forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

FORUM PRIVATHEIT UND SELBSTBESTIMMTES LEBEN IN DER DIGITALEN WELT

White Paper

DAS VERSTECKTE INTERNET

ZU HAUSE – IM AUTO – AM KÖRPER

White Paper

DAS VERSTECKTE INTERNET

ZU HAUSE – IM AUTO – AM KÖRPER

Redaktion:
Michael Friedewald[1], Murat Karaboga[1], Peter Zoche[1]

Autorinnen und Autoren:
Murat Karaboga[1], Tobias Matzner[2], Tina Morlok[7], Fabian Pittroff[5], Maxi Nebel[4], Carsten Ochs[5], Thilo von Pape[3], Julia Victoria Pörschke[8], Philip Schütz[1], Hervais Simo Fhom[6]

(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(2) Universität Tübingen, Internationales Zentrum für Ethik in den Wissenschaften (IZEW)
(3) Universität Hohenheim, Lehrstuhl für Medienpsychologie, Stuttgart
(4) Universität Kassel, Institut für Wirtschaftsrecht
(5) Universität Kassel, Fachgebiet Soziologische Theorie
(6) Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt
(7) Universität München, Institut für Wirtschaftsinformatik und Neue Medien (WIM)
(8) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel

Herausgeber:
Peter Zoche, Regina Ammicht Quinn, Marit Hansen, Jessica Heesen, Thomas Hess, Jörn Lamla, Christian Matt, Alexander Roßnagel, Sabine Trepte, Michael Waidner

Inhalt

1 Einleitung ... 3
1.1 Das „versteckte Internet“ ... 3
1.2 Fallauswahl ... 4

2 Das versteckte Internet zu Hause ... 5
2.1 Räumliche Privatheit ... 5
2.2 Erwartungshaltung der Nutzer ... 6
2.3 Smart Home ... 7
2.3.1 Smart TV: Technologie und Funktionsweise ... 7
2.3.2 Welche Daten fallen bei der Nutzung von Smart TVs an? ... 9
2.4 Rechtliche Rahmenbedingungen ... 10
2.5 Privatheitsrisiken und Überwachungspotenziale ... 12

3 Das versteckte Internet im Auto ... 13
3.1 Privatheit in der Öffentlichkeit ... 13
3.2 Erwartungshaltung der Nutzer ... 13
3.3 Smart Cars ... 14
3.3.1 Technologie und Funktionsweise ... 14
3.3.2 Welche Daten fallen bei vernetzten Fahrzeugen an? ... 15
3.4 Rechtliche Rahmenbedingungen ... 17
3.5 Privatheitsrisiken und Überwachungspotenziale ... 18

4 Das versteckte Internet am Körper ... 20
4.1 Privatheit in der Interaktion ... 20
4.2 Erwartungshaltung der Nutzer ... 21
4.3 Wearables ... 22
4.3.1 Smartwatches und intelligente Armbänder: Technik und Funktionsweise ... 23
4.3.2 Smartglasses: Technik und Funktionsweise ... 24
4.3.3 Welche Daten fallen bei Smartwatches und intelligenten Brillen an? ... 25
4.4 Rechtliche Rahmenbedingungen ... 26
4.5 Privatheitsrisiken und Überwachungspotenziale ... 28
4.5.1 Smartglasses ... 28
4.5.2 Smartwatches und intelligenter Armbänder ... 29

5 Schlussdiskussion ... 31
5.1 Zusammenfassung ... 31
5.2 Gestaltungspotenziale und Herausforderungen ... 32

Anmerkungen ... **36**

Anhang ... 48
Glossar ... 48
Abkürzungsverzeichnis ... 50

1
Einleitung

1.1 Das „versteckte Internet“

Computer sind effiziente Rechenmaschinen. Aber Computer sind auch Schreibgeräte, spielen Musik und Videos ab, sie sind Telefone und Adressbücher, Spielzeug und Steuerzentrale ganzer Fertigungshallen. Aus der Sicht der Informatik rechnen Computer auch, wenn sie Musik spielen, Termine speichern oder den Eintritt in virtuelle Welten ermöglichen. Denn all das funktioniert auf der Basis mathematischer Verfahren. Wir gehen mit diesen Rechenmaschinen für gewöhnlich aber nicht als Rechenmaschinen um. Wir denken nicht, dass wir ein Rechengerät benötigen, das eine digitale Abstraktion von Musik wieder in analoge Signale umrechnet, wenn wir Musik hören wollen – sondern wir greifen zum MP3-Spieler. Genauso wie Menschen einfach ins Auto steigen und losfahren, ohne sich groß Gedanken über die Funktionsweise des Motors oder der Servolenkung zu machen.

Dies sind Beispiele dafür, dass es auf jede Technologie, auf jedes Gerät oder Artefakt mehrere Sichtweisen gibt. Sie hängen davon ab, welche Rolle die Technologie in unseren täglichen Handlungen spielt. Sie sind nicht „richtig“ oder „falsch“, sondern parallel und verschieden. Auf Computer gibt es die Sicht der Programmierung, der Herstellung und diejenige der vielen Nutzungsweisen. Auf Autos gibt es etwa die Sicht der Fahrer, der Mechaniker oder der Verkehrsleitstellen. Das heißt, die Eigenschaften oder die Bedeutung einer Technologie können nicht erschlossen werden, wenn man diese isoliert als Gerät oder Artefakt betrachtet. Nur im Zusammenhang mit den Menschen, die sie nutzen, dem Ort und dem gesellschaftlichen Kontext ihres Einsatzes ist dies möglich.

Wenn wir im Folgenden über das „versteckte Internet“[1] sprechen, bezieht sich dies auf den Umstand, dass Computer seit einiger Zeit immer stärker in Geräte integriert werden, die nicht als Computer wahrgenommen werden und deren Funktionalität zunehmend bestimmen. Da diese Geräte meist auch über das Internet mit anderen Geräten oder einem Dienstleister kommunizieren, spricht man auch vom „Internet der Dinge“.[2]

Die Computerfunktionalitäten und Kommunikationsfähigkeit wird jeweils aus ganz bestimmten Sichtweisen erkennbar. Oft ist das in den hier diskutierten Fällen nicht die Sichtweise der Nutzer. Insbesondere liegt das daran, dass aus bestimmten Perspektiven Veränderungen an einer Technik vorgenommen werden können, die aus anderen Perspektiven nicht auffallen: Ein elektrisches Auto fährt sich mehr oder minder gleich wie ein benzinbetriebenes. Und erst recht gilt das für ein Auto, das allerlei Daten sammelt und diese über eine Internetverbindung an verschiedenste Stellen übermittelt. Die Tastatur am Smartphone bedient sich nach wie vor gleich, auch wenn inzwischen Eingaben unmittelbar an Internetdienstleister oder Hersteller übertragen werden, damit diese eine automatische Textergänzung anbieten können.[3]

Diese Unsichtbarkeit von technischen Veränderungen und Funktionalitäten – und eben auch der Einführung von netzbasierten Funktionen – ist oft gewollt. Nutzerfreundlichkeit bedeutet gerade, dass aus Sicht der Anwender die Dinge genauso verwendet werden können wie zuvor. Allerdings haben manche Veränderungen für die Anwender unerwartete Auswirkungen. Im Fall des versteckten Internets betrifft das ganz zentral die Privatheit der Anwender selbst sowie die Privatheit anderer Menschen, mit denen sie direkt oder indirekt technisch verbunden sind. Deshalb beruht ein wichtiger Ansatz einer sozialwissenschaftlichen, ethischen und politischen Beurteilung von Technik darauf, diese Sichtweisen untereinander abzugleichen und zu überprüfen, welche Aspekte, die sich in der einen Perspektive eröffnen, auch in anderen – und insbesondere derjenigen der Anwender – verfügbar sein sollten. Wenn auf diese Weise klar wird, dass internetbasierte Funktionen wahrnehmbar sein sollten, aber nicht sind, wird aus der

normalen Verschiedenheit der Sichtweisen ein problematisches Verstecken. Dieses White Paper leistet einen Beitrag, solche Defizite zu überwinden.

1.2 Fallauswahl

Das vorliegende White Paper konzentriert sich auf drei konkrete Anwendungsbereiche digital vernetzter Technik. Betrachtet werden das eigene Zuhause (Smart Home am Beispiel Smart TV), das Fahrzeug (Smart Car) sowie neuartige Endgeräte, die direkt am Körper (Wearables) getragen werden können.[4] In diesen drei Kontexten sind zahlreiche Geräte und Anwendungen bereits erfolgreich am Markt vertreten. Neben den von den Herstellern und Betreibern beworbenen Vorteilen bergen sie aber in der Regel auch potenzielle Gefahren für die Privatheit, auf die im Folgenden eingegangen wird.[5]

Die Vision des „vernetzten Hauses" und des „intelligenten Wohnens" wurde bereits seit Mitte der 1990er Jahre propagiert, die Technik fand aber aus unterschiedlichen Gründen zunächst wenig Verbreitung.[6] Dies scheint sich mit der Verbreitung von drahtlosen Netzwerken und Endgeräten wie Smartphones, Tablets und insbesondere Fernsehgeräten mit Internetverbindung mittlerweile zu ändern.[7] Solche „intelligenten" Fernsehgeräte (Smart TVs) ersetzen zunehmend den Gebrauch herkömmlicher Fernseher.[8] Eine vollständige Vernetzung von Unterhaltungselektronik, Haustechnik und Haushaltsgeräten ist allerdings auch in absehbarer Zukunft nicht zu erwarten.[9]

Neben dem häuslichen Umfeld kommen internetbasierte Anwendungen auch in Fahrzeugen vermehrt zum Einsatz und versprechen dort erhöhte Sicherheit und zusätzlichen Komfort für die Fahrer.[10] Marktforschungsunternehmen prognostizieren, dass die Vernetzung von Fahrzeugen (Smart Car) in Zukunft zum Standard werden wird.[11] Bis 2020 könnte ein Großteil der neu verkauften Fahrzeuge bereits digital vernetzt sein.[12] Zahlreiche neuere Fahrzeugmodelle beinhalten nicht nur Parkassistenten und Bremshilfen. Fahrer können zudem gezielt Informationen aus dem Internet abrufen. Als besonders zukunftsträchtig gelten Anwendungen, bei denen das Fahrzeug Informationen mit anderen Fahrzeugen, aber auch mit der Infrastruktur austauscht.[13] Solche Anwendungen sollen u. a. dazu beitragen Staus zu vermeiden, den Benzinverbrauch zu reduzieren oder multimodale Verkehrsangebote zu ermöglichen. Darüber hinaus können auch alle über das Internet verfügbaren Unterhaltungs- und Informationsmöglichkeiten im Auto (für die Passagiere) verfügbar gemacht werden.

Auch bei Wearables hat das Produktangebot in den vergangenen Jahren deutlich zugenommen. Immer mehr Anbieter bringen derzeit Fitnessarmbänder oder sog. Smartwatches auf den Markt, die mit Sensoren ausgestattet und mit dem Internet verbunden sind. Durch das dauerhafte Tragen am Körper werden nicht nur mehr, sondern auch reichhaltigere Daten generiert, die für neue Anwendungen genutzt werden. So können viele dieser Produkte den Puls des Trägers oder das Schlafverhalten genau messen.[14] Häufig sind diese Produkte für sportlich aktive Nutzer konzipiert und unterstützen den Trend zur „Selbstvermessung".

Dieser Beitrag liefert Hintergrundinformationen zu den Funktionalitäten und den rechtlichen Rahmenbedingungen für eine Auswahl an Technologien, die in den drei Anwendungsbereichen momentan stark positioniert sind. Darauf aufbauend werden mögliche Implikationen und Gefahren für die Privatheit der Nutzer dieser Technologien aufgezeigt.

2
Das versteckte Internet zu Hause

2.1
Räumliche Privatheit

Die lokale Privatheit[15] im Sinne abgegrenzter, den Blicken, dem Einfluss und dem Zugriff nicht-autorisierter Akteure entzogener Räumlichkeiten kann geradezu als Inbegriff der Alltagsvorstellungen von Privatheit gelten. Nicht zuletzt schimmert die räumliche Vorstellung von Privatheit noch im weit verbreiteten Begriff der „Privatsphäre" durch, und es ist sicherlich auch kein Zufall, dass Jürgen Habermas' Klassiker „Strukturwandel der Öffentlichkeit" die Entstehung der bürgerlichen Öffentlichkeit in der Privatsphäre der Salons der Privatwohnungen lokalisierte, in denen die zum Publikum versammelten Privatleute vom Eingriff der öffentlichen Gewalt abgeschirmt debattierten.[16] Jenseits solcher sozialhistorischen Überlegungen gilt indes grundsätzlich, dass soziale Akteure in der Privatwohnung als „bloße Privatpersonen", und damit als Teil der privaten Nutzungspraktiken agieren.[17] Darüber hinaus weist sowohl die Soziologie als auch die Sozialpsychologie[18] und die klassische Privatheitstheorie[19] der räumlichen Form der Privatheit eine ganze Reihe normativer Funktionen zu, die von liberalen Vorstellungen der Entfaltung des Individuums bis zum Funktionieren demokratischer Gemeinwesen reichen.[20]

Weniger normativ aufgeladen stellt die Soziologie in Rechnung, dass Raum (und Zeit) im sozialen Alltagsleben grundsätzlich in Zonen unterteilt wird, welche einsehbar, zugänglich oder zugreifbar sind, und solche, die vor Sichtbarkeit, Zugang oder Eingriffen geschützt sind.[21] Beispielsweise finden sich im Kaufhaus, im Restaurant, auf dem Amt, in der Schule, in der Wohnung – buchstäblich überall – „Vorder- und Hinterbühnen"[22], d. h. öffentliche Bereiche, auf denen die sozialen Inszenierungen des Alltagslebens erfolgen, welche von privaten Rückzugsbereichen abgesondert werden. In diesem Sinne lässt sich eine Allgegenwärtigkeit räumlicher Privatheit in der Alltagspraxis vermerken, die ihrerseits in einer Zentralstellung der räumlichen Privatheitsvorstellung in den wissenschaftlichen und alltäglichen Privatheitsdiskursen resultiert.[23] Nichtsdestotrotz dürfte das isolierte Abstellen auf die räumliche Dimension unter den gegenwärtigen soziotechnischen Bedingungen selbst für den Fall der Privatheit der eigenen vier Wände zu kurz greifen; oder pointiert: Bei räumlicher Privatheit geht es nicht nur um die Begrenzung von Raum, vielmehr stellt letzteres ein Vehikel für eine Vielzahl von Grenzziehungen dar. Analytisch lassen sich in dieser Hinsicht vier Dimensionen unterscheiden:

- Erstens in *visueller Hinsicht*, sofern die Akteure in der Privatheit der eigenen Wohnung die Erwartung hegen, unbeobachtet zu bleiben.

- Zweitens in *materieller Hinsicht*, denn die materiellen Dinge der Privatwohnung sind vor handfesten Zugriffen sowohl durch die öffentliche Gewalt (z. B. Wohnungsdurchsuchung) als auch durch Dritte (z. B. Diebstahl) geschützt.

- Drittens in *informationeller Hinsicht*, indem die Privatwohnung es ermöglicht, dass Informationen nicht „die eigenen vier Wände verlassen" – oder zumindest besteht i. Allg. diese Erwartung.

- Und viertens soll die Wohnung vor bestimmten ungewollten *sinnlichen Wahrnehmungen* abschirmen, z. B. Schutz vor Autolärm oder -abgasen bieten.

Ohne hier vorgreifen zu wollen, kann festgehalten werden, dass die im Rahmen des White Papers untersuchten Technologien vor allem die Frage aufwerfen, inwiefern die

Bezeichnung des Raums der eigenen Wohnung als „privat" zukünftig noch in informationeller Hinsicht angemessen sein wird.

2.2 Erwartungshaltung der Nutzer

Indem Kommunikationstechnik Menschen vernetzt, verleiht sie den Situationen, in denen sie verwendet wird, einen spezifischen sozialen Rahmen – den „Medienrahmen".[24] Dieser ergänzt jenen Rahmen, der das Miteinander der gerade anwesenden Personen beschreibt. So kann ein Radio Menschen, die alleine sind, in einen geselligen Rahmen versetzen, und ein Fernseher kann das Zusammensein einer Familie am Samstagabend wie ein Lagerfeuer verstärken. Jugendliche können sich aber in dieser Situation auch mittels ihres Smartphones bewusst dem familiären Miteinander entziehen indem sie z. B. über den Kopfhörer Musik hören oder sich etwa durch eine Chat-App in die Mitte ihrer Freunde versetzen lassen. Wie diese Beispiele schon zeigen ist Kommunikationstechnik folglich auch ein Mittel, um den im Rahmen der häuslichen Situation gegebenen Grad an Privatheit „nachzusteuern".

Zu einer Gefahr für Privatheit in der eigenen Wohnung kann Kommunikationstechnik werden, wenn die vom Medienrahmen erzeugte Privatheit nicht mit dem übereinstimmt, was die Nutzer davon erwarten. Diese Gefahr ist nicht neu, sie tritt immer dann auf, wenn die Dynamik des technischen Wandels das Vorstellungsvermögen der Nutzer überfordert. Ein Beispiel sind die sog. „Party-Lines" aus der Frühzeit des Telefons im 19. Jahrhundert. Erst schlechte Erfahrungen lehrten manchen Nutzer, dass der Medienrahmen des scheinbar vertraulich „von Haus zu Haus" geführten Dialogs technisch auch Dutzende andere einbezog, die diskret mithören konnten.[25]

Solche Rahmentäuschungen sind sogar ein viel verwendetes Prinzip beim Entwurf neuer Medien bzw. deren Benutzungsschnittstelle, wobei der Rückgriff auf Altbekanntes einerseits den Zugang der Nutzer erleichtert, aber auch neuartige Funktionsweisen verschleiert.[26] Dieser Wahrnehmung kommt häufig noch die Vermarktung der Technik entgegen, z. B. indem sie die zwischen Computer und Fernseher positionierten hybriden Geräte als *Smart TV* bezeichnet und wie Fernseher designt, bewirbt, verkauft und einrichten lässt, anstatt etwa von Fernsehcomputern zu sprechen. Dass Smart TVs und Internetradios keine reinen Empfangsgeräte mehr sind, sondern einen regen Datenfluss in beide Richtungen gewährleisten, wird von der Mehrzahl der Nutzer nicht erwartet und daher auch nicht problematisiert oder eingeschränkt.[27]

Im äußersten Fall sind die Nutzer sich gar nicht bewusst, durch die Nutzung einer Technik überhaupt in einen Medienrahmen eingebunden zu sein. Auch für solche Rahmentäuschungen könnte das Smart Home viel Anlass bieten, wenn klassisch überhaupt nicht als Kommunikationsgeräte wahrgenommene Objekte wie Thermostate, Glühbirnen und Waschmaschinen mit dem Internet verbunden werden.

Auch wenn solche Täuschungen den Nutzern mittelfristig bewusst sein sollten, können sich daraus noch weitere Herausforderungen für den Schutz von Privatheit ergeben. Bei der Einbindung von kommunikationsfähiger Technik in den Haushalt ist mittelfristig nämlich zu beobachten, dass die Medienrahmen und die sozialen Rahmen unterschiedlicher Orte und Situationen des Haushalts einander gegenseitig prägen. Die zunächst „wilde" Technik wird „domestiziert", also wie ein Tier an die häuslichen Umgangsformen gewöhnt, aber sie prägt dabei auch die häuslichen Strukturen.[28] Dies ist bei digitalen Medien gut zu beobachten. So waren vor zehn Jahren Geräte mit Prozessoren noch weitgehend auf Arbeitszimmer beschränkt und strahlten dort mit ihrem Gebläse, den Kabeln, Datenspeichern und Peripheriegeräten eine wenig wohnliche Atmosphäre aus. Schlafzimmer waren aus diesen Gründen fast frei von elektronischen Medien.[29] Heute tritt Computertechnik in so diskreten bis ausgemacht attraktiven Formen in Erscheinung, dass sie etwa als Wi-Fi-Lautsprecher vornehmlich in den Repräsentations- und Wohnräumen zuhause sind oder in Form von E-Readern, Tablets oder digitalen Bilder-

rahmen auch direkt neben den Nutzern im Schlafzimmer nächtigen dürfen. Von dort aus prägen sie ihrerseits auch den sozialen Rahmen der häuslichen Privat- und Intimsphäre.[30]

2.3 Smart Home

„Smart Home" ist ein Sammelbegriff für die Vernetzung verschiedener Geräte im häuslichen Bereich aus der sich die Möglichkeit zur Kommunikation der Geräte untereinander sowie komplexe Möglichkeiten der (Fern-)Steuerung einzelner Geräte ergeben. Smart Home-Systeme lassen sich in verschiedene Kategorien einteilen: Durch den Begriff der *Gebäude- oder Hausautomation* werden die fest am Haus installierten Einrichtungen wie Außen- und Innensensoren (z. B. Lichtmesser oder Bewegungsmelder), per Smartphone oder Webinterface fernsteuerbare Alarmanlagen, Rollläden, Einfahrt- und Garagentore, Außen- und Innenbeleuchtungssysteme und Heizungsthermostate zusammengefasst. Ein weiterer Aspekt von Smart Home bezieht sich auf *Smart Metering* als Bezeichnung von intelligenten Strom-, Wasser- oder Gaszählern. Im Innenbereich der Wohnung werden Smart TVs, vernetzte Spielekonsolen und Multimediacenter durch den Begriff *Home Entertainment* zusammengefasst. Schließlich bildet *Ambient Assisted Living* als Beschreibung von Assistenzsystemen, die z. B. durch tragbare und miniaturisierte Sicherheits- und medizinische Kontrollsysteme ein eigenständig geführtes Leben im fortgeschrittenen Alter oder bei gesundheitlichen Einschränkungen ermöglichen sollen, einen weiteren Bereich von Smart Home.[31]

Exemplarisch wird im Folgenden auf Smart TV als eine ausgewählte Technologie im Umfeld des Smart Home eingegangen.

