Smartes Panopticon: Können Objekte moralisch handeln?

Das Internet der Dinge ist keine Vision mehr, es entfaltet sich unsichtbar und durchdringt unseren Alltag auf leisen Sohlen. Die Innovationszyklen sind kurz und treiben eine Welle von Ideen, Spekulationen und Anwendungsszenarien vor sich her. Die smarten Akteure des IoT handeln autonom, der Mensch verschwindet zunehmend aus Entscheidungsprozessen und wird zum Subjekt maschineller Handlungen. Wenn der menschliche Akteur die Bühne verlässt, wer vertritt dann ethische Standpunkte im IoT? Können Objekte moralisch handeln? Der Artikel geht diesen Fragen nach und gibt einen Ausblick auf angepasste Design-Prozesse.

Das historische Panopticon

Ende des 18. Jahrhunderts entwickelte der britische Philosoph Jeremy Bentham ein Konzept, das die gleichzeitige Überwachung sehr vieler Menschen durch einen einzigen Aufseher ermöglichen sollte. Er nannte seine Arbeit „Panopticon – oder das Überwachungshaus“ und bündelte einen Gebäudeentwurf mit dem Prinzip der permanenten Sichtbarkeit der Beobachteten (**siehe Kasten 1**). Weltweit wurden etliche Gefängnisbauten nach Benthams Ideen realisiert, eines der bekanntesten ist das *Presidio Modelo* auf Kuba (**siehe Abbildung 1**).

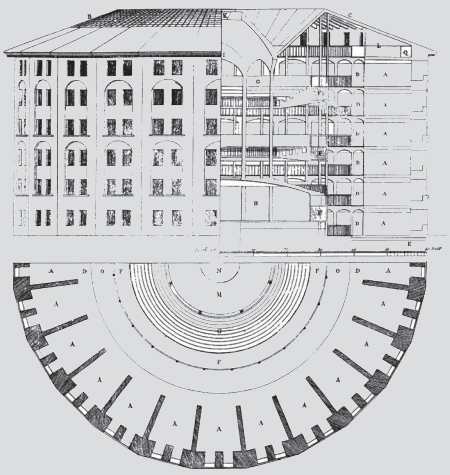
Der französische Philosoph Michel Foucault entwickelte in den 1970er Jahren seine Theorie des Panoptismus. Darin beschrieb er Mechanismen der Massendisziplinierung in modernen Gesellschaften durch Überwachungs- und Kontrollmechanismen. Er legte dar, wie die permanente Sichtbarkeit und Beobachtung zu einer Selbstdisziplinierung des Individuums und seiner Anpassung an die gegebenen Normen führt (vgl. [Fou77]).

Unsichtbare Beobachter

Das Panopticon wurde zu einer Metapher für die Massenüberwachung, in der der Einzelne jederzeit durchleuchtet werden kann, ohne seinen Beobachter zu kennen oder auch nur wahrzunehmen. Brauchten die panoptischen Gefängnisbauten noch Lampen und Mauern, so arbeiten digitale Methoden heute subtil und im Verborgenen.

Im Internet der Dinge (*Internet of Things – IoT*) kann jedes Objekt „smart“ werden und

Panoptisches Gebäude



1787 reiste Jeremy Bentham nach Russland und besuchte seinen Bruder Samuel, der dort mit diversen industriellen Projekten betraut war.

Der brüderliche Erfahrungsaustauch regte Bentham zum Entwurf des *Panopticon* an, einer Überwachungsanstalt, in der körperliche Strafen überflüssig werden sollten. Stattdessen sollte eine permanente Beobachtung die Insassen selbstdisziplinieren. Bentham sah bereits eine Vielzahl von Anwendungsmöglichkeiten im öffentlichen Raum vor und untertitelte seine Arbeit:

„ANWENDBAR FÜR ALLE GEBÄUDE, IN DENEN PERSONEN ÜBERWACHT WERDEN MÜSSEN [...]: GEFÄNGNISSE, ARMENHÄUSER, LAZARETTE, FABRIKEN, WERKSTÄTTEN, KRANKENHÄUSER, ARBEITSHÄUSER, IRRENANSTALTEN UND SCHULEN“ (vgl. [Ben1843]).

Er beschrieb die Architektur des Gebäudes detailliert und lies Konstruktionen und Zeichnungen anfertigen.

Die Grundidee des Panopticon ist ein ringförmiger Bau, dessen Zellen auf der Kreislinie liegen. Die Loge des Aufsehers liegt im Zentrum des Gebäudes, zwischen Zentrum und Rand befindet sich eine frei einsehbare Fläche. Die Zellen werden von außen beleuchtet – tagsüber durch große Fenster, nachts durch Lampen – sodass der Aufseher die Insassen im Gegenlicht beobachten kann. Jedes der Kabinette gleicht einem Schattentheater, das den Gefangenen abbildet. Der Wachturm liegt im Dunkeln und ist von den Zellen nicht einsehbar. Die Insassen wissen nie, ob sie gerade beobachtet werden, sind aber permanent sichtbar.

Im Laufe der Jahrhunderte wurden zahlreiche Gefängnisbauten nach dem Vorbild des Panopticon realisiert. Auf Kuba steht noch heute eine dieser Anlagen, das *Presidio Modelo* (spanisch für „Modellgefängnis“, **siehe Abbildung 1**). Es wurde unter dem Diktator Machado in den 1930er Jahren erbaut.

Die fünf Gebäude des Presidio Modelo waren für 2.500 Insassen dimensioniert, tatsächlich war das Gefängnis jedoch mit 6.000 bis 8.000 Häftlingen oft überfüllt. Die meisten überlebenden Aufständischen des Angriffs auf die Moncada-Kaserne, wie z. B. die Brüder Fidel und Raúl Castro, waren in den 1950er Jahren dort interniert. Auch nach der kubanischen Revolution von 1959 wurde das Gefängnis weiterhin zur Inhaftierung politischer Gefangener und anderer Missliebiger genutzt.

