



# Die Digitalisierung ist politisch

Der Einfluss der Technologien auf die Demokratie wird im öffentlichen Diskurs entweder über- oder unterschätzt. Es braucht eine aufgeklärte, breite Debatte – sonst regelt es der Markt. Demokratie-Check, Teil 5.

Von Adrienne Fichter und Davide Baroni (Illustration), 05.03.2020

Ben Rattray, der Gründer der Kampagnenplattform Change.org, machte vor vielen Jahren eine bemerkenswerte Aussage. Bereits 2014 befand er, Silicon Valley habe alle möglichen Bereiche demokratisiert: Kommunikation, Transport, Wohnungsvermittlung – nur nicht die Demokratie selbst. Stattdessen, so ergänzte Rattray sein Zitat später, bekam die Bevölkerung von der Tech-Industrie ein anderes «Geschenk»: personalisierte politische Werbung.

Wie richtig Rattray lag, zeigte sich in den darauffolgenden Jahren. Negative Schlagzeilen aus der gesamten Tech-Welt im Kontext der Demokratie erscheinen seither fast im Wochentakt. Doch anders als bei Politik und Wirtschaft tun sich die Medien oft schwer, diese adäquat einzuordnen. Gerade

Politikjournalistinnen interessieren sich oftmals nur dann für Technologie, wenn Politiker Shitstorms auslösen oder ihr Konto gehackt wurde.

Auf der anderen Seite werden Tech-News hochgehypert, über andere wird gar nicht erst berichtet, und bei vielen werden die falschen Fragen gestellt, oder sie werden nicht adäquat eingeordnet. Skandalisierung hier, Ignoranz dort: Beides verunmöglicht eine aufgeklärte Debatte über Digitalisierung, in der aktuelle Phänomene in einen grösseren demokratiepolitischen Kontext eingebettet werden.

Digital mündige Bürger aber brauchen kompetente Berichterstattung. Nicht nur zur Meinungsbildung, sondern um Gestaltungswünsche und Forderungen an die Politik und die Technologiekonzerne zu formulieren – als User ebenso wie als Citoyenne.

Wie sehr es bisher an einer konsistenten und kompetenten Berichterstattung mangelt, zeigt sich zum Beispiel an folgenden Themenkomplexen:

### **Desinformation**

Auch vier Jahre nach der Sensationswahl von Donald Trump lechzen Medienhäuser immer noch nach einfachen technologischen Erklärungen. Dabei stürzen sie sich oft auf frische sozialwissenschaftliche Studien, die noch nicht durch sogenannte Peer-Reviews evaluiert wurden – bei denen also noch kein kritisches Gegenlesen von anderen Wissenschaftlerinnen stattgefunden hat. Je nach Zeitdruck lesen Journalisten kaum über das Abstract hinaus, hinterfragen die Methoden nicht, sondern fassen grob die Befunde des «Executive Summary» zusammen.

Das renommierte Oxford Internet Institute hat im vergangenen Jahr eine Studie über Desinformationskampagnen publiziert. Fazit: In mindestens 70 Staaten fänden gross angelegte Fake-News-Operationen statt, die grossenteils von politischen Bots durchgeführt werden, zum Teil von Regierungen gesteuert. Der Report, dessen Trends durchaus richtig eruiert sein mögen, enthält aber keine Angaben darüber, nach welchen Kriterien diese Bots identifiziert worden sind.

Das Phänomen der sogenannten Bot-Armeen könnte also masslos übertrieben gewesen oder aber noch viel gravierender sein. Wir wissen es nicht. Die Autoren haben sich vor allem auf Medienberichte der einzelnen Länder und ein nicht näher definiertes Modell gestützt. Dennoch hielt dies die «New York Times» nicht davon ab, die Studieninhalte in einen Artikel über den grossen Desinformationskrieg weltweit zu verpacken. Kurz: Twitter-Analysen haben durchaus Aussagekraft, ihre Begrenzungen und vor allem ihre methodische Herleitung müssen aber von den Medienschaffenden stärker hervorgehoben und in einen Kontext gestellt werden.

Bei der gezielten Fabrikation und Streuung von vorsätzlichen Fake News scheinen nach wie vor menschliche Verfasser relevanter zu sein als Bot-Armeen: Donald Trump kann sich in diesem Wahljahr wieder auf eine digitale Armada von freiwilligen Helfern stützen, die allerlei lokale Newsportale für ihn betreiben werden – mal mit wahren Zeitungsinhalten, mal mit frei Erfundenem, jedenfalls mit einer klaren politischen Agenda dahinter.

Unter anderem in Michigan – einem der wichtigsten Swing States – haben Republikaner unter dem Decknamen Metric Media Foundation ein ganzes Netz von rund 40 lokalen Medien aufgespannt. Diese publizieren teils seriöse Nachrichten, teils Studien von religiösen und konservativen Thinktanks. Die Informationslage in den USA, einem Land mit einem oh-

nehin sehr polarisierten Mediensystem, wird 2020 mit diesen neuen Playern noch viel verworrener und verwirrender als vor vier Jahren.

### **Manipulation**

Seit den US-Wahlen 2016 ist die massive Beeinflussung des Wählerverhaltens ein Dauerthema. Die Netflix-Doku «The Great Hack» zeigt den Erfolg datengetriebener Beeinflussungsoperationen in Form von individualisierten Facebook-Werbeanzeigen – und präsentiert dies als unumstösslichen Fakt. Dabei steht bis heute der empirische Beweis des Erfolgs von *Behavioural Advertising* auf Social Media aus.

Das bedeutet nicht, dass solche Methoden in Zukunft nicht grössere Effekte zeitigen können. Aber es ist nach aktuellem Forschungsstand nicht erwiesen, dass psychometrische Modelle und Big-Data-Operationen hinter Facebook-Anzeigen unentschlossene Wählerinnen zu einem Kandidaten treiben. Deshalb sprechen Politologen wie Dave Karpf bei diesem Thema von einem hartnäckigen Mythos, der von Medien und vor allem in der Kommunikationswissenschaft fortgeschrieben werde.

Selbst Brad Parscale, Trumps Digitalchef, glaubte gemäss eigenen Angaben nicht an die Werbeversprechen von Cambridge Analytica, wie er in einem aufschlussreichen Interview in der Sendung «60 Minutes» ausführte. Er selber testete Seite an Seite mit beratenden Facebook-Mitarbeitern verschiedene diffamierende Botschaften und Desinformationstexte zur Persona Hillary Clinton. In die Anzeigen, mit denen die anvisierten Zielgruppen – junge Frauen, afroamerikanische Wähler und weisse männliche Industriearbeiter – am besten «performten», wurde noch mehr Budget investiert. Ein hochrangiger Facebook-Manager sprach von der bislang besten Kampagne. Offenbar waren Parscales evidenzbasierter Ansatz und seine Experimentierlust relevanter für Trumps Facebook-Erfolg.

### **Hacking**

Meldungen von Security-Firmen werden von Medien fast unwidersprochen übernommen, wenn sie bestimmte Narrative bestätigen. Etwa die News, dass die russische Hackergruppe Fancy Bear das ukrainische Gasunternehmen Burisma gehackt haben könnte. Notabene also jenes Unternehmen, in dessen Verwaltungsrat Joe Bidens Sohn Hunter bis April 2019 sass. Die Meldung wurde im Januar ein paar Wochen vor dem Ende des Impeachment-Verfahrens veröffentlicht. Aufgekommen ist die These vom Hacking in einem dünnen Bericht einer bislang unbekannten Firma Area 1, die sich auf unbekannte Experten berief und daraufhin gleich ihre Security-Produkte für demokratische Wahlen lobpreiste. Es hätte also, auch wegen des Zeitpunkts, gute Gründe gegeben, die Motivation der Security-Firma und die Urheberschaft kritisch zu hinterfragen, die Meldung besonders streng auf ihre Stichhaltigkeit zu überprüfen und offene Fragen transparent zu machen. Viele Medien transportierten die Meldung des Hacks jedoch als Fakt.

Hacking-Angriffe sind schwer zuzuordnen – selten lässt sich der geografische Herkunftsort des Angriffs ausfindig machen. Klar ist, wem die Meldung über das Hacking nützt: der Security-Firma, die ihre Produkte bewerben kann. Auch wenn tatsächlich die Gruppe Fancy Bear hinter dem Hacking-Angriff stecken soll: Wie soll die Leserin ohne Vermittlung solcher Kontexte die verbreitete Information adäquat einordnen können?

## Nur Technologie, die manipuliert, ist interessant

Die skandalorientierte öffentliche Debatte über Social Media hat nicht nur mit ungenauer Lektüre von sozialwissenschaftlichen Studien zu tun. Sondern auch mit einem einseitigen Fokus auf die Wirkungs- und Nutzungsebene: Datenbasierte Beeinflussungsmethoden werden erst dann zu einem medialen Thema, wenn sie Sensationslüsternheit bedienen und es potenziell um Manipulation geht. Fragen zu Software, IT-Sicherheit und Privatsphäre werden hingegen gar nicht als politisch wahrgenommen. Die Geschäftsmodelle der IT-Firmen und die Datenwirtschaft als solche sind kaum öffentlicher Gegenstand. Schnittstellen, Datenschutzerklärungen und Sicherheitspatches – so technisch diese Begriffe klingen mögen – haben jedoch weitreichende demokratiepolitische Implikationen.

Auch dazu eine Reihe von Beispielen.

### Schnittstellen

Gerade am Fall Cambridge Analytica lässt sich das soeben Gesagte gut illustrieren: Dass hier massenhaft persönlichste Daten von unwissenden Wählerinnen abgeflossen sind, war nicht etwa «missbräuchlich», wie uns die Facebook-Führungsriege mehrfach glauben machen wollte. Liest man die alten Nutzungsbedingungen von Facebook durch, so geschah dies mit dem Wissen und sogar nach dem Willen der Firma. Denn die betreffende technische Schnittstelle zwischen Plattform und externer App war lange Zeit ein legales Gratisgeschenk: an die App-Entwicklerinnen, an den damaligen Präsidenten Barack Obama für seine Mobilisierungskampagne 2012, für Wissenschaftlerinnen und Gamer auf der ganzen Welt, die über Abfragen jener Schnittstelle Facebooks Datenpool anzapfen konnten.

Weshalb hat also diese Datenstaubsaugerfunktion die Welt bisher nicht gross gekümmert?

Der vom «Guardian» enthüllte Sündenbock Cambridge Analytica ist ja keineswegs ein Einzelfall. Vielmehr steht die Firma stellvertretend für eine riesige Datenindustrie, die bis 2014 ihre Datenbanken mit Facebook-Likes von ahnungslosen Nutzerinnen gefüttert hat. Es ist vollkommen unklar, in wie vielen weiteren Datenbanken von dubiosen Big-Data-Unternehmen jede Einzelne von uns unwissentlich «verarbeitet» worden ist. Das allein wäre schon skandalös. Doch für die meisten von uns werden diese Datenlecks erst relevant, wenn sie grössere Manipulationsängste bedienen. Oder wenn damit politische Grossereignisse wie der Brexit erklärt werden.

### Entgrenzende Plattformen

Auch die Werbenetzwerke der Tech-Giganten wurden erst nach diversen Enthüllungen zum Politikum. Es brauchte Zuckerbergs zerknirschtes Eingeständnis der russischen Einflussnahme auf die US-Wahlen, um der Öffentlichkeit zu demonstrieren, dass auf globalen Plattformen nationalstaatliche Grenzen keine rechtsverbindliche Gültigkeit haben. Doch bereits vorher war antizipierbar: Im Datenselbstbedienungsladen von Google und Facebook kann sich jeder mit Netzanschluss und 50 Euro Budget in Referenden und Gemeinderatswahlen auf dem ganzen Planeten einmischen – egal ob in Wülflingen, Nabarangpur oder Rockhampton. Mit einer Anmeldung im Werbeanzeigenmanager als Werbekunde lassen sich innert wenigen Klicks Kampagnen aufsetzen, die innert wenigen Minuten automatisiert genehmigt werden.

In welche absurden Szenarien solche Werbemodelle münden, illustrieren Satiriker oftmals besser als die Medien: So hat Sacha Baron Cohen in einer Preisrede eindringlich davor gewarnt, dass die Nazis heute auf Facebook in wenigen Minuten eine 30-sekündige Videokampagne für die «Lösung der Judenfrage» aufschalten würden – und Facebook diese aufgrund seiner Gemeinschaftsrichtlinien nicht einmal stoppen würde. Cohen gelang es so, in einem Satz das Problem der automatisierten und unkontrollierten Werbemaschinerie auf den Punkt zu bringen.

### **Fragmentierte Öffentlichkeiten und polarisierender Algorithmus**

Jeder, der ein bisschen was von zeitgemäßem Onlinemarketing versteht, weiss: Jeder Userin kann in ein paar Sekunden eine andere Wahrheit präsentiert werden als ihrer Zimmernachbarin, ihrem Bruder oder der Arbeitskollegin. In der Offlinewelt haben wir als Gesellschaft zwar keine Einigung über eine bestimmte politische Lösung – aber wenigstens dasselbe Verständnis, was überhaupt die Ausgangslage ist. Mit dem werbebasierten Micro-Targeting und der zunehmenden Personalisierung wird dieses fundamentale Prinzip unterwandert. Indem Verschwörungstheoretiker ungehindert Desinformation an einzelne Profile ausspielen, diese nicht von Faktencheckern geprüft und somit die einzelne Empfängerin der Botschaft verwirrt wird. Theoretisch könnte nach diesem Prinzip jeder User unterschiedliche und widersprechende Informationen über das Coronavirus oder die Klimakrise erhalten.

Dies hat fatale Konsequenzen für den politischen Diskurs. Denn eine Demokratie ist auf eine politische Öffentlichkeit und Transparenz aller politischen Standpunkte angewiesen. Zwar hat Facebook in der Zwischenzeit mit der «Ad Library» hier etwas Transparenz geschaffen. Doch mit der Entscheidung für ein individualisiertes Werbemodell haben die Führungskräfte von Twitter und Co. sich nicht für offene Arenen, sondern für personalisierte Welten entschieden – eine klare Werteentscheidung. Mit politischer Relevanz.

Dasselbe gilt für eine andere Eigenheit beliebter Apps: Die meisten Netzwerke sind so designt, dass sie Suchtverhalten fördern: Weshalb verbringen wir so viel Zeit auf den Netzwerken? Weil sie Anreizstrukturen wie zum Beispiel die «belohnenden» Like-Buttons bieten und uns mit allem möglichen Content bei Laune halten. Mögen das Katzenvideos, Ferienbilder oder «Spiegel»-Schlagzeilen sein.

Auf politischer Ebene hat sich klar gezeigt: Je mehr Lärm und Empörung generiert wird, desto mehr Aufmerksamkeit gibt es dafür. Und desto höher fällt die Verweildauer der Nutzerinnen aus. Denn auf Metadaten ausgerichtete Algorithmen lernen: Eine Nachricht, die viele Shares erzeugt, ist eine gute Nachricht. Und nicht etwa jene, die einen moderaten Ton anschlägt oder besonders differenziert ausformuliert ist. Entscheidend ist die Teilbarkeit, nicht der Wahrheitsgehalt.

Es brauchte jedoch erst den Aufstieg der Social-Media-affinen rechtsextremistischen Parteien wie AfD und FPÖ sowie Donald Trumps Wahl als US-Präsident, bis die politische Sprengkraft der Algorithmen – und das opportunistische Businessmodell dahinter – endlich ins öffentliche Bewusstsein rückte.

### **Falsche Fragen**

Es gibt auch Beispiele ausserhalb der sozialen Netzwerke, in denen die öffentliche Debatte politische Kernfragen verfehlt: Bei der Publikation der

«New York Times» über die Gesichtserkennungs-Software Clearview AI wurde unter anderem moniert, dass die Erkennung der Software nicht gut genug funktioniere. Ihre Fehlerquote sei zu hoch, gerade dunkelhäutige Menschen würden den falschen Identitäten zugeordnet und somit als *false positives* in Polizeigewahrsam genommen. Dieser Argumentation zufolge müsste man Software einfach noch präziser «trainieren», sodass sie dann gerechterweise alle Menschen lückenlos identifizieren kann. Denn Technik sei ja – ein ebenso hartnäckiger Mythos – «neutral».

Doch wo beginnt genau der Schaden? Bei der falschen Zuordnung? Oder bei der Zuordnung per se? Akkurate Echtzeiterkennung von Gesichtern macht Strafverfolgung womöglich effizienter, bedeutet aber auch das Ende der Anonymität im öffentlichen Raum. Doch statt dass wir grundsätzlich über den Zweck und den Einsatz von automatisierter Gesichtserkennung diskutieren, reden wir über korrektes Matching von uns selbst als Datensubjekten.

Dass IT-Infrastruktur höchst politisch ist, müsste eigentlich auch beim medialen Dauerbrenner 5G deutlich sein.

Für die meisten Politikerinnen Europas ist es ein *no brainer*, dass bei der Wahl des richtigen 5G-Netzanbieters Fragen der technologischen Souveränität eine Rolle spielen. Und dass auch geopolitische Abhängigkeiten von den USA und China problematisiert werden müssen. Nicht so in der Schweiz: Hier dominiert allein die Gesundheitsdebatte. Politische Bedenken über die Verwundbarkeit durch die zunehmende Virtualisierung unserer IT-Infrastruktur? Fehlanzeige.

Hätte der Bund keinen temporären Marschhalt eingeläutet, wäre 5G bereits flächendeckend Ende dieses Jahr in der Schweiz verfügbar. Nach den Masterplänen von Swisscom und Co. sollen schnellstmöglich alle Häuser mit Sensoren versehen, ans Netz angeschlossen werden und miteinander kommunizieren – und das auf komplett ungesicherten Netzverbindungen.

Der Warnruf von Sicherheitsexperte Bruce Schneier, «Internetsicherheit muss genau gleich wie Flugsicherheit behandelt werden», ist in der Schweiz weder auf politischer noch auf gesellschaftlicher Ebene angekommen. Kein Wunder, machen sich die meisten Schweizerinnen mehr Sorgen über Strahlenwerte als darüber, ob ein künftig dank 5G autonom fahrendes Auto sie direkt in den Abgrund fahren könnte.

## **Eine demokratiefreundliche Digitalisierung ist möglich**

Weil die Politik in der Verarbeitung dieser agilen Entwicklungen hinterhinkt und den Redaktionen die analytische Kompetenz fehlt, haben die Datenkonzerne bisher leichtes Spiel. Sie können weiterhin klassische Pflasterchenpolitik betreiben. Ab und an werden sie ein wenig an den Softwarestellen schrauben, die Reichweiten gewisser Inhalte wieder herunterstufen, die Zahl von Empfängerkontakten reduzieren ...

Am Werbemodell von GAFAM, also den grossen fünf (Google, Amazon, Facebook, Apple und Microsoft), wird sich damit jedoch in naher Zukunft nichts ändern. Börsenkotierte Technologieunternehmen sind nämlich in erster Linie den Aktienwerten der Wallstreet verpflichtet und nicht dem Gemeinwesen. Die unsichtbare Hand des Datenkapitalismus sorgt dafür, dass sich die ungesättigten Big Five noch mehr Marktanteile einverleiben. Obwohl genau der entfesselte Datenkapitalismus und der permanen-

te Aufmerksamkeitswettbewerb für das toxische Klima in der Netzsphäre verantwortlich sind.

Dies führt dazu, dass immer mehr Internetnutzende in eine Art digitale Apathie verfallen, mit zwei Ausprägungen: Entweder entsagen sie sich ganz den sozialen Netzwerken und jeglichen Arten von Onlinediensten. Oder sie belassen ihre Passwörter bei «123456» und ändern nichts an den datenabsaugenden Voreinstellungen ihres Profils, bis sie selber von Ransomware betroffen sind und geschädigt werden.

Beide Bewältigungsstrategien sind Gift für einen konstruktiven Technologiediskurs. Denn verdrossene oder gleichgültige Bürger üben keine konstruktive Kritik zur Verbesserung von Produkten. Und die Politikerinnen sehen keinen Anlass, die Instrumente, deren sie sich selber gerne bedienen, zu regulieren.

Bei einer disparaten Medienberichterstattung und einem panikgetriebenen Digitalisierungsdiskurs wird das Denken in grösseren Zusammenhängen unmöglich. Was wären konkrete Alternativen zum gegenwärtigen Plattform-Kapitalismus? Der Wunsch des Change.org-Gründers Ben Rattray nach demokratieverbessernder Technologie ist keine Utopie, sondern durchaus machbar.

In der netzpolitisch engagierten Szene gibt es breiten Konsens darüber, was die Anforderungen dafür sind: grösstmögliche Transparenz über die Funktionsweise einer Software durch Open und Free Source, Hoheit der Daten bei den Bürgerinnen, dezentrale Serverstrukturen und Datenbanken sowie Datensparsamkeit als oberstes Prinzip. Neben der Technologie allein braucht es aber neue Prozesse, Moderationsformen und ein Design, das unsere Argumente sortiert und einordnet.

Kurz: Nicht nur ein freier und auf ethischen Prinzipien abgestützter Code spielt eine Rolle, sondern auch alle Kontrollen und sauber eingebaute Prozeduren der Ausführung. Und der politische Wille, genau solche Technologien mit öffentlichen Geldern zu fördern.

## **Accountability hinter Blackbox-Systemen**

Weil sich diese Erkenntnisse langsam, aber doch immer mehr durchsetzen, ein paar gute Nachrichten zum Schluss.

In der Schweiz und in Deutschland wächst das Bewusstsein für sogenannte Civic-Technologien, also Technik, die Engagement und Teilhabe der Bürger fördern will. Mit Förderfonds wie etwa dem Prototype Fund ist die Zivilgesellschaft aufgerufen, digitale Lösungen zu programmieren, welche die Partizipation fördern. Länder wie Taiwan, aber auch Metropolen wie Barcelona und Amsterdam machen vor, wie intelligente und überwachungsfreie Städte und deliberative Plattformen funktionieren können. Und die EU versucht mit ihrer neuen Digitalstrategie eine positive Vision einer europäischen Datenökonomie aufzubauen, gestützt auf die Datenschutz-Grundverordnung (DSGVO).

Auch in den Medien gibt es erfreuliche Beispiele: So arbeiten die «Rundschau» von SRF und der «Tages-Anzeiger» historische Vorgänge rund um den Überwachungsskandal Cryptoleaks akribisch und kontinuierlich auf. Zum Ärger der betroffenen Politikerinnen, die diese Vergangenheitsbewältigung lieber gestern als heute unter den Teppich kehren möchten.

Genau so geht politikrelevanter Technologiejournalismus: indem Accountability, eine Rechenschaftspflicht, geschaffen wird, wo vorher eine «Black-box» war. Indem Entscheidungsträger und ihr Spielraum hinter der Software konkret benannt, Missstände sichtbar gemacht werden und aufgezeigt wird, was die Alternativen gewesen wären. Wie bereits der Vordenker Evgeny Morozov in einem Interview mit der Republik sagte: «Hinter spezifischen Technologieeffekten stehen historisch gewachsene Machtstrukturen, die nicht notwendig die Form haben müssen, die sie haben. Sie können auch wieder verändert werden.»

Es braucht einen aufgeklärten Digitalisierungsdiskurs, der die Bürgerinnen befähigt, zu verhandeln, in welche Richtung die Digitalisierung in einer Demokratie verändert werden soll. Sonst regelt es nämlich der Markt.