2.3.1 Smart TV: Technologie und Funktionsweise

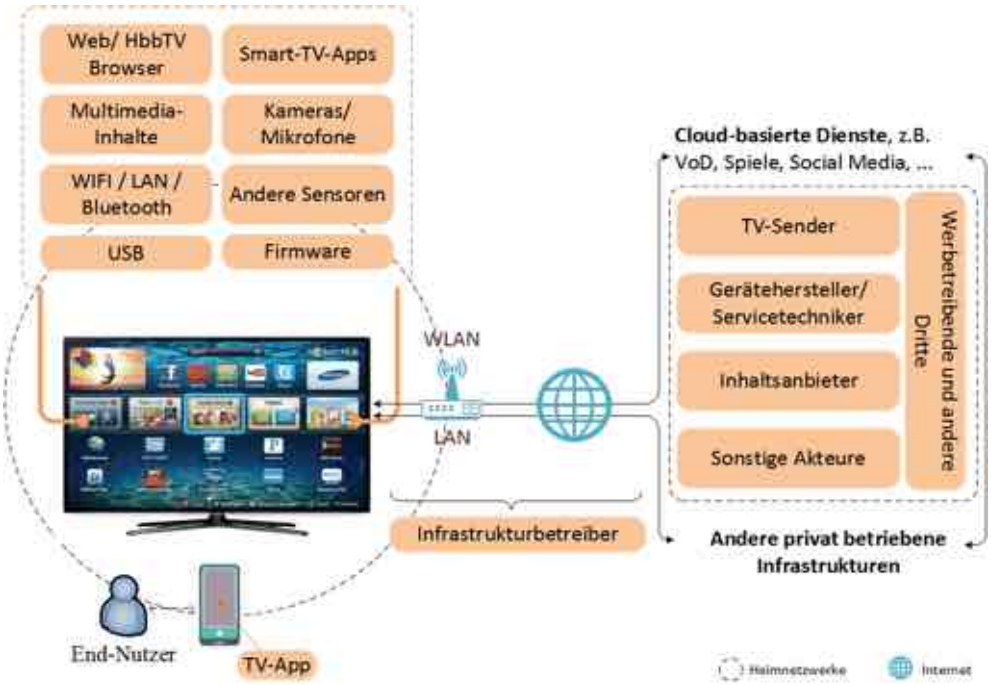
Die fortwährende Technologieentwicklung in den Bereichen Sensorik und Funknetzen ermöglicht in zunehmendem Maße die Vernetzung verschiedener Geräte im Haushalt.[32] Diese Geräte haben die Möglichkeit, Daten aus dem Internet zu empfangen und zu verarbeiten, mit anderen Smart Home-Geräten zu kommunizieren sowie aus dem Internet oder dem lokalen Netzwerk ferngesteuert oder kontrolliert zu werden. Diese Entwicklung ist besonders deutlich am Beispiel von Unterhaltungselektronik wie internetfähigen Set-Top-Boxen, Spielekonsolen, Blu-Ray-Playern oder modernen Fernsehgeräten zu sehen. Herzstück eines solchen Schrittes ist das Smart TV, also Fernsehgeräte, die mithilfe von Computertechnik zusätzliche Funktionen und Schnittstellen wie Internetanschluss, USB- sowie Speicherkarten-Ports in einem Gerät integrieren und mit weiteren im Heimnetzwerk angeschlossenen elektronischen Geräten Daten austauschen können. Neben dem Empfang von Rundfunksignalen können auch interaktive (sender- bzw. programmbezogene) Inhalte und Dienste aus dem Internet empfangen und dargestellt werden. Beim sog. Hybrid Broadcast Broadband TV (HbbTV) können Medieninhalte aus dem Internet zur laufenden Sendung oder damit verbundene Inhalte aus einer Mediathek zur Verfügung gestellt werden. Darüber hinaus bietet ein Smart TV die Möglichkeit im Internet zu surfen, Videos anzuschauen, Musik zu hören oder Video-Telefonie zu betreiben (vgl. Abb. 01).[33]

Technische Ausstattung

Anders als bei konventionellen Geräten, können moderne Fernseher über ihre LAN- oder WLAN-Schnittstelle direkt mit dem Internet verbunden werden, ohne dass ein zusätzlicher Computer oder eine Set-Top-Box angeschlossen werden muss. Ähnlich wie mobile Endgeräte sind moderne Smart TVs vernetzte Plattformen, die mit leistungsstarken Prozessoren sowie z. T. eingebauten Steuerungs- und Bewegungssensoren bestückt sind. Dazu gehören neben Mikrofon und Kamera zunehmend auch Näherungs-,

Temperatur-, Licht-, und Luftfeuchtigkeitssensoren. Diese stellen bi-direktionale Kanäle zur Verfügung, die neue Formen der Gerätebedienung (z. B. Sprach- und Gestensteuerung) ermöglichen: Vom Sofa aus und ohne Fernbedienung kann der Zuschauer mit einer Handbewegung den Fernseher an- und ausschalten. Dank Gesichts- und Stimmerkennung ist es möglich festzustellen, wer zuschaut, personalisierte Inhalte zu empfehlen oder die Benutzungsschnittstelle des Fernsehers individuell anzupassen. Darüber ist die Personalisierung die Grundlage für eine Beteiligung von Nutzern am TV-Programm und für Anwendungen wie Voice Chat oder soziale Netzwerke.

Abb. 01 Smart TV: Akteure und Architekturkomponenten



HbbTV-Standard

Die Verknüpfung von Rundfunk mit interaktiven Online-Diensten auf Smart TV-Geräten ist mit gängigen Web-Technologien möglich. Prominentes Beispiel ist der offene internationale Standard HbbTV.[34] HbbTV war ursprünglich eine pan-europäische Initiative zur Harmonisierung der Rundfunk- und Breitbandbereitstellung von Multimediainhalten durch internetfähige Fernseher. Mittlerweile wird der HbbTV-Standard über Europa hinaus als ernsthafte Alternative bzw. Ergänzung bestehender Rundfunkstandards betrachtet.[35] HbbTV eröffnet die Möglichkeit, neben linearem Fernsehen (herkömmliches Programmfernsehen), den Zuschauern per Knopfdruck sowohl zusätzliche Web-basierte Medienangebote (z. B. Programminformationen, Wetterberichte, Teletext etc.) zum laufenden und zukünftigen Programm, als auch On-Demand Dienste zur Verfügung zu stellen. Anbieter von HbbTV-Diensten und -Inhalten sind entweder die jeweiligen Fernsehanstalten oder die so genannten Entertainment Provider (z. B. Online-Videotheken wie Netflix). Für die Werbetreibenden und TV-Sender besteht die Möglichkeit, völlig neue Geschäftsmodelle für interaktives Fernsehen zu etablieren.[36]

Erweiterbare Plattform

Die Integration von Web-Technologien in das Fernsehen ermöglicht einen Zugriff auf Inhalte des World Wide Web, typischerweise sowohl durch einen (z. T. rudimentären) Web-Browser als auch durch unterschiedliche Anwendungen wie etwa Musik-Player, E-Mail, Spiele, Social Media, VoIP-Dienste oder Online-Banking. Web-Browser und andere

Anwendungen werden dem Nutzer in Form von Apps zur Verfügung gestellt. Ähnlich wie auf Smartphones, bieten Apps die Möglichkeit zur Erweiterung der Funktionalität eines Smart TV-Gerätes. Die meisten Fernsehgerätehersteller betreiben einen eigenen App-Store und bieten i. d. R. Apps für iOS oder Android-Geräte an. Dies ermöglicht u. a. eine Echtzeit-Synchronisierung zwischen den Smart TVs und einer mobilen App auf dem Smartphone oder Tablet („Second-Screen-Ansatz").[37]

Moderne Smart TVs gelten dementsprechend zunehmend als Multimedia-Center, die externe Kommunikations- und Fernsehdienste mit anderen intelligenten elektronischen Haushaltsgeräten bündeln können. Indes ist mehr als ein Fünftel der Smart TV-Nutzer in Unkenntnis über die Internetfunktionalität, und fast die Hälfte der Nutzer ist nur unzureichend über die Möglichkeiten von HbbTV als Schnittstelle zwischen Fernsehen und Internet informiert.[38]

2.3.2 Welche Daten fallen bei der Nutzung von Smart TVs an?

Bei der Verwendung eines Smart TVs wird eine Vielzahl von Daten erfasst, zum großen Teil ohne dass dies für den Nutzer erkennbar ist. Ein Teil dieser Daten sind personenbeziehbar oder gar personenbezogen. Zu diesen sensiblen Daten gehören:

Konto- und Registrierungsdaten

Einige Dienste auf Smart TVs erfordern eine Online-Registrierung des Gerätes oder ein Nutzerkonto bei den in Frage kommenden Diensten. Für das Tätigen von Einkäufen bei Home-Shopping-Sendern können sich Nutzer bereits heute einen Home-Shopping-Account anlegen. Beim Verknüpfen des Smart TV-Geräts mit einem Account erheben die jeweiligen Diensteanbieter verschiedene persönliche Daten wie z. B. Name, Geburtsdatum, Geschlecht, Adresse und ggf. Zahlungsinformationen der Nutzer. Darüber hinaus werden ggf. Benutzername und Kennwort für den wiederholten Zugriff auf einen Dienst im Speicher des Smart TVs abgelegt. Eine Nutzung des Smart TV ist zwar normalerweise auch ohne Registrierung möglich; die Verwendung vieler Dienste, die das Potenzial des Smart TV wirklich erschließen, erfordern aber meist eine Registrierung.

Nutzungs- und Fernsehverhaltensdaten

Bei der Verwendung des Smart TVs fallen Nutzungsdaten an. Diese ermöglichen einen Einblick in die von den Nutzern auf dem Fernseher aktivierten Inhalte, Apps bzw. Dienste sowie über die den Nutzern zur Verfügung stehende TV-Kanäle. Auf diese Weise lässt sich dann das Fernsehverhalten ermitteln: Welche TV-Programme werden wann und wie lange angesehen, nach welchen Begriffen wird gesucht, welche Inhalte genutzt, wie wird Werbung rezipiert: Bei der Nutzung bestimmter audiovisueller Inhalte bzw. non-linearer Online-Medien wird erfasst, welche Steuerungsaktionen (z. B. Play, Stop, Pause, Fast Forward etc.) genutzt wurden. Diese Daten werden kontinuierlich erfasst, gespeichert und ggf. über das Internet an Inhalte- und Diensteanbieter oder auch den Gerätehersteller übermittelt.

Auch bei HbbTV werden Nutzungsdaten erfasst und typischerweise schon mit Beginn der HbbTV-Nutzung an den Sender übermittelt. Über automatisierte Abfragen ermitteln einige Fernsehsender zudem detaillierte Informationen darüber, wie lange ein Zuschauer diesen Sender betrachtet hat. Bei einigen Fernsehsendern kommen auch Google Analytics oder andere Dienste zur Datenverkehrsanalyse zum Einsatz, die eine akkurate Verfolgung von Nutzeraktivitäten ermöglichen und sich vom Nutzer nicht abstellen lassen.[39] Über Cookies kommunizieren Smart TVs zusätzlich mit den Geräteherstellern und erlauben, trotz täglich neu zugewiesener IP-Adressen die eindeutige Identifikation eines Geräts. Noch bezieht sich diese Identifizierbarkeit lediglich auf das

Gerät und besitzt somit noch keinen unmittelbaren Personenbezug, dieser lässt sich jedoch durch einen Abgleich mit Nutzerkonten (s. o.) herstellen.[40]

Zwei weitere Typen von Nutzungsdaten sind Daten über das Browsing-Verhalten bzw. die Browsing-Historie der Zuschauer und die durch Smart TV-Sensoren erfassten Foto-, Audio- und Videoaufnahmen von Hausbewohnern und Besuchern. Aus den Sensordaten können u. U. biometrische Daten, wie Gesichtsgeometrie abgeleitet werden. Sie werden zunehmend genutzt, um das Fernsehen, z. B. durch Gesichts- bzw. Stimmerkennung stärker zu personalisieren.[41]

Gerätspezifische Daten

Zu den gerätespezifischen Daten, die erfasst werden können zählen u. a. der Name des Geräteherstellers, die Modellbezeichnung und ggf. Version des Geräts sowie der Typ und die Version des Betriebssystems oder der Firmware. Hinzu kommen Details über die Art der Netzwerkschnittstelle bzw. Netzwerkverbindung (WLAN, LAN, Bluetooth), die Netzwerkadresse (MAC- bzw. IP-Adresse) des Fernsehgerätes, Informationen über eingebaute Sensoren und ggf. der eindeutige Fernsehgeräte-Identifier („Unique Device ID").

Bei HbbTV-fähigen Geräten können auch die HbbTV-Einstellungen abgefragt und übermittelt werden (z. B. die Version des genutzten HbbTV-Standards und der HbbTV-Status). Weitere gerätspezifische Daten sind Angaben über die über das Heimnetzwerk mit dem Smart TV-Gerät verbundenen elektronischen Geräte inklusive der Zugangsdaten.

Ableitbare Daten

Eine Auswertung des Nutzungs- und Fernsehverhaltens erlaubt unter Umständen Rückschlüsse auf die politische Einstellung, Hobbys, Bildungsgrad, oder den ethnischen Hintergrund des Zuschauers. Darüber hinaus lassen sich anhand der Smart TV-Sensordaten und gerätspezifischer Daten Rückschlüsse auf den Familienstatus sowie Gewohnheiten in der unmittelbaren Umgebung des Fernsehgerätes (z. B. im Wohn- oder Schlafzimmer) ziehen. Die Auswertung des Browserverlauf und ggf. Korrelationen mit Konto- bzw. Registrierungsdaten können dazu verwendet werden, um weitere Persönlichkeitsmerkmale und private Attribute der Zuschauer – wie etwa sexuelle Orientierung bzw. Vorlieben – zu gewinnen. Aus der Interpretation der gerätspezifischen Daten und Netzwerkadresse des Fernsehers können Details über den Standort des Gerätes und damit des Zuschauers gewonnen werden. Dritte, etwa Werbetreibende oder Nachrichtendienste, können auf diese Weise nicht nur die Fernseh- und Nutzungsgewohnheiten der Zuschauer ausforschen, sondern auch diese gezielt überwachen.

2.4 Rechtliche Rahmenbedingungen

Die Wohnung ist der elementare Lebensraum und Mittelpunkt menschlicher Existenz.[42] Daher unterliegt sie dem besonderen verfassungsrechtlichen Schutz des Art. 13 GG, der ihre Unverletzlichkeit gewährleistet. Sie dient als absolut geschützter Eigenbereich der freien Entfaltung der Persönlichkeit.[43] Vom Schutzbereich umfasst ist die räumliche Sphäre der Wohnung, die der allgemeinen Zugänglichkeit durch eine räumliche Abschirmung entzogen und zur Stätte privaten Lebens und Wirkens gemacht wird.[44]

Vernetzte Haustechnologie eröffnet die Möglichkeit, das in der Wohnung stattfindende Privatleben aufzuzeichnen und so in den geschützten Eigenbereich vorzudringen. Unabhängig von dem durch Art. 13 GG gewährten Schutz sieht das Grundgesetz in bestimmten Fällen eine weitere, speziellere grundrechtliche Garantie vor, die das Individuum vor Angriffen auf Haustechnologien bewahrt: Smart Home-Technologien stellen

sog. eigengenutzte, informationstechnische Systeme dar. Kernmerkmal jener informationstechnischer Systeme ist es, dass sie allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erstellen.[45] Die Vertraulichkeit und Integrität derartiger Systeme wird durch das sog. Computergrundrecht geschützt, welches das Bundesverfassungsgericht 2008 aus dem allgemeinen Persönlichkeitsrecht hergeleitet hat.[46] Kommuniziert das Haussystem mit Systemen außerhalb der Wohnung, wird die Vertraulichkeit dieser Kommunikation nach außen durch das Fernmeldegeheimnis aus Art. 10 GG geschützt. Im Herrschaftsbereich der Wohnung unterliegen personenbezogene Daten zudem der informationellen Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

Von der konkreten Gestaltung des Systems ist es abhängig, ob das entsprechende System als ein Telemediendienst einzustufen ist. Voraussetzung ist, dass es eigene Inhalte wie Informations- und Kommunikationsdienste generiert und diese sinnlich wahrnehmbar darstellt. Besteht die Funktion nur in der Übertragung von Signalen über Telekommunikationsnetze, handelt es sich um einen Telekommunikationsdienst. Auch Mischsysteme sind denkbar, je nach Ausgestaltung kommt dann das Telemedien- (TMG) oder Telekommunikationsgesetz (TKG) zur Anwendung.[47] Soweit weder das TMG noch das TKG Anwendung finden, wird die Rechtmäßigkeit der Verarbeitung personenbezogener Daten nach den Datenschutzgesetzen des Bundes bzw. der Länder beurteilt.

Grundsätzlich besteht die Möglichkeit, dass der private Nutzer in seinen Rechten verletzt wird, z. B. indem ohne sein Wissen durch den Diensteanbieter Daten über sein Nutzungsverhalten verarbeitet werden. Darüber hinaus ist es aber auch denkbar, dass private Nutzer haftbar sind für Verletzungen der Rechte Dritter, wie z. B. von Gästen. Auf Privatpersonen sind in der Regel weder die Normen des TMG noch des TKG anwendbar. Beide Gesetze wenden sich ausschließlich an „Anbieter". Unter diesen Begriff fällt derjenige, der etwa einen Smart TV in seinem Wohnzimmer stehen hat und ihn bestimmungsgemäß nutzt, gerade nicht.[48]

Jedoch wird die Zulässigkeit der bei der Nutzung des Systems anfallenden Daten durch den Telemediendiensteanbieter bzw. den Telekommunikationsdiensteanbieter nach TMG bzw. TKG beurteilt. Bestandsdaten nach § 14 TMG bzw. § 95 TKG sind solche Daten, die zur Begründung, Ausgestaltung und Änderung eines Vertragsverhältnisses erforderlich sind. Dazu gehören Name, Kontaktdaten und Zahlungsinformationen des Nutzers. Je nach spezifischem Dienst können aber auch weitere Daten zur Ausgestaltung des Dienstes unerlässlich sein. Nutzungs- und Verkehrsdaten nach § 15 TMG bzw. § 96 TKG dürfen nur dazu verwendet werden, um die Inanspruchnahme des Dienstes zu ermöglichen und abzurechnen. Diese Daten sind auf die konkrete Nutzung oder Sitzung bezogen, etwa IP-Adressen, Cookies, Systeminformationen, oder aber Daten über Beginn und Ende der jeweiligen Nutzung. Die Einordnung ist stark abhängig von der konkreten Funktion des Dienstes oder Systems. Je mehr ein System mit Nutzern interagiert oder auf ihre Bedürfnisse reagiert, desto mehr Daten sind erforderlich, um den Dienst zu erbringen, die damit in die Kategorie der Nutzungs- bzw. Verkehrsdaten fallen. Alle übrigen anfallenden Daten sind sog. Inhaltsdaten; deren Zulässigkeit der Verarbeitung richtet sich nach §§ 28 ff. BDSG, etwa für eigene Geschäftszwecke.

2.5 Privatheitsrisiken und Überwachungspotenziale

Verlust oder Einschränkung der Entscheidungsfreiheit

Mit dem Einzug von Smart TVs in Haushalte dringt die datenbasierte Kommunikation über das Internet noch stärker in private Lebensbereiche ein. Doch da weder die Gerätehersteller noch die Fernsehanstalten historisch stark in der Datenschutztradition verankert sind, hat dies in Bezug auf Privatheitsrisiken ganz konkrete Implikationen: Wie verschiedene Skandale in der Vergangenheit aufgezeigt haben, werden ohne deren Wissen Daten über die Nutzer[49] gesammelt und über das Internet an Fernsehsender, Gerätehersteller und sonstige Inhaltsanbieter oder Werbetreibende übertragen. Damit geht ein Verlust oder eine Einschränkung der Entscheidungsfreiheit über die Weitergabe der bei der Fernsehnutzung entstehenden Daten einher.[50]

Intransparenz der (kommerziellen) Datenverarbeitung

Mit der Erweiterung des klassischen Fernsehers um Smart TV-Funktionen erschließt sich für Werbetreibende, Gerätehersteller, Fernsehanstalten und Konsumforscher eine Flut von potenziell wertvollen Nutzungsdaten. Wohin die Entwicklung gehen könnte, zeigt die Auswertung und Vermarktung der Lesegewohnheiten von E-Book-Lesern sowie der Nutzungsgewohnheiten von Video-on-Demand-Nutzern. Was wird wie lange, wie schnell gelesen oder angesehen? Wann wird das Programm am häufigsten pausiert oder abgebrochen? Über die Auswertung dieser Daten versprechen sich die unterschiedlichen Akteure besser vermarktbare Produkte zu schaffen. Ob dabei der Nutzen bei besseren Produktangeboten oder höheren Profiten liegt, muss an dieser Stelle offen bleiben und kann in der Regel aufgrund intransparenter unternehmensinterner Prozesse auch nicht nachvollzogen werden.

Tracking und Profilbildung

Durch Tracking und Profilbildung wird anonymes Fernsehen zunehmend unmöglich. Die Erweiterung des Fernsehers um Sensoren, wie Mikrofone und Kameras führt dazu, dass neben dem Smart TV-Besitzer und den im Haushalt lebenden Personen zudem auch weitere Besucher aufgezeichnet und per Gesichtserkennung identifiziert werden können. Dies wirft ähnlich wie bei Smartglasses (vgl. Kapitel 4) ganz neue Fragen im Umgang mit derartigen Technologien auf. Anders als bei Smartglasses bleibt eine öffentliche Diskussion hier bislang aus und so wächst die Zahl der Smart TV-Geräte in Haushalten beständig weiter.

Überwachung der Zuschauer sowie das Risiko einer Offenlegung vertraulicher Daten und Identitätsdiebstahl

Über die Privatheitsrisiken hinaus eröffnen technische Schwachstellen Angriffsmöglichkeiten auf Smart TVs.[51] Mit solchen Angriffen lassen sich eine Reihe von umfangreichen Überwachungsaktivitäten realisieren: Eine viel beachtete Untersuchung unterschiedlicher Smart TV-Modelle der Firma Samsung hat 2013 gezeigt, dass vorinstallierte Web-Anwendungen wie Skype oder Facebook von Angreifern gezielt manipuliert werden können, um die im Smart TVs eingebauten Webcams und Mikrofone für den Nutzer unbemerkt zu aktivieren. Solche Schwachstellen bieten Möglichkeiten zur Abschöpfung vertraulicher Daten, zu Identitätsdiebstahl sowie zur Massenausspähung von Bürgern.[52]

Kritikwürdig ist derweil, dass zwar einige Gerätehersteller und Fernsehanstalten nach dem Bekanntwerden von Sicherheitslücken und problematischen Datenübertragungen inzwischen – teils mit erheblichen Verzögerungen – Nachbesserungen vorgenommen haben, andere jedoch weiterhin Daten sammeln.[53]

3
Das versteckte Internet im Auto

3.1 Privatheit in der Öffentlichkeit

Im Alltagsverständnis wird oft mit einem dichotomischen Verständnis von Öffentlichkeit und Privatheit operiert; alles, was nicht dem privaten Bereich zuzuordnen ist, wird dann „der Öffentlichkeit" zugeschlagen. Insbesondere mit Blick auf die räumliche Privatheit findet eine solche Dichotomie üblicherweise Anwendung.[54] Dem zugrunde liegenden Denken zufolge müsste es sich auch beim Autofahren im öffentlichen Raum um öffentliche Praktiken handeln. Demgegenüber ist einzuwenden, dass Praktiken im öffentlichen Raum nicht automatisch und „in Gänze" als öffentliche Praktiken gelten können, auch wenn eine solche Sicht auf den ersten Blick völlig plausibel zu sein scheint: Sobald Leute den öffentlichen Raum betreten (oder befahren) und dort handeln, können sie sich schließlich kaum darüber beklagen, wahrgenommen und beobachtet zu werden; der Aufwand, der dafür zu betreiben wäre, damit dies nicht geschieht, wäre kaum zu rechtfertigen. Daher kann niemand, der sich im öffentlichen Raum aufhält, sinnvollerweise Privatheits-erwartungen hegen.[55] Während man dieser Ansicht intuitiv zustimmen mag, dürfte es den meisten Lesern gleichwohl kaum als gerechtfertigt erscheinen, dass z. B. die auf dem eigenen Smartphone befindlichen Fotoalben und Adressbücher durch eine andere Person in der räumlichen Öffentlichkeit ausgelesen werden.

Der an diesem Beispiel sichtbar werdende Unterschied in der verschiedenartigen Bewertung der unterschiedlichen Beobachtungsmodi verweist einmal mehr auf die Komplexität bzw. Multidimensionalität der Privatheit: Betrachten wir Akteure im öffentlichen Raum mit körperlich verfügbaren Sinnen, so erhalten wir vielleicht visuelle, auditive, möglicherweise auch olfaktorische und ggf. sogar taktile Eindrücke. Die Vorstellung vom öffentlichen Raum ist also damit verbunden, dass wir es in Kauf nehmen müssen, dass die Beobachtungen anderer all diese Wahrnehmungen beinhalten, sobald wir diesen Raum betreten. Daraus folgt jedoch nicht automatisch, dass wir jede Form von Privatheitserwartung aufgeben, sobald wir unsere Wohnung verlassen. Beispielsweise berechtigt das Betreten des öffentlichen Raumes andere keineswegs, uns anzufassen – die taktile „Privacy in Public"[56] bleibt also bestehen. Da nun dasselbe für informationelle „Privacy in Public" gilt, berechtigt der Umstand, dass die Praktiken im öffentlichen Raum stattfinden, niemanden automatisch dazu, Informationen über diese Praktiken, d. h. über die fraglichen Akteure und ihr Verhalten, einzuholen.

Aus diesem Grunde und in ähnlicher Weise stellt sich auch beim vernetzten Automobil die Frage, welche Formen von Beobachtung – und damit verbunden: Welche Formen von Privatheit-im-öffentlichen-Raum – als gesellschaftlich akzeptabel gelten können.