Das Presidio Modelo wurde 1967 geschlossen, zum nationalen Denkmal erklärt und beherbergt heute ein Museum.

Kasten 1: Panopticon – Theorie und Praxis.

(Foto: I. Friman).

Abb. 1: Panoptisches Gefängis – Presidio Modelo – auf Kuba.

Daten sammeln, verfügt es nur über die notwendige Technik und eine Anbindung ans Netz. Derartige Objekte können Sensoren, technische Geräte, Computer oder ein interagierender Mensch sein (**siehe Kasten 2**). Die Knoten des IoT handeln autonom und benötigen die folgende Basisausstattung:

- *Speicher:* Daten sammeln
- *Algorithmus:* Daten auswerten
- *Algorithmus:* Entscheiden
- *Kommunikation:* Verbinden und Übertragen
- *Rolle des Akteurs:* Autonomes Handeln

IoT-Objekte eignen sich aufgrund dieser Eigenschaften als *smarte Beobachter*: Jedes Ding kann ein anderes beobachten, die zentrale Hierarchie verliert sich in einem Netz gleichberechtigter Akteure.
Im IoT interagieren Menschen mit Objekten und Systemen. Es ist ein hybrides Geflecht belebter und unbelebter Subjekte, die Grenzen zwischen virtueller und realer Welt verschwimmen. Aus Sicht des IoT ist es vollkommen gleichgültig, ob es sich bei einem Objekt um einen Menschen oder um ein smartes Ding handelt, gemäß dem Leitsatz: „Es ist nicht wichtig, *was* du bist, Hauptsache ich weiß, *wo* du bist und *wer* du bist."
Für jedes Objekt werden so wichtige Informationen wie Ort, Kontext, Richtung, Geschwindigkeit und Identität bestimmt. Die folgenden Services sind daher essenzielle Bestandteile der IoT-Infrastruktur:

- Objekte *lokalisieren*
- Objekt *identifizieren*
- Mit anderen Objekten *kommunizieren*

Im IoT fallen Unmengen von Daten an, die zu unterschiedlichen Zwecken ausgewertet und zu Profilen akkumuliert werden können. In manchen Domänen lassen sich weitreichende Rückschlüsse über Gewohnheiten und private Gepflogenheiten eines Menschen aus den Daten ziehen (**siehe Tabelle 1**).

Allgegenwärtigkeit und Kennzeichnung

Die IoT-Technologie durchdringt die reale Welt, wird allgegenwärtig und gleichzeitig weitgehend unsichtbar. Brauchte Orwells „Big Brother" noch Kameras, so werden die smarten IoT-Objekte zu „Many Brothers" unter unbekannter Regie. Dem Bürger fehlt die sensorische Rückkopplung, er kann die Beobachter nicht wahrnehmen. Das IoT kann dadurch panoptische Züge annehmen. Der Mensch ist häufig als externer Stakeholder[1]) in IoT-Systeme einbezogen. Er kann das System nicht steuern, wird aber passiv eingebunden. Dies kann zu Gefühlen des Unbehagens und des Kontrollverlustes bis hin zu Aggression führen.

[1]) Externe Stakeholder sind von einem System betroffen, ohne es selbst zu nutzen. Beispiel: Ein Arbeitnehmer, der von einer Überwachungskamera in den Betriebsräumen gefilmt wird.

Vom Sensor zum Internet of Everything (IoE)

Der Begriff *Internet of Things (IoT)* wird Kevin Ashton zugeschrieben, einem Technologie-Experten, der unter anderem Standards für RFID-Sensoren entwickelte.
Im Jahr 1999 berichtete Ashton über Einsatzmöglichkeiten von RFID im Logistikbereich und betitelte seine Präsentation „Internet of Things". Er wollte damit den Unterschied zum *Internet of People* deutlich machen – dem Netz, in das alle Daten von Menschenhand in das System eingegeben werden mussten. Im IoT sollten die Computer selbstständig ihre Daten sammeln und in das Netz einspeisen. Zehn Jahre später äußerte sich Ashton erneut zu dem von ihm geprägten Begriff (vgl. [Ash09]):
„Wenn wir Computer hätten, die alles wüssten, was es über Dinge zu wissen gäbe [...], dann könnten wir alles nachverfolgen und berechnen [...]. Wir wüssten, wann Dinge ersetzt, repariert oder zurückgerufen werden müssten und ob sie noch verzehrbar oder bereits abgelaufen wären. Wir müssen Computer dazu befähigen, sich eigenständig Informationen zu beschaffen, sodass sie die Welt selbst sehen, hören und riechen können [...]. RFID und Sensor-Technologien ermöglichen es Computern, zu beobachten und zu identifizieren sowie die Welt zu verstehen, abseits der Einschränkungen der von Menschenhand erzeugten Daten."
Neuere Definitionen heben die Grenzen zwischen Dingen und Personen, virtuellen und physischen Objekten auf. Aus dem *Internet of Things (IoT)* wird das *Internet of Everything (IoE)*. Beispielhaft sei hier die Definition des IoT European Research Cluster (vgl. [IER]) aus dem Jahr 2015 zitiert (vgl. [Fri15]):
„IoT ist eine dynamische, globale und vernetzte Infrastruktur, welche in der Lage ist, sich selbst zu konfigurieren. IoT basiert auf standardisierten und interoperablen Kommunikationsprotokollen. Im IoT besitzen physische und virtuelle Dinge Identitäten, Attribute und virtuelle Persönlichkeiten. Die Dinge nutzen intelligente Schnittstellen und integrieren sich nahtlos in das Informationsnetz."

Kasten 2: Das IoT – Begriffsbestimmung.

