

Die Spione im eigenen Haus

Oliver Bendel

Bendel, Oliver. Die Spione im eigenen Haus. In: Martinsen, Franziska (Hrsg.). Wissen – Macht – Meinung: Demokratie und Digitalisierung. Die 20. Hannah-Arendt-Tage 2017. Velbrück, Weilerswist-Metternich 2018. S. 67 – 80.

Der Text im Sammelband wurde von der Herausgeberin gegen den Willen des Autors gegendert. Die vorliegende Version ist das Original in Standardsprache.

Einführung

Der private und halböffentliche Raum ist längst nicht mehr so geschützt wie früher. In jedem Haushalt finden sich mehrere Geräte, die uns beobachten und belauschen können. Auch der Supermarkt, in dem wir einkaufen, das Unternehmen, in dem wir arbeiten, das Krankenhaus und das Pflegeheim, in dem wir betreut werden, sind zu Orten geworden, an denen man kaum etwas für sich behalten kann. Ständig verrät man nicht nur private Informationen sowie politische und weltanschauliche Ansichten, sondern präsentiert auch die individuelle Stimme und Sprechweise, die womöglich tausende Kilometer entfernt von unbekannten Systemen und Personen analysiert werden.

Dem Auditiven gilt im vorliegenden Beitrag die Aufmerksamkeit, nicht dem Visuellen, das bereits vielfach abgehandelt wurde. Es werden diejenigen Funktionen und Geräte in den Vordergrund gerückt, die nicht der bewussten, benutzergesteuerten Aufzeichnung von Tönen bzw. Inhalten dienen, die aber Möglichkeiten der Überwachung und der Datenanalyse bieten. Diktiergeräte und Musikprogramme scheiden demnach aus. Smartwatches werden nicht thematisiert, da sie oft mit Smartphones zusammenwirken und teils ähnliche bzw. entlehnte Funktionen haben. Genauso werden Standrechner und Notebooks ausgeklammert, deren Probleme grundsätzlich die gleichen wie bei Handys und Tablets sind.¹

Beispiele und Funktionen auditiver Systeme

Smartphones und Tablets

In Smartphones und Tablets sind üblicherweise Mikrofon und Lautsprecher verbaut (Bendel 2015b). Das Mikrofon ist für Aufnahmen von Geräuschen und Klängen, für die Sprachsteuerung sowie für die Spracheingabe beim Telefonieren gedacht, der Lautsprecher gibt Signale, Weckrufe, Musik und

¹ Der vorliegende Beitrag folgt im Wesentlichen (Bendel 2015a) und (Bendel 2015b) und verwertet den Vortrag „Die Spione im eigenen Haus“, den der Verfasser während der Hannah-Arendt-Tage am 23. Januar 2018 im Rahmen der Ausstellung „Geheimnis“ im Tagungszentrum Schloss Herrenhausen in Hannover gehalten hat. In diesem ging es auch um visuelle Erfassung und Überwachung, und es standen Pflege- und Therapieroboter im Fokus.

Sounds von Computerspielen sowie die Stimme des Gesprächspartners am anderen Ende aus. Zusätzlich können Kopfhörer oder Headsets und separate Boxen angeschlossen werden.

Die genannten Gadgets werden überall genutzt, unterwegs, im Tram oder im Bus, oder bei der Arbeit und zu Hause. Auch im Unterricht an Schule und Hochschule sind sie massenhaft zu finden (Bendel 2015b) und konservieren die mehr oder weniger freie Rede der Lehrer und Dozenten. Sie sind, mit anderen Worten, omnipräsent, und der Benutzer weiß oft nicht, ob die Aufnahmefunktion aktiviert wurde, zumal dies durch einen Bedienungsfehler passieren kann. Über Schadsoftware kann vorgegaukelt werden, dass das Smartphone ausgeschaltet ist; in diesem Zustand droht ein Lauschangriff (Pakalski 2015). Auch Personen im Umfeld vermögen in der Regel nicht zu sagen, ob ihre Geräusche und Aussagen aufgezeichnet werden oder nicht. Die Aufnahme erfolgt sozusagen heimlich, still und leise, meist ohne ausdrückliches Einverständnis der Betroffenen (Bendel 2015b).

Sprachassistenten im Sinne virtueller Assistenten können Smartphones und Tablets eine Stimme verleihen. Siri und Cortana sind zwei bekannte und verbreitete Anwendungen (Bendel 2012a; Bendel 2015b). Sie kommunizieren in natürlicher Sprache, ähnlich wie Chatbots auf Websites, die aber meist auf Text spezialisiert sind, oder pädagogische Agenten (Bendel 2003). Ein weiteres Beispiel ist der Google Assistant. Mit dem Befehl „OK Google“ wird die Suchmaschine des Konzerns aktiviert, und eine künstliche Stimme beantwortet Fragen, etwa auf der Basis von Wikipedia. Wie Tests gezeigt haben, machen selbst ähnliche Befehle die Systeme scharf, im zuletzt genannten Fall etwa „OK Kuchen“ (Berger 2018). Zudem ist umstritten, was bereits vor einer Aktivierung aufgezeichnet und analysiert wird. Zur Spracherkennung gesellt sich immer mehr die Stimmerkennung.² Mit ihrer Hilfe kann Siri z.B. bestimmte Personen identifizieren und im Prinzip auch Merkmale der Stimme und die Sprechweise analysieren.