3.2 Erwartungshaltung der Nutzer

Wohl kein Konsumgut ist im Bewusstsein seiner Nutzer so unmittelbar mit dem Ideal von Selbstbestimmung verbunden wie das Automobil. Dies gilt zum einen für das kollektive Bewusstsein, in dem die massenhafte Verfügbarkeit von Autos verknüpft ist mit der wirtschaftlichen Emanzipation der Mittelschicht im Zuge des Aufschwungs der 1950er und 60er Jahre. Zum anderen geht auch in der individuellen Entwicklung das Recht auf Kontrolle über ein Auto mit dem Erwachsensein einher.[57] Das hinter dem Objekt stehende Prinzip der Automobilität ist eng verbunden mit den Prinzipien liberaler Konsumgesellschaften, drückt es doch in seiner Zusammenstellung aus, dass Freiheit mit Mobilität einhergeht. Zu den Werten, die Automobilität verkörpert, zählen insbesondere Freiheit, Privatheit, Bewegung und Fortschritt.[58]

Dabei zeichnet sich das Auto gerade dadurch aus, dass Privatheit hier nicht im Widerspruch zu Bewegung im öffentlichen Raum steht. Automobilität erlaubt es, in der privaten Kapsel zu bleiben, während man durch die Öffentlichkeit rollt.[59] Autos spiegeln in vieler Hinsicht die sozialen Strukturen wider, die auch im häuslichen Raum vorherrschen, so etwa in der räumlichen Aufteilung der Sitzplätze (Eltern vorne, Kinder hinten). Teilweise ist die Privatheit gegenüber dem familiären Rahmen sogar noch gesteigert, wie etwa im klassischen Beispiel des „car date"[60] Jugendlicher, das seit den 1950er Jahren zum Mythos des Autos dazugehört. Die in das Auto eingebaute Technik wie Lautsprecher, Musikanlagen, Heizungen und heutzutage auch Displays steigern noch einmal die Kluft zwischen dem Inneren des Autos und der Außenwelt.

Mit diesen Eigenschaften steht das Auto auch traditionell im Widerspruch zum öffentlichen Personennahverkehr, der seinen Teilnehmern weniger Privatheit zubilligt.[61] Über die letzten Jahre zeichnen sich allerdings Tendenzen ab, die eine Gleichstellung des Autos mit maximaler Privatheit und Selbstbestimmung in Frage stellen. Ausgelöst u. a. durch Überforderung der Verkehrswege, hohe Energiepreise, Umweltbedenken und Vekehrsunfälle, verbreiten sich Konzepte, die Konzessionen bei Privatheit und Selbstbestimmung der Fahrer verlangen. Dazu gehört etwa das Teilen von Autos, welche dann als wesentlich weniger privat empfunden werden und über die dann nicht mehr ganz autonom verfügt werden kann.[62] Experten sehen die Praxis des Carsharing auf globaler Ebene in einem anhaltenden Wachstum begriffen.[63] Auch die zunehmende Autonomie der Fahrzeuge - angefangen mit der automatisierten Gangschaltung bis hin zu Systemen zum Einhalten von Abständen und Spurtreue, zum Einparken und zum autonomen Fahren - trägt ihren Teil dazu bei.[64]

So können wir zwar grundsätzlich von äußerst hohen Erwartungen an Privatheit im Automobil ausgehen. Allerdings stellt sich die Frage, wie die fortschreitende Verbreitung von Angeboten wie Carsharing und autonomen Fahrzeugfunktionen mit diesen Erwartungen zu vereinbaren ist.

3.3 Smart Cars

3.3.1 Technologie und Funktionsweise

Smart Car ist als Sammelbezeichnung gebräuchlich für Fahrzeuge, die mit Hilfe eingebauter Hard- und Softwarekomponenten und entsprechenden drahtlosen Kommunikationsschnittstellen fahrzeuginterne Abläufe überwachen und unterschiedliche Daten über sich und ihre Umgebung erfassen und an die Außenwelt weiterleiten können. Nach Ansicht der Europäischen Kommission verspricht die wachsende Funktionsvielfalt von Informations- und Kommunikationstechnologien (IKT) in Fahrzeugen das Potenzial, ein ausgeklügeltes Netzwerk zwischen Fahrzeugen, Infrastruktur und jedem kommunikationsfähigen Gerät innerhalb und außerhalb des Fahrzeugs zu ermöglichen.[65]

Schließlich können moderne Fahrzeuge durch die IT-Durchdringung per Funk sowohl untereinander als auch mit externen IT-Diensten (bzw. mit einer Verkehrsinfrastruktur) kommunizieren. Daraus ergeben sich Möglichkeiten für vielfältige neue Anwendungen. Diese reichen von automatischen Gefahrenwarnungen zur Erhöhung der Sicherheit über Routenoptimierungen zur Steigerung der Effizienz[66], automatische Meldung eines Verkehrsunfalls[67], Maut-Management, neue Infotainment-Anwendungen[68] bis hin zu fahrverhaltensabhängigen Versicherungstarifen.[69]

Die Gesamtheit der im Fahrzeug eingebauten IT und elektronischen Komponenten werden als Bordnetz bezeichnet. Dieses besteht mittlerweile aus mehr als 70 Steuergeräten (sog. Electronic Control Units - ECUs), die verschiedene Funktionen in Hard- und Software realisieren.[70] Verschiedene Kommunikationsschnittstellen ermöglichen sowohl die Kommunikation der ECUs untereinander als auch mit der Außenwelt. CAN- und FlexRay-Busse[71] zur Datenübertragung im Kraftfahrzeug sind zwei Beispiele derartiger

Schnittstellen. Weitere Beispiele sind Bluetooth, RFID, WLAN und proprietäre Protokolle für die drahtlose Datenübertragung im Nahbereich. Diese Kommunikationsschnittstellen erweitern die Funktionalitäten des bereits in den 90er Jahren in Fahrzeugen vorgeschriebenen On-Board-Diagnose-Systemen (OBD-System), sowie der vorgesehene Unfalldatenrekorder (engl. Event Data Recorders, EDRs).[72]

Im Fahrzeug verbaute OBD-Systeme überwachen und zeichnen mittels Boardcomputern stetig Informationen über die Leistung und Funktionstüchtigkeit kritischer Fahrzeugkomponenten auf. Ziel dabei ist es einerseits die Fahrer bei Fehlfunktionen frühzeitig zu informieren. Anderseits sollen Kfz-Mechanikern und dem Technischen Überwachungsverein (TÜV) eine geeignete Datengrundlage für eine Reparatur oder Überprüfung der Fahrtauglichkeit zur Verfügung gestellt werden.

Unfalldatenrekorder sollen während der Fahrt kontinuierlich bestimmte Daten über den technischen Zustand und die Dynamik des Fahrzeugs erfassen. Darunter fallen die Fahrzeuggeschwindigkeit, Details zur Nutzung des Sicherheitsgurts, Auslösung des Airbags und Details zu Fahrerverhalten, wie Lenkung bei starkem Bremsen. Durch die nachträgliche Analyse der erfassten Daten wird dabei eine verbesserte Unfallklärung bzw. -forschung angestrebt.

Moderne Oberklassefahrzeuge sind bereits heutzutage über das Internet mit den Backend-Systemen der Hersteller verbunden. Die Car2X-Kommunikation, also die Kommunikation mit anderen (selbstfahrenden) Fahrzeugen sowie der Verkehrsinfrastruktur (z. B. Ampeln, Leitstellen) soll in Zukunft hinzukommen.[73]

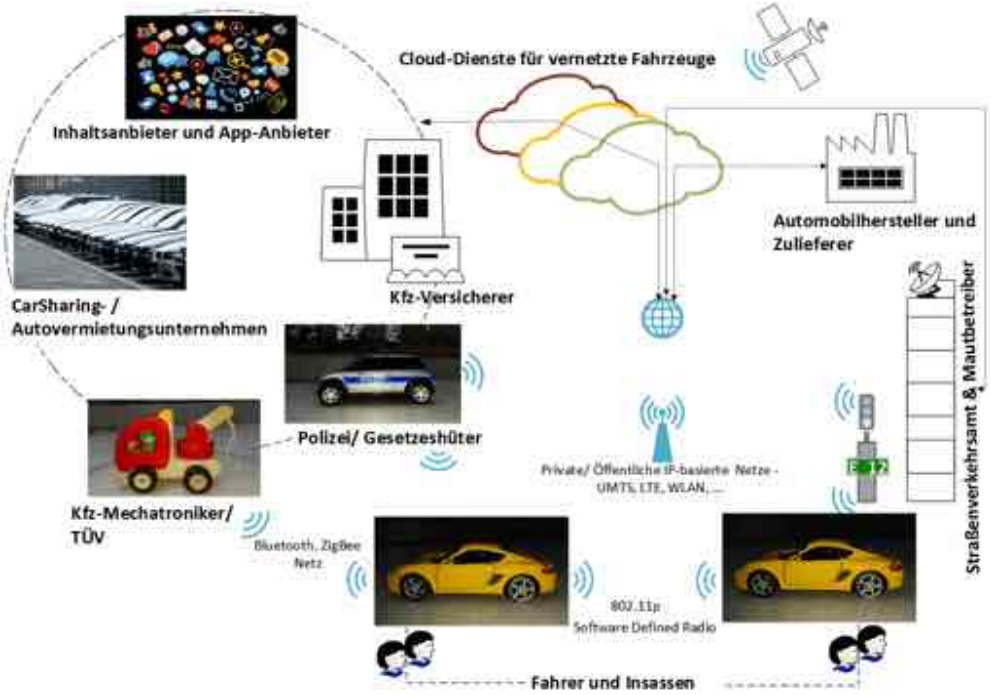


Abb. 02 Smart Car: Systemkomponenten und Kommunikation

3.3.2 Welche Daten fallen bei vernetzten Fahrzeugen an?

Konto- und Registrierungsdaten

Ähnlich wie bei Smart TV werden neue Funktionalitäten u. a. als Apps realisiert, die vom Fahrzeughersteller vorinstalliert sind oder von Diensteanbietern angeboten werden. Die Nutzung der Apps bzw. der neuen Dienste im Umfeld von Smart Cars erfordert gültige Nutzerkonten bzw. Nutzer-Accounts. Dabei müssen jeweils verschiedene persönliche Daten preisgegeben werden, wie Name, Geburtsdatum, Geschlecht, Adres-

se und ggf. Zahlungsinformationen der Nutzer. Diese Informationen werden i. d. R. zusammen mit dem Benutzernamen und Kennwort lokal im Fahrzeug gespeichert, ggf. auch bei den jeweiligen Anbietern der Online-Dienste. Ein solcher Online-Dienst kann der Betreiber eines automatischen Notrufsystems für Fahrzeuge „eCall" sein oder der Anbieter von so genannte Mehrwertdiensten (Value Added Service) wie z. B. von individualisierten, also von der jeweiligen Fahrweise abhängigen Kfz-Versicherungstarifen.

Nutzungsdaten

Nutzungsdaten umfassen Details über die Interaktion zwischen Fahrzeuginsasse(n) und dem Fahrzeug, über die Interaktion zwischen dem Fahrzeug und seiner Umwelt sowie Details über die von Fahrzeuginsassen genutzten Dienste. Hierzu gehören u. a. E-Mail oder MMS-Dienste, das Surfen während der Fahrt über einen integrierten WLAN-HotSpot, die Nutzung standortbasierter Dienste (z. B. Tank- oder Parkplatzsuche-App), etc.

Am Fahrzeug eingebaute Sensoren für das automatische Einparken zeichnen Informationen über die unmittelbare Umgebung des Fahrzeugs kontinuierlich auf und speichern diese für eine kurze Zeit.[74] Weitere von den Fahrzeugsensoren erfasste Daten umfassen u. a. die Außentemperatur, den Lichteinfall und den Luftdruck. Bei der Nutzung ortsabhängiger Dienste fallen typischerweise Standortdaten des Fahrzeugs und der Fahrzeuginsassen an.[75] Vermehrt im Autositz[76] und Lenkrad[77] eingebaute Sensoren ermöglichen eine permanente Erfassung der physiologischen und biometrischen Merkmale der Fahrer. Interne Kameras und Mikrofone können Aktivitäten im Fahrzeug registrieren und Video- und Audioaufnahmen erstellen. Die rechnergestützte Erfassung und Interpretation von Puls und anderen Vitalparameter des Fahrers sollen Müdigkeit und Kreislaufversagen am Steuer frühzeitig erkennen und zu mehr Sicherheit im Straßenverkehr beitragen. Zudem sollen physiologische und biometrische Merkmale des Fahrers in naher Zukunft genutzt werden, um mittels Augen- und Blickanalyse, über Stimmen- und Gesichtserkennung mehr Sicherheit (z. B. in Form von neuen Diebstahlschutzlösungen) und Komfort (personalisierte und automatische Anpassung des Sitzes, der Spiegel, usw.) im Fahrzeug zu realisieren.

Fahrzeugspezifische Daten

Fahrzeugspezifische Daten werden in erster Linie vom OBD-System und Unfalldatenrekorder erfasst. Dazu gehören neben Informationen über Geschwindigkeit, Drehzahl, Beschleunigung, Bremsleistung und Querbeschleunigung auch informationstechnische Informationen wie die Art der Netzwerkschnittstelle bzw. Netzwerkverbindung, die Netzwerk- bzw. IP-Adresse des Fahrzeugs, Firmware und ggf. der eindeutige Identifier (auch „Fahrzeugidentifikationsnummer"- FINs) des Fahrzeugs. Weitere fahrzeugspezifische Daten umfassen Angaben über Produktionsort, Fahrzeug- und Motortyp sowie über die eingebauten Steuer- und Sensorgeräte. Zugriff auf diese Daten haben typischerweise die Fahrzeughersteller, Kfz-Mechaniker und der TÜV. Erstere können je nach Szenario auch über einen Fernzugriff verfügen.

Ableitbare Daten

Die oben beschriebenen Datentypen können dazu genutzt werden, um ein Profil des Fahrzeugs und des Fahrers oder der Fahrerin zu generieren. So können beispielweise aus einer Auswertung der fahrzeugspezifischen und Nutzungsdaten Rückschlüsse auf Fahrstil, Aufenthaltsort und Routen bestimmter Fahrzeuge gezogen werden. Wenn diese Informationen mit anderen Datenbeständen abgeglichen werden, können sogar Rückschlüsse auf persönliche Attribute und Gewohnheiten der Fahrer gezogen werden. So ließe sich beispielweise ermitteln, ob eine religiöse Stätte besucht wurde, wie oft,

wo und wann eingekauft und ob und an welchen politischen Demonstrationen teilgenommen wurde.[78]

3.4 Rechtliche Rahmenbedingungen

Wird ein Smart Car in Betrieb genommen, vollzieht sich die Erhebung einer Vielzahl unterschiedlichster Daten nahezu unbemerkt (siehe Abschnitt 3.3.2). Die aus den personalisierten Servicefunktionen gewonnenen Daten stellen ebenso wie Daten für Fahrzeugfunktionen personenbezogene Daten dar, welche nicht nur grundrechtlichen Schutz genießen, sondern auch dem Datenschutzrecht unterliegen. All jenen Daten ist gemein, dass sie objektiv gesehen einem Dritten, der Kenntnisse, Mittel und Möglichkeiten besitzt, eine Zuordnung zu einer bestimmbaren Person ermöglichen. Personenbezogene Datenerhebungen sind nicht nur über Fahrer möglich, sondern auch – je nach Datenlage – über Mitfahrer, Fahrzeughalter, Vorbesitzer und andere Verkehrsteilnehmer, die mit einem intelligenten Fahrzeug kommunizieren.[79] Die für den Datenumgang und die Einhaltung der gesetzlichen Vorschriften verantwortliche Stelle unterscheidet sich je nach Anwendung. In Betracht kommen nicht nur die Fahrzeug- und Systemhersteller, sondern auch Diensteanbieter, die Applikationen zur Verfügung stellen, oder aber auch Versicherungen und Werkstätten, die Zugang zu den im Fahrzeug gespeicherten Daten haben.[80]

Ein mit IKT ausgestattetes Auto begründet ein erhöhtes Bedürfnis nach einem umfassenden Grundrechtsschutz: Als eigengenutztes informationstechnisches System von gewisser Komplexität unterliegt es der Gewährleistung der Vertraulichkeit und Integrität des Computergrundrechts, um Überwachung und Manipulation des Systems und damit Eingriffe in das Persönlichkeitsrecht zu verhindern.[81] Intelligente Fahrzeugsysteme können je nach Aufgaben- und Einsatzbereich dem sachlichen Schutzbereich dieses Grundrechtes unterliegen, wenn sie eine hohe Speicher- und Verarbeitungskapazität aufweisen, zudem vernetzt sind und durch die Erhebung personenbezogener Daten Einblicke in wesentliche Teile der Lebensgestaltung und ein aussagekräftiges Bild der Persönlichkeit bestimmbarer Personen zulassen.[82] Parallel hierzu sichert das *Recht auf informationelle Selbstbestimmung*, als Ausformung des allgemeinen Persönlichkeitsrechtes, den Schutz all jener personenbezogener Daten, welche durch die in dem Smart Car enthaltenen Technologien betroffen sein können. Um eine umfassende Sicherung der Auskunftsrechte der Betroffeneninteressen gewährleisten zu können, müssen geeignete Maßnahmen veranlasst und die notwendige Transparenz gewährleistet werden. Die Betroffenen haben ein Recht darauf zu erfahren, welche Daten zu welchen Zwecken erhoben und wie diese verwendet werden. Nur so können sich Betroffene frei bewegen, wenn sie davon ausgehen können, dass nicht ihr gesamtes Verhalten, ihre Bewegungen, Kontakte und Ähnliches aufgezeichnet und gegen sie verwendet wird.[83]

Die rechtlichen Anforderungen, die erfüllt sein müssen, um eine rechtmäßige Verarbeitung der durch das Smart Car gewonnenen personenbezogenen Daten zu gewährleisten, ergeben sich je nach Ausgestaltung und Art der erhobenen Daten aus unterschiedlichsten Rechtsgrundlagen.[84] Als zu beachtende Rechtsnormen kommen Vorschriften des TMG, des TKG und des BDSG in Betracht. Als speziellere Gesetze mit schutzintensiveren Anforderungen an die Datenverarbeitungsvorgänge muss zunächst die Anwendbarkeit des TMG oder des TKG geprüft werden, bevor auf die allgemeineren Schutzvorschriften des BDSG Regress genommen werden kann.

Werden nutzerbezogene Dienste bereitgestellt und nicht nur Signale zur Kommunikation mehrerer vernetzter Systeme übertragen, handelt es sich um Telemediendienste, mit der Folge, dass für Bestands- und Nutzungsdaten das TMG Anwendung findet. Kfz-Kommunikationsdienste sind praktisch durchgehend als Telemediendienste einzustufen. Ist das Telemedienrecht nicht anwendbar, weil nicht Bestands- und Nutzungsdaten verarbeitet werden, handelt es sich um die Verarbeitung von sog. Inhaltsdaten, welche den Anwendungsbereich des BDSG eröffnen.[85] Erfolgt die Signalübertragung unter

Nutzung eines Telekommunikationsnetzes, d. h. wird ein Telekommunikationsdienst bereitgestellt, so bilden die gesetzlichen Regelungen des TKG den Prüfungsmaßstab einer jeden Datenerhebung und -verwertung. Je nach Ausgestaltung des Smart Car-Systems und Anwendungsfall können gleichwohl auch andere datenschützende Normen die Bedingungen einer rechtmäßigen Erhebung und Verarbeitung personenbezogener Daten reglementieren. Dies gilt insbesondere für solche Fälle, in denen weder das Telemedienrecht noch das Telekommunikationsrecht relevant ist.

Zur Gewährleistung der informationellen Selbstbestimmung sowie der darauf basierenden einfachgesetzlichen Regelungen müssen Systeme in intelligenten Fahrzeugen sicherstellen, dass die Datenverarbeitung transparent stattfindet, Daten jederzeit eingesehen und gelöscht werden können, nicht mehr benötigte Daten umgehend gelöscht werden und die Daten im System sicher, vor allem anonym oder pseudonym verarbeitet werden.

3.5 Privatheitsrisiken und Überwachungspotenziale

Das bereits am Beispiel des Smart Home aufgeführte Grundproblem, dass durch das versteckte Internet viel mehr Menschen und Institutionen über das eigene Handeln informiert werden können, betrifft auch das versteckte Internet im Auto.

Intransparenz der Datenverarbeitung

Am Beispiel des Smart Car wird der eingangs thematisierte Unterschied zwischen verschiedenen Nutzerperspektiven besonders deutlich: Oben wurde ausgeführt, dass aus der Erwartungshaltung der Nutzer insbesondere PKWs für viele Menschen als *die* Form individueller Mobilität schlechthin gelten. Wer ein Auto fährt, versteht sich als Individuum auf dem Weg von einem Ort zum anderen und nicht als Teil eines komplexen soziotechnischen Systems namens Straßenverkehr. Letzteres ist aber die Perspektive, die oft das versteckte Internet im Smart Car betrifft: Durch die Datenerhebung im Fahrzeug und die Kommunikation der Daten mit der Außenwelt soll der Straßenverkehr vermessen und optimiert werden.

Überwachungspotenzial durch Tracking und Profilbildung

Das Automobil wird als mobiler Sensor verstanden, der nicht nur zusätzliche Daten zu Fahrzeug, Insassen und Straßenverkehr liefern, sondern auch die bereits als fester Teil der Verkehrsinfrastruktur vorhandenen Sensoren ersetzen soll.[86] Statt beispielsweise das Verkehrsaufkommen an einer einzelnen Stelle zu erfassen, ergibt sich mit den Daten aus einem Großteil der Fahrzeuge ein deutlich differenziertes Bild. Wie in Abschnitt 3.3. beschrieben, sind Bewegungsdaten aber auch geeignet, um Personen zu identifizieren und vielfältige Rückschlüsse über ihr Leben zu ziehen: Im Prinzip kann künftig jeder Ort, an den sich jemand mit dem Smart Car begibt, einer Person zugeordnet werden. Dabei ist zu beachten, dass die Gleichsetzung eines Fahrzeugs mit seinem Besitzer auch zu durchaus problematischen Fehlurteilen führen kann. Letztendlich wird hier immer nur das Auto, nicht eine Person verfolgt. Die oben in 3.3. angesprochene zunehmende Integration von anderen Geräten (z. B. Smartphones) und (biometrischen) Sensoren in das Bordnetz eines PKWs erlaubt jedoch auch die Erkennung von Fahrerinnen und Fahrern und somit die Erstellung differenzierterer Profile.

Darüber hinaus sind insbesondere Versicherungen an den Daten aus PKWs interessiert. Damit soll es gelingen, die Risiken ihrer Kunden noch besser einzuschätzen und individuell zuzuordnen.[87] Das kann aber auch dazu führen, dass es für bestimmte Bürger schwieriger wird, eine bezahlbare Versicherung zu bekommen. Angesichts des enor-

men Stellenwertes, den PKWs und individuelle Mobilität immer noch in unserer Gesellschaft haben, ist das eine schwerwiegende Einschränkung.

Dieser Punkt zeigt bereits, dass eine Beurteilung der Chancen und Risiken des versteckten Internets im Automobil nicht auf individuelle Privatheitsrisiken reduziert werden kann.

Werden Fahrzeuge als Teil des komplexen Personenverkehrssystems betrachtet, also aus der Perspektive der Verkehrspolitik, der Infrastruktur und zunehmend der Hersteller von Kraftfahrzeugen, gibt es auch gute Gründe, um die Vernetzung von Fahrzeugen zu befürworten: beispielsweise für Verbesserungen in den Bereichen Effizienz, Umweltschutz oder Sicherheit. Dabei wird allerdings vorausgesetzt, dass die Technologien auch erfüllen, was ihre Befürworter versprechen. Damit daraus aber keine technokratische Bevormundung wird, muss zuerst der Unterschied zwischen individueller Wahrnehmung – einschließlich der Grenzen individueller Abwägung – und überindividuellen Perspektiven deutlich werden. Sodann zeigt sich, dass es hier um eine Neuverteilung von Entscheidungsmöglichkeiten geht, die insbesondere einen Verlust *individueller* Entscheidungsfreiheit bedeutet.[88]

Verlust oder Einschränkung der Entscheidungsfreiheit

Langfristig ist zu erwarten, dass durch die Erhebung von Daten bei der Fahrzeugnutzung der Verkehr stärker geregelt wird oder zumindest durch Anreize (z. B. ein besserer Versicherungstarif) das Verhalten der Verkehrsteilnehmer beeinflusst werden soll. Die mit dem PKW verbundene Erwartungshaltung der selbstbestimmten Mobilität würde dann eingeschränkt. Auch wenn derartige Technologien gerade erst etabliert werden, kann das versteckte Internet im Auto hier zu neuen Pfadabhängigkeiten führen, welche die zukünftige Entwicklung beeinflussen. Die Akteure, denen die Daten zur Verfügung stehen, können mitbestimmen, wie diese verwendet werden. Im Moment fallen diese Daten vor allem bei Kfz-Herstellern an, die sich dadurch auch als wichtige Akteure bei der Gestaltung zukünftiger „Verkehrsdienstleistungen" sehen. Die Besitzer der Fahrzeuge sind sich oft nicht bewusst, dass durch ihre Fahrzeugnutzung Daten generiert werden, welche die Hersteller als ihr Eigentum betrachten und der Zugang für die Kundinnen und Kunden keineswegs selbstverständlich ist. Durch Vertragsklauseln zur Datennutzung, die bei Erwerb eines Fahrzeuges implizit mit abgeschlossen werden, entstehen neue, zusätzliche Abhängigkeiten (sowohl für Nutzer wie auch lokale Entscheidungsträger z. B. in Kommunen). Das wirft Fragen des Verhältnisses von öffentlichen Stellen und der Privatwirtschaft auf, für deren Klärung eine Untersuchung des versteckten Internets im Fahrzeug eine wichtige Rolle spielt.

