THE UNIVERSAL DECLARATION OF Human Rights

WHEREAS *recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world,*

WHEREAS *disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind, and the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people,*

WHEREAS *it is essential, if man is not to be compelled to have recourse, as a last resort, to rebellion against tyranny and oppression, that human rights should be protected by the rule of law,*

WHEREAS *it is essential to promote the development of friendly relations among nations,*

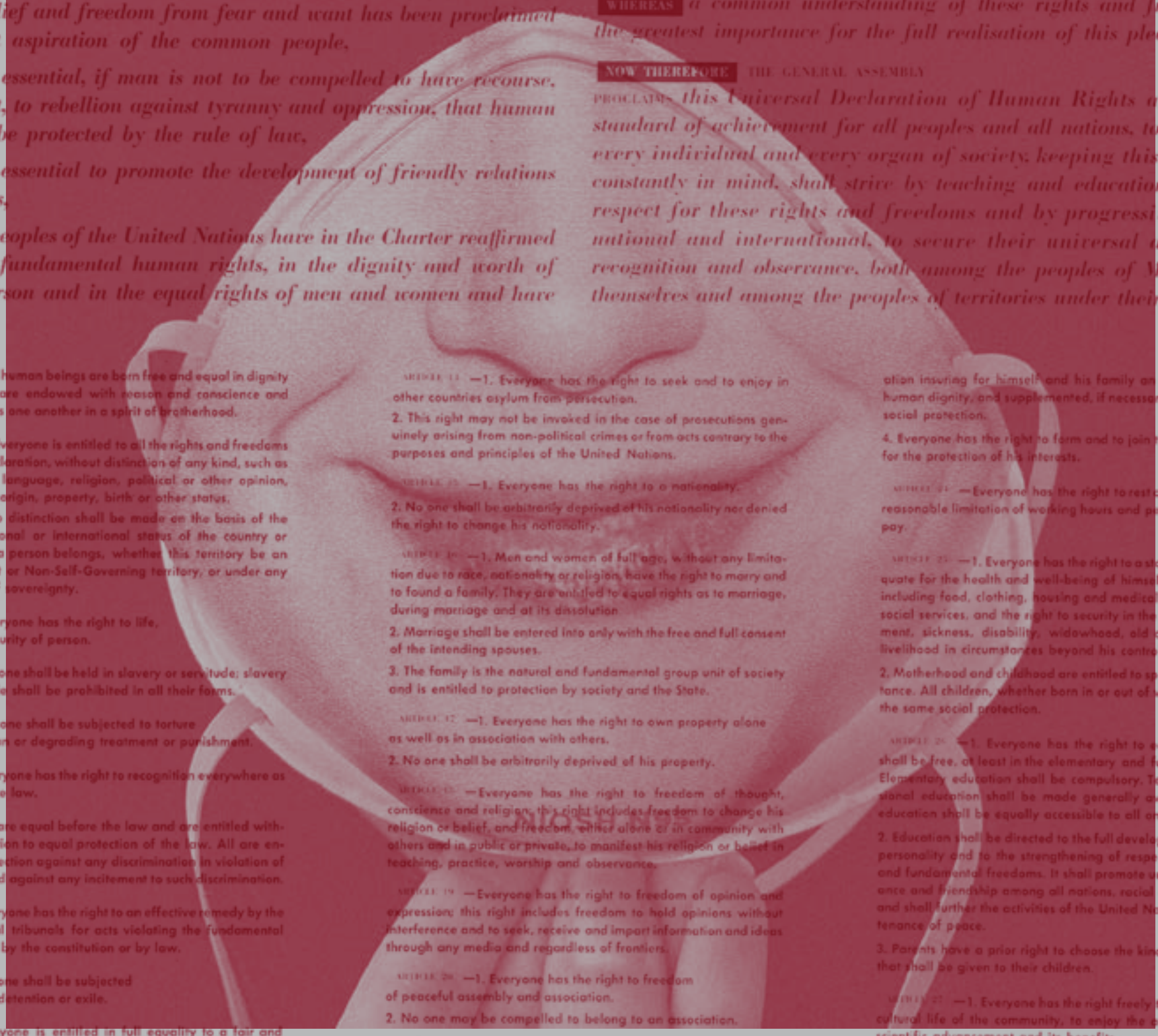
WHEREAS *the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedom,*

WHEREAS *Member States have pledged themselves to achieve, in co-operation with the United Nations, the promotion of universal respect for and observance of human rights and fundamental freedoms,*

WHEREAS *a common understanding of these rights and freedoms is of the greatest importance for the full realisation of this pledge,*

NOW THEREFORE THE GENERAL ASSEMBLY

PROCLAIMS *this Universal Declaration of Human Rights as a common standard of achievement for all peoples and all nations, to the end that every individual and every organ of society, keeping this Declaration constantly in mind, shall strive by teaching and education to promote respect for these rights and freedoms and by progressive measures, national and international, to secure their universal and effective recognition and observance, both among the peoples of Member States themselves and among the peoples of territories under their jurisdiction.*



ARTICLE 1 —All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

ARTICLE 2 —1. Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

2. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether this territory be an independent, Trust or Non-Self-Governing territory, or under any other limitation of sovereignty.

ARTICLE 3 —Everyone has the right to life, liberty and the security of person.

ARTICLE 4 —No one shall be held in slavery or servitude; slavery and the slave trade shall be prohibited in all their forms.

ARTICLE 5 —No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment.

ARTICLE 6 —Everyone has the right to recognition everywhere as a person before the law.

ARTICLE 7 —All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.

ARTICLE 8 —Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.

ARTICLE 9 —No one shall be subjected to arbitrary arrest, detention or exile.

ARTICLE 10 —Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him.

ARTICLE 11 —1. Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence.

2. No one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed.

ARTICLE 12 —No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ARTICLE 13 —1. Everyone has the right to freedom of movement and residence within the borders of each state.

2. Everyone has the right to leave any country, including his own, and to return to his country.

ARTICLE 14 —1. Everyone has the right to seek and to enjoy in other countries asylum from persecution.

2. This right may not be invoked in the case of prosecutions genuinely arising from non-political crimes or from acts contrary to the purposes and principles of the United Nations.

ARTICLE 15 —1. Everyone has the right to a nationality.

2. No one shall be arbitrarily deprived of his nationality nor denied the right to change his nationality.

ARTICLE 16 —1. Men and women of full age, without any limitation due to race, nationality or religion, have the right to marry and to found a family. They are entitled to equal rights as to marriage, during marriage and at its dissolution.

2. Marriage shall be entered into only with the free and full consent of the intending spouses.

3. The family is the natural and fundamental group unit of society and is entitled to protection by society and the State.

ARTICLE 17 —1. Everyone has the right to own property alone as well as in association with others.

2. No one shall be arbitrarily deprived of his property.

ARTICLE 18 —Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.

ARTICLE 19 —Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

ARTICLE 20 —1. Everyone has the right to freedom of peaceful assembly and association.

2. No one may be compelled to belong to an association.

ARTICLE 21 —1. Everyone has the right to take part in the government of his country, directly or through freely chosen representatives.

2. Everyone has the right of equal access to public service in his country.

3. The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.

ARTICLE 22 —Everyone, as a member of society, has the right to social security and is entitled to realisation, through national effort and international co-operation and in accordance with the organisation and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality.

ARTICLE 23 —1. Everyone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment.

2. Everyone, without any discrimination, has the right to equal pay for equal work.

3. Everyone who works has the right to just and favourable remuneration insuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection.

4. Everyone has the right to form and to join trade unions for the protection of his interests.

ARTICLE 24 —Everyone has the right to rest and leisure, including reasonable limitation of working hours and periodic holidays with pay.