Kommunikations- und Transaktionsgeräte

Amazons Echo liegt in mehreren Formen mit unterschiedlichen Bezeichnungen vor (Echo, Echo Dot, Echo Plus etc.). Das Kommunikations- und Transaktionsgerät, wie man es nennen könnte, wird mit Sprachbefehlen und einer App gesteuert (Bendel 2015b). Echo ist über W-LAN permanent mit dem Internet verbunden. Es sind Lautsprecher und sieben Mikrofone (bei anderen Modellen sind es weniger bzw. mehr) verbaut. Die Sprachanalyse findet in Amazons Rechenzentren statt (Fuest 2014). Angeblich wird sie nur durchgeführt, wenn das Codewort ausgesprochen wurde; ansonsten wird von Echo, so das Unternehmen, nichts aufgezeichnet und ausgewertet (Linden 2014; Fuest 2014). Das „Zauberwort“ ist der gängige Mädchenname „Alexa“, der Rufname der virtuellen Assistentin.

Fragen nach dem Wetter werden von Alexa ebenso beantwortet wie nach Fernsehserien. Zudem kann man sich Witze erzählen, Nachrichten vorlesen, To-do-Listen generieren und an Termine erinnern lassen (Fuest 2014). Das ausschnittsweise Vorlesen von Wikipedia-Artikeln wird – wie vom Google Assistant – ebenfalls beherrscht. Alexas Stimme ist immer menschenähnlicher. Seit geraumer

² Spracherkennung, eine Technologie, die im vorliegenden Kontext eine wichtige Rolle spielt, ist die automatisierte Erkennung gesprochener Sprache. Beispielsweise versteht ein System einen bestimmten Sprachbefehl. Stimmerkennung dient der Erkennung einer Stimme und mithin der Identifizierung einer Person oder der Analyse der Merkmale der Stimme und der Sprechweise einer Person. Über Stimmerkennung kann man, wie über Gesichtserkennung, Emotionserkennung betreiben.

Zeit kann sie flüstern, mit Hilfe eines neuen SSML-Befehls (Bendel 2018).³ Vor allem hilft das System beim Shoppen zu Hause: „Per Zuruf können Nutzer Produkte auf die Einkaufsliste setzen oder Musik aus Amazons Multimedia-Angeboten abrufen.“ (Fuest 2014) Die virtuelle Mitarbeiterin regt Bedürfnisse an und befriedigt diese, unter Vermeidung von Medienbrüchen. Sie ist in der Lage, die unterschiedlichen Personen in einem Haushalt oder im Büro anhand der Stimme zu erkennen und auseinanderzuhalten. Damit können peinliche Missverständnisse vermieden und individuelle Bedürfnisse befriedigt werden.

Die häusliche Situation ist eine besondere. Man befindet sich in den eigenen vier Wänden, die normalerweise nicht der Ort für Überwachung und Abhörung sind, außer wenn man Zielscheibe von Geheimdienst oder Polizei bzw. unter „Beobachtung“ des Partners oder der Partnerin ist (Bendel 2015b). Echo kann Geräusche und Anweisungen erfassen, die von einem entfernten Ort der Wohnung stammen („far-field technology“). Auch das Flüstern in einem Raum kann dadurch leicht eingefangen werden (selbst dasjenige einer anderen Alexa). Echo kann im Prinzip, wie angedeutet, auch in Büros oder Shared Workspaces aufgestellt werden. Ein Leuchtring am Kopf zeigt die Aktivität an. Dies ist für den Nichteingeweihten aber nicht unbedingt offensichtlich.

Smarte Fernseher

Moderne Digitalfernseher können neben dem Lautsprecher ein Mikrofon besitzen. Sinn und Zweck ist üblicherweise die Sprachsteuerung, etwa zum Umschalten der Programme und zum Bedienen des Menüs. Ein Beispiel ist der Samsung SmartTV (Taglinger 2015). Bei diesem werden Signalwörter über einen Service erkannt, der nicht zum Unternehmen gehört. Dieses hat 2015 darüber informiert, dass das Gesprochene aufgezeichnet und an eine „third party“ übermittelt wird (Hill/Harshaw 2015). Deutsche Verbraucherschützer haben die südkoreanische Firma verklagt (Kolokythas 2015).

Wiederum ist man im scheinbar abgesicherten Raum (Bendel 2015a; Bendel 2015b). Man macht es sich bequem, plaudert über eine Talkshow, einen Nachrichtensprecher oder den Präsidenten der USA. Die Fernseher können sich auch in Lokalen und im Freien befinden, was in südlichen Ländern und in ländlichen Gebieten nicht unüblich ist. Die Zuschauer und -hörer mussten bisher nicht damit rechnen, dass ihr Fernseher sie ausspionieren kann. Nicht allen ist die Funktion des Lämpchens klar, das beim erwähnten Modell während des Aufzeichnens leuchtet und auf das die Firma in ihrer Erklärung explizit hingewiesen hat (Taglinger 2015).