Für die Frage der Privatheit und der Selbstbestimmung bedeutet das, dass diese in Konkurrenz oder gar Widerspruch mit anderen Werten stehen: Z. B. eine sichere, eine ökonomisch rentable, eine umweltfreundliche Gestaltung des Verkehrs. Denn die zunehmende Verwirklichung des „versteckten Internets" lässt sich nicht darauf reduzieren, dass mehr Informationen über die Nutzung von technischen Geräten anfallen. Dieser Umstand ist vielmehr eine Folge der stärkeren Verbindung und Verschränkung von zuvor individuell genutzten Technologien und in diesem Sinn eine weitgehende Umstrukturierung des durch diese Technologien geschaffenen Handlungsraumes.

4
Das versteckte Internet am Körper

4.1 Privatheit in der Interaktion

„Wearable Computer, also kleine tragbare Geräte wie Datenbrillen oder spezielle Armbanduhren, sind einer der großen Trends auf der CES (Consumer Electronics Show) in Las Vegas", hieß es beim Deutschlandfunk Anfang Januar 2015.[89] Dabei ist es kein Zufall, dass gerade Brillen („Smartglasses") und Uhren („Smartwatches") beispielhaft angeführt werden, handelt es sich bei diesen doch um Produkte, die der Vorstellung zufolge die Wearable-Marktbildung gewissermaßen als „Pionierprodukte" vorantreiben sollen. Beide weisen das Potenzial auf, an der Transformation von Privatheitspraktiken mitzuwirken: In Bezug auf Smartwatches erfolgt dies anhand des Phänomens der „Selbstvermessung/-optimierung"; Datenbrillen behandeln wir indes mit Blick auf das Phänomen der sozialen Interaktion.

Dass Menschen motiviert sind, mit Smartwatches oder anderen Wearables, Daten über sich zu sammeln und diese zu veröffentlichen, ergibt sich offenkundig nicht allein aus der technischen Möglichkeit bzw. Verfügbarkeit entsprechender Angebote. Die Lust an der Selbstvermessung hat auch mit einer an Effizienz und Konkurrenz orientierten Gesellschaftsordnung zu tun.[90] Darüber hinaus sind Menschen heute mehr denn je selbst verantwortlich für ihre Lebensplanung, ihren Erfolg und ihre Gesundheit.[91] Selbstvermessung lässt sich in diesem Zusammenhang interpretieren als Ausdruck einer zeitgemäßen Versorgungslogik, die Risiken und Ängste auf die Individuen abschiebt: Finden sich die Akteure in einer Situation wieder, in der sie angehalten sind, ihr Leben selbstverantwortlich zu meistern, so begrüßen sie verständlicherweise Möglichkeiten der Selbstbeobachtung (-vermessung) und -optimierung. Solche „Technologien des Selbst", die es erlauben, Wissen über sich selbst zu erlangen und sich auf dessen Basis selbst zu verbessern, sind anthropologisch nicht neu – es gibt sie seit mindestens 2000 Jahren.[92] Doch gewinnen solche Technologien an neuer Brisanz in Situationen, in denen Flexibilität und Selbstverwirklichung zur sozialen Pflicht werden und es notwendig scheint, sich selbst zu bewerten und zu optimieren.[93] In punkto Privatheit können etwaige Veränderungen vor allem dadurch aufkommen, dass in einem bestimmten (etwa dem freizeitsportlichen) Kontext willentlich erhobene und veröffentlichte Daten für Akteure aus Kontexten abrufbar werden, die bislang keinen Zugriff auf diese Daten hatten (z. B. Krankenkassen, die dementsprechend Mitgliedertarife zuschneiden). In dem Sinne gerät die bislang für selbstverständlich gehaltene Abgrenzbarkeit verschiedener sozialer Kontexte ggf. in Turbulenzen.

Damit wollen wir uns nun dem Phänomen der Datenbrillen zuwenden; diese, so ist zu konstatieren, sind v. a. geeignet, transformierende Effekte in Bezug auf das Phänomen der sozialen Interaktion zu entfalten. Bei letzterer handelt es sich um eine überaus grundlegende Kategorie, sofern die Prämisse, dass Sozialität aus der Wechselwirkung zwischen Akteuren (also aus der Interaktion) entsteht, so alt ist wie die Soziologie selbst. Das gleiche gilt für die Beobachtung, dass der Charakter und Grad des Wissens um andere Personen die Interaktionen sowie die sich daraus entfaltenden Beziehungen maßgeblich prägt.[94] Dem Interaktionssoziologen Erving Goffman zufolge liegt genau hier der Grund dafür, dass wir alle im Alltag „Theater spielen"[95]: Sobald andere Akteure präsent sind, versuchen diese Informationen über uns zu erlangen, um uns, unser Agieren und die Gesamtsituation einschätzen zu können. Auch auf bereits erlangtem Wissen fundieren Akteure ihr Verhalten gegenüber anderen. Dabei versucht jeder Akteur einen bestimmten Eindruck von sich zu erzeugen. Eben dies nennt Goffman „impression management"[96], und fundamentaler Bestandteil dieser sozialen Alltagstechnik ist die Kontrolle der Informationen, die Akteure durch ihr jeweiliges Agieren anderen zugänglich machen.

Erweitert man die Interaktionsanalyse um die Erkenntnis, dass sich das Rollenspiel im Verlaufe eines beliebigen alltäglichen Tagesverlaufs vor einer Vielzahl ganz unterschiedlicher Publika vollzieht, so wird klar, dass aus der beschriebenen mikrosozialen Situation ein komplexes, aber geordnetes Geflecht von Erwartungshaltungen und Verhaltensweisen erwächst – Erwartungen und Verhaltensweisen, die Akteuren in jeweils spezifischen, sozial definierten Interaktionsbereichen entgegengebracht werden: In der Familie finden sich andere Erwartungshaltungen und Verhaltensweisen als bei der Arbeit oder im Gemüseladen usw. Die soziale Welt erweist sich demnach als geordnet, wobei diese Ordnung gleichermaßen ermöglichende und einschränkende Aspekte[97] für die Interaktion aufweist: So muss die Ordnung der Erwartungen und die Erwartbarkeit von Verhalten zwar in jedem Moment neu erzeugt werden, jedoch erfolgt dies nicht gänzlich *de novo*, sofern soziale Akteure auf ein zwar nicht starres, aber bereits in der Vergangenheit ausdifferenziertes, etabliertes und zumeist bewährtes Repertoire von Rollen zurückgreifen können (die Rolle der Familienmutter, die Rolle der Arbeitnehmerin, die Rolle der Käuferin). Genau hier zeigen sich die angesprochenen ermöglichenden und einschränkenden Aspekte, eröffnet die Rolleninterpretation den Akteuren doch einerseits Spielräume, während andererseits die Verfügbarkeit von Rollen sowie die Wahl der Rolle nicht gänzlich dem Gutdünken der Akteure unterworfen ist. Für unseren Zusammenhang von zentraler Bedeutung ist der Umstand, dass mit den Rollen wiederum die Preisgabe bzw. Zurückhaltung bestimmter Informationen – im Berufsleben andere als gegenüber Freunden, als Patient andere als als Vereinsmitglied usw. – verbunden ist. Aus Perspektive der Interaktionssoziologie spielen wir in diesem Sinne jeweils andere Rollen für jeweils andere Publika und innerhalb von Gesellschaften finden sich viele Techniken der Grenzziehung, die diese Publika voneinander abschirmen. Eine Frau kann z. B. gegenüber ihren Kindern liebevoll auftreten, während sie in ihrer Rolle als Vorstandsvorsitzende Härte zeigt, und im Alltag mischen sich die Publika „Familie" und „Vorstand" auch nicht. Dies beschreibt der Begriff der „audience segregation"[98]. Daher lässt sich davon ausgehen, dass der Zusammenbruch einer solchen Trennung verschiedener Publika in dem Moment droht, wenn Informationen über den zugehörigen sozialen Bereich hinweg abrufbar werden: Das Rollengefüge kann dann ins Wanken kommen, Verhaltenserwartungen können unklar werden. Kommen z. B. die Kinder in die Vorstandssitzung, wissen vielleicht weder die Vorsitzende, noch der Vorstand oder die Kinder, wie sie sich verhalten sollen, was bei allen Beteiligten als diffuse Peinlichkeit spürbar wird.

Dies gilt zumindest für soziale Situationen, wie wir sie bislang kannten. Wenn der Einsatz bestimmter Technologien nun dazu führt, dass Interaktionspartner in Alltagssituationen nicht mehr nur über situativ zugängliche Informationen verfügen, sondern – zumindest potenziell – über sämtliche persönliche Informationen, die über die jeweils anderen online verfügbar sind, dann können sich die Beteiligten nicht mehr sicher sein, was andere über sie wissen – und offenkundig machen Datenbrillen dies möglich. Die frühe soziologische Einsicht, dass Interaktionen von für die jeweiligen Interaktionen spezifischen „Wissensausschnitten" geprägt sind, wäre dann nicht mehr gültig. Für die Zukunft würde dies dann die Frage aufwerfen, wie Menschen interagieren, die kaum noch einschätzen können, was ihre Interaktionspartner über sie wissen.

4.2 Erwartungshaltung der Nutzer

Wearables sind der neueste Entwicklungsschritt in der Mobilkommunikation, die seit dem Aufkommen von Mobiltelefonen auf dem Massenmarkt vor ca. 20 Jahren unsere Alltagskommunikation dramatisch verändert hat.[99] Als Uhren, Armbänder, Headsets, Brillen und auch Schmuck setzen sie die mit dem Handy ausgelöste Entwicklung zu immer neuen Endgeräten fort, die einzeln und miteinander vernetzt Computertechnik und Internetanwendungen in den Alltag hineintragen.[100]

Da mobile Medien immer größere Bereiche des Alltags für die digitale Erfassung und Auswertung verfügbar machen, gelten sie heute als „pervasive interfaces“[101], also die Lebenswelt durchdringende Schnittstellen. So wie früher etwa die graphische Benutzeroberfläche dem Anwender als Schnittstelle zu den informatischen Abläufen eines Computers diente, so dienen mobile digitale Medien heute als Schnittstellen zu den öffentlichen Räumen, durch die man sich mit ihnen bewegt.[102] Sie bilden also eine Instanz zwischen den Nutzern und deren Umwelt, wodurch den Nutzern neue Möglichkeiten zur Steuerung der eigenen Interaktion mit der Umwelt geboten werden. Schon der Walkman erlaubte dem Pendler in der überfüllten U-Bahn, die Nähe zu anderen Menschen ganz auszublenden und sich ganz auf sich selbst zu konzentrieren. Durch dieses Verhalten, das auch als „cocooning“ bezeichnet wird[103], können Nutzer öffentliche Orte „privatisieren“.[104] Aktuelle Techniken können dabei die Sinne der Nutzer noch umfassender beschäftigen (etwa mobiles Fernsehen durch Bild und Ton), sie versprechen aber auch, die Vereinbarkeit von Medien- und Umweltwahrnehmung zu erleichtern (das ist jedenfalls der Anspruch von Smartglasses). Vernetzte mobile Techniken bieten aber auch neue Möglichkeiten zur Steigerung der Umweltwahrnehmung, etwa indem man sich durch Augmented Reality auf potenziell interessierende Objekte aus dem Umfeld hinweisen lässt oder durch RFID-Technik mit der Umwelt interagiert.[105]

Wearables zeichnen sich gegenüber vielen anderen mobilen Medienangeboten zudem dadurch aus, dass sie sich auch als Schnittstellen zum eigenen Körper eignen. Bislang eher schwer zugängliche Informationen etwa über den eigenen Puls oder das Schlafverhalten werden nicht nur leicht messbar, sondern sie werden auch grafisch und teils spielerisch attraktiv aufbereitet. Damit betreffen Wearables ganz besonders die körperliche Privatheit der Nutzer. Mit der Nutzung dieser Technik eröffnen Konsumenten dann auch Dritten eine Schnittstelle zum eigenen Körper und zu den eigenen Bewegungen im Raum, seien es Unternehmen, Regierungen oder Mitmenschen wie Partner, Eltern und Freunde. Besonders gefährdet sind damit die körperliche Privatheit und die örtliche Privatheit als Kontrolle von Information über den eigenen Aufenthaltsort.

Welche Bedenken und Verhaltensweisen bei den Nutzern dazu vorliegen, wurde bislang kaum empirisch erforscht. Erst im November 2014 ist eine umfassende Studie zu Privatheitseinstellungen vom PewResearch Internet Project veröffentlicht worden, in der auf Wearables nicht eingegangen wird.[106] Dass Bedenken vorliegen, lässt sich aber aus Befragungen zu örtlicher Privatheit im Kontext von standortbezogenen Diensten für das Smartphone ableiten. So hat eine Repräsentativbefragung von PewResearch unter US-Teenagern 2013 gezeigt, dass immerhin 46 Prozent der Jugendlichen, die Apps nutzen, die Funktionen zur Standortbestimmung mindestens einmal gezielt deaktiviert haben.[107]

4.3 Wearables

Wearable Computing bezeichnet eine Form der allgegenwärtig rechnergestützten Informationsverarbeitung, bei der miniaturisierte und vernetzte Computer am oder im menschlichen Körper getragen werden.[108] Solche Wearables halten vermehrt Einzug in unser tägliches Leben.[109] Sie werden in der Regel unauffällig getragen und sollen – anders als Smartphones – ohne unmittelbares, aktives Eingreifen des Nutzers, Daten über ihn und seine Umgebung erfassen, verarbeiten und übertragen. Uhren, Brillen, Armbänder, Sportbekleidung und Laufschuhe aber auch implantierte medizinische Geräte werden zunehmend mit relativ kompakten Mikroprozessoren, unterschiedlichen Sensorarten sowie Netzwerkschnittstellen bestückt. Die Unterstützung verschiedener Netzwerksprotokolle (z. B. UMTS, Bluetooth und WLAN) ermöglichen es, tragbare Geräte direkt oder über das Mobiltelefon mit dem Internet zu verbinden. Vorreiter unter den Wearables sind die sog. Fitnessarmbänder, Smartwatches und Smartglasses. Anders als bei bereits seit Jahren auf dem Markt vorhandenen Geräten mit einfacher Sensorik, sind bei heutigen Wearables modernste Sensoren integriert, die eine Erfassung

einer Vielzahl von Daten über ihre Träger und jeweiligen Umgebungen in Echtzeit ermöglichen. Basierend auf einer Analyse dieser Daten sollen die Bedürfnisse der Nutzer nach jederzeit verfügbarer Konnektivität sowie ortsunabhängigen und personalisierten Dienste erfüllt werden. Unternehmen versprechen sich die Möglichkeit, mehr über Off- und Online-Aktivitäten und Routinen potenzieller Kunden zu erfahren, um so ihre Dienste besser in den Alltag der Kunden zu integrieren. Die Anwendungsfelder erstrecken sich von Gesundheit und Fitness über medizinische Versorgung, Navigation bis zu professionellen Arbeitskontexten im Gesundheits- und Ingenieursbereich, Social Networking und Gaming.[110]

4.3.1 Smartwatches und intelligente Armbänder: Technik und Funktionsweise

Bei Smartwatches handelt es sich um mobile Endgeräte, die wie herkömmliche Armbanduhren aussehen, aber wie ein Smartphone mit Computer-Chips und Funktechnik ausgestattet sind, um Daten gewinnen, verarbeiten und weiterleiten zu können. In der Regel kommunizieren sie über Bluetooth oder WLAN mit anderen Geräten in der unmittelbaren Umgebung. Smartwatches verfügen über eine Vielzahl von Sensoren und bieten die Möglichkeit zur Funktionserweiterung durch Apps. Das Annehmen von Anrufen per Armbanduhr, Lesen von Nachrichten, Terminkalendern, Einkaufslisten oder das Darstellen von Bildern ist nur ein kleiner Ausschnitt der Funktionalität von Smartwatches, die von Smartphones übernommen wurde. Einige neue Modelle integrieren zusätzliche Funktionen wie Aktivitäts- bzw. Fitness-Tracking.

Im Gegensatz zu Smartwatches stellen intelligente Armbänder eine einfachere Variante von Wearables dar. Intelligente Armbänder verfügen über elektronische Funktionen und Sensoren, um die physiologischen Aktivitäten, Parameter und Körperfunktionen des Trägers aufzeichnen zu können, um diese Daten dann an externe Geräte wie das Smartphone oder den PC weiterzuleiten. Intelligente Armbänder für Freizeitsportler (so genannte Fitnessarmbänder) erfassen die Bewegung der Hand und zeigen Nutzern an, wie viel Energie durch die körperliche Aktivität verbraucht wird. Intelligente Armbänder werden derzeit in der Regel zusammen mit speziell für sie entwickelten Apps und Online-Diensten genutzt.

Diese Apps können auf der Basis der Informationen über den Nutzer (Alter, Geschlecht, Gewicht, etc.) und der erfassten Sensordaten beispielsweise Ernährungs- bzw. Aktivitätsempfehlungen abgeben. Bei dieser Art von Wearables stehen insbesondere das Sammeln und die Weitergabe von Daten an andere Geräte im Vordergrund. Eine Verarbeitung der Daten und unmittelbare eine Interaktion mit dem Nutzer ist meist nicht möglich.

Aktuelle Geräte sind mit einem UMTS/LTE-Chip bestückt und können so über das Mobilfunknetz direkt mit der Backend-Infrastruktur eines Diensteanbieters kommunizieren. Der Umfang der Datensammlung geht bei einigen Geräten besonders weit, etwa bei solchen mit Life-Logging Funktionen: Das Sony Smartband hat beispielsweise den Anspruch, den gesamten Tages- und Nachtablauf des Nutzers möglichst komplett aufzuzeichnen. Mit Hilfe der Lifelog App wird erfasst, wann mit Freunden gesprochen, eine E-Mail erhalten oder ein Film gesehen wurde.[111]

Ursprünglich stammt der Gedanke einer so umfangreichen Erhebung von Daten aus dem medizinischen Bereich, um chronisch kranke Patienten permanent überwachen zu können. Aber auch der Leistungssport machte sich diese Funktion für angestrebte Optimierungsprozesse von Profisportlern zunutze. In der klinischen Diagnostik ist mit dem Einsatz solcher Technologien das Ziel verbunden, nahezu kontinuierlich Informationen über Bewegungsabläufe und Vitalparameter, z. B. Herz- und Atemrhythmus, Schlafaktivität, Schlafposition, Körpertemperatur, Puls, Blutdruck, Blutzucker oder Sauerstoffsättigung zu sammeln und diese entsprechend auszuwerten.[112] Eng damit verbunden sind Technologien, die im Bereich Ambient Assisted Living (AAL) eingesetzt werden. Hier

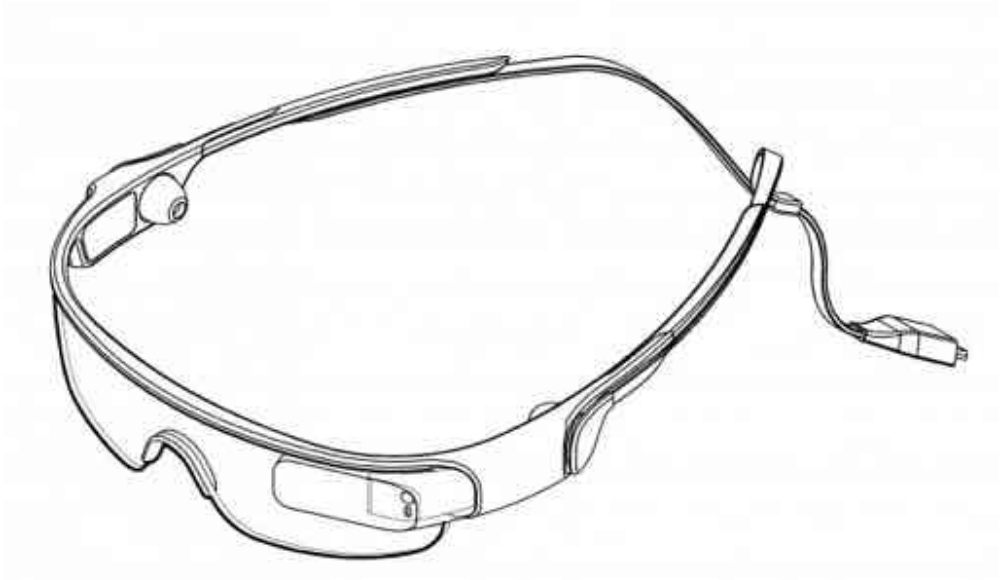
sollen altersgerechte technische Assistenzsysteme, die sich vor allem in der Wohnumgebung des Nutzers befinden, ein auch im höheren Alter selbstbestimmtes Leben ermöglichen. Wearables, die hier zum Einsatz kommen, können z. B. den Sturz eines Nutzers feststellen und automatisch einen Notruf absetzen. Mittels am Handgelenk befestigter Minicomputer soll diese Art und Weise des Home-Monitoring zusätzlichen Komfort für kranke und pflegebedürftige Personen bieten.[113]

Der allgemeine Trend des Einsatzes intelligenter Armbänder und Smartwatches im Privatnutzerbereich geht jedoch nach Plänen der Technologieentwickler und –anbieter zur umfassenden Vernetzung dieser Technologien mit anderen Geräten des Internets der Dinge. Danach könnte beispielsweise eine Smartwatch als zentrale Fernsteuerung im Bereich Smart Entertainment genutzt werden.

4.3.2 Smartglasses: Technik und Funktionsweise

Smartglasses (Intelligente Brillen) wie Google Glass oder Samsung GalaxyGlass sind Wearables mit integriertem Display, Mikrofon, Kamera, und Internetzugang (Abb. 03). Nach der Vision des Herstellers soll Google Glass in Verbindung mit zahlreichen Apps aus dem Google Play Store den Nutzer in vielfältigen Lebens- und Arbeitsbereichen unterstützen. Die Brille lässt sich sowohl durch eine leichte Berührung des im rechten Bügel integrierten Touchpads als auch über Sprachbefehle steuern. Das im rechten oberen Blickfeld der Brille montierte Display kann diverse Informationen einblenden. Ziel ist es, all das an Diensten anbieten zu können, was heute ein Smartphone bereits erledigen kann, dabei jedoch gleichzeitig die Sicht des Nutzers nur geringfügig einzuschränken. So sollen Informationen zu Telefonanrufen, E-Mails oder SMS, GPS-Navigation oder zusätzliche Details über Personen und Gegenstände im Blickfeld des Trägers eingeblendet werden, ohne den Nutzer – anders als beim Smartphone – vom Fahren, Laufen oder anderen Tätigkeiten abzulenken. Zudem können mit Hilfe des integrierten Mikrofons und der Kamera, Ereignisse in der Umgebung des Nutzers aufgezeichnet werden. Diese Bild, Audio- und Videodaten können anschließend lokal gespeichert oder in die Cloud hochgeladen bzw. mit Freunden in sozialen Netzwerken geteilt werden. Ohne einen kontinuierlichen Internetzugang, der durch eine Verbindung zum Smartphone hergestellt wird, lässt sich Google Glass allerdings kaum sinnvoll nutzen.

