JUST DO IT
HÖHERE ABTEILUNG FÜR
INFORMATIONSTECHNOLOGIE

tgm
Die Schule der Technik

Ethik-Ausarbeitung

Surveillance

Systemtechnik, Ethik
5YHITM 2016/17

Maximilian Seidl

Version 0.1
Note:
Betreuer: M.Graf
Begonnen am 21. Februar 2017
Beendet am 21. Februar 2017

Inhaltsverzeichnis

1 Was ist Surveillance?

1.1 Daten

Wenn man nichts zum Überwachen hat, dann macht Überwachen gar keinen Spaß. Dann kann man das Überwachen auch sein lassen. Aus Nichts lässt sich einfach Nichts machen. Wir brauchen also etwas, das wir betrachten können. Wir brauchen Daten. Mit den Daten fängt alles an. Ganz nüchtern formuliert repräsentieren Daten wertvolle Informationen. Daten alleine sind wertlos, wertvoll sind die Informationen, die in den Daten enthalten sind. Aber leider produziert das echte Leben keine Daten. Wenn mir ein Glas auf den Boden fällt, liegen da zwar ziemlich viele Scherben, aber elektronisch lesbare Daten wurden leider keine produziert.

Um Daten zu generieren, braucht es die Teilhabe von Informationstechnologie. Glücklicherweise wird unser Leben immer stärker durch Technologie unterstützt. Und überall, wo Informationstechnologie zum Einsatz kommt, entstehen Daten. Beispielsweise wenn wir bei der Bank handschriftlich eine Überweisung durchführen. Beispielsweise wenn wir im Hotel mit der Karte die Zimmertür aufmachen. Beispielsweise wenn wir uns einen Fahrschein für die Bahn am Automaten ziehen. Es gibt eigentlich kaum noch Prozesse, die ohne Informationstechnologie auskommen. Unser ganzes Leben produziert indirekt und permanent Daten. Aus diesem Grund ist es auch unmöglich geworden, sich der Überwachung zu entziehen. Jeder Vorgang, der Daten produziert, kann überwacht werden. Bei den Daten fängt alles an. Daten sind noch keine Überwachung, aber ohne Daten ist keine Überwachung möglich.

1.2 Speicherung

Daten entstehen, wenn man sie speichert. Strenggenommen entstehen Daten zwar schon vorher durch die Deklaration von Variablen im Programmablauf, aber das blenden wir jetzt mal aus. Speicherung an sich ist nichts grundsätzlich Schlechtes. Um Daten mit einem Zeitversatz zu verarbeiten, muss man sie einfach speichern. Wir schreiben uns zuhause einen Einkaufszettel (speichern) und streichen die Einträge später im Supermarkt wieder durch (löschen), sobald die Ware im Einkaufswagen liegt (verarbeiten). So gesehen erst einmal alles normal. Die Sache dreht sich erst, wenn Daten zeitlich über den Verwendungszweck hinaus gespeichert werden. Die Sache dreht sich erst, wenn Daten für eine artfremde Nutzung gespeichert werden. Die Sache dreht sich erst, wenn Daten ohne einen Mehrwert für mich gespeichert werden.

Gespeicherte Daten sind natürlich nicht böse. Böse ist nur, was man mit ihnen machen kann. Die gespeicherten Daten sind wie ein Protokoll. Und das Protokoll ist ein Fernglas in die Vergangenheit. Es gilt das gleiche Prinzip wie beim Videorekorder. Wir nehmen uns eine Sendung im Fernsehen auf, die wir nicht jetzt, sondern irgendwann später anschauen. Genauso machen das auch die Überwacher. Nur mit dem Unterschied, dass nicht eine einzelne Sendung, sondern sprichwörtlich das ganze Programm aufgezeichnet wird. Die Überwacher beschaffen sich also heute schon alle Daten über die Verdächtigen von Morgen. Zudem kennt man die künftigen Regeln und Gesetze ja noch gar nicht. Es ist also viel praktischer, wenn man einfach alle Daten speichert. Löschen ist vom System hier gar nicht vorgesehen.

1.3 Zugang

Um Daten zu speichern, benötigt man natürlich Zugriff auf die Datenquelle. Aber leider ist der Zugriff im Allgemeinen auf den eigenen Wirkungskreis beschränkt. Bei meinem Arbeitgeber habe ich keinen Zugriff auf die Gehaltsdaten meiner Kollegen. Auch die Wohnung meines Nachbarn ist immer abgeschlossen. Und zuhause fehlt mir das Passwort, um die Mails meiner Freundin zu lesen. Das gleiche Problem haben also auch die Überwacher. Die Daten der Anderen, da kommt man nicht so einfach dran.

