle. Problematisch wird dies, wenn in Abhängigkeitsverhältnissen die Freiwilligkeit einer Präsenz in den «Social media» sowie der Preisgabe von Standort- und Bewegungsdaten zur Illusion wird (s.a. Abschnitt 4.1.3).
- Hinzu kommt, dass die zunehmende Verwendung von Bildern in sozialen Netzen dazu führt, dass ortsbezogene Daten oftmals *ohne Kenntnis der betroffenen Person* über die Integration bzw. Weitergabe von Bildern in Netzen verteilt werden. Hierbei erfolgt die Einspeisung der Bilder zwar freiwillig, aber die Weitergabe der mit dem Bild verbundenen Ortsinformation geschieht oftmals aus Unwissenheit nicht bewusst und kann daher nicht als freiwillig bezeichnet werden (vgl. Geotagging, S. 24). In datenschutzrechtlicher Hinsicht ist eine solche Weitergabe zwar regelmässig unzulässig, jedoch führt dies kaum je zu Konsequenzen, weder für die Betreiber der Plattform noch für die Personen, die Fotos und andere persönliche Angaben ihrer Freunde weiteren Freunden zur Verfügung stellen, ohne erstere um Erlaubnis zu fragen.
- Die AGB für die Nutzung und Datenschutzrichtlinien sozialer Netze sind häufig mangelhaft abgestuft: Die Mitglieder haben in aller Regel keine Wahl zwischen verschiedenen Optionen bei den Nutzungsbedingungen und Datenschutzrichtlinien. Sie müssen diesen vollumfänglich zustimmen, wenn sie ein soziales Netz nutzen wollen, oder auf die Nutzung ganz verzichten. Insbesondere bei der Erhebung, Speicherung und Nutzung von ortsbezogenen Daten durch soziale Medien ist mit Blick auf die datenschutz-

rechtlichen Bestimmungen fraglich, ob eine einmal gegebene Einwilligung in die Ortung ausreichend ist.

Konfliktpotenzial, Gerechtigkeit

Fragen der Gerechtigkeit sind in folgenden Bereichen tangiert:

- Die Datenschutzrichtlinien der Anbieter der sozialen Netze sind meist sehr umfangreich und in einer für viele Nutzer unverständlichen Sprache abgefasst. Dies liegt daran, dass entscheidende Teile in einer für den Laien unverständlichen Fachsprache abgefasst oder nur in der englischen Formulierung verbindlich sind. Passagen zur Erfassung, Speicherung und Nutzung von Standortdaten müssen oftmals regelrecht gesucht werden. Nutzergruppen mit geringerer Sprach- oder Fachkompetenz sind also bei der Wahrung ihrer Grundrechte in sozialen Netzen tendenziell benachteiligt bzw. gar nicht in der Lage, eine informierte Einwilligung vorzunehmen.
- Die Voreinstellungen zum Schutz der Privatsphäre sind bei der Eröffnung eines Accounts unter Schutzaspekten nicht immer ausreichend. In vielen sozialen Netzen herrscht trotz kritischer Stimmen aus dem Datenschutz immer noch das Opt-out-Verfahren vor, nicht aber die ausdrückliche Einwilligung (Opt-in) der Mitglieder in bestimmte Dienste und in die Verarbeitung personenbezogener Daten zu definierten Zwecken. Fragen der sozialen Gerechtigkeit sind hier insofern tangiert, als nicht alle Mitglieder der sozialen Netze über ausreichende Kompetenzen im Umgang mit Verfahren der Änderung von Standardeinstellungen verfügen.[113] Die automatische Aktivierung von Werbung und Datenfreigaben – z.B. im Hinblick auf die Erfassung von Ortsdaten – in sozialen Netzen könnte Nutzergruppen mit geringer Medienkompetenz in der Wahrung ihrer Persönlichkeitsrechte benachteiligen.

[113] Der schweizerische Bundesrat hat in seinem Bericht über die Rechtslage hinsichtlich sozialer Medien in Reaktion auf das so genannte Postulat Amherd festgehalten, dass die Nutzer mit dem Versuch, die unerwünschte Verwendung ihrer Daten zu verhindern, oft überfordert sind (http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113912).

Nutzungsbedingungen sozialer Netze – massgebliche Sprache

Foursquare bietet seine Nutzungsbedingungen teilübersetzt an, weite Passagen existieren nur in englischer Sprache. Oftmals ist zudem – auch bei übersetzten Nutzungsbedingungen – die englische Sprachversion bindend. Bei Foursquare heisst es beispielsweise:

«Massgebliche Sprache: Wenn foursquare eine Übersetzung der englischen Sprachversion dieser Nutzungsbedingungen in eine andere Sprache bereitstellt, dann willigst Du ein, dass die übersetzte Version lediglich zu Deiner Information zur Verfügung gestellt wird und dass die englische Sprachversion der Nutzungsbedingungen für Deine vertragliche Beziehung zu foursquare massgeblich ist. Falls zwischen der englischen Sprachversion und der übersetzten Version der Nutzungsbedingungen ein Konflikt bestehen sollte, dann ist ausschliesslich die englische Sprachversion bindend.»[114]

Facebook Places/Orte und Google Latitude zählen im Zusammenhang mit der Einwilligung insofern zu positiven Beispielen, als sie die erforderliche Einwilligung zur Erhebung, Speicherung und Nutzung der ortsbezogenen Daten nicht nur einmalig, sondern regelmässig wiederkehrend einholen.

Klärungsbedarf

Aufgrund der oftmals internationalen Organisation von sozialen Netzen sind internationale Datenschutzregelungen erforderlich. Wie in Abschnitt 3.7 beschrieben, sind sowohl auf der Ebene der Europäischen Union als auch im Europarat Bestrebungen zur Verbesserungen des Datenschutzes im Gange. Angesichts des «weiten Arms» des schweizerischen Datenschutzrechts (siehe Abschnitt 3.5.6) lohnt sich indes auch bereits eine Verbesserung des nationalen Datenschutzes. Zudem ist wichtig, dass nicht nur neue Normen geschaffen werden; entscheidend ist vielmehr ein starkes Augenmerk auf die tatsächliche Rechtsdurchsetzung.

[114] https://de.foursquare.com/legal/terms

Mangelnde Resilienz

Im Bereich der Cyberkriminalität erleben die sog. Phishing-Attacken auf soziale Netze einen regelrechten Boom. Angriffe auf soziale Netze waren im zweiten Halbjahr 2010 für 84,5% aller Zugriffe auf Phishing-Seiten verantwortlich (Microsoft, 2011). Dabei versuchen Betrüger, über gefälschte Webseiten an die Zugangsdaten für soziale Netze heranzukommen. Über Links in einer E-Mail gelangen die Nutzerinnen auf eine Seite, die jener des sozialen Netzwerks täuschend ähnlich sieht. Versuchen sie sich dort einzuloggen, können die Betrüger Nutzername und Passwort «abfischen» und anschliessend Daten einsehen und ändern, Nachrichten verschicken und chatten. Die Freunde bemerken diesen Identitätsdiebstahl nicht und schreiben alle Änderungen und Nachrichten der betroffenen Person zu. Neuerdings sind die mobilen Zugänge zu den sozialen Netzen besonders gefährdet (Microsoft, 2011).

Auf einen organisierten Identitätsdiebstahl durch kriminelle Gruppen oder ausländische Geheimdienste ist die Gesellschaft nicht vorbereitet. Häufig dient das Wissen, welche Orte jemand besucht hat und was er dort getan hat, als Beleg seiner Identität (z.B. beim Sperren von Kreditkarten per Telefon). Diese Möglichkeit der Plausibilisierung einer Identität wird durch ortsbezogene soziale Netze untergraben. Ein erfolgreicher Identitätsdiebstahl kann deshalb wahrscheinlich längere Zeit unbemerkt bleiben und erheblichen Schaden anrichten.

Untersuchungsergebnisse verweisen auf Defizite im Jugendschutz.[115] Ein Grundproblem ist allein schon, dass es keine effektive Möglichkeit der Altherskontrolle in sozialen Netzen gibt. Verfahren zur Ermittlung des tatsächlichen Alters der Mitglieder wie *PostIdent* werden nicht genutzt, weil sie Geld kosten und unbequem sind. Hinzu kommen die im Folgenden erläuterten Problembereiche sexueller Übergriffe, Cybermobbing und Cyberstalking, die grundsätzlich auch für Erwachsene bestehen, für Jugendliche aufgrund ihres oft sorgloseren Umgangs mit privaten Informationen aber besonders bedeutend sind.

- Cyber-Mobbing: Mitglieder von sozialen Netzen können von anderen systematisch attackiert werden. Dies kann beispielsweise durch demonstrativen Ausschluss aus Freundeskreisen oder Verbreitung schwerer Beleidigungen erfolgen. Oft wird das Opfer auch durch Veröffentlichung von verfälschten,

[115] Ebenso weist der Bundesrat in seinem Bericht über die Rechtslage hinsichtlich sozialer Medien in Reaktion auf das «Postulat Amherd» auf Probleme beim Jugendschutz hin. (http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113912)

peinlichen oder offenherzigen Bildern belästigt und schikaniert. Insbesondere nach einer Trennung von Teenager-Paaren kommt es zu Vorfällen dieser Art. Auch der Aufbau von Beziehungen unter falscher Identität ist ein beliebtes Mittel des Cybermobbing. Cybermobbing kann bei jugendlichen Opfern Wut, Trauer, Konzentrationsschwierigkeiten, körperliche Beschwerden bis zu Suizidgedanken auslösen (Pro Juventute, 2010). Es ist vorstellbar, dass Ortungsfunktionen in sozialen Netzen zusätzliche Angriffsflächen für Cybermobbing schaffen.

- Cyberstalking: Cyberstalking ist ein Sammelbegriff für die Verfolgung und Belästigung von Personen über das Internet. Cyberstalker können unechte Profile anlegen, in denen sie sich als eine reelle oder fiktive andere Person ausgeben. So können sie unerkannt andere Personen über das soziale Netz belästigen. Oftmals werden die Einstellungen auf fremden Handys geändert und die Person dann unbemerkt in ihrem Alltagshandeln beobachtet und physisch verfolgt.
- Grooming: Eine Gefahr bei der Nutzung von sozialen Netzen stellen Menschen dar, die sich in krimineller Absicht auf die Suche nach Kindern und Jugendlichen machen, um diese sexuell auszubeuten. Grooming ist eine geplante Tat, die mit dem Aufbau eines Vertrauensverhältnisses beginnt. Der Austausch von Ortungsdaten erleichtert das Treffen des Opfers.

Die Problembereiche Cybermobbing, Cyberstalking und Grooming erfahren durch die Erhebung, Speicherung und Nutzung ortsbezogener Informationen durch die sozialen Netze eine Verschärfung der grundsätzlich auch ohne Ortungsdaten bestehenden Risikosituation.

Für die Kontrolle und Abwehr der genannten Tatbestände im Zusammenhang mit dem Jugendschutz in sozialen Medien existieren bislang keine geeigneten Strukturen und Institutionen. Hier besteht vor allem im Bereich der Aufklärung und Bildungsarbeit politischer Handlungsbedarf.

Aus polizeilicher Sicht sind mit dem zunehmendem Einsatz sozialer Netze mit Ortsbezug zudem die Problembereiche Spionage und Einbruch verbunden. Der Vorwurf der Spionage trifft dann zu, wenn Bewegungsprofile für den Zweck der Spionage von Mitgliedern der sozialen Netze – und im Falle von betrieblichen Mitarbeiter-Handys von Mitarbeitenden – gespeichert und ausgewertet werden. Die Einbruchskriminalität wird durch Hinweise auf (z.B. urlaubsbedingt) leer stehende Wohnungen und Häuser oder auch hohe Wertgegenstände gefördert.

Aus Sicht mancher Akteure soll der Schutz der informationellen Selbstbestimmung grundsätzlich um den speziellen Schutz der «location privacy» erweitert werden. Begründet wird dies damit, dass mit der Verbreitung von sozialen Netzen die Möglichkeiten zunehmen, Ortsinformationen einfach und kostengünstig zu sammeln und zu Bewegungsprofilen auszuwerten. «Es ist dieser Wandel hin zu einem System, in welchem Informationen über Ihren Aufenthaltsort umfassend, unbemerkt und kostengünstig gesammelt werden, der uns beunruhigt.» (Blumberg & Eckersley, 2009; Übers. durch die Autoren). Ist diese Transformation erst einmal schleichend vollzogen, so die Argumentation, lässt sich die Entwicklung nur schwer wieder rückgängig machen.

Kriminalität in sozialen Netzen

Die Präsenz von Pädo-Kriminellen in sozialen Netzen hat signifikant zugenommen. Im Jahr 2009 hat beispielsweise MySpace auf eine Aufforderung des Generalstaatsanwalts des US-Bundesstaates Connecticut hin 90 000 identifizierte Sexualstraftäter aus seinen Mitgliederlisten entfernt und deren Daten an die zuständigen Behörden weitergeleitet. Ursächlich hierfür waren Berichte über Versuche von Männern, über MySpace Kontakte zu Jugendlichen oder Kindern zu knüpfen (Spiegel Online, 2009).[116]

Allein bei der «Beratung+Hilfe 147» von Pro Juventute suchen täglich Kinder und Jugendliche wegen Cybermobbing Rat.

Die Website «PleaseRobMe»[117] berichtete eine Zeitlang der Onlinewelt, wer gerade nicht zuhause war. Die Plattform wollte damit vor den Gefahren des freizügigen Umgangs mit persönlichen Daten warnen. Hierfür wurden die Meldungen aus Foursquare mit den Nachrichten aus Twitter verknüpft. Wer bei beiden Diensten angemeldet war und über Twitter mitteilte, gerade wieder zu Hause angekommen zu sein, hatte seine Wohnadresse damit öffentlich gemacht. Einbrecher müssen – so die Annahme – nur die nächste Mitteilung der Person abwarten, dass sie ihr Zuhause wieder verlassen hat.

[116] http://www.spiegel.de/netzwelt/web/0,1518,605566,00.html
[117] http://www.pleaserobme.com

7 Strukturierung der Auswirkungen

Ortungstechnologien bergen – wie die meisten Technologien – sowohl Chancen als auch Risiken für die Gesellschaft. Die vorausgegangenen Kapitel haben dies durch eine Analyse der heute realisierten und zukünftig zu erwartenden Anwendungen aufgezeigt und dabei die Anwendungsfelder «Mobilität» und «Soziale Netze» vertieft behandelt.

Nachfolgend werden wir die wichtigsten gesellschaftlichen Auswirkungen zusammenstellen und strukturieren, die sich aus den Analysen der vorgängigen Kapitel herauskristallisiert haben. Diese Gesamtschau bildet die Grundlage für die Ableitung von Handlungsbedarf in Kapitel 8.

Dabei ordnen wir die Auswirkungen nach zwei Dimensionen:

1. Auswirkungen auf

   - das Individuum
   - das Zusammenleben in Partnerschaft, Familie, Freundeskreis
   - Organisationen (z.B. Unternehmen)
   - die Gesellschaft insgesamt

2. Einteilung in

   - Chancen
   - ambivalente Auswirkungen
   - Risiken

Die Einteilung der Auswirkungen von Technologien in Chancen (Nutzenpotenziale) und Risiken (Schadenspotenziale) ist offensichtlich nicht wertneutral, sondern setzt bereits einen normativen Rahmen voraus.

Einen normativen Rahmen zu definieren, ist in der Technologiefolgen-Abschätzung stets eine heikle Aufgabe, denn Konflikte um neue Technologien und ihre

Anwendung haben ihre Ursache häufig gerade in normativen Differenzen, also in abweichenden Wertvorstellungen (vgl. Abschnitt 4.1). Es hat sich gezeigt, dass gerade in der hier behandelten Thematik der Ortungstechnologien das Kriterium der *Ambivalenz* (kein Konsens über die Bewertung der Auswirkungen) für einen wesentlichen Teil der Anwendungen erfüllt war (vgl. Abschnitte 5.4 und 6.2).

Es kann nicht die Aufgabe dieser TA-Studie sein, in Fällen gesellschaftlich ambivalenter Auswirkungen die Rolle eines Schiedsrichters einzunehmen. Wir haben uns deshalb entschlossen, uns mit Bewertungen zurückzuhalten und keinen Versuch zu unternehmen, die Ambivalenz aufzulösen. Deshalb gehen wir wie folgt vor:

1. Mögliche Auswirkungen, die in der Gesamttendenz eindeutig positiv gesehen werden, d.h. in der berücksichtigten Fachliteratur bzw. in den Medienberichten nicht in Frage gestellt wurden, klassifizieren wir als Chancen (Beispiel: Verringerung der Zahl von Unfalltoten als Auswirkung verbesserter Ortung im Rettungswesen).
2. Entsprechend klassifizieren wir klar negativ bewertete Auswirkungen als Risiken. Dazu zählen insbesondere alle Auswirkungen, die geltendem Recht zuwiderlaufen, etwa eine erwartete Zunahme krimineller Handlungen oder die erschwerte Durchsetzung geltender Rechtsnormen.
3. *Alle übrigen* Auswirkungen betrachten wir als ambivalent, also nicht eindeutig positiv oder negativ zu bewerten (Beispiel: die verstärkte Kontrolle des öffentlichen Raumes, die in der Literatur kontrovers diskutiert wird, siehe Abschnitt 5.4).

Die zwei genannten Dimensionen sind in Abbildung 10 als Achsen aufgetragen. Jede Ellipse entspricht einer möglichen Auswirkung von Ortungstechnologien (Extrakt aus den vorausgegangenen drei Kapiteln). Die exakte Anordnung der Auswirkungen – insbesondere in der Horizontalen – sollte nicht überinterpretiert werden; sie bildet keine abschliessende Beurteilung, sondern lediglich eine Diskussionsgrundlage.

Abbildung 10: Übersicht über die wichtigsten Auswirkungen von Ortungstechnologien

Die in Abbildung 10 gezeigten Auswirkungen lassen sich zu Clustern gruppieren, die jeweils einen zentralen Aspekt der Veränderung repräsentieren:

1. *Handeln im privaten und beruflichen Alltag:* Jene Auswirkungen, die die Bedingungen für das private und berufliche Alltagshandeln (positiv oder negativ) verändern.
2. *Handeln in der Öffentlichkeit und Wahrnehmung demokratischer Grundrechte:* Alle Auswirkungen der Ortungstechnologien, die das Handeln des Individuums gegenüber der Öffentlichkeit verändern, insbesondere die Wahrnehmung von demokratischen Grundrechten wie freie Meinungsäusserung oder Versammlungsfreiheit.
3. *Missbrauch technischer Möglichkeiten:* Die Nutzung der neuen technischen Möglichkeiten zu Handlungen, die geltendes Recht verletzen.

4. *Wirtschaftsentwicklung:* Die durch die Ortungstechnologien bewirkten Veränderungen wirtschaftlicher Prozesse und Strukturen.
5. *Infrastrukturen:* in der Nutzung und Kritikalität von Infrastrukturen.

Die folgenden Abschnitte diskutieren die Auswirkungen in der Struktur dieser Cluster.

7.1 Handeln im privaten und beruflichen Alltag

Die Entwicklung in Richtung billiger, schneller und auch unauffälliger Ortung wird sich weiter fortsetzen und sich auf das Alltagshandeln auswirken. Neben den Navigationsgeräten, die bereits zum Alltag gehören, werden sich besonders Notrufsysteme und Tracking-Systeme in der alltäglichen Mobilität noch stärker ausbreiten (vgl. Abschnitte 2.4.5 und 5.3). Technisch wird es sich dabei meist um GPS-, Mobilfunk-, WLAN- oder RFID-Ortung oder eine Kombination solcher Technologien handeln.

- Für das Individuum zeichnet sich hier ein grosses, heute erst ansatzweise ausgeschöpftes Nutzenpotenzial für die persönliche Sicherheit ab, etwa für die Rettung bei Unfällen oder die Unterstützung bei akuten Gesundheitsproblemen oder physischer Bedrohung.
- Auch für die Sicherung beweglicher Sachgüter gegen Diebstahl oder missbräuchliche Verwendung sind hier noch wesentliche Innovationen zu erwarten.

Ambivalente Auswirkungen sehen wir in den folgenden Bereichen:

- Überwachung von Schutzbefohlenen (wie Kindern, Schülern, Patienten): Hier können Wert- und Zielkonflikte auftreten, insbesondere die Frage der Abwägung zwischen Fürsorge und Autonomie. Dies ist ein ethisches Dilemma, das sich in jeder Situation neu stellt, in der technische Möglichkeiten es erlauben, anderen auch gegen ihren Willen «Gutes» zu tun: Setzt man die Fürsorge (in diesem Fall die automatische Überwachung zum Zwecke der Sicherheit) absolut, resultiert Paternalismus. Setzt man dagegen die Autonomie des Schutzbefohlenen absolut, resultiert Gleichgültigkeit. Verändern technische Möglichkeiten die bisher eingespielte Praxis im Umgang mit diesem ethischen Dilemma, muss ein neues

Gleichgewicht gefunden werden. Die Situation ist aber insofern komplex, als die neue technische Lösung (in diesem Fall der *Tracker* oder auch der *Geofence*, vgl. S. 35) durchaus auch mehr Autonomie für den Betroffenen bedeuten kann, insofern als sie andere Begrenzungen (Zäune, Mauern, verschlossene Türen) ersetzt.

- Bei der Überwachung von Personen, wenn verschiedene Zwecke verknüpft werden: Eine Überwachung zur Erhöhung der Sicherheit einer Person kann gleichzeitig der Effizienz, der Dokumentation erbrachter Leistungen oder der Entlastung von Verantwortung dienen. Die Vermischung verschiedener Einsatzzwecke kann zu einer für die Betroffenen schwer einzuschätzenden Situation führen. Als Beispiel sei auf die Kontroverse um den Einsatz von RFID-Tags für Schüler an US-amerikanischen und britischen Schulen verwiesen (siehe Abschnitt 2.4.5).

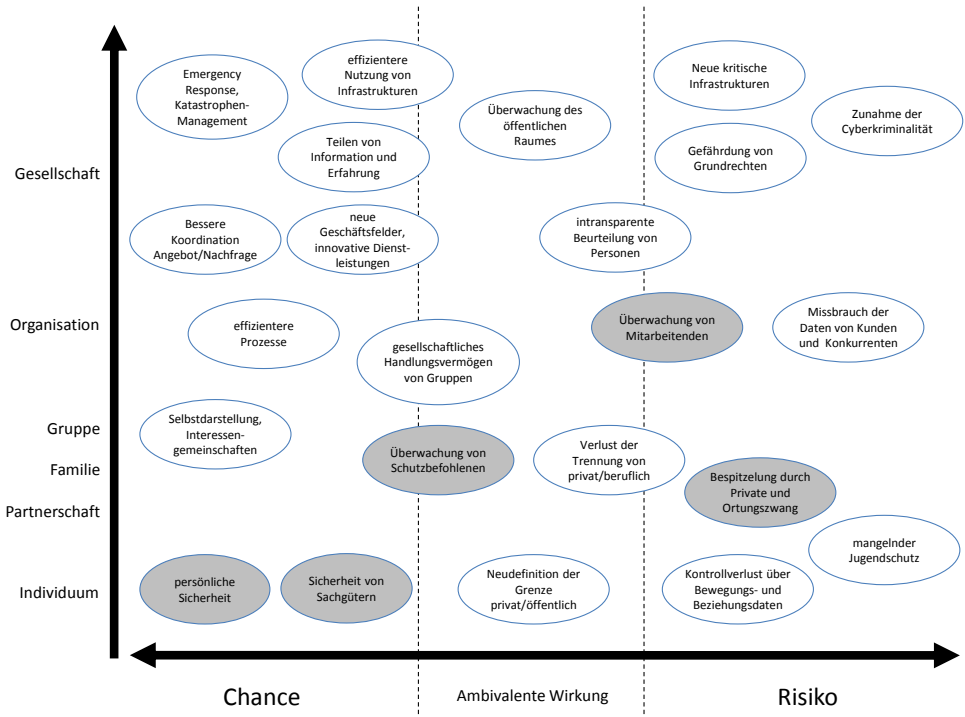


Abbildung 11: Cluster «Handeln im privaten und beruflichen Alltag»

Als Risiko sehen wir zunehmend die Überwachung von Privatpersonen durch Privatpersonen, deren Zunahme zu einem generellen Klima des Misstrauens führen kann. Hier zeichnen sich folgende Problembereiche ab:

- Bespitzelung: Fälle von heimlicher Überwachung aus dem nächsten persönlichen Umfeld (Partner, Familie) werden umso mehr zunehmen, je leichter und kostengünstiger die technische Realisierung wird. Laut Auskunft des EDÖB gibt es viele Anfragen von Personen, die aus dem nächsten Umfeld geortet werden oder befürchten, dies könnte der Fall sein.
- Ortungszwang: Damit bezeichnen wir die formal freiwillig akzeptierte Überwachung von Personen, die aber auf einem sozialen Druck beruht. Wenn es durch die Verfügbarkeit der technischen Mittel zum Normalfall wird, den eigenen Standort anderen offenzulegen, kann ein entsprechender Druck entstehen, dies permanent zuzulassen. Das Ausschalten der Ortung könnte in einer von Ortungstechnologien geprägten Gesellschaft zu einer Handlung werden, für die Partner, Eltern, Kinder oder Freunde, aber auch der Arbeitgeber und Kollegen eine Erklärung erwarten (vgl. Abschnitt 4.1.3).[118]
- Eine besondere Situation ist am Arbeitsplatz gegeben. Die direkte Überwachung von Mitarbeitenden am Arbeitsplatz durch Ortungstechnologien unterliegt engen gesetzlichen Schranken (vgl. Abschnitt 3.3 und S. 118). Neue technische Möglichkeiten schaffen aber Formen der Überwachung, die *indirekt* auf das Verhalten von Mitarbeitenden schliessen lassen, z.B. die Überwachung von Fahrzeugen, Maschinen und Werkzeugen. Hier besteht das Risiko, dass die Durchsetzung der Rechte der Arbeitnehmenden aufgrund der technischen Entwicklung auf zunehmende praktische Schwierigkeiten stossen wird.

[118] Erläuterung zum zweiten Punkt: Die Entwicklung der IKT hat in der Vergangenheit schon oft zu einer «Umkehrung von Defaults» geführt. War früher das Kopieren von Daten die Ausnahme und recht aufwändig, muss man heute das Kopieren mit hohem Aufwand verhindern. Bedurfte es besonderer Anstrengung, Daten aufzubewahren oder zugänglich zu machen, sind sie heute im Normalfall nicht mehr aus dem Internet zu löschen. War es einem Jahrzehnt den «early adopters» vorbehalten, ihre Persönlichkeit im WWW zu offenbaren, muss man sich heute legitimieren, wenn man nicht in einem (oder mehreren) sozialen Netzen präsent ist. Es ist deshalb denkbar, dass auch die Ortung dieser Umkehrung von Defaults unterliegen wird, wenn die sich entwickelnden sozialen Normen nicht reflektiert werden.