Intelligentes Spielzeug

Immer mehr Puppen, Stofftiere und Gerätschaften für Kinder weisen Computerchips auf und sind mit KI-Systemen wie IBM Watson verknüpft, die Gesprochenes verstehen und auswerten (Bendel 2015a; Boie 2015).⁴ Bekannte Beispiele sind der Dinosaurier von CogniToys, Hello Barbie von Mattel, die

³ Mit der Speech Synthesis Markup Language (SSML) gestaltet man synthetische Stimmen. Man kann sie z.B. weicher und jünger machen oder etwas mit mehr Unsicherheit oder mehr Begeisterung aussprechen lassen. Man kann damit auch einfach nur festlegen, wie eine Zahl wie 2018 ausgesprochen wird, als Zweinulleinsacht oder als Zweitausendachtzehn.

⁴ Die Disziplin der Künstlichen Intelligenz (KI) hat die künstliche Intelligenz zum Gegenstand. Die KI ist ein eigener wissenschaftlicher Bereich der Informatik, der sich mit dem menschlichen Denk-, Entscheidungs- und

Ende 2015 auf den Markt gekommen ist, und die Puppe My Friend Cayla von Genesis Toys. Alle drei verfügen über natürlichsprachliche Fähigkeiten und animieren die Kinder zu bestimmten Interaktionen. Cayla, wie sie kurz genannt wird, ist mit dem Internet verbunden, hat Mikrofon und Lautsprecher sowie Spracherkennung und -ausgabe. Sie kann über eine App gesteuert und eingeschränkt werden.

Da sich viele Eltern pädagogische Vorteile versprechen und manche von ihnen an zusätzlichen Kontrollfunktionen interessiert sind (Parental Control ist hier aber nur am Rande das Thema), ist ein Siegeszug des intelligenten Spielzeugs naheliegend. Über die Risiken dürften nicht alle informiert sein, obwohl die Berichterstattung in den Medien omnipräsent ist. Vor allem Hello Barbie rief ein breites Echo hervor (Reese 2015), und ihr wurde – wie dem Bundesnachrichtendienst und Amazon – der Big Brother Award 2015 verliehen (Thoma 2015). Cayla könnte laut Bundesnetzagentur eine „versteckte, sendefähige Anlage“ sein. Sie hat die Puppe Anfang 2017 verboten.

Die „smart toys“, wie sie im Englischen genannt werden, können ins Kinderzimmer hineinhorchen und nicht nur den Heranwachsenden, sondern auch den Herstellern die Resultate ihrer Analysen liefern. Die Erziehungsberechtigten werden zu den Handlangern der Datenkraken. Sie füttern sie, indem sie die Geräte verschenken, und in manchen Fällen ziehen sie selbst Daten ab, um die Kinder zu kontrollieren. Mit Barbie (und Ken) spielen oft mehrere Freundinnen zusammen. Sie ahmen Lebenssituationen nach, erfinden Phantasiewelten, äußern Wünsche und Hoffnungen.

Serviceroboter

Serviceroboter sind für Dienstleistung, Unterhaltung und Zuwendung zuständig, holen Nahrungsmittel und Medikamente herbei, überwachen die Umgebung ihrer Besitzer oder den Zustand von Patienten und halten ihr Umfeld im gewünschten Zustand (Bendel 2017b). Mäh-, Saug- und Putz- sowie Pflege- und Therapieroboter sind in Haushalten und Einrichtungen im Einsatz. Sie sind häufig (teil-)autonom und ein Stück weit lernfähig, etwa insofern sie sich Namen behalten oder je nach Behandlung unterschiedlich entwickeln und ausrichten können. Oft haben die Roboter auditive Schnittstellen wie Mikrofone und Lautsprecher. Sie geben Töne von sich oder kommunizieren natürlichsprachlich. Zum einen müssen sie Befehle und Fragen entgegennehmen können, zum anderen ist es üblich, dass bestimmte elektronische Geräte auch etwas zum Status und zur Funktionsfähigkeit mitteilen.

Robear von Riken ist ein Prototyp eines Pflegeroboters, der im Tandem mit der Pflegekraft arbeiten und Hand anlegen kann (Bendel 2017a). Er kann Patienten hochheben, sie umbetten oder in einen Rollstuhl setzen. Er verfügt u.a. über Drehmoment- und Tastsensoren, zudem über Kameras und ein Mikrofon. Care-O-bot vom Fraunhofer-Institut für Produktionstechnik und Automatisierung ist ein Pflegeroboter (ein Begriff, den die Forschungseinrichtung nicht gern hört), der Dinge transportiert und Patienten informiert (Bendel 2017a). Er hat einen Lautsprecher, Mikrofone zur Spracherkennung und Kameras für Gesichts- und Gestikerkennung. Er ist nicht zuletzt in Shopping Malls zu finden, in der armlosen Version namens Paul. Pepper, ein Companion-Robot, hat sich ebenfalls neue Felder erobert, Krankenkassen und Pflegeheime auf der einen, Einkaufszentren auf der anderen Seite. Er hat vier Mikrofone, zwei HD-Kameras sowie einen Abstandssensor und ist W-LAN-fähig. Er kann mit

Hilfe von Gesichtserkennung bestimmte Personen identifizieren und beherrscht Mimik- und Gestikanalyse, zudem Stimmanalyse.

