Trustable Technology: *Vertrauensbildung im digitalen & analogen Kontext*

Ein Bericht des Center for the Cultivation of Technology, vorgelegt von Julia Kloiber & Zara Rahman

Intro

> ***"Trust is an optimistic attitude that someone holds toward a person in a situation of uncertainty that said person is equipped with the capacity for judgement."***[1]
>
> *"Was ist das Verhältnis zwischen Vertrauen und Technologie? Könnte man Vertrauen selbst als soziale und politische Technologie verstehen? Schließlich macht erst eine Verarbeitung durch internalisierte Prüfmechanismen Risiken und Unsicherheiten (vordergründig) beherrschbar. Einfach ausgedrückt beschreibt Vertrauen rekursive Prozesse von Einordnung und Wahrscheinlichkeit. Auf der technischen Ebene wäre das Gegenstück ein Protokoll, das definiert, wie genau Prozesse und Vorgänge ablaufen.*
> *Wie verhalten sich diese beiden Formen zueinander in ihrer Fähigkeit, Regelmäßigkeit aufzubauen, Vertrauensvorschüsse zu gewähren und die Welt zu gestalten?"*[2]

Gesellschaften und ihr globaler Kontext werden immer komplexer. Gleichzeitig werden immer weitere Bereiche unseres Alltags und des gesellschaftlichen Zusammenlebens von Technologien durchdrungen.

Diese Situationen bieten Chancen wie auch Herausforderungen:
Wenn Vertrauen im Allgemeinen die Grundlage für die Konstitution sozialer Interaktion ist, die die Entwicklung von Gemeinschaften ermöglicht, wie genau kann dann der (technologische) Zustand dieser Vertrauensbeziehungen erfasst werden?[3]
Und wie kann man etwas Vertrauen, dass zum Großteil unsichtbar ist und aus abstrakten Bits und Bytes besteht?

Hanna Ahrendt schreibt in "The Human Condition/Vita activa" zum politischen Handeln: "*Menschen sind ausschließlich in der Lage, gemeinsam zu handeln. Handlungen liegen zwischen Menschen insofern, als eine Person zwar einen Akt beginnen kann, aber nicht in der Lage ist, allein seine Folgen zu kontrollieren. (...) Wann immer wir wirklich handeln,(...)*

---

[1] vgl.Loh, siehe Fußnote 3
[2] #Vertrauen und Technik
[3] Aufschlussreich hierzu auch: Trust & Technology: Dr. Janina Loh in: https://philtech.univie.ac.at/fileadmin/user_upload/p_philtech/HIIG__Schildhauer___Pernice__2017__-_IoT___Trust.pdf

sind der Verlauf und die Ergebnisse unvorhersehbar und unumkehrbar. Es gibt kein definiertes Ende oder Ergebnis einer Handlung, da Handlungen nicht isoliert betrachtet werden können. (...)Eine Handlung führt zu weiteren Handlungen. Am wichtigsten ist, dass wahres Handeln mit der proaktiven Beurteilung einer Situation verbunden ist. Ohne diese kann man nicht agieren".

Vertrauen ist also ein Zwischenkonzept, da es in Kontexten, in denen umfassendes Wissen vorhanden ist, nicht benötigt wird und in Situationen, in denen es überhaupt keine Informationen gibt, nicht möglich ist. Vertrauen ist deshalb auch ein wichtiges Element in Innovationskontexten[4]: Innovation bedeutet qua Definition, etwas Neues zu versuchen. Wenn man diesen Prozess beginnt, ist sich niemand des Ergebnisses sicher.
Um das auszuhalten, braucht es Grundvertrauen.

Es besteht ein Unterschied zwischen gerechtfertigten Erwartungen aufgrund von Wissen über Rollen, Regeln und (Natur-)Gesetze auf der einen Seite und echtem Vertrauen aufgrund der Summe der Urteilsfähigkeit, die diese Rollen, Regeln und Gesetze interpretiert, auf der anderen Seite.
Allgemein vertrauen wir nur Menschen und nicht Dingen.
Was bedeutet es für die Gesellschaft, Vertrauen (auch) in technischen Architekturen und Infrastrukturen abzubilden?