7.2 Handeln in der Öffentlichkeit und Wahrnehmung demokratischer Grundrechte

Der verbindende Aspekt dieses Clusters ist die Wechselwirkung zwischen dem Individuum und der Gemeinschaft, die als abgestufte Öffentlichkeit erfahren wird: von der Öffentlichkeit innerhalb (sich formierender) sozialer Gruppen bis hin zur allgemeinen Öffentlichkeit:

- Die Selbstdarstellung in sozialen Netzen ist generell eine Chance, Personen mit ähnlichen Interessen zu finden und Gruppen zu bilden. Gerade darin liegt auch eine Chance für die Ausübung von Grundrechten. Die Ortungsfunktionen könnten das Potenzial zur Bildung von Interessengemeinschaften und anderen sozialen Gruppen noch vergrössern, weil sie das virtuelle Umfeld wieder mit dem geographischen zur Deckung bringen.
- Ortungstechnologien erweitern das gesellschaftliche Handlungsvermögen, indem sie die Kosten für die Organisation politischen Handelns senken und auch spontane Gruppenbildung ermöglichen (Flashmobs). Die Möglichkeit, sich schnell mit vielen Personen an einem bestimmten Ort zu treffen, ist eine neue, beschleunigte Form der Wahrnehmung eines der elementarsten Grundrechte, der Versammlungsfreiheit.
- Das Teilen von Information und Erfahrung wird durch die Ortungstechnologien erleichtert. Die Schwelle wird niedriger, Beobachtungen und Erfahrungen weiterzugeben, die einen geographischen Bezug haben. Von der ausgefallenen Strassenlampe (siehe S. 113) bis hin zur Empfehlung eines Lokals oder der Warnung vor Gefahren kann auf diese Weise jeder seine Beobachtungen der Allgemeinheit zur Verfügung stellen.

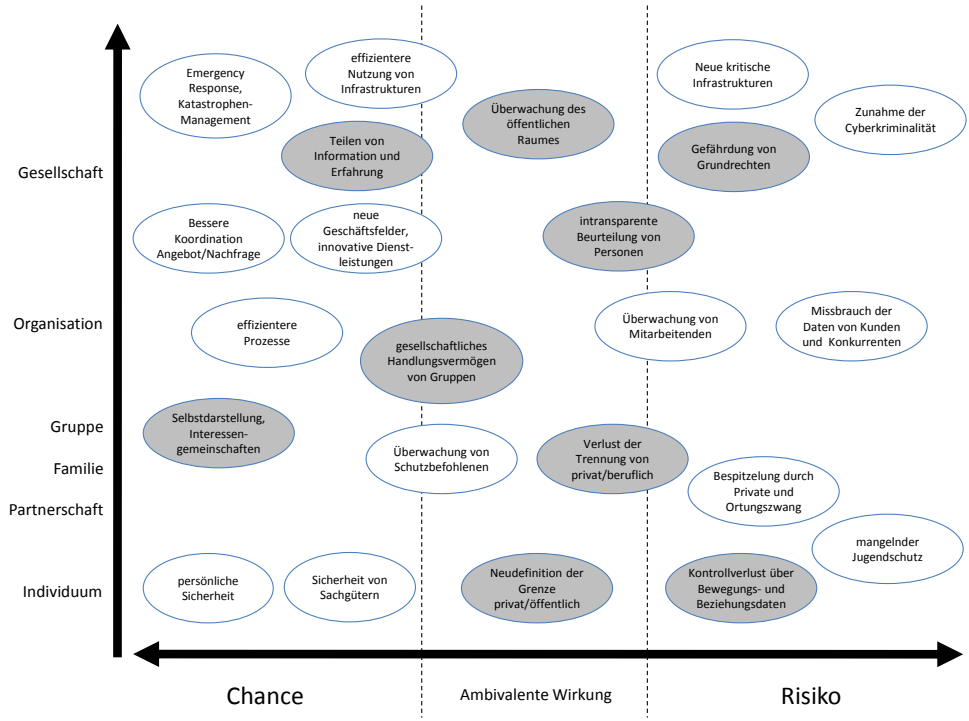


Abbildung 12: Cluster «Handeln in der Öffentlichkeit und Wahrnehmung demokratischer Grundrechte»

Die Nutzung dieser Chancen birgt paradoxerweise auch das Risiko, die Kontrolle über die eigenen Daten zu verlieren und damit eine Gefährdung der Persönlichkeits- und Grundrechte zu riskieren. «Verlust der Kontrolle» bedeutet dabei die Unfähigkeit, den Fluss der ortsbezogenen Daten zu *verfolgen* und zu steuern, zugleich aber auch den Verlust der *Interpretationshoheit* über die eigenen Daten. Dabei sehen wir drei problematische Aspekte:

- In sozialen Netzen werden Ortungsdaten nicht nur für definierte Empfänger offen gelegt, sondern sie bleiben möglicherweise gespeichert und können – durch die Allgemeinen Geschäftsbedingungen gedeckt oder auch illegal – an Dritte weitergegeben werden. Nachträgliche Auswertungen erlauben dann z.B. die Erstellung von Bewegungs- und Persönlichkeitsprofilen.
- Bewegungsdaten sind Beziehungsdaten: An Orten hält man sich häufig gemeinsam mit anderen Personen auf. Es entstehen also nicht nur Be-

wegungsprofile, sondern auch Informationen über (tatsächliche oder vermeintliche) Beziehungen, die möglicherweise mehr aussagen als die Liste von «Freunden» im sozialen Netz, weil sie das tatsächliche Handeln wiedergeben. Diese Daten sind deshalb ähnlich sensibel wie die Verbindungsdaten der Telekommunikationsprovider.

- Verzicht auf Datenschutzrechte: Beim Beitritt zu einem sozialen Netz verzichten die Mitglieder praktisch vollständig auf ihre Datenschutzrechte (Baeriswyl, 2011), was u.a. an der mangelnden Abstufung der jeweiligen Allgemeinen Geschäftsbedingungen und Datenschutzrichtlinien liegt. Hinzu kommt, dass gerade im Zusammenhang mit standortbasierten Diensten oft mehrere Anbieter Kooperationen eingehen, so dass die tatsächliche Nutzung der Daten für das Mitglied noch undurchschaubarer wird (siehe auch 6.1).
- Gefahr des Missbrauchs von staatlicher Seite: Es kann nicht ausgeschlossen werden, dass staatliche Behörden im In- oder Ausland erfolgreich Druck auf Betreiberfirmen ausüben, ortsbezogene Daten herauszugeben, etwa im Rahmen von Ermittlungsverfahren oder von staatlich gestützter Wirtschaftsspionage.

Ambivalente Auswirkungen sehen wir in folgenden Bereichen:

- Durch die heutige Nutzung sozialer Netze wird die Grenze zwischen Privatsphäre und Öffentlichkeit neu definiert. Besonders Jugendliche erkennen darin häufig nur Vorteile; sie schaffen sich ihre «persönlichen Öffentlichkeiten» und glauben die Konsequenzen ihrer Veröffentlichungen unter Kontrolle zu haben. Problematisch erscheint hier vor allem der Widerspruch zwischen der Illusion von Kontrolle über die Daten und dem praktischen Verzicht auf informationelle Selbstbestimmung (der durch die Allgemeinen Geschäftsbedingungen der meisten Plattformen besiegelt wird).
- Eine weitgehende Entgrenzung erfolgt zwischen Privat- und Berufsleben: Die zunehmende Ortbarkeit der Mitarbeitenden könnte eine weitere Flexibilisierung der Arbeitsverhältnisse nach sich ziehen. Immer mehr Privates wird am Arbeitsplatz, immer mehr Berufliches zuhause erledigt, auch vermischen sich private und berufliche Informationen im sozialen Netz immer mehr. Diese Entgrenzung kann bei Spannungen zum Risiko werden: Wenn die «persönliche Öffentlichkeit» mit Arbeitskollegen und Vorgesetzten geteilt wird, können in Konkurrenzsituationen oder Konflikten am Arbeits-

platz die im sozialen Netz zugänglichen Informationen einschliesslich der Bewegungsdaten zu «Munition» werden.

- Intransparente Beurteilung von Personen: Es gibt viele Situationen, in denen Personen beurteilt werden: Bewerbung (vgl. Weichert, 2011), Kreditvergabe, Vermietung, Einschätzung eines Risikos durch eine Versicherung und bei jeder Form von «Kundendiskriminierung». Dabei können Beurteilende eine Vielzahl von im Netz hinterlassenen Spuren auswerten und diese potenziell zum Nachteil der Betroffenen auslegen, ohne dass diese davon erfahren. Man kann in der erhöhten Transparenz der Vorgeschichte von Personen einen Vorteil sehen – oder zumindest kein Problem, da die Beurteilenden ja nur ihr Grundrecht auf Informationsfreiheit wahrnehmen, indem sie öffentlich zugängliche Informationen auswerten. Fragwürdig ist aber die de facto unendliche Aufbewahrungsdauer einmal im Internet veröffentlichter Informationen, welche sich durch den zeitlichen Abstand immer weiter von ihrem Entstehungskontext entfernen. Ihre Interpretation, Gewichtung und nicht zuletzt die Prüfung auf Korrektheit würde deshalb die Mitwirkung der Betroffenen und somit die Transparenz der Entscheidungsprozesse für die Betroffenen erfordern.[119]
- Zunehmende Überwachung des öffentlichen Raumes, insbesondere durch eine Ausweitung der Videoüberwachung, bessere Speichermöglichkeiten von Videodaten und verbesserte Personenidentifikation auf Bildern. Dem erhöhten Sicherheitsempfinden stehen hier Bedenken hinsichtlich Verlagerungseffekten und der Verwandlung des «Miteinanders» von Akteuren in ein «Nebeneinander» gegenüber (vgl. S. 120).

Das Risiko, dass durch allgegenwärtige Ortung langfristig die Ausübung demokratischer Grundrechte gefährdet wird, ist wie folgt begründet:

- «Findet eine Lokalisierung des Aufenthaltsortes der Menschen statt, so gibt es u.U. keine Möglichkeit, sich dieser Form der Überwachung zu entziehen. Dadurch findet unweigerlich eine Verhaltensänderung der Betroffenen statt. Diese werden Orte zu meiden versuchen, mit denen unerwünschte Reaktionen auf Grund der Überwachung zu erwarten sind. Tangiert sind u.U. nicht nur das Grundrecht auf informationelle Selbstbestimmung, sondern

[119] Die lange Aufbewahrungsdauer an sich gilt als Eingriff in das Recht auf informationelle Selbstbestimmung (vgl. auch Abschnitt 3.2).

auch sonstige Grundrechte, die einen Raumbezug haben, z.B. die Versammlungsfreiheit.» (Weichert, 2007, S. 114).

- Ähnlich argumentiert Heesen, wenn sie «Selbstdisziplinierung» als mögliche Auswirkung von Überwachung anführt. Sie hält es allerdings für möglich, dass die allgegenwärtige Beobachtung mit der Möglichkeit, personalisierte Dienste in Anspruch zu nehmen, auch positiv gewendet und als «allgegenwärtige Assistenz» akzeptiert werden könnte. Andererseits könne «die Präsenz eines digitalen Kommunikationspartners zu einem Gefühl der Beobachtung führen (vom Dienstboten zum Spion). Die Fähigkeit der Anwendungen, mein Verhalten aufzuzeichnen und daraus Konsequenzen zu ziehen, können ein Gefühl von Unsicherheit ... erzeugen.» (Heesen, 2008, S. 236).

7.3 Missbrauch der technischen Möglichkeiten

Eindeutig zu beurteilen sind Fälle der Nutzung von Ortungstechnologien, die geltendes Recht verletzen bzw. seine Durchsetzung erschweren. Aus unserer Analyse ergeben sich hier die folgenden Risiken durch Ortungstechnologien:

- Der Jugendschutz wird im Internet nur unzureichend umgesetzt, Altersverifikationen finden in der Regel nicht statt. Kommt der Ortsbezug hinzu, wird es beispielsweise für Pädokriminelle leichter, ihre Opfer zu treffen.
- Der Missbrauch von Ortungstechnologien durch Unternehmen kann geschehen durch Verletzung von Persönlichkeits- und Datenschutzrechten der Kunden oder Mitarbeiterinnen, zur Wirtschaftsspionage oder auch zur Schädigung der Reputation von Konkurrenten.
- Ortungstechnologien schaffen neue Möglichkeiten für Cyberkriminalität: Durch standortbasierte Dienste werden die Folgen von Identitätsdiebstahl (z.B. durch Phishing-Seiten) schwerwiegender. Beispielsweise kann ortsbezogenes Wissen verwendet werden, um Opfer zu täuschen und zu schädigen. Auch für Erpressung, Cyberstalking, Cybermobbing und für Eigentumsdelikte bieten sich zusätzliche Möglichkeiten durch Ortungsdaten.

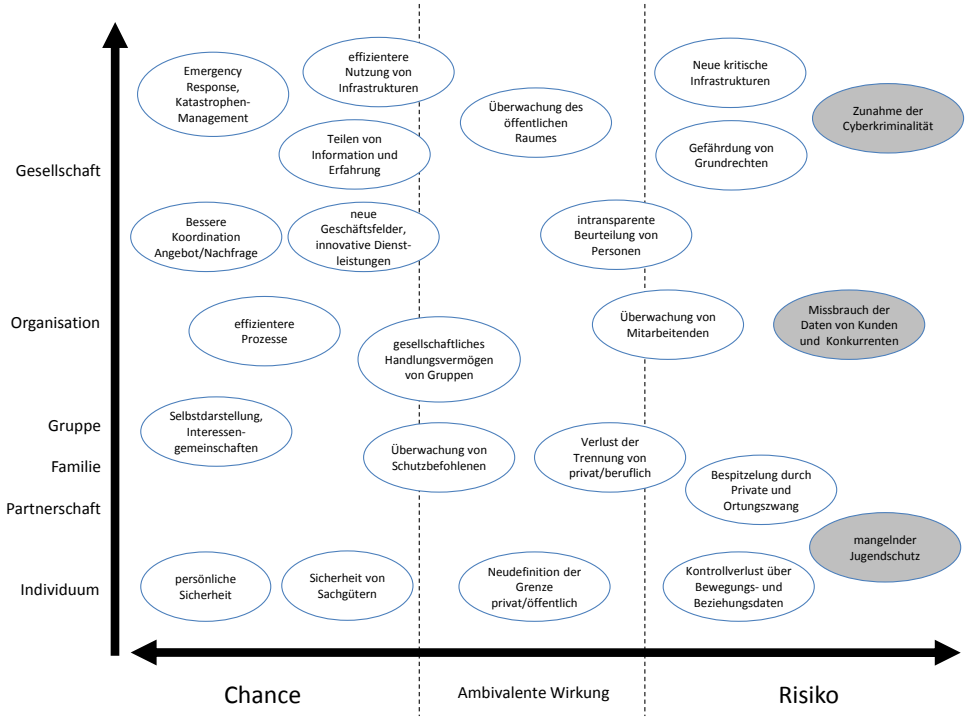


Abbildung 13: Cluster «Missbrauch der technischen Möglichkeiten»

7.4 Wirtschaftsentwicklung

Das Potenzial der Ortungstechnologien für die Wirtschaft ist noch bei weitem nicht ausgeschöpft. Chancen zeigen sich vor allem in folgenden zentralen Bereichen:

- Eine bessere Koordination von Angebot und Nachfrage u.a. durch standortbasierte Dienste, was zu einer Senkung von Transaktionskosten und einer effizienteren Allokation von Ressourcen führen kann (z.B. im privaten und im öffentlichen Verkehr, bei kulturellen Veranstaltungen und jeder Form von lokalen Angeboten).

- Die Erschliessung neuer Geschäftsfelder, insbesondere bei innovativen Dienstleistungen, die Cyberspace und lokale Umgebung koordinieren (z.B. Anwendungen von Augmented Reality).
- Verbesserung der Effizienz von Prozessen in Unternehmen, z.B. in der Logistik, im Management von Fahrzeugflotten, Werkzeugen, Maschinen und Räumlichkeiten. Beispielsweise kann die Einsatzplanung von Aussendienstmitarbeitern effizienter werden, Fahrzeuge können ad hoc disponiert und damit die Reaktionszeiten für Kunden insgesamt verkürzt werden. Arbeitsorte können flexibilisiert und Büroräume eingespart werden. Auch die Werbung wird effizienter, weil Kunden auf der Basis von ortsbezogenen Daten gezielter angesprochen werden können.

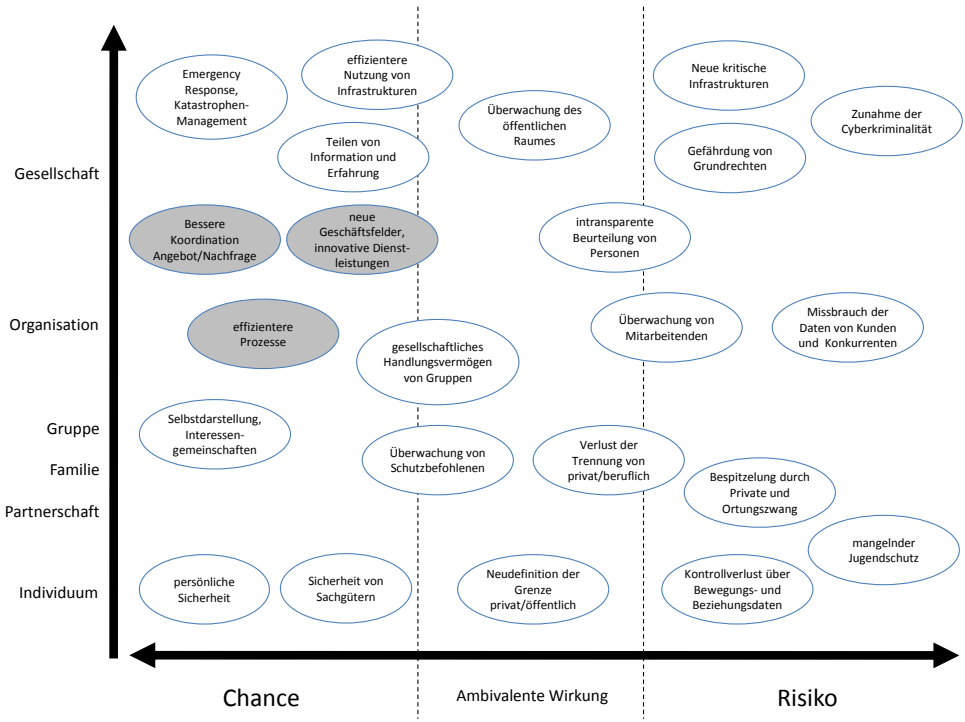


Abbildung 14: Cluster «Wirtschaftsentwicklung»

Ortungstechnologien können insgesamt zu einem Strukturwandel in Richtung einer stärker «dematerialisierten» Dienstleistungsgesellschaft beitragen, indem

sie erstens die Allokation materieller Ressourcen optimieren helfen (u.a. auch durch die leichtere Erhebung verursachungsgerechter Preise, etwa im Verkehr) und zweitens innovative Formen der Wertschöpfung mit weitgehend immateriellen Dienstleistungen ermöglichen. Damit leisten sie auch einen potenziellen Beitrag zu einer nachhaltigen Entwicklung.

Für eine abschliessende Beurteilung ist allerdings zu beachten, dass abhängig von den gegebenen Rahmenbedingungen jeder Zuwachs an Effizienz durch Rebound-Effekte kompensiert werden kann. Das ist z.B. dann der Fall, wenn effizientere Verkehrsflüsse unter dem Strich zu mehr Verkehr führen, weil der Verkehr billig und schnell ist und die Menschen dann weitere Pendlerdistanzen in Kauf nehmen. Zu Rebound-Effekten siehe auch Binswanger (2001) und Hilty et al. (2006).

7.5 Infrastrukturen

Die Gesellschaft ist abhängig von zuverlässigen Infrastrukturen. Hier sind insbesondere die kritischen Infrastrukturen zu nennen, die der Versorgung mit grundlegenden Gütern wie Mobilität, Energie oder Kommunikation dienen. Sie verändern sich mit der Entwicklung der IKT und damit auch der Ortungstechnologien (vgl. 5.3.1). Dabei zeichnen sich die folgenden Chancen und Risiken ab:

- Wesentliche Chancen liegen in der Verbesserung der Infrastrukturen für das Notfall- und Rettungswesen sowie den Katastrophenschutz.
- Die Effizienz der Infrastrukturen kann zunehmen, wenn Ortungstechnologien zur Flexibilisierung, Optimierung und Integration von Infrastrukturnetzen eingesetzt werden.[120]
- Ein Risiko besteht darin, dass die Kommunikationsnetze und Ortungssysteme selbst zu einer kritischen Infrastruktur werden, von der andere kritische Infrastrukturen abhängig sind. Der potenzielle Schaden infolge

[120] Beispiel: In Zukunft könnte ein Elektroauto zugleich als Verkehrsmittel und als mobiler Energiespeicher für das Elektrizitätsnetz disponiert werden; die Aufenthaltsorte geparkter oder noch fahrender «Pufferbatterien auf Rädern» würden in die Disposition der zu verteilenden elektrischen Leistung eingehen.

technischen Versagens, Fehlkonfigurationen oder krimineller Manipulation dieser grundsätzlich verwundbaren Systeme ist hoch.

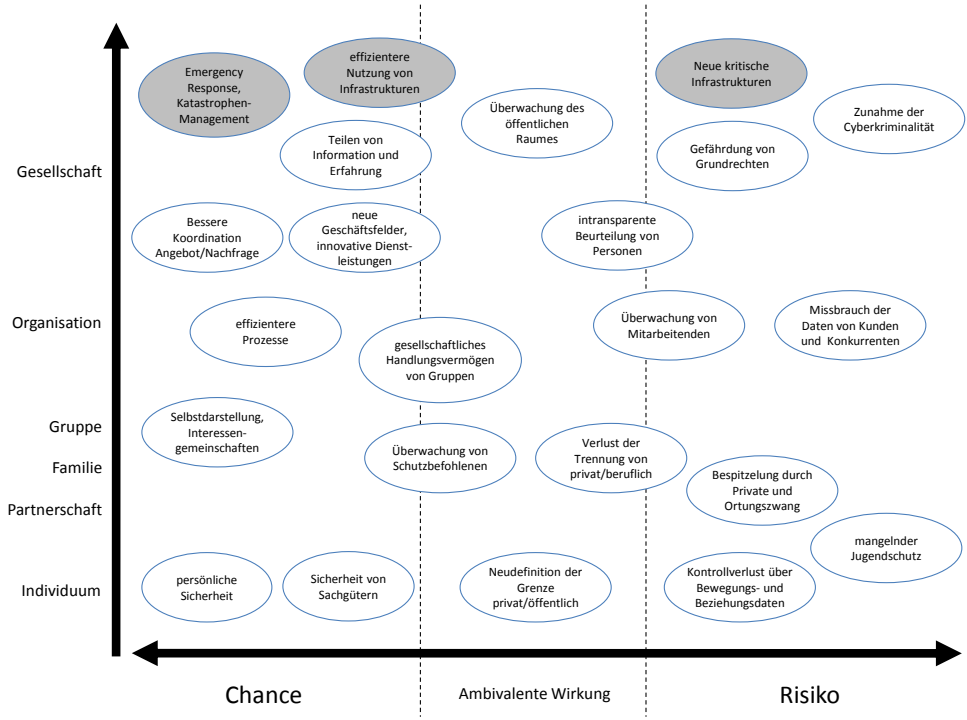


Abbildung 15: Cluster «Infrastrukturen»

8 Handlungsbedarf und Empfehlungen

Wir haben im letzten Kapitel die möglichen positiven und negativen Auswirkungen (Chancen und Risiken) identifiziert, die mit der breiten Anwendung von Ortungstechnologien einher gehen. In diesem Kapitel geht es nun darum, den daraus resultierenden politischen Handlungsbedarf festzustellen. Auch erhebliche Risiken müssen nicht unbedingt auf einen Handlungsbedarf hindeuten, da die gegebenen Rahmenbedingungen (insbesondere der Rechtsrahmen) möglicherweise ausreichend sind, um das Risiko zu begrenzen.

Deshalb beurteilen wir zunächst die *Relevanz* der in Kapitel 7 dargestellten gesellschaftlichen Auswirkungen der Ortungstechnologien (8.1) in Bezug auf politischen Handlungsbedarf.

Darauf aufbauend formulieren wir die Handlungsempfehlungen an die Politik und an weitere Akteure, die zur Maximierung der Chancen und zur Minimierung der Risiken der Ortungstechnologien geboten erscheinen (8.2).

8.1 Relevanzbeurteilung

8.1.1 Vorgehensweise

Wir haben im Abschnitt 4.2 Kriterien eingeführt, um die gesellschaftliche Relevanz von *Anwendungen* der Ortungstechnologien zu beurteilen. Diese Kriterien verwenden wir nun erneut, um die Relevanz der gesellschaftlichen *Auswirkungen* zu beurteilen und jene zu identifizieren, aus denen sich dringender Handlungsbedarf ableitet.[121] Für diese werden anschliessend Handlungsempfehlungen formuliert. Abbildung 16 veranschaulicht die Vorgehensweise.

[121] Die ursprünglich für *Anwendungen* formulierten Kriterien werden sinngemäss uminterpretiert. Daraus ergibt sich kein logisches Problem, da die Anwendungen und ihre direkten Auswirkungen nur die ersten zwei Glieder in einer Kausalkette sind, die sich prinzipiell beliebig fortsetzen lässt: Die Auswirkungen haben ihrerseits Auswirkungen usw.; deshalb ist beispielsweise das Kriterium «Veränderungspotenzial» auch auf Auswirkungen anwendbar.

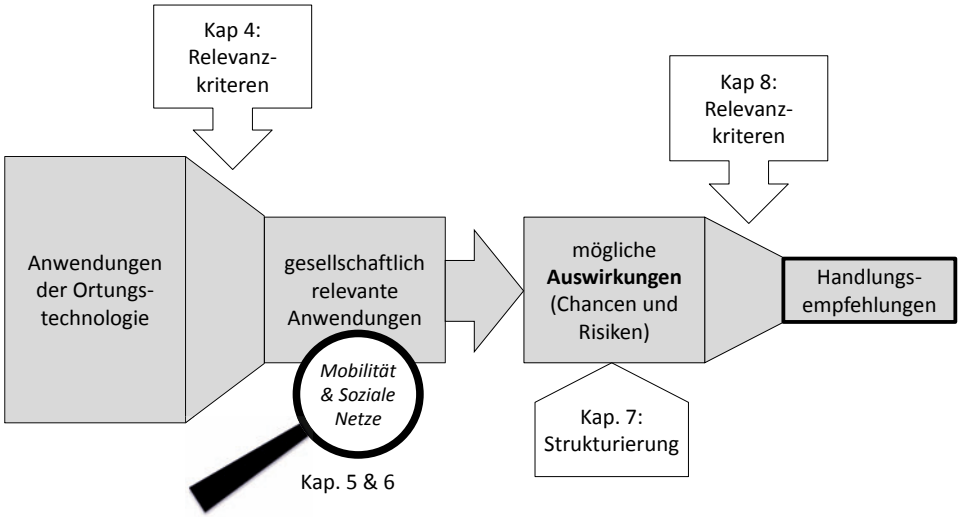


Abbildung 16: Vorgehensweise zur Identifikation des Handlungsbedarfs

Die Hauptkriterien sind: *Veränderungspotenzial, Ambivalenz, Konfliktpotenzial* und *mangelnde Resilienz* (vgl. S. 76). Für ein erstes Screening der Anwendungsgebiete in 4.2 war es ausreichend, diese Kriterien nebeneinander zu stellen, ohne ihre logischen Abhängigkeiten zu berücksichtigen. Zur Ableitung von Handlungsbedarf ist es nun aber erforderlich, sie in einen logischen Zusammenhang zu stellen. Um die Auswirkungen mit dem dringendsten Handlungsbedarf zu identifizieren, werden wir deshalb wie folgt vorgehen:

1. Kriterium *Veränderungspotenzial*: Dieses betrachten wir als notwendige Voraussetzung. Auswirkungen mit einem geringen gesellschaftlichen Veränderungspotenzial werden nicht weiter betrachtet.
2. Unter den Auswirkungen mit hohem Veränderungspotenzial verfolgen wir jene weiter, die mindestens eines der beiden Kriterien *Ambivalenz* und *Konfliktpotenzial* erfüllen. Denn grosse zu erwartende Veränderungen, die in der Bewertung (Chance oder Risiko) ambivalent sind, erfordern offensichtlich eine verstärkte Diskussion und vielleicht weitergehende Massnahmen. Dies gilt umso mehr für Auswirkungen mit hohem Konfliktpotenzial.