Abb. 03 Schematische Darstellung eines Smartglass (Samsung GalaxyGlass)



Display und Kamera des Smartglass ist in der Peripherie des Sichtfeldes am Brillenrahmen montiert. Hardware zur Datenverarbeitung und Kommunikation sind im Brillengestell oder –bügel eingebaut.

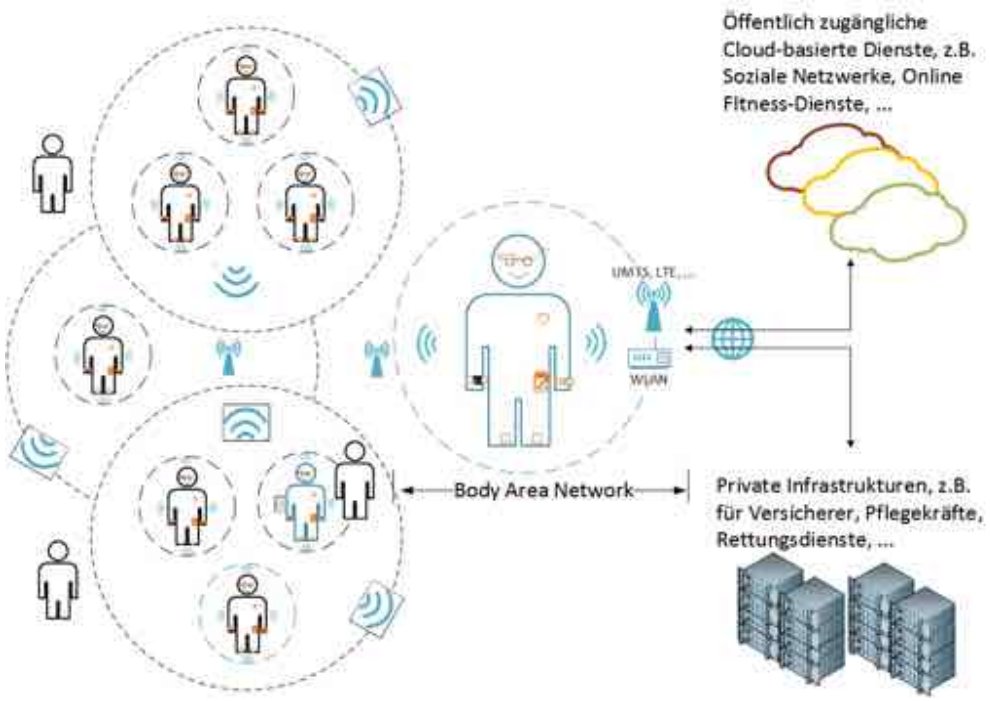


Abb. 04 Wearables: Geräte: Dienste und Kommunikation

4.3.3 Welche Daten fallen bei Smartwatches und intelligenten Brillen an?

Konto- und Registrierungsdaten

Um Wearables in vollem Umfang verwenden zu können, müssen Nutzer die Geräte i. d. R. online registrieren und für die unterschiedlichen Dienste Benutzerkonten anlegen. Dabei werden Daten wie (Profil-) Name, E-Mail-Adresse, Geschlecht und Geburtsdatum erfasst. Bei der Möglichkeit zur Einmalanmeldung, etwa über den bestehenden Facebook- oder Twitter-Account (sog. Single Sign-on, SSO)[114] werden auch dort gespeicherte Daten (teilweise) abgerufen und gespeichert. Beispiele hierfür sind Namen, Profilfoto, Wohnort und Freundesliste. Je nachdem, ob Bezahldienste mit dem Wearable genutzt werden, werden auch Daten wie Kreditkartenummer und Anschrift erfasst.

Nutzungsdaten

In Anschluss an eine erfolgreiche Registrierung werden Nutzer, insbesondere im Falle von Fitness- und Lifestyle-Geräten, gebeten, weitere Informationen über die eigene Person einzugeben. Diese können Angaben über Körpergröße, Gewicht, Schlafzeiten oder über verzehrte Lebensmittel und Getränke sein. Sobald die Geräte am Körper getragen bzw. aktiviert werden, erfassen sie kontinuierlich unterschiedliche Informationen über ihre Träger sowie deren Umgebung.

Bei Fitnessarmbändern sind dies Herzfrequenz, Blutdruck, Hauttemperatur, Umgebungstemperatur, aktueller Standort und Beschleunigungsdaten. Basierend auf diesen Daten werden für den Träger personalisierte Statistiken generiert, etwa Details über Schlafaktivitäten (Intensität und Dauer) und die zeitliche Verteilung des Kalorienverbrauchs, Anzahl gegangener Schritte, zurückgelegte Strecken und sonstige Tagesaktivitäten. Über eine entsprechende App für PC und Smartphone können Nutzer ihre Statistiken mit Freunden auf spezialisierten Plattformen teilen [115]. Dafür werden i. d. R. ein temporärer Zugriff auf die Kontaktliste im Smartphone und ein Zugriff auf einen externen Webserver vorausgesetzt. Bei der Nutzung der dedizierten App werden mittels unterschiedlicher Tracker-Technologien (u. a. Cookies und Web Beacons)[116] Details

über die Interaktion zwischen dem Träger des Wearable-Gerätes und der App bzw. zwischen dem Träger und dem Gerät gesammelt. Solche Informationen umfassen die Version der App, die zuvor besuchte IP-Adresse, die Zugangszeit, die Dauer der Nutzung, angeklickte Links sowie weitere Web-Metadaten, die z. B. aus dem Surfverhalten und der Suchmaschinennutzung entstehen.

Bei der Nutzung von intelligenten Brillen entstehen in erster Linie Foto-, Audio- und Videoaufnahmen von Individuen und Objekten in der unmittelbaren Umgebung des Trägers. Ähnlich wie bei Fitnessarmbändern fallen bei intelligenten Brillen Umweltdaten (Standort, Temperatur, Luftdruck usw.) und Web- bzw. Search-Metadaten an. Zumindest im Fall von Google Glass ist eine unmittelbare und kontinuierliche Übertragung aller ermittelbaren Daten in die Google Cloud für weitere Analysen vorgesehen.

Gerätspezifische Daten

Bei der Verwendung dedizierter Apps werden gerätspezifische Informationen gesammelt, etwa Gerätetyp, Geräteidentifikationsnummer, Name des Herstellers, Modell und Version des Betriebssystems. Über die bereits erwähnten Zugriffsmöglichkeiten auf Sensorschnittstellen können Diensteanbieter auch technische Merkmale der im Wearable-Gerät eingebauten Sensoren abfragen.

Ableitbare Daten

Eine regelmäßige und genaue Ermittlung von Standortdaten ermöglicht Rückschlüsse auf Bewegungen des Nutzers. In Verbindung mit externen (häufig öffentlich zugänglichen) Information können genaue Standortdaten konkreten Einrichtungen, wie etwa einem Supermarkt, einer religiösen Stätte oder einer Arztpraxis zugordnet werden. Damit besteht die Möglichkeit, Routinen und Lebensgewohnheiten der Nutzer abzuleiten. Eine Analyse der Informationen über Schlaf und körperliche Aktivitäten können nicht nur Details über Gesundheit und körperliche Fitness der Nutzer, sondern auch Hinweise auf mögliche Erkrankungen liefern. Darüber hinaus lassen sich mit Hilfe fortgeschrittener Bildanalyseverfahren Informationen aus Foto-, Audio- und Videoaufnahmen von Individuen und Objekten in der Umgebung der Brillenträger extrahieren.[117] Beispiele für derartige Daten sind Gesichter, markante Gebäude und Nummernschilder.

4.4 Rechtliche Rahmenbedingungen

Technik am Körper entfaltet zweierlei Wirkung: Einerseits sammelt sie Daten über den eigenen Körper, zur Selbstoptimierung und Sichtbarmachung der Körpereigenschaften. Dies unterliegt der allgemeinen Handlungsfreiheit, mit dem eigenen Körper tun und lassen zu können, wie einem beliebt. Sie dient auch der Persönlichkeitsentfaltung, indem der Körper vermessen wird und sich das Individuum mehr Selbsterkenntnis verschafft. In der Regel erfolgt der Einsatz der Technik freiwillig, so dass die informationelle Selbstbestimmung bzgl. der aufgezeichneten personenbezogenen Daten nicht berührt ist, solange die Verwendung der Daten dem Einzelnen bekannt ist. Eingeschränkt werden kann sie jedoch dann, wenn die Daten aus dem Gerät nicht lokal gespeichert, sondern an einen Server übermittelt, personenbezogene Daten womöglich in der Cloud weiterverarbeitet oder für fremde Zwecke verwendet werden, die vom Betroffenen bei der Nutzung nicht antizipiert waren.

Andererseits ermöglichen am Körper getragene Techniken ihrem Verwender Erkenntnisse über die eigene Umwelt zu erlangen. Persönlichkeitsrechte Dritter, welche in den Wirkungsbereich des Trägers eines Wearables gelangen, können verletzt werden. Beispielsweise genügt ein bloßer akustischer Befehl des Trägers an sein Smartglass, um nahezu unbemerkt Fotoaufnahmen von anderen Personen anzufertigen. Das bislang

erforderliche Anvisieren mit einer Kamera o. Ä. wird obsolet; für den Dritten ist das Erkennen des Aufnahmemodus nur schwer möglich. Das Recht am eigenen Bild resultiert aus dem allgemeinen Persönlichkeitsrecht und findet seine einfachgesetzliche Ausprägung im Kunsturheberrechtsgesetz (KunstUrhG). Es gewährt jedem Einzelnen das Recht, zu bestimmen, ob und in welchem Zusammenhang Bilder von ihm veröffentlicht werden und gerät in eine bislang noch unbekannte Gefährdungsposition, wenn das im Geheimen angefertigte Bild oder gesprochene Wort einer Person ohne dessen Wissen und Wollen aufgenommen, gespeichert oder gar in der Cloud weiterverarbeitet wird.[118] Bereits mit der Anfertigung des Bildes wird in das Selbstdarstellungsrecht des Betroffenen eingegriffen und das Bildnis in der konkreten Form der Kontrolle und Verfügungsgewalt des Abgebildeten entzogen.[119] Auch in geschützte Räume kann durch am Körper getragene Technik eingedrungen werden, etwa in die Wohnung einer Person. Art. 13 GG gewährleistet die Unverletzlichkeit der Wohnung nicht nur gegenüber dem Staat, sondern auch gegenüber Dritten.

Datenschutzrechtlich besteht die größte Hürde in der Bestimmung des anwendbaren Rechts, insbesondere bei Anwendungen, bei denen Daten nicht nur auf dem Gerät, sondern auf den Server des Anbieters geladen und dort verarbeitet werden. Befinden sich diese Server im außereuropäischen Ausland, sind sie dem Anwendungsbereich deutscher und europäischer Gesetze entzogen. Selbst wenn hiesige Datenschutzvorschriften, insbesondere Betroffenenrechte, anwendbar sind, weil die Daten im Inland erhoben wurden (§ 1 Abs. 5 BDSG), ist die Durchsetzung dieser Rechte u. U. mit erheblichen Schwierigkeiten verbunden.

Darüber hinaus stellt sich die Frage, inwiefern Produkte wie Google Glass und Smartwatches Telemedien sind, um bereichsspezifische Gesetze wie das Telemediengesetz zur Anwendung zu bringen.[120] Sollten nur die allgemeinen Regelungen des BDSG anwendbar sein, stellt sich insbesondere bei solchen Technologien, die Rechte Dritter beeinträchtigen können, die Frage, inwiefern diese nur zur familiären und persönlichen Zwecken dienen, da andernfalls die datenschutzrechtlichen Vorschriften zur Beurteilung der Zulässigkeit der Datenverarbeitung, insbesondere hinsichtlich der Abwägung der Interessen des Betroffenen nach § 28 BDSG, keine Anwendung finden würden.

Beim Tragen des Smartglasses oder der Smartwatch muss sich jede Person darüber im Klaren sein, dass eine Auswertung der mit Smartglasses aufgezeichneten Daten im außereuropäischen Ausland durchaus möglich ist und die Schutzvorkehrungen des europäischen und deutschen Datenschutzrechtes insofern leerlaufen könnten. Auf Basis der übermittelten GPS-Daten können beispielsweise Bewegungsprofile einer Person erstellt werden. Umso wichtiger ist es, etwa im Falle eines Verlustes oder Diebstahls solcher Geräte, die nötige Sorgfalt walten zu lassen und von der Möglichkeit des Remotezugriffes Gebrauch zu machen, um auf dem Gerät gespeicherte Daten alsbald löschen zu können.

Dritten, deren Rechte durch die unbefugte Nutzung eines Wearables verletzt worden sind, stehen die herkömmlichen Rechtswege offen. Der Träger des Wearables ist nicht nur zivilrechtlichen Ansprüchen[121] ausgesetzt, sondern bringt sich ggf. auch in die Gefahr einer strafrechtlichen Verfolgung,[122] wenn er widerrechtlich, d. h. ohne Zustimmung oder gegen den Willen eines Dritten, Aufnahmen anfertigt und diese anschließend im Internet verbreitet.

4.5 Privatheitsrisiken und Überwachungspotenziale

4.5.1 Smartglasses

Was Smartglasses von anderen Wearables besonders unterscheidet, ist ihr nach außen gerichteter visueller Beobachtungscharakter.[123] Zwar beinhaltet beispielsweise Google Glass auch zahlreiche andere Features und Innovationen wie Sprachsteuerung, Knochenleitungslautsprecher und Miniaturprojektor, aber insbesondere die das Sichtfeld des Trägers aufzeichnende Kamera erregt Bedenken.[124] An sich sind die Funktionen der Video- und Tonaufzeichnung sowie die Übermittlung von Standortdaten nicht neu und entsprechen den gängigen Funktionen eines Smartphones. Allerdings ist die Datenbrille von Google das erste mit dem Internet vernetzte, am Körper getragene Gerät, das dem Nutzer ermöglicht, seine Umwelt und die ihn umgebenden Personen ständig audiovisuell aufzunehmen, ohne dass diese Personen zwangsläufig davon erfahren. Zudem ist für Dritte nicht ersichtlich, ob die Kamera aktuell aktiviert ist. Und auch die Aktivierung der Kamera kann durch Augenzwinkern in einer für die Außenwelt sehr „versteckten" Art und Weise erfolgen.[125]

Durch die direkte Verbindungsmöglichkeit ins Internet, um Bilder und Videos in die Cloud zu laden, diese mit Freunden in sozialen Netzwerken zu teilen oder mit Hilfe von Apps einen Livestream zu schalten, gerät Bild- und Videomaterial, auf dem teilweise völlig unbekannte Personen zu sehen sind, in Echtzeit in die (Netz-)Öffentlichkeit. Hier wird gespeichert, kopiert, analysiert, zweckentfremdet, usw., d. h. der Smartglass-Träger kann leicht die Kontrolle über die gemachten Aufnahmen verlieren, obwohl er juristisch verantwortlich dafür ist, welche Inhalte er ins Netz lädt.

Es ist zudem davon auszugehen, dass der Anbieter einer Smartglass keine Möglichkeit außer Acht lassen wird, die anfallenden Daten kommerziell für sich nutzbar zu machen. Das fängt an beim Interesse an einer Vergrößerung des Bild- und Videodatenbestandes von Personen, um Algorithmen für Gesichtserkennung, die auf Basis von Abgleichsmechanismen mit umfangreichen Bilddatenbanken funktionieren, zu optimieren und reicht bis zu der Auswertung einzigartiger Einblicke in private und öffentliche Gebäude oder unzugängliches Gelände, wo eine digitale Vermessung bis jetzt an ihre Grenzen gestoßen ist. Der Nutzer selbst wird so immer mehr zum eigentlichen Lieferanten von Daten über sich, andere Personen und seine physische Umwelt; perfekte Voraussetzung also, um ein möglichst umfassendes Bild Einzelner oder Gruppen von Nutzern zeichnen zu können, deren Beeinflussung in Verhalten und Entscheidungen – sei es beim Kauf eines bestimmten Produktes oder der Wahl eines Staatsoberhauptes – damit möglich wird.[126]

Mit der Gesichtserkennung sorgte ein weiteres Feature von Google Glass, das jedoch nicht standardmäßig von Google vorgesehen war, für Aufsehen. Die Idee, in der Öffentlichkeit ständig identifizierbar zu sein, missfiel einem Großteil der Menschen. Nach anhaltenden Protesten reagierte Google im Sommer 2013 mit einem generellen für App-Entwickler geltenden Verbot solcher Programme.[127] Allerdings konnte dies nicht verhindern, dass weitere Gesichtserkennungs-Apps für Google Glass entwickelt und vermarktet wurden.[128]

Darüber hinaus besteht durch potenzielle Sicherheitslücken in der Software der Datenbrille die Möglichkeit, auf diese und ihre audiovisuellen Funktionen von außen zuzugreifen. Die Praxis zeigt, dass im Internet der Dinge Datensicherheit bis jetzt kaum eine Rolle spielt.[129] Und auch bei der Sicherheitsarchitektur für die von Google Glass verwendete Version des Android-Betriebssystems wurde offensichtlich nicht ausreichend viel Aufwand betrieben: Nach bereits zwei Stunden gelang 2013 einem Softwareentwickler, die volle Kontrolle über eine Developer-Version von Google Glass zu erlangen.[130]

Während sich ein Großteil der kritischen Stimmen vor allem dem nach außen und auf Dritte gerichteten Überwachungspotenzial der Datenbrille widmet, wird häufig übersehen, dass auch der Träger eines solchen Gerätes höchst private Informationen über sich preisgibt. Ein Beispiel dafür ist die von offizieller Seite nicht bestätigte Funktion eines Augen-Sensors, der Auskunft über die Weitung der Pupille bei Drogenkonsum oder die Fokussierung des Blicks auf bestimmte Personen oder Gegenstände im Sichtfeld des Nutzers geben könnte.[131] Aber auch bei der Sprachsteuerung, die auf Grundlage eines ständigen Abgleichs der Sprachdaten mit Inhalten auf den Servern der Anbieter personalisiert und optimiert wird,[132] fallen höchst sensible Daten an, über die der Nutzer nicht nur einwandfrei identifiziert werden kann,[133] sondern die auch Aufschluss über Herkunft (Akzent), Gesundheit (Sprachfehler) oder Gemütslage des Nutzers geben können. Im Gegensatz zu Smartphones ist bei einem Smartglass die Funktion der Sprachsteuerung durch innovative Steuerungsmöglichkeiten am Körper selbst ergänzbar. Beispielsweise wird gerade an einer Schnittstelle zur Gedankensteuerung auf Basis der Messung von elektrischen Impulsen des Gehirns gearbeitet,[134] was wiederum neue Fragestellungen zur Überwachung des Trägers mit sich bringt.[135]

Nicht nur in Deutschland, wo ein ausgewiesen kritischer Umgang mit technologischen Innovationen gepflegt wird und ausländische Unternehmen ihre neuen Produkte vor Markteinführung in anderen Ländern einem letzten Härtetest unterziehen, sondern auch in den USA hat sich gesellschaftlich und medial massiv Widerstand geregt: Ob in Restaurants, Kinos oder Krankenhäusern, eindeutige Verbotsschilder weisen immer häufiger deutlich auf das Unerwünschtsein Smartglass tragender Personen hin.[136] In den USA und vor allem San Francisco, wo durch die Nähe zum Silicon Valley überproportional viele technikaffine Menschen zu den Smartglass-Trägern gehören, werden solche *personae non gratae* mittlerweile sogar als „Glassholes" verspottet.[137]

Zudem scheinen auch die Kunden der Brille auszubleiben.[138] Obwohl generell Neugier und Interesse besteht, sind nur die wenigsten Privatnutzer tatsächlich dazu bereit, für ein Gerät, dessen alltäglicher Nutzwert gerade auch im Vergleich zum häufig identischen Funktionsumfang eines Smartphones fraglich ist, umgerechnet rund 1000 € auszugeben.[139] Nachdem sich in Deutschland die Einführung von Google Glass von Jahr zu Jahr verzögerte und auch der Mutterkonzern Investitionen in die Weiterentwicklung des Produktes massiv zurückfuhr,[140] beschloss Google schließlich Anfang 2015 den gesamten Verkauf der ersten Version der Brille an Privatnutzer einzustellen.[141] Indem man sich nun verstärkt auf hoch spezialisierte Berufsgruppen wie Ingenieure, Ärzte oder Polizisten als Abnehmer konzentriert, scheint sich ein Strategiewechsel bzgl. einer Markteinführung von Google Glass abzuzeichnen.[142]

Dies bedeutet aber auch, dass Smartglasses nicht vollständig vom Markt verschwinden werden, sondern zunächst einmal in Nischenbereichen ihren Einsatz finden, bevor ein erneuter Versuch gestartet wird, diese Technologie einer breiteren Masse schmackhaft zu machen. Zukünftige Innovationspotenziale im Bereich intelligenter Datenbrillen liegen zum einen in der weiteren Miniaturisierung des Gerätes. Hier wurde bereits ein Patent zur Entwicklung von Kontaktlinsen mit ähnlichem Funktionsumfang wie bei Google Glass eingereicht,[143] und zum anderen in neuartigen Steuerungsarten wie der erwähnten Gedankensteuerung.

4.5.2 Smartwatches und intelligente Armbänder

Smartwatches sind liegen im Trend, da sie auf dem bereits gängigen Accessoire der Armbanduhr aufbauen, relativ preiswert sind und im Gegensatz zu Smartglasses auf den ersten Blick keinen bedeutenden Eingriff in die eigene Privatheit oder die anderer vermuten lassen. Und auch das Tragen intelligenter Armbänder überschreitet keine kulturelle Barriere, was sie für ihre Träger zu unauffälligen aber immer präsenten Wegbegleitern macht.

Neben Möglichkeiten zur Kontrolle von anderen Geräten und zum Aufrufen bzw. Anzeigen von Informationen greift bei der Nutzung dieser Form von Wearables insbesondere der Trend zur Selbstvermessung um sich.[144] Hier ist eine regelrechte Bewegung entstanden, die sich zum Ziel gesetzt hat mit Hilfe von am Körper getragenen, datensammelnden Technologien ein tieferes Verständnis der Funktionsweise von Körper und Geist zu erlangen, um darauf aufbauend Selbstoptimierungsprozesse in Gang setzen zu können.[145] Die Datenauswertung findet auf Basis statistischer Verfahren statt und ist zumeist Teil eines Service, der im Rahmen einer App angeboten wird.

Obwohl der Selbstoptimierungsgedanke zentral ist, sind die konkreten Motive der Selbstvermessung vielfältig. Während der allmorgendliche Jogger an einer Messung des Pulses, der gelaufenen Schritte und seines allgemeinen Fitness-Zustandes interessiert ist,[146] versuchen ernährungsbewusste Nutzer ihre Wearables als Messinstrument für einen möglichst effektiv funktionierenden Ernährungsberater auf dem Smartphone einzusetzen.[147] Allerdings verschwimmen in der Praxis die Grenzen zwischen den Anwendungsbereichen Sport, Ernährung und Gesundheit. Viele Nutzer motiviert es zwar enorm, den technisch gestützten, inkrementellen Fortschritt z. B. beim Abnehmen beobachten und/oder ggf. ihr Verhalten bei Misserfolg anpassen zu können.[148] Die Motive der Selbstvermessung, wie schlank, muskulös oder besonders fit sein zu wollen, sollten jedoch sowohl mit Bezug auf das Individuum als auch auf die Gesellschaft kritisch betrachtet werden. Denn zum einen birgt die digitale Selbstvermessung die Gefahr eines individuellen Selbstoptimierungswahns, der durch die Quantifizier- und Kommunizierbarkeit des eigenen Verhaltens in Verbindung mit einem erhöhten sozialen Druck zusätzlich verstärkt wird. Dies ist beispielsweise bei der Selbstvermessung mit dem Ziel des Gewichtsverlustes und bestimmten Magersucht befürwortenden Communities zu beobachten.[149] Zum anderen verstärkt die Bewegung aber auch soziale Normierungsprozesse bzw. setzt diese in Gang, die neue Maßstäbe von Werten wie Gesundheit, Fitness und Schönheit definieren.

