Gruppe 1: Targeting and personalized Environment

"[F]iltering has been used to show higher-paying job ads to men more often than to women, to charge more for standardized test prep[aration] courses to people in areas with a high density of Asian residents, and many other forms of coded inequity. [...] While the gender wage gap and the "race tax" (non-Whites being charged more for the same services) are nothing new, the difference is that coded inequity makes discrimination easier, faster, and even harder to challenge, because there is not just a racist boss, banker, or shopkeeper to report. Instead, the public must hold accountable the very platforms and programmers that legally and often invisibly facilitate the [autonomic reproduction of discrimination], even as we reckon with our desire for more "diversity and inclusion" online and offline."

Ruha, Benjamin (2019): Race After Technology: Abolitionist Tools for the New Jim Code, 25.

Impulsfragen:

- Welche Gefahren entstehen durch die Intransparenz/ Verborgenheit von personalisierter Werbung?
- Der 3. Artikel des Grundgesetzes gebietet eine Gleichberechtigung von Menschen. Inwieweit ist Durchsetzung des Gesetz gegenüber Targeting erschwert?
- Sind personalisierte Inhalte demokratiegefährdent und fördern Polarisierung?
- Kennt ihr weitere Beispiel?
- Wie sollte Targeting eingeschränkt werden?

Gruppe 2: Targeting and personalized Environment

Donald Trumps Wahlkampf stützte sich unter anderem auf detaillierte Persönlichkeitsprofile von mehr als 87 Millionen Facebook-Nutzern. Dank investigativer Recherchen [kam] ans Licht, wie die verantwortliche Firma Cambridge Analytica an die Daten kam und wie sie arbeitete. [...] Zentral [war] die App eines Drittanbieters, mit der Facebook-Nutzer einen Persönlichkeitstest machen konnten. Die Anwendung „thisisyourdigitallife" [,unter wissenschaftlicher Begleitung von Aleksandr Kogan, Assitenzprofessor am Lehrstuhl für Psychologie der Universität Cambridge,] sammelte allerdings nicht nur Informationen über die etwa 270.000 Menschen, die sie bewusst genutzt haben, sondern auch über deren Facebook-Kontakte. [...] Dass die persönlichen Daten von Millionen Facebook-Nutzern ohne ihr Wissen bei einer Firma landen, die ihr Leben analysiert, psychologische Profile erstellt und für den Wahlkampf einsetzt, war für viele nicht vorstellbar. Dabei ist dies das logische Produkt [...] der Big-Data-Branche. Die Rede vom Datenleck ist deshalb irreführend. Sie lenkt davon ab, dass Facebook selbst das System geschaffen hat, in dem die Daten von Millionen Menschen ohne ihre Einwilligung bei anderen Firmen landen. Das Werbeunternehmen [Facebook] wusste seit 2015 davon, dass Kogan [wissenschaftlicher Begleitung von „thisisyourdigitallife"] seine Daten über Millionen Facebook-Nutzer an Cambridge Analytica [weiterverkauft] hat. Zwar sperrte es damals wohl den Zugang von Kogans Firma GSR und forderte Cambridge Analytica [...] auf, die unrechtmäßig erlangten Daten zu löschen – eine Überprüfung, ob dies geschehen ist, erfolgte jedoch nicht. [...] Facebook unterließ es zudem, betroffene Nutzer darüber zu informieren, dass Dritte illegal an ihre Daten gelangt waren. [...] Facebook profitierte massiv von den vielen Drittanbieter-Apps: 30 Prozent jedes In-App-Kaufes mussten diese an die Plattform abführen, dafür gewährte Facebook den Programmierern unkontrollierte Freiheit. [...] [Das Erstenn von] Persönlichkeitsprofile[n] wurden den Berichten zufolge eingesetzt, um die Botschaften der Trump-Kampagne im US-Wahlkampf auf möglichst kleine Zielgruppen zuzuspitzen. Dass diese Technik des sogenannten Microtargeting sowohl online als auch offline (nicht nur in diesem) US-Wahlkampf eingesetzt wurde, war grundsätzlich bereits bekannt. So berichtete das Schweizer Magazin 2016, dass Trumps Freiwillige im Haustürwahlkampf über eine App möglichst genaue Informationen über die von ihnen besuchten potenziellen WählerInnen und auf 32 Persönlichkeitstypen zugeschnittene Gesprächsleitfäden bekommen hätten. [...] Whistleblower Christopher Wylie beschreibt nun ergänzend, dass Cambridge Analytica ein ganzes Informationsökosystem von Webseiten und Blogs aufgesetzt habe, die nicht als Teil der Trump-Kampagne erkennbar waren. Sie seien genutzt worden, um Wähler gezielt mit vermeintlich unabhängigen Informationen zu versorgen, für die sie laut ihrem Profil besonders ansprechbar sind. So seien Wähler immer genau mit den Forderungen und Versprechen Trumps bespielt worden, die bei ihnen die größte Wirkung erzielen würden. Wiley selbst bezeichnet das von ihm mitentwickelte System inzwischen als „Werkzeug der psychologischen Kriegsführung". Cambridge Analytica hat diese Methoden nachweislich auch in anderen Wahlkämpfen eingesetzt, vor allem in der Karibik und Afrika. So prahlten Verantwortliche vor versteckter Kamera damit, für „jedes Element" der (erfolgreichen) Kampagnen des kenianischen Präsidenten Uhuru Kenyatta 2013 und 2017 verantwortlich zu sein. Auch in der Pro-Brexit-Werbung hat die Firma mitgemischt.

