Unsere Daten

Veränderte Bereiche durch Digitalisierung:

- Einkaufen, Filme, Telefone, Arbeitsplätze, Unternehmen, Bäckereien, Parken, U-Bahn-Fahren, Spielzeug, Häuser, Verkehr, Autos, Flugtickets, Dating, Fast Food, Musik, Banken, Kochen, Lernen, Kommunikation

Denn dass der Alltag mittlerweile zu einem bedeutenden Teil von meinem digitalen Leben durchdrungen ist, ist für diverse Akteure interessant.

Da wir, wenn wir all das online machen, Spuren hinterlassen, birgt diese Entwicklung ein Problem: Wir geben unsere Privatsphäre auf, werden gläsern. Verweigern wir uns diesem Mechanismus, sind wir von vielem ausgeschlossen.

Was geschieht mit unseren Daten?

Wie entstehen Daten über uns?

- Wer war heute schon im Internet? Wer hat Smartphone oder Hand yimmer dabei?

Sobald ich eine **Internetseite** öffne, registrieren sogenannte Trackingseiten meinen Besuch. Tracker zeichnen meine Aktivitäten dort mit

- Besuchte Seiten, Verweildauer auf welchen Inhalten, Gerät
- der Rhythmus, mit dem wir die Tastatur bedienen, gibt Einsicht in unsere Konsumlaune

Tracker werten die Daten aus und verknüpfen sie intelligent mit den Informationen über andere Nutzer*innen. Anders als wenn ich bspw. online etwas bestelle und selbst Daten eingebe (Präferenzen, Interessen, Kontaktdaten), wird beim Tracking dieses Profil erstellt, ohne selbst aktiv Daten einzugeben.

Mein **Smartphone** hingegen übermittelt Standortdaten, Kontakte, Bilder

- Soziale Netzwerke wie WhatsApp nehmen Kontaktinformationen aus Adressbuch, um andernorts neue Freunde vorzuschlagen
- Bewegungsdaten im Supermarkt bei eingeschaltetem WLAN
- Ohnehin tauscht man bei der Nutzung jedes freien WLANs Privatsphäre ein: „jedes Mal, wenn Sie sich mit einem WLAN-Hotspot verbinden, erlauben die von Ihnen akzeptierten Nutzungsbedingungen den Zugriff auf die persönlichen Daten in Ihrem Handy
- All diese Informationen werden zusammengeführt und übermitteln einerseits ein Bild meiner Interessen, mit wem ich mich treffe etc.

- Zum anderen zeigen die den Algorithmen zugrundeliegenden Rechenvorschriften Datenübereinstimmungen, kategorisieren Nutzerdaten und weisen Informationen eine bestimmte Priorität zu. Die Funktionsweise der Bewertungsalgorithmen bleibt dabei allerdings meist im Dunkeln.
- Daraus werden jedoch detaillierte Nutzertypen erstellt, die in Konsumtypen, Informationstypen gruppiert werden
- Diese Informationen werden verkauft.
- Führend beim Datensammeln Facebook und Google, aber auch andere Seiten verkaufen die gesammelten Informationen, denn die sind „eine Goldgrube für Menschen, die Ihnen etwas verkaufen wollen"

Über uns ist unheimlich viel bekannt – und für diese Infos zahlen Unternehmen, die detaillierte Konsument*innenprofile haben wollen, um uns gezielt passende Produkte anzubieten.

- „passende" Werbung bspw. durch Gesichtserkennung in der Postfiliale für alters- und geschlechtergerechte personalisierte Werbung
- „passende" Informationen: Informationsseiten, die uns psychologisch einordnen um uns Nachrichten anzubieten, die bei uns etwas triggern.

Den finanziellen Gegenwert bekommen wir nie genannt, wenn wir in den AGBs einer Internetseite zustimmen, dass alle über mich bekannten Informationen weitergegeben werden.

Bei all dem geht es nicht nur um eigene Privatsphäre und informationelle Selbstbestimmung. Sobald man Teil der Datenerhebungsmaschine wird, werden die eigenen Daten verwendet um andere zu beurteilen. Ich werde als Vergleichsobjekt herangezogen für Menschen, die im Gegensatz zu mir Auffälligkeiten aufweisen und unter Verdacht gestellt werden.

Es findet ein soziales Sortieren aufgrund von Typenzuordnung auf Grundlage der hinterlassenen Datenspuren statt – Folge: Digitale Diskriminierung.

- individualisierte Preisbildung aufgrund des errechneten „sozialen Status" (durch Nutzungsverhalten)
- Schufa, die von uns ein Risikoprofil erstellt auf Grundlage von Kriterien, die sie nicht offenlegt, die aber darüber entscheiden können, ob wir eine Mietwohnung bekommen oder eine Versicherung
- Bewerbungen werden durch selbstlernende Algorithmen vorsortiert
- In Australien sind bei einem Experiment der Finanzbehörden mit Datenabgleichen massive Steuerschulden von Millionen Menschen berechnet worden

Das Datensammeln und –verwerten kann auch ernste Konsequenzen bei repressiver Sicherheitspolitik haben.