ARTICLE 25 —1. Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, clothing, housing and medical care and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control.

2. Motherhood and childhood are entitled to special care and assistance. All children, whether born in or out of wedlock, shall enjoy the same social protection.

ARTICLE 26 —1. Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit.

2. Education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms. It shall promote understanding, tolerance and friendship among all nations, racial or religious groups, and shall further the activities of the United Nations for the maintenance of peace.

3. Parents have a prior right to choose the kind of education that shall be given to their children.

ARTICLE 27 —1. Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.

2. Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

ARTICLE 28 —Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized.

ARTICLE 29 —1. Everyone has duties to the community in which alone the free and full development of his personality is possible.

2. In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

3. These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations.

ARTICLE 30 —Nothing in this Declaration may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein.

Während die Digitalisierung in den letzten dreissig Jahren zahlreiche Lebens- und Arbeitsbereiche radikal verändert hat, passierte beim Verhältnis zwischen Staat und BürgerInnen diesbezüglich wenig.

Die Ankündigung der E-Government-Strategie 2020–2023 sowie die Anstrengungen zur privaten Herausgabe einer E-ID stellen in diesem Jahr deshalb eine bedeutende Zäsur dar. Plötzlich scheint es nicht schnell genug zu gehen: Zentrale staatliche Aufgaben sollen unter Abhängigkeit von privaten Dienstleistern gestellt und ohne den nötigen sorgfältigen breiten politischen Diskurs möglichst rasch digitalisiert werden. Im Herbst 2019 stimmten sowohl der National- wie auch der Ständerat einer privaten Herausgabe einer E-ID zu. Statt sich daran zu orientieren, welche Anliegen im Sinne der Bevölkerung sind, überlassen Bundesrat und Parlament die digitale Transformation privaten Unternehmen.

Die permanente Litanei, dass die Privatwirtschaft in Sachen Digitalisierung über umfassendere Kompetenzen verfügt, hat gewirkt: Der Missstand wird jedoch nicht als Weckruf dafür verstanden, sich die Fähigkeiten selbst anzueignen. Vielmehr wird er als Legitimation verwendet, diese Komptenzen deshalb in die Privatwirtschaft auszulagern. Die Bürgerinnen und Bürger ihrerseits werden jäh aus dem digitalen Dornröschenschlaf wachgeschüttelt. Und anstelle eines Prinzen erwartet sie vielleicht bald eine dicke Kröte.

Die Sicherung der Identität gilt gemeinhin als zentrale Staatsaufgabe, die bisher der demokratischen Kontrolle unterstand. Gibt der Staat solche Ausgaben aus der Hand, geht damit auch allgemeine staatliche Legitimität verloren.

Die Folgen einer solchen Delegitimierung sollten nicht auf die leichte Schulter genommen werden. Die Frage nach der konkreten Ausgestaltung unserer digitalen politischen Strukturen betrifft letztlich auch die BürgerInnenrechte und den Service Public. Die Digitalisierung war lange ein Phänomen, das zuerst an den Hochschulen und erst danach in der Wirtschaft und den Medien stattgefunden hat. Das glorifizierte Potential der Befreiung und Emanzipation blendete die Sicht auf die kommenden Schwierigkeiten für die bestehenden Grundrechte. Erst die Diskussionen um die Netzneutralität liessen Ende der Nullerjahre einen kleinen Teil der Bevölkerung aufhorchen und ahnen, was im Zusammenhang von Digitalisierung und Service Public noch auf dem Spiel stehen wird.

In dieser Ausgabe widmen wir uns folgenden Fragen: Wie können wir die Digitalisierung für demokratische Prozesse nutzen, bisherige gesellschaftliche Errungenschaften angemessen transformieren und einem Abbau von (digitalen) BürgerInnenrechten entgegen treten?

Editorial von Ivan Sterzinger

DAS MÄRCHEN VON DER NEUTRALEN TECHNIK

Im New York der 1920er Jahre wurde der Diskriminierung ein bauliches Denkmal gesetzt. Der einflussreiche Stadtplaner Robert Moses war damals sehr darauf bedacht, dass das Naturschutzgebiet Jones Beach auf Long Island vor allem der weissen Mittel- und Oberschicht zugute kommt. Daher veranlasste er, dass zahlreiche niedrige Brücken über die Zugangswege gebaut werden, wodurch die Strecken für die dreieinhalb Meter hohen Busse des öffentlichen Personennahverkehrs nicht mehr befahrbar waren. Dieser architektonische Kniff führte dazu, dass es für ärmere Bevölkerungsschichten ungemein schwierig wurde, den Jones Beach zu erreichen. Die wohlhabende weisse Mittelschicht hingegen bemerkte von dieser baulichen Segregationsmassnahme nichts – sie verfügte über eigene PKWs und konnte problemlos ihre Wochenendausflüge dorthin planen. Die Autorin und Mathematik-Professorin Hannah Fry verdeutlicht in ihrem Buch ‹Hello World› (2018) anhand dieser Geschichte, wie wichtig es ist zu prüfen, inwiefern unter der Oberfläche harmlos wirkender Massnahmen nicht doch insgeheim gesellschaftliche Machtgefälle zementiert werden. Der Schwerpunkt von Hannah Frys Arbeit liegt dabei keineswegs auf städtebaulichen Massnahmen; sie beschäftigt sich in ihrem Buch vielmehr mit zentralen Fragen der digitalen Infrastruktur unserer Zeit. Sie sagt, dass bewusst oder unbewusst getroffene Entscheidungen bezüglich der Architektur von Software das Potential haben, massiv in unser Leben einzugreifen. Fehlt eine kritische Folgeabschätzung, kann dies fatale Konsequenzen haben.

Was das konkret bedeutet, lässt sich etwa beim Thema Arbeit beobachten. Immer mehr Unternehmen setzen auf elektronische Hilfsmittel, um die ideale Bewerberin für eine vakante Stelle zu finden. Die Firma Xerox wollte hierbei ein neues Verfahren ausprobieren. Lange Arbeitswege sind nachweislich ein grosser Stressfaktor für viele Beschäftigte. Unter der Annahme, dass Arbeitnehmende mit einem kurzen Arbeitsweg dem Unternehmen langfristig eher treu bleiben, wäre es daher nur logisch, bereits bei der Bewerberauswahl eine geringe Distanz zwischen Wohn- und Arbeitsort als Pluspunkt zu werten. Bei gleichen Qualifikationen würde dann die Bewerberin mit einem kurzen Arbeitsweg den Vorzug bekommen. Für das Unternehmen Xerox stellte sich dies als ein gutes Verfahren dar. Dabei wurde allerdings ein nicht unerhebliches Detail übersehen. Bewerber, die es sich mit ihrem derzeitigen Gehalt schlichtweg nicht leisten können, näher am Unternehmenssitz in einem wohlhabenden Stadtteil zu wohnen, sind bei einem solchen Verfahren klar im Nachteil. Die Folge: Bestimmte soziale Gruppen werden am beruflichen Aufstieg gehindert. Als dem Unternehmen dies klar wurde, sind sie schnell zum Ergebnis gekommen, das Kriterium Wohnortnähe lieber doch nicht berücksichtigen zu wollen. Das Beispiel zeigt, dass es bei neuen Formen von auf Algorithmen basierender Diskriminierung nicht einmal eines Vorsatzes bedarf, es reicht eine Unachtsamkeit. Für die Betroffenen sind die Folgen nichtsdestotrotz gravierend.