Serviceroboter erobern den privaten, halböffentlichen und öffentlichen Raum, nicht allein aus wirtschaftlichen Gründen (Bendel 2017b). Bei humanoiden Varianten ist meist klar, dass Aussagen und Fragen verstanden werden. Was die Auswertung und Weitergabe der Daten anbetrifft, dürften die Betroffenen weniger gut informiert sein. Bei Dementen, geistig Behinderten und manchen Älteren müssen ebenfalls Einschränkungen im Verständnis angenommen werden. Bei Patienten kommt die Situation der Krankheit hinzu. Die Maschinen erfassen potenziell Daten zu Körperfunktionen, Geistes- und Gesundheitszustand. Tierähnliche oder „gegenständliche“ Roboter sind womöglich noch schwieriger als menschenähnliche einzuschätzen.

Besonders pikant sind im vorliegenden Kontext die Sexroboter und Liebespuppen, die seit ein paar Jahren mit schöner Regelmäßigkeit Medien und Moralisten erfreuen, aber auch philosophische Ethiker beschäftigen.⁵ Wenn sie natürlichsprachliche Fähigkeiten besitzen (Bendel 2018), beherrschen sie nicht nur Dirty Talk, sondern belauschen die Partnerinnen und Partner bei deren Dirty Talk, ob dieser mit ihnen oder nur neben ihnen stattfindet.

Die Perspektive der Ethik

Dass uns Sprach- und Tonsysteme belauschen, wird mehr und mehr von Medien, von Parteien und Behörden und auch von den Vertretern der Bereichsethiken (insbesondere der Informationsethik, daneben von Technik- und Medienethik) thematisiert. Endkonsumenten werden als gläserne Bürger erkannt und beschrieben. Das „Verwanzen“ des Kinderzimmers mit seinen wehrlosen Bewohnern sorgt für gesellschaftliche und politische Empörung und lädt zur wissenschaftlichen Betrachtung ein (Boie 2015). Big Data und Observation sind Reizthemen, die man in den Onlinezeitungen und deren Foren und in wissenschaftlichen Journals erörtert (Mayer-Schönberger/Cukier 2013).

Bei auditiven Systemen kann man in Hinsicht auf verbale Äußerungen, wie bereits angedeutet, mehrere Ebenen unterscheiden (Bendel 2015b). Erstens können sie die Stimme auswerten. Diese verrät Geschlecht und Alter und liefert u.U. auch Hinweise auf Körpergröße und -volumen. Zweitens sind sie in der Lage, die Sprechweise zu analysieren, die Lautstärke, den Rhythmus, den Fluss, die Betonung, Sprachfehler und -störungen. Drittens wird die Sprache erkannt, wobei nicht jedes System mit (z.B. dialektalen) Varianten zurechtkommt. Viertens sind die Inhalte verfügbar, in Form von Befehls-, Aussage- und Fragesätzen oder einzelnen Wörtern, mit ihren jeweiligen Bedeutungen, die maschinell mehr oder weniger gut erfasst und eingeordnet werden können, etwa über Thesauri und Ontologien. Zudem können die Systeme u.U. die Zahl anwesender Personen eruieren, ihre Größe und ihre Position im Raum. Ferner sind auditive Informationen erhältlich, die nicht von Personen, sondern aus anderen Quellen stammen, von Geräten und Tieren. Auch sie lassen Rückschlüsse auf Aufenthaltsort und Lebensweise zu.

In den folgenden Abschnitten wird von einem zentralen Konzept der Informationsethik ausgegangen, der sogenannten informationellen Autonomie – leicht fokussiert bzw. rechtlich konnotiert spricht

⁵ Man kann zwei Entwicklungslinien ausmachen. Zum einen sind ein paar wenige Sexroboter auf dem Markt, die i.d.R. auch Stimmen haben. Zum anderen sind die früheren Gummipuppen zu modernen Liebespuppen („love dolls“) geworden, die künstliche Haut und darunter künstliches Fleisch haben und die immer wieder erweitert werden, auch mit natürlichsprachlichen Fähigkeiten.

man von informationeller Selbstbestimmung –, mit ihren Aspekten der Privatheit und der Überwachung sowie der Aggregation und Manipulation der Daten (Bendel 2012b; Bendel 2016).⁶ Zudem wird die persönliche Autonomie behandelt, für deren Erörterung sich Technik- und Informationsethik berufen fühlen, im Gegenüber von menschlicher und maschineller Autonomie, und die letztere im Zusammenhang mit der Sprachkompetenz und der Tendenz zu Wahrheit oder Unwahrheit. Am Rande interessiert die persönliche Freiheit im Informationszeitalter.

