Für einen digitalen Humanismus

Automatisiertes Verfolgen von Menschen und Waren

Ein junger Angestellter des *U.S. Census Bureau*, Hollerith, konzipiert 1880 ein Prinzip lesbarer Karten aus Karton mit standardisierter Lochung. Jedes Loch entspricht einem Merkmal einer Person: Geschlecht, Nationalität, Beruf. Die Karten können mit einer entsprechenden Maschine wieder ausgelesen werden. Millionen von Lochkarten werden auf Basis der US-Volkszählung erstellt und ausgewertet.

Hollerith verkauft 30 Jahre später Lizenzen seiner Lochkartenfirma, die 1924 in I*nternational Business Machines* (IBM) umbenannt wird, an das deutsche Unternehmen DEHOMAG, welches später als IBM-Tochtergesellschaft ab 1933 vom Regime Adolf Hitlers damit beauftragt wird, Lochkarten mit Informationen einer neuen deutschen Volkszählung herzustellen. Damit wird die Identifizierung von Juden, Sinti und Roma und anderen unerwünschten ethnischen Gruppen vorerst in Deutschland, später auch in den besetzten Gebieten systematisiert und automatisiert. Sie hat den Holocaust massgeblich ermöglicht und beschleunigt[1].

Daten darüber, wer wo lebt, Angaben zu Person und Geschlecht, sowie Familienstand werden seit 1938 ausserdem in Melderegistern erfasst. In vielen anderen europäischen Ländern existiert kein solches zentrales Melderegister wie in Deutschland.

Auch heute sind Menschen automatisiert verfolgbar. Nicht nur britische Autokennzeichen und unsere Reisepässe haben gemeinsam, dass sie eine kleine Antenne enthalten. Diese Antenne, in Form einer Spule, kann durch Radiowellen aktiviert werden, die in der Spule Strom induzieren. Wenn der Lesevorgang beginnt, also Strom induziert wird, kann die Antenne eine eindeutige Identifikationsnummer an das Lesegerät, dass die Radiowellen ausliest, zurückschicken. Die *Radio Frequency IDentification* (RFID) wird schon lange in Logistikzentren, Supermärkten und in grossen Kleidungsmärkten genutzt, wo die kleinen flachen Antennen in Etiketten eingeklebt sind und damit die Automatisierung der Verteilung und das Verfolgen von Waren vereinfachen.

Tiqqun würde sagen, der Mensch ist eben auch nur eine Ware: *„La destination de l'espace public est l'échange et la circulation des marchandises. Comme toutes les autres marchandises, les hommes s'y déplacent librement.“* [2] (Der öffentliche Raum ist für den freien Güterverkehr bestimmt. Menschen können sich in ihm frei bewegen, wie alle anderen Waren auch.)

1 Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*, 2001.

2 Tiqqun, *Dernier avertissement au parti imaginaire concernant l'espace public,* Poster, ca. 2001

Algorithmen erkennen, profilieren und lernen

In den 1990er Jahren verbreitet sich die Installation von Überwachungskameras, in Europa vor allem in Grossbritannien und Frankreich. Zahlen aus Frankreich zeigen allerdings, dass auch die systematische Überwachung von Plätzen keinen senkenden Einfluss auf die Kriminalitätsstatistik hat[3]. Während diese Kamerasysteme anfangs nur Bilder aufzeichnen und in eine Zentrale schicken, in der Polizeibeamte die Bilder ansehen, ist die Technologie seit Anfang der 2000er Jahre dahingehend weiter entwickelt worden, dass Bilder nun automatisch analysiert werden können. Texte, zum Beispiel Autokennzeichen, können automatisch gelesen werden, was in Grossbritannien zur Überwachung der Autobahnen genutzt wird. Auch Bewegung kann einfach erkannt werden. Es handelt sich hierbei um eine simple mathematische Operation des Vergleichens zweier Bilder. Das heute von Bilderkennungsprogrammen praktizierte Erkennen und Zuordnen einzelner Objekte und Gesichter ist jedoch das Resultat komplexer Algorithmen, die an Datenbanken gekoppelt werden und Wahrscheinlichkeiten berechnen. Wie wahrscheinlich ist es, dass die Person auf dem Bildschirm eine Frau, ihr T-Shirt grün und ihr Auto ein Kleinwagen ist? Je mehr Daten diese Systeme zum Vergleichen zur Verfügung haben, desto exakter können die Abgleiche stattfinden, die Wahrscheinlichkeiten berechnet werden. Oft stecken dahinter sogenannte künstliche neuronale Netze, die mit Methoden wie der des sogenannten *Deep Learning* ihre Ergebnisse immer weiter optimieren. Einige dieser Netze werden initial mit von billigen Arbeitskräften erstellten Datensets gefüttert[4], denn alles ganz allein lernen kann eine solche Maschine nicht.