Domäne	Daten	Missbrauchs-Szenario	Ethische Werte (+/-)
Smart Home	Zeitsteuerungen Zugangsdaten	Ausspionieren regelmäßiger Abwesenheitszeiten	Nachhaltigkeit (+) Sicherheit (-)
Smart Home	Video-/Audio-Zugangsdaten	Überwachung von Familienmitgliedern Überwachung von Angestellten	Sicherheit (+) Vertrauen (-)
Smart Grid	Stromverbrauch	Erstellung von Nutzungsprofilen Berechnung von Abwesenheit und Ruhezeiten	Nachhaltigkeit (+) Privatsphäre (-) Sicherheit (-)
Smart Health	Gesundheitsdaten	Veröffentlichung strafrechtlich geschützter Daten	Wohlergehen (+) Unversehrtheit (+) Privatsphäre (-)

Tabelle 1: Beispiele von Gefahren missbräuchlicher Datennutzung im IoT.

Die folgenden Fragen müssen für viele IoT-Objekte verneint werden, was Misstrauen fördert und schließlich zur Ablehnung von IoT-Technologien führen kann (**siehe Kasten 3**).

- Kann ich erkennen, ob ein Gegenstand „dumm“ oder „intelligent“ ist?
- Kann ich feststellen, ob ein Gerät Daten übermittelt?
- Kann ich die Daten einsehen?
- Kann ich die Daten löschen?
- Kann ich die Datenspeicherung unterbinden?

Beim Fernseher oder anderen elektronischen Geräten ist der moderne Mensch sensibilisiert und wittert die Technik. Aber bei Alltagsgegenständen wie Kleidung oder Warenverpackungen sieht die Sache anders aus. Aus diesem Grund sollen RFID-Tags mit Inkrafttreten der EU-Datenschutzrichtlinie durch einen Hinweis gekennzeichnet und damit für den Verbraucher sichtbar gemacht werden. Der Entwurf dieser Richtlinie wurde im Juni 2015 verabschiedet, mit einem Inkrafttreten ist frühestens 2018 zu rechnen.

Ethische Fragen

Das IoT bietet ein großes Potenzial zur Lösung drängender Problemen dieses Jahrhunderts. Hinter Schlagwörtern wie „Smart Home“, „Smart City“, „Smart Country“, „Smart Farming“, „Smart Cars“, „Smart Health“, „Smart Learning“ und „Smart Wearables“ verbergen sich innovative Lösungen beispielsweise zur

- Erreichung von Klimazielen
- Entlastung unserer Verkehrswege
- Verbesserung des Gesundheitswesens
- Optimierung unseres Pflegesystems
- Verbesserung von Bildungschancen
- Aufrechterhaltung der Infrastruktur im ländlichen Raum
- Anpassung an den demografischen Wandel

Diese Chancen für unsere Gesellschaft werden begleitet von Risiken für den einzelnen Bürger. Es stellen sich ethische Fragen, unter anderem bezüglich des Rechts auf Privatheit, des verantwortlichen Handelns, der Nachhaltigkeit und der sozialen Gerechtigkeit.
Die Europäische Kommission rief 2010 eine Expertengruppe IoT ins Leben, die Visionen für die Integration des IoT in die *Digitale Agenda für Europa*[2]) entwickeln sollte (**siehe Kasten 4**). Nach zwei Jahren wurde die Expertengruppe geschlossen und die Untergruppe *Ethik* veröffentlichte 2012 ihren Abschlussbericht (vgl. [Hov12]). Die Autoren fordern darin die Etablierung geeigneter Standards, um ethische Regularien im IoT auch *technisch* zu verankern.
Damit reiht sich die Europäische Kommission in den Tenor anderer Experten ein, die beispielsweise *Ethics-by-Design* fordern (vgl. [Dra14]) oder sich um ein *Social-Ethical Framework* bemühen (vgl. [Abb14]).
Ethische Fragen haben Einfluss auf IT-technische Aufgaben, egal ob es um Spezifikationen, Design-Entscheidungen, Aufzeichnungspflichten etc. geht. Die Anforderungsanalyse und das System-Design müssen sich anpassen und Werte wie die folgenden als nicht-funktionale Anforderungen in ihren Prozessen berücksichtigen:

- Privatsphäre
- Vertrauen

Das Smart-Grid-Projekt in den Niederlanden

Die Niederlande wollten sich nach der Jahrtausendwende für die Erreichung der Klimaziele wappnen. Man führte ein Smart Grid als Piloten ein und stattete teilnehmende Haushalte mit intelligenten Strommessern aus. Diese Smart-Meter-Objekte sendeten in kurzen Intervallen Verbrauchsdaten an die Leitstellen.
Als bekannt wurde, dass sich mit etwas Aufwand aus den Daten sehr persönliche Gewohnheiten der Hausbewohner ablesen ließen (z. B. „Gestern Nacht sahen sie den Film xy“), entwickelte sich eine stark ablehnende Haltung in der Bevölkerung.
Der Pilot schaffte es nicht in den Betrieb, jahrelange Forschung und Entwicklung verpufften wirkungslos. Die landesweite Einführung wurde vom Parlament schließlich abgelehnt und der Plan eines Smart Grid wurde aufgegeben. Der ethische Wert einer nachhaltigen Energieversorgung musste aufgegeben werden, da der Wert der Privatsphäre nur unzureichend berücksichtigt worden war (vgl. [Hov12]).

Kasten 3: Scheitern eines IoT-Projekts aufgrund der Vernachlässigung ethischer Werte.

[2]) Die Digitale Agenda ist eines der zentralen Anliegen im Rahmen der „Europa 2020 Strategie“ der Europäischen Union, einem Programm zur Förderung von Forschung und Entwicklung und zur Erhöhung des Wirtschaftswachstums.