3. Für alle Auswirkungen, die nach den Schritten 1 und 2 in die engere Auswahl gelangen, beurteilen wir nun den *Klärungsbedarf* und die *mangelnde Resilienz*. Wenn mindestens eines dieser beiden Kriterien erfüllt ist, besteht Handlungsbedarf. Klärungsbedarf bedeutet hier, dass die Rahmenbedingungen (insbesondere die rechtlichen) unklar sind, unter denen die Gesellschaft mit dem Problem umgeht, um Schaden abzuwenden. Wenn ein ausreichender Rahmen besteht, sind vielleicht keine weiteren Massnahmen notwendig. Mangelnde Resilienz bedeutet, dass die Strukturen und Institutionen fehlen, um im Falle einer eingetretenen Krise wieder in einen akzeptablen Zustand zurückzukehren.

Das Gleiche lautet formal ausgedrückt (in Aussagenlogik):

hoher Handlungsbedarf $\equiv$

hohes Veränderungspotenzial $\wedge$

(hohe Ambivalenz $\vee$ hohes Konfliktpotenzial) $\wedge$

(hoher Klärungsbedarf $\vee$ niedrige Resilienz)

Dabei ist die Schwelle für «hoch» bzw. «niedrig» nur im Sinne einer qualitativen Einschätzung zu verstehen.

8.1.2 Durchführung

Tabelle 6 zeigt die Einschätzung der einzelnen Auswirkungen durch das Projektteam nach den genannten Kriterien (kein ‹+› bedeutet: nicht vorhanden; ‹+›: niedrig; ‹++›: hoch; ‹+++›: sehr hoch). Die Einschätzungen werden im nachfolgenden Text erläutert. Anschliessend werden wir das oben beschriebene Auswahlverfahren anwenden, um jene Auswirkungen «herauszufiltern», bei denen der dringendste Handlungsbedarf besteht.

Tabelle 6: Einschätzung der Auswirkungen der Ortungstechnologien nach dem Kriterienraster

	Veränderungs-potenzial	Ambivalenz	Konflikt-potenzial	Klärungs-bedarf	Mangelnde Resilienz
Handeln im privaten und beruflichen Alltag					
persönliche Sicherheit	++		+	+	
Sicherheit von Sachgütern	+			+	
Überwachung von Schutzbefohlenen	++	++	++	++	
Bespitzelung durch Private und Ortungszwang	+		++		
Überwachung von Mitarbeitenden	++	+	+++	+++	
Öffentliches Handeln und Wahrnehmung demokratischer Grundrechte					
Selbstdarstellung, Interessengemeinschaften	++				
gesellschaftliches Handlungsvermögen von Gruppen	++	+	+		
Kontrollverlust über Bewegungs- und Beziehungsdaten	++		+++		+++
Neudefinition der Grenze privat/öffentlich	++	+	++	++	
Verlust der Trennung privat/beruflich	++	+	++	++	
intransparente Beurteilung von Personen	++	+	+++		++
Teilen von Information und Erfahrung	++				
Überwachung des öffentlichen Raumes	++	++	+++	+	
Gefährdung von Grundrechten	++		+++	+	+++
Missbrauch technischer Möglichkeiten					
mangelnder Jugendschutz	++		++	+++	+
Missbrauch der Daten von Kunden und Konkurrenten	++		++	+	+
Zunahme der Cyberkriminalität	++		++		++
Wirtschaftliche Entwicklung					
bessere Koordination Angebot/Nachfrage	+++		+		
neue Geschäftsfelder, v.a. Dienstleistungen	++		+		
effizientere Prozesse	++	+	+		
Infrastrukturen					
Emergency Response, Katastrophenschutz	+		++		+
effizientere Nutzung von Infrastrukturen	++	++	+		+
neue kritische Infrastrukturen	++		++	+	+++

Handeln im privaten und beruflichen Alltag

Von den fünf Auswirkungen in diesem Cluster haben nur zwei sowohl ein hohes Veränderungs- als auch ein hohes Konfliktpotenzial: *Überwachung von Schutzbefohlenen* und *Überwachung von Mitarbeitenden.* In den anderen Fällen sind entweder die Veränderungen begrenzt (*Sicherheit von Sachgütern*, *Bespitzelung durch Private*[122]) oder es sind keine schweren Konflikte zu erwarten (*persönliche Sicherheit, Gesundheit*).

Der Grund für das Konfliktpotenzial liegt in den bestehenden Abhängigkeitsverhältnissen in den beiden genannten Gebieten. Zusätzlich zum Konfliktpotenzial ist hier ausserdem der Klärungbedarf hoch, weil die geltenden Regelungen auf die neuen technischen Möglichkeiten nur unzureichend anwendbar sind (vgl. die Ausführungen zur Ortung von Minderjährigen, Demenzkranken und Arbeitnehmenden in 5.4, S. 115).

Im Falle der *Überwachung von Schutzbefohlenen* kommt die hohe Ambivalenz hinzu (vgl. die Ausführungen zur Ambivalenz der Überwachung von Personen in Abschnitt 4.1.2).

Handeln in der Öffentlichkeit und Wahrnehmung demokratischer Grundrechte

Dieses Cluster unterscheidet sich vom ersten darin, dass hier nicht Beziehungen unter einander bekannter Personen, sondern das Verhältnis des Einzelnen zu einer grösstenteils anonymen Öffentlichkeit betroffen sind.

In diesem Cluster lassen sich die Auswirkungen schwer nach Veränderungspotenzial differenzieren, da es aufgrund der Breitenwirkung (besonders der sozialen Netze, vgl. Kapitel 6) generell hoch ist.

Nur geringes Konfliktpotenzial oder geringe Ambivalenz haben wir folgenden drei Auswirkungen zugesprochen, die wir deshalb nicht weiterverfolgen: *Selbstdarstellung, Interessengemeinschaften; gesellschaftliches Handlungsvermögen von Gruppen* und *Teilen von Information und Erfahrung.* Die übrigen sind wie folgt beurteilt.

[122] Wir gehen davon aus, dass die Bespitzelung von Privatpersonen durch Privatpersonen (z.B. von Partnern) ein geringeres gesellschaftliches Veränderungspotenzial aufweist als die Überwachung von Personen in einem Abhängigkeitsverhältnis.

Kontrollverlust über Bewegungs- und Beziehungsdaten: Hier sind sowohl die Unfreiwilligkeit als auch die mangelnde Resilienz sehr hoch. Unfreiwilligkeit liegt vor, weil die Daten oft nicht im Bewusstsein der Konsequenzen abgetreten werden. Die Weitergabe von Ortungsdaten ist auch schwer zu vermeiden, wenn man überhaupt Angebote nutzen will, die Ortungstechnologien einsetzen. Hinzu kommt die mangelnde Resilienz, weil die Kontrolle über einmal aufgebaute Datenbestände, die für die Betroffenen nicht transparent sind, die auch nach expliziter Löschung nicht endgültig gelöscht werden,[123] und deren physischer Speicherort möglicherweise nicht einmal bekannt ist, praktisch unmöglich wiederzuerlangen ist und die Gesellschaft über keinerlei Institutionen verfügt, den Einzelnen bei der Widererlangung seiner informationellen Selbstbestimmung wirkungsvoll zu unterstützen.

Neudefinition der Grenze privat/öffentlich und *Verlust der Grenze privat/beruflich*: Auch diese Veränderungen geschehen in vielen Fällen unfreiwillig, denn es kann ein sozialer Druck entstehen, Ortungsdaten offenzulegen. In beiden Fällen besteht ausserdem hoher Klärungsbedarf; im ersten Fall hinsichtlich der AGB entsprechender Angebote im Internet (vgl. Kapitel 6) im zweiten Fall in arbeitsrechtlicher Hinsicht.

Intransparente Beurteilung von Personen: Wenn Personen aufgrund von Standortdaten, Bewegungsdaten oder daraus abgeleiteten Beziehungsprofilen beurteilt werden, ohne dass sie einbezogen sind,[124] ist dies offensichtlich unfreiwillig und birgt deshalb hohes Konfliktpotenzial. Relevant ist dies im Zusammenhang mit der Preisbildung für Güter und Dienstleistungen (auch Versicherungen), aber auch bei Bewerbungen oder Bonitätsprüfungen. Personen und Orte, die als unrentabel oder risikoreich eingestuft werden, können – von den Betroffenen unbemerkt – benachteiligt werden. Wenn jemand die Möglichkeit ausschliessen möchte, dass er auf intransparente Weise auf der Basis von Ortungsdaten beurteilt wird, so müsste er viele Nachteile in Kauf nehmen, falls es überhaupt praktikabel ist. Beispielsweise dürfte er nicht mehr online einkaufen, da die Anbieter ihre Kundschaft aufgrund der Wohn- oder IP-Adresse differenzieren. Weil die Beurteilung auf Grundlage geographischer Informationen wahrscheinlich bestimmte Bevölkerungsgruppen systematisch benachteiligt, steht hier auch die Gerechtigkeit in Frage, was ebenfalls zum

[123] vgl. Cheng (2012) zur Löschung von Fotos auf Facebook.
[124] vgl. Weichert (2011) zum Trend des Scorings von Personen bei Bewerbungen in den USA.

Konfliktpotenzial beiträgt. Aus den gleichen Gründen wie oben (*Kontrollverlust über Bewegungs- und Beziehungsdaten*) ist auch die Resilienz nicht gegeben.

Überwachung des öffentlichen Raumes: Im Gegensatz zu den anderen Auswirkungen in diesem Cluster ist hier aufgrund des Zielkonflikts zwischen Sicherheit und Freiheit eine hohe Ambivalenz gegeben. Weil man überwachten Orten und Verkehrswegen nur begrenzt ausweichen kann, ist hier auch Unfreiwilligkeit und damit Konfliktpotenzial gegeben

Gefährdung demokratischer Grundrechte: Diese kann eintreten, wenn (wie in 7.2 argumentiert) sich Menschen überwacht fühlen. Praktisch ist dies durch Ortung in Echtzeit oder auch durch die Entstehung von Datensammlungen möglich. Sammlungen personenbezogener Daten werden zu einem Machtfaktor, der das Verhalten der Menschen selbst dann beeinflusst, wenn von ihm kein Gebrauch gemacht wird. Die blosse Existenz der Daten kann zu Anpassung und damit zum Verzicht auf die Ausübung demokratischer Grundrechte führen. Dies wäre nicht nur eine sehr weitreichende Veränderung, sie erfolgte auch schleichend und würde erst nachträglich bewusst. Aufgrund des schleichenden Charakters dieser Auswirkung ist die Freiwilligkeit eingeschränkt und daher ein hohes Konfliktpotenzial gegeben. Mangelnde Resilienz liegt vor, weil ein Vertrauensverlust in demokratische Institutionen (wie z.B. das Wahlgeheimnis oder die Versammlungsfreiheit) nur sehr schwer wieder rückgängig zu machen ist.

Missbrauch der technischen Möglichkeiten

Der *Jugendschutz* ist im Bereich von Ortungstechnologien besonders wichtig, weil Jugendliche und Kinder einerseits zu den breitesten Nutzergruppen neuer technischer Entwicklungen zählen, andererseits als potenzielle Opfer besonders gefährdet sind. Aufgrund des sozialen Drucks, «dazu zu gehören», kann die Kontaktaufnahme via soziale Netze (insbesondere mit Ortungsfunktion) nicht als völlig freiwillig betrachtet werden und birgt daher Konfliktpotenzial.

Es ist derzeit unklar, wie altersbezogene Regelungen des Jugendschutzes im Internet umgesetzt werden sollen, da keine wirksame Altersfeststellung gegeben ist. Insbesondere stellt sich die Frage, wie weit Kinder und Jugendliche davor geschützt werden können, sich und andere orten zu lassen und damit

hohe Risiken einzugehen. Den Klärungbedarf in diesem Bereich haben wir deshalb als sehr hoch eingestuft.

Der *Missbrauch der Daten von Kunden oder Konkurrenten* durch Unternehmen ist ein weiteres relevantes Risiko. Für die Betroffenen undurchschaubare Geschäftsmodelle, die auf der Weitergabe von Daten beruhen, verstossen oft gegen geltendes Datenschutzrecht. Datenmissbrauch kann sich aber auch gegen Konkurrenten richten, etwa indem der Ruf ihrer Produkte oder die Reputation der Firma geschädigt werden. In diesem Bereich besteht zwar hohes Konfliktpotenzial, aber wir gehen davon aus, dass klare Verstösse gegen geltendes Recht grundsätzlich auch mit den Mitteln des Zivil- und Strafrechts bekämpft werden können. Deshalb sind die übrigen Kriterien nicht hoch bewertet.

Ortungstechnologien ermöglichen neue Varianten von *Cyberkriminalität*. Im Bereich des Möglichen liegen beispielsweise die Fälschung von GPS-Signalen zum Umleiten von Fahrzeugen oder zur Sabotage von Infrastrukturen, der Handel mit personenbezogenen Ortungsdaten, beispielsweise für Erpressungszwecke oder die gezielte Suche nach Opfern mit einem passenden Profil. Neben dem hohen Konfliktpotenzial ist hier auch ein Mangel an Resilienz gegeben, weil die Gesellschaft auf diese neuen Formen der Cyberkriminalität nicht vorbereitet ist.

Wirtschaftliche Entwicklung

Wesentliche Veränderungen sind im Bereich der *Koordination von Angebot und Nachfrage* zu erwarten, da die Ortungstechnologien eine ortsbezogene Feinplanung und Feinabstimmung ermöglichen. Damit einhergehende Risiken (z.B. Kontrollverlust über Ortungsdaten) sind nicht spezifisch für diesen Punkt und bereits durch andere Punkte abgedeckt.

Neue G*eschäftsfelder, v. a. Dienstleistungen* werden auf Basis der Ortungstechnologien entstehen und in nahezu allen Sektoren *Prozesse effizienter* organisieren. In diesen Punkten gehen wir davon aus, dass die Entwicklung durch den Markt geregelt wird und dass folglich kein besonderer Handlungsbedarf besteht.

Infrastrukturen

Hohes Veränderungspotenzial besteht hier bei der *effizienteren Nutzung von Infrastrukturen* und bei den entstehenden *neuen kritischen Infrastrukturen*.

Die effiziente Nutzung von Infrastrukturen ist ambivalent, weil Rebound-Effekte auftreten können (vgl. Abschnitt 7.5).

Ortungstechnologien tragen aber nicht nur zur Effizienz von Infrastrukturen bei, sie schaffen im Gleichschritt auch neue Abhängigkeiten und können zur Monopolisierung von kritischen Daten und Einrichtungen führen. So entstehen Infrastrukturen, deren Ausfall oder Manipulation schwerwiegende Folgen haben kann. Damit ist eine Unfreiwilligkeit der Nutzung und damit Konfliktpotenzial gegeben. Ein Mangel an Resilienz liegt vor, sobald die Rückkehr in den alten Zustand nicht mehr möglich ist.

8.1.3 Bereiche mit dringendem Handlungsbedarf

Aufgrund der obigen Überlegungen bleiben nach Anwendung der Kriterien von den ursprünglich betrachteten Auswirkungen der Ortungstechnologien die folgenden Bereiche übrig, in denen sich dringender Handlungsbedarf ergibt (die Reihenfolge bedeutet keine Priorisierung):

1) Überwachung von Schutzbefohlenen
2) Überwachung von Mitarbeitenden
3) Kontrollverlust über Bewegungs- und Beziehungsdaten
4) Neudefinition der Grenze privat/öffentlich
5) Verlust der Trennung privat/beruflich
6) Intransparente Beurteilung von Personen
7) Gefährdung von Grundrechten
8) Mangelnder Jugendschutz
9) Zunahme der Cyberkriminalität
10) Neue kritische Infrastrukturen

Im nächsten Abschnitt werden Handungsempfehlungen formuliert, die sich aus dem Handlungsbedarf in diesen Problembereichen ableiten.

8.2 Handlungsempfehlungen

Die schweizerische Rechtsordnung enthält Instrumente und Prozesse, um für die oben beschriebenen Problembereiche in Aushandlungsprozessen angemessene Lösungen zu entwickeln.

Die Verfassung schützt die je nach wirtschaftlicher und persönlicher Perspektive teils divergierenden Interessen an einer ungehinderten oder eingeschränkten Anwendung ortungstechnologischer Innovation im Grundsatz gleichermassen. So kommt der Wirtschaftsfreiheit ein sehr grosser Stellenwert zu. Auch die Informations- und Kommunikationsgrundrechte gebieten Zurückhaltung vor (zu) restriktiven Regelungen innovativer Technologien. Auf der anderen Seite erfordern das Grundrecht auf informationelle Selbstbestimmung, der Persönlichkeitsschutz und der Anspruch auf Schutz vor Diskriminierung vom Staat wirksame Massnahmen zur Gewährung dieser Rechte sowohl gegenüber dem Staat wie auch in privatrechtlichen Verhältnissen, soweit dort aufgrund asymmetrischer Machtverhältnisse ein Schutz notwendig ist. Zu beachten ist ferner, dass bei einer Grundrechtskollision den eher ideellen Grundrechten (wie dem verfassungsrechtlichen Persönlichkeitsschutz) gegenüber den primär wirtschaftlichen Interessen (Wirtschaftsfreiheit, Eigentumsfreiheit) ein Vorrang zukommt (Rhinow & Schefer, 2009, S. 207).

Vor diesem Hintergrund leiten wir aus dem in 8.1 ermittelten Handlungsbedarf eine Reihe von allgemeinen und speziellen Handlungsempfehlungen ab:

- Die allgemeinen Empfehlungen betreffen die Gestaltung der Rahmenbedingungen für die Ortungstechnologien und minimieren die Risiken ihrer Anwendung insgesamt.
- Die speziellen Empfehlungen betreffen einzelne Anwendungsfelder, denen durch besondere Massnahmen Rechnung getragen werden sollte, etwa die Überwachung Demenzkranker oder den Jugendschutz.

Die Handlungsempfehlungen werden in den nachfolgenden Abschnitten ausführlich dargestellt.

8.2.1 Allgemeine Empfehlungen

Wie in unserem Bericht an mehreren Stellen deutlich wird, bringen die Ortungstechnologien sowohl Chancen wie Risiken mit sich. Auch für die Verwirklichung des positiven Potenzials der vielfältigen Anwendungen kann sich im jeweiligen Sachzusammenhang die Notwendigkeit ergeben, den rechtlichen Rahmen den technischen Entwicklungen anzupassen.

Bei unseren nachfolgenden allgemeinen Empfehlungen fokussieren wir indes stärker auf die Risiken und die rechtlichen Möglichkeiten zu ihrer Begrenzung. Sind personenbezogene Ortungsdaten einmal erhoben, können sie zu vielfältigen Zwecken missbraucht werden (siehe auch Abschnitte 4.1.1 und 7.3). Es ist allgemein anerkannt, dass in der Praxis der individuellen Durchsetzung von Persönlichkeits- und Datenschutzrechten hohe Hürden (Prozesskosten, Beweisprobleme, Fehlen abschreckender Sanktion usw.) entgegenstehen. Es kommt hinzu, dass im Datenschutzrecht die behördlichen Sanktionsmöglichkeiten eher bescheiden sind. So fehlt es beispielsweise an der Möglichkeit, gegen Datenschutzverletzer ausreichende Bussen mit individual- und generalpräventiver Wirkung zu verhängen (siehe dazu Abschnitt 3.4). Das kaum reale Risiko für die Datenbearbeiter, im Falle von Datenschutzverletzungen zur Rechenschaft gezogen zu werden, verstärkt das Missbrauchspotenzial.

Eine Verbesserung des Rechtsschutzes bzw. eine Verstärkung der behördlichen Sanktionsmöglichkeiten im schweizerischen Datenschutz löst nicht die Problematik der in vielen Fällen fehlenden Zuständigkeit schweizerischer Behörden bzw. der Nichtanwendbarkeit schweizerischer Rechtsvorschriften in vielen Konstellationen der Bearbeitung von Ortungsdaten. Diese Problematik wird dadurch akut, dass regelmässig Ortungsdaten über Personen in der Schweiz im Ausland bearbeitet werden, wo häufig kein dem schweizerischen Datenschutzrecht gleichwertiger Schutz vor Missbrauch gegeben ist.

Auf diese beiden Probleme (mangelnde Durchsetzungsmöglichkeiten für bestehendes Recht im Inland und fehlende Zuständigkeit bei Datentransfer ins Ausland) sowie die Erarbeitung von Wissensgrundlagen für wirksame Regulierung zielen die folgenden allgemeinen Handlungsempfehlungen, über die Tabelle 7 eine Übersicht gibt.

Tabelle 7: Allgemeine Handlungsempfehlungen

	Empfehlung	**Kommentar**
A1	Einführung effizienter Sanktionsmöglichkeiten gegen den Missbrauch personenbezogener Daten, insbesondere Ortungsdaten	Diese beiden Empfehlungen betreffen die Rechtsdurchsetzung im Bereich des Datenschutzes auch unabhängig von Ortungstechnologien; das Aufkommen der allgegenwärtigen Ortungssysteme erhöht jedoch die Dringlichkeit der empfohlenen Massnahmen.
A2	Massnahmen zur Durchsetzung datenschutzrechtlicher Prinzipien im internationalen Raum	
A3	Aufnahme der Ortungssysteme in das Schweizer Programm zum Schutz Kritischer Infrastrukturen	
A4	Zertifizierung verlässlicher und transparenter Softwareprodukte mit Ortungsfunktionen	
A5	Recht auf «Vergessen» von personenbezogenen Ortungsdaten	Bei dieser Empfehlung steht die technische, organisatorische und rechtliche Machbarkeit in Frage. Dennoch diskutieren wir sie als eine prinzipiell sinnvolle Forderung.
A6	Empirische sozialwissenschaftliche Forschung zum Umgang mit Ortungstechnologien	

A1: Einführung effizienter Sanktionsmöglichkeiten gegen den Missbrauch personenbezogener Daten, insbesondere Ortungsdaten

Aufbauend auf die vorangehenden Überlegungen empfehlen wir dem schweizerischen Gesetzgeber, den individuellen Rechtsschutz und die Rechtsdurchsetzung bei Datenschutzverletzungen allgemein im DSG zu ergänzen. Unsere Vor-

schläge sind dabei nicht spezifisch für Ortungstechnologien; sie sind zwar durch die besonderen Bedrohungen für die Persönlichkeitsrechte durch Ortungstechnologien motiviert, bezwecken aber die Verbesserung des Datenschutzes generell. Im Einzelnen schlagen wir vor:

- Einführung einer Beweislasterleichterung bei Klagen Privater wegen Persönlichkeitsschutzverletzungen durch Private.
- Einführung einer Pönalentschädigung bei Datenschutzverletzung durch Private nach dem Vorbild des Gleichstellungsgesetzes. Im Hinblick auf die Höhe einer solchen Entschädigung und die Voraussetzungen, wann eine solche entrichtet werden muss, besteht weiterer Prüfungsbedarf.
- Auch der individuelle Rechtsschutz gegenüber Datenschutzverletzungen durch Behörden ist zu verstärken. Dazu sind Regelungen im DSG und in den kantonalen Datenschutzgesetzen notwendig.

Ergänzend zur Verbesserung des individuellen Rechtsschutzes befürworten wir eine Verstärkung der behördlichen Durchsetzungsrechte im DSG und auch in den kantonalen Datenschutzerlassen. Im DSG soll der EDÖB die Kompetenz erhalten, Verstösse gegen die Datenbearbeitungsprinzipien Privater, die er im Rahmen seiner Tätigkeit nach Art. 29 DSG feststellt, mit Bussgeldern sanktionieren zu können. Bei der Aufsicht über die Bundesorgane (Art. 27 DSG) sind dem EDÖB Kompetenzen zu verleihen, die über die blosse «Empfehlung» hinausgehen. Die Form der Sanktion bei Verstössen gegen das Datenschutzgesetz durch Bundesorgane bedarf einer näheren Prüfung. Den kantonalen Gesetzgebern wird empfohlen, die behördliche Rechtsdurchsetzung im Anwendungsbereich der kantonalen Datenschutzerlasse zu prüfen.

Als weitere Ergänzung der Rechtsdurchsetzung kommt auch eine Verschärfung der strafrechtlichen Vorschriften im Bereich des Datenschutzrechts und/oder im Strafgesetzbuch in Frage.

Die vorgeschlagenen Verbesserungen des Rechtsschutzes und der Rechtsdurchsetzung auf Bundesebende sind durch das Bundesamt für Justiz und Einbezug der betroffenen Bundesstellen auf ihre Umsetzung und Kohärenz zu prüfen.

A2: Massnahmen zur Durchsetzung datenschutzrechtlicher Prinzipien im internationalen Raum

Wie wir an verschiedenen Stellen unseres Berichts aufzeigen (siehe Abschnitte 3.5.6, 5.4 und Kapitel 6) scheitert in der Rechtsrealität die Durchsetzung des schweizerischen Datenschutzrechts auch daran, dass sowohl die gerichtliche Zuständigkeit in der Schweiz als auch das anwendbare Schweizer Recht durch Allgemeine Geschäftsbedingungen wegbedungen werden. Wie weit eine solche vertragliche Beschneidung von Rechten aufgrund von Vorschriften des Internationalen Zivilprozessrechts bzw. des Internationalen Privatrechts überhaupt zulässig ist, kann nicht generell festgehalten werden, vielmehr kommt es auf die konkreten Umstände des Einzelfalles an. So ist relevant, wer von wo aus welche Personendaten bearbeitet hat und wo ein Schaden ein bzw. eine allfällige Persönlichkeitsverletzung auftritt. Die Komplexität der Rechtslage stellt für viele Betroffene eine Überforderung dar.

Vor diesem Hintergrund empfehlen wir den schweizerischen Behörden, die Nutzerinnen von Ortungstechnologie über die bestehenden Grenzen zulässiger Vereinbarungen in AGB zu informieren (siehe dazu auch Empfehlung S1). Weiter sind die Behörden und ist die Politik aufgerufen, sich in internationalen Gremien für einen wirksamen Schutz vor missbräuchlicher Bearbeitung von Ortungsdaten einzusetzen. Die Schweiz kann entsprechende Initiativen im Rahmen des Europarates einbringen.

In Bezug auf die Situation zwischen der Schweiz und den USA (hier haben viele Anbieter von Ortungstechnologien und sozialen Netzen ihren Sitz) sollte grundsätzlich das so genannte «Safe-Harbor-Abkommen» zwischen der Schweiz und den USA[125] garantieren, dass US-Unternehmen bei der Bearbeitung von Personendaten aus der Schweiz einen gleichwertigen Datenschutz gewähren. Die Wirksamkeit dieses Abkommens wird teilweise kritisch eingeschätzt; aus Kreisen deutscher Datenschutzbeauftragter wird die Kündigung und Neuverhandlung des Abkommens angeregt. Wir empfehlen den zuständigen schweizerischen Behörden, die Wirksamkeit des Safe-Harbor-Abkommens zu evaluieren und ggf. auf eine Verbesserung hinzuwirken. Ein solches Vorgehen müsste indes auch berücksichtigen, dass die grossen Unternehmen wie Facebook und Google in zahlreichen Ländern Rechenzentren betreiben.