Ein anderer Fall macht dies noch deutlicher. Im Jahr 2018 verkündete Amazon, es werde nicht länger eine KI zur Auswahl von Bewerbungen benutzt. Es hatte sich nämlich herausgestellt, dass die künstliche Intelligenz systematisch Frauen diskriminierte. Auch hier ist unwahrscheinlich, dass ein Vorsatz des Unternehmens dahintersteckte. Um das System zu trainieren, wurden schlichtweg Daten von vergangenen Bewerbungen genutzt und die KI damit angefüttert. Die künstliche Intelligenz war bestrebt, in den Datensätzen Muster dafür zu finden, was die menschlichen Recruiter als den «idealen Bewerber» ansahen. Eine Regel lag für die KI auf Grundlage der Daten auf der Hand: Da in der Vergangenheit Männer sowohl öfter Bewerbungen eingereicht hatten als auch häufiger den Zuschlag bekamen, «lernte» die KI, dass das Geschlecht anscheinend ein wichtiges Kriterium sein müsse. Frauen wurden infolge dessen systematisch benachteiligt.

Angesichts solcher Fälle mag es für manche nahe liegen, jegliche Form softwarebasierter Entscheidungshilfen als «kalt» oder gar «unmenschlich» zu verteufeln. Doch ganz so einfach ist es dann doch nicht. Ebenso wäre es denkbar gewesen, Software dazu zu nutzen, um die Unterlagen von Bewerberinnen zu anonymisieren, damit Nebensächlichkeiten wie Alter, Aussehen und Geschlecht nicht mehr von der fachlichen Qualifikation eines Bewerbers ablenken. Solche Beispiele für den positiven Einsatz von Technik zur Beseitigung von Diskriminierung gibt es eben auch. Das Beispiel der misogynen Amazon-KI zeigt vor allem die Risiken eines leichtfertigen Technologieeinsatzes auf. Eine systematische Datenanalyse bisheriger Einstellungsentscheidungen hätte problemlos genutzt werden können, um vergangene Diskriminierung sichtbar zu machen. Werden die Daten bisheriger Einstellungsprozesse aber unreflektiert als «vorbildlicher» Trainingsdatensatz für eine KI übernommen, entsteht die Gefahr, dass bestehende Ungerechtigkeiten nicht nur weitergetragen, sondern sogar verschlimmert werden. Wird die Entscheidung einer KI überlassen, wird zudem die Verantwortung delegiert. Wer hinterfragt schon, ob die Maschine wirklich die «beste» Entscheidung getroffen hat? Und was wäre eigentlich, wenn eine solche Software gar von einem externen Dienstleister bereitgestellt werden würde, der sich bei der Forderung nach mehr Transparenz in Bezug auf die Kriterien einfach auf sein Geschäftsgeheimnis beruft und Prüfungen auf Fehler im System ablehnt, da dies schlecht fürs Marketing wäre? Sich gegen diese neuen Formen von Diskriminierung zur Wehr zu setzen, würde für Betroffene damit zu einem Ding der Unmöglichkeit werden.

In den vergangenen Jahren sind zahlreiche kommerzielle Angebote zur «objektiveren» Bewertung von Arbeitnehmenden wie Pilze aus dem Boden geschossen. Bei manch einem Produkt beschleicht einen jedoch das Gefühl, dass die Heilsversprechen der Anbieter mehr mit Esoterik als Wissenschaftlichkeit gemein haben. Dienstleister bieten mittlerweile an, grosse Datenberge nach Hinweisen zu Bewerbern zu durchforsten. Der blinde Zahlenglaube, der beim Einsatz solcher Systeme zum Ausdruck kommt, kann teilweise skurrile Ausmasse annehmen. So stellte ein auf Bewerbungsalysen spezialisiertes Unternehmen anhand seiner Datenanalyse etwa fest, dass Bewerberinnen, die einen aktuellen Browser benutzen, angeblich eher zu den Top-Performern gehören würden. Und wer in einem oder zwei sozialen Netzwerken angemeldet sei, bliebe angeblich länger im Job als die Vergleichsgruppe mit nur einem oder keinem Account. In den USA dürfen solche Recherchen zudem nicht nur öffentlich zugängliche Daten, sondern auch Daten von Auskunfteien und Datenhändlerinnen mit einschliessen. Damit wird plötzlich nicht mehr nur der Lebenslauf, sondern auch die private Lebensgestaltung zum Gegenstand einer Bewerbung. Würden solche Verfahren zum Standard, bedeutet dies, dass Arbeitnehmende sich mit einem nie enden wollenden Bewerbungsprozess zur Evaluierung ihrer ökonomischen Verwertbarkeit konfrontiert sähen.

Wenn Menschen anhand von Merkmalen in Schubladen sortiert werden, ist dies immer auch mit Risiken in Bezug auf Diskriminierung behaftet. Abseits der offensichtlichen moralischen und grundrechtlichen Fragen ist ein zentrales Problem derartiger Verfahren, dass die Grenze zwischen Wahrheit und Wahrscheinlichkeit verschwimmt. Eine Korrelation, also ein statistisches Zusammenfallen zweier Merkmale, wird innerhalb derartiger Herangehensweisen häufig wie eine Kausalität behandelt. Und ob die Datengrundlage für derartige Schlüsse wirklich valide ist, wird selten geprüft. Eine derartige Logik findet sich nicht nur bei vermeintlich innovativen Bewerbungsverfahren. Mag sein, dass Hobbyköche mit einer Vorliebe für Fenchel eine grössere Wahrscheinlichkeit haben, eine Hausratsversicherung weniger in Anspruch zu nehmen. Aber sollte dies rechtfertigen, Menschen mit anderen Ernährungsvorlieben weniger Rabatte anzubieten? Ist es gerecht, die Kreditwürdigkeit von Nutzerinnen des chinesischen Sesame-Credit Scortingdienstes aufgrund einer Vorliebe für Online-Games herunterzustufen? Und wie legitim ist es eigentlich anzunehmen, dass die täglich absolvierte Schrittzahl einer Krankenversicherung Auskunft darüber geben kann, ob ein Mensch sich um sein körperliches Wohlbefinden sorgt? Je umfassender der Datensatz ist, der bei einem solchen Optimierungsansatz zu Rate gezogen wird, desto umfassender ist auch der Druck, in bestimmte Schubladen zu passen. Und zwar unabhängig davon, wie absurd die Schubladen sind.

Kürzlich sorgte eine Meldung über ein Patent im Besitz des Unternehmens Airbnb für heftige Diskussionen. Mithilfe der automatisierten Analyse von Online-Aktivitäten soll die vermeintliche «Vertrauenswürdigkeit» von Usern gemessen werden können. Ziel sei es dabei, Hinweise auf negative Persönlichkeitsmerkmale wie Narzissmus und psychopathische Charakterzüge zu finden. Nun ist es natürlich so, dass sich in der Liste der angemeldeten Patente der meisten grossen Tech-Konzerne zahlreiche fragwürdige Ideen finden – viele davon werden nie umgesetzt. Gleichwohl hatte Airbnb in der Vergangenheit wiederholt mit Beschwerden von KundInnen zu kämpfen, die von ihren GastgeberInnen massiv belästigt wurden. Eine Software könnte eine günstige Methode sein, dieses Problem anzugehen. Doch bedeutet eine solche Software wirklich, dass Gemeingefährliche und Psychopathen treffsicher ausgesiebt werden könnten? «Nein», sagt die IT-Expertin Frederike Kaltheuner. «Es heisst lediglich, dass Airbnb alle seine Nutzer anhand einer Skala für Psychopathen bewertet.» Neue Formen von Diskriminierung sind hier unvermeidbar. Wie würde eine solche Software das Nutzerverhalten von beispielsweise Autisten oder Künstlerinnen bewerten, die sich womöglich ganz anders als der Durchschnitt ausdrücken? Und: Wie würde sich dies auf den demokratischen Diskurs im Netz auswirken, wenn wir Gefahr laufen würden, für bestimmtes Verhalten plötzlich umfassend durch die freie Wirtschaft abgestraft zu werden? Eine Zukunft, in der nicht etwa eine Psychologin mit unserer Einwilligung unseren Geisteszustand prüft, sondern jedes beliebige Unternehmen, erscheint wenig verlockend. Es wäre eine wahr gewordene Dystopie.