Expertengruppe IoT der Europäischen Kommission

Die Expertengruppe *Internet of Things Expert Group (IoT-EG)* wurde im Jahr 2010 gegründet und sollte einen Erfahrungsaustausch zwischen Experten befördern. Sie erarbeitete Strategien und Visionen für die Entwicklung und den Betrieb des IoT. Ihre 39 Mitglieder vertraten unterschiedliche Belange und stammten aus den folgenden Bereichen:

- Forschung (Wissenschaft und Institute)
- Interessenverbände (Öffentlichkeitsarbeit, Informatik, Forschung, Energie, Verbraucherschutz, Flächenbewirtschaftung, Gesundheitswesen)
- NGO (Verbraucherschutz)
- Unternehmen (Industrie, Gesundheitssektor)
- Gewerkschaften (Arbeitnehmerinteressen)
- Nationale Verwaltungen

Einzelne Themen vertieften die Experten in den folgenden Untergruppen:

- IoT-Architektur
- IoT-Privatheit, Datenschutz, Sicherheit
- IoT-Governance-Architektur
- Standards
- Identifizierung
- Ethik

Die Gruppe wurde Ende 2012 geschlossen, gemeinsam mit ihren Untergruppen veröffentlichte sie mehrere Abschlussberichte (vgl. [IoT]).

Kasten 4: Expertengruppe IoT-EG.

- Verantwortung
- Persönliche Autonomie
- Nachhaltigkeit
- Menschliches Wohlergehen
- Freiwillige Zustimmung
- Verantwortung und Zurechenbarkeit für Handlungen
- Vermeiden von Beeinflussung und Manipulation

Die folgenden Abschnitte beleuchten exemplarisch einige dieser Werte im Kontext des IoT.

Privatsphäre und Vertrauen

Überwachungsmaßnahmen können sich auf den Einzelnen oder auf die Masse beziehen. Im ersten Fall geht es darum, möglichst viel über eine Person in Erfahrung zu bringen, der Überwachte steht im Zentrum aller Aktivitäten. Die Methoden der *operativen Kontrolle*, mit denen die DDR-Staatssicherheit missliebige Bürger bespitzelte und drangsalierte, sind ein Beispiel für diese Form der Überwachung.

Im zweiten Fall, der *Massenüberwachung*, benutzt man einen umfangreichen Datenpool zur Identifizierung von Auffälligkeiten. Die Frage des „wer“ ist irrelevant, oft steht vorab noch nicht einmal fest, wonach was gesucht wird. Die Abweichung von der Masse erweckt Verdacht und begründet weitere Maßnahmen. Beispiele hierfür sind die Rasterfahndung der 1970er Jahre und die Methoden der NSA, die von Edward Snowden enthüllt wurden.

Die Technologie des IoT bietet hervorragende Möglichkeiten für die Massenüberwachung: Daten werden gesammelt, gespeichert und zugeordnet. Auswertungen können später, zu einem geeigneten Zeitpunkt durchgeführt werden. Fragestellungen können in der Zukunft formuliert werden. Die Datensammlung erfolgt in großen Teilen unbemerkt und kann durch den Einzelnen kaum reguliert oder unterbunden werden. Die dezentrale Infrastruktur des IoT ermöglicht losgelöst von Institutionen auch die Überwachung von *Person-zu-Person*, wie die folgenden Beispiele zeigen:

1. Familien kontrollieren ihre Putzfrau.
2. Eltern überwachen die Aktivitäten ihrer Kinder.
3. Patriarchen überwachen die Familie daheim.
4. Aktivisten unterbrechen ihr „Still-alive“-Signal.

Zu 1: Sind Sie auch fleißig?

Smart-Home-Lösungen ermöglichen sowohl die Fernsteuerung als auch die Fernkontrolle des Hauses. Ein deutscher Anbieter warb bis vor Kurzem damit, dass seine Produkte die Überwachung der Putzhilfe ermöglichen (vgl. [Ste14]). Derartige Kontrollen mögen illegal sein, sind aber nicht unüblich, wie die Skandale von unzulässiger Arbeitnehmerüberwachung gezeigt haben. Systeme werden zur Überwachung von Personen zweckentfremdet.

Zu 2: Ich sehe, was du getan hast.

Eltern können bereits heute ihr Kind mit dessen Smartphone überwachen, sofern die entsprechenden Apps freigeschaltet sind. Radikalere Lösungen ermöglichen die Beobachtung von Aktivitäten im Kindergarten, dann stehen sowohl das Betreuungspersonal als auch die Kinder unter dauerhafter Beobachtung.

Kinder benötigen Vertrauen, um zu eigenständigen und selbstständigen Persönlichkeiten heranwachsen zu können. Weicht das Vertrauen der übermäßigen Kontrolle, so kann dies zu Abhängigkeit und Angst führen. Fanden derartige Tabubrüche früher in der realen Welt statt (zum Beispiel im heimlichen Lesen eines Tagebuches), so werden sie heute ins Virtuelle verlagert. Die Methoden sind modern, die entwicklungspsychologischen Gefahren bleiben die alten.

Zu 3: Ich regle alles zu eurem Besten.

Ein indisches Unternehmen wirbt für seine Smart-Home-Produkte mit dem Slogan: „Be the commandant of your home, even if you are miles away“ (vgl. [Ste14]).

Da in Indien Ein-Personen-Haushalte eher selten sind, ist es naheliegend, dass die Oberherrschaft über die Familie im Zentrum der Aktivitäten steht. Häufig sind Smart-Home-Systeme nicht für den Mehrbenutzer-Betrieb ausgelegt. Wer das System bedient, besitzt die Kontrolle über Eingangssysteme, Lichtschalter usw. Wer kam?

Wer ging? Zu welcher Zeit?
Mit der Fernsteuerung eines Wohnhauses lassen sich Strukturen der Dominanz, Kontrolle und Alleinherrschaft verfestigen, obwohl sie als digitaler Lifestyle modern wirken. Das Home-System, das Ziele wie Energieeffizienz und ein intelligentes User-Interface verkörpert, kann dazu missbraucht werden, Familienmitglieder zu überwachen, zu kontrollieren und zu entmündigen.