Ohne Zugriff ist aber keine Überwachung möglich. Deswegen werden die Überwacher immer kreativer, wenn es darum geht, sich einen Zugang zu beschaffen. Da werden transatlantische Internetkabel angebohrt, um den Internetverkehr mitzulesen. Da werden Hintertüren in Programme und Hardware eingebaut, um jederzeit einen Zielcomputer auszuspionieren. Da werden Firewalls von Privatpersonen, Unternehmen und ganzen Staaten aufgebrochen. Überwachung impliziert also immer eine Zugriffsmöglichkeit, die eigentlich nicht existieren dürfte. Überwachung ist verbotener Zugriff in ein fremdes System hinein.

1.4 Beobachtung

In der Welt der Informationstechnik spricht man auch von Monitoring. Beim Monitoring liegt der Schwerpunkt nicht im Aufzeichnen, sondern im Beobachten. Die Beobachtung erfolgt dabei in Echtzeit, optional auch mit Speicherung. Das bringt einen ungeheuren Nutzen für unseren Alltag. Wenn die Heizung anspringt, sobald die Temperatur in der Wohnung unter 10 Grad fällt. Wenn das Antivirusprogramm Alarm schlägt, sobald es verdächtige Aktivitäten auf dem Computer entdeckt. Oder wenn das Auto piept, sobald wir die zugelassene Höchstgeschwindigkeit übertreten (natürlich versehentlich).

Es geht also um Grenzwerte. Man beobachtet den akzeptierten Normalzustand. Und sobald ein zuvor definierter, anderer Zustand eintritt, wird ein festgelegtes Protokoll von Aktivitäten gestartet. Leider starten diese Protokolle auch, wenn wir böse Wörter beim Telefonieren benutzen. Oder gewisse Menschen am Flughafen einchecken. Oder wenn normale Menschen abnormales Verhalten zeigen. Die Beobachtung ist in der Regel komplett durchautomatisiert. Automation ist auch viel besser als doofe Menschen. Automation ist billiger, zuverlässiger und schneller. So viele Überwachungsmenschen wie man zum Beobachten bräuchte, wären auch gar nicht auf der Welt vorhanden.

1.5 Metainformationen

Jetzt lassen sich Daten aber in ihrer ursprünglichen Form ganz schlecht bearbeiten. Daten sind wie Fließtext. Ein Fließtext ist zwar schön zu lesen, aber das war es dann auch schon. Man stelle sich vor, man suche einen Textabschnitt in einem Buch, das weder Seitenzahlen noch Kapital hat. Reiner Fließtext ist also unhandlich. Es fehlt Struktur. Es fehlt Vermessung. Es fehlt Deklaration. Es fehlt Klassifizierung. Aus diesem Grund hat man Metainformationen erfunden. Metainformationen sind additiv und ergänzen eine bestehende Information durch eine weitere Information. Durch Metainformation erhalten Daten einen zusätzlichen Mehrwert.

Mit Hilfe von Metainformationen können wir unsere Kontakte auf Facebook beispielsweise in „enge Freunde“ und „Bekannte“ unterteilen. Dadurch ist es möglich, sehr private Informationen

ausschließlich für enge Freunde zugänglich zu machen. Genauso arbeiten auch die Überwacher. Beispielsweise mit der Unterscheidung „ist ein Terrorist“, „ist vielleicht ein Terrorist“ und „ist kein Terrorist“. Und durch diese Mehrinformation entfalten Daten nun ihre wahrhafte Sprengkraft. Mit Metadaten lassen sich Informationen sortieren, filtern und klassifizieren. Und somit lassen sich völlig neue Level von Wissen und Erkenntnis generieren. Metainformationen sind manchmal sogar viel wichtiger als die eigentliche Information selbst. In Wahrheit geht es oft ausschließlich nur um Metadaten, für den eigentlichen Inhalt interessiert sich keiner.

Die Sache hat nur einen Nachteil, Metainformationen müssen erstens integer (also richtig), und zweitens auch aktuell gehalten werden. Schließlich ändert sich die Welt permanent, die Metadaten müssen sich also ständig ebenso ändern. Doof nur, dass bei der Erfassung von Metadaten sehr viele Fehler gemacht werden (ist ja auch ein sehr langweiliger, monotoner Vorgang). Außerdem sind Metadaten unmöglich aktuell zu halten (ist einfach viel zu viel Arbeit). Die Datenqualität ist also eher so mittelgeil. Und auf diesen mittelgeilen Daten treffen Überwacher echte Entscheidungen.