Gerade in Bezug auf den Einsatz von Software im staatlichen Sektor täten wir gut daran, die zugrunde liegenden Annahmen hinter so mancher softwarebasierten Dienstleistung kritisch zu hinterfragen. Das gilt insbesondere für die Bereiche Strafverfolgung und Justiz. In mehreren US-Bundesstaaten können Richter bereits heute auf Software zurückgreifen, die anhand «objektiver Kriterien» ein «angemessenes» Strafmass vorschlägt. Die damit verbundene Hoffnung ist, dass Urteile dadurch gerechter werden. Untersuchungen haben nämlich gezeigt, dass das von Richtern und Richterinnen verhängte Strafmass oft von irrationalen Faktoren beeinflusst wird. Etwa, ob ein Fall kurz vor der Mittagspause verhandelt wurde und welches Geschlecht die Kinder des jeweiligen Richters haben. Die Intention zum Einsatz entsprechender Software ist daher durchaus nachvollziehbar.

Schwierig wird es allerdings, wenn man sich anschaut, wie einzelne Unternehmen ihre entsprechenden Lösungsangebote für dieses Problem konkret ausgestaltet haben. Wissenschaftliche Untersuchungen deuten darauf hin, dass Straftäter mit niedrigem Einkommen ein höheres Risiko aufweisen, erneut eine Straftat zu begehen. Aber rechtfertigt dies, dass eine softwarebasierte Entscheidungshilfe für US-Richter laut Recherchen von Bürgerrechtsorganisationen höchstwahrscheinlich auch sozioökonomische Faktoren mit einbezieht und darauf basierend bei bestimmten Fällen ein höheres Strafmass zwecks «Abschreckung» vorschlägt? Arm zu sein ist schliesslich kein Verbrechen.

Der Versuch der Beseitigung der einen Ungerechtigkeit droht somit neue Formen der Diskriminierung zu schaffen. Bei einem Gesetz kann schwarz auf weiss nachgelesen werden, was Recht und was Unrecht ist. Sowohl staatliche Stellen als auch Unternehmen sind allerdings äusserst zurückhaltend bei der Preisgabe von Informationen über die Kriterien, nach denen derartige Algorithmen Angeklagte beurteilen. Zahlreiche Hersteller entsprechender Systeme berufen sich auf ihr Geschäftsgeheimnis. Die softwaregestützte Urteilsverkündung gleicht somit einer BlackBox.

Die Vision, dass mit dem Einzug von technischen Entscheidungssystemen in immer mehr Bereichen unserer Gesellschaft neue Formen von Diskriminierung drohen, ist mitnichten ein dystopisches Schreckgespenst. Diese Entwicklung ist in vollem Gange. Längst gibt es eine ganze Reihe von Anbietern, die für die «Optimierung» jedes vermeintlichen Problems eine «objektive» softwaregestützte Lösung zur Hand haben. Wir wären gut beraten, derartige Heilsversprechen nicht vorschnell für bare Münze zu nehmen. Vielmehr müssen wir uns die grundsätzliche Frage stellen: In welchen Bereichen wollen wir überhaupt Technik einsetzen? Welche Möglichkeiten brauchen Betroffene, um Diskriminierung sowohl zu erkennen als auch um sich dagegen zur Wehr zu setzen? Wie müssen gerechte Regeln in Bezug auf Transparenz, Haftung und Nachvollziehbarkeit aussehen, damit sie mit unserem Wertesystem vereinbar sind? Das Problem an diesem ganzen Themenkomplex ist: Wenn wir als Zivilgesellschaft diese Fragen nicht in den nächsten Jahren beantworten, werden es andere für uns tun. Derartig fundamentale Entscheidungen der unsichtbaren Hand des Marktes zu überlassen wäre ein kolossaler Fehler. Denn der Markt regelt alles mögliche, aber er gibt sicherlich keine Antwort darauf, wie eine lebenswerte Welt im digitalen Zeitalter aussehen kann.

Von Katharina Nocun

Katharina Nocun ist Autorin und Bürgerrechtlerin. Sie bloggt unter kattascha.de, betreibt den Denkangebot Podcast und ist in Deutschland an mehreren Verfassungsbeschwerden zum Thema staatliche Datensammlungen beteiligt. Ihr Buch ‹Die Daten, die ich rief› erschien 2018 bei Lübbe.

WE VALUE YOUR PRIVACY

EIN UPDATE FÜR DIE DEMOKRATIE

Die Explosion des Meinens im Netz bedeutet einen Stresstest für die Demokratie. Wie eine digitale Demokratie funktionieren kann, zeigt eine Initiative aus Taiwan.

Mit dem World Wide Web war einst die Utopie einer herrschaftsfreien Kommunikation verbunden, einer globalen Cyber-Agora, in der Ideen frei flottieren und alle ungehindert ihre Meinungen zu Markte tragen können. Noch 1996 schrieb der Internetpionier John Perry Barlow in seiner «Unabhängigkeitserklärung des Cyberspace» an die «Regierungen der industriellen Welt, ihr müden Giganten aus Fleisch und Stahl»: «Ich komme aus dem Cyberspace, der neuen Heimat des Geistes. Im Namen der Zukunft bitte ich Euch, Vertreter einer vergangenen Zeit: Lasst uns in Ruhe! Ihr seid bei uns nicht willkommen. Wo wir uns versammeln, besitzt Ihr keine Macht mehr.»

Allein, diese Hoffnungen sind zerstoben. Autoritäre Regime zensieren das Netz und errichten elektronische Sperrzäune, Troll-Fabriken verbreiten Fake-News, Hasskommentare vergiften das diskursive Klima, Meinungsroboter torpedieren ganze Wahlkämpfe. Soziale Netzwerke und die zugrunde liegende Algorithmentechnik haben zu einer beispiellosen Polarisierung der Gesellschaft geführt. Noch nie war der Ton so rau wie heute. Das Internet, so der einhellige Befund, ist kaputt und muss repariert werden. Nur wie?

Das Problem ist nicht nur, dass die bürgerliche Öffentlichkeit das Transparenzgebot gegenüber Black-Box-Algorithmen nicht einfordern kann, sondern auch, dass die Öffnung politischer Foren durch soziale Netzwerke die Demokratie enorm unter Druck setzt. Pro Minute werden eine halbe Million Facebook-Kommentare abgesetzt. Diese Datenmenge kann das politische System kaum verarbeiten. Die Folge: Die Responsivität schwindet, die Systemperformanz leidet. Die sich beschleunigenden Ereignisströme vermitteln den für die Demokratie fatalen Eindruck, dass die Politik ihre Aufgaben nicht erledigt und den Wählerwillen ignoriert, was letztlich auch dem globalen Populismus Vorschub leistet.

Die Politik hat das revolutionäre Potenzial des Internets und seiner Vehikel, der Smartphones, unterschätzt – und das nicht nur, weil alle mit einer Handy-Kamera herumlaufen und Skandale publik machen können. Auch hat die Klickhaftigkeit des Mediums und seiner Bedienelemente die Illusion erzeugt, dass gesellschaftliche Veränderungen per Knopfdruck herbeigeführt werden könnten. Zwischen den Zyklen des Internets und der Demokratie klafft ein eklatantes Missverhältnis. Man kann im Netz sekündlich seine Stimme abgeben, aber nur alle paar Jahre oder Monate (in einem direktdemokratischen System wie der Schweiz) auf dem Wahlzettel. Diese Desynchronisation von Stimmungen und Stimme verfestigt ein Gefühl, dass sich die Welt immer schneller dreht, aber politisch alles stillsteht. Womöglich ist das Phänomen Donald Trump, der mithilfe von Computerbefehlen auf Twitter und dem Gehorsamsprinzip der Followerschaft eine neue Form der Echtzeit-Herrschaft begründet hat, genau auf diese Zeitkrise der Demokratie zurückzuführen.