Medien als Vermittler von Weltgeschehen, Transparenz garantierende Institutionen, Bürgertechnologien, die Diskussion um Blockchains oder kybernetisch organsierte Kontrolle – Vertrauen ist, so unsere Ausgangsüberlegung, ein basaler Aspekt der Technik und technologischen Entwicklung.

Der vorgeschlagene Themenschwerpunkt beschäftigt sich daher mit Vertrauen in und mittels digitale(r) Technologie.
Damit, welche Rolle Vertrauen in der Interaktion von Gesellschaft und Technologie spielt und welche Maßnahmen und Prinzipien sich positiv auf Vertrauensbildung im digitalen, aber auch analogen Raum auswirken können.

In der analogen Welt haben wir u.a. Gesetze (wie z.B. Regelungen zum Verbraucherschutz) und Protokolle (wie z.B. ingenieurtechnische Prüfverfahren) eingeführt, um uns vor unintendierten Auswirkungen (nicht nur) von Technologien zu schützen.

Wie sähe oder sieht hierfür eine digitale Entsprechung aus? Müssen und wollen wir uns auch hier neue Regeln geben, um die digitale Infrastruktur unserer Gesellschaft weiter für **Deliberation, Information und Kommunikation** nutzen zu können?
In welchen Gebieten und zu welchem Preis bieten Technologien Potenziale für erweiterte gesellschaftliche Teilhabe?

[4] i.a.: "Who can you trust?", Rachel Botsman:
https://decolonizedlibrarian.wordpress.com/2018/01/29/book-review-who-can-you-trust/

Aktueller Bezug des Themenschwerpunkts

In Zeiten von Datenskandalen und digitaler Überwachung sind diese sozio-technischen Fragen spannender denn je. Der “digitale” Kontrollverlust wirkt sich auch in die analoge Welt und ihre Institutionen aus. Reports haben gezeigt: Das Vertrauen in Institutionen, eine wichtige Metrik auf dem Radar des gesellschaftlichen Zusammenhalts, schwindet aktuell.[5]

In den letzten Jahren und Monaten wurde das Vertrauen von Nutzer*innen auch durch viele Skandale im Technologiebereich erschüttert. Kaum ein Unternehmen blieb davon ausgenommen.
Oft hatten diese Vertrauensbrüche damit zu tun, dass Nutzerdaten technisch nicht ausreichend gesichert wurden – oder ganz aktiv das Design von Technologien ausgenutzt wurde[6], um undeklariert an große Mengen von Informationen zu gelangen oder Fehlinformationen zu streuen.
So war z.B. das soziale Netzwerk Facebook in eine Vielzahl an Datenskandalen[7] verwickelt, anderenorts wurden durch mangelnde Sicherheitsvorkehrungen E-Mail-Adressen und Passwörter[8] gestohlen oder Sicherheitslücken in kritischer Hardware wie Routern gefunden.[9]

Zusätzlich wird Technologie mit neuen Entwicklungen wie zum Beispiel im Bereich der künstlichen Intelligenz oder dem maschinellem Lernen immer mehr zur Blackbox (wie in Runde 5 thematisiert). Selbst Entwickler*innen fällt es schwer, komplexe Systeme zu durchblicken und deren Entscheidungen nachvollziehen zu können.

Und trotz der negativen Schlagzeilen: Während Technologie all diese problematischen Potenziale inherent innewohnen, bietet sie gleichzeitig auch Lösungsansätze: Im Daten- und Investigativjournalismus und Civic & Governance Tech ist sie zu einem Werkzeug geworden, ohne das Teilhabe und Transparenz kaum mehr möglich wäre.