Privatheit, Privat- und Betriebsgeheimnis

Die Aufzeichnung von Stimmen und Geräuschen wurde bald nach ihrer Erfindung zum Problem, wenn man an die informationelle Autonomie und die Wahrung der Privatsphäre (und das eine oder andere Gegenstück, vom Stalking bis zur Überwachung) denkt. Die Digitalisierung vermehrt die Möglichkeiten und Herausforderungen. Smartphones und smarte Fernseher sind omnipräsent, intelligentes Spielzeug ist im Kommen. Aufzeichnungen sind im großen Maßstab möglich, ebenso Auswertungen. Im Persönlichen steigt die Gefahr des Verlusts in der Informationsflut, im Öffentlichen wirken dem Data Mining und Big Data entgegen (Mayer-Schönberger/Cukier 2013).

Die Mikrofone erlauben Momentaufnahmen und Verlaufsprotokolle in der öffentlichen Welt der Stimmen und Geräusche (Bendel 2015b). Ein Problembereich ist der Abzug persönlicher Informationen (wie ausgeführt, können z.T. konkrete Personen identifiziert werden), wobei Stimme, Sprechweise und Inhalte (eventuell Sprache) gleichermaßen betroffen sind. Auf der Ebene der Inhalte werden Lebensdaten, Standpunkte und Weltanschauungen erhoben. Ein besonderer Aspekt sind Geheimzahlen, Passwörter und Kreditkartennummern, über die sich Unbefugte Zutritt zu Konten und Accounts verschaffen können. Dabei müssen die Angaben allerdings laut ausgesprochen werden. Einige Geräte holen über das Codewort sozusagen eine Bewilligung zur Aufnahme ein, wobei es problematisch ist, wenn jenes häufig fällt, weil es identisch mit dem Namen einer Person ist („Alexa“), oder wenn ein ähnliches Wort die gleiche Wirkung hat. Wenn der Betreiber die Daten auswertet oder weitergibt (auch an Mittler, wie bei Samsung SmartTV und beim LG Smart TV), ist die Gefährdung der informationellen Autonomie wahrscheinlich (Hill/Harshaw 2015; Bendel 2015b).

Sobald die Geräte in Situationen und Umgebungen benutzt werden, die als vertraut und geschützt eingestuft werden, wie es bei Kommunikations- und Transaktionsgeräten wie Echo (und mit Einschränkungen bei Smartphone und Notebook) der Normalfall ist, tauchen weitere Risiken für Privatheit, Intimsphäre und Datenschutz auf (Bendel 2015b). In nicht- oder teilöffentlichen Räumen spricht man anders, teilt man etwas anderes mit, hat man Privat- und Betriebsgeheimnisse, und die Diskrepanz zwischen dem Vermögen der Geräte, die permanent etwas aufnehmen, abspeichern und weitergeben können, und dem Bedürfnis nach Privatsphäre, Persönlichkeitsschutz und Geheimhaltung ist groß. Das Eindringen in den Bereich der Sexualität kann als besonders gravierend angesehen werden – man denke nur, auf der stimmlichen Ebene, an das Stöhnen oder, auf der semantischen Ebene, an Kosewörter oder den erwähnten Dirty Talk. Bei Heranwachsenden ergibt sich die Schwierigkeit, dass sie oft nicht um ihre Überwachung und Belauschung wissen. Wenn sie darum wissen, kann sich dies auf ihr Verhalten auswirken. Die Unternehmen sind an den Aktivitäten und Aussagen der Jüngsten interessiert, um künftige Produktionen planen und anpassen zu können. Wenn Familiensituationen nachgespielt werden, entsteht womöglich kompromittierendes Material.

⁶ Die informationelle Autonomie ist die Möglichkeit, selbstständig auf Informationen zuzugreifen, über die Erfassung und Verbreitung von eigenen Äußerungen und persönlichen Abbildungen selbst zu bestimmen sowie die Daten zur eigenen Person einzusehen und gegebenenfalls anzupassen.

Unter dem permanenten Druck ändern sich bei allen Betroffenen die Gepflogen- und Gewohnheiten. Man senkt die Stimme, spart Details aus, vermeidet Pointen und Spitzen, Privatsprache und Kosenamen sowie Aufstoßen und Flatulieren. Manche Geräte können im Prinzip auskundschaften, ob überhaupt jemand an einem Ort ist, und welche Position die Personen haben, wo sie sind, ob sie sitzen, ob sie liegen. Damit sind weitere Rückschlüsse auf Verhaltensweisen und Geisteshaltungen möglich.

Zusammenführung von Daten

Die systematische Zusammenführung von Daten ist aus virtuellen Umgebungen seit langem bekannt. Bestimmte Informationen präsentieren sich auf elektronischen Plattformen anders. Das Nebensächliche kann in den Vordergrund rücken, das Hauptsächliche durch die Datenmenge verschwinden. Die Aggregation kann zu überraschenden und hochproblematischen Ergebnissen führen, zu einer erheblichen Beeinträchtigung der informationellen Autonomie und der Intim- und Privatsphäre. Detektive, Geheimdienste und die Polizei sind Aggregationen seit jeher zugetan. Sie fügen Stück für Stück in einem Puzzle zusammen, sammeln und verbinden Indizien und Beweise, um schließlich die richtige Person zu fangen oder zu überführen (Bendel 2015b). Mehr und mehr spielen dabei digitale Daten eine Hauptrolle.