Zu 4: Hilfe, ich bin in Gefahr!
Die schwedische Menschenrechtsorganisation Civil Rights Defenders stattet gefährdete Aktivisten weltweit mit „Still-Alive"-Armbändern aus. Im Falle eines Übergriffs kann der Träger mit dem Armband unauffällig einen Alarm absetzen. Die Organisation löst dann einen Aktionsplan aus und informiert schützende Personen oder auch die Öffentlichkeit. Sie versucht damit, Fälle wie die Erschießung der tschetschenischen Journalistin Natalia Estemirova in Grosny zu verhindern, und benannte das Projekt nach der getöteten Aktivistin als „Natalia Project" (vgl. [Nat]).
Dieses Beispiel zeigt, dass es auch uneingeschränkt begrüßenswerte IoT-Anwendungen gibt. Zwar liegen hier ebenfalls zwei ethische Werte im Widerstreit: die Privatsphäre der Aktivisten und die Abwendung von Schaden für Leib und Leben. Da die Gefahr jedoch groß ist, geben die Aktivisten dem Schutzschild den Vorzug vor ihrer Privatsphäre.
In potenziell lebensbedrohlichen Situationen vertrauen wir Assistenzsystemen und sind bereit, Kontrolle abzugeben. Der Überlebensinstinkt ist größer als der Wunsch nach Privatheit, weshalb IoT-Anwendungen wie Notrufsysteme (beispielsweise *eCall*) oder die medizinische Überwachung gefährdeter Patienten breite Akzeptanz finden.

Verantwortung

Im Internet der Dinge agieren Objekte eigenständig, ohne dass es einer menschlichen Handlung bedarf. Die Knoten des IoT entscheiden situativ und kontextbezogen aufgrund der aktuellen Datenlage und vorhandener Algorithmen. Derartige Aktionen können sich auf den einzelnen Menschen geringfügig oder auch sehr weitreichend auswirken, wie die folgenden Beispiele zeigen:

5. Nachbestellung von Verbrauchsgütern.
6. Einschalten eines Haushaltsgerätes.
7. Güterabwägung bei einer unausweichlichen Kollision.
8. Töten eines Gegners.

Klingen die ersten beiden Situationen noch relativ läppisch, so wird weiter unten schnell klar, dass die Frage nach der Zurechenbarkeit und Verantwortung schwerwiegend sein können: entweder, weil etwas schief lief oder weil die Handlungen eines IoT-Akteurs ein moralisches Dilemma in sich bergen. Betrachten wir die Situationen etwas genauer.

Zu 5: Der Vorrat geht dir niemals aus.
Der Toner im Drucker ist alle, das Gerät bestellt automatisch nach und die Kosten der Warenlieferung werden auf Grund der Informationen im Benutzerprofil automatisch abgebucht. Es ist aber noch Toner im Vorrat, der Besitzer, Herr A., ist nicht an der Lieferung interessiert.
Ist die Bestellung rechtsverbindlich? Wenn Herr A. zwischenzeitlich manuell bestellt hat, wieso hat er die Nachbestellung im Gerät nicht deaktiviert? Hat er nicht gewusst, dass diese Funktion voreingestellt ist? Oder war er nicht in der Lage, das Gerät zu konfigurieren? Muss auch ein durchschnittlicher Benutzer ein Gerät bei der Inbetriebnahme auf voreingestellte Abos überprüfen? Wer hat bestellt: das Gerät oder der Besitzer?
Hier geht es um Fragen der Rechtsverbindlichkeit und damit der Zurechenbarkeit einer Handlung. Darüber hinaus werden ethische Werte wie *informierte Zustimmung*[3]) und *Freiheit von Manipulation* berührt.

Zu 6: Waschen, wenn der Strom günstig ist.
Familie B. nimmt am Smart Grid teil. Frau B. befüllt morgens die Waschmaschine und verlässt anschließend das Haus. Während sie im Büro ist, wird die Waschmaschine im Smart Grid aktiviert, das Waschprogramm läuft an. Leider löst sich ein Abwasserschlauch und nach kurzer Zeit stehen das Bad und bald auch das gesamte Geschoss unter Wasser. Ein Fall für die Versicherung. Wirklich?
Wer ist für den Wasserschaden verantwortlich? Frau B., die die Waschmaschine ohne Beaufsichtigung ließ, oder der Energieversorger, der das Waschprogramm gestartet hat? Hier bahnt sich ein Rechtsstreit zwischen Familie B., dem Stromerzeuger und der Versicherung der Familie an. Im schlechtesten Fall schließt der Versicherer den Leistungsfall aus und der Netzbetreiber die Haftung. Dann bleibt Familie B. auf ihrem Schaden sitzen.
Wie harmonieren Geschäftsbedingungen von IoT-Service-Anbietern und Versicherungen? Zurzeit bewerten Hausratversicherungen das Verlassen der Wohnung bei laufender Waschmaschine als grobe Fahrlässigkeit – der Kunde muss den entstandenen Schaden aus eigener Tasche bezahlen. Smart Grid ist aber nur dann sinnvoll, wenn Haushaltsgeräte auch ohne menschliche Kontrolle genutzt werden können.
Werden die Risiken auf den Verbraucher abgewälzt? Schon heute ist es dem Einzelnen kaum mehr möglich, die unzähligen Nutzungsbedingungen von Software, Geräten und Diensten zu prüfen oder gar Einfluss darauf zu nehmen. Viele Unternehmen handeln nach dem Prinzip „Friss oder Stirb" – wer dabei sein will, muss die Kröten schlucken. Die Vorstellung, ein Verbraucher könne die Geschäftsbedingungen einer Versicherung und eines Energieversorgers zum Zweck der Harmonisierung „nachverhandeln", erscheint geradezu aberwitzig naiv.
Der Problemkreis berührt die Werte *Zurechenbarkeit*, *Vertrauen* (=Vermeidung von Schaden) und *freiwillige Zustimmung*.