Der Vorwurf, den einige Internetaktivistinnen und Libertäre der Demokratie machen, ist, dass ihre Institutionen veraltet seien und mit ihrer tradierten Informationstechnologie nicht auf die rasanten Entwicklungen der Technik reagieren könnten.

Das Argument ist nicht ganz von der Hand zu weisen: Die Wahlperioden stammen noch aus einer analogen Zeit, in der man morgens die Zeitung las, mittags Radio hörte und abends die Nachrichten im Fernsehen schaute. Dazwischen passierte ausser dem üblichen Politikbetrieb von Gremiensitzungen und Plenardebatten nicht viel. Es gab keine twitternden Präsidenten und keine Hasskommentare im Netz. Natürlich gab es den Hass, der heute öffentlich im Netz überquillt, auch vor 30 oder 50 Jahren schon, er wurde nur eben in «nicht-öffentlichen» Sitzungen am Stammtisch ventiliert. Diese Ressentiments, die sich in der Wahl von extremen Parteien artikulierten, waren auch damals ein Problem, aber zumindest keines, auf das binnen weniger Minuten in einem Tweet reagiert werden musste. Sie waren auch nicht in dem Ausmass wahrnehmbar, weil die Filterblasen der Gesellschaft damals noch intakt(er) waren. Das politische System war vor allem durch die grosse Verzögerungszeit der Medien ein recht überschaubarer Raum, in dem in einem geordneten und für alle nachvollziehbaren Verfahren Interessen ausgehandelt wurden.

Durch die Digitalisierung und damit einhergehende Verkürzung der Latenzzeiten ist dieser politische Raum jedoch überfüllt. Im Sekundentakt prasseln Forderungen auf das politische System ein, die dort wie nicht abgeholte Pakete herumstehen. Ein Parteimitglied setzt einen Tweet ab, der die Reaktion eines Hinterbänklers provoziert, der sonst weder auf dem Parteitag noch in den Abendnachrichten zu Wort gekommen wäre, was wiederum die Ministerin zu einer Stellungnahme nötigt und, angeheizt durch algorithmische Feedbacksystem, eine nicht mehr enden wollende Informationskaskade in Gang setzt. Daten sind die Treiber des politischen Systems, dessen Repräsentanten wie Getriebene agieren. Überall heisst es, die Politik müsse «liefern», als wäre Politik ein Bestellservice à la Amazon, wo die Ware per Knopfdruck an die Haustür geliefert kommt. Die soziale Kompression dampft den (Spiel-)Raum des Politischen immer weiter ein.

Für den israelischen Historiker Yuval Noah Harari ist die Demokratie ein Datenverarbeitungssystem, das im Informationszeitalter gegenüber der Diktatur einen entscheidenden Wettbewerbsnachteil habe: «Da sowohl Menge als auch Geschwindigkeit der Daten zunehmen, könnten altehrwürdige Institutionen wie Wahlen, Parteien und Parlamente obsolet werden – nicht weil sie unmoralisch wären, sondern weil sie Daten nicht effizient genug verarbeiten können», schreibt Harari in seinem 2015 erschienenen Buch ‹Homo Deus›.

Gewiss ist es verkürzend, Demokratien auf ein Datenverarbeitungssystem zu reduzieren, weil sie nicht nur Daten, sondern auch Ideen «verarbeiten» und produzieren. Und natürlich kann Geschwindigkeit kein Kriterium der Legitimität sein, weil demokratische Prozesse Raum und Zeit benötigen. Doch die gigantische Datenmenge stellt die Problemlösungsfähigkeit demokratischer Systeme auf eine Belastungsprobe. Informationstheoretisch gibt es zwei Optionen: Entweder die Datenmenge wird durch Internetsperren oder Account-Löschungen reduziert, was autoritär wäre. Oder man versucht, sie zu bearbeiten.

Unter dem Motto «Reboot Democracy» läuft in Taiwan seit einigen Jahren ein interessantes Demokratieexperiment. Nachdem die Sonnenblumen-Bewegung 2014 gegen das geplante Handelsabkommen mit China demonstrierte, lud die Regierung in Taipeh Aktivistinnen und Hacker der Gruppe «Gov Zero» (unter anderem die spätere Digitalministerin Audrey Tang) ein, ein Online-Konsultationsverfahren zu entwickeln.

Der Grundgedanke der Hacker war, dass periodische stattfindende Wahlen nicht genügend Informationen an die Regierung übermitteln. Die direkte Demokratie in Form von Plebisziten würde die Gesellschaft spalten, das Internet erzeuge zu viel Lärm und statistisches Rauschen, als dass sich daraus Präferenzen ableiten liessen. Also bräuchte es ein neues, webbasiertes Verfahren, das Entscheidungsprozesse und die Rückkopplung an den Souverän optimiert.

Die Hacker entwickelten eine Open-Source-Plattform namens vTaiwan, auf der User über Gesetzesinitiativen debattieren können. In einem vierstufigen Prozess werden zunächst Probleme (wie zum Beispiel die Nutzung von Segways auf öffentlichen Strassen) diskutiert und Lösungsvorschläge eingebracht. Im zweiten Verfahrensschritt, der sogenannten «Opinion Stage», werden mithilfe eines Algorithmus die Kommentare der Diskussionsteilnehmenden, die mit Zustimmung, Ablehnung oder Enthaltung reagieren können, geclustert und in sogenannten «Meinungslandschaften» visualisiert. Man sieht also den Standpunkt der User auf einer politischen Landkarte (das dazugehörige Tool pol.is kommt auch bei Willensbildungsprozessen in anderen Organisationen wie etwa Universitäten zum Einsatz). In der dritten Stufe findet eine öffentliche Anhörung der beteiligten Akteure (etwa Lobbyvertreter) statt, die im Netz live gestreamt wird und kommentiert werden kann. Im vierten Schritt, der Ratifikationsphase, werden die Vorschläge schliesslich in eine Gesetzesinitiative gegossen und dem Parlament zugeleitet.

Das Besondere an der Online-Petitionsplattform ist, dass sie nicht nur konsultativen, sondern obligatorischen Charakter hat: Seit 2017 ist jedes Ministerium verpflichtet, einen Bürgerbeteiligungsbeauftragten zu bestellen, der den Gesetzgebungsprozess begleitet. Die Online-Plattform fungiert wie eine Art politische Kammer. Mittlerweile sind 26 nationale Gesetze auf vTaiwan angestossen worden. Als Musterbeispiel gilt die Abstimmung über die Zulassung des Fahrdienstleisters Uber, wo es über die Webkonsultation gelang, einen Konsens zwischen Befürworterinnen und Gegnern herzustellen.

Es gab ja schon einige Experimente in Sachen digitaler Demokratie, wie die gescheiterte Crowdsourcing-Verfassung in Island, wo Mitglieder des Verfassungsrats Entwürfe auf einer Webseite posteten, die von der Community kommentiert werden konnten. In Mexico City hat das Stadtparlament 2016 einen crowdgesourcten Verfassungsentwurf ratifiziert. Und in der Schweiz hat der Netzaktivist Daniel Graf im gleichen Jahr die Online-Plattform Wecollect lanciert, die es BürgerInnen ermöglichen soll, sich aktiver in politische Prozesse einzuschalten.