In den meisten Fällen werden die erfassten Körperdaten nicht nur auf dem Wearable oder dem dahinter geschalteten Smartphone gespeichert und verarbeitet, sondern auch der jeweilige App-Anbieter hat über Analyse- und Auswertungsservices ebenfalls Zugriff auf diese Daten, um anschließend ein Ergebnis präsentieren oder eine Empfehlung an den Nutzer aussprechen zu können.[150]

Obwohl gerade Gesundheitsdaten der datenschutzrechtlichen Kategorie besonderer Arten personenbezogener Daten und damit strengeren Regeln unterliegen, wächst der Markt mit solchen Daten weltweit besonders stark. Das Interesse an Gesundheits-, Körper- und Fitnessdaten ist insbesondere bei Versicherungen besonders groß. So haben erste Krankenkassen auf den Trend der Selbstvermessung reagiert und neue Bonusprogramme in Verbindung mit dem Angebot einer entsprechenden App ins Leben gerufen, wodurch nachweislich gesundheitsbewusstes Verhalten von Versicherten prämiert werden soll.[151]

Die bei der Selbstvermessung umfangreich anfallenden Daten können schlussendlich auch dazu beitragen, das ohnehin schon recht präzise Bild eines Nutzers weiter zu schärfen, um ihn in seinen Entscheidungen noch besser verstehen und leiten zu können. Zumindest der zugrunde liegende Gedanke der selbstbestimmten Optimierung wird durch diese Form und Möglichkeit der Manipulation und Fremdbestimmung ad absurdum geführt.

5
Schlussdiskussion

5.1 Zusammenfassung

Mit dem „Internet der Dinge“ tritt die moderne Datenverarbeitung abermals in eine neue Phase ein. Dabei wird die Menge der anfallenden Daten in den kommenden Jahren weiter massiv ansteigen. Immer mehr Geräte werden in Zukunft mit dem Internet verbunden sein und somit auch eine Kommunikation der Geräte untereinander ermöglichen. Die Einführung netzbasierter Zusatzfunktionen fügt sich in die Benutzung allerdings meist dermaßen unsichtbar ein, sodass den Nutzerinnen und Nutzern kaum noch ersichtlich ist, wie viele Daten wo, wann und zu welchem Zweck erhoben werden.

Dies wiederum hat Auswirkungen auf die Privatheit der Nutzer selbst und zunehmend auch auf die Privatheit anderer, sich in Sensornähe aufhaltender Menschen.

Das White Paper zeigt anhand dreier Anwendungsbereiche auf, wo und wie das versteckte Internet zu Hause, im Auto und am Körper Gefährdungen von informationeller Selbstbestimmung und Privatheit mit sich bringt.

Zu Hause: Smart TV

Fernseher sind heutzutage weniger reine Empfangsgeräte als vielmehr komplexe Multimediageräte, die über zahlreiche Zusatzfunktionen und Schnittstellen verfügen. Dabei fallen eine Reihe von Daten an: Schon beim gewöhnlichen Fernsehen werden Nutzungs- und Verhaltensdaten erhoben. Über die in moderne Smart TVs eingebauten Sensoren können mithilfe von Foto-, Audio- und Videoaufnahmen Hausbewohner und Besucher identifiziert werden. Im Zuge der Verbreitung anmeldepflichtiger Dienste fallen Konto- und Registrierungsdaten an, die dazu verwendet werden können, Rückschlüsse auf Persönlichkeitsmerkmale und private Attribute zu geben. Durch die Auswertung von Nutzungs- und Verhaltensdaten können politische Einstellung, Hobbys, Bildungsgrad oder ethnischer Hintergrund abgeleitet werden. Die Hinzuziehung von Sensor- und gerätspezifischen Daten ermöglicht darüber hinaus Einblicke in Gewohnheiten oder familiäre Verhältnisse. Alles in allem bieten moderne Smart TVs somit die Möglichkeit einer gezielten Überwachung einzelner Personen bis hin zur Massenüberwachung aller Smart TV-Nutzer und stellen somit eine Gefährdung der informationellen wie der lokalen Privatheit dar.

Im Auto: Smart Car

Auch das ehemals rein mechanisch betriebene Transportmittel Auto wurde in den vergangenen Jahrzehnten kontinuierlich um informationstechnische Komponenten erweitert. Smart Cars erfassen fahrzeugbezogene Daten, das Verhalten des Fahrers und der Insassen sowie Daten über die Umgebung und übermitteln diese über drahtlose Kommunikationsschnittstellen an andere Verkehrsteilnehmer, die Verkehrsinfrastruktur und an die Fahrzeughersteller. Gerade aus der Interaktion mit dem Fahrzeug entsteht eine Vielzahl an Nutzungsdaten, die einen Einblick in wesentliche Teile der Lebensgestaltung bieten können. Durch die Verknüpfung mit Konto-, Registrierungs- und fahrzeugspezifischen Daten sind Rückschlüsse auf Fahrstil, Aufenthaltsort und zurückgelegte Fahrstrecke möglich. Kombiniert mit weiteren Daten können daraus schließlich persönliche Attribute und Gewohnheiten abgeleitet werden.

Am Körper: Wearables

Durch intelligente Armbänder wird es möglich, Gesundheitsdaten zu sammeln und diese mithilfe des heimischen Computers zu analysieren und ggf. über das Internet an einen Diensteanbieter weiterzuleiten. Damit setzt sich ein Trend fort, der mit dem Erfolg von Smartphones einen ersten Höhepunkt erreichte: Ständig mit dem Internet verbundene Geräten erfassen private Lebensumstände auch im öffentlichen Raum und stellen diese meist diskret Dritten zur Verfügung.

Die neueste Generation tragbarer vernetzter Geräte in Form von Smartwatches und Smartglasses bietet darüber hinaus die Möglichkeit einer umfassenden, unauffälligen und permanenten Erfassung von Daten über die Träger und deren Umgebung sowie die Möglichkeit der unmittelbaren, automatisierten Verarbeitung und Weiterleitung der erfassten Daten. Die auf diesem Wege gewonnenen Informationen ermöglichen einen tiefgehenden, detaillierten Einblick in das Leben und die Gedankenwelt der Nutzer. Foto-, Audio- und Videoaufnahmen betreffen darüber hinaus insbesondere Interaktionen mit der Umwelt, sodass über die Träger hinaus andere Personen betroffen sein können.

Privatheitsrisiken und Überwachungspotenziale

Das versteckte Internet zu Hause, im Auto und am Körper birgt also vielfältige Gefahren für die informationelle Selbstbestimmung und Privatheit der Nutzer: Vielfach ist es gar nicht mehr möglich zu erkennen, welche Daten wann, zu welchem Zweck und wohin übertragen werden. Die Intransparenz von Datenerhebungen und Tracking von Personen führen zu einer Erosion der Entscheidungsfreiheit. Mängel in der Sicherheitsarchitektur der Geräte bergen das Risiko der Offenlegung vertraulicher Daten, des Identitätsdiebstahls und der Wirtschaftsspionage. Dadurch werden Tracking und Profilbildung und letztendlich sogar eine gezielte Überwachung von Nutzern möglich, von denen nicht nur die Nutzer der Geräte betroffen sind, sondern auch Unbeteiligte, die sich in der Reichweite der verwendeten Sensoren aufhalten.

5.2 Gestaltungspotenziale und Herausforderungen

Mehr Transparenz für ein selbstbestimmtes Leben im digitalen Zeitalter?

Um den Risiken entgegenzutreten, mit denen die Privatheit von Nutzern konfrontiert ist, wird in der öffentlichen Debatte vielfach mehr Transparenz gefordert.[152]

Diese Forderung bedeutet, in Bezug auf das versteckte Internet die Einbindung netzbasierter Funktionen aus Sicht der Nutzerinnen und Nutzer erfahrbarer zu machen: Also nach einer klaren Kommunikation darüber, welche Daten wann, für wie lange und zu welchem Zweck gesammelt werden und welche diesbezüglichen Rechte die Betroffenen besitzen.

Transparenz als einem grundlegenden Datenschutzprinzip kommt hinsichtlich des Schutzes der informationellen Selbstbestimmung eine in jedem Fall wichtige Funktion zu: So kann ein Hinweis in den Allgemeinen Geschäftsbedingungen (AGBs) oder den Nutzungsbestimmungen durchaus die Erfordernisse des Transparenzgebots erfüllen, wenn die Nutzer zu Beginn eines Vorgangs über die Art, den Umfang und den Zweck der Erhebung in allgemein verständlicher Form unterrichtet werden.

Doch stößt das Transparenzgebot ohne begleitende Maßnahmen angesichts sich ausweitender intransparenter Datenmärkte, des zunehmend allgegenwärtigen Internets der Dinge und nicht zuletzt im Zuge des Anwachsens von Big Data-Analysen auch vielfach an seine Grenzen.

Intransparente Datenmärkte und ihr Überwachungspotenzial

Daten sind längst zum zentralen Rohstoff vieler IKT-Anwendungen und -Unternehmen geworden, und auch außerhalb der einzelnen Unternehmens finden Daten Verwendung. In der Tat haben die zahlreichen neuen IKT-Anwendungen und die oft automatisiert im Hintergrund ablaufende Erhebung und Speicherung von Daten zu der Entstehung sog. „Datenmärkte" geführt, in denen Daten auch zwischen Unternehmen gehandelt werden.[153] Die involvierten Unternehmen konzentrieren sich auf die kommerzielle Verwendung und Weiterverarbeitung der von ihnen erhobenen Nutzerdaten.[154] Unklar ist indes, welche Unternehmen im deutschsprachigen Raum die relevanten Akteure in diesen Datenmärkten sind und wie ihre jeweiligen Geschäftsmodelle beim Handel mit Daten konkret aussehen. Auch lässt sich die reale Ausgestaltung der Wertschöpfungskette bisher aufgrund fehlender Informationen kaum nachvollziehen. Hinzu kommt der Umstand, dass es auch für Individuen momentan nur wenig ersichtlich ist, in welcher Form Unternehmen ihre persönlichen Nutzer- und Nutzungsdaten verarbeiten und welchen monetären Wert ihre Daten besitzen.[155]

Intransparente Datenübertragungen sind aber auch im Verhältnis zwischen Unternehmen und Behörden keine Ausnahme, sondern die Regel: So hat der NSA-Skandal verdeutlicht, in welchem Maße Nachrichtendienste eine Praxis der offenen und verdeckten Datenbeschaffung aus Unternehmensnetzwerken pflegen, um diese für Überwachungs- und Strafverfolgungszwecke zu verwenden. Neben Metadaten, also Verbindungs- und Verkehrsdaten, handelt es sich hierbei häufig auch um Inhaltsdaten.[156] Neben Geheimdiensten nutzen aber auch die Polizei und andere Behörden von Unternehmen erhobene Daten. So steigert die starke Verbreitung von sozialen Netzwerken beispielsweise deren Attraktivität für Behörden, da sie hier mögliche Informationsquellen zur Strafverfolgung ausmachen.[157]

Eigenverantwortung und Selbstdatenschutz

Doch wird die Gewährleistung von Transparenz nicht allein durch die Intransparenz der Datenmärkte erschwert: Daneben führen allgegenwärtige Datenschutzprobleme schon heute dazu, dass Nutzer mit der Informationsflut, die es für einen funktionierenden (Selbst-) Datenschutz im Blick zu behalten gilt, überfordert sind.[158] Und je mehr Geräte in das Internet der Dinge integriert werden, umso schwerer wird es für den Einzelnen sein, den Überblick über die Masse an Daten zu behalten und einen verantwortungsvollen Umgang damit zu pflegen. Symbole, die bestimmte Datenerhebungs- oder Verarbeitungsszwecke einfach verständlich kennzeichnen, sind dabei die eine Möglichkeit. Eine Flut an schwer verständlichen Informationen, die zwar Transparenz herstellen sollen, aber letztlich aufgrund ihrer Komplexität – wie schon heute die meisten AGBs und Datenschutzbestimmungen – weggeklickt werden, sind dagegen die Kehrseite. Im Internet und auf PCs existiert u. a. mit Verschlüsselungs- und Anonymisierungstools immerhin eine Reihe von Möglichkeiten, mit denen bei ausreichend Interesse, Zeit und technologischem Verständnis ein Selbstdatenschutz realisierbar ist. Im Internet der Dinge, das aus „smarten" Endgeräten besteht, die sich im Gegensatz zu ihren nicht smarten Vorgängern meist kaum konfigurieren lassen, fehlen – insbesondere bei Smart Cars und Wearables – vergleichbare Techniken bisweilen. Existierende Möglichkeiten sind entweder sehr rudimentär, wie das Abkleben der Smart TV-Kamera, oder driften ab ins Impraktikable, wenn etwa empfohlen wird, das Smart TV erst gar nicht mit dem Internet zu verbinden, womit allerdings auch wünschenswerte Zusatzfunktionen nicht mehr nutzbar sind, die meist überhaupt der Grund für die Anschaffung eines Smart TVs sein dürften.

Zweckbindung und Big Data-Analysen

Schließlich stößt das Transparenzgebot durch Big Data-Analysen schlicht an seine Grenzen: Big Data-Analysen zeichnen sich gerade durch das Auffinden von Zusammenhängen auf, wo vorher keine erkennbar waren. Damit können durch die Analyse vieler Daten aus unterschiedlichen Datenbanken neuartige Verwendungszwecke gefunden werden, die sich erst im Ergebnis der Big Data-Analyse erschließen und somit auch nicht im Vorfeld im Sinne des Transparenzgebots kommuniziert werden können.

Die Zukunft der informationellen Selbstbestimmung und Implikationen für die Technikentwicklung

Der herausgearbeitete Befund ist deutlich: Bisherige Ansätze des Datenschutzes werden angesichts der technischen Entwicklungen zunehmend dysfunktional und müssen ergänzt werden. Das Datenschutz-Ziel der Transparenz bedarf daher einer entsprechenden Erweiterung durch weitere Datenschutzprinzipien[159] und deren Umsetzung durch Hersteller, Anbieter und Politik, um volle Wirksamkeit entfalten zu können.

Der berechtigte Ruf nach Transparenz darf also nicht dafür genutzt werden, die Gewährleistung einer sicheren Nutzung des Internets der Dinge vollständig in den Verantwortungsbereich der Einzelnen zu verlagern.

Stattdessen sollten Hersteller und Anbieter schon bei der Konzeption und Implementierung ihrer Produkte auf eine datenschutzkonforme Ausgestaltung achten. Datenvermeidung, also die Gestaltung der Systeme dergestalt, dass von Anfang an so wenige Daten wie möglich erhoben werden, bewirkt eine Verringerung des Risikos: Wo gar keine personenbezogenen Daten sind, können diese nicht missbraucht werden.[160] Mit technischen und organisatorischen Maßnahmen muss zudem dafür gesorgt werden, dass die erforderlichen personenbezogenen Daten nur rein zweckgebunden verwendet werden und sich nicht über verschiedene Kontexte verknüpfen lassen, z. B. zu Profilen über die Nutzer.[161]

Darüber hinaus sind Verfahren so zu gestalten, dass alle daran beteiligten Akteure (Betroffene, datenverarbeitende Stellen, Aufsichtsbehörden) dazu befähigt werden, Einfluss auf die Datenverarbeitungsprozesse zu nehmen.[162] Für die Betroffenen bedeutet dies im Speziellen, dass sie ihre Rechte effektiv wahrnehmen können: Dazu gehören Berichtigungs- und Löschungsansprüche sowie das Recht auf Widerruf einer zuvor erteilten Einwilligung.

Derzeitig werden durch die Hersteller die datenverarbeitenden Prozesse, die damit verbundenen Risiken und Möglichkeiten für Nutzer ungenügend dargestellt, um jenen die Folgen ihrer (Einwilligungs-) Entscheidungen vollends zu vergegenwärtigen. Daher müssen die Hersteller ein ganz besonderes Augenmerk auf die Gestaltung der Benutzungsoberflächen legen. Dabei ist es wichtig, entsprechende Hinweise auf die Aufnahmefähigkeit und -bereitschaft des Nutzers abzustimmen. Dies kann durch die Hersteller auf unterschiedlichem Wege erfolgen: Bereits beim Verkauf des Produkts muss eine umfassende, allgemeine Information für die späteren Nutzer bereitgestellt werden. Im Sinne des Verbraucherschutzes wäre hierbei z. B. die Einführung eines entsprechenden Piktogramms oder Icons auf der Verpackung des Produkts denkbar, das bereits optisch beim Kauf des Produktes auf dessen Internetkonnektivität hinweist.[163] Zudem wäre es sinnvoll, dem Nutzer situationsbezogen Informationen per visuellem oder akustischem Signal zukommen zu lassen. Allerdings nicht nur vorab, sondern auch während des Betriebs, wenn dies im konkreten Fall erforderlich ist. Dies ist mindestens dann der Fall, wenn die bekannte Nutzungsweise des Gerätes erstmalig um neue Funktionen ergänzt wird, aber auch regelmäßig, wenn ein smartes Gerät Foto-, Audio- oder Videoaufnahmen macht oder machen möchte. Die Nutzer sollen durch auf dem Display erscheinende allgemeine Hinweise befähigt werden, selbst zu entscheiden, ob und vor

allem in welcher Detailfülle sie weitergehende Erläuterungen wünschen. Dieses Konzept ist als „Layered Policy Design" bekannt.

Da ein Schutz nicht nur für die Nutzerinnen und Nutzer bestehen soll, die ihr System umkonfigurieren wollen, ist „Privacy by Default" wichtig: Dementsprechend müssen die smarten Systeme bereits im Auslieferungszustand mit datenschutzfreundlichen Grundeinstellungen versehen sein. Im Falle der Smart TVs würde dies beispielsweise erfordern, dass eine Aktivierung und Verbindung mit dem Internet oder der Sensoren trotz eines eingesteckten LAN-Kabels erst dann erfolgt, wenn die Nutzerinnen und Nutzer diese Funktionen nach Erhalt eines entsprechenden Hinweises gesondert und bewusst aktivieren. Eine sinnvolle Nutzung der Produkte muss auch in der Grundeinstellung möglich sein.

Auch vonseiten der Politik können Maßnahmen ergriffen werden, um eine datenschutzfreundlichere Ausgestaltung smarter Technologien zu erzielen. So könnten bereits klare, zeitgemäße rechtliche Rahmenbedingungen, wie sie etwa durch die EU-Datenschutz-Grundverordnung geschaffen werden sollen, die angesprochenen Ansätze forcieren und damit zukunftsweisende Vorgaben zur Gewährleistung von Privatheit im digitalen Zeitalter schaffen.

Erforderlich ist demnach, dass institutionell und rechtlich verankerte Datenschutzprinzipien einen Rahmen setzen, der gegenüber den Nutzern eine akzeptable Verarbeitung ihrer Daten gewährleistet. Selbst wenn die Einrichtung eines solchen institutionellen und rechtlichen Rahmens gelingt, bleibt aber das Problem, dass Nutzerinnen und Nutzer nicht unbedingt alles mit ihren Daten geschehen lassen wollen, was rechtlich erlaubt ist. Wenn sich beispielsweise die Gesetze auf die Regelung von Datenmärkten richten, bleibt immer noch die Frage, ob man überhaupt an solch einem Markt teilnehmen möchte. Die Frage der Balance zwischen Entscheidungen durch Individuen einerseits und Staaten und Unternehmen andererseits bleibt eine Konstante gesellschaftlicher Auseinandersetzung und somit auch weiterhin ein wichtiges Forschungsfeld.

Hier ist auch zu erwägen, welche Institutionen und sozialen Prozesse (z. B. Verbraucherschutzverbände oder Initiativen zur Schulung von Medienkompetenz) jenseits von individueller Entscheidung oder juristischer Festsetzung das Niveau des Datenschutzes verbessern können. Die Initiative „Marktwächter Digitale Welt" ist in diesem Zusammenhang hervorzuheben: Als gemeinsames Vorhaben des Verbraucherzentrale Bundesverbandes (vzbv) und der Verbraucherzentralen der Länder beobachten sog. Marktwächter[164] nicht nur die Strukturen der digitalen Welt, sondern sammeln und werten auch Verbraucherbeschwerden aus. Nach der Devise „Erkennen – Informieren – Handeln" sollen die Marktwächter helfen, bestehende Missstände an die zuständigen Aufsichtsbehörden zu melden und die Rechte der Verbraucher durchzusetzen. Aus dieser und hoffentlich weiteren Initiativen könnten wertvolle Impulse gewonnen werden, wie etwa die Entwicklung von Best-Practice-Modellen im Bereich der AGB-Gestaltung.

Ein verantwortungsbewusster Umgang mit modernen Technologien kann dann gelingen, wenn sich der Staat seiner Schutzpflichten bewusst ist, wirtschaftliche Akteure ihren Gestaltungsspielraum zur Herstellung sicherer Technologien gewissenhaft nutzen und Nutzerinnen und Nutzer ihr Bewusstsein im Umgang mit ihren Daten schärfen.

Anmerkungen

[1]Der in diesem White Paper verwendete Begriff „verstecktes Internet“ ist klar von den eher technisch geprägten Termini Deep Web, Dark Net, Hidden oder Invisible Web bzw. Verstecktes Web, die sich vor allem auf nicht von Suchmaschinen erfasste und somit schwer auffindbare Internetinhalte beziehen, abzugrenzen.

[2] Mattern, F.; Flörkemeier, C. (2010): Vom Internet der Computer zum Internet der Dinge. In: Informatik-Spektrum 33, Nr. 2, S. 107-121.

[3] So ist es z. B. Anbietern von Tastatur-Apps wie SwiftKey und Swype, die ein schnelleres Schreiben auf der virtuellen Tastatur ermöglichen, durch ihre AGB erlaubt, die eingegebenen Schreibinhalte zu speichern und weiterzuverarbeiten, vgl. http://swiftkey.com/en/privacy/ bzw. http://www.nuance.com/company/company-overview/company-policies/privacy-policies/index.htm (24.02.2015); Steinschaden, J. (2014): SwiftKey: Die Smartphone-Tastatur, die gerne nach Hause telefoniert. In: Online Magazin Netzpiloten.de, erschienen am: 17.06.2014, http://www.netzpiloten.de/swiftkey-die-smartphone-tastatur-die-gerne-nach-hause-telefoniert/ (26.11.14).

[4] In der vergangenen Jahren hat es sich eingebürgert, informationstechnisch angereicherte Gegenstände des täglichen Gebrauchs als „intelligent“ oder „smart“ zu bezeichnen, ohne dass sich eine einheitliche Sprachregelung entwickelt hätte. Mit Intelligenz im herkömmlichen Sinne hat diese Bezeichnung wenig zu tun, vielmehr folgen sie der Bedeutung des englischen Begriffs „intelligence“. Dieser kann schlicht mit „Informationen“ übersetzt werden, auf denen die Funktionalität „intelligenter Systeme“ basieren.

[5] Arabo, A., Brown, I., & El-Moussa, F. (2012): Privacy in the age of mobility and smart devices in smart homes. In: Privacy, Security, Risk and Trust (PASSAT), 2012 International Confernece on Social Computing (SocialCom), IEEE, S. 819-826; Dötzer, F. (2006): Privacy issues in vehicular ad hoc networks. In: Privacy enhancing technologies, Berlin Heidelberg: Springer, S. 197-209; Raij, A., Ghosh, A., Kumar, S., & Srivastava, M. (2011): Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, S. 11-20.

[6] Meyer, S.; Schulze, E.; Helten, F.; Fischer, B. (2001): Vernetztes Wohnen: Die Informatisierung des Alltagslebens. Berlin: Edition Sigma.

[7] Deloitte (2013): Licht ins Dunkel – Erfolgsfaktoren für das Smart Home. In: Studienreihe intelligente Netze, Stand 11/2013, https://www2.deloitte.com/content/dam/Deloitte/de/Documents/technology-media-telecommunications/TMT-Studie_Smart%20Home.pdf (14.07.2015).

[8] PwC (2013): Media Trend Outlook – Smart-TV: Mehrwert für den Konsumenten, mehr Umsatz für die Medienbranche, 11/2013, www.pwc.de/de/technologie-medien-und-telekommunikation/assets/whitepaper-smart-tv.pdf (14.11.2014).

[9] Gartner (2014): Gartner Says a Typical Family Home Could Contain More Than 500 Smart Devices by 2022. In: Newsroom, erschienen am: 8.9.2014, www.gartner.com/newsroom/id/2839717 (13.11.2014).

[10] Naughton, K. (2015): Putting the Mobile into Automobile. In: Bloomberg Businessweek (4410), S. 30-32.