Dachwitz, Ingo; Rudl, Tomas, Rebiger, Simon (2018): Was wir über den Skandal um Facebook und Cambridge Analytica wissen [UPDATE], in: netzpolitik.org, 21.03.2018.

Impulsfragen:

- Welche Gefahren entstehen durch die Intransparenz/ Verborgenheit von personalisierter Werbung?
- Der 3. Artikel des Grundgesetzes gebietet eine Gleichberechtigung von Menschen. Inwieweit ist Durchsetzung des Gesetz gegenüber Targeting erschwert?
- Sind personalisierte Inhalte demokratiegefährdent und fördern Polarisierung?
- Kennt ihr weitere Beispiel?
- Wie sollte Targeting eingeschränkt werden?

Gruppe 3: Data Sharing + DataFusion

Data Science with Whose Interests and Goals?

Far too often, the problem is not that data about minoritized groups are missing but the reverse: the databases and data systems of powerful institutions are built on the excessive surveillance of minoritized groups. This results in women, people of color, and poor people, among others, being overrepresented in the data that these systems are premised upon. In Automating Inequality, for example, Virginia Eubanks tells the story of the Allegheny County Office of Children, Youth, and Families in western Pennsylvania, which employs an algorithmic model to predict the risk of child abuse in any particular home. The goal of the model is to remove children from potentially abusive households before it happens; this would appear to be a very worthy goal. As Eubanks shows, however, inequities result. For wealthier parents, who can more easily access private health care and mental health services, there is simply not that much data to pull into the model. For poor parents, who more often rely on public resources, the system scoops up records from child welfare services, drug and alcohol treatment programs, mental health services, Medicaid histories, and more. Because there are far more data about poor parents, they are *oversampled* in the model, and so their children are overtargeted as being at risk for child abuse—a risk that results in children being removed from their families and homes. Eubanks argues that the model "confuse[s] parenting while poor with poor parenting." This model, like many, was designed under two flawed assumptions: (1) that more data is always better and (2) that the data are a neutral input. [...] [D]ata are never neutral; they are always the biased output of unequal social, historical, and economic conditions[.] So this raises our next who question: Whose goals are prioritized in data science (and whose are not)? In this case, the state of Pennsylvania prioritized its bureaucratic goal of efficiency, which is an oft-cited reason for coming up with a technical solution to a social and political dilemma. Viewed from the perspective of the state, there were simply not enough employees to handle all of the potential child abuse cases, so it needed a mechanism for efficiently deploying limited staff—or so the reasoning goes. This is what Eubanks has described as a *scarcity bias*: the idea that there are not enough resources for everyone so we should think small and allow technology to fill the gaps. Such thinking, and the technological "solutions" that result, often meet the goals of their creators—in this case, the Allegheny County Office of Children, Youth, and Families—but not the goals of the children and families that it purports to serve.

D'Ignazio, Catherine und Klein, Laure. Data Feminism. 2020. Data Feminism. Einführung und Kapitel 1.

Impulsfragen:

- Welche Gefahren und welche Vorteile entstehen aus Data Sharing und Data fusion?
- Wie werden Menschen berücksichtigt, die von einem Machtungleichgewicht benachteiligt werden?
- Welche gesellschaftlichen Gruppen profitieren von Data sharing und Data fusion?
- Wie können Data sharing und Data fusion für aktivistische Zwecke genutzt werden, welche Vorteile für Gleichbehandlungs Initiativen ergeben sich?