Geräusche und Äußerungen werden entweder von Geräten und Apps direkt oder durch online vorhandene bzw. von „Spionen“ betriebene Dienste aggregiert (Bendel 2015b). Zu bedenken ist, dass Smartphone, Notebooks etc. zusammenwirken können. Die Aggregation verleiht dem Aggregator eine gewisse Macht. Dieser steht die Ohnmacht der Person gegenüber, die man observiert und analysiert und deren Aussagen und Fragen, Ankündigungen, Reflexionen und Handlungen man verknüpft. Während das einzelne Datum oft wenig aussagekräftig ist, vermittelt die Zusammenführung ein vielleicht vollständiges und entlarvendes Bild des Betroffenen. Wird dieses weitergereicht, an die Wirtschaft oder die Polizei, oder in soziale Medien eingespeist, können dem Betroffenen wiederum Nachteile erwachsen. Es entstehen, zusätzlich zur digitalen Identität, die man selbst auf Facebook, Instagram und Co. mit der Zeit generiert hat und die einem nach und nach außen (in die Öffentlichkeit) und nach innen (zum Betreiber hin) entgleitet, weitere digitale Identitäten, die noch weniger in unserer Hand liegen, die fremdbestimmt sind und uns fremdbestimmt machen.

Besonders heikel scheint die Verknüpfung (innerhalb) der Ebenen Stimme, Sprechweise, Sprache und Inhalte zu sein. Über die Stimme kann man, wie angedeutet, Geschlecht, Gesundheit und Alter bestimmen (Bendel 2015b). Sie ist bei deutlich artikulierten Worten und Sätzen, ferner bei Lauten und Geräuschen von Bedeutung, bei Ausrufen des Entsetzens oder Schmerzensbekundungen. Die Kennzeichen der Sprechweise gestatten Rückschlüsse auf Intelligenz (auch von Kindern), Bildungshintergrund, Sprachvermögen, Sozial- und Kommunikationsfähigkeit. Die Sprache verrät die Herkunftsländer, ja sogar die Landstriche, aus denen man stammt, wenn Akzent oder Dialekt vorliegen. Die Inhalte beziehen sich auf die Welt, die nähere Umwelt der Person und die Person selbst, und zwar in Bezug auf die Gegenwart, auf die Vergangenheit, in Form von Geschichten, Berichten und Beichten, und auf die Zukunft, in Form von Voraussagen, Plänen, Hoffnungen und Ängsten; durch die Zusammenziehung entsteht sozusagen die Timeline des Betroffenen mit ihren inneren und äußeren Ereignissen. Zu bedenken ist dabei, dass Systeme wie Google Assistant und Alexa in immer mehr Anwendungen zur Verfügung stehen und im Prinzip rund um die Uhr empfangsbereit sind. Die Verknüpfung der Ebenen lässt tiefe Einblicke in die Persönlichkeitsstruktur

und in die kurze oder lange Lebensgeschichte zu. Zudem führt sie zu einem eindeutigen Fingerabdruck. Bereits die Stimme ist mehr oder weniger unverwechselbar, zumindest für Maschinen – die Kombination mit Sprechweise, Sprache und Inhalt ist es ohne Zweifel.

Unbefugtes Eindringen und unerlaubte Manipulation

Auditive Systeme können von Schadprogrammen befallen und von Hackern bzw. Crackern attackiert werden. Bei eingebetteten und vernetzten Systemen sind unbefugtes Eindringen und feindliche Übernahme oft recht einfach zu bewerkstelligen. Bei der Übernahme wird häufig gegen Gesetze verstoßen, und wenn sie in einer gewissen Weise oder für eine Weile passiert, kann neben dem unbefugten Eindringen auch Diebstahl geltend gemacht werden, sei es von Daten oder der Maschine respektive Gerätschaft selbst. Die Thematik kann überdies im Kontext von Freiheit und Autonomie (und von Überwachung) behandelt werden, geht aber darüber hinaus; zudem ergeben sich rechtliche (nicht zuletzt datenschutzrechtliche) Implikationen.

Gezeigt wurde, dass man mittels Malware dem Benutzer vorspielen kann, dass sein Smartphone ausgeschaltet ist (Pakalski 2015). Wenn sich eine Person die Mühe macht, dieses zu übernehmen, liegt die Vermutung nahe, dass sie Schaden anrichten will. Sie will das Mikrofon benutzen, um den Benutzer oder seine Umgebung auszuhorchen oder sich in irgendeiner Form, geistig oder körperlich, zu befriedigen. Damit wären wiederum Privatsphäre und Betriebsgeheimnis betroffen und Stalking und Überwachung oder Wirtschaftsspionage möglich. Es ist zudem denkbar, dass auditive Informationen verändert, entfernt oder hinzugefügt werden (Bendel 2015b). Das Ergebnis könnte man gegen den Benutzer verwenden, oder diesem würde etwas fehlen, wenn er Berichte der Medien entkräften oder Beweise vor Gericht vorlegen wollte. Hier wird neben der informationellen Autonomie die individuelle Freiheit in der Informationsgesellschaft verletzt, das Recht auf Unversehrtheit eigener Geräte, der Nutzung im normalen Umfang, und das Recht auf Freiheit vor falscher Beschuldigung mit Hilfe technischer Manipulation (Bendel 2015b).