[11] Telefónica (2013): Connected Car Branchenbericht 2013, erschienen am: 20.06.2013, https://blog.telefonica.de/wp-content/uploads/2023/06/Telefonica-Digital-Connected-Car-Report-GERMAN-2013-06-20.pdf (13.11.2014).

Anmerkungen

[12] Gartner (2013): What to Expect at CES 2014 - Connected Cars. In: Newsroom, erschienen am: 11.12.2013, http://www.gartner.com/newsroom/id/2636121 (13.11.2014).

[13] Stephen, M. (2014): Connected Cars – Getting on the Information Highway. In: Canadian Plastics 72, Nr. 4, S. 14-18.

[14] PwC (2014): The Wearable Future. In: Consumer Intelligence Series, erschienen am: 10.2014, http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/assets/PWC-CIS-Wearable-future.pdf (12.11.2014).

[15] Rössler, B. (2001): Der Wert des Privaten. Frankfurt am Main: Suhrkamp.

[16] Habermas, J. (1990): Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft. Frankfurt: Suhrkamp.

[17] Habermas, J. (1995): Theorie des kommunikativen Handelns. Bd. I: Handlungsrationalität und gesellschaftliche Rationalisierung. Frankfurt: Suhrkamp.

[18] Altman, I. (1975): The environment and social behavior: Privacy, Personal space, Territory, Crowding. Monterey, Calif.: Brooks/Cole Publishers.

[19] Westin, A. F. (1967): Privacy and freedom. New York: Atheneum.

[20] Nicht verschwiegen werden soll die normative Ambivalenz räumlicher Privatheit, welche sich daran zeigt, dass neuere Privatheitstheorien eben auch negativ konnotierte Funktionen des räumlichen Privatheitstyps ausmachen. Vgl. hierzu: MacKinnon, C. A. (1989): Toward A Feminist Theory Of The State. Cambridge: Harvard University Press. Oder: Allen, A. L. (2003): Why Privacy Isn't Everything. Lanham, Maryland: Rowman & Littlefield Publishers. Dessen ungeachtet geht es uns in diesem Papier v. a. um die Transformationseffekte der behandelten Technologien, und weniger um eine normative Bewertung dieser oder jener Privatheitsform bzw. ihrer Veränderung oder ihres Verlustes.

[21] Giddens, A. (1995): Die Konstitution der Gesellschaft. Grundzüge einer Theorie der Strukturierung. Frankfurt: Campus.

[22] Goffman, E. (1973): The Presentation of Self in Everyday Life. Woodstock/New York: The Overlook Press.

[23] Vgl. Elias, N. (2006): L'espace privé: „Privatraum" oder „privater Raum"? In: Ders.: Aufsätze und andere Schrifften II. Frankfurt a.M.: Suhrkamp, S. 345-359.

[24] Höflich, J. R. (2003): Mensch, Computer und Kommunikation. Frankfurt: Peter Lang.

[25] Marvin, C. (1988): When old technologies were new: Thinking about electric communication in the late nineteenth century. New York: Oxford University Press, S. 96-97.

[26] Friedewald, M. (2009): Der Computer als Werkzeug und Medium: Die geistigen und technischen Wurzeln des Personal Computers. 2., korrigierte Aufl. Berlin und Diepholz: GNT-Verlag (Aachener Beiträge zur Wissenschafts- und Technikgeschichte des 20. Jahrhunderts, 3); Reeves, B.; Nass, C. I. (1996): The Media Equation: How People Treat Computers, Televisions, and New Media like Real People and Places. Stanford, CA: CSLI Publications.

[27] Tomorrow Focus Media AG (2013): Smart TV-Effects 2013-1, erschienen am: 01.06.2013, www.tomorrow-focus-media.de/uploads/tx_mjstudien/Smart_TVEffects_2013-I_neuerMaster.pdf (11.12.2014).

[28] Silverstone, R.; Haddon, L. (1996): Design and the domestication of information and communication technologies: Technical change and everyday life. In: Silverstone, R.;

Anmerkungen

Mansell, R. (Hrsg.), Communication by design: The politics of information and communication technologies. Oxford: Oxford University Press, S. 44-74.

[29] Quandt, T., & Pape, T. V. (2010): Living in the mediatope: a multimethod study on the evolution of media technologies in the domestic environment. In: The Information Society 26, Nr. 5, S. 330-345.

[30] Hertlein, K. M.; Blumer, M. L. C. (2013): The couple and the family technology framework: Intimate relationships in a digital age. New York, NY: Routledge.

[31] Dostert, Elisabeth (2015): IT für ältere Menschen - Wie Technologie Senioren zu mehr Freiheit verhelfen soll. In: Sueddeutsche.de, erschienen am: 11.02.2015, http://www.sueddeutsche.de/digital/technologie-fuer-senioren-mehr-freiheit-ohne-stigma-1.2344622 Siehe auch: Fraunhofer-Allianz Ambient Assisted Living (AAL). Online: http://aal.fraunhofer.de/index.html (10.03.2015).

[32] Statista (2010): Wie wird sich der Markt für Smart Home bis 2020 entwickeln? Online: http://de.statista.com/statistik/daten/studie/183271/umfrage/prognose-zur-entwicklung-von-smart-home-aus-sicht-der-hersteller/ (16.11.2014).

[33] PwC (2013): Media Trend Outlook – Smart-TV: Mehrwert für den Konsumenten, mehr Umsatz für die Medienbranche, Online: www.pwc.de/de/technologie-medien-und-telekommunikation/assets/whitepaper-smart-tv.pdf (14.11.2014).

[34] ETSI (2012): ETSI TS 102 796 V1.2.1. Online: http://www.etsi.org/deliver/etsi_ts/102700_102799/102796/01.02.01_60/ts_102796v010201p.pdf (16.11.2014).

[35] Deutsche TV Plattform (2014): Deutsche TV Plattform. Online: http://www.tv-plattform.de/images/stories/pdf/marktanalyse_smart-tv_2014_de.pdf (17.11.2014).

[36] BLM (2012): HbbTV beinhaltet Chancen für Lokalfernsehen - Smart-TV-Anwendungen können Reichweiten und Umsätze lokaler TV-Anbieter erhöhen. Online: http://www.blm.de/de/infothek/pressemitteilungen/2012.cfm?object_ID=436 (16.11.2014).

[37] Kuri, J. (2013): CE Week: Der Kampf um den "Second Screen". In: heise.de, erschienen am: 28.06.2013, http://www.heise.de/newsticker/meldung/CE-Week-Der-Kampf-um-den-Second-Screen-1902324.html (16.11.2014).

[38] Vgl. PwC 2013.

[39] Ghiglieri, M. (2014): I Know What You Watched Last Sunday - A New Survey Of Privacy In HbbTV, Workshop Web 2.0 Security & Privacy 2014 in conjunction with the IEEE Symposium on Security and Privacy. San Jose, CA, USA.

[40] Vgl. Ghiglieri 2014: S. 5 f.

[41] Kim, Yeong Gon, et al. (2012): Multimodal Biometric Systems and Its Application in Smart TV. Computer Applications for Database, Education, and Ubiquitous Computing. Springer. 219-226. Berlin Heidelberg; Lendino, J. (2014): Panasonic Unveils Voice-Activated TVs With Facial Recognition. In: PCMag, erschienen am: 06.01.2014, http://www.pcmag.com/article2/0,2817,2429165,00.asp (16.11.2014).

[42] BVerfGE 18, 121 (131 f.).

43 BVerfGE 42, 212 (219); 89, 1 (12); Gornig, G. (2011): v. Mangoldt/Klein/Starck – Kommentar zum Grundgesetz Bd. 1, 6. Aufl., München: Vahlen, Art. 13 GG, Rn. 1; Kühne, J.-D. (2011): Sachs – Grundgesetz Kommentar, 6. Aufl., München: Beck, Art. 13 GG, Rn. 9.

[44] BGHSt 44, 138 (140); Jarass: Jarass/Pieroth – Grundgesetz für die Bundesrepublik Deutschland, 12. Aufl., , München: Beck, Art. 10 GG, Rn. 4; Gornig, G. (2010): v.

Mangoldt/Klein/Starck – Kommentar zum Grundgesetz Bd. 1, 6. Aufl., München: Vahlen, Art. 13 GG, Rn. 15.

[45] Lang, H (2014): Beck'scher Online-Kommentar GG , Ed. 23, München: C. H. Beck, Art. 2 GG, Rn. 46.

[46] BVerfGE 120, 274

[47] Ausführlich: Skistims, H. (erscheint vsl. 2015): Smart Home, Kassel: Dissertation Universität Kassel, S. 275 ff.

[48] Vgl. Raabe, O.; Weis, E. (2014): Datenschutz im „SmartHome". In: Recht der Datenverarbeitung (RDV) 2014, S. 231 (234).

[49] 22% Prozent der Smart TV-Besitzer wissen nicht, ob ihr Fernseher mit dem Internet verbunden ist und 46% sind nicht über die Möglichkeiten von HbbTV informiert. Vgl. PwC 2013.

[50] Vgl. Doctor Beet's Blog (2013): LG Smart TVs logging USB filenames and viewing info to LG servers. In: DoctorBeet's Blog, erschienen am: 18.11.2013, http://doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html (03.12.2014); Vgl. Ghiglieri 2014; Heise Online (2013): LG Smart TVs spähen Nutzer aus. In: Heise Online, erschienen am: 21.11.2013, http://www.heise.de/newsticker/meldung/LG-Smart-TVs-spaehen-Nutzer-aus-2051973.html (02.12.2014).

[51] Ghiglieri, M.; Lange, B.; Simo, H.; Waidner, M. (vsl. 2015): Security and Privacy bei Smart TVs: Bedrohungspotential und technische Lösungsansätze. Fraunhofer-Institut für Sichere Informationstechnologie SIT.

[52] Price, M. (2014): I'm Terrified of My New TV: Why I'm Scared to Turn This Thing On — And You'd Be, Too. In: Brennan Center for Justice at New York University School of Law, erschienen am: 30.10.2014, http://www.brennancenter.org/analysis/im-terrified-my-new-tv-why-im-scared-turn-thing (02.12.2014).

[53] Vgl. Ghiglieri 2014; Heise Online 2013; sowie: Ghiglieri, M.; Oswald, F.; Tews, E. (2013): HbbTV – I Know What You Are Watching. In: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): 13. Deutscher IT-Sicherheitskongress des BSI. Informationssicherheit stärken – Vertrauen in die Zukunft schaffen. SecuMedia Verlags-GmbH S. 225–238.

[54] Ganz in diesem Sinne etwa sieht Norbert Elias „die Öffentlichkeit" dort beginnen, wo der Privatraum seines Appartements endet: Sinngemäß beschreibt er die Türen seines Hauses als Grenze, und alles dahinterliegende als Öffentlichkeit, weshalb selbst der Wald, zu dem die Hintertür führt, Öffentlichkeit darstelle (Elias 2006: 346). Während die Reduktion der Bestimmung von Privatheit auf diese Dichotomie zu kurz griffe, muss eine zeitgemäße Privatheitstheorie doch in der Lage sein, diese zu integrieren; hier ist nicht der Ort um dies auszubuchstabieren, weshalb wir lediglich anmerken wollen, dass die skizzierte Dichotomie eine Form darstellt, in der die Unterscheidung öffentlich/privat praktiziert wird.

[55] Nissenbaum, H. (2009): Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press.

[56] Ebenda.

[57] Kingsley, D.; Urry, J. (2009): After the car. Cambridge: Polity Press.

[58] Böhm, S.; Jones, C.; Land, C.; Paterson, M. (2006): Part one conceptualizing automobility: Introduction: Impossibilities of automobility. In: The Sociological Review 54, Nr. 1, S. 1-16.

Anmerkungen

[59] Sheller, M.; Urry, J. (2003): Mobile transformations of ‚public' and 'private' life. In: Theory, Culture & Society 20, Nr. 3, S. 107-125.

[60] Insbesondere in den Fünfziger und Sechziger Jahren des vergangenen Jahrhunderts galt das Auto für viele Jungendliche und junge Erwachsene als ein intimer Rückzugsort in einem ansonsten konservativen Umfeld. Diese meist romantischen Begegnungen wurden als *car date* bezeichnet.

[61] Vgl. Kingsley; Urry 2009.

[62] Böhm, S.; Jones, C.; Land, C.; Paterson, M. (2006): Part one Conceptualizing Automobility: Introduction: Impossibilities of automobility. In: The Sociological Review 54, Nr. 1, S. 1-16.

[63] Shaheen, S.; Cohen, A. P. (2012): Carsharing and Personal Vehicle Services: Worldwide Market Developments and Emerging Trends. In: International Journal of Sustainable Transportation 7, Nr. 1, S. 5-34.

[64] Vgl. Kingsley; Urry 2009.

[65] Europäische Kommission (2007). Für eine europaweit sicherere, sauberere und effizientere Mobilität: Erster Bericht über die Initiative „Intelligentes Fahrzeug". KOM(2007) 541 endg. Brüssel.

[66] BMBF Projekt INVENT „Intelligenter Verkehr und nutzergerechte Technik". 2002-2005. Online: http://www.invent-online.de/index.html

[67] http://de.euroncap.com/de/rewards/bmw_assist_advanced_ecall.aspx (30.03.2015).

[68] Dirscherl, H.-C. (2013): Google und Audi entwickeln Android-Infotainment-System. In: PCWelt, erschienen am: 30.12.2013, http://www.pcwelt.de/news/Google_und_Audi_entwickeln_Android-Infotainment-System-CES_2014-8372073.html (12.02.2015).

[69] Heise Online (2014): Signal Iduna analysiert Fahrstil für individuelle Kfz-Versicherung. In: Heise Online, erschienen am: 30.10.2014, http://www.heise.de/newsticker/meldung/Signal-Iduna-analysiert-Fahrstil-fuer-individuelle-Kfz-Versicherung-2438280.html?wt_mc=nl.ho (15.02.2015). Jüngst plant die HUK-Coburg als größter Autoversicherung in Deutschland die Anpassung ihrer Tarife an das Fahrverhalten ihrer Kunden. Vgl. Deutsche HandwerksZeitung vom 22.05.2015: Kfz-Versicherer: Überwachung von Autofahrern geplant. Abrufbar unter: http://www.deutsche-handwerks-zeitung.de/kfz-versicherer-ueberwachung-von-autofahrern-geplant/150/3097/294067 (15.06.2015).

[70] Charette, R. N. (2009). This Car Runs on Code. In: IEEE Spectrum, erschienen am: 01.02.2009, http://www.spectrum.ieee.org/feb09/7649 (04.02.2015).

[71] Kuther, T. (2008): Netzwerke im Auto - CAN, LIN, FlexRay – Stand und Chancen der Bussysteme. In: Elektronik Praxis, erschienen am: 10.03.2008, http://www.elektronikpraxis.vogel.de/themen/hardwareentwicklung/datenkommunikationsics/articles/111425/ (13.01.2015).

[72] Deutscher Verkehrssicherheitsrat e.V. (2014). Einführung eines Event Data Recorders - Beschluss des DVR-Vorstands vom 23. Mai 2014 auf der Basis der Empfehlung des Vorstandsausschusses Fahrzeugtechnik unter Mitberatung der Vorstandsausschüsse Erwachsene Verkehrsteilnehmer und Recht. Online: http://www.dvr.de/dvr/vorstandsbeschluesse/ft_eventdatarecorder.htm (23.02.2015).

[73] FAZ.NET (2015): Dobrindt plant Teststrecke für selbstfahrende Autos. In: FAZ.NET, erschienen am: 25.01.2015, http://www.faz.net/aktuell/wirtschaft/neue-mobilitaet/f-a-z-exklusiv-dobrindt-plant-teststrecke-fuer-selbstfahrende-autos-13390268.html (23.02.2015).

[74] Stockburger, C (2014): Automatische Parkplatzsuche: Los, auf die Plätze, fertig. In: Spiegel Online, erschienen am: 03.02.2014, http://www.spiegel.de/auto/aktuell/automatische-parkplatzsuche-mit-sensoren-und-apps-a-945229.html (23.02.2015).

[75] United States Government Accountability Office (2013): In-Car Location Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers. Report to the Chairman, Subcommittee on Privacy, Technology and the Law, Committee on the Judiciary, U. S. Senate, December 2013. Online: http://www.gao.gov/assets/660/659509.pdf (23.02.2015).

[76] Wittich, H. (2014): EKG im Autositz, Sensoren sollen Müdigkeit erfassen. In: Auto Motor und Sport, erschienen am: 15.07.2014, http://www.auto-motor-und-sport.de/news/ekg-im-autositz-sensoren-sollen-muedigkeit-erfassen-8465721.html (23.02.2015).

[77] Pudenz, K. (2011): Lenkradintegrierte Sensoreinheit erfasst Vitalfunktionen. In: ATZ-online.de, erschienen am: 04.11.2011, http://www.springerprofessional.de/lenkradintegrierte-sensoreinheit-erfasst-vitalfunktionen-14805/3951454.html (23.02.2015).

[78] Dewri, R.; Annadata, P.; Eltarjaman, W.; Thurimella, R. (2013): Inferring Trip Destinations From Driving Habits Data. In: Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society (WPES '13). ACM, New York, NY, USA, S. 267-272. Online: http://doi.acm.org/10.1145/2517840.2517871 (16.03.2015).

[79] Weichert, T. (2014): Datenschutz im Auto – Teil 1. In: Straßenverkehrsrecht (SVR) 2014, 201 (204); Kremer, S.: Connected Car – intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz? In: Recht der Datenverarbeitung (RDV) 2014, 240 (244); Roßnagel, A. (2014): Fahrzeugdaten – wer darf über sie entscheiden? Zuordnungen – Ansprüche – Haftung. In: Straßenverkehrsrecht (SVR) 2014, 281.

[80] Weichert, T. (2014): Datenschutz im Auto – Teil 1. In: Straßenverkehrsrecht (SVR) 2014, 201 (205); Roßnagel, A. (2014): Fahrzeugdaten – wer darf über sie entscheiden? Zuordnungen – Ansprüche – Haftung. In: Straßenverkehrsrecht (SVR) 2014, 281.

[81] BVerfGE 120, 274.

[82] BVerfGE 120, 274 (314 f.); Hoffmann-Riem, W. (2008): Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, Juristenzeitung (JZ) 2008, 1009 (1011); Schulz, T.: Autonome Systeme, Dissertation Universität Kassel i. E. 2015, Seite 262.

[83] BVerfGE 65, 1 (43).

[84] Detailliert zu den einzelnen Fallgestaltungen vgl. Weichert, T. (2014): Datenschutz im Auto – Teil 1. In: Straßenverkehrsrecht (SVR) 2014, 201 ff; Weichert, T. (2014): Datenschutz im Auto – Teil 2. In: Straßenverkehrsrecht (SVR) 2014, 241 ff.; Roßnagel, A. (2014): Fahrzeugdaten – wer darf über sie entscheiden? Zuordnungen – Ansprüche – Haftung. In: Straßenverkehrsrecht (SVR) 2014, 281 (283).

[85] Schulz, T.: Autonome Systeme, Dissertation Universität Kassel i. E. 2015, Seite 172 f.; ebenso Weichert, T. (2014): Datenschutz im Auto – Teil 1. In: Straßenverkehrsrecht (SVR) 2014, 201 (203).

[86] Abdelhamid, S.; Hassanein, H. S.; Takahara, G. (2014): Vehicle as a Mobile Sensor. In: Procedia Computer Science, Nr. 34, S. 286-295.

[87] Biermann, K. (2013): Wer zu hart bremst, verliert seinen Versicherungsrabatt. In: Zeit Online, erschienen am: 13. November 2013, http://www.zeit.de/digital/datenschutz/2013-11/versicherung-telematik-ueberwachung-kfz (28.11.2014).

Anmerkungen

[88] Weyer, J. (2006). Die Zukunft des Autos – das Auto der Zukunft. Wird der Computer den Menschen ersetzen? Soziologische Arbeitspapiere 14. Dortmund: Wirtschafts- und Sozialwissenschaftliche Fakultät, Universität Dortmund.

[89] Rähm, J. (2015): Computer Electronics Show – Smarte Elektronik auf dem Vormarsch. In: Deutschlandfunk, erschienen am: 11.01.2014, http://www.deutschlandfunk.de/computer-electronics-show-smarte-elektronik-auf-dem.684.de.html?dram:article_id=274320 (23.02.2015).

[90] Selke, S. (2014): Lifelogging als soziales Medium? – Selbstsorge, Selbstvermessung und Selbstthematisierung im Zeitalter der Digitalität, in: Jähnert, J.; Förster, C. (Hrsg.): Technologien für digitale Innovationen, Interdisziplinäre Beiträge zur Informationsverarbeitung, Wiesbaden: Springer VS, S. 173-200, S. 185-186, 196.

[91] Beck, U. (1986): Risikogesellschaft: Auf dem Weg in eine andere Moderne. Frankfurt am Main: Suhrkamp, S. 217.

[92] Foucault, M. (1993): Technologien des Selbst, in: Martin, L.; Gutman, H.; Hutton, P. (Hrsg.): Technologien des Selbst, Frankfurt a.M.: Fischer, S. 24-62, 190 S., S. 26.

[93] Leistert, O.; Röhle, T. (2011), Identifizieren, Verbinden, Verkaufen, in: Dies. (Hrsg.), Generation Facebook, Über das Leben im Social Net, Bielefeld: Transcript, S. 7-30, 283 S., S. 22.

[94] Simmel, G. (2013): Soziologie: Untersuchungen über die Formen der Vergesellschaftung. Frankfurt: Suhrkamp.

[95] Vgl. Goffman 1973.

[96] Vgl. Goffman 1973, S. 208 ff.

[97] Vgl. Giddens 1995, S. 215.

[98] Vgl. Goffman 1973, S. 137.

[99] Fortunati, L. ; Katz, J. ; Riccini, R. (2003). Introduction. In: Dies. (Hrsg.): Mediating the Human Body: Technology, Communication, and Fashion. Mahwah, NJ: Lawrence Erlbaum Associates. S. 1-11.

[100] Satyanarayanan, M. (2001): Pervasive computing: Vision and challenges. In: Personal Communications, IEEE 8.4. S. 10-17.

[101] Gane, N.; Beer, D. (2008) New Media: The Key Concepts. Oxford: Berg.

[102] Farman, J. (2012): Mobile Interface Theory: Embodied Space and Locative Media. New York: Routledge. De Souza e Silva, A.; Frith, J. (2010): Locational Privacy in Public Spaces: Media Discourse on Location-Aware Mobile Technologies. In: Communication, Culture & Critique 3, Nr. 4, S. 503-525.

[103] Berry, M.; Hamilton, M. (2010). Changing Urban Spaces: Mobile Phones on Trains. In: Mobilities 5, Nr. 1. S. 111-129.

[104] Vgl. De Souza e Silva; Frith 2010.

[105] Katz, J. (2013): Mobile gazing two-ways: Visual layering as an emerging mobile communication service. In: Mobile Media & Communication 1, Nr. 1. S. 129-133.

[106] Pew Research Center (2014): Public Perceptions of Privacy and Security in the Post-Snowden Era. Erschienen am: 12.11.2014, http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (12.12.2014).

[107] Pew Research Center (2013): Location-Based Services. Erschienen am: 12.09.2013, http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Location-based%20services%202013.pdf (12.12.2014).

Anmerkungen

[108] "What's a Wearable?". Online: http://www.media.mit.edu/wearables/ (30.03.2015); "Ubiquitous Computing". Online: http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Ubiquitous_computing.html (30.03.2015).

[109] Bilton, N. (2012): Wearable Computers Are the Next Big Devices, Report Says. In: Bits, erschienen am: 17.04.2012, http://bits.blogs.nytimes.com/2012/04/17/wearable-computers-are-the-next-platform-wars-report-says/ (04.03.2015). BITKOM (2014): Die Zukunft der Consumer Electronics. Online: http://www.bitkom.org/files/documents/140908_CE-Studie_Online.pdf (30.03.2015).

[110] Accenture Interactive (2014): State of the Internet of Things Study from Accenture Interactive Predicts 69 Percent of Consumers Will Own an In-Home IoT Device by 2019. Online: http://newsroom.accenture.com/news/2014-state-of-the-internet-of-things-study-from-accenture-interactive-predicts-69-percent-of-consumers-will-own-an-in-home-iot-device-by-2019.htm (30.03.2015).