[125] http://www.admin.ch/ch/d/sr/i2/0.235.233.6.de.pdf

A3: Aufnahme der Ortungssysteme in das Schweizer Programm zum Schutz Kritischer Infrastrukturen

Jene technischen und organisatorischen Systeme, die explizit dem Zweck der Ortung dienen und in der Schweiz weit verbreitet sind, sollen in das Schweizer Programm zum Schutz Kritischer Infrastrukturen aufgenommen werden. Eine Aufnahme in den Sektor «Informations- und Kommunikationstechnologien» erscheint geboten. Damit wäre auch für die genannten Ortungssysteme ein Rahmenprozess festzulegen, der «als Grundlage zur Sicherstellung der kontinuierlichen Leistungsfähigkeit der Infrastrukturen, respektive der raschen Wiederaufnahme der Kernprozesse im Fall von Störungen dient» (BABS, 2010).

Zu den technischen und organisatorischen Systemen, die explizit dem Zweck der Ortung dienen und in der Schweiz weit verbreitet sind, gehören heute die Satellitenortung durch GPS und die Funkzellenortung in Mobilfunknetzen. Aufgrund der technischen Entwicklung können sich die Technologien und die sich auf sie stützenden Systeme, die für die Gesellschaft den Charakter von kritischen Ortungs-Infrastrukturen aufweisen, im Laufe der Zeit jedoch ändern. Die Empfehlung ist deshalb nicht als einmalige Aufforderung mit Bezug auf bestimmte (heutige) Technologien zu verstehen, sondern als generelle Anforderung an die entsprechenden Organisationen und Schutzprogramme.

Kritische Infrastrukturen «sind Infrastrukturen, deren Störung, Ausfall oder Zerstörung gravierende Auswirkungen auf das Funktionieren der Gesellschaft, der Wirtschaft und des Staates haben.» (BABS, 2010) Der Individualverkehr, Notrettungsdienste und ein zunehmender Anteil der wirtschaftlichen Prozesse sind von Ortungssystemen abhängig und wären bei einem Ausfall oder einer Störung – z.B. durch eine gezielte Überlagerung oder Verfälschung von Satellitensignalen durch Störsender – gravierend betroffen.

Diese Empfehlung richtet sich primär an das Bundesamt für Bevölkerungsschutz (BABS). Wir empfehlen ferner die Zusammenarbeit mit dem Bundesamt für Kommunikation (BAKOM) aufgrund seiner Zuständigkeit für «Berichte über die Sicherheitsinteressen der Schweiz an Rundfunk- und Telekommunikationsinfrastrukturen in ausserordentlichen Lagen» (BABS, 2010) und mit dem Informatiksteuerungsorgan des Bundes (ISB), weil die Bundesverwaltung als Anwender von Ortungssystemen besondere Sicherheitsanforderungen stellt.

A4: Zertifizierung verlässlicher und transparenter Softwareprodukte mit Ortungsfunktionen

Für Anwendungssoftware, insbesondere kleine Anwendungprogramme für mobile Geräte (Apps), die Ortungsfunktionen nutzen, soll eine Möglichkeit zur Zertifizierung geschaffen werden, die sicherstellt, dass die Programme den folgenden Anforderungen genügen:

- Das Programm erzeugt und verarbeitet nur Ortungsdaten, die für die jeweilige Funktion notwendig sind.
- Das Programm überträgt keine Ortungsdaten an Dritte, die diese zur Erbringung der vom Nutzer angeforderten Leistung nicht benötigen.
- Die Ortung ist für die Nutzerin transparent; das Programm ist so gestaltet, dass keine vom Nutzer unbemerkte Ortung erfolgt. Dies kann beispielsweise durch ein Warn-Icon (wie von der «Artikel 29» Gruppe[126] vorgeschlagen) oder durch eine regelmässig wiederholte Statusmeldung realisiert werden.
- Ortungsfunktionen sind durch das Programm standardmässig deaktiviert, müssen also explizit eingeschaltet werden.
- Eine vom Nutzer erteilte Einwilligung in die Weitergabe personenbezogener Ortungsdaten ist in ihrer Wirkung zeitlich begrenzt.
- Ortungsdaten werden automatisch soweit technisch möglich anonymisiert, sofern der Personenbezug für die jeweilige Funktion nicht notwendig ist.
- Alle lokal gespeicherten oder auf einen Server übertragenen Ortungsdaten, die auf die Person der Nutzerin beziehbar sind, können von dieser auf einfache und sichere Weise ohne Zusatzkosten jederzeit vollständig eingesehen und bei Bedarf endgültig gelöscht werden.

Eine solche Zertifizierung wäre besonders nützlich für Apps, die von Behörden oder gemeinnützigen Organisationen angeboten werden und dem Gemeinwohl dienen. Für den Erfolg solcher Apps ist es besonders wichtig, dass die Nutzer darauf vertrauen können, mit ihrer Verwendung kein Risiko einzugehen. Das Zertifikat kann jedoch auch zu einem Werbeargument für kommerzielle Pro-

[126] vgl. Abschnitt 3.7.2, S. 63ff.

dukte werden und einen Wettbewerb um datenschutzgerechte Lösungen anregen.

Eine Zertifizierungsrichtlinie für ortungsrelevante Software (als Produkt oder als Dienstleistung) auf mobilen Geräten wäre von grossem Nutzen. Das DSG sieht die Zertifizierung von Systemen, Verfahren und ihre Organisation vor. Nach Art. 5 Abs. 3 der Zertifizierungsverordnung (VDSZ) erlässt der EDÖB Richtlinien zu datenschutzspezifischen Kriterien im Rahmen der Zertifizierung eines Produkts.

Auch wenn laut Bericht des EDÖB vom Februar 2011 Arbeiten in Richtung einer Zertifizierung von Softwareprodukten in der Schweiz vorerst eingefroren sind (EDÖB, 2011), weisen wir darauf hin, dass aus den oben genannten Gründen dringender Handlungsbedarf besteht. Der EDÖB sieht technische und rechtliche Hindernisse für eine Zertifizierung von Hard- und Software. Er weist auch darauf hin, dass «die geltende Gesetzgebung Lücken und Ungenauigkeiten» aufweise, indem in Artikel 5 der Verordnung über die Datenschutzzertifizierungen (VDSZ) nur die Zertifizierung von Systemen, nicht aber von Dienstleistungen vorgesehen sei (EDÖB, 2011).

Den Ausschluss von Dienstleistungen erachten wir als schwerwiegendes Hindernis, weil Software aus technischer Sicht immer als Produkt *oder* als Dienstleistung angeboten werden kann. Das Angebot von «Software as a Service» (SaS) produziert bei gleichem Funktionsumfang in der Tendenz eher noch mehr Ortungsdaten, da diese u.U. schon zum Zweck der Leistungsabrechnung anfallen. Aus technischer Sicht wäre es deshalb naheliegend, das DSG und die betreffenden Verordnungen (wie die VDSZ) bei der nächsten Revision so zu ändern, dass die Zertifizierung von Dienstleistungen der Zertifizierung von Produkten oder Systemen völlig gleichgestellt wird.

A5: Recht auf «Vergessen» von personenbezogenen Ortungsdaten

Zur Stärkung der Persönlichkeits- und Grundrechte soll jede natürliche Person, über deren Aufenthaltsorte Daten aufgezeichnet werden, das Recht haben, dass diese Daten nach einer gesetzlich festzulegenden oder vertraglich vereinbarten Frist (z.B quartals- oder jahresweise) gelöscht werden. In bestimmten Fällen kann es notwendig sein, bei Ablauf der Frist aktiv die Zustimmung der betroffenen Person zur Löschung der Daten einzuholen (z.B.

für den Fall, dass die Löschung gegen die Interessen der betroffenen Person verstösst).

Ausgenommen sind Daten, die unter gesetzliche Vorschriften zur Aufbewahrung von Daten fallen und aus diesem Grund nicht nach Ablauf der oben erwähnten Frist bzw. erst nach Ablauf der jeweils relevanten gesetzlichen Frist gelöscht werden dürfen. Mit «Löschung» von Daten ist hier die irreversible Vernichtung der Daten gemeint; ein Vorgang, der unter bestimmten Bedingungen die Wiederherstellung der Daten erlaubt, ist keine Löschung im Sinne dieser Empfehlung.

Das heutige Datenschutzrecht sieht zwar in Art. 15 Abs. 1 für Verfahren gegen Private und in Art. 25 Abs. 3 DSG bei Datenschutzverletzungen durch Bundesorgane vor, dass u.a. die Datenvernichtung verlangt werden kann. Zur Geltendmachung des Vernichtungsanspruchs muss die betroffene Person im Zivilprozess nachweisen, dass die beklagte Partei die Personendaten in persönlichkeitsverletzender Weise bearbeitet hat und weiter bearbeitet. Mit dieser heutigen Bestimmung im DSG – vergleichbare Normen finden sich im kantonalen Datenschutzrecht – lässt sich der oben erwähnte Anspruch auf Löschung von Personendaten nicht verwirklichen. Über den gerichtlich – theoretisch – durchsetzbaren Anspruch auf Vernichtung der Daten hinaus bietet das im DSG (und in den kantonalen Datenschutzerlassen) verankerte Verhältnismässigkeitsprinzip eine mögliche Grundlage zur Geltendmachung des Löschens von Daten; nicht mehr erforderliche Daten sind zu löschen. Durch die Verankerung einer ausdrücklichen Regelung im Datenschutzrecht wird auch eine erhöhte Sensibilität sowohl der Datenbearbeiter wie auch der Personen, über die Daten bearbeitet werden, erreicht.

Wir empfehlen deshalb dem schweizerischen Gesetzgeber – je nach Kompetenzbereich Bund bzw. Bund und den Kantonen – die ausdrückliche gesetzliche Verankerung eines Rechts auf Löschung von Personendaten einer eingehenden Prüfung zu unterziehen. Eine solche Regelung muss zwingend vorsehen, dass ein Löschungsanspruch in einem einfachen und raschen Verfahren durchgesetzt werden kann. Zur Wirksamkeit einer entsprechenden gesetzlichen Regelung empfehlen wir weiter, dass gesetzeswidriges Nichtlöschen (bzw. nicht endgültiges Löschen) der Daten (verwaltungs)strafrechtliche Konsequenzen nach sich zieht. Ein Recht auf Vergessen personenbezogener Ortungsdaten muss konzeptionell durchdacht und durch technische Massnahmen ergänzt

werden. Die Bemühungen der EU zur Postulierung eines Grundrechts auf Vergessen sind in diesem Prozess zu beachten. Die Schaffung eines «Grundrechts auf Vergessen» kann (wie von Weber, 2011, vorgeschlagen) indes in einem System konkreter Ansprüche erfolgen, die es auf gesetzlicher Ebene zu konkretisieren gilt.

A6: Empirische sozialwissenschaftliche Forschung zum Umgang mit Ortungstechnologien

Bisher gibt es noch fast keine Forschungsergebnisse zum tatsächlichen Umgang der Nutzer mit Ortungstechnologien im Alltag. Dieses Wissen wäre aber notwendig, um die Chancen und Risiken besser einschätzen und Ansatzpunkte für wirkungsvolle Massnahmen (z.B. Regulierung) finden zu können.

Hier wäre zu prüfen, wie spezifische Ortungstechnologien im Alltag benutzt und wahrgenommen (gelebt) werden. Relevante Forschungsfragen sind: Entsprechen die tatsächlichen Nutzungsformen den vorgesehenen (angenommenen) Nutzungsarten? Inwiefern wird Technologie im Alltag neu definiert, d.h. spezifischen Alltagsbedürfnissen und Praktiken angepasst? Wie sind aus dieser Perspektive die sozialen Konfliktlinien dieser Technologien zu beurteilen? Was müsste konkret aus User-Sicht getan werden (z.B. rechtliche, technische Massnahmen, Aufklärung, etc.), um die Technologien aufzuwerten bzw. um negative Auswirkungen zu vermindern?

Weitere Forschungsfragen betreffen mehr die soziale Komplexität und Dynamik: Wie werden bestimmte Ortungssysteme in der Praxis entwickelt und verhandelt? Welche Akteure, welche Interessen, welche Kompetenzen, welche Austauschbeziehungen und Abhängigkeiten (zum Beispiel zwischen privaten und öffentlichen Akteuren) entstehen?

Diese Empfehlung richtet sich an die Institutionen der Forschungsförderung, insbesondere den Schweizerischen Nationalfonds, aber auch Stiftungen und die Entscheidungsträger für die Festlegung von Forschungsprogrammen.

8.2.2 Spezielle Empfehlungen

In bestimmten Bereichen der Anwendung und Auswirkungen von Ortungstechnologien bieten sich spezielle Massnahmen an, die die gesellschaftlichen Risiken minimieren bzw. die Nutzung der Chancen verbessern können. Tabelle 8 gibt einen Überblick über die 11 speziellen Empfehlungen.

Tabelle 8: Spezielle Handlungsempfehlungen

	Empfehlung	**Kommentar**
S1	Informationsmassnahmen zu Allgemeinen Geschäftsbedingungen und Einwilligungserklärungen beim Beitritt zu sozialen Netzen	
S2	Handlungsanweisungen zur Nutzung von Ortungssystemen am Arbeitsplatz (de lege lata)	Diese beiden Empfehlungen sind komplementär: Die erste bezieht sich auf die Konkretisierung von geltendem Recht auf der Ebene von Weisungen und Merkblättern, die zweite auf eine Verankerung einer klaren Regelung im Arbeitsgesetz.
S3	Klare(re) Regelung der Zulässigkeit der Ortung am Arbeitsplatz (de lege ferenda)	
S4	Einbeziehung des Themas Ortung in Massnahmen zur Förderung der Medienkompetenz bei Kindern und Jugendlichen	
S5	Einführung einer wirksamen Altersfeststellung der Nutzer von Internetdiensten, die personenbezogene Ortungsdaten verarbeiten	

S6	Beitritt der Schweiz zur Europaratskonvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch	Die Ratifizierung der Europaratskonvention könnte im Jahr 2012 oder 2013 erfolgen.
S7	Evaluation der Anwendung von Ortungssystemen zur Überwachung von Demenzkranken	
S8	Nutzung des Vorbildcharakters staatlicher Anwendungen von Ortungstechnologien	Diese beiden Empfehlungen zielen darauf ab, dass der Staat die Chancen der Ortungstechnologien zur Erfüllung seiner Aufgaben nutzt und dabei zugleich deutlich macht, wie eine grundrechtskonforme Anwendung dieser Technologien auszusehen hat.
S9	Datenschutzgerechte Nutzung von Crowdsourcing im Verkehr	
S10	Einheitliche Regelung der Video-Ortung	
S11	Ausdehnung des Prinzips «Robinsonliste» auf digitale Medien, insbesondere standortbezogenes Marketing	

S1: Informationsmassnahmen zu Allgemeinen Geschäftsbedingungen und Einwilligungserklärungen beim Beitritt zu sozialen Netzen

Wer soziale Netzwerke nutzen will, muss regelmässig sehr weitgehende Allgemeine Geschäftsbedingungen (AGB) akzeptieren und willigt dabei in sehr weitreichende Datenbearbeitungsvorgänge ein. Teilweise widersprechen die AGB's der durch die Gerichtspraxis anerkannten Unklarheits- bzw. Ungewöhnlichkeitsregel[127]. Die durch die genannten Regeln bereits in Ansätzen bestehende

[127] Nach der sogenannten Unklarheitsregel sind mehrdeutige Wendungen in vorformulierten Vertragsbedingungen im Zweifel zu Lasten jener Partei auszulegen, welche sie verfasst hat

gerichtliche Inhaltskontrolle allgemeiner Geschäftsbedingungen wurde durch die Revision des Bundesgesetzes über den unlauteren Wettbewerb (UWG) vom 17. Juni 2011 durch die Neuformulierung von Art. 8 UWG verstärkt. Die Bestimmung lautet: «Unlauter handelt, wer allgemeine Geschäftsbedingungen verwendet, die in Treu und Glauben verletzender Weise zum Nachteil der Konsumentinnen und Konsumenten ein erhebliches und ungerechtfertigtes Missverhältnis zwischen den vertraglichen Rechten und Pflichten vorsehen.» Viele der heute gängigen AGBs sehen sehr weitgehende Einwilligungen zur einer umfassenden Datenbearbeitung vor. Die durch Einwilligung übernommenen Vertragsinhalte verstossen teilweise gegen die allgemein anerkannten Schranken der Vertragsfreiheit[128].

Nach Art. 29 DSG kann der EDÖB zudem von sich aus oder auf Meldung Dritter hin Abklärungen treffen, wenn (lit. a): Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler). Werden in AGB's möglicherweise systematisch zwingende Inhaltsnormen des schweizerischen Rechts verletzt, so liegt ein solcher Systemfehler vor. Damit sind die Voraussetzungen einer Intervention durch den EDÖB gegeben. Die Zuständigkeit des EDÖB für eine Intervention auf der Grundlage von Art. 29 DSG kann sich angesichts regelmässig fehlender schweizerischer Niederlassungen der Anbieter sozialer Netze als fraglich erweisen. Der EDÖB hat jedoch nach Art. 28 DSG auch eine Beratungspflicht in Fragen des Datenschutzes gegenüber privaten Personen. Wir stellen fest, dass eine aktualisierte behördliche Information an die Nutzer sozialer Netze über die Einwilligungsproblematik und die Grenzen der Gültigkeit von AGBs notwendig wäre. Eine solche Information muss auch Fragen der Rechtsdurchsetzung beinhalten.

Wir regen weiter an, dass auf Bundesstufe ein eigentliches «AGB-Monitoring» für ortungsintensive Angebote durchgeführt wird. Die Kriterien umfassen:

- Einhaltung des Schweizer Datenschutzrechts
- Allgemeinverständlichkeit

(BGE 124 III 155 Erw. 1b). Die Ungewöhnlichkeitsregel führt dazu, dass aussergewöhnliche Bestimmungen in AGBs, mit der die zustimmende Partei nicht gerechnet hat und auch nicht hat rechnen müssen, unverbindlich sind (BGE 135 III 1, Erw. 2.1; siehe auch bereits BGE 119 II 443, Erw. 1a).

[128] Nichtigkeit von Vertragsbestimmungen, die gegen die öffentliche Ordnung, die guten Sitten und das Recht der Persönlichkeit verstossen, Art. 19/20 OR in Verbindung mit Art. 27 ZGB

- Notwendigkeit der aktiven Einwilligung der georteten Person in die Ortung
- Die Voreinstellungen führen zu einem möglichst geringen Umfang an personenbezogenen (Ortungs-)Daten, die erzeugt und bearbeitet werden.
- Keine zeitlich unbeschränkte Abtretung der Rechte an den von der Nutzerin generierten Daten an den Anbieter.
- Geeignete Bestimmungen über den Umgang mit den gespeicherten Daten nach dem physischen Tod des Nutzers.

Das AGB-Monitoring und die Veröffentlichung der Ergebnisse würden den Nutzerinnen helfen, datenschutzfreundliche Angebote von Angeboten zu unterscheiden, die ihre Persönlichkeitsrechte und Grundrechte möglicherweise gefährden.[129] Es würde die Position eines Nutzers, der seine Rechte durch eine Klage gegen einen Anbieter durchsetzen will, stärken. Das AGB-Monitoring kann sowohl durch eine Bundesstelle – naheliegend wäre der EDÖB – oder auch von einer Konsumentenorganisation im Auftrag des Bundes durchgeführt werden.

S2: Handlungsanweisungen zur Nutzung von Ortungssystemen am Arbeitsplatz (de lege lata)[130]

Der Einsatz von GPS und anderen Ortungssystemen im Arbeitsverhältnis ist in den Schranken der datenschutzrechtlichen Bestimmungen (Art. 328b OR und Bestimmungen des DSG) und – sofern die Arbeitnehmenden überwacht werden – unter Beachtung der Vorschriften des Arbeitsgesetzes (ArG) bzw. der Verordnung 3 zum ArG zulässig. Nicht erlaubt ist die Überwachung, sofern sie einzig der Überwachung des persönlichen Verhaltens dient, aus anderen Zwecken ist sie grundsätzlich erlaubt, soweit Gesundheit und Bewegungsfreiheit nicht beeinträchtigt werden.

Sowohl das DSG wie das ArG bzw. die Verordnung 3 zum ArG enthalten lediglich Grundsätze, die eine Konkretisierung auf der Ebene von Weisungen und Merkblättern erfordern.

[129] Es könnte ausserdem Anbieter dazu motivieren, ihre AGB datenschutzgerecht zu gestalten. Vgl. dazu auch den von Wiedemeier (2010) entwickelten Leitfaden für die datenschutzkonforme Gestaltung von AGB bei der Nutzung von Geodaten.

[130] nach geltendem Recht

Angesichts der bereits heute bestehenden Anwendungen von Ortungssystemen zur Steuerung und Überwachung von Arbeitsprozessen und der damit verbundenen Personenortung ist eine verbesserte behördliche Information über Zulässigkeit und Schranken des Einsatzes von Ortungssystemen in der Arbeitswelt zu erstellen. Eine Möglichkeit wäre, dass der EDÖB das bereits bestehende Dokument «Erläuterungen zur Videoüberwachung am Arbeitsplatz» und den Leitfaden «Bearbeitung von Personendaten im Arbeitsbereich» um ein Kapitel «Ortungsdaten» ergänzt.

Dem Staatssekretariat für Wirtschaft (seco) empfehlen wir ferner, in der Wegleitung zu Verordnung 3 zum Arbeitsgesetz den Kommentar zu Art. 26 um die Dimension der Überwachung durch ortungstechnologische Systeme zu ergänzen.

Sowohl in den Informationen des EDÖB wie des seco sollen die Gebote der Verhältnismässigkeit, Zweckbindung, Transparenz, Datenrichtigkeit und Datensicherheit kontextbezogen konkretisiert werden. Auch klare Aussagen zur Frage der Einwilligung sind notwendig.

Weiter obliegt es den Sozialpartnern, die Frage der Ortungstechnologie zur Überwachung von Arbeitsprozessen und Arbeitnehmenden einerseits je in ihren Verbänden zu thematisieren und andererseits auch zum Gegenstand von Regelungen in Gesamtarbeitsverträgen zu machen.

S3: Klare(re) Regelung der Zulässigkeit der Ortung am Arbeitsplatz (de lege ferenda)[131]

Zwar ist im schweizerischen Arbeitsrecht nach Art. 26 Abs. 1 der Verordnung 3 zum Arbeitsgesetz (Gesundheitsvorsorge ArGV 3, SR 822.113) der Einsatz von Überwachungs- und Kontrollsystemen, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, verboten und sind der Überwachung aus anderen Gründen nach Art. 26 Abs. 2 ArGV 3 enge Grenzen gesetzt. Das Bundesgericht hat jedoch in einem jüngeren Entscheid die Gesetzmässigkeit dieser Bestimmung in Frage gestellt (Bger 6B_536/2009). Aus Gründen der Rechtssicherheit und weil die Ortung von Arbeitnehmenden angesichts des Machtungleichgewichts im Arbeitsvertrag eine besonders intensive Bedrohung der

[131] nach zu schaffendem Recht

Persönlichkeitsrechte bedeutet, empfiehlt sich eine ausdrückliche Regelung der Rahmenbedingungen für die Ortung von Arbeitnehmenden auf Gesetzesstufe. Mit Blick auf den umfassenden Anwendungsbereich ist die künftige Regelung im Arbeitsgesetz (ArG) zu verankern.

Als Orientierung kann dabei auf eine Regelung im geplanten deutschen «Beschäftigtendatenschutzgesetz»[132] (BDatG-Entwurf) zurückgegriffen werden. In Art. 32g BDatG-Entwurf wird die Zulässigkeit der Bearbeitung (erheben, verarbeiten, nutzen) von Beschäftigtendaten durch elektronische Einrichtungen zur Bestimmung eines geographischen Standortes auf die Zwecke «zur Sicherheit des Beschäftigten» und «zur Koordinierung des Einsatzes des Beschäftigten» reduziert. Darüber hinaus ist erforderlich, dass keine überwiegenden schutzwürdigen Interessen der Beschäftigten gegen den Ausschluss der Datenbearbeitung vorliegen. Zudem ist die Erhebung von personenbezogenen Ortungsdaten auf die Arbeitszeit beschränkt. Weiter muss die Arbeitgeberin den Einsatz der Ortungssysteme durch geeignete Massnahmen für die Beschäftigten erkennbar machen und diese über den Umgang der Aufzeichnungen und die vorgenommenen Auswertungen regelmässig informieren. Die geplante deutsche Regelung sieht weiter vor, dass die Daten unverzüglich zu löschen sind, wenn sie zur Erreichung des Zweckes der Speicherung nicht mehr erforderlich sind oder schutzwürdige Interessen der Beschäftigten einer weiteren Speicherung entgegensteht.

Im schweizerischen Recht ist eine in den Grundzügen ähnliche Regelung anzustreben. Auch wenn die meisten Ziele einer solchen Bestimmung bereits dem Datenschutzgesetz immanent sind (Transparenz, Verhältnismässigkeit usw.) so bringt die Verankerung im Arbeitsgesetz mehrere Vorteile. Zum einen können datenschutzrechtliche Grundsätze im spezifischen Kontext des Arbeitsverhältnisses konkretisiert werden und zum anderen wird die Einhaltung der Vorschriften des Arbeitsgesetzes von Amtes wegen kontrolliert und mittels Sanktionsandrohung und Sanktion durchgesetzt.

[132] Bundestag vom 15.12.2010, Drucksache17/4230.

S4: Einbeziehung des Themas Ortung in Massnahmen zur Förderung der Medienkompetenz bei Kindern und Jugendlichen

Die bereits in der Schweiz bestehenden Aktivitäten zur Förderung von Medienkompetenz sollen um das Thema Ortung ergänzt werden. Hierzu zählen beispielsweise:

- Die NetLa-Kampagne[133] des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und des Rates für Persönlichkeitsschutz für die Zielgruppen «S» (5–6 Jahre), «M» (7–10 Jahre) und «L» (11–14 Jahre) sowie für Lehrpersonen und Eltern. Die Kampagne will schon früh für den richtigen Umgang mit persönlichen Daten im Internet sensibilisieren, da Kinder und Jugendliche im Internet oft zu bereitwillig persönliche Daten angeben.
- Die «Geschichten aus dem Internet, die man selbst nicht erleben möchte …»[134] sind Resultat einer Partnerschaft verschiedener Stellen aus Bund und Kantonen. Herausgeber ist das Bundesamt für Kommunikation BAKOM. Mit Comic-Geschichten soll möglichst vielen Menschen in der Schweiz die Gelegenheit gegeben werden, über ihre eigenen Erfahrungen mit dem Internet nachzudenken, diese zu diskutieren und ihr Wissen weiter auszubauen. Das Ziel besteht darin, die Sicherheit und das Vertrauen der Bevölkerung im Umgang mit den IKT zu stärken.
- Die Tipps und Links für Jugendliche sowie die Datenschutzlehrmittel für den Schulunterricht des EDÖB. Neu (27.1.2012) ist das Lehrmittel «Elementare Datensicherheit», das jungen Erwachsenen Wissenswertes und Tipps zum sicheren Umgang mit ihren Daten in den Neuen Medien vermittelt.[135]

Die Aktivitäten zur Förderung von Medienkompetenz bei Kindern und Jugendlichen thematisieren zwar den Umgang mit Datenfreigaben in den verschiedenen Internetdiensten wie Chat oder soziale Netze. Sie verweisen aber bislang nicht auf den sinnvollen Umgang mit Ortungsdaten bzw. bieten in diesem Kontext noch keine Tipps und Erfahrungen an.