Manipulation kann auch zu wirtschaftlichen Zwecken stattfinden. Die Geräte belauschen die jetzigen und zukünftigen Kunden. Alexa könnte etwas einflüstern, Produkte vorstellen und empfehlen. Barbie kann die Wünsche der Kinder in Erfahrung bringen. Sie kann theoretisch Wünsche erzeugen, indem sie den Mädchen (oder den Jungen) etwas über ihren Partner Ken erzählt, ihre Kinder, ihre Eltern, ihre Geschwister, ihre Freundinnen, ihre Berufe, die sie ausgeübt hat und ausüben will und die nachgespielt werden sollen. Selbst auf die Persönlichkeit des Kindes könnte sie Einfluss nehmen, könnte es religiös, politisch und anderweitig infiltrieren. Stand die traditionelle Barbie im Kreuzfeuer von Feministinnen, gerät die technisierte Version ins Visier von Verbraucher- und Datenschützern.

Zusammenfassung und Ausblick

Auditive Systeme sind seit Jahrzehnten ein bevorzugtes Mittel für das Ausspionieren von Menschen, das Auswerten des Verhaltens der Bevölkerung und die Erstellung von Prognosen. In den 2010er-Jahren erleben sie eine Renaissance. Nicht mehr als gewöhnliche Wanzen, nicht nur als konventionelle Telefonüberwachung. Sondern in Form von Alltagsgeräten, die für uns teilweise unverzichtbar sind, teilweise zumindest bereitwillig ausprobiert werden. Es werden offensichtlich immer mehr, und dass man sogar Spielzeug mit Lautsprechern und Mikrofonen, mit Spracherkennung und künstlicher Intelligenz ausrüstet, dass Hello Barbie und CogniToys-Dinosaurier auf dem Markt sind, darf kaum noch verwundern.

Nicht in die Tiefe gegangen wurde in Bezug auf das Betroffensein und die Entwicklung von Minderjährigen. Während Erwachsene sich mancher Gefahren bewusst sind oder immerhin bewusst sein könnten, ist das Kind den Erfindungen des Unternehmens ausgeliefert. Es könnte, wie angedeutet, sein Verhalten ändern, wenn es etwas von der Überwachung mitbekommt oder diese selbst erkennt. Es könnte die Überwachung auch, mit dieser aufwachsend, völlig normal finden und später bei dieser Kritik- und Distanzlosigkeit bleiben. Einiges von dem, was George Orwell in „1984“ geschildert hat, ist längst eingetreten, ohne dass die Mehrheit der Mitglieder der Informationsgesellschaft davon sonderlich beunruhigt wäre. Big Brother sieht nicht nur, er hört auch zu, aber wir halten ihm die Tür auf, holen ihn zu uns herein, schicken ihn zu den Schutzbefohlenen, die zu Schutzlosen werden. Und noch mehr: Wir werden selbst zum Big Brother und spähen uns gegenseitig aus.

Manche Geräte sind singuläre Systeme, andere mit Rechnern und Dingen verbunden bzw. Teil einer Cloud-Computing-Lösung. Die Daten werden zusammengeführt und aufbereitet, mit maschineller Hilfe und künstlicher Intelligenz und im Zusammenhang mit maschineller oder menschlicher Entscheidung. Die Verbindung mit visuellen Schnittstellen potenziert die Probleme. Man kann versuchen, auf bestimmte Geräte zu verzichten oder mit weiteren Maschinen gegen diese kämpfen. Der Einzelne wird allerdings dem Ansturm der Möglichkeiten ausgeliefert sein. Deshalb braucht es zusätzliche ethische Überlegungen und verschiedene rechtliche Konsequenzen. Die Informationsgesellschaft soll weiterhin eine Gesellschaft sein, in der die Nutzung von Technologien Spaß macht und Gewinn bringt. Aber sie muss für den Einzelnen zugleich möglichst vertrauenswürdig und sicher sein. Gewiss sind Dilemmata vorhanden, die sich nicht auflösen lassen, gerade im Bereich von Pflege und Therapie. Die Sammlung und Auswertung von Daten kann hier lebensnotwendig sein, und oft wird man die Situation antreffen, dass die persönliche Autonomie gestärkt, die informationelle Autonomie geschwächt wird. Solchen moralischen Herausforderungen müssen sich speziell Informations- und Technikethik widmen.