Das Konzept der Liquid Democracy als einer deliberativen Demokratieform gilt seit dem Niedergang der Piratenpartei in Deutschland als gescheitert, nicht zuletzt, weil die Beteiligung viel zu gering war und der Leitgedanke des Delegated Voting durch die Delegation von Wertentscheidungen an Algorithmen konterkariert wurde. Bei der Uber-Debatte auf vTaiwan stimmten lediglich 31.000 BürgerInnen ab (was bei 19 Millionen Wahlberechtigten einer Wahlbeteiligung von 0,16 Prozent entspricht).

Die niedrige Wahlbeteiligung war schon immer die Achillesferse der Demokratie, und die mangelnde Input-Legitimation könnte sich auch für das digitale Demokratiemodell als problematisch erweisen, zumal es weniger technologieaffine Wählende oder solche ohne Internet a priori ausschliesst. Die flüssige Demokratie muss sich daher den Vorwurf gefallen lassen, dass sie letztlich das Projekt einer Tech-Elite ist.

Die Diskussionsplattform in Taiwan könnte dennoch zur Blaupause einer digitalen Demokratie werden, weil sie den opaken algorithmischen Prozeduren auf Facebook oder Twitter ein offenes und vor allem transparentes Modell der Interessenaggregation entgegenstellt, das nicht auf maximalen Profit und «user engagement», sondern auf Konsens ausgerichtet ist. Wenn es stimmt, dass Wahlen in demokratischen Systemen nicht mehr als Transmissionsriemen geeignet sind, um politische Präferenzen in Mandate bzw. Mehrheitsverhältnisse zu übersetzen, dann bräuchte es möglicherweise alternative, datengestützte Partizipationsmodi wie eine Debattenplattform, deren Ergebnisse in den politischen Prozess eingespeist werden.

Wir müssen nur Sorge tragen, dass diese Feedbackschleifen nicht auf eine politische Kybernetik bzw. algorithmische Regulierung hinauslaufen, die etwa mit dem Bau von Smart Citys implementiert wird: Das Geschwindigkeitslimit wird automatisch an das Wetter und Verkehrsaufkommen angepasst, und die smarte Mülltonne meldet von selbst, wenn sie voll ist. Dieser Teilautomation von Städten liegt ja auch der Gedanke einer postpolitischen bzw. postideologischen Form des Regierens zugrunde, wo es keine Proteste mehr gibt, sondern bloss noch Störungen. Die Demokratie muss nicht reibungslos wie eine gut geölte Politikmaschine funktionieren. Aber sie muss dort, wo Reibungen entstehen, institutionalisierte Verfahren anbieten.

Von Adrian Lobe

Adrian Lobe ist Politikwissenschaftler und freier Publizist. Vor kurzem erschien sein Buch ‹Speichern und Strafen. Die Gesellschaft im Datengefängnis› bei C.H. Beck.

MIT E-VOTING ZUR ENTERTAINMENT-DEMOKRATIE

Demokratische Entscheide werden in der Schweiz werden traditionsgemäss breit akzeptiert. Das Vertrauen in die Verfahren ist gross und Resultate sind nachvollziehbar. Aber mit der elektronischen Stimmabgabe wird die Schweizer Demokratie zum Spielfeld für Manipulationen und Hackerangriffe.

Ein Blick zurück

Grundsätzlich war E-Voting als technische Modernisierung angedacht, eine Option, um die Demokratie unmittelbarer, dynamischer und intensiver zu gestalten. Politikerinnen, Behörden und Firmen versuchen uns deshalb das elektronische Abstimmen schmackhaft zu machen. Scheinbar sei E-Voting schneller, günstiger, mobiler und besser. Es wird behauptet, mit E-Voting steige die Stimmbeteiligung, JungbürgerInnen werden besser mobilisiert. Dank toller Technik werden Bevölkerungs-Gruppen wie Sehbehinderte oder Auslandschweizerinnen besser einbezogen. Deshalb hat E-Voting sogar heute noch viele Anhänger.

Der Bund hat vor rund 20 Jahren ein Projekt gestartet, unsere Schweizer Demokratie um diesen dritten, elektronischen Stimmkanal zu erweitern. Seither wurden gesetzliche Grundlagen erarbeitet, Testbetriebe bewilligt, Systeme geprüft und die Anforderungen verschärft.

2015 gab es den ersten grossen Rückschlag: Das E-Voting-System von neun Kantonen wurde eingestampft, weil eine Lücke beim Schutz der Stimmgeheimnisses entdeckt wurde. 2018 schaltete auch der Kanton Genf sein System CHvote ab. Damit verblieb nur noch ein System der Post, das vom spanischen Anbieter Scytl S.A. entwickelt wurde, der auch noch in US-amerikanischer Hand ist. Dieses E-Voting System ist also in etwa so schweizerisch, wie wenn man auf chinesische Schoggi ein Schweizer Wappen kleben würde.

Der Post-demokratische GAU

Die Post nutzte diese Chance aufs Monopol und musste gemäss gesetzlichen Vorgaben den Quellcode offenlegen. Ein sogenannter Intrusionstest sollte Anfang 2019 die Sicherheit des Post-Scytl-Systems bestätigen. Die abstrusen Rahmenbedingungen dazu stiessen aber auf Ablehnung: Nur mittels Registrierung wurde sehr restriktiv Zugang zum Source-Code gewährt. Entdeckte Fehler durften nicht öffentlich publiziert werden. Alle klassischen Manipulations-Möglichkeiten wurden explizit verboten. Bekannte Hacker und Security-Firmen kanzelten diesen Intrusionstest deshalb als reinen PR-Gag ab und nahmen gar nicht erst teil. Eine Farce… bis zum Tag, als der Code als Kopie im Internet auftauchte. Expertinnen konnten sich nun ohne Registrierung Einblick verschaffen. Sofort gab es Meldungen über schlechte Code-Qualität und mangelhafte Kryptografie. Kurz darauf waren komplette Anleitungen vorhanden, die Fehler und Manipulationsmöglichkeiten dokumentierten. Eine besonders schwerwiegende Sicherheitslücke war Scytl und der Post scheinbar seit 2017 bekannt. Diese wurde aber nie behoben und danach auch bei Audits durch die KPMG oder von verantwortlichen Behörden nie entdeckt. Alle beteiligten Instanzen hatten massiv versagt.

Als Erkenntnis bleibt: E-Voting funktioniert (noch) nicht, auch wenn behauptet wird, die perfekte Software werde in Kürze fertiggestellt. Wir warten also weiter und werden noch viele Sicherheitslücken erleben.

Eine technisch-demokratische Rundumschau

Unter dem Begriff E-Voting wird heute primär die Form der Mausklick-Demokratie beschrieben: Durch Anwendungen auf privaten Computern, Tablets oder Smartphones sollen die Bürgerinnen ihre Stimme abgeben. Dazu sind mehrere Probleme zu lösen.

Knackpunkt Stimmgeheimnis: Im Bundesgesetz über die politischen Rechte steht: Das Stimmgeheimnis ist zu wahren. Zum einen soll also jede Stimme anonym abgegeben werden können und zum anderen ist keine Behörde oder Person befugt, ein Stimmverhalten zu ermitteln. Das ist auch der grosse Unterschied zum E-Banking, welches gerne als Vergleich herangezogen wird. Aber: Die Bank darf und muss den Kontostand wissen. Im Gegensatz dazu soll beim E-Voting jeder Bürger frei von Zwang entscheiden und ohne Konsequenzen auch für unpopuläre Anliegen einstehen können, sozusagen als Grundvoraussetzung für freie und faire Entscheide. Beim E-Voting ist das Stimmgeheimnis jedoch ein komplexes Problem: Hackerinnen zeigten 2018 auf, wie das Abstimmungsverhalten an Computern problemlos überwacht oder manipuliert werden kann. Und 2019 zeigten Doktoranden der ETH Zürich auf, wie elektronischer Stimmenhandel im grossen Stil möglich ist und E-Votes über eine Börse den Meistbietenden verkauft werden können.