Erhöhte gesellschaftliche und Informations-Komplexität aber auch die Chance, Daten anders auswerten zu können: Was bedeutet Vertrauen im digitalen Kontext?

Angst-Szenarien und berechtigte Sorgen vor Missbrauch neuer Technologien (KI, Überwachung, etc.) erfordern starkes Vertrauen. Wie kann dies gebildet werden?

[5]https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/Gesellschaftlicher_Zusammenhalt/ST-LW_Studie_Schwindendes_Vertrauen_in_Politik_und_Parteien_2019.pdf
[6] https://shiba.computer/essay/on-weaponised-design/
[7] https://www.wired.com/story/facebook-scandals-2018/
[8] https://www.cnet.com/news/massive-breach-leaks-773-million-emails-21-million-passwords/
[9] https://www.nytimes.com/2019/05/21/opinion/internet-security.html

Ein kürzlich erschienener Bericht des Weltwirtschaftsforums[10] bietet einen guten Rahmen, um differenziert über Vertrauen als Akt sprechen zu können. In dem Bericht wird zwei Arten von Vertrauen unterschieden:**'mechanical trust'** und **'relational trust'**.[11]
'Mechanical trust' wird definiert als die Zuverlässigkeit eines Systems, das tut, was ein Benutzer von ihm erwartet.
Im Gegensatz dazu umfasst 'relational trust', die sozialen Normen und Vereinbarungen. Damit konzentriert sich 'relational trust' auf Menschen, Entscheidungen und darauf, wie eine Technologie funktionieren sollte.

Vertrauensbildung ist kein rein technisches Problem ist, sondern bezieht sich auch auf die soziale und politische Ebene.
Ob Menschen jemanden oder etwas vertrauen, hängt von unterschiedlichen Faktoren ab. Es geht dabei um wiederkehrende Prozesse von Einordenbarkeit und Wahrscheinlichkeit. Um Eventualitäten, Risiken und Unsicherheiten und wie sich diese überprüfen lassen. Auf technischer Ebene gibt es deshalb Protokolle und Standards, die definieren wie Prozesse und Vorgänge ablaufen.[12]
Sowohl auf der Ebene von mechanical trust, als auch auf der Ebene von relational Trust, können Designer*innen und Programmierer*innen – kurz: diejenigen die Technologie entwickeln – Vertrauensbildung beeinflussen.
Darauf, wie dies konkret aussehen kann, wird in den nachfolgenden Kapiteln eingegangen.

Vertrauen durch Protokolle und Systeme

Mechanical trust – also die Zuverlässigkeit eines Systems – kann über mehrere Mechanismen und Protokolle beeinflusst werden. Im Folgenden wird mechanical trust in Bezug auf Sicherheit diskutiert:

Blackbox vs. Open Box

Die meisten kommerziellen Softwarelösungen sind Closed Source, was bedeutet, dass es nicht möglich ist, sich den Quellcode anzusehen oder diese unabhängigen Audits zu unterziehen.
Nutzer*innen müssen darauf vertrauen, dass die Softwareentwickler Sicherheitsstandards bestmöglich implementiert haben, und die Daten der Nutzer*innen damit geschützt sind.
Ist der Quellcode einer Anwendung unter einer offenen Lizenz, also Open Source, kann er von externen Experten überprüft und kontrolliert werden. Öffentlicher Code ist transparent und nachprüfbar. Schwachstellen können so im Idealfall unmittelbar behoben werden. Doch die Vergangenheit hat gezeigt, dass es nicht immer so einfach ist. Selbst wenn der Quellcode in der Theorie von jedermann überprüft werden kann, werden Fehler häufig nicht sofort erkannt. Das hat unter anderem mit einem Mangel an Ressourcen wie Zeit,

[10] https://www.weforum.org/reports/data-collaboration-for-the-common-good-enabling-trust-and-innovation-through-public-private-partnerships
[11] https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech/
[12] https://www.w3.org/Protocols/