Literatur

Bendel O (2018) SSML for Sex Robots. In: Cheok, Adrian David; Levy, David (Hrsg.). Love and Sex with Robots. Third International Conference, LSR 2017, London, UK, December 19–20, 2017, Revised Selected Papers. Springer International Publishing, Cham 2018, S. 1 – 11

Bendel O (2017a) Soll uns Robear pflegen? In: IT for Health, 7 (2017) 2, S. 20 – 21

Bendel O (2017b) Service Robots in Public Spaces. In: Telepolis, 25. Juni 2017. <https://www.heise.de/tp/features/Service-Robots-in-Public-Spaces-3754173.html>, letzter Zugriff: 17.03.2018

Bendel O (2016) 300 Keywords Informationsethik: Grundwissen aus Computer-, Netz- und Neue-Medien-Ethik sowie Maschinenethik. Springer Gabler, Wiesbaden

Bendel O (2015a) Auditive Systeme im Wohn- und Arbeitsbereich: Big Brother hört mit. ICTkommunikation (Online-Ausgabe), 19. Oktober 2015. <http://ictk.ch/content/auditive-systeme-im-wohn-und-arbeitsbereich-big-brother-h%C3%B6rt-mit>, letzter Zugriff: 17.03.2018

Bendel O (2015b) Der kleine Lauschangriff: Auditive Systeme aus Sicht der Ethik. Telepolis, 5. Juli 2015. <http://www.heise.de/tp/artikel/45/45319/1.html>, letzter Zugriff: 17.03.2018

Bendel, O (2012a) „Siri ist hier.“: Der Sprachassistent von Apple in der Schweiz aus linguistischer und ethischer Sicht. mediensprache.net, Juli 2012. <http://www.mediensprache.net>

Bendel O (2012b) Informationsethik. Beitrag für das Gabler Wirtschaftslexikon. Springer Gabler, Wiesbaden. <http://wirtschaftslexikon.gabler.de/Definition/informationsethik.html>, letzter Zugriff: 17.03.2018

- Bendel O (2003) Pädagogische Agenten im Corporate E-Learning. Dissertation. Difo, St. Gallen 2003
- Berger D (2018) „OK Kuchen“: Googles Sprachassistent reagiert nicht nur aufs Signalwort. In: heise online, 13. März 2018. <https://www.heise.de/newsticker/meldung/OK-Kuchen-Googles-Sprachassistent-reagiert-nicht-nur-aufs-Signalwort-3992075.html>, letzter Zugriff: 17.03.2018
- Boie J (2015) Lauschangriff im Kinderzimmer. SZ.de, 18. April 2015. <http://www.sueddeutsche.de/digital/spielzeug-lauschangriff-im-kinderzimmer-1.2440374>, letzter Zugriff: 17.03.2018
- Fuest B (2014) Wie Amazon unseren Alltag übernehmen will. DIE WELT ONLINE, 7. November 2014. <http://www.welt.de/wirtschaft/webwelt/article134121365/Wie-Amaon-unseren-Alltag-uebernehmen-will.html>, letzter Zugriff: 17.03.2018
- Hill K, Harshaw P (2015) It's not just Samsung TVs – lots of other gadgets are spying on you. Fusion, 17. Februar 2015. <http://fusion.net/story/49352/all-the-smart-gadgets-are-spying-on-you/>, letzter Zugriff: 17.03.2018
- Kolokythas P (2015) Datenkrake im Smart-TV: VZ NRW verklagt Samsung. PC-Welt, 5. November 2015. <http://www.pcwelt.de/news/Datenkrake-im-Smart-TV-VZ-NRW-verklagt-Samsung-9843285.html>, letzter Zugriff: 17.03.2018
- Linden M (2014) Amazon hört und spricht ins Wohnzimmer. Golem, 6. November 2014. <http://www.golem.de/news/amazon-echo-amazon-hoert-und-spricht-ins-wohnzimmer-1411-110371.html>, letzter Zugriff: 17.03.2018
- Mayer-Schönberger V, Cukier K (2013) Big Data Meets Big Brother: The Privacy Risks of Big Data. The European Business Review, 8. September 2013. <http://www.europeanbusinessreview.com/?p=1229>, letzter Zugriff: 17.03.2018
- Pakalski I (2015) Vermeintlich ausgeschaltetes Smartphone hört mit. golem.de, 20. Februar 2015. <http://www.golem.de/news/android-schadsoftware-vermeintlich-ausgeschaltetes-smartphone-hoert-mit-1502-112496.html>, letzter Zugriff: 17.03.2018
- Reese H (2015) Wi-Fi-enabled 'Hello Barbie' records conversations with kids and uses AI to talk back. TechRepublic, 10. November 2015. <http://www.techrepublic.com/article/wi-fi-enabled-hello-barbie-records-conversations-with-kids-and-uses-ai-to-talk-back/>, letzter Zugriff: 17.03.2018
- Taglinger H (2015) Jetzt haben wir Dich, Du Stimme. Telepolis, 11. Februar 2015. <http://www.heise.de/tp/news/Jetzt-haben-wir-Dich-Du-Stimme-2544214.html>, letzter Zugriff: 17.03.2018
- Thoma J (2015) Lauschende Barbie erhält Big Brother Award. Golem, 18. April 2015. <http://www.golem.de/news/negativauszeichnung-lauschende-barbie-erhaelt-big-brother-award-1504-113588.html>, letzter Zugriff: 17.03.2018