Knackpunkt Vertrauen in Prozesse und Resultate: Papierwahlverfahren sind einfach und transparent: Stimmrechtsausweise werden getrennt von den Stimmzetteln eingereicht, Urnen werden in breit abgestützten Gremien gemeinsam geöffnet, ebenso die Stimmen gezählt, und es gibt viele und sehr simple Kontrollmechanismen, die allgemein verständlich sind.

Manipulationen in einzelnen Stimmlokalen können mittels statistischer Verfahren relativ einfach erkannt werden, und um eine Wahl massgeblich zu fälschen, müssten viele Personen in zahlreichen Stimmlokalen gemeinsam manipulieren. Beim E-Voting wäre das viel einfacher, es könnte sogar nur eine Einzelperson erfolgreich eine Abstimmung fälschen.

Auch die Anwendung und Kontrolle ist für die Stimmbürgerin viel komplizierter: Die Stimmrechte und Antwortmöglichkeiten werden als Codes generiert. Speziell vertrauenswürdige und abgesicherte Druckereien müssen diese Codes mit Sicherheitsmerkmalen oder Rubbelfeldern auf die Abstimmungsunterlagen aufbringen. Der Stimm-

Sogenannte Smart Devices verbreiten sich rasant in unserem Alltag. Die dafür notwendige Technik, die Sensoren und Kameras sind mittlerweile so klein und günstig, dass sich diese in zahlreichen Geräten unterbringen lassen. So werden in verschiedenen Städten Werbedisplays (SEITE 12) getestet, die Besucherströme messen oder Werbung adaptiv auf eine Zielgruppe anzeigen können. Letztes Jahr stattete der Autobauer Tesla seine Fahrzeuge per Software-Update mit einem Diebstahlmodus aus, der alle verfügbaren Sensoren inkl. Kameras für die Überwachung der Fahrzeugumgebung einsetzt. Ob und inwiefern solche Kameras in digitalen Werbedisplays oder Diebstahlsicherungen wie Teslas Sentry Mode (SEITEN 6–7) dabei die Grenze der Privatsphäre überschreiten, hängt dabei zum einen von den jeweiligen Gesetzen ab. Doch auch wenn eine Verletzung der Privatsphäre vorliegt, ist diese für die Betroffenen oft nicht oder nur schwer ersichtlich. In der Schweiz liegt eine Verletzung am Recht am eigenen Bild dann vor, wenn jemand ohne seine Zustimmung um seiner Person willen fotografiert oder gefilmt wird. Artikel 10 der Schweizerischen Bundesverfassung garantiert jedem Menschen das Recht auf persönliche Freiheit, insbesondere auf körperliche und geistige Unversehrtheit und Bewegungsfreiheit. Doch mit der Frage, wie sich die Individuen diese Unversehrtheit in digitalen Belangen – sowohl im öffentlichen Raum wie auch im Digitalen – bewahren können, bleiben sie meist sich selbst überlassen. Wie sich die eigene Identität schützen und ausweisen lässt, ist eine Frage, die mit der zunehmenden Transformation im Rahmen der Digitalisierung immer dringlicher wird. Einen doppeldeutigen Umgang dafür hat die Produktdesignerin Danielle Baskin mit den von ihr kürzlich vorgeschlagenen N95 Atemschutzmasken gefunden (seite 1), auf die man sein eigenes Gesicht aufdrucken lassen kann. Ob sich damit nach wie vor das Smartphone entsperren lässt oder ob sie letzten Endes eine günstige Möglichkeit sein könnte, der Überwachung im öffentlichen Raum zu entkommen, wird wohl offen bleiben.

bürger muss zahlreiche solcher Codes korrekt abtippen und eventuell noch mit Prüfcodes abgleichen. Ein einfaches Abstimmungs-Ja-Nein führt somit locker zu 20–30 Buchstaben-Zahlen-Kombinationen. Die E-Voting-Server speichern und bewerten danach das Ganze, sogenannt «universell und individuell verifizierbar». Und irgendein Resultat erscheint auf einem Bildschirm.

Die verwendete Mathematik für die Kryptografie füllt ein ganzes Studium, hinzu kommt, dass diese Mathematik auch noch in Computeralgorithmen übertragen werden muss. Diese Fähigkeiten werden die wenigsten mitbringen, wenn es überhaupt jemanden gibt, der so ein System in seiner Gänze überblicken und verstehen kann. Darüber hinaus bleiben auch noch das Internet und die Geräte der Endnutzer als grosser Unsicherheitsfaktor.

Knackpunkte Hardware & Software: Diese Elemente können grundsätzlich als unsicher angesehen werden. Jedes elektronische Gerät bekommt heutzutage regelmässig Updates, meistens Fehlerkorrekturen. Konstruktionsfehler gibt es immer, auch beim Programmieren. Der Kern der E-Voting Applikation der Post besteht aus über 275'000 Zeilen Code. Dazu kommen Code-Bibliotheken, Compiler, Betriebssysteme, Gerätetreiber, Hardware und viele weitere Geräte. Selbst Mikroprozessoren haben kritische Fehler, welche nie mehr repariert werden können (siehe Spectre / Meltdown).

Somit sind alle eingesetzten Komponenten beim E-Voting potentiellen Sicherheitslücken ausgesetzt: Vom Kernsystem über die Druckerei, zum privaten Computer bis zum Stimmausschuss. Jeder Schwachpunkt kann genutzt werden, um Stimmen zu sammeln, zu überwachen oder zu manipulieren, teilweise frei skalierbar über zehntausende Stimmen mit nur einem Klick – von einer einzelnen Person.
Jede Infrastruktur ist ein beliebtes Ziel von Hackern. Im Januar 2020 wurden tausende Firmen und Gemeindeverwaltungen teilweise lahmgelegt, weil Angriffstools für die stark verbreitete Citrix-Software im Umlauf waren. Damit hätten Hackerinnen problemlos Stimmrechte oder Stimmresultate manipulieren können. Eine grössere Gefahr geht von kriminellen Organisationen oder Geheimdiensten aus: Backdoors in Geräten gehören heute zum Standard: So werden die weit verbreiteten Cisco-Router immer wieder mit Spionage-Lücken der amerikanischen Geheimdienste versehen. Und kürzlich wurde bekannt, dass der Schweizer Chiffriergeräte-Hersteller Crypto AG vor Jahrzehnten von Geheimdiensten aufgekauft wurde, die ihre Geräte systematisch mit Überwachungsmöglichkeiten ausrüsteten. Andere Staaten können ein grosses Interesse haben, wie Abstimmungen in der Schweiz ausgehen, z.B. bei Kampfflugzeugen mit Milliarden-Kosten. Das macht unser E-Voting zu einem interessanten Ziel.

Gemäss den Snowden-Enthüllungen schrieb die NSA in einem Strategiepapier schon vor Jahren: «activities such as ... e-voting ... beg to be mined», also in etwa: «E-Voting bettelt geradezu darum, ausgebeutet zu werden». E-Voting ist also nicht sicher, auch wenn Kryptografie-Expertinnen rein theoretisch sichere Lösungen entworfen haben. Es scheitert an der Umsetzung, und eine akzeptable Balance zwischen Sicherheit, Benutzerfreundlichkeit und Kosten ist nicht herzustellen.