[133] NetLa – Eine Kampagne des Eidg. Datenschutz- und Öffentlichkeitsbeauftragten sowie des Rates für Persönlichkeitsschutz. http://www.netla.ch/de
[134] http://www.geschichtenausdeminternet.ch/
[135] http://www.derbeauftragte.ch/

Die Empfehlung richtet sich an alle Initiatoren bzw. Anbieter von Informations- und Kommunikationsmassnahmen zur Förderung von Medienkompetenz von Kindern und Jugendlichen in der Schweiz.

S5: Einführung einer wirksamen Altersfeststellung der Nutzer von Internetdiensten, die personenbezogene Ortungsdaten verarbeiten

Die Anbieter von Internetdiensten, die personenbezogene Ortungsdaten verarbeiten, sollen verpflichtet werden, praktikable technische Mittel zur Altersverifikation der Nutzer einzusetzen. Dabei müssen klare Vorgaben gemacht werden, welche ortsbezogenen Daten – ggf. auch im Zusammenhang mit der Weitergabe von Bildern – Minderjährige überhaupt von sich preisgeben dürfen bzw. in welchen Fällen Einwilligungen durch die Erziehungsberechtigten erforderlich sind. Sinnvollerweise wird dabei eine Altersdifferenzierung vorgenommen (z.B. 12, 14, 16 Jahre), wie sie auch im Bereich Film praktiziert wird.

Internetdienste wie soziale Netze haben aufgrund ihrer Geschäftsmodelle in der Regel ein Interesse an niedrigen Eintrittsschwellen. Die Anmeldung soll unkompliziert sein und schnell gehen, um so viele Menschen wie möglich anzuziehen. Deshalb wird gegenwärtig kein wirksamer Jugendschutz durchgeführt. Kinder und Jugendliche nutzen zwar intensiv Internetdienste, die auch personenbezogene Daten bearbeiten, haben jedoch oft noch nicht das nötige Problembewusstsein, was mit ihren personenbezogenen Ortungsdaten kurz-, mittel- und langfristig gemacht werden kann. Cyberstalking sei hier nur als ein Beispiel genannt, um die Bedeutung von ortsbezogenen Daten im Hinblick auf den Jugendschutz zu unterstreichen.

Die gesetzeskonforme Identifikation per PostIdent-Verfahren ist für viele Verbraucher zu aufwändig, denn für jede Transaktion muss eine autorisierte Stelle – in der Regel die Schweizerische Post – die Identität des Antragstellers beglaubigen. Neben diesem Verfahren praktizieren Dienstanbieter auch eine Reihe «weicher» Methoden wie Webcam-Kontrolle oder Zufaxen des Ausweise, die aber nicht rechtssicher sind.

Eine gesetzliche Regelung zu Altersgrenzen im Internet und insbesondere deren Durchsetzung ist mit zahlreichen praktischen Problemen verbunden, die es sorgfältig zu analysieren gilt. In Deutschland erlitt eine für 2011 geplante Einführung einer gesetzlichen Novellierung des Jugendmedienschutzes und

damit zusammenhängend die Verankerung von Altersgrenzen für die Internetnutzung politisch Schiffbruch; zu viele praktische Fragen waren im entsprechenden Gesetzesentwurf ungelöst und zu stark gewichteten auch Befürchtungen gegenüber staatlicher Internetzensur.[136] Vor diesem Hintergrund empfehlen wir einerseits den zuständigen Bundesbehörden (BJ, BSV, BAKOM), Möglichkeiten einer gesetzlichen Regelung einer Vorprüfung zu unterziehen. Dabei wird zu prüfen sein, ob und inwieweit sich die Rechtslage bezüglich Altersgrenzen für Filme und DVD auf Internetangebote übertragen lässt. Die Empfehlung richtet sich andererseits auch an die Internetdienstanbieter; diese haben Formen der Selbstregulierung zu prüfen.

S6: Beitritt der Schweiz zur Europaratskonvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch

Die Europaratskonvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch soll vor dem Hintergrund des zunehmenden Einsatzes von Ortungssystemen baldmöglich umgesetzt und ratifiziert, die Anpassungen des StGB entsprechend vorgenommen werden. Die Konvention verpflichtet die Mitgliedstaaten unter anderem, das sexuell motivierte Anbahnen von Kontakten mit Unmündigen im Internet – das sogenannte Grooming – unter Strafe zu stellen, wenn der Kontaktaufnahme konkrete Handlungen für ein Treffen folgen. Die Ratifizierung der Konvention würde somit auch darauf reagieren, dass Kinder bei Treffen mit Personen sexuell missbraucht werden, die sie vorher im Internet (z.B. in sozialen Netzen) kennengelernt und möglicherweise geortet haben.

Das durch Ortungssysteme vereinfachte Beobachten und Verfolgen von Personen (z.B. im Zusammenhang mit Cyberstalking) kann dazu beitragen, dass der entscheidende Schritt zum Versuch, von dem es kein Zurück mehr gibt, im Vergleich zu Chats eben doch überschritten wird. Der Einsatz von Ortungssystemen führt dazu, dass die Handlungen nicht mehr im virtuellen Raum bleiben, die Möglichkeit zum Personenbezug und zum realen Aufeinandertreffen

[136] Geplant war eine Ergänzung des Jugendmedienschutz-Staatsvertragsgesetz (JMStV-E2010), das Projekt scheiterte am Widerstand einzelner Bundesländer.

von potenziellem Opfer und Täter gegeben ist. Zu schützende Personen können damit als konkret gefährdet gelten.[137]

Die am 1. Juli 2010 in Kraft getretene Konvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch ist das erste internationale Instrument, das die verschiedenen Formen sexuellen Kindesmissbrauchs umfassend für strafbar erklärt. Das Übereinkommen des Europarates, ETS 201, verlangt in Artikel 23 die Kriminalisierung der Kontaktanbahnung zu Kindern zu sexuellen Zwecken (auch «Grooming» genannt). Die Staatengemeinschaft des Europarates hat mit der Annahme dieses zusätzlichen Tatbestands Neuland betreten, aber eindeutig zum Ausdruck gebracht, dass auch Vorbereitungshandlungen für spätere Sexualdelikte strafwürdig erscheinen. Die Schweiz hat die Konvention am 16. Juni 2010 unterzeichnet, aber bis heute (1.1.2012) noch nicht ratifiziert. In einzelnen Punkten geht die Konvention weiter als das geltende Strafrecht, so dass der Beitritt der Schweiz verschiedene Anpassungen des StGB bedingt. Am 17. August 2011 hat der Bundesrat eine Anpassung des Strafgesetzbuches in die Vernehmlassung geschickt. Die Vernehmlassung dauert bis Ende November 2011. (EJPD, 2011a) Die bundesrätliche Botschaft soll anschliessend dem Parlament noch in der ersten Jahreshälfte 2012 unterbreitet werden; ein Inkrafttreten dürfte möglicherweise noch 2012, ggf. aber auch erst 2013 realistisch erscheinen. Die spezifischen Gefahren, die durch die Möglichkeiten der Kontaktanbahnung durch Ortungsfunktionen im Internet geschaffen werden, erfordern Massnahmen namentlich zum Schutz von Kindern. Mit der Ratifikation der Konvention kann hier ein ausdrückliches Zeichen gesetzt werden, dass die Schweiz den Schutz der Kinder vor sexueller Ausbeutung ernst nimmt.

Die Empfehlung richtet sich an das Parlament, die Europaratskonvention zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch baldmöglichst zu ratifizieren. Wir empfehlen, dass die Verwaltung in der bundes-

[137] Das Bundesgericht äussert sich in einem Entscheid aus dem Jahr 2005 zur Frage der Abgrenzung zwischen Versuch und strafloser Vorbereitungshandlung bei sexuell motiviertem Chatten mit Kindern. Dabei kam es zum Schluss, dass mit dem Chatten der entscheidende Schritt zum Versuch, von dem es kein Zurück mehr gibt, nicht überschritten werde. Die Handlungen blieben beim Chatten im virtuellen Raum und man agiere anonym. Die zu schützende Person als solche werde noch nicht konkret gefährdet. Zudem sei die Beweisbarkeit der Festigung des Tatentschlusses zu einem derart frühen Zeitpunkt ungenügend. Das Verhalten der erwachsenen Person sei erst dann strafbar, wenn der letzte entscheidende Schritt vorgenommen wird, von dem es in der Regel kein Zurück mehr gibt. Vgl. hierzu: BGE 131 IV 105 Erwägung 8.1.

rätlichen Botschaft das Parlament (auch) auf die spezifische Problematik der Ortungstechnologie hinweist.

S7: Evaluation der Anwendung von Ortungssystemen zur Überwachung von Demenzkranken

Der verstärkte Einsatz von Ortungssystemen zur Überwachung von Demenzkranken in Privatwohnungen, Pflegeeinrichtungen und Krankenhäusern soll grundsätzlich durch eine Evaluation der Anwendung unter ethischen, juristischen und gesamtgesellschaftlichen Aspekten begleitet werden. Die Ethik-Charta der «Stiftung für elektronische Hilfsmittel» (vgl. S. 74) bietet Ansatzpunkte für die Evaluation der zunehmenden Personenortung von Menschen mit Demenz. Neben der Evaluation ist es dringend geboten, das Problem der Sicherheit von Demenzkranken und dem damit verbundenen Einsatz von Ortungssystemen öffentlich zu diskutieren, damit nicht nur ein fachlicher, sondern auch ein gesellschaftlicher Konsens entstehen kann, der demenzkranken Personen mit ihrer individuellen Problematik gerecht wird. Dabei gilt es auch zu berücksichtigen: Der Einsatz der Ortungstechnologie kann auch zu einem Freiheitsgewinn führen, da je nach Situation die Ortung desorientierter Menschen als Alternative zu weitergehenden Freiheitsbeschränkungen eine humanere Lösung darstellt.

Heute leben etwa 107 000 Menschen mit Alzheimer oder einer anderen Form von Demenz in der Schweiz. Im Jahr 2030 werden es voraussichtlich doppelt so viele sein und im Jahr 2050 bereits mehr als 300 000 (Schweizerische Alzheimervereinigung, 2010). Bei der Betreuung von Menschen mit Demenz gewinnt der Einsatz von Technologien immer grössere Bedeutung. In den Pflegeheimen werden technische Hilfen zunehmend in Form von Personenortungssystemen verwendet, die dem Pflegepersonal die Betreuung von Demenzerkrankten mit Weglauftendenzen erleichtern sollen. Durch diese Vorrichtungen werden Demenzerkrankte entweder sofort am Verlassen des Heimes gehindert oder nach Verlassen des Heimes auf dem Gelände leichter aufgefunden. Bei der Verwendung von Ortungssystemen stellen sich bislang nicht ausreichend geklärte Fragen insbesondere im Zusammenhang mit ethischen und rechtlichen Aspekten. So zählen Freiheitseinschränkungen, Kontrolle und Überwachung zu denjenigen Massnahmen, die in der Regel als ethisch bedenklich angesehen werden. Massstab ist hierbei aber der gesunde

Mensch, der im Vollbesitz seiner geistigen Kräfte und in einem emotionalen Gleichgewicht lebt. Dies ist aber bei Demenzerkrankten nicht der Fall, vielmehr benötigen diese bei fortgeschrittener Erkrankung immer Dritte, die für Sicherheit und Gefahrenfreiheit sorgen. In juristischer Hinsicht berührt der Einsatz von Ortungssystemen die Grundrechte der persönlichen Freiheit und der informationellen Selbstbestimmung und in privatrechtlichen Verhältnissen den Schutz der Persönlichkeit. Bei nicht vorhandener Urteilsfähigkeit der betroffenen Personen stellen sich die vertretungsrechtlichen Fragen ab 2013 auf der Basis des neuen Erwachsenenschutzrechts. Zu beachten sind unter dem bisherigen wie auch unter dem neuen Recht einschlägige Patientenverfügungen. Diese Ausgangslage – technologische Neuerungen einerseits und ein neuer rechtlicher Rahmen andererseits – erfordert eine sorgfältige Beachtung der Praxis.

Unsere Empfehlung richtet sich an die kantonalen Erwachsenenschutzbehörden, die zu einem koordinierten Vorgehen aufgefordert werden, um die zunehmenden Anwendungen von Ortungstechnologien systematisch zu evaluieren und auf dieser Grundlage Schlussfolgerungen im Hinblick auf eventuellen Regelungs- und Diskussionsbedarf zu ziehen.

S8: Nutzung des Vorbildcharakters staatlicher Anwendungen von Ortungstechnologien

Für staatliche Stellen bieten die Ortungstechnologien grosse Chancen zur optimierten Wahrnehmung ihrer Aufgaben unter freiwilliger Beteiligung der Bürger. Der Staat soll diese Chancen nutzen und dabei diese Anwendungen so gestalten, dass sie eine Vorbildfunktion erfüllen, insbesondere in Bezug auf die Umsetzung der Grundsätze des Datenschutzrechts. Staatliche Anwendungen sollen freiwillig bereitgestellte Daten der Bürger soweit wie möglich anonymisiert oder pseudonymisiert verarbeiten, einer strikten Zweckbindung unterliegen und Daten nach Gebrauch zuverlässig löschen (vgl. auch Empfehlung A4 für konkretere Anforderungen).

Chancen für die Optimierung staatlicher Aufgaben liegen besonders im Bereich des standortbezogenen Crowdsourcing (vgl. auch Empfehlung S9 als Spezialfall). Beispiele:

- Umweltmonitoring durch Smartphone-Nutzerinnen, etwa zur Erstellung von Lärmkarten (wie z.B. im Projekt Nosetube, www.noisetube.net).

- Überprüfung von staatlichen Umweltmonitoring-Daten durch die Bürger, die eigene Beobachtungen per SMS melden (wie z.B. das Projekt Eye on Earth der Europäischen Umweltagentur).

- Monitoring von Gesundheitsbelastungen zur Beobachtung des Verlaufs von epidemischen Erkrankungen und anderen die Gesundheit der Bevölkerung betreffenden Entwicklungen.

- Früherkennung von Notfallsituationen und sich anbahnenden katastrophalen Ereignissen, Emergency Response bei Massenveranstaltungen.

Wir empfehlen den zuständigen Bundesämtern (BAfU, BAG, BABS und evtl. weitere), Konzepte für eine entsprechende Nutzung von Ortungsdaten zu erarbeiten und von Beginn an sichere und vertrauenswürdige Verfahren zur möglichst weitgehenden Anonymisierung bzw. Pseudonymisierung von Daten technisch und organisatorisch vorzusehen, ebenso Massnahmen zur Transparenz, zur strikten Zweckbindung und zur endgültigen Löschung der Daten. Damit würde ein De-facto-Standard für vertrauenswürdige Crowdsourcing-Apps geschaffen, der auch zum Massstab für privatwirtschaftliche Angebote werden könnte.

S9: Datenschutzgerechte Nutzung von Crowdsourcing im Verkehr

Heute nutzen viele Verkehrsteilnehmer Ortungssysteme und darauf basierende Dienstleistungen wie Routenplanung oder Standortbestimmung über mobile Endgeräte wie Navigationssysteme, Smartphones oder Tabletcomputer. Viele dieser Anwendungen leiten die erfassten Bewegungsdaten auch weiter. Damit lassen sich kollaborative Formen der Leistungserbringung (Crowdsourcing) realisieren, etwa um Verkehrsinformationen in Echtzeit zu generieren, Empfehlungen für die aktuell optimale Route und Geschwindigkeit abzugeben oder aktuelle Auslastungen im öffentlichen Verkehr präzise zu bestimmen und die Statistik zu verbessern.

Auch die Instandhaltung von Verkehrsinfrastrukturen kann durch standortbasiertes Crowdsourcing optimiert werden.

Wir empfehlen den zuständigen Stellen, beispielsweise dem UVEK, dem Verband öffentlicher Verkehr und dem ASTRA, Konzepte für eine entsprechende

Nutzung von Ortungsdaten zu erarbeiten und von Beginn an sichere und vertrauenswürdige Verfahren zur Anonymisierung technisch und organisatorisch vorzusehen, damit der Aufbau und der erfolgreiche Einsatz entsprechender Anwendungen nicht durch einen Missbrauchsverdacht gefährdet werden. Die Umsetzung dieser Konzepte kann im Rahmen einer Public-Private Partnership erfolgen.

Dabei ist ein fairer Umgang mit den entstehenden Datenbeständen nicht nur gegenüber den Bürgern, sondern auch zwischen Bund und Kantonen und anderen beteiligten Akteuren (beispielsweise zwischen den verschiedenen Unternehmen des öffentlichen Verkehrs) zu beachten. Selbst vollständig anonymisierte Daten können einen hohen Wert für die Marktforschung und andere strategische Aufgaben darstellen und sollten deshalb nicht monopolisiert werden, wenn sie durch freiwillige Mitwirkung der Bürger erhoben wurden.

Wenn entsprechende Applikationen und die zugehörigen Dienstleistungen von öffentlichen Stellen oder in deren Auftrag angeboten werden, können die aus den Daten gewonnenen Informationen am besten auf öffentliche Aufgaben zugeschnitten und die Zweckbindung der Daten bzw. der Datenschutz gewährleistet werden. Für die Verkehrsteilnehmer, die ihre Daten freiwillig bereitstellen, ergeben sich dabei Vorteile hinsichtlich der Vertrauenswürdigkeit der Stellen, denen sie die Daten offenlegen.

S10: Einheitliche Regelung der Video-Ortung

Die Bearbeitung von Daten der Videoüberwachung, auf denen Personen erkennbar sind, greift in das in Art. 8 EMRK geschützte Recht auf Achtung des Privatlebens und in den grundrechtlich geschützten Anspruch auf Schutz vor Missbrauch der persönlichen Daten ein (BGE 133 I 77 Erw. 3.2). Sowohl die Video-Ortung in Echtzeit wie die Aufbewahrung der durch die Video-Ortung gewonnenen Personendaten stellen einen schwerwiegenden Grundrechtseingriff dar und erfordern eine gesetzliche Grundlage und ein öffentliches Interesse oder den Schutz der Grundrechte Dritter an der Überwachung. Überdies muss die Überwachung dem Grundsatz der Verhältnismässigkeit genügen (BGE 133 I 77 Erw. 4.1).

Über diese Grundregeln hinaus bestehen in der Schweiz kaum einheitliche Regelungen zu den Voraussetzungen, Möglichkeiten und Schranken der Video-

Ortung. Einzig im Bereich der Personenbeförderung wurde im Personenbeförderungsgesetz, PBG) vom 20. März 2009 eine einheitliche Regelung geschaffen. Diverse bundesrechtliche Vorschriften regeln überdies die Videoüberwachung staatlicher Verwaltungs-, Parlaments- und Regierungsgebäude und orientieren sich dabei an den unterschiedlichen Anforderungen. Das Eidgenössische Justiz- und Polizeidepartement wies 2007 auf ungenügende Regelungen hinsichtlich Existenz und Qualität der rechtlichen Grundlagen hin: «Diejenigen Kantone und Gemeinden, die über keine oder nur ungenügend bestimmte formellgesetzliche Grundlagen für die Videoüberwachung mit Personenerkennbarkeit verfügen, erfüllen die verfassungsmässigen Voraussetzungen für die Einschränkung von Grundrechten nicht.» (EJPD, 2007, S. 2).

Wir empfehlen die Schaffung einer in der ganzen Schweiz geltenden einheitlichen Regelung, die insbesondere die Präzisierung des Verhältnismässigkeitsprinzips durch technische und organisatorische Massnahmen, namentlich durch den Einsatz von Privacy-Filtern, die Verschlüsselung von Bildmaterial, kurze Aufbewahrungszeiten oder die Beschränkung des Aufnahmebereichs der Videokamera nur für den verfolgten Zweck beinhaltet.

Dabei müssen zukünftige technische Fortschritte in der Aufnahmetechnik sowie der automatisierten Erkennung von Gesichtern, Fahrzeugkennzeichen und anderen identifizierenden Merkmalen von Personen oder Sachen vorausschauend berücksichtigt werden. Der Abgleich von aufgenommenen Daten mit grösseren Datenbeständen durch Anwendung solcher Verfahren muss ausgeschlossen oder mit ausreichend hohen Hürden versehen werden, der Schwere des Grundrechtseingriffs bzw. Eingriffs in das Recht der Persönlichkeit angemessen sind.

Aufgrund der Kompetenzverteilung zwischen Bund und Kantonen empfiehlt es sich, eine solche gesetzliche Regelung über den Mindeststandard bei Video-Ortung einerseits im DSG (bindend für den Bund und Private) und in den kantonalen Datenschutzerlassen (bindend für die Kantone in ihrem Kompetenzbereich) zu erlassen.

S11: Ausdehnung des Prinzips «Robinsonliste» auf digitale Medien, insbesondere standortbezogenes Marketing

Das Prinzip der «Robinsonliste» für Personen, die keine Direktwerbung wünschen, soll auf digitale Medien, insbesondere standortbezogenes Marketing bzw. Mikromarketing ausgedehnt werden. Die Einrichtung soll helfen, als belästigend empfundene Werbung im Zusammenhang mit standortbasierten Diensten zu vermeiden. Der Eintrag in die Robinsonliste zum Schutz gegen unangeforderte Werbung soll für den Verbraucher kostenlos sein. Privatpersonen, die keine standortbezogene Werbung bekommen möchten, können ihre jeweiligen Daten (z.B. SIM-Card-Nr. oder Nutzername bei Internetdiensten) in die Liste eintragen lassen.

Die Robinsonliste für standortbezogenes Marketing wäre vergleichbar zu der bestehenden Liste für adressierte Werbung in der Schweiz: Privatpersonen, die keine adressierte Werbung mehr in ihrem Briefkasten wünschen, können sich in eine Adressdatei eintragen lassen. Die Robinsonliste für adressierte Werbung ist eine sogenannte Negativliste, die monatlich an die Mitglieder des Schweizer Direktmarketing Verbandes (SDV) geschickt wird. Diese Firmen verpflichten sich, künftig keine adressierten Werbesendungen mehr an die in der Robinsonliste eingetragenen Adressen zu senden. Der SDV verwaltet derzeit die Robinsonlisten für adressierte Werbung und Direct Sales. Dieses Prinzip soll auf digitale Medien ausgedehnt werden, was besonders bei standortbezogener Werbung – die ja von lokalen Anbietern stammt – aussichtsreich erscheint.

Diese Empfehlung richtet sich an den Schweizer Direktmarketing Verband. Als alternative Träger kommen Konsumentenorganisationen in Betracht.

Literaturverzeichnis

Abi-Müller, R. (2005): Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Habil. Abhandlungen zum schweizerischen Recht (ASR) Bd. 710, Stämpfli Verlag, Bern.

Aka-Aki (2011): Aka-Aki Blog. Online verfügbar unter http://blog.aka-aki.com/ (24. Februar 2012).

Alasdair, A.; Warden, P. (2011): Got an iPhone or 3G iPad? Apple is recording your moves. Online verfügbar unter http://radar.oreilly.com/2011/04/apple-location-tracking.html (24. Februar 2012).

All Things (2011): Foursquare and Groupon Planning Distribution Deal. Online verfügbar unter http://allthingsd.com/20110523/foursquare-and-groupon-planning-distribution-deal/ (24. Februar 2012).

Allmaier, M. (2011): Die Welt in der Tasche. Online verfügbar unter http://www.zeit.de/2011/02/Elektrifizierter-Tourist (24. Februar 2012)

ARE – Bundesamt für Raumentwicklung (2009): Faktenblatt Freizeitverkehr: Zusatzauswertungen des Mikrozensus zum Verkehrsverhalten 2005. Bern.

Arnold, M. (2004): Intelligente Transportsysteme (Hausarbeit). Universität Ulm, Ulm. Online verfügbar unter https://cs05.informatik.uni-ulm.de/ki/Edu/Proseminare/KI/SS04/Ausarbeitungen/05-Arnold.pdf (24. Februar 2012).

ASTRA – Bundesamt für Strassen (2010): Verkehrsentwicklung und Verfügbarkeit der Nationalstrassen: Jahresbericht 2009. Bern. Online verfügbar unter http://www.news.admin.ch/NSBSubscriber/message/attachments/20434.pdf (24. Februar 2012).

ASTRA – Bundesamt für Strassen (2011): 1,9 Milliarden Franken für Bau, Ausbau und Unterhalt der Nationalstrassen. Bern. Online verfügbar unter http://www.astra.admin.ch/00638/index.html?lang=de&msg-id=38026 (24. Februar 2012).

AUDIO MOBIL Elektronik GmbH (2012): Vehicle-to-x-kommunikation: Echtzeitdaten für intelligentes Verkehrsmanagement. Online verfügbar

unter http://www.audio-mobil.com/de-car-kommunikation.htm (24. Februar 2012).

Aviva (2006): Norwich Union launches innovative «Pay As You Drive» insurance with prices from 1p per mile. Online verfügbar unter http://www.aviva.co.uk/media-centre/story/2840/norwich-union-launches-innovative-pay-as-you-drive/ (24. Februar 2012).

BABS – Bundesamt für Bevölkerungsschutz (2010): Das Schweizer Programm zum Schutz Kritischer Infrastrukturen. Bern. Online verfügbar unter http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/themen/ski.parsysrelated1.82246.downloadList.32191.DownloadFile.tmp/factsheetd.pdf (24. Februar 2012).

Baeriswyl, B. (2009a): Die Anwendbarkeit des Datenschutzgesetzes: Schweizerisches Datenschutzrecht ist auch auf den Internetdienst «Street View» anwendbar. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Baeriswyl, B. (2009b): Entwicklungen im Datenschutzrecht, SJZ 105, 2009, S. 442ff.

Baeriswyl, B. (2010): Kleingedrucktes unter der Lupe. Die allgemeinen Geschäftsbedingungen von sozialen Netzwerken versprechen keinen Datenschutz. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich, S. 56ff.

Baeriswyl, B. (2011): Neuer Datenschutz für die digitale Welt – Ein wirksames Datenschutzkonzept muss die tatsächlichen Risiken für die Privatheit minimieren können. In: digma - Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Beisswenger, A. (Hrsg.) (2010): YouTube und seine Kinder: Wie Online Video, Web TV und Social Media die Kommunikation von Marken, Medien und Menschen revolutionieren. Baden-Baden: Nomos, Edition Reinhard Fischer. Online verfügbar unter http://www.worldcat.org/oclc/646402854 (24. Februar 2012).

Belser, E. M.; Epiney, A.; Waldmann, B. (2011): Datenschutzrecht. Grundlagen und öffentliches Recht. Stämpfli: Bern, Berlin und München.

Beresford, A. R. (2005): Location Privacy in Ubiquitous Computing. Technical Report, Number 612, University of Cambridge. Online verfügbar unter http://www.cl.cam.ac.uk/research/dtg/www/publications/public/arb33/UCAM-CL-TR-612.pdf (24. Februar 2012).

Beresford, A. R.; Stajano, F. (2003): Location Privacy in Pervasive Computing. Pervasive Computing, IEEE, Volume: 2 Issue:1, S. 46–55. Online verfügbar unter http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1186725&tag=1 (24. Februar 2012).

Bernet PR (2011): Social Media Studie Schweiz: Viel Präsenz, wenig Strategie. Online verfügbar unter http://www.bernet.ch/socialmediastudie (24. Februar 2012).

Bernet PR (2011): Social Media Studie Schweiz: Vom Web 2.0 zum Online-Dialog. Online verfügbar unter http://www.bernet.ch/studien# (24. Februar 2012).

Bernhard, N. (2010): Chip soll Bahnbillett ersetzen. BZ – Berner Zeitung. Online verfügbar unter http://bazonline.ch/schweiz/standard/Chip-soll-Bahnbillett-ersetzen-/story/11236262 (24. Februar 2012).

BFS – Bundesamt für Statistik (2007): Mobilität in der Schweiz: Ergebnisse des Mikrozensus 2005 zum Verkehrsverhalten. Neuchâtel.