Gruppe 3: Data Sharing + DataFusion

“Data sharing” ist nicht neu. Einzelpersonen, Organisationen und Regierungen haben seit der Existenz von Computern und Netzwerken Daten ausgetauscht. In den letzten zehn Jahren haben Fortschritte in digitaler Kompetenz, Technologie und Anpassung der rechtlichen Rahmenbedingungen schnelleren datenaustausch ermöglicht in einem noch nie dagewesenem Umfang. Die Data sharing Beispiele, die wir auf SCDS sammeln demonstrieren diesen Wandel. JoinData, beispielsweise unterstützt die nachhaltige Innovation in der niederländischen Landwirtschaft, indem Landwirte in die Lage versetzt werden, ihre Daten schnell, einfach und sicher zu teilen. Drei Faktoren haben das Spektrum der Möglichkeiten für den Informationsaustausch dramatisch verändert:
Der erste Faktor ist die verbesserte Verfügbarkeit und Qualität der Daten und die einfachere und günstigere Art und Weise sie zu speichern, zu verarbeiten und zu teilen.
Der zweite Faktor ist der Kulturwandel: Heute verstehen wir die Daten besser, wir sind bereit, sie als Ressource zu betrachten und in diese zu investieren – dies gilt für Regierungen, private Organisationen und Einzelpersonen gleichermaßen.
Der dritte Faktor ist die Einbeziehung von politischen Entscheidungsträgern, die die Auswirkungen der Digitalisierung für Bürger besser verstehen als in der Vergangenheit, und entschlossen sind, diesem Bereich zu regulieren. Das Bewusstsein für die Chancen und Risiken einer gemeinsamen Nutzung von Daten ist ein wesentlicher Bestandteil dieses Prozesses.
Regulierung bedeutet nicht unbedingt eine Einschränkung – z. B. den Schutz personenbezogener Daten –, sondern auch die Stärkung der Interessenträger, um ihre Chancen besser zu nutzen, indem ein Rahmen geschaffen wird, der definiert was legal ist und was nicht.
Diese drei Faktoren zu kombinieren schafft enorme Chancen:
Organisationen und Behörden können mehr Daten untereinander austauschen auf sichere, faire und rechtmäßige Weise und unter Wahrung der Rechte derer, die die Daten betreffen.
Die Kombination von Daten aus verschiedenen Quellen kann die Leistung und den Wert von Diensten und Serviceangeboten um ein Vielfaches steigern. Es ermöglicht bessere Forschung und Entwicklung sowie die Herstellung und Distribution besserer Produkte.
Der Austausch von Daten ermöglicht beispiellose Zusammenarbeit, datengesteuerte Entscheidungsfindung und Politikgestaltung und eine Verstärkung der sozialen Wirkung.
Obwohl es derzeit nur wenige Studien gibt, die den potenziellen Nutzen einer gemeinsamen Nutzung von Daten untersucht und quantifiziert haben, ist es nicht nur intuitiv, dass die optimale Nutzung dieser Möglichkeiten von entscheidender Bedeutung ist. Es ist der Ehrgeiz des SCDS(Support Centre for Data Sharing), Sie bei dieser Entdeckung zu unterstützen.

[Das Support Centre for Data Sharing beschreibt hier Data sharing, das SCDS wurde von der Europäischen Komission 2019 im Kontext eines besseren europäischen Binnenmarktes ins Leben gerufen.]

Impulsfragen:

- Welche Gefahren und welche Vorteile entstehen aus Data Sharing und Data fusion?
- Wie werden Menschen berücksichtigt, die von einem Machtungleichgewicht benachteiligt werden?
- Welche gesellschaftlichen Gruppen profitieren von Data sharing und Data fusion?
- Wie können Data sharing und Data fusion für aktivistische Zwecke genutzt werden, welche Vorteile für Gleichbehandlungs Initiativen ergeben sich?

Gruppe 5: Data Bias/ Reproduktion + privilege hazard

“When sexism, racism, and other forms of oppression are publicly unmasked, it is almost never surprising to those who experience them.”

Joy Buolamwini, a Ghanaian-American graduate student at MIT, was working on a class project using facial-analysis software. But there was a problem—the software couldn’t “see” Buolamwini’s dark-skinned face (where “seeing” means that it detected a face in the image, like when a phone camera draws a square around a person’s face in the frame). It had no problem seeing her lighter-skinned collaborators. She tried drawing a face on her hand and putting it in front of the camera; it detected that. Finally, Buolamwini put on a white mask, essentially going in “whiteface” (figure 1.3). The system detected the mask’s facial features perfectly.