- Wären Sie einverstanden, wenn die Polizei Ihnen sagen würde: Wir installieren Videokameras in Ihrem Wohnzimmer, im Bad, Schlafzimmer, in Ihrer Tasche und unter Ihrer Mütze, aber wir schalten sie nur ein, wenn Sie ein Verbrechen begehen?

Dazu haben wir aber längst zugestimmt, diese Infrastruktur ist schon installiert, denn genau das macht unser Smartphone.

Selbst wenn ich mir Sorgen um die Verwendung meiner Daten mache, habe ich nicht allzu viele Möglichkeiten, sie zu schützen. Bei den meisten der von mir besuchten Webseiten muss ich die Nutzungsbedingungen akzeptieren, um auf die Seite zuzugreifen.

Dabei können wir heute noch gar nicht absehen, welche Daten in Zukunft relevant sein werden und wann welche Information uns womöglich zum Nachteil gereicht.

Missbrauch der Daten möglich:

So bringt das Vertrauen in die etablierten **kommerziellen Plattformen** Abhängigkeit

Wissen ist Macht – Wer Zugriff auf die Daten von Menschen hat, hat Macht über sie und kann sie kontrollieren. Aber wer diese Macht hat, bleibt in der Regel intransparent.

Wenn kommerzielle Akteure – Verfügungsgewalt an der richtigen Stelle?

Beispiel für Macht der Plattformen: Charlotteville und gesperrte Facebook-Accounts durch Firmen

Missbrauch auch von **staatlicher** Seite

Seit den Enthüllungen von Edward Snowden ist bekannt, dass Sicherheitsbehörden all diese Informationen gezielt abrufen.

NSA, BND etc. verschaffen sich trotz Unzulässigkeit gezielt Zugang zu Daten

Für Sicherheitsbehörden: Abweichungen vom Regelfall verdächtig

- die Justiz in den USA prognostiziert mit Algorithmen bereits die Rückfallwahrscheinlichkeit von Straftätern und betreibt preventive policing
- In China soll künftig mit einem "Citizen Score" die soziale Zuverlässigkeit der Bürger berechnet und mit scharfen Sanktionen unterlegt werden.
- Ukraine: bei einer friedlichen regierungskritischen Demo bekamen Tausende Demonstranten eine SMS „Sie haben an einer illegalen Demo teilgenommen"

Von meinem Profil, meinem Verhalten, meinen Interessen, wird auf das anderer geschlossen und umgekehrt. Beim Nutzer kommen davon zunächst nur vermeintlich passende Inhaltsvorschläge an, die zu dem für ihn/sie erstellten Profil passen. Daher sind die etablierten Plattformen ja so attraktiv und smart – tatsächlich interessieren mich einige der Veranstaltungen, die mir Facebook vorschlägt und einige der Bücher, von denen rebuy meint, sie könnten mir auch gefallen.

Genuss dieses scheinbar kostenlosen Service. Aber nichts davon ist umsonst.

Vielmehr gibt es ein starkes Gefälle zwischen Anbieter- und Nutzerseite hinsichtlich Transparenz und Macht. Was tue ich, wenn mein Schufa-Score unerklärlich schlecht ist? Wie lange dauert es, eine Falschinformation über mich aus den Google-Ergebnissen zu entfernen? Und interessiert sich zu dem Zeitpunkt noch jemand für die Richtigstellung? Oder eine negative Bewertung auf einer Plattform für Ferienwohnungen?

Durch die deregulierte Digitalisierung werden wir vollkommen gläserne Konsument*innen (während Algorithmen intransparent sind) und Bürger*innen.

Wir werden auf unsere Daten, unser Digitales Leben reduziert und auf dieser Grundlage behandelt.

Aber die dahinterstehenden Strukturen sind nicht ethisch eingeordnet worden, während die kommerziellen Plattformen Tatsachen geschaffen haben, die fern von Verbraucherschutz stehen, und während die Sicherheitsbehörden von diesen Möglichkeiten nutznießen.

Datifizierung, Personifizierung → Gerechtigkeit? , Entscheidung auf Grundlage von Algorithmen, also Wahrscheinlichkeiten von Korrelationen, Verantwortungsverlagerung Mensch/ Maschine/ Programmierer*in

- Wem würden Sie Ihr Smartphone geben, um zehn Minuten lang die Inhalte anzuschauen? Nebenstehende*r, Partner*in, Bekannten, Supermarktkassierer*in?

Onlinedurchsuchung und Staatstrojaner werden als Standardinstrument im Kampf gegen Kriminelle eingesetzt – Ermittler dürfen die Geräte von Verdächtigen hacken.