Vorreiter in der Gesichtserkennung ist China. Das Land hat 170 Millionen Überwachungskameras, Tendenz steigend, und nutzt solche Systeme sowohl zur Überwachung des öffentlichen Raums als auch zum Abheben von Geld an Geldautomaten, an Türen von Firmen und Büros. Ab 2020 soll im Land zudem ein s*ocial credit system* entstehen, das jedem Bürger Punkte zuweist, je nachdem, wie er sich verhält. Diese Punkte könnten dann Einfluss darauf haben, ob jemand eine Studienförderung oder einen Arbeitsplatz bekommt.

Vor Deutschland macht diese Entwicklung keineswegs halt. Im Sommer 2017 hat die Bundespolizei am Berliner Bahnhof Südkreuz versuchsweise Kameras installiert, die die Gesichter von vorbeilaufenden Menschen mit Bildern einer Datenbank vergleichen. Die dabei benutzten Datenbanken zum Abgleich könnten biometrische Passbilder von Ausweisen und Reisepässen enthalten, sowie Bilder aus sozialen Medien[5].

Das Öl des 21. Jahrhunderts - Profile und Vorhersagen

Welche Daten werden gesammelt? Grundsätzlich wird unterschieden zwischen Daten und Metadaten. Daten sind Inhalte, zum Beispiel Texte, Briefe, Emails, Fotos, Sounds, Videos. Metadaten sind Daten über Daten, sie beschreiben die Inhalte. Im Digitalen sind sie für den Nutzer meist nicht sichtbar. Beispielsweise enthält ein digitales Bild Metadaten über den benutzten Fotoapparat, Modell, Belichtungszeit, Blende, oder über das Programm, mit dem das

3 Jean-Marc Manach, *Un rapport prouve l'inefficacité de la vidéosurveillance*, 2009. Online unter http://bugbrother.blog.lemonde.fr/2009/11/13/un-rapport-prouve-linefficacite-de-la-videosurveillance/

4 Vgl. die Arbeit des Künstlers Sebastian Schmieg, Online unter http://sebastianschmieg.com/works/segmentation-network/

5 BKA schließt Probelauf zur Gesichtserkennung ab, 2017. Online https://netzpolitik.org/2017/bka-schliesst-probelauf-zur-gesichtserkennung-ab/; Bitte lächeln: Interpol startet neue Datenbank zur Gesichtserkennung, 2016. Online https://netzpolitik.org/2016/bitte-laecheln-interpol-startet-neue-datenbank-zur-gesichtserkennung; EU erweitert polizeiliche Datenbanken mit Fähigkeiten zur Gesichtserkennung, 2016. Online https://netzpolitik.org/2016/eu-erweitert-polizeiliche-datenbanken-mit-faehigkeiten-zur-gesichtserkennung

Bild erstellt wurde. Weiterhin können geographische Koordinaten enthalten sein. Andere Dateitypen enthalten ebenfalls Metadaten über das zum Erstellen benutzte Programm, den Autor, die Dateigrösse oder die Erstellungszeit des Dokuments.

Verbindungsdaten sind auch Metadaten. In E-Mails beispielsweise steht im versteckten sogenannten Header, wann und von wo der Besitzer des E-Mail-Kontos sich zum Mailserver verbunden hat. Auch mit OpenPGP verschlüsselte E-Mails verschlüsseln nur die Inhalte der E-Mails, aber nicht die Header, und noch weniger, wer wem schreibt. Auch in den sozialen Netzwerken können durch das Sammeln solcher Verbindungs- und Kontaktdaten genaue Profile von unseren sozialen Kreisen erstellt werden: wer kennt sich, wer kennt sich gut, wer redet wie oft mit wem? Schreibe ich oft abends oder eher während der Arbeitszeit?

Ähnliche Daten fallen an, wenn wir Kundenkarten in Supermärkten benutzen oder online einkaufen. Wann kauft der Mensch wo welche Produkte, wie oft, in welcher Kombination? Natürlich geht es dabei vor allem darum, uns gezielte Werbung zu schicken, damit wir noch mehr kaufen. Dabei ist es interessant zu wissen, wo wir wohnen, wie alt wir sind, ob wir ein Auto haben. Je nachdem erhalten wir dann Werbung für Ökoprodukte oder Autozubehör. Ausserdem werden diese Daten oft weiter verkauft, an andere Firmen, die uns ebenfalls etwas verkaufen möchten.