BFS – Bundesamt für Statistik (2010): Mobilität und Verkehr 2010 (Statistik der Schweiz No. 11). Neuchâtel. Online verfügbar unter http://www.bfs.admin.ch/bfs/portal/de/index/news/publikationen.Document.139559.pdf (24. Februar 2012).

BFS – Bundesamt für Statistik (2011a): Informationsgesellschaft – Indikatoren: Haushalte und Bevölkerung – Internetnutzung. Online verfügbar unter http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html?open=5,1#1 (24. Februar 2012).

BFS – Bundesamt für Statistik (2011b): Verkehrsleistungen – Daten, Indikatoren. Online verfügbar unter http://www.bfs.admin.ch/bfs/portal/de/index/themen/11/05/blank/key/verkehrsleistungen/leistungen.html (24. Februar 2012).

BFS – Bundesamt für Statistik (2011c). Verkehrsunfälle und Umweltauswirkungen – Daten, Indikatoren. Online verfügbar unter http://www.bfs.admin.ch/bfs/portal/de/index/themen/11/06/blank/key/01/aktuel.html (24. Februar 2012).

Biermann, K. (2011): Daten sind Twitters Geschäftsmodell. Online verfügbar unter http://www.zeit.de/digital/datenschutz/2011-04/twitter-daten-firehose (24. Februar 2012).

Biermann, K. (2011): Was Vorratsdaten über uns verraten. Online verfügbar unter http://www.zeit.de/digital/datenschutz/2011-02/vorratsdaten-malte-spitz (24. Februar 2012).

Binswanger, M. (2001): Technological progress and sustainable development: what about the rebound effect? Ecol Econ 36:119–132

Blonski, D. (2011): Schweizerisches Bundesverwaltungsgericht, Urteil vom 30. März 2011 in Sachen Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB gegen Google Inc. sowie Google Switzerland GmbH bezüglich der Empfehlung des EDÖB vom 11. September 2009 (A-7040/2009). In: AJP 6/2011, S. 840 ff.

BlueSky Positioning (2010): A-GPS on SIM card technology from BlueSky Positioning powers Celesta mobile workforce solutions. Online verfügbar unter http://www.blueskypositioning.com/uploaded_files/A-GPS%20on%20SIM%20card%20technology%20from%20BlueSky%20Positioning%20powers%20Celesta%20mobile%20workforce%20solutions.pdf (24. Februar 2012).

Blumberg, A. J.; Eckersley, P. (2009): On Locational Privacy, and How to Avoid Losing it Forever. Online verfügbar unter http://www.eff.org/wp/locational-privacy (24. Februar 2012).

Bondallaz, S. (2007): La protection des personnes et de leurs données dans les télécommunications, Zürich/Basel/Genf 2007, S. 411ff.

Borsboom, B.; van Amstel, B.; Groeneveld, F. (2011): Please rob me out – Social Network. Online verfügbar unter http://pleaserobme.com/ (24. Februar 2012).

Bosien, A. (2008): Bewertung von Technologien zur Ortung und Identifizierung. Online verfügbar unter http://carma.ti5.tuharburg.de/docs/D311_OI_V100.pdf (24. Februar 2012).

Boukerche, A.; Oliveira, H. A.; Nakamura, E. F.; Antonio, A. L. (2008): Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems. Computer Communications, (31), S. 2838–2849.

Bradsher, K. (2007): China Enacting a High-Tech Plan to Track People. The New York Times. Online verfügbar unter http://www.nytimes.com/2007/08/12/business/worldbusiness/12security.html?pagewanted=all (24. Februar 2012).

Brandon, J. (2011): Crowdsourcing für bessere Strassen. Technology Review. Online verfügbar unter http://heise.de/-1244830 (24. Februar 2012).

Brightkite (2011): Brightkite Terms of Use. Online verfügbar unter http://brightkite.com/pages/bk_terms_of_service.html (22. September 2011).

Brunner, S. C. (2009): Zur Umsetzung von «Schengen» und «Dublin» im Bereich des Datenschutzes: Drei Thesen. In: Epiney, A.; Hobi, P. (Hrsg.) (2009): Die Revision des Datenschutzrechts, Zürich, S. 39 ff.

Brunner, S. C. (2011): Mit rostiger Flinte unterwegs in virtuellen Welten?, Jusletter 4. April 2011.

Buderi, R. (1996): The Invention That Changed the World: How a Small Group of Radar Pioneers Won the Second World War and Launched a Technological Revolution (Sloan Technology Series). Simon & Schuster, 1st edition.

Bundesministerium des Innern. (o. D.). Fragen und Antworten zum EasyPass. Online verfügbar unter http://www.bmi.bund.de/SharedDocs/FAQs/DE/Themen/Sicherheit/PaesseundAusweise/EasyPass_FAQ.html?nn=109628 (24. Februar 2012).

Bundesrat (2001): Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz. Online verfügbar unter: http://www.ejpd.admin.ch/content/dam/data/staat_buerger/evaluation/bj/ber-br-datenschutz-d.pdf (24. Februar 2012).

Burson-Marsteller (2010): The Global Social Media Check-up: Insights from the Burson-Marsteller Evidence-Based Communications Group. Online verfügbar unter http://www.burson-marsteller.com/Innovation_and_insights/blogs_and_podcasts/BM_Blog/Documents/Burson-Marsteller%202010%20Global%20Social%20Media%20Check-up%20white%20paper.pdf (24. Februar 2012).

Capkun, S. (2011): (Selected) Security Issues in Mobile Computing. 16th Symposium on Privacy and Security, ETH Zürich.

Cheng, J. (2012): Over 3 years later, «deleted» Facebook photos are still online. Arstechnica. Online verfügbar unter http://arstechnica.com/business/news/2012/02/nearly-3-years-later-deleted-facebook-photos-are-still-online.ars (24. Februar 2012).

Coroama, V. (2006): The Smart Tachograph - Individual Accounting of Traffic Costs and its Implications. In: Fishkin, K. P.; Schiele, B.; Nixon, P.; Quigley, A. J. (Hrsg.): Proceedings of Pervasive 2006, Springer, S. 135–152.

Coroama, V.; Langheinrich, M. (2006): Personalized Vehicle Insurance Rates – A Case for Client-Side Personalization in Ubiquitous Computing. In: Kobsa, A.; Chellappa, R. K.; Spiekermann, S. (Hrsg.): Proceedings of the Workshop on Privacy-Enhanced Personalization at CHI 2006.

Crum, C. (2010): Twitter Sells Data, Provides Analytics, Gives Users «Reputation Scores»: Lots Happening Since Twitter CEO Transition. Online verfügbar unter http://www.webpronews.com/twitter-sells-data-provides-analytics-gives-users-reputation-scores-2010-11 (24. Februar 2012).

D'Anna-Huber, Ch. (2011) Digital Natives. Wie braucht die «Generation Internet» das Internet? Bern: TA-Swiss.

Dasser, F. (2007) In: Honsell, H.; Vogt, N.P.; Schnyder, A.K.; Berti, S. V.(Hrsg.) (2007): Internationales Privatrecht. Basler Kommentar, 2. Aufl., Basel, Rz. 39 zu Art. 139 IPRG.

Die Johanniter (2011): Rettung via GPS-Ortung: Johanniter stellen Einsatz für Dokumentarfilm nach. Online verfügbar unter http://www.johanniter.de/die-johanniter/johanniter-unfall-hilfe/juh-vor-ort/lv-nordrhein-westfalen/aktuelles/nachrichten/archiv-2011/rettung-via-gps-ortung/ (24. Februar 2012).

Die Wochenzeitung (2011): Ohne Handy an die Demo. 2011-06-23.

Dimov, D.; Zlateva, N.; Marinov, A. (2008): CBIR approach to face recognition.

Dodel, H.; Häupler, D. (2010): Satellitennavigation (German Edition). Springer, 2., korr. u. erw. Aufl.

dpa (2010): Google und TU Braunschweig: Roboter-Autos auf den Strassen. Faz.net. Online verfügbar unter http://www.faz.net/-010j3 (24. Februar 2012).

DSB Kanton Zürich – Datenschutzbeauftragter des Kantons Zürich (2008): Tätigkeitsbericht 2007. Zürich. Online verfügbar unter http://www.dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/taetigkeitsberichte.html (24. Februar 2012).

DSB Kanton Zürich – Datenschutzbeauftragter des Kantons Zürich (2010): Videoüberwachung durch öffentliche Organe (ohne Strafverfolgungsbehörden) (Version 10). Zürich. Online verfügbar unter http://www.datenschutz.ch/fileadmin/user_upload/datenschutz/04_Publikationen/Leitfaden_Video%C3%BCberwachung_durch_%C3%B6ffentliche_Organe.pdf (30. August 2011).

DSW – Deutsche Stiftung Weltbevölkerung (2011): Weltbevölkerungsuhr. Online verfügbar unter http://www.weltbevoelkerung.de/info-service/weltbevoelkerungsuhr.php?navid=3 (24. Februar 2012).

EDÖB – Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (2010): Erläuterungen zu Sozialen Netzwerken.

EDÖB – Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (2011): 18. Tätigkeitsbericht 2010/2011. Bern.

Egli, U. (2011): Soziale Netzwerke und Arbeitsverhältnis – Über die Auswirkungen von Facebook, Xing & Co auf den betrieblichen Alltag. In: Jusletter 17. Januar 2011.

EGMR – Europäischer Gerichtshof für Menschenrechte (2011): Protection des données personelles. Fiche thématique. Online verfügbar unter http://www.echr.coe.int/NR/rdonlyres/26507FA5-66F3-435F-8950-341545344709/0/3235359_Fiche_thematique_pour_la_presse__Protection_des_donnees.pdf (24. Februar 2012).

EJPD – Eidgenössisches Justiz- und Polizeidepartement (2007): Videoüberwachung zu Sicherheitszwecken in Bahnhöfen, Flughäfen und an anderen öffentlichen Orten: Bericht des EJPD. Online verfügbar unter http://www.ejpd.admin.ch/content/dam/data/pressemitteilung/2007/pm_2007-09-28__bericht/070926_bericht_videoueberwachungpubld.pdf (24. Februar 2012).

EJPD – Eidgenössisches Justiz- und Polizeidepartement (2011a): Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch. Online verfügbar unter http://www.ejpd.admin.ch/ejpd/de/home/themen/kriminalitaet/ref_gesetzgebung/ref_sexuelleausbeutung.html (24. Februar 2012).

EJPD – Eidgenössisches Justiz- und Polizeidepartement (2011b): Den Datenschutz stärken. Der Bundesrat heisst den Bericht über die Evaluation des Datenschutzgesetzes gut. Online verfügbar unter http://www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2011/2011-12-09.html (24. Februar 2012).

El Emam, K.; Brown, A.; AbdelMalik, P. (2008): Evaluating Predictors of Geographic Area Population Size Cut-offs to Manage Re-identification Risk Journal of American Medical Informatics Association. Online verfügbar unter http://www.jamia.org/cgi/ content/abstract/ 16/2/256 (11. August 2011).

Elwood, S.; Leszczynski, A. (2011): Privacy, reconsidered: New representations, data practices, and the geoweb. Geoforum, 42(1), 6–15. doi:10.1016/j.geoforum.2010.08.003.

Emarketer (2010): Social Network Ad Spending to Approach $1.7 Billion This Year. Online verfügbar unter http://www.emarketer.com/Article.aspx?R=1007869#page;http://www.emarketer.com/Article.aspx?R=1007869 (24. Februar 2012).

Enisa – European Network and Information Security Agency (2010): Instantly Online – 17 Goldene Regeln zur Bekämpfung von Online-Risiken und für sichereres Surfen mobiler sozialer Netzwerke: Pressemitteilung vom 08.02.2010. Online verfügbar unter http://www.enisa.europa.eu/media/press-releases/prs-in-german/msnde (24. Februar 2012).

Epiney, A. (2009): Zu den völker- und europarechtlichen Rahmenbedingungen der Revision des Datenschutzgesetztes. In: Epiney, A.; Hobi, P. (Hrsg.) (2009): Die Revision des Datenschutzrechts, Zürich, S. 1 ff.

Epiney, A. (2011): Neuere Entwicklungen im EU-Datenschutzrecht und Auswirkungen für die Schweiz, Aktuelle Juristische Praxis AJP 5/2011, S. 641 ff.

Epiney, A.; Schleiss, Y. (2011): Völker- und europarechtlicher Rahmen. In: Belser, E. M.; Epiney, A.; Waldmann, B. (Hrsg.) (2011): Datenschutzrecht. Grundlagen und öffentliches Recht, Bern, S. 53 ff.

EUCAR – European Council for Automotive Rad (2010): Collaborative R&D for Automotive Innovation 2010-2011. Online verfügbar unter http://www.eucar.be/publications/EUCAR%20Projects (24. Februar 2012).

Europäische Kommission (2009): Entscheidung der Kommission vom 6. Oktober 2009 über die Festlegung der Merkmale des europäischen elektronischen Mautdienstes und seiner technischen Komponenten. Online verfügbar unter http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:268:0011:0029:DE:PDF (24. Februar 2012).

Europäische Union (2009): Mehr Leben retten auf Europas Strassen: Mobilfunkbetreiber verpflichten sich zur Einführung von eCall: Pressemitteilung vom 09.09.2009. IP/09/1290. Brüssel. Online verfügbar unter http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/488&format=HTML&aged=0&language=DE&guiLanguage=en (24. Februar 2012).

Europäische Union (2010): Notrufe: Kommission begrüsst Einführung des eCall-Systems in Kraftfahrzeugen durch weitere Mitgliedstaaten: Pressemitteilung vom 04.05.2010. (IP/10/488). Brüssel. Online verfügbar unter http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/488&format=HTML&aged=1&language=DE&guiLanguage=en (24. Februar 2012).

Europäische Union (2011): Digital Agenda: Children using social networks at a younger age; many unaware of basic privacy risks, says survey: Pressemitteilung vom 18.04.2011. (IP/11/479). Online verfügbar unter http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/479&format=HTML&aged=0&language= (24. Februar 2012).

European Commission (2011): Privacy and Data Protection Impact Assessment Framework for RFID Applications. 12 January 2001. Online verfügbar unter http://ec.europa.eu/information_society/policy/rfid/library/index_en.htm (24. Februar 2012).

Facebook (2009): Facebook Pages. Online verfügbar unter http://www.facebook.com/advertising/FacebookPagesProductGuide.pdf (24. Februar 2012).

Facebook (2010): Facebook's Privacy Policy. Online verfügbar unter http://www.facebook.com/policy.php (24. Februar 2012).

Facebook (2011): Erklärung der Rechte und Pflichten. Online verfügbar unter http://de-de.facebook.com/terms.php?ref=pf (24. Februar 2012).

Facebook (2011): Statistics: Global Reach. Online verfügbar unter http://www.facebook.com/press/info.php?statistics (24. Februar 2012).

faz.net (2010): Google und TU Braunschweig: Roboter-Autos auf den Strassen. Online verfügbar unter http://www.faz.net/artikel/C31151/google-und-tu-braunschweig-roboter-autos-auf-den-strassen-30001154.html (24. Februar 2012).

Fink, S.; Zerfass, A. (2010): Social Media Governance 2010: Ergebnisse einer Studie bei Kommunikationsverantwortlichen in Unternehmen, Behörden,Verbänden und Non-Profit-Organisationen in Deutschland. Leipzig, Wiesbaden. Online verfügbar unter http://www.ffpr.de/fileadmin/user_upload/PDF-Dokumente/Studie_Social_Media_Governance_2010_-_Studienergebnisse.pdf (24. Februar 2012).

Finke, T.; Kelter, H. (2004): Radio Frequency Identification – Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443-Systems. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/RFID/Abh_RFID_pdf.pdf?__blob=publicationFile (24. Februar 2012).

Forgo, N.; Krügel, T. (2010): Der Personenbezug von Geodaten. Cui bono, wenn alles bestimmbar ist? Zeitschrift für Informations-, Telekommunikations-und Medienrecht (MMR), S. 17–23.

Forgo, N.; Krügel, T.; Müllenbach, K.; Schütze, B. (2010): Gutachten Google Street View, 18. Februar 2010, Hannover.

Foursquare (2011a): Foursquare Labs, Inc. Privacy Policy. Online verfügbar unter https://de.foursquare.com/legal/privacy (24. Februar 2012).

Foursquare (2011b): Foursquare Labs, Inc. Terms of use. Online verfügbar unter https://de.foursquare.com/legal/terms (24. Februar 2012).

Foursquare (2011c): Location-based mobil platform. Online verfügbar unter https://de.foursquare.com/about (24. Februar 2012).

friendticker (2011): Allgemeine Geschäftsbedingungen für die Nutzung von friendticker. Online verfügbar unter http://de.friendticker.com/home_page/show_agb (24. Februar 2012).

Fuller, J. (2008): How Bluetooth Surveillance Works. Online verfügbar http://electronics.howstuffworks.com/bluetooth-surveillance.htm (24. Februar 2012).

Geiser, T.; Uttinger, U. (2010): Google Street View und Persönlichkeitsschutz. medialex, (3):124–129.

GeoCentrics (2011): Gypsii. Online verfügbar unter http://www.gypsii.com/ (24. Februar 2012).

Glaser, B. (2009): Private Überwachung im öffentlichen Raum. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Gonggrijp, R.; Hengeveld, W.-J.; Bogk, A.; Engling, D.; Mehnert, H.; Rieger, F.; Scheffers, P.; Wels, B. (2006): Nedap / Groenendaal ES3B

Goodchild, M. (2007): Citizens as sensors: the world of volunteered geography. GeoJournal, 69(4), 211–221. doi:10.1007/s10708-007-9111-y

Google (2011): Orkut. Online verfügbar unter http://www.google.com/support/orkut/bin/answer.py?hl=de&answer=11559 (24. Februar 2012).

Google Mobil (2011): Google Buzz für Handys. Online verfügbar unter http://www.google.com/intl/de_ALL/mobile/buzz/ (24. Februar 2012).

Greene, W.; Lancaster, B. (2007): Over the Top Services: Article for Pipeline Magazine, 12 2007. Online verfügbar unter http://www.ltcinternational.com/insideout/uploads/ltc_otts_whitepaper.pdf (23. August 2011).

Grifantini, K. (2011): Extraauge fürs Auto. Technology Review. Online verfügbar unter http://www.heise.de/tr/artikel/Extraauge-fuers-Auto-1270356.html (24. Februar 2012).

Grossenbacher, T. (2011): Möglichkeiten der algorithmischen Auswertung von Standortdaten. Universität Zürich.

Hagenacker, J. (2011): Dreck-Ecken per Handy melden. NGZ online. Online verfügbar unter http://www.ngz-online.de/kaarst/nachrichten/dreck-ecken-per-handy-melden-1.1819330 (24. Februar 2012).

Hallberg, J.; Nilsson, M.; Synnes, K. (2002): Bluetooth Positioning. Proceedings of the Third Annual Symposium on Computer Science and Electrical Engineering. (CSEE 2002), Luleå, Sweden, 27–28 May 2002.

Hamann, G. (2010): Behavioral Targeting: Der Mensch denkt, das Handy lenkt. Zeit Online. 09.12.2010.

Hämmerli, B. M. (2011): IT-Security: Die nächsten zehn Jahre – Ein Versuch, aus IT-Entwicklungstrends die Herausforderungen für die IT-Sicherheit abzuleiten. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Hangartner, I. (1987): Zur Konzeption der Handels- und Gewerbefreiheit. In: Dicke, D. Ch.; Fleiner-Gerstner, T. (Hrsg.) (1987): Staat und Gesellschaft, Festschrift für Leo Schürmann, Freiburg, S. 117 ff.

Härter, H. (2011): Bordnetzarchitektur nutzt fahrzeugübergreifende Informationen. Online verfügbar unter http://www.elektronikpraxis.vogel.de/themen/hardwareentwicklung/datenkommunikationsics/articles/299425 (24. Februar 2012).

Hartinger, R. (2009): Patrick Comboeuf: Mobile wird mehr Umsatz generieren als der Online-Shop: Interview. Online verfügbar unter http://blog.internet-briefing.ch/2009/11/11/patrick-comboeuf-mobile-wird-mehr-umsatz-generieren-als-der-online-shop/ (24. Februar 2012).

Heesen, J. (2008): Keine Freiheit ohne Privatsphäre – Wandel und Wahrung des Privaten in informationstechnisch bestimmten Lebenswelten. In: Gayken S.; Kurz, C. (Hrsg.): 1984.exe – Gesellschaftliche, politische

und juristische Aspekte moderner Überwachungstechnologien. Transcript: Bielefeld, S. 231–246.

Heise Online (2011): Google+: Googles Angriff auf Facebook vom 29.06.2011.

Herfurt, M.; Mulliner, C. (2004): Blueprinting Remote Device Identification based on Bluetooth Fingerprinting Techniques White Paper (Version 0.3), S. 1–8.

Hilty, L. M. (2007): Risiken und Nebenwirkungen der Informatisierung des Alltags. In: Mattern, F. (Hrsg.): Der Computer im 21. Jahrhundert. Die Informatisierung des Alltags. Perspektiven, Technologien, Auswirkungen. Springer, Berlin, S. 187–205.

Hilty, L. M.; Behrendt, S.; Binswanger, M.; Bruinink, A.; Erdmann, L.; Fröhlich, J.; Köhler, A.; Kuster, N.; Som, C.; Würtenberger, F. (2003): Das Vorsorgeprinzip in der Informationsgesellschaft – Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. Herausgegeben vom Zentrum für Technologiefolgen-Abschätzung (TA-SWISS), Bern (TA 46/2003).

Hilty, L. M.; Köhler, A.; Von Schéele, F.; Zah, R.; Ruddy, T. F. (2006): Rebound effects of progress in information technology. Poiesis and Praxis: International Journal of Technology Assessment and Ethics of Science 4:1. S. 19–38.

Hilty, L. M.; Som, C.; Köhler, A. (2004): Assessing the human, social, and environmental risks of pervasive computing. Human and ecological risk assessment: An International Journal, 10(5): 853–874.

Hobi, A. (2010): SBB: In Zukunft mit Chip oder Handy reisen? Online verfügbar unter http://schweizweit.net/2010/07/01/fasttrack-siemens-sbb-rfid-chip-handy/ (24. Februar 2012).

Hochschule Darmstadt (2011): Cyberstalking. Online verfügbar unter http://www.stopptdiemobber.h-da.de/index.php?id=10629 (24. Februar 2012).

Höffken, S.; Papastefanou, G.; Zeile, P. (2008): Google Earth, GPS, Geotagging und neue Möglichkeiten für die Stadtplanung – Ein emotionales Kiezportrait. In: Schrenk, M. (Hrsg.): Mobility nodes as innovation hubs. REAL CORP 008; Tagungsband; Tagungsband – proceedings; 13th International Conference on Urban Planning, Regional Development and Information Society ; 13. Internationale Konferenz zu Stadtplanung, Regionalentwicklung und Informationsgesellschaft ; May, 19–21 2008, Vienna International Airport, Office Park 3. Schwechat-Rannersdorf: Selbstverl. des

Vereins CORP – Competence Center of Urban and Regional Planning, S. 275–281. Online verfügbar unter http://www.corp.at/archive/CORP2008_64.pdf (24. Februar 2012).

Holznagel, B.; Schumacher P. (o.J.): Die Freiheit der Internetdienste, online-Publikation, http://collaboratory.de/discussion_papers/no1#6 (6.6.2011).

Homfeldt, H. G.; Hünerdorf, G. (Hrsg.) (1997): Soziale Arbeit und Gesundheit. Neuwied: Luchterhand.

Honold, P. (1971): Sekundär Radar, Grundlagen und Gerätetechnik. Berlin, München: Siemens.

Horizon.net (2011): Goldman Sachs verschickt Finanzkennzahlen von Facebook / Umsatz von 1,2 Milliarden Dollar. Online verfügbar unter http://www.horizont.net/aktuell/digital/pages/protected/Goldman-Sachs-verschickt-Finanzkennzahlen-von-Facebook--Umsatz-von-1,2-Milliarden-Dollar_97263.html (24. Februar 2012).

Hornig, F. (2009): Who needs newspapers when you have Twitter? Chris Anderson, Wired's editor in chief, discusses the Internet's challenge to the traditional press. Online verfügbar unter http://www.salon.com/2009/07/28/wired_2/ (24. Februar 2012).

Howard, B. (2008): Insurer stops «pay as you drive». Online verfügbar unter http://news.bbc.co.uk/2/hi/programmes/moneybox/7453546.stm http://media.csee.ltu.se/publications/2002/hallberg02bluetooth.pdf http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf http://www.vs.inf.ethz.ch/events/uc07privacy/papers/01-finder.pdf (24. Februar 2012).

Hutter, T. (2011): Facebook: Automatische Gesichtserkennung in Fotos auch ausserhalb der USA verfügbar. http://www.thomashutter.com/index.php/2011/06/facebook-automatische-gesichtserkennung-in-fotos-auch-ausserhalb-der-usa-verfugbar/ (24. Februar 2012).

IBM Verkehrsentlastung in Stockholm durch neues Mautsystem. Online verfügbar unter http://www-05.ibm.com/ch/ (23. August 2011).

ICTswitzerland (2011): Entscheid Bundesverwaltungsgericht zu Google Street View: Falsche Signale für den Innovationsstandort Schweiz. Online verfügbar unter http://www.ictswitzerland.ch/de/medienmitteilungen/entscheid-bundesverwaltungsgericht-zu-google-street-view-falsche-signale-fuer-den-innovationsstandort-schweiz?page=1 (24. Februar 2012).

iDynamics AG (2010): GPS Ortung – wo sind die Grenzen. SKR – Die schweizerische Kommunal-Revue, (4), 126–127. Online verfügbar unter http://www.idynamics.ch/download/dokumente/flyer/GPSOrtungSKR411.pdf (24. Februar 2012).

IG Metall (2011): Rüge für Daimler-Beschäftigte wegen Facebook-Kommentar – Durch einen Mausklick zuviel in der Bredoulle. Online verfügbar unter http://www.igmetall.de/cps/rde/xchg/internet/style.xsl/ruege-wegen-facebook-kommentar-7773.htm. In: Proc. of A&I'08 Conf., 01–04.10.2008, Sofia, Workshop on Multisensor signal, image and data processing, 02.10.2008, S. IV.21-26. Online verfügbar unter http://www.iit.bas.bg/PR/A&I'08_CBIR_Face_Rec.pdf (24. Februar 2012).

Intelligentes Forschungfahrzeug (2010): Roboterauto «Leonie» rollt durch Braunschweig, stern.de. Online verfügbar unter http://www.stern.de/auto/service/intelligentes-forschungfahrzeug-roboterauto-leonie-rollt-durch-braunschweig-1611991.html (24. Februar 2012).

Interverband für Rettungswesen (2011): Rund um die Uhr in Bereitschaft – doch kaum bekannt. Bern. Online verfügbar unter http://www.ivr-ias.ch/rettungsdienst.php?t=Medienmitteilung+zum+14.4.2011&read_article=159 (24. Februar 2012).

ITU – International Telecommunication Union (2005): The internet of things. ITU Internet Reports.

ITU – International Telecommunication Union (2009): Measuring the Information Society. The ICT Development Index.

ITU – International Telecommunication Union (2010): ITU sees 5 billion mobile subscriptions globally in 2010. Strong global mobile cellular growth predicted across all regions and all major markets.

Janssen, J.-K. (2011): Wo bist´n Du? Googles Dienst Latitude. In: c´t 2011, Heft 3, S. 86–88.

Johnston, C. (2010): Cell phones show human movement predictable 93% of the time. Online verfügbar unter http://arstechnica.com/science/news/2010/02/cell-phones-show-human-movement-predictable-93-of-the-time.ars (24. Februar 2012).

Jorns, O.; Zhendong, M. (2011): Wo bin ich, wo sind wir, wo ist alles? – Ortsbezogene Dienste bieten Vorteile und immense Möglichkeiten, allerdings auch Gefahr des Verlusts der Privatsphäre. In: digma –

Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Jüngling, T. (2009): Handy-Ortung – Wenn das Mobiltelefon neue Freunde findet. In: Welt online vom 23.08.2009.

Kantonsrat Basel-Stadt (2011): Ausgabenbericht betreffend Installation und Betrieb einer Videoüberwachungsanlage für die Kantonspolizei Basel-Stadt (No. JSD/P110637). Basel.

Kantonsrat Zürich (2008): Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich: 1869. Anfrage (Elektronisches Ticket beim ZVV) (No. KR-Nr. 327/2008). Zürich.

Kaplan, A. M.; Haenlein, M. (2010): Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 53(1), 59–68. doi:10.1016/j.bushor.2009.09.003.

Karjoth, G. (2011): Wo war wer wann? Ihr Smartphone weiss es. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Kettiger, D. (2010): Rechtliche Rahmenbedingungen von Location Sharing Systemen in der Schweiz. Jusletter 9. August 2010, S. 173ff.

Khoury, H. M.; Kamat, V. R. (2009): Evaluation of position tracking technologies for user localization in indoor construction environments. Automation in Construction, (18), 444–457. Online verfügbar unter http://pathfinder.engin.umich.edu/documents/Khoury%26Kamat.AIC.2009.pdf (24. Februar 2012).

Klauser, F. R. (2007): Difficulties in Revitalizing Public Space by CCTV.: Street Prostitution Surveillance in the Swiss City of Olten. European Urban & Regional Studies, 14(4), 337–348.

Kloer, T. (2011): Open Compute Project – Facebook legt sein Data Center offen. In: Computerwoche vom 08.04.2011. Online verfügbar unter http://www.computerwoche.de/hardware/data-center-server/2369540/ (24. Februar 2012).

Klöpper, M. (2011): Notruf-App alarmiert Schweizer Luftretter. Online verfügbar unter http://www.feuerwehrmagazin.de/magazin/nachrichten/news/notruf-app-alarmiert-schweizer-luftretter-16078 (24. Februar 2012).

Knoke, F. (2011): Sony twitterte geheimen PS3-Schlüssel. Online verfügbar unter http://www.spiegel.de/netzwelt/web/0,1518,744750,00.html (24. Februar 2012).

Kollmann, T. (2011): E-Business: Grundlagen elektronischer Geschäftsprozesse in der Net Economy (4., überarb. u. erw). Wiesbaden: Gabler.

Kolodziej, K. W.; Hjelm, J. (2006): Local Positioning Systems: LBS applications and Services.

Kosta, E.; Zibuschka, J. (2011): Datenschutzgerechte ortsbasierte Dienste. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Krumm, J. (2009): A survey of computational location privacy. Personal and Ubiquitous Computing 13:6, S. 391–399.

Kuenzi, R. (2011): Wenn Kameras ganze Verhaltensmuster «lesen». Online verfügbar unter http://www.swissinfo.ch/ger/news/magazin/Wenn_Kameras_ganze_Verhaltensmuster_lesen.html?cid=29725092 (24. Februar 2012).

Kuhn, C.; Wilson, W. (2002): «Tagging» Alzheimer's Patients. WebMD Health News. Online verfügbar unter http://www.webmd.com/alzheimers/news/20021017/tagging-alzheimers-patients (24. Februar 2012).

Kündig, A.; Bütschi, D. (2008): Die Verselbständigung des Computers. Vdf Hochschulverlag AG an der ETH Zürich.

Langheinrich, M. (2009): Privacy in Ubiquitous Computing. In: Krumm, J. (Hrsg.): Ubiquitous Computing. Chapman & Hall, CRC Press, S. 95–160. Online verfügbar unter http://www.inf.usi.ch/faculty/langheinrich/articles/papers/2009-ucbook-privacy.pdf (24. Februar 2012).

Langheinrich, M. (2010): Location Privacy. Seminar of the IFIP WG 11.2 Pervasive Systems Security, Istanbu, Turkey, Jun 7, 2010. Online verfügbar unter http://www.cs.ru.nl/ifip-wg11.2/events/Slides-seminar2010/Langheinrich.pdf (24. Februar 2012).

Langheinrich, M.; Coroama, V.; Bohn, J.; Rohs, M. (2002): As we may live – Real-world implications of ubiquitous computing. Technical report, ETH Zurich.

Lenhart, A.; Purcell, K.; Smith, A.; Zickuhr, K. (2010): Social media and mobile internet use among teens and young adults. Washington, DC: Pew Research Center 2010. Online verfügbar unter http://pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx (24. Februar 2012).

Leupold, M.; Wüger, D. (2008): 15 Jahre Internetnutzung – der Stand der Dinge im Schuld-, Kollisions-und Datenschutzrecht. sic!-online, 3, S. 181–199.

Lingner, S.; Lutterbeck, B.; Pallas, F. (Hrsg.) (2010): Die Zukunft der Räume. Gesellschaftliche Fragen auf dem Weg zur «Ambient Intelligence». Graue Reihe, (50).

LinkedIn Press Center. Über LinkedIn. Online verfügbar unter http://press.linkedin.com/about/Ueber-LinkedIn.php (24. Februar 2012).

Lischka, K. (2010): Wie Handys die Welt beobachten. Online verfügbar unter http://www.spiegel.de/netzwelt/web/0,1518,701230,00.html (24. Februar 2012).

Lischka, K. (2011). Marktforschung per Gesichtsanalyse: Schau mich an – und ich weiss, wer du bist. Spiegel online. Online verfügbar unter http://www.spiegel.de/netzwelt/netzpolitik/0,1518,797683,00.html (24. Februar 2012).

Litman, T. (2003): Distance-based vehicle insurance. Technical report, Victoria Transport Policy Institute, Victoria, BC, Canada.

Madden, M. (2010): Older adults and social media. Socialnetworking use among those ages 50 and older nearly doubled over the past year. Washington, DC: Pew Research Center 2010. Online verfügbar unter http://pewinternet.org/Reports/2010/Older-Adults-and-Social-Media.aspx (24. Februar 2012).

Martin, M. (2009): Es lohnt sich, Bits statt Atome zu transportieren. Swiss Engineering STZ.

Mattern, F. (2005): Die technische Basis für das Internet der Dinge. In: Fleisch, E.; Mattern, F. (Hrsg.): Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis, Springer, Berlin.

Mattern, F. (2007, Hrsg.): Der Computer im 21. Jahrhundert. Die Informatisierung des Alltags. Perspektiven, Technologien, Auswirkungen. Springer, Berlin.

Matzat, L. (2011): Malte Spitz' Vorratsdaten: Der Datensatz unter der Lupe. Online verfügbar unter http://blog.zeit.de/open-data/2011/02/24/vorratsdaten-unter-der-lupe/ (24. Februar 2012).

Maurer-Lambrou, U.; Steiner, A. (2008): Kommentar zu Art. 4 DSG. In: Maurer-Lambrou U., Vogt, N. P. (Hrsg.) (2008): Basler Kommentar zum Datenschutzgesetz, 2. Auflage 2008, S. 3 ff.

McCarthy, C. (2009): Meet Vine, Microsoft's superhero software. Online verfügbar unter http://pownce2.ning.com/profiles/blogs/meet-vine-microsofts-superhero (24. Februar 2012).

Meier, Ph. (2011): À l'impossible nul n'est tenu... sauf Google? In: Medialex 2011, S. 69 ff.

Microsoft Corporation (2011): Microsoft Security Intelligence Report Ausgabe 10 Juli bis Dezember 2010.

Monheim, H.; Monheim-Dandorfer, R. (1990): Strassen für alle: Analysen und Konzepte zum Stadtverkehr der Zukunft. Hamburg: Rasch & Röhring.

Mühlethaler, F.; Arend, M., Axhausen, K., Martens, S., Steierwald, M. (2003): Das vernetzte Fahrzeug – Verkehrstelematik für Strasse und Schiene. Arbeitsdokument des Zentrums für Technologiefolgen-Abschätzung, TA-SWISS, Bern.

Müller, R. (2011): Big Versicherungs-Brother is watching you. Versicherungsjournal.de. Online verfügbar unter http://www.versicherungsjournal.de/versicherungen-und-finanzen/big-versicherungs-brother-is-watching-you-107469.php. (24. Februar 2012).

myspace (2011): Fact Sheet: MySpace Backgrounder. Online verfügbar unter http://www.myspace.com/pressroom/fact-sheet/ (3. April 2011).

Netlog NV (2011): Impressum. Online verfügbar unter http://de.netlog.com/go/about (24. Februar 2012).

netzwelt.de (2011): Facebook, Twitter, MeinVZ und Wer-Kennt-Wen: Soziale Netzwerke: Unterwegs mit Facebook, Twitter und Co. Online verfügbar unter http://www.netzwelt.de/news/85561-soziale-netzwerke-unterwegs-facebook-twitter-co.html (24. Februar 2012).

nextiraone (2011): Mitarbeitende – Das wichtigste Kapital einer Unternehmung Applikationsunterstützte Lokalisierung im Notfall. Kloten. Online verfügbar unter http://www.nextiraone.eu/ch_de/content/download/10349/147798/file/CR_Basler_D.pdf (23. August 2011).

Nielsen Media Research GmbH (2010a): Facebook, Youtube und Wikipedia sind die beliebtesten Social Media Seiten in Europa und in den USA. Online verfügbar unter http://de.nielsen.com/news/NielsenPressemeldung02.02.2010-SocialMediaSites.shtml (24. Februar 2012).

Nielsen Media Research GmbH (2010b): Starke Nutzerzuwächse für Facebook und Twitter im Vorjahresvergleich. Online verfügbar unter

http://de.nielsen.com/news/NielsenPressemeldung05.05.2010-SocialNetworks.shtml

NRC – Natural Resources Canada (2009): Executive Summary. Research Related to Privacy and the Use of Geospatial Information.

NRC – Natural Resources Canada (2010a): Final Report International Comparative Analysis of Geospatial Information Privacy.

NRC – Natural Resources Canada (2010b): Geospatial Privacy Awareness and Risk Management Guide for Federal Agencies.

NZZ – Neue Zürcher Zeitung Online (2008): Breite Videoüberwachung in Tram, Bus und S-Bahn. Online verfügbar unter http://www.nzz.ch/nachrichten/zuerich/breite_videoueberwachung_in_tram_bus_und_s-bahn_1.678987.html (24. Februar 2012).

o. V. (2011b): Sheen will mit Twitter Millionär werden. In: Manager Magazin, 04.03.2011.

Oertel, B.; Wölk, M.; Hilty, L. M.; Köhler, A. (2005): Security Aspects and prospective Applications of RFID systems.

Ozguner, U. (2010): Introduction to Special Issue: Vehicular Wireless Communication Networks for Transportation. Transportation Research Part C, (18), 333–334.

Palma, A. de; Lindsey, R. (2009): Traffic congestion pricing methodologies and technologies. Transportation Research Part C: Emerging Technologies, in Press, Corrected Proof. doi:10.1016/j.trc.2011.02.010.

Pärli, K. (2009): Vertragsfreiheit, Gleichbehandlung und Diskriminierung im privatrechtlichen Arbeitsverhältnis. Stämpfli: Bern.

Pärli, K. (2011): Datenschutz durch Selbstregulierung? Auslegeordnung, Probleme und Regulierungsperspektiven bei Location Based Services. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Parliamentary Office of Science and Technology (2009): Intelligent Transport Systems. postnote, 322.

Paulus, P. (1997): Soziale Netzwerke, soziale Unterstützung und Gesundheit. In: Homfeldt, H. G.; Hünerdorf, G. (Hrsg.): Soziale Arbeit und Gesundheit. Neuwied: Luchterhand, S. 175–203.

PBG – Bundesgesetz über die Personenbeförderung, Bundesversammlung der Schweizerische Eidgenossenschaft 2009.

Peng, C.; Shen, G.; Zhang, Y.; Li, Y.; Tan, K. (2007): BeepBeep: a high accuracy acoustic ranging system using COTS mobile devices.

Petri, T. (2010): Wertewandel im Datenschutz und die Grundrechte. In: Zeitschrift Datenschutz und Datensicherheit-DuD. Volume 34, Number 1 / Januar 2010. Vieweg Verlag, S. 25–29.

Popular Events Online Newspaper (2011): Facebook Game Market to Increase. Online verfügbar unter http://www.popeve.org/2011/04/13/facebook-game-market-to-increase/pov/stockholm/index.html (22. August 2011).

Pro Juventute (2010): Cybermobbing: Täglich suchen Kinder Hilfe bei der nationale Beratungsstelle von Pro Juventute, Pressemitteilung. Online verfügbar unter http://www.projuventute.ch/index.php?id=1362&L=0&tx_ttnews%5Btt_news%5D=283&cHash=16bc61238f0630b09a310c2c5b18f70c (24. Februar 2012).

Probst, Th. (2010): Die Verknüpfung von Personendaten und deren rechtliche Tragweite. In: Epiney A.; Probst, T.; Gammentahler N. (Hrsg.) (2010): Datenverknüpfung – Problematik und rechtlicher Rahmen, Freiburg.

Progressive (2004): Innovative Auto Insurance Discount Program to be Available to 5,000 Minnesotans Progressive To Use Data-Logging Device to Help Drivers Save Money On Auto Insurance.

Purcell, K. (2010): The state of online video. Washington, DC: Pew Research Center 2010. Online verfügbar unter http://pewinternet.org/Reports/2010/State-of-Online-Video.aspx (24. Februar 2012).

Raddatz, P. (2010): Erst der Anfang. Markenartikel, (3), 26–27.

Rapp, P. M. (2007): Mobility Pricing: Kurzfassung Synthesebericht (No. VSS 2005/910). Online verfügbar unter http://www.astra.admin.ch/themen/00901/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDd3x5gmym162epYbg2c_JjKbNoKSn6A-- (24. Februar 2012).

Rapp, P. M.; Jordl, P.; Deuber, M. (2009): Grundlagen für eCall in der Schweiz: Technical and Organisational Basis for eCall in Switzerland (No. VSS 2007/903). Online verfügbar unter http://www.rapp.ch/wAssets-de/docs/trans/fachartikel-referate/2009/dokumente/vss_2007_903_ecall_schweiz.pdf (24. Februar 2012).

Rapp, P. M.; Oehry, B.; Egeler, C. (2007): Mobility Pricing: Synthesebericht (No. VSS 2005/910). Online verfügbar unter http://www.astra.admin.ch/themen/00901/index.html?lang=de&downlo

ad=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDd3x6fmym162epYbg2c_JjKbNoKSn6A-- (24. Februar 2012).

Rebmann, K.; Marconi, D. (2009): Bericht zum Detailkonzept: Mikrozensus Mobilität und Verkehr 2010. (MZMV2010) (No. 11-08.411.3/Ev). Online verfügbar unter http://www.bfs.admin.ch/bfs/portal/fr/index/infothek/erhebungen__quellen/blank/blank/mz/00/02.Document.125892.pdf (24. Februar 2012).

Retscher, G., Kealy, A. (2005): Ubiquitous Positioning Technologies for Intelligent Navigation Systems. In: Papers presented at the 2nd Workshop on Positioning, Navigation and Communication 2005, University of Hannover, Germany, March 17–18, 2005, Hannoversche Beiträge zur Nachrichtentechnik, Band 0.2, Shaker Verlag, S. 99–108.

Rey, L. (2004): Publifocus road pricing. Ein Spiel mit dem kleinsten gemeinsamen Nenner; Bericht eines Mitwirkungsverfahrens. Bern: TA-Swiss.

RFID. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 5. Juni 2011, 18:38 UTC. URL: http://de.wikipedia.org/w/index.php?title=RFID&oldid=89686686 (8. Juni 2011).

Roche, S.; Propeck-Zimmermann, E.; Mericskay, B. (2011): GeoWeb and crisis management: issues and perspectives of volunteered geographic information. GeoJournal, 1-20. doi:10.1007/s10708-011-9423-9.

Rodriguez, M. (2009): 2010 kommt die Videoüberwachung im Tram. Tagesanzeiger Zürich. Online verfügbar unter http://www.tagesanzeiger.ch/zuerich/stadt/2010-kommt-die-Videoueberwachung-im-Tram/story/14836608 (24. Februar 2012).

Rosenthal, D.; Jöhri, Y. (2008): Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich.

Rossnagel, A. (2007): Datenschutz in einem informatisierten Alltag: Gutachten im Auftrag der Friedrich-Ebert-Stiftung. Medien- und Technologiepolitik. Berlin: Friedrich-Ebert-Stiftung.

Roth, P. (2011): Infografik: Facebook Photo Nutzung – 6.000.000.000 Photos auf Facebook pro Monat… Online verfügbar unter http://allfacebook.de/zahlen_fakten/infografik-facebook-photo-nutzung-6-000-000-000-photos-auf-facebook-pro-monat (24. Februar 2012).

Röttger, M. (2010): Pkw schlängelt sich fahrerlos durch Stadtverkehr. Financial Times Deutschland. Online verfügbar unter

http://www.ftd.de/auto/:autonomes-auto-pkw-schlaengelt-sich-fahrerlos-durch-stadtverkehr/50180284.html (24. Februar 2012).

Rouf, I.; Miller, R.; Mustafa, H.; Taylor, T.; Oh, S.; Xu, W.; Gruteser, M.; Trappe, W.; Seskar, I. (2010): Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. In Proceedings of USENIX Security Symposium'2010. S. 323–338. Online verfügbar unter http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf (24. Februar 2012).

Rudin, B. (2008): Das Recht auf Anonymität, Anonymität als Teil der informationellen Selbstbestimmung: wenig geregelte Anwendungsfälle und viel Handlungsbedarf. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich, S. 6–13.

Rudin, B. (2011): Um Dimensionen brisanter: Facebooks Gesichtserkennung. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Rudin, B.; Stämpfli, S. (2009): Wunderheilmittel Videoüberwachung? In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Rungg, A. (2011): Fussgängerzone wird zum Facebook-Revier. Online verfügbar unter http://www.ftd.de/it-medien/medien-internet/:ortsbasierte-werbung-fussgaengerzone-wird-zum-facebook-revier/60005987.html.

Sadeh, N.; Hong, J.; Cranor, L.; Fette, I.; Kelley, P.; Prabaker, M.; Rao, J. (2008): Understanding and Capturing People's Privacy Policies in a People Finder Application. Online verfügbar unter http://www.vs.inf.ethz.ch/events/uc07privacy/papers/01-finder.pdf (24. Februar 2012).

Saeed, R. A.; Khatun, S.; Mohd, B. (2006): Performance of Ultra-Wideband Time-of-Arrival Estimation Enhanced With Synchronization Scheme. Ecti transactions on electrical Eng., Electrionics, and communications, Vol. 4, No. 1:1–7.

Safko, L.; Brake, D. K. (2009): The social media bible: Tactics, tools, and strategies for business success. Hoboken, N.J: John Wiley & Sons.

Sander, R. (2010): «Facebook Orte» ist hier: Deutschland. Online verfügbar unter http://www.stern.de/digital/online/neuer-dienst-places-facebook-orte-ist-hier-deutschland-1610627.html (24. Februar 2012).

Scheffel, U. (2009): [IFA] iNanny: GPS-Routentracker mit Hilferuf. tom's hardware.

Schmidt, H. (2009): Das Web 2.0 erreicht die Gewinnschwelle. Online verfügbar unter http://faz-community.faz.net/blogs/netzkonom/archive/2009/09/28/soziale-netzwerke-naehern-sich-der-gewinnschwelle.aspx (24. Februar 2012).

Schmidt, H. (2011): Mobiles Internet: Das Geschäft mit den Ortsdaten. In: FAZ.net. Online verfügbar unter http://www.faz.net/-01tk5p (24. Februar 2012).

Schmidt, J.-H. (2010): Das neue Netz. Praktiken und Konsequenzen des «Web 2.0». Wiesbaden. Online verfügbar unter http://vhs-wiesbaden.de/fileadmin/images/aktuelles/2010-2_das_neue_netz.pdf (3. April 2011).

Schmiegelow, A.; Milan, M. (2010): Markenführung in sozialen Medien – Neue Wege zum Konsumentenherz. In: Beisswenger, A. (Hrsg.): YouTube und seine Kinder. Wie Online Video, Web TV und Social Media die Kommunikation von Marken, Medien und Menschen revolutionieren. Baden-Baden: Nomos, Edition Reinhard Fischer, S. 105–121.

Schrenk, M. (Hrsg.) (2008): Mobility nodes as innovation hubs: REAL CORP 008; Tagungsband; Tagungsband – proceedings; 13th International Conference on Urban Planning, Regional Development and Information Society; 13. Internationale Konferenz zu Stadtplanung, Regionalentwicklung und Informationsgesellschaft ; May, 19–21 2008, Vienna International Airport, Office Park 3. Schwechat-Rannersdorf: Selbstverl. des Vereins CORP – Competence Center of Urban and Regional Planning.

Schwan, B. (2010): Twitter verkauft User-Daten – Jeder zweite Tweet wird ausgewertet. Online verfügbar unter http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/jeder-zweite-tweet-wird-ausgewertet/ (24. Februar 2012).

Schweizer, R. (2008): Kommentar zu Art. 13 BV. In: Ehrenzeller, B.; Mastronardi, Ph.; Schweizer, R.; Vallender, K. A. (Hrsg.) (2008): Die schweizerische Bundesverfassung, Kommentar, 2. Auflage, Zürich, St. Gallen, Basel, Genf.

Schweizerische Alzheimervereinigung (2010): Leben mit Demenz in der Schweiz – Eckdaten, Schweizerische Alzheimervereinigung, Yverdon-les-Bains.

Schwindt, M. (2009): Fotos mit Geodaten: Geotagging: So vergessen sie nie wieder, wo sie ein Foto gemacht haben. Franzis Verlag.

Seethaler, F. (2008): Entstehungsgeschichte DSG. In: Maurer-Lambrou U.; Vogt, N. P. (Hrsg.): Basler Kommentar zum Datenschutzgesetz, 2. Auflage 2008, S. 3 ff.

SF – Schweizer Fernsehen (2010): Bundesrat fasst «Mobility Pricing» ins Auge. Online verfügbar unter http://www.tagesschau.sf.tv/Nachrichten/Archiv/2010/09/17/Schweiz/Bundesrat-fasst-Mobility-Pricing-ins-Auge (24. Februar 2012).

Siemens Schweiz AG (Hrsg.) (2010): Fast Track. Mobile Stellwerke. Combino bei VBZ. Scuol-Tarasp.100 Jahre Berninabahn. Panorama – Kundenzeitschrift der Siemens Schweiz AG, (2). Online verfügbar unter http://www.google.de/url?sa=t&source=web&cd=1&sqi=2&ved=0CBkQFjAA&url=http%3A%2F%2Fwww.siemens.ch%2Fmobility%2FPanorama_1-10%2Fpdf%2FPanorama_2-10.pdf&rct=j&q=panorama%20siemens%20100%20Jahre%20Berninabahn&ei=lO7kTdXaCMyE-wbMpP21BQ&usg=AFQjCNGTyXazfUEk132ZczQPEYW6iJ_LzQ&cad=rja (24. Februar 2012).

Singer, N. (2011, November 12): Face Recognition Makes the Leap From Sci-Fi. NYTimes.com. Online verfügbar unter http://www.nytimes.com/2011/11/13/business/face-recognition-moves-from-sci-fi-to-social-media.htm?_r=1 (24. Februar 2012).

Sobel, D. (2005): Längengrad: Die wahre Geschichte eines einsamen Genies, welches das grösste wissenschaftliche Problem seiner Zeit löste. Bvt berliner taschenbuch verlag; auflage: 1., aufl. edition.

Som, C.; Hilty, L. M., Köhler, A. R. (2009): The Precautionary Principle as a Framework for a Sustainable Information Society. Journal of Business Ethics 85 (3), S. 493–505.

Som, C.; Hilty, L. M.; Ruddy, T. F. (2004): The precautionary principle in the information society. Human and ecological risk assessment, 10 (5), S. 787–799.

Spiegel Online (2009): MySpace identifiziert 90.000 Sex-Täter. Online verfügbar unter http://www.spiegel.de/netzwelt/web/0,1518,605566,00.html (24. Februar 2012).

Spiegel Online (2011a): Facebook soll 65 Milliarden wert sein. Online verfügbar unter http://www.spiegel.de/wirtschaft/unternehmen/0,1518,749119,00.html (24. Februar 2012).

Spiegel Online (2011b): Google droht Street-View-Stopp in der Schweiz. Online verfügbar unter http://www.spiegel.de/netzwelt/web/0,1518,761964,00.html (24. Februar 2012).

Steen, C. (2008): Das satellitengestützte Mautsystem von Toll Collect in Deutschland. Wissen Heute, 61(2), 4–5.

Steier, H. (2011): Der beste Weg ist das Ziel: TomTom will dank Staudaten Gas geben. NZZ Online. Online verfügbar unter http://www.nzz.ch/nachrichten/digital/wie_tomtom_aus_der_krise_navigieren_will_1.10405893.html (24. Februar 2012).

Stelzel-Morawietz, P. (2010): Wenn das Auto Hilfe ruft. Online verfügbar unter http://www.sueddeutsche.de/auto/notrufsystem-ecall-wenn-das-auto-hilfe-ruft-1.1026695 (24. Februar 2012).

Stelzel-Morawietz, P. (22.11.2010): Notrufsystem eCall: Wenn das Auto Hilfe ruft. sueddeutsche.de.

Stiftung Warentest (2010): Soziale Netzwerke – Datenschutz oft mangelhaft. test, (4), 40–45.

Strassmann, B. (2010): Intelligente Navigation. Mobile Staumelder. Online verfügbar unter http://www.zeit.de/zeit-wissen/2011/01/Navigation-Staumelder-Handy (24. Februar 2012).

T-Mobile (2011): Handyortung kostenlos für alle Mobiltelefone -jetzt beim Handylocator.

Tagesanzeiger Zürich (2010): Videoüberwachung im Cobra-Tram. Online verfügbar unter http://www.tagesanzeiger.ch/zuerich/stadt/Videoueberwachung-im-CobraTram/story/18455052 (24. Februar 2012).

TCS – Touring Club Schweiz (2007): Road Pricing / Strassenzölle: Kritische Würdigung des Berichts des Bundesrat. Online verfügbar unter http://www.tcs.ch/etc/medialib/main/rubriken/der_tcs/politik/pdf/road_pricing.Par.0017.File.tmp/arg_court_de.pdf (24. Februar 2012).

Teege, G. (2001): Geodaten im Internet. Ein Überblick. Informatik_Spektrum, S. 193–206.

Thalmann, A. (2007): Zur Anwendung des schweizerischen Datenschutzgesetzes auf internationale Sachverhalte, Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht (sic), S. 341 ff.

Theissen, S. (2009): Risiken informations- und kommunikationstechnischer (IKT-) Implantate im Hinblick auf Datenschutz und Datensicherheit. Schriften des Zentrums für angewandte Rechtswissenschaft. Band 11. Universitätsverlag Karlsruhe.

Thurm, S.; Kane, Y. I. (2010): Your Apps are watching you. Online verfügbar unter http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html (24. Februar 2012).

Tinnefeld, M.-Th. (2011): Einbrüche der Privatheit im digitalen Netz – Grundprobleme und technologische Ansätze des Grundrechtschutzes, Jusletter 1. September.

TNS Emnid Medien- und Sozialforschung & Radiozentrale (2011): Heimat to go – medial verankert in der Region: Studie zur mobilen Mediennutzung und location based services 2011 von TNS Emnid im Auftrag der Radiozentrale. Online verfügbar unter http://www.radiozentrale.de/site/uploads/tx_rzdownloadfiles/Heimat_to_go_Handout_Ergebnis-Charts.pdf (24. Februar 2012).

TomTom (2010): White paper: How TomTom's HD Traffic and IQ Routes data provides the very best routing – Travel Time Measurements using GSM and GPS Probe Data. Technical report.

Tsai, J. Y.; Kelley, P. G.; Cranor, L. F.; Sadeh, N. (2010): Location-Sharing Technologies: Privacy Risks and Controls. Online verfügbar unter http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf (24. Februar 2012).

Tschofeniga, H.; Arumaithuraib, M.; Schulzrinnec, H.; Abobad, B. (2010): How secure is the next generation of IP-based emergency services architecture? International Journal of Critical Infrastructure Protection, (3), 41–50.

Twitter (2010): Twitter for Business. Online verfügbar unter http://business.twitter.com/ (24. Februar 2012).

Twitter (2011): Ein paar Zahlen zu Twitter. Online verfügbar unter http://www.twitter-welt.ch/2011/05/ein-paar-zahlen-zu-twitter/

uber die festlegung der merkmale des europäischen elektronischen mautdienstes und seiner technischen komponenten: 2009/750/eg.

Using Position-Aware Market Mechanisms. In: Lingner, S.; Lutterbeck, B.; Pallas, F. (Hrsg.) (2010): Die Zukunft der Räume. Gesellschaftliche Fragen auf dem Weg zur «Ambient Intelligence». Graue Reihe, Nr. 50

UVEK (2010): Zukunft der internationalen Infrastrukturnetze der Schweiz: Bericht des Bundesrats. Online verfügbar unter http://www.uvek.admin.ch/themen/02536/02545/02549/index.html?download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdn19fmym162epYbg2c_JjKbNoKSn6A--&lang=de (24. Februar 2012).

VCS – Verkehrs-Club der Schweiz (2008): Roadpricing: Positionspapier des VCS Kanton Bern. Online verfügbar unter http://www.vcs-be.ch/fileadmin/user_upload/Sektion_Bern/Roadpricing_Pos-pap.pdf (24. Februar 2012).

Versicherungsmagazin (2009): Versicherer treten bei Neuentwicklung auf die Kostenbremse. Online verfügbar unter http://www.versicherungsmagazin.de/Aktuell/Nachrichten/195/12084/Versicherer-treten-bei-Neuentwicklung-auf-die-Kostenbremse.html (24. Februar 2012).

Videoüberwachungsverordnung ÖV (2009): Verordnung vom 4. November 2009 über die Videoüberwachung im öffentlichen Verkehr, Schweizerischer Bundesrat.

Virtuelles Datenschutzbüro (2011): «Identified» - Menschenscoring und -rating für die Arbeitsplatzsuche in den USA. Online verfügbar unter http://www.datenschutz.de/news/alle/detail/?nid=5224 (24. Februar 2012).

Watzlawick, P.; Beavin, J. H.; Jackson, D. D. (1996): Menschliche Kommunikation. Formen, Störungen, Paradoxien. Bern, Göttingen, Toronto, Seattle: Hans Huber.

Weber, R. (2011): Der Ruf nach einem Recht auf Vergessen. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich, S. 102ff.

Weber, R. H.; Fercsik Schnyder, O. (2009): Was für 'ne Sorte von Geschöpf ist euer Krokodil? -Zur datenschutzrechtlichen Qualifikation von IP-Adressen. sic!, S. 577–589.

Weichert, T. (2007): Der Personenbezug von Geodaten. Datenschutz und Datensicherheit -DuD, 31(1):17–23.

Weichert, T. (2009): Der Fall «Street View» in Deutschland. «Street View» in Mitteleuropa: ein unüberwindbarer Konflikt oder bloss der schwierige Beginn einer langen Freundschaft? In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Weichert, T. (2009): Geodaten – datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen. Datenschutz und Datensicherheit – DuD, 33(6), S. 347–352.

Weichert, T. (2011): Identified – Menschenscoring und -rating für die Arbeitsplatzsuche in den USA. Virtueles Datenschutzbüro, 20.11.2011. Online verfügbar unter: http://www.datenschutz.de/news/alle/detail/?nid=5224 (24. Februar 2012).

Weigert, M. (2011): Ein Meilenstein für Facebook Credits. Online verfügbar unter http://netzwertig.com/2011/01/25/1-juli-2011-ein-meilenstein-fuer-facebook-credits/ (24. Februar 2012).

Weigert, M. (2011): Pendant zu Facebook Places: Die VZ-Netzwerke integrieren friendticker. Online verfügbar unter http://netzwertig.com/2011/04/19/pendant-zu-facebook-places-die-vz-netzwerke-integrieren-friendticker/ (24. Februar 2012).

Weinberg, T. (2010): Social media marketing: Strategien für Twitter, Facebook & Co. Beijing [u.a.]: O'Reilly. Online verfügbar unter http://www.worldcat.org/oclc/594193034 (24. Februar 2012).

Wermelinger, A. (2005): GPS-Überwachung von Mitarbeitenden. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Werner, M. (2011): Datenschutz in ortsbasierten Diensten. In: digma – Zeitschrift für Datenrecht und Informationssicherheit. Schulthess Juristische Medien AG, Zürich.

Wessel, S. (2006): DSRC. Dedicated Short Range Communications.

Wex, F.; Bodenstein, Ch.; Neumann, D. (2010). Coordinating Emergency Response. : Using Position-Aware Market Mechanisms. In: Lingner, S.; Lutterbeck, B.; Pallas, F. (Hrsg.) (2010): Die Zukunft der Räume: Gesellschaftliche Fragen auf dem Weg zur «Ambient Intelligence», Graue Reihe Nr. 50. Europäische Akademie Bad Neuenahr-Ahrweiler.

Wiedemeier, J. (2010): Datenschutzaspekte bei der Nutzung von Geodaten. Datenschutzkonforme Gestaltung von Allgemeinen Geschäftsbedingungen (AGB) bei der Nutzung von Geodaten durch Unternehmen. Bachelorarbeit, Universität Zürich.

Worldometers – World statistics uploaded in real time (2011): Society & Media: Internet users in the world. Online verfügbar unter http://www.worldometers.info/ (24. Februar 2012).

Xing AG (2011): Geschäftsbericht 2010. Online verfügbar unter http://corporate.xing.com/fileadmin/user_upload/XING_AG_jahresergebnisse_2010.pdf (24. Februar 2012).

Xing AG (2011): Online verfügbar unter http://corporate.xing.com/no_cache/deutsch/unternehmen/xing-ag/ (24. Februar 2012).

Zanetti, M.; Vodoz, V.; Oberli, R. (2008): Lösungsansätze zur Erfassung der Routenwahl mittels Geokodierung während CATI Befragungen. Online verfügbar unter http://www.bfs.admin.ch/bfs/portal/it/index/themen/11/22/lexi.Document.111163.pdf (24. Februar 2012).

Zeit Online (2011): Navi-Hersteller TomTom verkauft Nutzerdaten an den Staat. Online verfügbar unter http://www.zeit.de/digital/datenschutz/2011-04/navi-polizei-radarfalle (24. Februar 2012).

Zenger, Y. (2010): Der digitale Tod 2.0. In: Heimspiel 3/10.

Zenz, M.; Fritsche, W. (2009): Auf den Punkt genau: Arbeitssicherheit gewinnen durch Personenortung. CAV Nr. 11. Leinfelden-Echterdingen: Konradin, S. 14–15.

Zepf, M. (2000): Urbanität und öffentlicher Raum: Gedanken zu einem integrierten Planungsansatz. DISP, (141), 35–43.

Zogg, J.-M. (2007): Woher kommt der Notruf?: Standortbestimmung im Schweizer Mobilfunknetz. Bulletin SEV/VSE, (21), 16–20. Online verfügbar unter http://www.bulletin-online.ch/uploads/media/article_115496.pdf (3. April 2011).

Verzeichnis der Projektbeteiligten

Projektleitung TA-Swiss:

Dr. Sergio Bellucci
Geschäftsführer TA-Swiss

Nadia Ben Zbir, lic. phil.
Wissenschaftliche Mitarbeiterin

Projektgruppe:

Prof. Dr. Lorenz M. Hilty (Projektleitung)
Institut für Informatik, Universität Zürich, und Abteilung Technologie und Gesellschaft, Empa, St.Gallen

Britta Oertel, M. A.
Institut für Zukunftsstudien und Technologiebewertung gem. GmbH, Berlin

Michaela Wölk, M. A.
Institut für Zukunftsstudien und Technologiebewertung gem. GmbH, Berlin

Prof. Dr. Kurt Pärli
Leiter Zentrum für Sozialrecht, Zürcher Hochschule für Angewandte Wissenschaften ZHAW, Winterthur

Weitere Mitarbeitende:

Patrizia Huber, B. A.
Studentische Hilfskraft, Institut für Informatik, Universität Zürich

Melanie Studer
School of Management and Law, Zürcher Hochschule für Angewandte Wissenschaften ZHAW, Winterthur

Verzeichnis der Begleitgruppen-mitglieder

Dr. Bruno Baeriswyl
Datenschutzbeauftragter des Kantons Zürich, TA-SWISS-Leitungsausschuss (Präsident der Begleitgruppe)

Florence Bettschart
Fédération Romande des Consommateurs (FRC), Lausanne

Dr. Erwan Bigan
Swisscom Innovation Competence Center, Swisscom (Schweiz) AG, Bern

Alain Buogo
Bundesamt für Landestopografie swisstopo, Wabern

Dr. Christine Giger
Giger GeoIT, Embrach

Prof. Dr. Gudela Grote
ETH Zürich, Arbeits- und Organisationspsychologie, Zürich

Dr. Jessica Heesen
Internationales Zentrum für Ethik in den Wissenschaften, Eberhard Karls Universität Tübingen

Dr. Rainer Humbel
Bundesamt für Statistik, Neuenburg

Thomas Kallweit
FELA Management AG, Diessenhofen

Dr. Francisco Klauser
Geografie Institut, Universität Neuenburg

Dr. Michael Kocheisen
Swisscom Innovation Competence Center, Swisscom (Schweiz) AG, Bern

Ulrich Lattmann
Schweizerische Akademie der Technischen Wissenschaften (SATW), Zürich

Urs Luther
Bundesamt für Strassen (ASTRA), Bern

Dr. Franziska Meister
Die Wochenzeitung, Zürich

Cyrill Osterwalder
Google Schweiz, Zürich

Hans Kaspar Schiesser
Verband öffentlicher Verkehr, Bern

Philipp Stüssi
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, Bern

Prof. Dr. Rolf H. Weber
Zentrum für Informations- und Kommunikationsrecht, Universität Zürich, Zürich

Dr. Franz Zeller
Bundesamt für Kommunikation (BAKOM), Biel

Verzeichnis der Fachgesprächspartner

Martin Boess
Geschäftsleiter SKP, Schweizerische Kriminalprävention, Bern

Nino Cozzio
Direktor Soziales und Sicherheit, Stadt St. Gallen

Martin Hermida
Produktentwicklung Medien & Konsum, Stiftung Pro Juventute

Andreas Knöpfli
Präsident SWICO, Der Wirtschaftsverband für die Digitale Schweiz, Schaffhausen

Michael Laux
VBZ, Verkehrsbetriebe Zürich

Simon Stöckli
Vertretungsberechtigter Geschäftsführer Reputationmanagers, Dishy! AG, Zug

Glossar

Ambient Intelligence	«Umgebungsintelligenz». Technikvision, nach der die Alltagsumgebung die Handlungen der Menschen erkennt und unterstützend darauf reagiert, z.B. Beleuchtung und Heizung durch Anwesenheit reguliert werden oder die Wohnung den Gesundheitszustand ihrer Bewohner einschätzen kann. Die Grenzen zu ↑Pervasive Computing und ↑Ubiquitous Computing sind fliessend.
Augmented Reality	«erweiterte Realität». Verfahren, bei dem die Wahrnehmung der Realität durch zusätzlich eingeblendete Informationen ergänzt wird, beispielsweise kann eine Kamera mit Ortungsfunktionen die Namen von Sehenswürdigkeiten ins Bild einblenden; eine digitale Arztbrille könnte das Röntgenbild des Patienten auf dessen Körper projizieren; Fahrerassistenzsysteme können Navigations- und Verkehrsinformationen in die Windschutzscheibe einblenden; die Spezialbrille eines Kundenberaters könnte in Zukunft Name, Alter und geschäztes Einkommen einer Kundin einblenden, wenn diese den Laden betritt.
Biometrischer RFID-Pass	Pass, der biometrische Daten enthält, die verwendet werden, damit die Identität des Passinhabers überprüft werden kann. Diese Daten sind auf einem passiven ↑RFID-Transponder gespeichert, damit sie kontaktlos ausgelesen werden können.
Bluetooth	Industriestandard für die drahtlose Datenübertragung zwischen Geräten über kurze Distanz.
Cookie	Ein Datensatz, der von einem Webserver zum Browser des Nutzers gesendet und dort gespeichert wird, damit der Server beim nächsten Besuch der Website erkennen kann, dass es sich um den gleichen

	Browser (und damit häufig um die gleiche Person) handelt, die auf die Website zugreift. Dadurch ist es z.B. möglich, Sitzungen fortzusetzen, die Website an bestimmte Nutzerinnen anzupassen oder deren Verhalten zu beobachten.
Crowdsourcing	Lösung einer Aufgabe durch zahlreiche Internet- oder Mobilfunknutzer, die freiwillig daran mitwirken.
Data Mining	Systematische Anwendung von Auswertungsmethoden auf einen Datenbestand mit dem Ziel, darin neue Muster zu entdecken.
Endgerät	In der Informationstechnik und der Telekommunikationstechnik ein Gerät, welches an einen Netzanschluss eines öffentlichen oder privaten Daten- oder Telekommunikationsnetzes angeschlossen ist, z.B. ein Telefon oder ein mit dem Internet verbundener Computer. *Mobile* Endgeräte verbinden sich drahtlos mit dem jeweiligen Netz.
Engpassortung	Identifikation von Objekten, wenn sie Kontrollpunkte passieren, z.B. mit Hilfe von ↑RFID-Transpondern.
Feldstärke	Stärke eines elektromagnetischen Feldes an einem gegebenen Punkt. Die Feldstärke nimmt mit zunehmender Entfernung von seinem Ursprung (z.B. einer Sendeantenne) ab und kann deshalb auch als Mass für den Abstand von der Antenne verwendet werden.
Funkzelle	Zelle in einem ↑zellularen Netzwerk.
Funkzellenortung	Ortung eines mobilen ↑Endgeräts aufgrund der ↑Funkzelle, in der es sich aktuell befindet.
Geokodierung	Bestandteil der Georeferenzierung. Dabei werden Daten ohne Georeferenz in ein gewünschtes Referenzsystem (Koordinatensystem) transformiert. Ein Beispiel ist das Adresskodieren: dabei werden geometrisch-topologische Beziehungen des Strassennetzes mit den Hausnummernbereichen der Strassen

	verrechnet. Jeder Adresse wird dann ein Geocode in Form von Koordinaten zugewiesen.
Geolokalisierung	Ortung eines Objekts auf der Erdoberfläche; im Kontext dieser Studie synonym zu ↑Ortung.
Geotag	Satz von Metadaten (Daten über Daten), der geographische Information über die Daten mitliefert, wie z.B. bei Bildaten den Ort der Aufnahme. Dabei werden üblicherweise Längen- und Breitengrad sowie ein Zeitstempel gespeichert, aber auch zusätzliche Informationen wie Land, Ortsnamen oder Höhe über Meer können in einem Geotag enthalten sein.
Hotspot	↑WLAN-Hotspot.
Infrarot-Ortung	Ein Verfahren, das Gegenstände oder Personen aufgrund der von ihnen ausgesandten Infrarotstrahlung lokalisiert.
Kuppe-/Dome-Kamera	Video-Überwachungskamera, die in eine Halbkugel (Kuppel) aus transparentem, getöntem Kunststoff eingebaut ist. Anders als bei konventionellen Überwachungskameras ist die «Blickrichtung» des Objektivs von aussen nicht oder nur schwer zu erkennen.
Location Privacy	Die Möglichkeit, den eigenen Aufenthaltsort vor anderen geheim zu halten, sowohl bezogen auf den aktuellen als auch auf frühere Aufenthaltsorte.
Lokalisierungsdaten	↑Ortungsdaten.
Maut	Strassenbenutzungsgebühr.
Mautbrücke	Eine über einer mautpflichtigen Strasse aufgestellte Schilderbrücke, die zur automatischen Abrechnung der ↑Maut dient oder die Bezahlung derselben kontrolliert.

Mobile Advertising	Werbung, die den Kunden auf mobilen ↑Endgeräten erreicht und den lokalen Kontext berücksichtigt. Bestandteil des Location-Based Marketing.
Mobile Couponing	Versenden von Coupons über das Mobiltelefon, wobei der Herausgeber einer ausgewählten Personengruppe gegen Vorlage eines Coupons einen Vorteil wie z.B. einen Rabatt oder eine kostenlose Zugabe gewährt.
Mobile Ticketing	Mobile Tickets ersetzen Eintrittskarten, Fahrscheine oder andere bisher übliche Belege durch einen auf ein Handy oder ein ähnliches Gerät gesendeten und dort gespeicherten Datensatz.
Onboard-Unit (OBU)	In ein Fahrzeug eingebautes Gerät, das während der Fahrt Daten aufzeichnet. Enthält in der Regel ein GPS-Modul und zeichnet Position, Fahrtrichtung und Geschwindigkeit des Fahrzeugs mit Datum und Uhrzeit auf.
Ortung	Feststellung des Ortes, an dem sich eine Sache oder eine Person befindet, mit technischen Mitteln. Der Ort ist genau genommen kein geometrischer Punkt, sondern eine Fläche oder ein Volumen, auf die/das der Aufenthaltsort des Objekts durch Ortung eingeschränkt werden kann. Je kleiner diese Fläche bzw. das Volumen, desto genauer die Ortung.
Ortungsdaten	Durch ↑Ortung gewonnene Daten, Ergebnis der Ortung.
Pay as you drive	Ein Typ von Auto-Haftpflichtversicherung, bei der die Prämienhöhe aus der Art der tatsächlichen Fahrzeugnutzung errechnet wird.
Pay-per-Risk-Modell	Prämienmodell von Versicherungen, das sich an Risikofaktoren ausrichtet und beispielsweise bei KfZ-Versicherungen Fahrverhalten, Zeit und Ort der Fahrt (Stadtteil, Strassentyp) sowie weitere mittels Ortungstechnologien gewonnene Daten berücksichtigt.

Pay-per-Use-Modell	Geschäftsmodell, bei dem Nutzer möglichst exakt für die tatsächlich erfolgte Nutzung einer Leistung oder Infrastruktur bezahlen, wobei der Preis der Nutzung auch von der Qualität abhängig sein kann (im Verkehr z.B. die Nutzung von Fahrzeugen, Fahrspuren, Erste-Klasse-Waggons).
Peripheriegerät	An einen Computer angeschlossenes Gerät, das diesen mit der Aussenwelt verbindet (z.B. Maus, Tastatur, Monitor, Mikrofon, Lautsprecher, Drucker, CD-Laufwerk).
Pervasive Computing	«Rechnerdurchdringung». Technikvision, nach der Alltagsgegenstände von untereinander drahtlos vernetzten Computern durchdrungen werden und alle Alltagshandlungen wie z.B. die Benutzung von Werkzeugen, Möbeln oder Räumen Daten erzeugen bzw. durch «smarte» Dinge optimiert werden. Die Grenzen zu ↑Ubiquitous Computing und ↑Ambient Intelligence sind fliessend.
Piconetz	Netzwerk von Geräten, die sich über den Funkstandard ↑Bluetooth zum Datenaustausch verbunden haben.
Positionsbestimmung	Ursprünglich nur Selbstortung, wird heute weitgehend als Synonym für ↑Ortung (Selbst- oder Fremdortung) verwendet (vgl. Abschnitt 2.2.1).
Privacy-Filter	Physische und softwaregestützte Einrichtung zum Schutz von vertraulichen oder privaten Informationen.
«Recht auf Vergessen»	Forderung u.a. der EU-Kommission, dass Nutzer jederzeit und selbstbestimmt ihre persönlichen Daten löschen können, insbesondere die Daten, die sie selbst im Internet ablegen.
RFID	Radio Frequency Identification, Identifikation durch Radiofrequenzsignale. ↑RFID-Transponder.

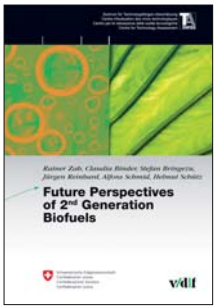
RFID-Transponder	Preisgünstiger ↑Transponder, der i.d.R. auf ein Trägerobjekt aufgebracht wird, damit dieses durch die drahtlose Abfrage digitaler Daten automatisch identifiziert werden kann.
Robinsonliste	Datenbank, in die sich Privatpersonen eintragen lassen können, die keine adressierte Werbung in ihren Briefkasten zugestellt bekommen möchten. Die Liste umfasst ungefähr 100 000 Haushalte in der Schweiz.
Software-Schlüssel	Alphanumerischer Code, der von Anwendungsprogrammen bei der Installation oder Anmeldung abgefragt wird.
Spam	Unerwünschte, unverlangt zugestellte Nachrichten mit meist werbendem Inhalt, in der Regel in elektronischen Medien.
Spoofing	Verschleierung der Identität, insbesondere um den Empfänger einer Nachricht über den Absender zu täuschen.
Telematikbox	↑Onboard-Unit.
Transponder	(Kunstwort aus *Trans*mitter und Res*ponder.*) Ein Gerät, das ein Funksignal automatisch beantwortet, um seine Anwesenheit (und in vielen Fällen auch seine Identität und weitere Daten) bekannt zu geben. Heute werden fast ausschliesslich ↑RFID-Transponder eingesetzt.
Triangulation	Im Kontext der Ortung die Bestimmung eines unbekannten Eckpunktes eines Dreiecks aus zwei bekannten Eckpunkten sowie zwei Winkeln oder zwei Entfernungen zum unbekannten Punkt.
Trusted Third Party	«vertrauenswürdige dritte Partei». Eine dritte Instanz, der zwei Parteien vertrauen.
Ubiquitous Computing	«Rechnerallgegenwart». Technikvision, nach der vernetzte Rechenleistung überall und jederzeit unauffällig zur Verfügung steht, Computer also allgegen-

	wärtig sind. Die Grenzen zu ↑Pervasive Computing und ↑Ambient Intelligence sind fliessend.
Ultraschall-Ortung	Verfahren, das Gegenstände oder Personen aufgrund der von ihnen ausgesandten oder reflektierten Ultraschallwellen lokalisiert (Prinzip der Fledermaus).
WLAN	Drahtloses lokales Datennetz. WLANs werden häufig für den mobilen Zugang zum Internet verwendet.
WLAN-Hotspot	Zugangspunkt für drahtlosen Zugang zum Internet für ↑WLAN-fähige Endgeräte wie Laptops oder Smartphones, der (in der Regel gegen Bezahlung) allgemein zugänglich ist.
Zellulares Netzwerk	Ein drahtloses Netzwerk, das in Zellen eingeteilt ist, für die jeweils eine Sende-/Empfangsstation (Basisstation) zuständig ist.

Weitere Publikationen von TA-SWISS

Rainer Zah, Claudia Binder, Stefan Bringezu, Jürgen Reinhard, Alfons Schmid, Helmut Schütz

Future Perspectives of 2nd Generation Biofuels



2010, 328 Seiten, zahlr. Grafiken und Tabellen, durchg. farbig, Format 16 x 23 cm, broschiert
ISBN 978-3-7281-3334-2
auch als eBook erhältlich

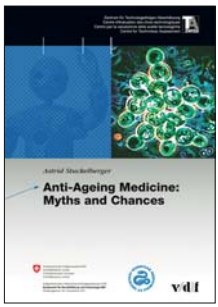
Martin Möller, Ulrike Eberle, Andreas Hermann, Katja Moch, Britta Stratmann

Nanotechnologie im Bereich der Lebensmittel

2009, 228 Seiten, zahlreiche Tabellen und Grafiken, Format 16 x 23 cm, broschiert
ISBN 978-3-7281-3234-5
auch als eBook erhältlich

Astrid Stuckelberger

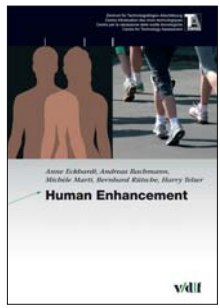
Anti-Ageing Medicine: Myths and Chances



2008, 328 Seiten, zahlreiche, z.T. farbige Abb. und Grafiken, Format 16 x 23 cm, broschiert
ISBN 978-3-7281-3195-9
auch als eBook erhältlich

Anne Eckhardt, Andreas Bachmann, Michèle Marti, Bernhard Rütsche, Harry Telser

Human Enhancement



2011, 300 Seiten, zahlreiche Abbildungen und Tabellen, Format 16 x 23 cm, broschiert
ISBN 978-3-7281-3396-0
auch als eBook erhältlich

vdf Hochschulverlag AG an der ETH Zürich, Voltastrasse 24, VOB D, CH-8092 Zürich
Tel. +41 (0)44 632 42 42, Fax +41 (0)44 632 12 32, verlag@vdf.ethz.ch, www.vdf.ethz.ch

www.ta-swiss.ch

Ein Kompetenzzentrum der
Akademien der Wissenschaften Schweiz

Immer mehr Alltagshandlungen hinterlassen Datenspuren, die darüber Auskunft geben, wo wir uns aufgehalten haben und mit wem wir in Verbindung stehen. Ob wir mobil telefonieren, auf das Internet zugreifen, von einer Videokamera erfasst werden, ein Foto auf eine Internetplattform hochladen, mit einem Chip eine Tür öffnen oder bargeldlos bezahlen: Fast immer entstehen dabei Daten, die sich zu Bewegungsprofilen zusammenfügen lassen und Rückschlüsse auf unsere Lebenssituation zulassen.

Neben der Satellitenortung durch GPS gibt es mehr als ein Dutzend Technologien, die indirekt die Ortung von Personen zulassen. Welche gesellschaftlichen Chancen und Risiken resultieren aus der Verbreitung dieser Technologien? Wer kann, wer darf unter welchen Bedingungen Ortungsdaten erfassen, speichern, verarbeiten, weitergeben oder löschen? Welche Massnahmen können Bürgerinnen und Bürger, Unternehmen und der Gesetzgeber ergreifen, um dem Missbrauch von Ortungsdaten vorzubeugen und eine rechtsstaatliche, demokratische Nutzung der Ortungstechnologien zu fördern?

Das Buch untersucht die Situation in der Schweiz und berücksichtigt dabei Entwicklungen zum Datenschutz in der Europäischen Union und im Europarat.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ufficio federale delle strade USTRA

Ufficio federale di statistica UST

Ufficio federale di topografia swisstopo

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Strassen ASTRA

Bundesamt für Statistik BFS

Bundesamt für Landestopografie swisstopo

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral des routes OFROU

Office fédéral de la statistique OFS

Office fédéral de topographie swisstopo

Zürcher Hochschule für Angewandte Wissenschaften
zh aw School of Management and Law

EMPA
Materials Science & Technology

Universität Zürich[UZH]
Institut für Informatik

IZT
Institut für Zukunftsstudien und Technologiebewertung
Institute for Futures Studies and Technology Assessment

TA-SWISS 57/2012

ISBN 978-3-7281-3460-8 (Print)
ISBN 978-3-7281-3477-6
DOI-NR. 10.3218/3477-6

vdf