Arbeitskraft und Expertise zu tun.[13] Open Source Projekte haben nicht selten geringe finanzielle Mittel und die Instandhaltung der Software wird häufig nur von wenigen Personen gestemmt.[14]

Sicherheit von Software

Wenn der Nutzer*innen sicher sein kann, dass die Software vertrauenswürdig ist, bleibt eine andere Frage offen: Wie kann man sich versichern, dass die Software, die man auf seinen Geräten installiert, nicht manipuliert wurde? Ob Open oder Closed Source, ist die Frage nach der Integrität der Software eine wesentliche Frage, wenn es darum geht, Tools zu vertrauen. Ist die Software originalgetreu und fehlerfrei? Ist sie vor unautorisierten Änderungen geschützt?

Die Frage der Integrität ist die Frage der Vertrauenswürdigkeit von Lieferketten für Computerprogrammen. In den letzten Jahrzehnten wurde Software aus vielen ungeprüften Quellen von Nutzer*innen von Betriebssystemen wie z.B. Microsoft heruntergeladen und installiert. Nur wenige aufwändige Prozesse wie die manuelle Verifizierung von SHA-Prüfsummen und GPG-Signaturen ermöglichten es fortgeschritteneren Nutzer*innen, sicher zu sein, dass die von ihnen installierten Pakete eine genaue Kopie der Software waren, die sie herunterladen wollten. Dadurch können Nutzer*innen anfällig für Attacken, z.B. "Man in the Middle"-Angriffe, werden, wodurch Geräte kompromittiert werden können - ein bedeutendes Risiko für gefährdete Personen wie Journalisten, politische Dissidenten usw.
Durch Plattformen wie App-Stores, die die Qualität von Software prüfen und sichern, haben sich Schutzmechanismen in den letzten Jahren weiterentwickelt. Gleichzeitig befördern diese zentralen Ausgabestellen proprietäre Systeme.
Bleibt die Überprüfung, ob der Binärcode genau vom Quellcode abstammt: Dies ist bis heute ein komplizierter Prozess, für den derzeit Lösungen entwickelt werden.

Ein Beispiel dafür ist das vom Prototype Fund geförderte Projekt Reproducible Builds, das Binärcode aus verschiedenen Entitäten erstellt und die Ergebnisse abgleicht, um sicherzustellen, dass jeder Nutzer genau die gleiche Version der Software erhält, die er herunterladen möchte.
Obwohl Open-Source-Systeme die Möglichkeit bieten, dass jeder Code überprüfen kann (wie wir auch in Förderrunde 4, Power to the Users, gezeigt haben, bedeutet eine Vielzahl von Problemen (einschließlich eines gravierenden Mangels an Ressourcen für die Entwicklung von Open-Source-Software), dass schwerwiegende Probleme nicht immer sofort erkannt werden.

[13] https://www.theguardian.com/commentisfree/2014/apr/10/stop-next-heartbleed-bug-open-source-support-open-ssl
[14] https://www.wired.com/2014/04/heartbleedslesson/

Sichere Kommunikation & Verschlüsselung

Nicht nur die Software kann verändert werden, bevor sie den Computer eines Nutzers erreicht, sondern auch alle Daten, die an diesen Nutzer*innen gesendet werden. Das bedeutet: Die in den Nachrichten gesendeten Informationen können vor dem Erreichen des Empfängers geändert werden, Links können eingefügt werden, E-Mail-Anhänge mit Schadsoftware können hinzugefügt werden. Ein Beispiel dafür ist Phishing.
Wie bei der Software existieren seit Jahrzehnten Lösungsangebote, in Form von digitalen, kryptographischen Signaturen zum Beispiel.
Ähnlich wie bei der Überprüfung von Software, waren diese Verfahren bis vor kurzem kompliziert und nur mit fortgeschrittenem Wissen zugänglich.

Während GPG, das neben der Verschlüsselung auch das Signieren von E-Mails und Dateien ermöglicht, von Expertengruppen intensiv genutzt wird, hat die Smartphone-Ära neue, einfach zu bedienende Kommunikationswerkzeuge in Form von Messengern hervorgebracht, die immer häufiger Verschlüsselungsprotokolle implementieren, die kryptographische Signaturen enthalten. Beispiele dafür sind z.B. die Open Source Secure Messenger Wire and Signal, das verschlüsselte Messaging-Protokoll OMEMO oder das von dem Prototype Fund geförderte Projekt “Schleuder”[15], das GPG-Verschlüsselung und Signaturen für Mailinglisten implementiert.

Neben der technischen Absicherung durch Verschlüsselung, können aber auch ganz einfache Routinen und Praktiken im alltäglichen Umgang mit Software vor Viren und Schadsoftware schützen. Dazu zählt zum Beispiel, keine Anhänge von unbekannten Absendern zu öffnen und Passwortmanager zu verwenden.

Vertrauen durch Normen, Transparenz & Netzwerke

Neben dem *mechanical trust* gibt es, wie anfangs beschrieben, auch den relational trust.
Also Vertrauen, das auf gesellschaftlichen Normen und Vereinbarungen basiert.

In der Vertrauensbildung ist dieser Teil ist ebenso wichtig, wie das durch Protokolle, Systeme und technische Oberflächen gestützte Vertrauen.

Bildlich gesprochen ist mechanical trust wie die Bremsen in einem Auto: Sie sind TÜV–geprüft und funktionieren zuverlässig. Relational trust steht für die Absprache oder das Regelwerk, diese Bremsen an einer roten Ampel auch zu betätigen.

[15] https://prototypefund.de/en/project/schleuder/

Ohne diese Regel, würden selbst die best funktionierendsten Bremsen nichts bringen. Auch beim Einsatz neuer Technologien braucht es solche Regeln und Normen, die besagen wann, wie, warum und wozu diese Technologien eingesetzt werden.

Um diese Regeln zu entwickeln, braucht es Menschen, Prozesse und Werkzeuge. Es braucht Frameworks für Rechenschaftspflicht, Überprüfbarkeit, Transparenz und ethische Leitlinien.[16]

Transparenz, Nachvollziehbarkeit von Entscheidungen und Rechenschaftspflicht

Beispiel Datenschutzgrundverordnung der EU:

Die Einführung der Datenschutzgrundverordnung gibt Menschen in der EU und darüber hinaus ein Instrumentarium an die Hand, nachvollziehen zu können, wie mit ihren Daten umgegangen wird und ein Auskunftsrecht darüber, von wem Daten erhoben, gespeichert, weitergegeben und genutzt werden.
So können Personen beispielsweise eine Auflistung über alle über sie gespeicherten Daten anfragen.
Das erhöht nicht nur die Transparenz, sondern auch die Mündigkeit des Einzelnen, denn Nutzer*innen können bestimmen wer, wann, welche Daten über sie erheben und nutzen darf. Im Fall der Datenschutzgrundverordnung wird das Vertrauen über Regulierung gefördert.

Auch auf technischer Ebene gibt es Werkzeuge, die versuchen Nutzer*innen mehr Information über Tracking, Nutzungsbedingungen und Datensammlungen zur Verfügung zu stellen.
Ein Beispiel ist die Website Terms of Service Didn't Read[17] – die komplizierte Texte zu Nutzungsbedingungen in einfache Sprache übersetzt und aufzeigt, welche Effekte diese ToS auf Nutzer*innen haben können. Ein Tool das unsichtbares Tracking im Netz sichtbar macht, ist das vom Prototype Fund geförderte Tool Lightbeam.[18] Das Browser Plugin visualisiert von wem Nutzer*innen im Netz getrackt werden.

Die Wichtigkeit von Transparenz und Nachvollziehbarkeit, am Beispiel YouTube:

In 2017 wurde eine Reihe von Inhalten auf der Plattform Youtube ohne weitere Erklärung des Plattformbetreibers entfernt.
Die Ereignisse passierten, kurz nachdem Youtube erklärt hatte, dass es nun neueste maschinelle Lernverfahren anwendet, um extremistische Inhalt und Inhalt mit Terror-Bezug zu löschen. Einige der von der Löschung betroffenen Videos waren Dokumentationen von Kriegsverbrechen in Krisenregionen. Wichtige Zeitdokumente, die durch intransparenten Entscheidungen auf Seiten des Plattformbetreibers entfernt wurden.

[16] https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech/
[17] https://tosdr.org
[18] https://addons.mozilla.org/en-US/firefox/addon/lightbeam/

Nicht nur die Inhalte waren verloren, auch das Vertrauen derjenigen, sie sie online gepostet hatten.
Das Beispiel zeigt, wie wichtig transparente Entscheidungsprozesse für Plattformen wie Youtube, mit großem Einfluss auf Geschäftsmodelle und öffentliche Meinungen, sind[19].

Transparente Prozesse sind wichtig, um Vertrauen zu stiften und für die Nutzer*innen kalkulierbar zu sein. Sind diese Prozesse nicht vorhanden, haben Nutzer*innen keine institutionellen Möglichkeiten, nachzuvollziehen warum Inhalte entfernt wurden und die Wiederherstellung zu beantragen.

Vertrauen in Institutionen:

Eine der gängigen Hypothese im Bereich von Civic Tech ist, dass Technologieprojekte durch verbesserten Informationszugang, dazu beitragen können, Vertrauen zwischen Nutzer*innen und Institutionen aufzubauen.
Ein Beispiel dafür ist das Projekt Frag Den Staat[20], eine Plattform über die Anfragen nach dem Informationsfreiheitsgesetz gestellt werden können. Durch die Förderung von Transparenz und Informationsflüssen zwischen öffentlichen Einrichtungen und Bürger*innen, hat das Portal das Potenzial, das Vertrauen zwischen den Parteien zu fördern.

Weitere Beispiele für digitale Werkzeuge die Transparenz fördern sind: **Follow the Grant**[21], **Open Data City Census**[22] und **Meine Stadt Transparent**.[23]

In ähnlicher Weise stellen auch Förderinstitutionen mehr Informationen zur Verfügung, als in der Vergangenheit.
Der Prototype Fund selbst, wie auch große internationale Geldgeber wie Luminate[24], veröffentlichen Daten über ihre Förderung so, dass andere sie beforschen und untersuchen können.
Auch Open Data Portale von Ländern und Städten funktionieren auf eine ähnliche Art und Weise, sie liefern Daten zu bisher unzugänglichen Themen, die jeder und jede erkunden und nutzen kann.

Netzwerke und Communities

Auch Netzwerke und Communities können dabei helfen Vertrauen aufzubauen.

[19] https://www.buzzfeednews.com/article/evanhill/silicon-valley-cant-be-trusted-with-our-history
[20] https://fragdenstaat.de
[21] https://prototypefund.de/project/follow-the-grant/
[22] https://prototypefund.de/en/project/automated-open-data-city-census/
[23] https://prototypefund.de/project/open-source-ratsinformationssystem/
[24] https://luminategroup.com

Im Journalismus:

In den USA untersucht das Projekt The Membership Puzzle[25], was es bedeutet einen Newsroom basierend auf Vertrauen aufzubauen.
Das Projekt ist eine Kollaboration zwischen der niederländischen Journalismusplattform De Correspondent und der New York University.
Ziel ist es, eine nachhaltige Nachrichtenorganisation aufzubauen, die das Vertrauen in den Journalismus wiederbeleben soll. Mitglieder sollen nicht nur für den Journalismus bezahlen, sondern in die Arbeit rund um die Berichterstattung mit einbezogen werden. Auch neue Technologie ist im Spiel. Ein digitaler Werkzeugkasten namens Hearken[26], ermöglicht es der Redaktion, besser auf das Publikum einzugehen.

Vom Prototype Fund geförderte Tools, die dabei helfen Desinformation zu bekämpfen: **Syrian Archive**, **ACCID**, **Approxi**, **Fake Files**.

Social Media:

In sozialen Netzwerken bauen Vertrauen und Glaubwürdigkeit oft auf Metriken wie z.B. einer hohen Anzahl an Followern auf.
Dabei können solche Metriken einfach überlistet werden, indem sich Accounts Follower kaufen, zum Beispiel.
Anstatt sich nur von diesen Metriken und Zahlen leiten zu lassen, ist es daher wichtig, sich auch das “Web of Trust” um eine Person/einen Account herum anzusehen.

Verschwörungstheorien und falsche Fakten finden in sozialen Medien schnelle Verbreitung. In sozialen Netzwerken kann es besonders schwer sein, herauszufinden welchen Inhalten man trauen kann und welchen nicht.
In den letzten Monaten haben einige Plattformen damit begonnen, neue Mechanismen für die Überprüfung von Inhalten einzuführen.
Eine solche Neuerung die Kritik erfahren hat, kommt von der Plattform YouTube.
YouTube CEO Susan Wojciki kündigte in 2018[27] an, zu Videos mit Verschwörungstheorien die entsprechenden Wikipedia Artikel mit korrekten Fakten zum Thema zu verlinken.
Das Vorhaben wurde kritisiert, weil eine große finanzkräftige Plattform wie YouTube sich auf ein von Ehrenamtlichen betriebenes Projekt stützen will, ohne dieses weiter zu fördern.[28]

Ein vom Prototype Fund gefördertes Beispiel für geschützere, datensparsame, selbstverwaltete Soziale Netzwerke ist Blockparty.[29]

[25] https://membershippuzzle.org/about
[26] https://www.wearehearken.com
[27] https://www.wired.com/story/youtube-will-link-directly-to-wikipedia-to-fight-conspiracies/
[28] https://www.nytimes.com/2018/03/19/business/media/youtube-wikipedia.html
[29] https://prototypefund.de/project/blockparty/

Vertrauen durch Design

Die Frage ob etwas vertrauenswürdig erscheint oder nicht, ist auch eine Frage der visuellen Gestaltung von Anwendungen.

Einfache Design-Entscheidungen können dazu führen, dass sich Nutzer*innen befähigt oder der Technologie ausgeliefert fühlen.

In dieser Problemlage geht es auch um Kommunikation, darum wie gut man seine Zielgruppe kennt, um bedarfsorientiert gestalten und kommunizieren zu können.

Die Verwendung von einfacher Sprache kann beispielsweise nicht-technik affinen Menschen eine Hilfestellung sein, um komplexe Sachverhalte zu navigieren und für sich die entsprechend richtige Entscheidung zu treffen.
In der Gestaltung ist es wichtig, über unterschiedliche Vorlieben, potenzielle Bedrohungen und kulturelle Unterschiede von Zielgruppen Bescheid zu wissen.
Eine Möglichkeit Nutzer*innen mehr Freiheit, Flexibilität und damit Mündigkeit zu geben, liegt darin unterschiedliche Auswahlmöglichkeiten und Zustimmungsmodelle zu entwickeln.

Im Gegensatz zu Trust by Design stehen ‘Dark Patterns’. Sie sollen die Benutzer*innen absichtlich dazu verleiten, sich auf bestimmte Weise zu verhalten, z.B. indem sie dazu ermutigen, die Zustimmung für bestimmte Aktionen zu erteilen, oder nicht erkennen, dass ein System ohne ihre Zustimmung im Hintergrund läuft.

Outro

Es sollen mit dem Rundenschwerpunkt Sphären wie **Journalismus, demokratische Willensbildung und politische Kontrollfunktion, aber auch klassische IKT-Tools** betrachtet werden.
Außerdem **größere technologische Frameworks, die Dezentralisierung zur Grundlage von Vertrauen machen**.
Mit Prototypen in diesen Gebieten soll erschlossen werden, wie Tools und Technologien in genannten Kontexten eingesetzt werden (können).

Um Vertrauen in und mittels digitaler Technologie zu stiften und zu fördern, braucht es Entwickler*innen, Unternehmen und Organisationen die Sicherheit und Selbstbestimmung von Nutzer*innen ins Zentrum von Technologieentwicklung stellen.
Wir nennen diese Technologie ‘Trustable Technology’. Diese digitalen Werkzeuge und Plattformen setzen auf Transparenz, Nachvollziehbarkeit und Offenheit.

In den vergangenen Prototype Runden gab es bereits gute Beispiele dafür, wie Trustable Tech in der Praxis aussehen kann. Als Abschluss dieses Berichts, listen wir eine Reihe an Anwendungen auf, die sich auf den Schwerpunkt Technologie und Vertrauen beziehen.

- **Lightbeam:** Visualisiert Browser-Tracking und informiert Nutzer*innen darüber von welchen Seiten, sie wann getrackt werden.
- **Reproducible Builds:** Ermöglichen es, die Authentizität von Open-Software zu verifizieren.
- **GNU Taler:** Entwickelt Infrastruktur für bargeldlose Zahlungen ohne Überwachung.
- **Follow The Grant:** Zeigt, welche Ärzt* innen und Wissenschafler*innen Geld von Unternehmen erhalten.

Projekte die Missstände aufdecken und darauf abzielen, Nutzer*innen zu ermächtigen und ihnen mehr Kontrolle über ihr online Verhalten zu geben:

- **Tricky Sites**, eine Seite die sogenannte Dark Patterns auf E-Commerce Webseiten aufdeckt: https://trickysites.cs.princeton.edu
- https://www.darkpatterns.org/, eine Seite die Muster aufzeigt, die Nutzer*innen dazu verleiten sollen bestimmte Aktionen durchzuführen
- **Ghostery**, ein Browser-Plugin das anzeigt, wie man von Werbeunternehmen getrackt wird und den Nutzer*innen gleichzeitig mehr Kontrolle gibt https://www.ghostery.com/
- **Privacy Badger**, ein Browser-Plugin, das aus dem Verhalten eines Benutzers lernt, welche Tracker blockiert werden müssen, und eine "weiße Liste" aller erlaubten Tracker veröffentlicht: https://www.eff.org/privacybadger

Projekte, die darauf abzielen, Vertrauen von Nutzer*innen aufzubauen:

- **Provenance**: eine Plattform, die wichtige Produktinformationen und Reisen in Lieferketten sammelt und teilt.: https://www.provenance.org/
- **Plattformen für Bürgerhaushalte**: https://library.theengineroom.org/participatory-budgeting/
- **Hearken**, ein Werkzeugkasten, der Redaktionen dabei hilft, besser auf ihr Publikum einzugehen https://www.wearehearken.com/
- **Lean Data Practices** von Mozilla, eine Technik zur Datenverwaltung, die dabei hilft, Vertrauen bei den Mitgliedern aufzubauen und das operationelle Risiko zu reduzieren: https://mozilla.github.io/lean-data-practices-cso/

Weitere **Projekte zum Thema Vertrauensbildung online**:

- Eine Erläuterung über die '**Evolution des Vertrauens**' von Nicky Case: https://ncase.me/trust/
- '**New Organs**', ein Projekt der Künstler Tega Brain und Sam Lavigne, dass Theorien und Tatsachen zur Unternehmensüberwachung sammelt, archiviert und untersucht: https://neworgans.net/

- ‘**The End of Trust**’, eine Sonderausgabe des McSweeney’s Magazins, analysiert von EFF: https://www.eff.org/deeplinks/2018/11/end-trust-sale-bookstores-and-free-download-now
- ‘**Networks of Trust**’, ein Projekt der Künstlerin Kyriaki Goni http://kyriakigoni.com/portfolio/NoT.html