Auch bei kostenlosen E-Mail-Anbietern, in sozialen Medien und auf Shopping-Seiten erhält der Nutzer einen praktischen Service umsonst. Doch ist er damit selbst zum Produkt geworden, denn im Austausch für den kostenlosen Dienst gibt er seine Daten preis. Jedes Senden einer Nachricht, jedes Anschauen eines Bilds, jede unserer Aufmerksamkeiten generiert sogenannte *page views* und damit Werbeeinnahmen. Nicht zuletzt deshalb gehören die GAFA (Google, Apple, Facebook, Amazon) zu den reichsten Firmen der Welt, obwohl ihre Dienste umsonst sind. Das sogenannte *Data Mining*, das Daten und Metadaten (*Big Data*) mittels Algorithmen auf Querverbindungen und Trends analysiert, nutzt nicht umsonst die Metapher der Förderung (engl: *to mine*) von Rohstoffen und damit der Wertschöpfung. Die Aussage, *Big Data* sei das Öl des 21. Jahrhunderts, scheint nicht von weit hergeholt.

Durch die Analyse von Metadaten ist es möglich, unser Verhalten zu studieren und es sogar vorherzusagen. Auf individueller Ebene ist es möglich, mit hoher Wahrscheinlichkeit unser Geschlecht zu bestimmen, unsere sexuelle Orientierung, unsere Werte, unsere Lebensgewohnheiten, die Anzahl unserer Partner und Kinder zu kennen. Banken nutzen Systeme, die aufgrund der über uns bekannten Daten berechnen, wie kreditwürdig wir sind. Das Vorhersagen von Verhalten ist besonders problematisch: Menschen, die einem bestimmten (sozialen, ökonomischen, Herkunfts-)Profil entsprechen, könnten nach vermeintlich ähnlichen Mustern handeln und stehen damit unter Generalverdacht.

Aber auch auf gesellschaftlicher Ebene ist es durch *Data Mining* und Algorithmen möglich geworden, Wahlverhalten, Demonstrationen und Aufstände vorherzusagen oder sogar zu beeinflussen. Über soziale Netzwerke, die Daten auch an Staaten verkaufen, können Aufstände, Demonstrationen und sogar Epidemien in Realzeit verfolgt, analysiert und kartographiert werden. In Polizeiwachen wird mittels *Predictive Policing*-Software vorhergesagt, wie wahrscheinlich es ist, dass in einer bestimmten Gegend ein Einbruch geschieht oder ein straffällig gewordener Mensch erneut eine Straftat begeht. Hier wird deutlich, dass *Big Data* zur Bevölkerungskontrolle, Stimmungsanalyse und politischen Manipulation genutzt werden kann.

Es stellt sich die Frage nach Mitbestimmung und nach Besitz: welche dieser Daten dürfen gesammelt und analysiert werden und von wem? Wie werden sie genutzt? Dürfen wir das mitbestimmen? Ausserdem stellt sich die Frage der Identität: inwiefern sind wir unsere Daten? Welche Handlungsspielräume bleiben uns, wenn ein Computer ausgerechnet hat, dass wir mit

hoher Wahrscheinlichkeit straffällig werden?

Ausserdem sind die Algorithmen, die benutzt werden, um Profile zu erstellen weder öffentlich noch sind sie Gesetzen unterworfen. Arbiträr sind sie sowohl Spiegel als auch Wurzel von Diskriminierungen.

Ich habe nichts zu verbergen!

Das „Ich-habe-nichts-zu-verbergen"-Argument ist weit verbreitet und es ist schwierig, darauf angemessen zu reagieren.

Im „Ich habe nichts zu verbergen"-Argument manifestiert sich die Verbindung von Privatsphäre zu Sicherheit. Viele Menschen sind bereit, ihre Privatsphäre für mehr Sicherheit aufzugeben, in der Annahme, dass nur Menschen, die unmoralisch und gesetzwidrig handeln, etwas zu verbergen hätten. Doch es handelt sich hierbei um einen Trugschluss.

- „Ich habe nichts zu verbergen!"
-- „Hast du Vorhänge an den Fenstern?"

Nicht jeder, der Vorhänge vor seine Fenster hängt, will seinen Lebenspartner umbringen…

- „Ich habe nichts zu verbergen!"
-- „Darf ich mal deine Kontakte und Fotos auf dem Smartphone ansehen?"
- oder:
-- „Zeigst du mir deine Kontoauszüge der letzten drei Jahre?"

Intimität ist ein Gut, dass mit Unmoral nichts zu tun hat.

„Die Verletzung der Freiheit schmerzt nicht, man spürt sie nicht, man erlebt keine Krankheit, keine Überflutung, keine Chancenlosigkeit am Arbeitsmarkt. Die Freiheit stirbt, ohne dass die Menschen physisch verwundet werden. In allen politischen Systemen ist das Versprechen auf Sicherheit der eigentliche Kern der staatlichen Gewalt und Legitimation. Während Freiheit immer zweitrangig ist oder wirkt."[6]

Inwiefern ist Sicherheit überhaupt ein Zustand? Handelt es sich nicht vielmehr um eine Idee oder ein Versprechen? Inwiefern ist dieses Versprechen imaginär, inwiefern konkret? Können durch das Sammeln und systematische Analysieren von Daten Verbrechen wie Korruption, Waffen- oder Drogenhandel, Genozide, Profitgier, Wilderei, Verbrechen an unserer Umwelt aufgedeckt werden? Wir müssen es bezweifeln.

Inwiefern werden die gesammelten Daten also zu moralisch guten Zwecken genutzt und nicht, als Beispiel, zur Industriespionage zwischen Staaten? Und wer bestimmt was moralisch „gut" ist? Ist heute etwas gut, was morgen nicht mehr gut ist - und können unsere Daten dann rückwirkend analysiert werden? Wer hat Zugang zu den gesammelten Daten? Wer bestimmt, was mit den Daten geschieht, wie lange sie gespeichert werden? Gibt es ein Recht auf Vergessen?

6 Der Soziologe Ulrich Beck im Gespräch: *Digitaler Weltstaat oder digitaler Humanismus?* 2013. Online unter http://www.faz.net/aktuell/feuilleton/debatten/der-soziologe-ulrich-beck-im-gespraech-digitaler-weltstaat-oder-digitaler-humanismus-12287900.html?printPagedArticle=true#pageIndex_0

Was ist Privatsphäre?

Wir verstehen Privatsphäre als Recht auf nichtöffentliche Lebensbereiche, in denen ein Mensch sein Recht auf freie und autonome Entfaltung der Persönlichkeit wahrnehmen kann, ohne von aussen beeinflusst, beobachtet oder in seiner Würde verletzt zu werden; Recht welches jedoch zum Schutze des Allgemeinwohls beschnitten werden darf.

Nach Daniel J. Solove ist Privatsphäre nicht gleichzusetzen mit dem Begriff der Intimität[7]. Nicht alle privaten Informationen oder Entscheidungen sind intim, wie beispielsweise unsere politischen Orientierungen oder unsere Religion. Solove bemerkt, dass es schwer fällt, Privatsphäre in ihrem Wesen zu definieren, denn viele Konzepte seien zu einseitig. Daher bietet der Professor für Jura an, Privatsphäre als Netzwerk von sich überlappenden Konzepten und Ähnlichkeiten zu verstehen. Dazu hat er eine Taxonomie erstellt, die aus vier Oberbegriffen und mehreren Unterbegriffen besteht[8]:

- Sammeln von Information (Überwachung, Vernehmung)
- Verarbeiten von Information (Bearbeitung, Aggregation, Identifizierung, Unsicherheit, Fremdnutzung, Ausschluss)
- Verbreitung von Information (Vertrauensbruch, Veröffentlichung, Austellung, erhöhte Zugreifbarkeit, Erpressung, Aneignung, Verzerrung)
- Invasion (Eingriff, entscheidungsbedingte Interferenz)

Diese Punkte beschreiben allesamt Formen der Invasion in die Privatsphäre. Wobei ich mit Joseph Weizenbaum argumentieren will, dass die Verwendung des Informationsbegriffs bei Solove inkorrekt ist. Denn es handelt sich nicht um „Informationen sondern [um] Daten oder Signale […]. Aber ich kann daraus Informationen gewinnen. Ich muß diese Informationen jedoch tatsächlich erst herstellen.“[9] Der Mensch interpretiert Datensätze, zum Beispiel indem er Algorithmen programmiert, die durch Überlagerungen, das Erkennen von Mustern oder von Abweichungen ebendieser Muster erst zu Informationen werden.

Wenn man die Privatsphäre nach Solove als „Pluralität verwandter Probleme“ begreift, wird klar, dass das Verstecken vermeintlich unmoralischer Dinge vor systematischer Überwachung durch Geheimdienste wie die NSA nur ein Problemfeld darstellt, in dem der Begriff der Privatsphäre dem des Allgemeinwohls oder der Gesellschaft antagonistisch gegenübergestellt wird. Durch die Generalüberwachung werden aber auch legale Aktivitäten beobachtet und aufgezeichnet, was Menschen davon abhalten kann, sich zu engagieren oder sich zu äussern[10]. Hier wird die Problematik der generalisierten Überwachung extrem deutlich: sie beschneidet und interferiert mit dem Recht auf freie Entfaltung und autonome Entscheidungen.

Durch fehlende Transparenz und Mitbestimmung im Sammeln und Verarbeiten der Daten können Fehler und Missbrauch entstehen, kafkaeske Situationen, in welchen das Individuum zwar keinen Handlungsspielraum hat, wohl aber Subjekt der Untersuchung ist.

---

7 Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 2008. Online unter http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications

8 Ebd.

9 Joseph Weizenbaum, *Information-Highways and the Global Village - vom Umgang mit Metaphern und unsere Verantwortung für die Zukunft*, Vortrag Universität Osnabrück, 1996. Online unter http://www.sommeruni.uni-osnabrueck.de/08_stage.htm

10 Vgl. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy.*

In welcher Welt wollen wir leben?

Der Datensammlung können wir uns kaum entziehen. Wir sind dabei nicht Subjekt, unsere vermeintliche Identität wird von außen konstruiert, wenn eine konkrete Anfrage an Datenbanken gestellt wird. Doch müssen wir versuchen, unsere Privatsphäre zu schützen, sowohl als Akt des Behauptens unserer realen Identität als auch als Akt des Schutzes und der Erweiterung unserer Handlungsspielräume. Wenn Maschinen vorhersagen, wie wir handeln werden, spricht uns das jede Individualität, Möglichkeit zur Veränderung und Mündigkeit ab.

Wir glauben, dass Maschinen schneller „denken" können als wir. Dass sie in der Lage sind, schneller logische Entscheidungen zu treffen[11]. Doch der algorithmischen, künstlichen „Intelligenz" – der Begriff selbst bedarf einer eigenen Untersuchung – fehlen grundlegende menschliche Qualitäten, wie das Bauchgefühl oder die emotionale Intelligenz. Computer denken nicht, sie können nur rechnen und vergleichen. (Wir sollten sie öfter „Rechner" nennen.) Auch neuronale Netze und *Deep Learning* basieren letzten Endes auf Vergleichen. Computer können das durchaus schneller als der Mensch. Sie können auch mehr Daten speichern. Dabei entstehen neue, sich stets vergrößernde Gebilde indexierter, und damit durchsuchbarer und verwertbarer Daten und Informationen. Totgeglaubte kybernetische Utopien, die in diesen selbstgesteuerten, quasi-intelligenten, Gebilden und Systemen Optimierung und vernunftbasiertes Handeln verorten, erscheinen verführerisch. Doch auch im Digitalen geht es immer noch darum, wem die Daten gehören und was damit gemacht wird.

Nach Ulrich Beck beruht das „digitale Imperium [...] auf Merkmalen der Moderne, die wir noch gar nicht richtig durchdacht haben. [...] Es verfügt [...] über die extensiven und intensiven Kontrollmöglichkeiten in einer Breite und Tiefe, die letztlich alle individuellen Präferenzen und Schwächen offenlegen - wir alle werden gläsern, durchsichtig."[12] Auch deshalb sind es nicht nur Journalisten, Whistleblower, Aktivisten, Anwälte, Bürger in politisch instabilen Ländern oder Menschen, die vor (häuslicher) Gewalt und Verfolgung fliehen, die ihr Recht auf Privatsphäre ausüben können müssen.

Der digitale Fortschritt sollte nicht die Dystopie einer, durch Menschen geschaffenen, von Maschinen und Algorithmen beherrschten Welt in die Realität umsetzen. Wie Sebastian Schmieg erklärt, verändern Algorithmen schon heute nicht nur unsere Konzepte der Arbeit, sondern auch unseren Umgang mit anderen Menschen, die mehr und mehr wie *software extensions* behandelt und jederzeit de/aktiviert werden können[13].

Schlussfolgernd. Ein Hammer kann dazu benutzt werden, einen Nagel in die Wand zu schlagen, oder jemandem auf den Kopf zu hauen. Wie jedes Werkzeug könnten auch *Big Data*, neuronale Netze und Algorithmen dazu verwendet werden, uns zu helfen, eine gerechtere und nachhaltigere Welt zu bauen. Wir haben die Verantwortung für das, was wir mit unseren Werkzeugen tun. Deshalb müssen wir auf gesellschaftlicher Ebene darüber nachdenken, wie wir es tun und in welcher Welt wir in Zukunft leben wollen. Eine humanistische digitale Ethik kann selbstverständlich nicht unabhängig von ökonomischen und politischen Gesichtspunkten gedacht werden. Das heißt, solange Konzerne und deren Interessen über den Interessen der Menschen, anderer empfindsamer Wesen und der nachhaltigen Entwicklung unseres Planeten stehen, riskieren wir, dass diese Technologien fast ausschließlich die Diener der totalen Verwertbarkeit und Profitabilität eines globalisierten Kapitalismus bleiben.

---

11 Vgl. Interview Peter Reichl zum Digitalen Humanismus. Online unter http://www.point-of-science.com/artikel/2017/2/3/digitaler-humanismus

12 Vgl. Ulrich Beck, *Digitaler Weltstaat oder digitaler Humanismus?*

13 Sebastian Schmieg, *Humans as software extensions*, Vortrag 34C3, 2017, Online unter https://media.ccc.de/v/34c3-9077-humans_as_software_extensions

Zum Weiterlesen:

- Gesichtserkennung in China.
  https://netzpolitik.org/2017/china-mit-gesichtserkennung-gegen-klopapierdiebstahl/
- Gesichtserkennung am Berliner Südkreuz.
  https://netzpolitik.org/tag/suedkreuz/
- How-To Analyze Everyone – Teil VII: Zeig mir dein Gesicht
  https://netzpolitik.org/2014/how-to-analyze-everyone-teil-vii-zeig-mir-dein-gesicht/
- How to analyze everyone – Teil II: Wie findest du eigentlich Zombiefilme?
  https://netzpolitik.org/2014/how-to-analyze-everyone-teil-ii-wie-findest-du-eigentlich-zombiefilme/
- How-To Analyze Everyone – Teil IV: Kunden, die diese Feueraxt gekauft haben, mögen Zombiefilme https://netzpolitik.org/2014/how-to-analyze-everyone-teil-iv-kunden-die-diese-feueraxt-gekauft-haben-moegen-zombiefilme/
- How-To Analyze Everyone – Teil VI: Neurotisch? Extrovertiert? Dein Provider könnte es wissen.
  https://netzpolitik.org/2014/how-to-analyze-everyone-teil-vi-neurotisch-extrovertiert-dein-provider-koennte-es-wissen/
- How-To Analyze Everyone – Teil IX: Predictive Policing oder wenn Vorurteile Algorithmen füttern
  https://netzpolitik.org/2014/how-to-analyze-everyone-teil-ix-predictive-policing-oder-wenn-vorurteile-algorithmen-fuettern/
- Algorithmen und Kriminalität. Er wird, er wird nicht, er wird… 2016.
  http://www.taz.de/!5243783/
- Wenn man diese 25 Produkte kauft, ist man mit grosser Wahrscheinlichkeit schwanger.
  http://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2?IR=T
- Metadaten: Wie dein unschuldiges Smartphone fast dein ganzes Leben an den Geheimdienst übermittelt.
  https://netzpolitik.org/2014/metadaten-wie-dein-unschuldiges-smartphone-fast-dein-ganzes-leben-an-den-geheimdienst-uebermittelt/
- Real-Time Disease Surveillance Using Twitter Data: Demonstration on Flu and Cancer.
  http://chbrown.github.io/kdd-2013-usb/kdd/p1474.pdf
- Internes Dokument belegt: BND und Bundeskanzleramt wussten von Wirtschaftsspionage der USA gegen Deutschland, 2015.
  https://netzpolitik.org/2015/internes-dokument-belegt-bnd-und-bundeskanzleramt-wussten-von-wirtschaftsspionage-der-usa-gegen-deutschland/
- So spionieren Geheimdienste deutsche Firmen aus/NSA Untersuchungsausschuss, 2017.
  https://www.welt.de/wirtschaft/article162217929/So-spionieren-Geheimdienste-deutsche-Firmen-aus.html

Ulrike Uhlig, Januar 2018