Zu 7: Welches Leben ist wichtiger?
Ein SmartCar befindet sich im autonomen Modus, ein Kind läuft vor das Auto. Der Bremsweg reicht nicht aus, um einen Unfall zu vermeiden. Ein Ausweichen nach links führt zu einem Frontalzusammenstoß mit einem anderen Pkw, ein Ausscheren nach rechts gefährdet eine Menschengruppe auf dem Gehweg.
Wie soll das Fahrzeug in dieser Situation reagieren? Das Kind überfahren, in die Menschengruppe steuern oder beim Frontalzusammenstoß das eigene Leben und das der anderen Fahrzeuginsassen gefährden? Das Dilemma ist unauflösbar, es gibt kein Falsch oder Richtig. Ein Mensch entscheidet in derartigen Situationen intuitiv innerhalb von Sekundenbruchteilen. Der Algorithmus eines autonomen Fahrzeuges muss derartige Anwendungsfälle berücksichtigen und Faktoren gewichten, um zu einer Entscheidung zu kommen.
Wer spezifiziert solch lebenswichtige Entscheidungen? Auf Grund welcher Faktoren? Wer ist im Unglücksfall verantwort-

[3]) „Informierte Zustimmung" bedeutet, dass ein Benutzer einer Hintergrund-Aktivität eines Systems ausdrücklich zustimmt und dabei über die Konsequenzen seines Handelns informiert wird. Beispiel: Zustimmung zum Speichern von Cookies im Browser.

lich und haftet wirtschaftlich? Hier sind die Werte *Unversehrtheit*, *Wohlergehen* der Unfallopfer sowie *Schuld* und *Zurechenbarkeit* der Akteure (=Fahrer und Smart-Car) involviert.

Zu 8: Ein spontaner Akt der Gnade?
Vollautomatische Waffensysteme brauchen keine externen Befehle, um Menschen zu töten. Derartig mächtige Systeme sind bereits heute als autonome Drohnen im Einsatz. Sie entscheiden aufgrund der Datenlage und wählen ihr Ziel sowie den Zeitpunkt des Angriffs selbstständig aus. Die Technologie geht damit weit über bisherige ferngesteuerte Drohnen hinaus, denn das Militär gibt erstmalig die Entscheidungsgewalt aus der Hand.
Die Eliminierung des Menschen aus dem Kriegsgeschäft könnte man einerseits begrüßen, schließlich verheißen autonome Waffensysteme hochriskante Einsatzmöglichkeiten bei gleichzeitiger Schonung der eigenen Soldaten. Aber wie sicher ist es, Objekten die Zielauswahl zu überlassen? Im Zeitalter asymmetrischer Kriege ist die völkerrechtlich gebotene Unterscheidung zwischen zivilen und militärischen Ziele ausgesprochen schwierig.
Darüber hinaus stellen sich sehr tiefgehende Fragen. Die *Befehlsverweigerung aus Gewissensgründen* ist für ein autonomes System undenkbar, Begriffe wie *Gnade* und *Zweifel* sind keine Option für eine smarte Drohne. Damit drohen selbst die winzigsten Inseln der Humanität aus dem Kriegsgeschehen zu verschwinden.

Ökologie und Nachhaltigkeit

Etliche IoT-Domänen wollen zur Erreichung von ökologischen Zielen beitragen und streben einen nachhaltigen Umgang mit Ressourcen an. Die folgenden Beispiele illustrieren, dass es auch hier nicht konfliktfrei zugeht:

9. Obsoleszenz[4])
10. Recycling

Zu 9: Muss ich die Waschmaschine wegwerfen?
Familie E. nimmt am Smart Grid teil. Der Energieversorger macht von seinem vertraglich vereinbarten Recht Gebrauch, Services jederzeit einzustellen oder Schnittstellen zu ändern. Nach einem Update lässt sich die Waschmaschine nicht mehr ansteuern. Die Software des vier Jahre alten Geräts ist nicht mehr kompatibel zum Smart Grid Interface, ein Update ist nicht verfügbar. Muss Familie E. die tadellos funktionierende Waschmaschine gegen ein neues Gerät austauschen?
Viele der smarten Anwendungen verbinden Dinge unterschiedlicher Lebensdauer und Innovationszyklen fest zu einem neuen Produkt. Im Allgemeinen hat Hardware (z. B. eine Waschmaschine und die Smart-Home-Infrastruktur aus Schaltern, Kabeln, Motoren usw.) eine längere Lebensdauer als die zugehörige Steuerungselektronik.
Ändern sich Software und Schnittstellen, so können ins IoT eingebundene Geräte frühzeitig veralten und unbrauchbar werden. Dadurch entsteht mehr Müll und der Ressourcenverbrauch steigt durch die Produktion neuer Güter. Der ethische Wert der Nachhaltigkeit, der im Smart Grid verwirklicht werden soll, kann sich bereits im System konterkarieren.