Digging deeper into the code and benchmarking data behind these systems, Buolamwini discovered that the dataset on which many of facial-recognition algorithms are tested contains 78 percent male faces and 84 percent white faces. When she did an intersectional breakdown of another test dataset—looking at gender and skin type together—only 4 percent of the faces in that dataset were women and dark-skinned. In their evaluation of three commercial systems, Buolamwini and computer scientist Timnit Gebru showed that darker-skinned women were up to forty-four times more likely to be misclassified than lighter-skinned males. It’s no wonder that the software failed to detect Buolamwini’s face: both the training data and the benchmarking data relegate women of color to a tiny fraction of the overall dataset.

Buolamwini’s work has been widely covered by the national media in articles that typically contain a hint of shock. This is a testament to the social, political, and technical importance of the work, as well as to how those in positions of power—not just in the field of data science, but in the mainstream media, in elected government, and at the heads of corporations—are so often surprised to learn that their “intelligent technologies” are not so intelligent after all.

D’Ignazio, Catherine und Klein, Laure. Data Feminism. 2020. Data Feminism. Einführung und Kapitel 1.

Impulsfragen:

- Welche Gefahren kann Data Bias bergen?
- Welche Umstände führen zum Bias?
- Welchen Gruppen nützt ein Data Bias, welchen nicht?
- Welche Gruppen können Biases aufdecken?
- Welche Regeln/Initiativen/Taten können verhindern, dass ein Bias sich durchsetzt?

Gruppe 6: Data Bias/ Reproduktion + privilege hazard

Overall, though cognitive biases can negatively impact people in various ways, they can also be beneficial in some cases. This is true both on an individual scale, such as when biases encourage people to prepare for the future, and on a group scale, such as when biases encourage cooperation. Accordingly, from an evolutionary perspective, cognitive biases are sometimes viewed as adaptive *features* rather than maladaptive *flaws*. Because of this, it's important to understand that cognitive biases can sometimes help you to make optimal decisions, even if they distort your view of the situation. At the same time, however, it's still important to be aware of them, so that you can understand how they affect you, and determine whether you will benefit from reducing their influence. State of AI Bias by DataRobot revealed that companies with biased algorithms experienced harmful consequences. Data bias in artificial intelligence (AI) and machine learning (ML) is an error that occurs when specific data points in a dataset are over or underrepresented. As the input data is skewed, you get errors in the output.

Machine learning models trained on biased data inaccurately represent the desired use cases. As a result, the quality, accuracy, and reliability for analysis are low.

The most common AI data bias types are the following:

- Social or systemic biases that discriminate against the specific group(s).
- Data sampling that over- or underrepresents specific groups.
- The cognitive biases of a data scientist, analyst, or researcher.
- In the field of data science, bias is perpetuated by the wrong methods of data analysis, data collection, clearing and formatting.
- Implicit biases representing attitudes and stereotypes we hold about others, even when we are unaware of it.

The concern around data bias is growing. DataRobot conducted a survey on 350 U.S. and U.K.-based technology leaders, including CIOs, IT directors, IT managers, data scientists, and development leads, who use or plan to use AI.

According to the survey analysis, 54% of technology leaders say they are very or extremely concerned about AI bias. It's 12% more than in 2019 (42% shared such a sentiment). At the same time, the overwhelming majority (81%) are calling for more AI regulation. So, the main concerns around bias in AI are fear of losing customer trust, reputation, and exposure to detailed compliance checks.Out of 350 organizations surveyed, 36% (126 organizations) said their organization suffered from biased data in one or several of their algorithms.
For example, the Consumer Federation of America states that in Oregon, women will be charged more for their car insurance. It's on average $976.05 annually for basic coverage, while men will be quoted a premium of $876.20. With everything else being equal it's a $100 gap or 11.4% gender penalty. This AI bias can easily lead to loss of customers' trust and, as a consequence, the revenue. Every client who is outraged by the inequality might find a fairer insurance company.

(Statice -"The impact of data bias on your business & the benefits of fair AI")

Impulsfragen:

- Welche Gefahren kann Data Bias bergen?
- Welche Umstände führen zum Bias?
- Welchen Gruppen nützt ein Data Bias, welchen nicht?
- Welche Gruppen können Biases aufdecken?
- Welche Regeln/Initiativen/Taten können verhindern, dass ein Bias sich durchsetzt?