- Wer nichts zu verbergen hat, der hat doch nichts zu fürchten, und wenn es denn der Sicherheit dient…

Datenerhebung, -speicherung, -verwendung und -weitergabe an Dritte bedrohen Privatsphäre und Selbstbestimmung.

Dadurch verschiebt sich das **Verhältnis zwischen Bürger*in und Staat**, wenn wir massenhaft ausgespäht werden, denn die Unschuldsvermutung wird umgekehrt. Dabei ist Privatsphäre ein Menschenrecht.

Was geschieht mit uns?

- Wenn Sie wüssten, dass die gesamte Stadt videoüberwacht wird und Sensoren Sie auf Schritt und Tritt durch Ihr Smartphone verfolgten – würden Sie dann zu einer Demo gehen oder eher nicht?

- Verhaltensadaption: Chilling effect, Geistige und emotionale Verarmung durch vorauseilenden Gehorsam

Wie können wir Herr unserer Daten werden?

Wer ist in der Verantwortung dafür?

Spätestens seit den Enthüllungen von Edward Snowden wissen wir als Bürger*innen, in welchem Ausmaß wir alle auch von Sicherheitsbehörden ausgespäht werden, sobald wir online gehen oder ein Gerät mit Funkverbindung nutzen. Wir wissen es, haben vielleicht kurz gestutzt oder vielleicht eine Phase der Abstinenz eingelegt oder kleine Einstellungsänderungen vorgenommen und nutzen die Angebote jetzt eben doch.

Das Internet nicht zu nutzen, ist kaum mehr möglich, wenn man den Anschluss nicht verlieren will. Der Umgang mit dem Internet wird mittlerweile als Grundkompetenz angesehen, die sich jede Bürgerin und jeder Bürger anzueignen hat.

Aber gerade wegen der Ubiquität des Digitalen ist es doch fundamental, dass die neuen Medien **sicher** genutzt werden können.

Also gewisse Passivität auf Verbraucherseite – liegt es am cultural lag? "Kulturelle Phasenverschiebung". Der Fortschritt lässt uns ratlos zurück. Weil wir noch halbe Affen sind, die Welt aber schon Science Fiction, kommen wir geistig nicht mit."

Was können wir also tun für unsere Digitale Souveränität?

Verbraucher*innen selbst:

AGBs mal lesen? (Herodes-Klausel)

Laut einer Studie müssten wir 76 Tage pro Jahr aufwenden, um alle AGB zu lesen, die uns im Alltag begegnen → keine Option

Einstellungen am Smartphone überprüfen, unterwegs WLAN ausschalten, alle Kommunikation verschlüsseln (dann nur bei gezieltem Verdacht Zugriffsmöglichkeit, statt undifferenzierter Massenüberwachung), einen Browser wählen, der unsere Nutzerdaten nicht an den Betreiber zurückspielt und weitergibt. Der Post und dem Supermarkt mitteilen, dass wir nicht ausgespäht werden wollen.

Aber das ist nur Kleinklein. Das strukturelle Problem ist nur politisch zu lösen, auch das der **Überwachung**.

Der Fokus meiner Betrachtung lag auf den Schattenseiten des Datensammelns.

Allerdings ist nicht zu vergessen, dass die Digitalisierung auch Liberalisierungs- und demokratiestiftendes Potenzial birgt, ein Instrument ist um mehr Teilhabe, Gemeinschaft oder Zugang zu Wissen zu ermöglichen.

Wir könnten uns daran erinnern, was der Philosoph John Locke vom Staat dachte: Der Staat dient uns. Er ist ein Vertrag mit uns selbst, dessen Inhalte wir bestimmen. Verstößt er dagegen, müssen wir ihn zügeln.

Dazu eröffnet die Digitalisierung eben auch neue Möglichkeiten.

Sie ermöglicht es eben auch, mit ein paar wenigen Klicks nachzusehen, wie meine Wahlkreisabgeordnete zur Vorratsdatenspeicherung steht, und sie ermöglicht es mir auch, sie direkt anzuschreiben oder öffentlich zur Rede zu stellen.

Das Internet eröffnet neue Möglichkeiten uns zu organisieren, um Verbraucherschutz zu fordern, Überwachungspraxis in die Schranken zu weisen, die Sammelwut der Wirtschaft zu kritisieren. Es bietet neue Öffentlichkeiten, die vielleicht ein Transparenzgebot für Algorithmen fordern können oder eine genossenschaftliche Organisation der Plattformen diskutieren.

Die ethischen Fragen um unsere Daten sind teilweise nicht neu. Durch die Reichweite der Digitalisierung jedoch sind ihre Implikationen heute bisweilen unmittelbar und drastisch und erfordern daher einen breiten gesellschaftlichen Diskussions- und Meinungsbildungsprozess.

Digitale Souveränität! – wie wir dahin kommen, darüber können wir hier ins Gespräch kommen.