1.6 Suchen

Es wird gespeichert, es wird gespeichert, es wird gespeichert. Ein riesiger Datenberg entsteht. Aber am Ende kann man mit diesen vielen Daten eigentlich gar nichts anfangen. Man stelle sich das Internet ohne Suchmaschine vor. All die wertvollen Informationen, aber wir kommen trotzdem nicht dran.

Das Suchen in heterogenen Datenstrukturen ist ein anderes Suchen als das Suchen auf gleichartigen Internetseiten. Um Daten durchsuchen zu können, muss man die Daten indizieren. Das bedeutet, über diese Daten wird, ähnlich wie bei den Metainformationen, noch eine weiterer Ebene gelegt. Diese Ebene ist der Index. Der Index macht die Daten durchsuchbar. Ohne Suchmöglichkeit ist jede Speicherung faktisch eingeschränkt. Letztlich gilt, Suchen ist Überwachen. Die Überwacher suchen uns genauso wie wir unsere Exfreunde im Internet.

1.7 Entschlüsselung

Postkarten. Postkarten werfen wir in den Briefkasten und dann geht die Botschaft auf die Reise. Theoretisch könnte nun jeder Postmitarbeiter die Postkarte lesen. Praktisch haben die Postmitarbeiter dafür gar keine Zeit. Ich stelle mir manchmal vor, dass dies vor 20 Jahren noch anders war und finde es irgendwie romantisch. Im Unterschied zum Brief ist der Inhalt bei der Postkarte nicht verschlossen. Genauso ist es auch im Internet. Jedes Datenpaket ist wie eine Postkarte. Die im Datenpaket enthaltenden Informationen werden ganz offen durch das Internet getragen.

Um aus der Datenpostkarte einen Datenbrief zu machen, muss man die Informationen oder den Datenverkehr verschlüsseln. Im Unterschied zum Brief kann auch nicht jedermann verschlüsselten Datenverkehr einfach so aufmachen, sondern man braucht dafür einen ganz speziellen Schlüssel. Wenn man diesen Schlüssel nicht hat, sieht man nur Datensalat. Die Information ist zwar da, aber irgendwie auch nicht. Man kann sie einfach nicht lesen. Das ist schon ärgerlich. Das lassen sich die Überwacher natürlich auch nicht gefallen und sind echte Profis im Aufbrechen (Hacken) der Verschlüsselung. Wir dürfen das übrigens nicht. Das Hacken von verschlüsselten Daten ist nach deutschem Recht in vielen Fällen strafbar. Ich weiß zwar nicht warum, aber dieses Verbot gilt nicht für die Überwacher.

1.8 Kombination

Eine weitere Ebene von Information wird erreicht, wenn verschiedene Daten miteinander kombiniert werden. Die Kombination von Daten ist ein grundlegender und alltäglicher Vorgang der Informationstechnik. Unternehmen vergleichen völlig automatisiert die Zahlungseingänge auf dem Konto mit der Liste offener Rechnungen. Dieser Fall ist also die auf die eigenen Unternehmensdaten beschränkt. Aber natürlich kann man auch Daten kombinieren, welche unter völlig verschiedenen Gesichtspunkten von verschiedenen Organisationen gespeichert wurden. Man kann beispielsweise Steuerdaten mit Bankdaten vergleichen. Das wäre jetzt nicht mehr so lustig. Das bringt völlig neue Sachverhalte an das Tageslicht. Leider sind diese Vergleiche seit ein paar Jahren alltäglich geworden.

Wenn riesige Datenbestände miteinander kombiniert und analysiert werden, nennt man das BIG-DATA. Die Technologie steht noch ganz am Anfang und die Algorithmen sind relativ neu. Auch die erforderliche Rechenkraft ist noch nicht lange verfügbar. Insgesamt alles sehr abstrakt. Die Analysen sind hochwissenschaftlich. Kein Mensch kann sich die Sache richtig vorstellen. Aber das ist auch kein Wunder, es fängt ja gerade erst an. Letztlich geht es darum, komplexe Analysen auf große heterogene Datenmengen aus unterschiedlichen Quellen anzuwenden. Und was Überwacher damit alles anstellen werden, will ich gar nicht wissen.