[111] Leo K. (2014): CES 2014: Sony shows off life logging app and kit. In: BBC News Technology, erschienen am: 07.01.2014, http://www.bbc.co.uk/news/technology-25633647 (16.03.2015).

[112] Christl, W. (2014): Kommerzielle Digitale Überwachung im Alltag. Studie im Auftrag der österreichischen Bunderarbeitskammer, Cracked Labs - Institut für Kritische Digitale Kultur, Wien, Österreich.

[113] Bieber, G.; Fernholz, N.; Gaerber, M. (2013): Anomalienerkennung durch Analyse der körperlichen Aktivität, Fraunhofer IGD, Rostock; Angelini, L et. al (2013): Designing a Desirable Smart Bracelet for Older Adults, University of Applied Sciences and Arts Western Switzerland, Fribourg, Switzerland; Rhodes, H. (2014): Accessing and Using Data from Wearable Fitness Devices. In: Journal of AHIMA 85, no. 9, S. 48-50.

[114] Biennier, F. (2011): Web Single Sign On and SAML. In: Encyclopedia of Cryptography and Security. Springer US, S. 1377-1382.

[115] Z. B. mit der neuen iOS-8-App „Health".

[116] Simo H.; Kelbert F.; Shirazi F.; Wüchner T.; Buchmann J.; Pretschner A.; Waidner M. (2012): State of Online Privacy: A Technical Perspective. In: Buchmann J. (Hrsg.) Internet Privacy - Eine multidisziplinäre Bestandsaufnahme / A Multidisciplinary Analysis. Springer: Berlin.

[117] Starbug (2014): Ich sehe, also bin ich ... Du. Gefahren von Kameras für (biometrische) Authentifizierungsverfahren. In: CCC Congress 2014, erschienen am: 29.12.2014, https://events.ccc.de/congress/2014/Fahrplan/events/6450.html (16.03.2015); Rawlinson, K. (2015): Facial recognition technology: How well does it work? In: BBC News, erschienen am: 03.02.2015, http://www.bbc.com/news/technology-31112604 (16.03.2015).

[118] Solmecke, C.; Kocatepe, S. (2014): Google Glass – Der Gläserne Mensch 2.0. In: Zeitschrift für Datenschutz (ZD) 2014, S. 23 f..

[119] Dreier, T.; Schulze, G. (2006): Urheberrechtsgesetz. 2. Aufl., München: C. H. Beck. § 22 KUG, Rn. 13 m.w.N.; Götting, H. P. In: Schricker, G.; Loewenheim U. (2010), Urheberrecht, 4. Aufl., München: C. H. Beck. § 22 KUG, Rn. 5, 35 m.w.N.; OLG Karlsruhe: Neue Juristische Wochenschrift (*NJW) 1982, 123*.

[120] Solmecke; Kocatepe 2014: S. 24 f.; Schwenke, T. (2013): Google Glass - Eine Herausforderung für das Recht. In: Kommunikation und Recht (K&R) 2013, S. 689.

[121] Gegen den Verbreiter bestehen Unterlassungsansprüche aus § 1004 Abs. 1 S. 2 BGB analog i.V.m. § 823 Abs. 2 BGB i.V.m. §§ 22, 23 KUG; Schadensersatzansprüche folgen aus § 823 Abs. 2 BGB i.V.m. §§ 22, 23 KUG. Weiterhin sind auch der Ersatz immaterieller Schäden, sowie Herausgabe- und Vernichtungsansprüche denkbar.

Anmerkungen

[122] Vgl. § 201 StGB, § 201a StGB; § 33 Abs. 1 KUG. Zudem kann der Betroffene gegen den Träger des Wearables wirksam von seinem Notwehrrecht Gebrauch Machen und letzterem ggf. das Smartglass abnehmen, OLG Hamburg, AfP 2012, 392.

[123] Für einen aktuellen Überblick zu Wearables und Privatheitsrisiken siehe z. B. Zeno Group (Imperial College) (2014): The Wearables Privacy Report, erschienen im Oktober 2014, https://workspace.imperial.ac.uk/business-school/Public/research/ZENO%20GROUP%20PUL%20Framework%20with%20foreword.pdf (09.01.2015).

[124] Biermann, K. (2012): Google Glass ist "cool, aber verwirrend". In: Zeit Online, erschienen am: 12.09.2012, http://www.zeit.de/digital/mobil/2012-09/google-glass-test (12.01.2015); Lesnes, C. (2013): Les Google Glass déjà regardées de travers. In: Le Monde - M le magazine du Monde, erschienen am: 21.03.2014, http://www.lemonde.fr/le-magazine/article/2014/03/21/les-google-glass-deja-regardees-de-travers_4386476_1616923.html (15.01.2015); Cano, R. J. (2013): Google Glass llegará en 2014. In: El País Online, erschienen am: 23.04.2013, http://tecnologia.elpais.com/tecnologia/2013/04/23/actualidad/1366719454_230981.html (17.01.2015).

[125] Heise Online (2013): Google-Glass-Update: Unbemerkt knipsen per Zwinkern. In: Heise Online, erschienen am: 18.12.2013, http://www.heise.de/newsticker/meldung/Google-Glass-Update-Unbemerkt-knipsen-per-Zwinkern-2068429.html (18.01.2015).

[126] Duhigg, C. (2012): Campaigns Mine Personal Lives to Get Out Vote. In: The New York Times, erschienen am: 13.10.2012, http://www.nytimes.com/2012/10/14/us/politics/campaigns-mine-personal-lives-to-get-out-vote.html?pagewanted=all&_r=0 (18.02.2015).

[127] Zeit Online (2013): Google Glass: Google verbietet Gesichtserkennung in der Datenbrille. In: Zeit Online, erschienen am: 01.06.2013, http://www.zeit.de/digital/mobil/2013-06/google-glass-gesichtserkennung-verbot (11.01.2015).

[128] Schulz, S. (2014): App für Gesichtserkennung. „Seien Sie kein Fremder!". In: Frankfurter Allgemeine Zeitung, erschienen am: 13.01.2014, http://www.faz.net/aktuell/feuilleton/medien/app-fuer-gesichtserkennung-seien-sie-kein-fremder-12749493.html (13.01.2015).

[129] Siehe hierzu beispielsweise: HP Report (2014): Internet of Things Research Study. Hewlett-Packard Development Company, erschienen im September 2014, http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en (11.01.2015); Heise Online (2015): Das Internet der (verräterischen) Dinge: Heimvernetzung weckt Interesse von Angreifern. In: Heise Online, erschienen am: 22.01.2015, http://www.heise.de/newsticker/meldung/Das-Internet-der-verraeterischen-Dinge-Heimvernetzung-weckt-Interesse-von-Angreifern-2523737.html (23.01.2015); Thoma, J. (2013): Elektronische Wegfahrsperre: Kaum Updates trotz Unsicherheiten. In: Golem.de, erschienen am: 06.07.2013, http://www.golem.de/news/elektronische-wegfahrsperre-kaum-updates-trotz-unsicherheiten-1307-100235.html (22.01.2015); Symantec (2014): How safe is your quantified self? Tracking, monitoring, and wearable tech. In: Symantec Official Blog, Symantec Corporation, erschienen am: 30.07.2014, http://www.symantec.com/connect/blogs/how-safe-your-quantified-self-tracking-monitoring-and-wearable-tech (24.01.2015).

[130] Spiegel Online (2013): Datenbrille: Google Glass ist schon gehackt. In: Spiegel Online, erschienen am: 28.04.2013, http://www.spiegel.de/netzwelt/gadgets/datenbrille-google-glass-ist-schon-gehackt-a-897034.html (05.12.2014).

[131] Postinett, A. (2014): Zukunft von Google Glass getrübt. Die große Pleite im Silicon Valley. In: Handelsblatt, erschienen am: 19.11.2014, http://www.handelsblatt.com/unternehmen/it-medien/zukunft-von-google-glass-getruebt-die-grosse-pleite-im-silicon-valley/10998866.html (05.12.2014).

[132] Jasinski, M. (2013): Die inoffizielle deutsche Siri-Referenz - Das umfassende Nachschlagewerk für Apples Sprachsteuerung - über 500 Befehle. 2. Auflage. Berlin: epubli, S. 65.

[133] Talbot, D. (2012): Siris großer Bruder. In: Technology Review, erschienen am: 10.07.2012, http://www.heise.de/tr/artikel/Siris-grosser-Bruder-1635042.html (19.01.2015).

[134] Lee, D. (2014): Google Glass hack allows brainwave control. In: BBC News, erschienen am: 09.07.2014, http://www.bbc.com/news/technology-28237582 (06.12.2014).

[135] Hallinan, D.; Schütz, P.; Friedewald, M.; Hert, P. d. (2015): Wer kann sie erraten? In: Süddeutsche Zeitung vom 31. Januar/1. Februar 2015, S. 17.

[136] Beuth, P. (2013): Google Glass: Verbotszonen für Google Glass. In: Zeit Online, erschienen am: 08.05.2013, http://www.zeit.de/digital/mobil/2013-05/google-glass-verboten (14.01.2015).

[137] Lobo, S. (2013): Googles fahrlässige Glass-Kampagne. In: Spiegel Online, erschienen am: 07.05.2013, http://www.spiegel.de/netzwelt/web/sascha-lobo-googles-fahrlaessige-glass-kampagne-a-898512.html (14.01.2015).

[138] Wohlsen, M. (2014): Failure Is the Best Thing That Could Happen to Google Glass. In: Wired.com, erschienen am: 15.04.2014, http://www.wired.com/2014/04/failure-is-the-best-thing-that-could-happen-to-google-glass/ (19.012015).

[139] Clauß, U. (2015): Warum Googles Datenbrille an Produktbetrug grenzt. In: Welt Online, erschienen am: 25.01.2015, http://www.welt.de/debatte/kommentare/article136740013/Warum-Googles-Datenbrille-an-Produktbetrug-grenzt.html (29.01.2015).

[140] Donath, A. (2014): Datenbrille: Google Glass erscheint nicht mehr dieses Jahr. In: Golem.de, erschienen am: 17.11.2014, http://www.golem.de/news/datenbrille-google-glass-erscheint-nicht-mehr-dieses-jahr-1411-110578.html (20.01.2015); Oreskovic, A.; McBride, S.; Nayak, M. (2014): Google Glass future clouded as some early believers lose faith. In: Reuters, erschienen am: 14.11.2014, http://www.reuters.com/article/2014/11/14/us-google-glass-insight-idUSKCN0IY18E20141114 (20.01.2015).

[141] FAZ Online (2015): Google stoppt den Verkauf seiner Datenbrille. In: Faz.net, erschienen am: 15.01.2015, http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google/google-glass-neuanfang-fuer-die-datenbrille-13372678.html (20.01.2015).

[142] Sauter, M. (2014): Google Glass: New Yorks Polizei probiert Datenbrille aus. In: Golem.de, erschienen am: 06.02.2014, http://www.golem.de/news/google-glass-new-yorks-polizei-probiert-datenbrille-aus-1402-104403.html (20.01.2015); Heise Online (2014): Polizei: Mit Google Glass gegen Verkehrssünder. In: Heise Online, erschienen am: 13.03.2014, http://www.golem.de/news/polizei-mit-google-glass-gegen-verkehrssuender-1405-106646.html (19.01.2015).

[143] Donath, A. (2014): Nachfolger von Google Glass: Google patentiert Kontaktlinsen mit Kameras. In: Golem.de, erschienen am: 15.04.2014, http://www.golem.de/news/nachfolger-von-google-glass-google-patentiert-kontaktlinsen-mit-kameras-1404-105895.html (19.01.2015).

[144] Janssen, J.-K. (2012): Das vermessene Ich. In: c't, Nr. 18/12 (2012), http://www.heise.de/ct/artikel/Das-vermessene-Ich-1662987.html (19.01.2015).

Anmerkungen

[145] Zillien, N.; Fröhlich G.; Dötsch, M. (2015): Zahlenkörper. In: Hahn, K.; Stempfhuber, M. (Hrsg.): Präsenzen 2.0 - Körperinszenierungen in Medienkulturen. Wiesbaden: Springer, 2015, S. 77–94.

[146] Berliner Morgenpost (2015): Fitness-Tracker – Selbstvermessung liegt im Trend. In: Berliner Morgenpost, erschienen am: 25.01.2015, http://www.morgenpost.de/web-wissen/fit-in-berlin/article136759045/Fitness-Tracker-Selbstvermessung-liegt-im-Trend.html (29.01.2015).

[147] Als Beispiel siehe hierzu: Heise Online. „Fitness-Tracker fürs Ohr überwacht die Essgewohnheiten. In: Heise Online, erschienen am: 14. November 2014. http://www.heise.de/newsticker/meldung/Fitness-Tracker-fuers-Ohr-ueberwacht-die-Essgewohnheiten-2457645.html (19.01.2015).

[148] Grannemann, K.. (2014): Gesundheits-Apps. Das große Geschäft mit Wearables. In: Wirtschaftswoche, erschienen am: 01.08.2014, http://www.wiwo.de/technologie/gadgets/gesundheits-apps-das-grosse-geschaeft-mit-wearables-/10280576.html (07.12.2014).

[149] Mahdawi, A. (2014): The Unhealthy Side of Wearable Fitness Devices. In: The Guardian, erschienen am: 03.01.2014, http://www.theguardian.com/commentisfree/2014/jan/03/unhealthy-wearable-fitness-devices-calories-eating-disorders-nike-fuelband (09.01.2015); Boero, N.; Pascoe, C. J. (2012): Pro-Anorexia Communities and Online Interaction: Bringing the Pro-Ana Body Online. In: Body & Society, Vol. 18, Nr. 2, S. 27–57, erschienen am: 01.06.2012, http://bod.sagepub.com/content/18/2/27.short (09.01.2015).

[150] Lobe, A. (2014): Mein Körper ist meine App. In: Der Tagesspiegel Online, erschienen am: 08.08.2014, http://www.tagesspiegel.de/medien/die-vermessung-des-ich-mein-koerper-ist-meine-app/10310504.html (28.01.2015).

[151] Wohin diese Form des manchmal totalitär anmutenden Gesundheitswahns führen kann, beschreibt Juli Zeh in ihrem bereits 2009 veröffentlichten Buch Corpus Delicti. Vgl. außerdem: Brüggen-Freye, C. (2014): Kassen nutzen Fitness-Apps zur Datensammlung. In: Welt Online, erschienen am: 20.05.2014, http://www.welt.de/wirtschaft/webwelt/article128208548/Kassen-nutzen-Fitness-Apps-zur-Datensammlung.html (07.12.2014).

[152] Article 29 Data Protection Working Party (2014): Opinion 8/2014 on the Recent Developments on the Internet of Things. Adopted on 16 September 2014. Online: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (30.01.2015). Maas, H. (2015): Raus aus der digitalen Bronzezeit! In: Zeit Online, erschienen am: 28.01.2015, http://www.zeit.de/digital/datenschutz/2015-01/datenschutz-internet-europa-heiko-maas/komplettansicht (02.03.2015).

[153] Schreiner, M.; Hess, T. (2012): Ökonomie der Privatsphäre: Eine Annäherung aus drei Perspektiven. In: DuD - Datenschutz und Datensicherheit 36, Nr. 2, S. 105-109.

[154] Gustafson T., und Fink D. (2013).Winning within the data value chain. Innosight. http://www.innosight.com/innovation-resources/strategy-innovation/winning-within-the-data-value-chain.cfm (Abgerufen am: 17.07.2015) sowie Schermann, M., Krcmar, H., Hemsen, H., Markl, V., Buchmüller, T. B., and Hoeren, T.(2014). Big Data – Eine interdisziplinäre Chance für die Wirtschaftsinformatik. Wirtschaftsinformatik 5/2014, S. 281-287.

[155] Vgl. Schreiner; Hess 2012.

[156] Greenwald, G. (2014): Die globale Überwachung: Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen. München: Droemer Knaur.

Anmerkungen

[157] Unabhängiges Landeszentrum für Datenschutz (2012): Polizeiliche Recherchen in sozialen Netzwerken zu Zwecken der Gefahrenabwehr und Strafverfolgung. Erschienen am: 12.03.2012, https://www.datenschutzzentrum.de/polizei/20120312-polizeiliche-recherche-soziale-netzwerke.pdf (17.07.2015).

[158] Karaboga, M.; Masur, P.; Matzner, T. et al. (2014): White Paper Selbstdatenschutz. 2. Aufl. Karlsruhe: Fraunhofer ISI (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt). https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf (25.02.2015).

[159] Die sog. Datenschutzziele liefern hierzu einen wertvollen Impuls. Hierzu Rost, M.; Pfitzmann, A. (2009): Datenschutz-Schutzziele – revisited. In: DuD - Datenschutz und Datensicherheit 33, Nr. 6, S. 353-358; Rost, M.; Bock, K. (2011): Privacy by Design und die Neuen Schutzziele: Grundsätze, Ziele und Anforderungen. In: DuD - Datenschutz und Datensicherheit 35, Nr. 1, S. 30-35.

[160] Einige Smart TV-Hersteller und Fernsehanstalten folgten diesem Beispiel bereits und haben seit dem Bekanntwerden von unnötigen Datenerfassungen diese inzwischen gestoppt. Vgl. Ghiglieri 2014.

[161] Dies entspricht dem Datenschutzziel der Nicht-Verkettbarkeit.

[162] Vgl. das hierin enthaltene Datenschutzziel der Intervenierbarkeit.

[163] Derartige optische Hinweis- und Logopflichten auf Produkten sind auf EU-Ebene bereits für sog. RFID-Produkte für Hersteller verpflichtend.

[164] Vgl. hierzu die Pressemitteilung des Verbraucherzentrale Bundesverbandes: Aufbau der Marktwächter startet, http://www.vzbv.de/pressemeldung/aufbau-der-marktwaechter-startet (26.01.2015).

Anhang

Glossar

Ambient Assisted Living (AAL)	AAL steht für intelligente Umgebungen, die sich selbstständig, proaktiv und situationsspezifisch den Bedürfnissen und Zielen von Nutzerinnen und Nutzern anpassen, um sie im täglichen Leben zu unterstützen. Intelligente Umgebungen sollen insbesondere auch älteren, behinderten und pflegebedürftigen Menschen ermöglichen, selbstbestimmt in einer privaten Umgebung zu leben.
Augmented Reality	Mit Augmented Reality (erweiterte Realität) wird die computergestützte Erweiterung der Realitätswahrnehmung bezeichnet. Häufig fallen darunter visuelle Erweiterungen (wie z. B. die Darstellung der Torentfernung in Freistoßsituationen bei Fußballübertragungen), aber auch andere Sinne können angesprochen werden.
Backend-Infrastruktur bzw. -System	Mit Backend wird der Teil einer IT-Infrastruktur bezeichnet, der im nicht sichtbaren Hintergrund läuft und durch unterschiedliche Systemprozesse wie z. B. Datenbank-Verwaltung, die Nutzer-Eingaben verarbeitet und damit die Nutzung von Anwendungen im sichtbaren Bereich (Frontend) ermöglicht.
HbbTV	HbbTV eröffnet die Möglichkeit, den Zuschauern neben linearem Fernsehen sowohl zusätzliche Webbasierte Medienangebote (z. B. weiterführende Informationen, Werbung, Wetterberichte oder Teletext) zum laufenden und zukünftigen Programm als auch On-Demand Dienste zur Verfügung zu stellen.
Knochenleitungslautsprecher	Knochenleitung, auch Knochenschall genannt, bezeichnet die Weiterleitung von Schall-Schwingungen bzw. Vibrationen durch den das Gehörorgan umgebenden Schädelknochen unter Umgehung des Mittelohrs. Die Wahrnehmung des „Knochenschalls“ wird wegen des hohen Schallwellenwiderstands des Schädelknochens normalerweise von den als Luftschall übertragenen Signalen überdeckt.
5.2.1.1.1.1.1 On-Board-Diagnose-System (OBD-System)	OBD-Systeme sind in das Fahrzeug integrierte, elektronische Systeme zur Überwachung aller abgasbeeinflussenden Systeme bzw. der gesamten Elektronik des Fahrzeugs.
Set-Top-Box	Set-Top-Boxen sind Beistellgeräte, die an ein anderes Gerät, häufig einen Fernseher angeschlossen werden, um Anwendern zusätzliche Inhalte und Nutzungsmöglichkeiten, wie Satellitenfernsehen oder Pay-TV-Inhalte zu ermöglichen.

Pervasive Computing	Die Alltagswelt zunehmend durchdringende Computertechnik.
Smart Car	Als Smart Cars werden Fahrzeuge bezeichnet die mit Hilfe eingebauter Hard- und Softwarekomponenten und entsprechenden drahtlosen Kommunikationsschnittstellen, fahrzeuginterne Abläufe überwachen und unterschiedliche Daten über sich und ihre Umgebung erfassen und an die Außenwelt weiterleiten können.
Smart TV	Smart TVs sind Fernsehgeräte, die über Funktionen wie eine Internet-, Netzwerk- oder USB-Anbindung verfügen und mithilfe dieser Zusatzinhalte oder z. B. über Kameras und Mikrofone Interaktionsmöglichkeiten mit der Außenwelt bieten.
Video-on-Demand (Video auf Abruf)	Mit Video-on-Demand wird die Möglichkeit bezeichnet, bei der Zuschauer Videomaterial gegen ein entsprechendes Entgelt aus einem Archiv abrufen und mithilfe des Internets oder eines Fernsehgerätes empfangen können.
Web Single Sign-On (WebSSO)	Mit dem Konzept wird ein Authentifizierungsverfahren bezeichnet, bei dem nach einmalig erfolgter Anmeldung auf mehrere unabhängige, aber miteinander verbundene Systeme zugegriffen werden kann, ohne dass bei einem Zugriff auf ein verbundenes System eine erneute Authentifizierung nötig wird.
Wearables	Mit Wearables wird eine Form der allgegenwärtig rechnergestützten Informationsverarbeitung bezeichnet, bei der miniaturisierte und vernetzte Computer, auch Wearables genannt, am bzw. im menschlichen Körper getragen werden. Wearables werden typischerweise unauffällig getragen und sollen – anders als Smartphones – ohne unmittelbares, aktives Eingreifen des Nutzers Daten über ihn und seine Umgebung erfassen, verarbeiten und weiterleiten.

Abkürzungsverzeichnis

(W)LAN	(Wireless) Local Area Network
AAL	Ambient Assisted Living
AGB	Allgemeine Geschäftsbedingungen
BDSG	Bundesdatenschutzgesetz
CAN	Controller Area Network
CES	Consumer Electronics Show
DER	Data Event Recorder
ECU	Electronic Control Unit
FIN	Fahrzeugidentifikationsnummer
GG	Grundgesetz
GPS	Global Positioning System
HbbTV	Hybrid Broadcast Broadband TV
IKT	Informations- und Kommunikationstechnologien bzw. -techniken
iOS	iPhone Operating System
IP	Internet Protokoll
ISP	Internet Service Provider
LTE	Long Term Evolution (Mobilfunkstandard)
MMS	Multimedia Messaging Service
OBD	On-Board-Diagnose-System
OBD	On-Board-Diagnose
QS	Quantified Self
RFID	Radio-frequency identification
SSO	Single Sign-on
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TÜV	Technischer Überwachungsverein
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP

IMPRESSUM

Kontakt:
Peter Zoche
Koordinator Sicherheitsforschung und Technikfolgenabschätzung

Telefon +49 721 6809-152
Fax +49 721 6809-315
E-Mail info@forum-privatheit.de

Fraunhofer-Institut für System- und Innovationsforschung ISI
Breslauer Straße 48
76139 Karlsruhe

www.isi.fraunhofer.de
www.forum-privatheit.de

Schriftenreihe:
Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt
ISSN-Print 2199-8906
ISSN-Internet 2199-8914

1. Auflage: 500 Stück
Juli 2015

Druck
Stober GmbH Druck und Verlag, Eggenstein

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz.

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

PROJEKTPARTNER

Fraunhofer

Natur Technik Kultur Gesellschaft
UNIKASSEL VERSITÄT

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

UNIVERSITÄT HOHENHEIM
LEHRSTUHL FÜR MEDIENPSYCHOLOGIE

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

INTERNATIONALES ZENTRUM FÜR ETHIK IN DEN WISSENSCHAFTEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein