Materielle Gegenpraktiken zu Big Data

Widerständige Metaphern und Netzwerke

Isabel Paehr

Beitrag zur Veranstaltung »Big Data and Algorithms of Intersectionality: Grounding Critical Queer-Feminist Research in the Digital Age« der Sektion Frauen- und Geschlechterforschung

Einleitung: Mehr als (Un-)Sichtbarkeit

In meiner aktuellen Forschung beschäftige ich mich mit Praktiken und Metaphern von Aktivist*innen in digitalisierten Räumen. Obwohl Sichtbarkeitspolitiken zentral in queer feministischen Diskursen sind, vermeiden viele aktivistische Coder*innen die Begriffe Sichtbarkeit und Unsichtbarkeit. Sie gehen davon aus, dass ‚Auge' und ‚Kamera' bereits konzeptuell mit überwachenden Strukturen verknüpft sind – so zeigt zum Beispiel das Logo des Information Awareness Office ein Auge, das die Welt betrachtet, wobei das Bild auch als Auge gelesen werden könnte, das die Welt erzeugt.[1] Nicht nur das Erarbeiten widerständiger Netzwerke, sondern auch das Erfinden neuer Metaphern jenseits der Sichtbarkeit ist die Aufgabe von aktivistischen Coder*innen. Statt über Sichtbarkeit schreiben sie über Anonymität und Verbindungen, sowie über konkrete Handlungen wie Senden, Übertragen, Empfangen, Teilen, Verschlüsseln, Handshakes.

Als Programmiererin und künstlerisch Forschende interessieren mich die Bildlichkeiten und Metaphern, die aktivistische Coder*innen erfinden, um bestehende Big Data-Regimes zu entkräften. In meinem Vortrag auf der DSG Konferenz 2018 habe ich aktivistische Strategien gegen Big Data-Regimes vorgestellt und ihr queeres Potential untersucht. Dabei verstehe ich ‚queer' im Sinne Donna Haraways: Als das verunsichern „‚normaler' Kategorien" (Haraway 2008, S.25).

Die Blackbox künstlerisch befragen: Was ist Big Data?

Big Data Technologien werden eingesetzt, um große Datenmengen zu generieren, in ihnen Muster zu erkennen und quantitativ begründete Ergebnisse hervorzubringen. Typisch ist die Speicherung, Verarbeitung und Auswertung von massenhaft, auf den ersten Blick oft unwichtigen, Daten, die erst durch

[1] http://media.portland.indymedia.org/images/2005/12/331119.jpg

ihre algorithmische Verschränkung vermeintlich aussagekräftig werden. In Bezug auf Big Data-Algorithmen sprechen Theoretiker*innen und Programmierer*innen auch von ‚Black Boxes', da diese Algorithmen nicht *open source* und somit nicht öffentlich zugänglich sind. Beobachten lassen sich meist nur die Auswirkungen von Big Data, nicht die Prozesse des Datensammelns und Auswertens.

Im interdisziplinären Forschungsprojekt *Privacy Arena* der Universitäten Kassel und Tübingen entstand 2016 eine materielle Auseinandersetzung mit Big Data. Meine Gruppe aus visuell Forschenden, bestehend aus Mike Huntemann, Jörn Röder und mir, entwickelte einen spezifischen Big Data-Algorithmus, der die Metadaten von YouTube-Videos nach dem Begriff ‚Data' durchsucht und aus den YouTube-Videos kurze Sequenzen ausschneidet. Im Zusammenschnitt dieser Sequenzen ergibt sich ein Video, das durch die Aneinanderreihung der entkontextualisierten Schnipsel aussagelos erscheint. Interessant ist jedoch der Blick auf die dargestellten Räumlichkeiten, die Akteure (welche größtenteils hellhäutige Männer sind) und die Bildsprache der Videos. Prozess und Ergebnis zeigen Strukturen und Probleme von Big Data auf, in dem die Vorgehensweise von Big Data-Algorithmen programmatisch imitiert wird.

Video Still, 2016. Das Video kann auf https://vimeo.com/219681139 angesehen werden.

Wie strukturieren Big Data-Algorithmen Identitäten?

In ihrem Buch *Algorithms of Oppression* (2018, New York University Press) verbindet Safiya Umoja Noble ihre Kritik an heutigen Big Data Praktiken mit historischen, fortwirkenden Klassifizierungspraktiken von Bibliotheken, spezifisch der amerikanischen *Library of Congress* (Kongressbibliothek). Eines ihrer Beispiele ist der Protest von Studierenden der *Dartmouth University*, die 2014 forderten, dass die Library of Congress Begriffe wie ‚illegal aliens' nicht weiter als Klassifizierungskategorie nutzen solle. Noble zeigt auf, dass Klassifizierung auf dominanten, teils rassistischen Wissenspraktiken beruht. Sie fordert,

jene, die von den negativen Auswirkungen dieser Praktiken betroffen sind, in zukünftige Klassifizierungsentscheidungen einzubinden.

Big Data-Algorithmen beruhen nicht nur auf Identität als statisch, heteronormativ und rassifiziert, sondern strukturieren Identitäten nach diesen Parametern. Dies zeigt die Arbeit von Latanya Sweeney, die das *Data Privacy Lab* der *Harvard University* leitet. Sweeney hat in ihrer Studie *Discrimination in Online Ad Delivery* länderübergreifend 120.000 Google Ads untersucht und herausgefunden, dass Google-Ergebnisse für Namen, die mit dunkler Hautfarbe in Verbindung gebracht werden, mit Werbung für Kriminalregister und ‚background checks' verknüpft werden (2013, Communications of the ACM).

Konsequenzen von Big Data und algorithmischen Überwachungsstrukturen sind zum Beispiel angepasste Versicherungsbedingungen und -preise, angepasste Zulassungen für Arbeitsplätze und Visen, nach vermuteter Bonität zugeschnittene Preise, Zinsen und Darlehen, sowie kombiniert mit Geo-Blocking, Zugriff oder Zensur bestimmter Informationen. Dadurch entstehen algorithmische Filter-Bubbles, wobei ich die Metapher der Blase als zu ungenau und weich in Frage stelle, da die Strukturen, die Big Data-Algorithmen erzeugen, zu wahrnehmbaren Konsequenzen und konkreten Festschreibungen in den Kategorien Gender, Rassifizierung und Klasse führen.

Aktivistische Tools und neue Metaphern

Im Folgenden möchte ich einige aktivistische Tools vorstellen und dabei zeigen, welche Möglichkeiten es gibt, sich Big Data-Regimes gegenüber widerständig zu verhalten. Ich stelle drei materielle Praktiken und ihre Strategien vor.

Cryptocat bietet überwachungsfreie Räume an

Cryptocat ist ein Chat-Programm, das verschlüsselte Kommunikation ermöglicht. Hierbei werden Nachrichten verschlüsselt, bevor sie die Endgeräte der Kommunizierenden verlassen, so dass auch Internetanbieter keine Einsicht in die Kommunikation haben. In *Cryptocat* ist sowohl die Privatheit der Kommunikation gewährleistet, als auch die Integrität der Kommunizierenden und der Nachricht. Diese Strategie entzieht die IP-Adressen und Namen der Kommunizierenden sowie ihre Nachrichten der sonst überwiegend überwachten Online-Kommunikation und somit auch Big Data-Algorithmen.

Auf der Website https://crypto.cat beschreiben der Entwickler Nadim Kobeissi und das Team aus Coder*innen, die das open-source-Projekt weiterentwickeln, das Projekt in ähnlicher Weise, in der der rebellische Hauself Dobby seinem Freund Harry Potter den Raum der Wünsche präsentiert. Sie schreiben: „[…] the project's goal has been to provide easy, fun and private chat to anyone in the world who cares to ask for it, regardless of any technical background" (2018, https://crypto.cat). Dobby beschreibt den Raum der Wünsche als Raum „[…] that a person can only enter when they have real need of it. Sometimes it is there, and sometimes it is not, but when it appears, it is always equipped for the seeker's needs" (Dobby in Harry Potter 5).

Nachtrag: Im Februar 2019 kündigte Nadim Kobeissi an, Cryptopcat einzustellen.

Domain Fronting heißt: Identitäten fälschen

Das Paper *Blocking-resistant communication through domain fronting* (Fifield et al. 2015) erörtert, wie Coder*innen Zensur entgehen können, indem sie so tun, als würden sie mit einem erlaubten Anbieter kommunizieren, während sie tatsächlich nur unter dem Decknamen des erlaubten Anbieters einen

unerlaubten – das heißt: zensierten – Anbieter nutzen. Die dafür genutzte Technik heißt *Domain Fronting*.

Der Messenger *Signal* bietet Android und iOS Nutzer*innen Ende-zu-Ende verschlüsselte Kommunikation an. Erfunden wurde Signal von *Open Whisper Systems*, was übersetzt offenes Flüstersystem bedeutet. Damit adressiert Signal nicht Sichtbarkeit, sondern leises Sprechen und aufmerksames Zuhören. Das Protokoll *Signal Protocol* ist open source, demnach ist der dem Programm zugrunde liegende Code einsehbar und nutzbar. Weil Signal *TSL-Handshakes* nutzt, die Signal's Hostnamen in Klartext im Header tragen, ist es Internetanbietern prinzipiell möglich, Signal zu erkennen und den Zugriff auf den Messenger zu blockieren. Signal praktiziert(e) Domain fronting, um ihren Dienst in Ägypten, Oman, Qatar und den Emiraten anbieten zu können. Das heißt, dass sich Signal als jemand anderes ausgeben musste, um in diesen Ländern erreichbar zu sein. Open Whisper Systems nutzte zuerst die *Google App Engine* zum Vortäuschen von falscher Identitäten, und später Amazons *Cloudfront*. Die entsprechenden Länder hätten Google und später Amazon blockieren müssen, um Signal zu blockieren. Amazon geht allerdings aktuell gegen Signal vor, um Domain Fronting zu verbieten.

Onion Routing zum Signifikanten tauschen und Noise erzeugen

Das Symbol von *Tor*, einem weltweiten Netzwerk, ist die Zwiebel. Tor implementiert Verschlüsselung in verschiedenen Ebenen, die wie die Schichten einer Zwiebel funktionieren. An dieser Metapher ist außerdem schön, dass wer eine Zwiebel zerschneidet, tränende Augen bekommt. Eine Taktik zur Gewährleistung von Anonymität ist hier das systematische Verketten von Geräten und deren IP-Adressen. Im Tor-Netzwerk fungiert jedes kommunizierende Gerät als ein *Node*, also Knotenpunkt. Wenn einzelne User*innen zum Beispiel eine Website aufrufen wollen, geht ihre Anfrage durch viele andere Knotenpunkte, die jeweils nur den vorherigen und den nächsten Node kennen. Welches Gerät die entsprechende Website angefragt hat, ist durch die anonyme, verschlüsselte Aneinanderreihung der teilnehmenden Nodes nicht mehr feststellbar. Dieses *Layering* von Verschlüsselung macht das Netzwerk nicht-diskriminierend, da Teilnehmer*innen anonymen Anderen Zugang ermöglichen. Das Netzwerk wird sicherer, je größer es wird.

Wahrnehmungsdimensionen verschieben

Aktivist*innen flüstern und hören zu, sie schicken, empfangen und codieren Signale und sie tauschen IPs. Sie wählen ihre (Un-)Sichtbarkeiten und implementieren Praktiken, die Wahrnehmungsdimensionen verschieben und anonyme Verbindungen generieren. Die vorgestellten Technologien und Tools erlauben es User*innen, sich den Reglementierungsmechanismen von Big Data-Regimes zu entziehen. Durch das Nutzen von falschen Signifikanten (IPs), oder durch das Ausleihen der Signifikanten anderer User*innen, ‚verunreinigen' sie Datensätze. Diese fortlaufenden Entwicklungen und Performances bedrohen Big Data-gestützte Regierungsformen und verunmöglichen im Idealfall die durch Daten gerechtfertigte Kriminalisierung von spezifischen Akteuren und Menschengruppen. Personen, die so kommunizieren, wissen, dass ihre Technologien öffentlich kriminalisiert werden, zum Beispiel ist eine Abkehr von dem indexierten *World Wide Web* in Form des *Dark Net* mit Illegalität konnotiert. Bekannte Programmierer*innen und *Whistleblower*, die die genannten Technologien mitentwickelt haben, werden in einigen Staaten wie zum Beispiel den USA verfolgt.

Verschränkung von menschlichen Körpern und digitalen Performances

Die von Begehren nach Kontrolle und Linearität gesteuerte Massenüberwachung, aus der sich Big Data speist und die durch Big Data-Algorithmen verstärkt wird, nimmt zu. Besorgniserregend sind versuchte Gleichschaltungen von menschlichen Körpern und ihren digitalen Performances: Verifizierungs- und Identifizierungsprozesse werden ohne das Wissen und die Zustimmung von Bürger*innen mit Fingerabdrucks- und Gesichtserkennungssoftware verzahnt.

Ein aktuelles Beispiel ist der Zugriff der Firma IBM auf Überwachungskamera-Aufnahmen aus Manhattan. Im Auftrag der New Yorker Polizei entwickelte IBM Analyse-Software für Videoaufnahmen. Laut dem Onlinemagazin *The Intercept* nutzte IBM das Videomaterial bis 2016, um Algorithmen zu trainieren, in Videobildern nach Menschen mit zum Beispiel spezifischen Hautfarben zu suchen. Das NYPD gibt an, die Hautfarben-Analyse nicht genutzt zu haben. Da jegliche Analysemethoden der Öffentlichkeit nicht bekannt waren, hatten Menschen, die aufgrund von Analysen angehalten oder verhaftet wurden, nicht die Möglichkeit, den Grund ihrer Verhaftung nachzuvollziehen.

Setzen staatliche Exekutivorgane außerdem Big Data-basierte Prognosetechnologien wie *Precops* ein, um automatisiert (Wiederholungs-)Verbrechen für spezifische Regionen und Communities zu prognostizieren, werden unrechtmäßige Verurteilungen wahrscheinlich. Obwohl gerade die Blindheit von Algorithmen in Onlineräumen zum Ausgangspunkt für widerständige Praktiken wird, ist die Blindheit von Algorithmen in Räumen, die Körperlichkeit erfordern, Ausgangspunkt für Big Data-gestützte Diskriminierung.

Möglichkeiten für Körper, widerständig zu agieren

Widerständig handeln heißt, den Kreislauf zu unterbrechen, in dem digitale Performance und Körperlichkeit verschränkt werden, das entstehende Datenbild anhand heteronormativer und rassifizierter Parameter analysiert wird und die Ergebnisse als Konsequenzen zu einzelnen Menschen zurückgespielt werden. Während die vorgestellten Online-Praktiken in Deutschland oft nur verbal kriminalisiert werden, sind manche der denkbaren Praktiken in städtischen Räumen tatsächlich illegal und strafbar, wie zum Beispiel Vermummung im öffentlichen Raum oder das Zerstören von Überwachungsstrukturen. Queere Strategien sind relevant, um Körper von Signifikanten zu lösen und Körper als flexible Materialien zu begreifen. Können Körper sich, durch die online von aktivistischen Coder*innen erprobten Praktiken, als intelligente Materialien von soziokulturellen Zuschreibungen und algorithmischen Projektionen emanzipieren? Digitale Performances wo möglich von der eigenen Körperlichkeit unabhängig zu machen, schützt auch User*innen, die in prekäreren Datensituationen sind. Ich schlage vor, die zuvor analysierten Strategien auf körperliche Dimensionen zu erweitern:

Kommunikation schützen und überwachungsfreie Räume anbieten

- Stadtkarten herstellen, die Überwachungspunkte in der Stadt dokumentieren
- Kameras zukleben
- Crypto-Parties machen und gemeinsam über Verschlüsselung lernen
- Tor und andere Tools in Bibliotheken und Universitäten installieren, um anderen Zugriff auf anonymisierte Kommunikation zu ermöglichen

- Auf datensichere Räume bestehen, zum Beispiel Smartphones und/oder Kameras und/oder Audioaufnahmen einschränken

Identitäten fälschen

- mit den Kreditkarten anderer bezahlen, Payback-Karten tauschen, in kommerziellen Kontexten bei Kontaktformularen die Adressen großer Unternehmen angeben

Signifikanten tauschen und Noise erzeugen

- Router im öffentlichen Raum mit Pseudoinformationen füttern, künstlerische Strategien erfinden
- Eigene und unabhängige Netzwerke bauen und nutzen
- Masken und Schminke nutzen und weiterentwickeln, die Gesichtserkennungssoftware nicht lesen kann

Zach Blas hat den *Facial Weaponization Suite* entwickelt, der vor biometrischer Erfassung durch Kameras schützt. In Workshops entwickelt er mit den Teilnehmer*innen kollektive Masken, die sich aus den biometrischen Daten der Teilnehmenden zusammensetzen.

Zusammen mit Jasper Meiners habe ich die Webcamera Obscura 3D-gedruckt, die als Aufsatz für Webcams genutzt werden kann und performativ potentielle Überwacher*innen durch eine Toilette gucken lässt. Unsere Forderung ist, sich nicht zu verstecken, sondern Kontrolle über das eigene überwachte Abbild zurückzuerlangen.

Literatur

Blas, Zach. Escaping the face: Biometric facial recognition and the facial weaponization suite. *Journal of the New Media Caucus* 9(2). ISSN 1942-017X.

Cryptocat. https://crypto.cat (Zugegriffen: 09.09.2018)

Fifield, D., C. Lan, R. Hynes, P. Wegmann und V. Paxson. 2015. Blocking-resistant communication through domain fronting. *Proceedings on Privacy Enhancing Technologies* 2015 (2):1–19.

Haraway, Donna. 2008. Companion species, mis-recognition, and queer worlding. In *Queering the non/human*, Hrsg. Noreen Giffney und Myra J. Hird, xxiii–xxvi. Aldershot: Ashgate Publishing.

Huntemann, Röder, und Isabel Paehr. 2016. DataDataData. Video in der Ausstellung *Privacy Arena*. Interim Kassel.

Meiners, Jasper und Isabel Paehr. 2016. Webcamera Obscura. In *The 3D Addivist Cookbook*, Hrsg. Morehshin Allahyari und Daniel Rourke, http://www.morehshin.com/3d_additivist_cookbook/.

Noble, Safiya Umoja. 2018. *Algorithms of oppression: How search engines reinforce racism.* New York: NYU Press.

Signal. https://signal.org/blog/looking-back-on-the-front/ (Zugegriffen: 09.09.2018)

Sweeney L. Discrimination in Online Ad Delivery. *Communications of the ACM* 56(5):44–54.