1.9 Identität

Wenn man einen Datenstrom unter dem Mikroskop anschaut, dann sieht der Datenstrom in etwa so aus: 100101010011110. Ist das nicht total interessant? Alle Informationen bestehen letztlich nur aus einer Kombination von zwei Werten, 0 und 1. Ich finde das sehr faszinierend. Genauso faszinierend ist der Sachverhalt, dass die meisten Daten nur deswegen wertvoll sind, weil man sie einer Person oder einem Objekt zuordnen kann. Wenn man diese Zuordnung zerstört, also anonymisiert, vernichtet man implizit den ganzen Datenberg. Schließlich bringt das ja nichts, wenn man jemanden überwacht, aber gar nicht weiß, wen man überwacht. Überwachung impliziert also immer eine 1:1 Zuordnung.

Überwachung fokussiert sich immer auf ein Zielobjekt (also einen Menschen). In der Wissenschaft simulieren wir teilweise die gleichen Vorgänge und trotzdem entspringt dem Sachverhalt keine Dramatik. Weil man sich auf der Metaebene bewegt. Weil man die Daten aggregiert und am Einzelfall gar nicht interessiert ist. Weil man alle Daten anonymisiert und ein Umkehrschluss nicht möglich ist. Genau auf diesen Umkehrschluss sind aber die Überwacher angewiesen. Sonst ist all die Überwachung umsonst.

1.10 Konsequenz

Neben den technischen Aspekten trägt Überwachung auch eine inhaltliche Botschaft in sich. Diese Botschaft besteht aus einem Interesse und aus einer Erwartung. Das Interesse liegt in einem gewünschten Zustand, der meistens schon vorliegt, und den es zu schützen gilt. Und die Erwartung liegt in der Vermutung auf Gegenwehr. Die Gegenwehr wehrt sich natürlich gegen die bestehenden Verhältnisse. Der Zustand ist also krumm, was auch die Systemverteidiger wissen. Sonst würde es ja keinen Widerstand geben, dem es durch Überwachung frühzeitig zu begegnen gilt. Folglich ist Überwachung kein Selbstzweck. Überwachung ist Schutz und Abwehr. Überwachung indiziert

Systemschwächen. Überwachung ist Machterhalt. In der Konsequenz geht mit der Überwachung ein ganz konkretes Maßnahmenbündel einher. Dieser Aktionsplan ist die eigentliche Gefahr.

In unserer Wohnung überwacht ein Thermostat den Wasserbehälter. Fällt die Temperatur unter 40 Grad, springt der Boiler an. Die Gefahr ist also nicht der Thermostat. Die Gefahr ist der Boiler. Der Boiler ist das Maßnahmenbündel, welches über uns hereinbricht, wenn die Überwachung inhaltlich erkennt, was sie erkennen will. Nun ist aber nicht alles so einfach zu messen wie die Temperatur. Ein Überwacher unterliegt natürlich auch seiner Rolle. Wer einen Hammer hat, der sieht überall Nägel. Wer Überwacher ist, der sieht überall Verdacht. Und so steht die Polizei (der Boiler) schneller vor der Tür als man annehmen mag. Es ist aber nur der erste Schritt, wenn Überwachung Alarm schlägt. Die wahre Konsequenz steht noch aus und ist von ganz anderer Qualität.

1.11 Überwachung

Überwachung setzt sich also aus mehreren unterschiedlichen Komponenten zusammen, welche situativ individuell kombiniert werden. Wir nutzen diese Werkzeuge in spezifischen Szenarien selbst und ziehen viele Vorteile daraus. Für jeden Kontext stellt sich die Frage, ob man eine zielgerichtete Überwachung seines Selbst akzeptiert und befürwortet. In vielen Fällen wurden wir jedoch gar nicht gefragt und deshalb hört auch niemand unsere Antwort (sie lautet Nein). Selbst wenn wir wollten, wir können uns der Überwachung nicht mehr entziehen. Dafür produziert unser alltägliches Leben zu viele Daten. Parallel dazu wachsen die technischen Möglichkeiten fortlaufend. Schon morgen befindet sich eine vollständige Kopie der Wirklichkeit im Rechenzentrum der Überwacher. Dann ist es für jede Gegenwehr zu spät.