Zu 10: Kann ich das Ding im Wertstoffhof abgeben?
Frau L. möchte ihren Fernseher verschenken. Das Gerät ist noch relativ neu, aber der Bildschirm ist ihr zu klein, schließlich beginnt die Fußball-EM in zwei Wochen. Auf der Fahrt zum Wertstoffhof kommen Frau L. Bedenken: Der Fernseher war in das hauseigene WLAN eingebunden, dass Passwort ist im Gerät gespeichert. Gibt sie mit dem Fernseher den Zugang zu ihrem WLAN aus der Hand?
Selbst im Bereich von PCs und Tablets werden Daten vor dem Recycling nicht immer forensisch sicher gelöscht, obwohl es einfach anwendbare Tools dafür gibt. Daten-Leaks treten auch in sensiblen Bereichen wie Apotheken oder Arztpraxen gelegentlich auf.
Bei smarten Objekten ist die Lage weitaus schwieriger, denn deren Datenspeicher sind schwer zu erkennen und oft unzugänglich. Eine Benutzungsschnittstelle zum Löschen der Daten ist kaum vorhanden. Um im Beispiel zu bleiben: Manche Fernsehgeräte lassen nur die Eingabe und Änderung eines WLAN-Accounts zu, aber das Löschen der Daten ist unmöglich. Wer einen derartigen funktionsbereiten Fernseher weitergeben möchte, muss vorher umständlich Nonsens-Werte konfigurieren. Das ist unkomfortabel und wäre technisch vermeidbar. Wer ganz sicher gehen will, folgt den – nicht ganz ernst gemeinten – Empfehlungen zur sicheren Datenlöschung bei Smartphones: *Den Hammer nehmen und draufschlagen.*
Eine andere Alternative wäre es, sich auf die Kompetenzen des Wertstoffhofes zu verlassen. Damit würde der Wertstoffhof aber die Rolle des professionellen Datenlöschers übernehmen müssen, mit rechtlichen und organisatorischen Konsequenzen. Dieses

Value Sensitive Design (VSD)

VSD ist ein iterativer Prozess für das Design technischer Systeme unter ethischen Gesichtspunkten (vgl. [Fri05]). Die Methode integriert Wertvorstellungen wie die folgenden als nicht-funktionale Anforderungen in den Design- und Entwicklungsprozess:

- Privatsphäre
- Vertrauen
- Gleichheit
- Persönliche Autonomie
- Informierte Zustimmung
- Ökologische Nachhaltigkeit
- Menschliches Wohlergehen
- Verantwortung und Zurechenbarkeit für Handlungen
- Vermeiden von Beeinflussung und Manipulation

Die klassischen Methoden der Anforderungsanalyse und des Anwendungsdesigns – zu denen mittlerweile auch die agilen Methoden gehören – konzentrieren sich auf harte messbare Fakten wie Performance, Bedienbarkeit, Robustheit, Skalierbarkeit usw. VSD beleuchtet zusätzlich die Wertvorstellungen interner und externer Stakeholder.

Kasten 5: Werte als nicht-funktionale Anforderungen.

[4]) Produkte veralten und sind nicht mehr nutzbar, also obsolet. Die geplante Obsoleszenz ist eine Sonderform. Hier werden Produkte künstlich unbrauchbar gemacht, zu einem Zeitpunkt, zu dem die Funktionsfähigkeit technisch noch gegeben ist. Die geplante Obsoleszenz steht einem nachhaltigen Umgang mit Ressourcen entgegen.

Szenario scheint in absehbarer Zeit kaum vorstellbar. Für IoT-Objekte wird daher Privacy-by-Design gefordert (vgl. [Sch14]):

- Smart Objects müssen ihre Datenspeicher sichtbar ausweisen.
- Der Speicher sollte vorzugsweise physikalisch abtrennbar sein.
- Das Gerät muss über eine einfache und sichere Methode der Datenlöschung verfügen.

Soziale Gerechtigkeit und digitale Spaltung

Beispiele für ethische Wertkonflikte finden sich schnell im Umfeld unserer Arbeitsstätten sowie im Umgang mit elektronischen Geräten:

11. Messen der Arbeitnehmer-Performance
12. Digitale Inkompetenz

Zu 11: Sie haben fünf Minuten pausiert.
Im August 2015 gerieten die Arbeitsbedingungen beim Online-Händler Amazon wieder einmal in die Schlagzeilen. Dabei wurde bekannt, dass auch in Deutschland die Daten der Scanner personenbezogen gespeichert werden. Arbeitnehmer-Vertreter vermuten, dass diese Daten zum Zwecke der Leistungsmessung der Mitarbeiter ausgewertet werden. Das Unternehmen streitet dies ab.
Unbestreitbar bleibt, dass eine fünfminütige Arbeitspause technisch völlig problemlos „aufgedeckt" werden kann. Für Arbeitnehmer ist es aber nahezu unmöglich zu beweisen, dass etwaige Rügen oder Abmahnungen auf Grund unerlaubter Datenauswertungen erfolgt sind.
Wie bei anderen Überwachungsszenarien ist hier der Wert der *Privatheit* betroffen, aber es geht auch um *soziale Gerechtigkeit* im Kräftespiel zwischen Arbeitgebern und Arbeitnehmern. Der Arbeitsplatz ist auch in Deutschland immer wieder Schauplatz von Szenen unerlaubter Beobachtung. Vielleicht ist es an der Zeit, den digitalen Ungehorsam zu proben und kreative Wege zu gehen. Was wäre, wenn die Lageristen ihre Scanner tauschen oder zufällig aus einem Pool wählen würden?

Zu 12: Das Gerät raubt mir den letzten Nerv.
Herr K. verkauft sein Auto. Bevor er den Wagen an den Käufer übergibt, möchte er das Telefonbuch, das Adressbuch und sämtliche aufgezeichneten Fahrten aus dem elektronischen System löschen. Das Löschen der Telefonnummern gelingt ihm schnell, aber er findet keinen Zugang zu den Navigationsdaten. Nach mehreren Stunden gibt er frustriert auf und setzt das System auf „Werkseinstellungen" zurück. Ein mulmiges Gefühl bleibt. Wird jetzt noch alles funktionieren wie zuvor? Sind seine persönlichen Daten wirklich gelöscht? Der Zugang zur Datenspeicher-Funktionalität smarter Objekte ist oft nur für Experten ausgelegt. Diese verschaffen sich Zugang mit speziellen Adaptern und Lesegeräten. Der Wert der Privatsphäre des Autofahrers fällt im Beispiel unter den Tisch.
Ganz allgemein ist die Anpassung technischer Geräte an die persönlichen Anforderungen oft nur von technikaffinen Personen zu meistern. Es droht die Inkompetenz-Falle: Die Dinge verselbstständigen sich, das Gerät macht, was es will, und die Benutzer sind frustriert. Menschen werden immer abhängiger von Tools und Maschinen, müssen zwangsweise auf faire Voreinstellungen vertrauen und verlieren eigene Kompetenzen.
Werte wie die *persönliche Autonomie* der Benutzer und deren *freiwillige Zustimmung* bleiben unberücksichtigt, die soziale Spaltung vergrößert sich: Eine digitale Elite schafft es, ihre Werte dank Expertenwissen zu verteidigen, der gewöhnliche Nutzer muss die Dinge out-of-the-box hinnehmen.