Wenn wir aber die Freiheit verlieren, dann verlieren wir auch unser eigenes Leben. Überwachung setzt Grenzen und innerhalb dieser Schranken befindet sich unsere eingeschränkte Identität. Die Grenzen haben wir nicht selbst errichtet. Das haben die Überwacher getan. Wir verbleiben nur noch als Funktionskörper, die auf festen Bahnen kreisen. Alles beginnt und endet beim Menschen. Datum

1.12 Quelle

`https://en.wikipedia.org/wiki/Surveillance`
`http://study.com/academy/lesson/what-is-surveillance-definition-systems-techniques.html`
`conflict.lshtm.ac.uk/page_68.htm`

2 Ethische Urteilsfindung

2.1 Sachverhaltsdarstellung

Zurzeit ist Überwachung des öffentlichen Raum ein heiß diskutiertes Thema. Immer wieder kommen neue Skandale ans Licht, welche sich mit der Privatsphäre anderer Menschen befassen. Das neu herausgebrachte Buch "Technologischer Totalitarismus" von Frank Schirrmacher, befasst sich mit den aktuellen Überwachungstechnologien und den Umgang mit Daten. "Wer liest, wird gelesen, wer kauft, wird selber zum Produkt", bringt es Schirrmacher knapp auf den Punkt. Zur Abwehr einer Überwachungs-, Kontroll- und Manipulationsgesellschaft muss die Macht von Informationskraken wie Facebook, Amazon, Apple oder Google eingehegt und in verträgliche Bahnen gelenkt werden.

2.2 Ethische Fragestellung

Wird mit den aufgenommenen Daten auch verlässlich umgegangen, bzw. werden diese auch nur wenigen Personen zugänglich gemacht?

Darf man prinzipiell davon ausgehen, das jede Person eine potentielle Gefahr für andere oder eine Gesellschaft darstellt?

Wollen wir in einer Überwachungsgesellschaft leben, die für Gerechtigkeit für alle sorgen könnte, doch ohne Privatsphäre für irgendwem?

2.3 Situationanalyse

Überwachung setzt sich also aus mehreren unterschiedlichen Komponenten zusammen, welche situativ individuell kombiniert werden. Wir nutzen diese Werkzeuge in spezifischen Szenarien selbst und ziehen viele Vorteile daraus. Für jeden Kontext stellt sich die Frage, ob man eine zielgerichtete Überwachung seines Selbst akzeptiert und befürwortet. In vielen Fällen wurden wir jedoch gar nicht gefragt und deshalb hört auch niemand unsere Antwort (sie lautet Nein). Selbst wenn wir wollten, wir können uns der Überwachung nicht mehr entziehen. Dafür produziert unser alltägliches Leben zu viele Daten. Parallel dazu wachsen die technischen Möglichkeiten fortlaufend. Schon morgen befindet sich eine vollständige Kopie der Wirklichkeit im Rechenzentrum der Überwacher. Dann ist es für jede Gegenwehr zu spät.

Wenn wir aber die Freiheit verlieren, dann verlieren wir auch unser eigenes Leben. Überwachung setzt Grenzen und innerhalb dieser Schranken befindet sich unsere eingeschränkte Identität. Die Grenzen haben wir nicht selbst errichtet. Das haben die Überwacher getan. Wir verbleiben nur noch als Funktionskörper, die auf festen Bahnen kreisen. Alles beginnt und endet beim Menschen. Datum

2.4 Pruefung der Verhaltensalternativen

2.4.1 Pro: Surveillance

- Kameras und Internetüberwachung machen Welt sicherer
- Überwachung hilft gegen Terroristen und schützt Bürger
- mehr Kameras würden eine einzig wirkliche Kontrolle und Balance bieten

2.4.2 Contra: Surveillance

- Menschen ohne Privatssphäre in der Öffentlichkeit
- Regierung setzt Überwachung ein um Bürger zu beobachten, dann führt das zu einem gegenteiligen Effekt

2.5 Normenpruefung

Recht auf Wahrung der Privatsspähre

- (1) Wer rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreift oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet, hat ihm den dadurch entstandenen Schaden zu ersetzen. Bei erheblichen Verletzungen der Privatsphäre, etwa wenn Umstände daraus in einer Weise verwertet werden, die geeignet ist, den Menschen in der Öffentlichkeit bloßzustellen, umfasst der Ersatzanspruch auch eine Entschädigung für die erlittene persönliche Beeinträchtigung.
- (2) Abs. 1 ist nicht anzuwenden, sofern eine Verletzung der Privatsphäre nach besonderen Bestimmungen zu beurteilen ist. Die Verantwortung für Verletzungen der Privatsphäre durch Medien richtet sich allein nach den Bestimmungen des Mediengesetzes, BGBl. Nr. 314/1981, in der jeweils geltenden Fassung.

2.6 Quellen

http://derstandard.at/2000018068147-2000018067071/Frank-Schirrmacher-Wer-liest-wird-selbst
https://www.jusline.at/1328a_am_Recht_auf_Wahrung_der_Privatsph%C3%A4re_ABGB.html

Tabellenverzeichnis

Listings

Abbildungsverzeichnis