Fazit

Die Grundeigenschaften des IoT wie *Allgegenwärtigkeit, Unsichtbarkeit, Lokalisierbarkeit* der Subjekte und die *Identifizierbarkeit* des Beobachteten, begünstigen panoptische Überwachungsszenarien in einem System unbekannter Akteure. Der Bürger kann sich dem IoT nicht entziehen, er wird oft ungefragt und ungewollt als externer Stakeholder in das System eingebunden. Daraus entstehen Interessenskonflikte zwischen den Werten und Zielen der IoT-Systembetreiber und den ethischen Werten und Vorstellungen der Bevölkerung.
Eine unzureichende Berücksichtigung der ethischen Werte der externen Stakeholder kann zur Ablehnung von Systemen und der gesamten Technologie führen, wie das Smart-Grid-Beispiel aus den Niederlanden illustriert (siehe Kasten 3). Die Berücksichtigung ethischer Standards in der Realisie-

Literatur & Links

[Abb14] R. Abbas, K. Michael, M.G. Michael, Using a Social-Ethical Framework to Evaluate Location-Based Services in an Internet of Things World, in: International Review of Information Ethics (IRIE), 12/2014

[Ash09] K. Ashton, That ‚Internet of Things' Thing, 2009, siehe: http://www.rfidjournal.com/articles/view?4986

[Ben1843] J. Bentham, The Works of Jeremy Bentham, Vol. 4 (Panopticon, Constitution, Colonies, Codification), 1843, siehe: http://oll.libertyfund.org/titles/bentham-the-works-of-jeremy-bentham-vol-4

[Dra14] L. Draetta, C. Rizza, The „silence of the chips" concept: towards an ethics(by-design) for IoT, in: International Review of Information Ethics (IRIE), 12/2014

[Fou77] M. Foucault, Überwachen und Strafen – Die Geburt des Gefängnisses, 1977

[Fri05] B. Friedman, P. Kahn, A. Borning, Value Sensitive Design and Information Systems, in: P. Zhang & D. Galletta (Hrsg.), Human-Computer Interaction in Management Information Systems: Foundations, 2005

[Fri15] D. Friess, O. Vermesan, Building the Hyperconnected Society – IoT Research on Innovation Value Chains Ecosystems and Markets, River Publishers Series in Communication, 2015

[Hov12] J. v. d. Hoven, Fact sheet -Ethics Subgroup Internet of Things – Version 4.01, Delft University of Technology, European commission, 2012, siehe: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=7662&no=11

[IER] IERC, European Research Cluster on the Internet of Things, siehe: http://www.internet-of-things-research.eu

[IoT] Internet of Things Expert Group (IoT-EG), European Commission, siehe: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2514

[Nat] Natalia Project, siehe: http://natalia.civilrightsdefenders.org/

[Sch14] B. Schafer, D-waste: Data disposal as challenge for waste management in the Internet of Things, in: International Review of Information Ethics (IRIE), 12/2014

[Ste14] B. Stengel, Ethische Überlegungen zu Smart Home, in: International Review of Information Ethics (IRIE), 12/2014

rung, der Weiterentwicklung und im Betrieb des IoT ist daher unerlässlich.

Wissenschaften wie die Medizin, Physik oder Biologie haben auf ethische Fragen ihrer Disziplinen unter anderem mit der Etablierung von Kommissionen reagiert. Im Zuge der digitalen Revolution hat die Informationstechnik eine große gestaltende Kraft, die unsere Gesellschaft nachhaltig verändert. Es wäre daher an der Zeit, dem Vorbild anderer Wissenschaften zu folgen und ethischen Fragen auch in der Informatik einen Platz in Forschung und Berufspraxis einzuräumen. Fragen der Privatheit, Sicherheit und Nachhaltigkeit müssen auch unter IT-Experten diskutiert werden und den Weg in Spezifikationen, Entwürfe und Anforderungskataloge finden. Die Probleme, die sich aus der Nutzung neuer Technologien ergeben, sollten frühzeitig erkannt und diskutiert werden. Unvermeidbare ethische Dilemmas müssen abgewogen werden, bevor das Kind in den Brunnen gefallen ist.

Die Praktiken der Anforderungsanalyse und die Design-Prozesse müssen sich weiterentwickeln, um ethische Fragen in der Systementwicklung zu berücksichtigen (**siehe Kasten 5**). Große Unternehmen legen auch in Deutschland ethische Richtlinien für das unternehmerische Handeln in einem Verhaltenskodex fest (*Code of Conduct*). Ethische Aspekte sollten die Ebene der Absichtserklärungen verlassen und als konkrete Anforderungen in die Produktentwicklung eingehen. Hierfür benötigen wir wertorientierte Entwicklungsprozesse. ‖

Der Autorin

‖ Kerstin Dittert
(kerstin.dittert@oocon.de)
ist freie Beraterin mit den Schwerpunkten Anforderungsmanagement, Softwarearchitektur und agile Prozesse. Sie plädiert für eine kritische Auseinandersetzung mit den Folgen der digitalen Revolution, interdisziplinär und auch unter IT-Experten.