Abwiegeln, verharmlosen, ignorieren

Obwohl die Anforderungen an sichere und nachvollziehbare Abstimmungen und Wahlen relativ klar sind, erleben wir seit Jahren eine Art der Kommunikation durch Systembetreiber und Behörden, die unserer Demokratie nicht würdig ist. Dazu einige Beispiele:

Als im Jahr 2015 Joël Boissard vom Westschweizer Fernsehen aufzeigte, wie er mit E-Voting zweimal abstimmen konnte, wurde er verklagt und verurteilt, obwohl er den Fehler umgehend der Staatskanzlei gemeldet hatte. Als der Entscheid gefällt wurde, dass das erste E-Voting System Consortium wegen der Gefährdung des Stimmgeheimnisses nicht mehr verwendet werden durfte, war die Begründung klar und nachvollziehbar. Doch anstatt einer kritischen Betrachtung und Debatte durch Kantone und Medien kam der Aufschrei «Bundesrat lehnt Einsatz von E-Voting bei Nationalratswahlen ab» und die Kantone nannten den Beschluss einen «deutlichen Rückschlag».

Als 2018 Hacker des Chaos Computer Club im Schweizer Fernsehen eine Manipulationsmöglichkeit aufzeigten, mit der Wählerinnen auf eine gefälschte E-Voting-Website umgeleitet wurden, klagte die Staatskanzlei Genf gegen die Urheber wegen Verstosses gegen das Wappenschutzgesetz.

Allen Vorfällen gemein war jeweils die Reaktion von Herstellern, Behörden und andere Verantwortlichen: Abwiegeln, verharmlosen, ignorieren und teilweise den Rechtsweg beschreiten, um die Überbringer der schlechten Botschaft mundtot zu machen.

Als dann im Frühjahr 2019 mehrere äusserst gravierende Sicherheitslücken im Post-Scytl-System gefunden wurden, drittete die Kommunikation der Verantwortlichen ins Absurde ab: Zuerst wurden die externen Sicherheitsexperten diskreditiert, danach die Fehler kleingeredet. Und als der Bund die Bewilligung entzog, hiess es lapidar: «Die Post setzt ihr E-Voting-System befristet aus.» Gleichzeitig begann die Post mit der nächsten PR-Offensive und versprach den Kantonen innert wenigen Monaten ein neues System aufzubauen, was schlicht unmöglich, unglaubwürdig und unseriös war. Unterdessen spricht die Post vom Jahr 2021 für die nächste Version. Die Behörden kommunizieren immer noch, dass bereits hunderte E-Voting-Versuche stattgefunden haben, erfolgreich und fehlerfrei, obwohl ein essentieller Fehler im Post-System bereits seit 2016 vorhanden war!

Seit Beginn des E-Voting Testbetriebs heisst es immer wieder, Sicherheit komme vor Tempo. Doch die warnenden Stimmen, zahlreichen Fehler und Rückschläge hielten den Bundesrat nicht davon ab, im Jahr 2019 eine Vernehmlassung zu starten, um den E-Voting-Testbetrieb in den ordentlichen Betrieb zu überführen. Dieses ignorante Vorgehen zeigt, dass E-Voting und insbesondere die Abläufe und vor allem die beteiligten Gruppen bis heute nicht vertrauenswürdig genug sind für elektronische Abstimmungen.

Glücklicherweise wurde im Frühling 2019 eine Volksinitiative für ein E-Voting-Moratorium lanciert. Der damit aufgebaute politische Druck konnte zumindest den Fahrplan des Bundesrates bremsen. Dennoch bleibt diese Initiative essentiell, um zumindest vorläufig eine sichere und vertrauenswürdige Demokratie beizubehalten. Dazu gehört unter anderem, dass sich die Stimmberechtigten ohne besondere Sachkenntnis davon überzeugen können, dass ein Abstimmungs-System sicher ist und ihr Vertrauen verdient.

Obwohl sich die Technik, Kryptografie und sogar die digitale Kompetenz laufend weiterentwickeln, ist E-Voting je länger desto weniger betriebsbereit. Wer damit spielen will, soll es tun, doch bitte nicht mit unserer Demokratie und zu diesem hohen Preis. Denn was die Behörden und insbesondere die kommerziellen Hersteller heute machen ist keine Demokratie, sondern teures Entertainment.

Von Jorgo Ananiadis

Jorgo Ananiadis ist Co-Präsident der Piratenpartei Schweiz, Mitglied der Digitalen Gesellschaft und der Internet Society und im Komitee der Volksinitiative für ein E-Voting-Moratorium.

www.e-voting-moratorium.ch

REFERENDUM GEGEN DAS E-ID-GESETZ

Es besteht Bedarf nach einer benutzbaren und vertrauenswürdigen elektronischen Identifizierung. Sie ist ein Pfeiler der digitalen Demokratie und wird auch für die Ausübung von Volksrechten zum Einsatz kommen. Wir benötigen dementsprechend eine echte digitale Erweiterung von ID, Pass und Ausländerausweis und keine E-Commerce-ID. Das E-ID-Gesetz muss den Bürgerinnen und Bürgern dienen – und nicht der Wirtschaft. Wie die Herausgabe der bereits bestehenden Ausweisdokumente muss daher auch diese öffentliche Aufgabe vom Staat wahrgenommen werden. Das Recht auf Privatsphäre – gerade im Internet – muss zudem gestärkt und darf nicht weiter ausgehöhlt werden. Das beschlossene Gesetz erfüllt dies nicht. Darum wurde erfolgreich das Referendum dagegen ergriffen.

Wozu eine E-ID?

Die BewohnerInnen der Schweiz sollen eine elektronische Identität bekommen. Speziell E-Government-Lösungen würden davon profitieren, da bis anhin jede Gemeinde und jeder Kanton sich einzeln darum kümmern muss, wie die Benutzerinnen und Benutzer auf ihren Portalen authentifiziert werden können. Eine E-ID kann auch das Abschliessen von Verträgen, bei denen eine Ausweispflicht besteht oder die eine Schriftlichkeit voraussetzen, online vereinfachen. In den meisten Fällen sind aber weder ein Ausweis noch eine Unterschrift die Voraussetzung, um Dienstleistungen nutzen oder Verträge abschliessen zu können. Dies muss auch online so bleiben. Eine staatliche E-ID muss für private Online-Portale nutzbar sein, falls solche Anforderungen zur Identifikation oder Vertragserfüllung bestehen. Beispiele dazu sind das Eröffnen eines Bankkontos oder das Abschliessen eines Mobilfunkvertrags. Es ist aber kein Gesetz nötig, das ein universelles Login schafft, welches auf möglichst vielen Websites funktioniert.

Eine E-ID muss dementsprechend in erster Linie sicher und vertrauenswürdig sein, und jeder Mensch in der Schweiz soll ein Anrecht darauf haben. Es darf jedoch keinen Zwang zu einer generellen Verwendung auf Internetportalen geben. Auch wenn die E-ID gegenwärtig kein international anerkanntes Reisedokument ist, übernimmt sie online dieselbe Funktion, wie es ein amtlicher Ausweis beim Abholen von eingeschriebenen Briefen, der Bescheinigung des Alters beim Kauf von Spirituosen und beim Bezug eines Betreibungsregisterauszugs tut. Die E-ID ist das elektronische Äquivalent zur Identitätskarte und keine E-Commerce-ID. Es geht hier um die digitale Erweiterung von Ausländerausweis, ID und Pass.

Das E-ID-Gesetz

Die Pläne des Bundes sind aber anders: Die staatliche E-ID soll von Privaten herausgegeben werden. Nicht etwa das Passbüro oder die Gemeindekanzlei wären für das Antragsverfahren zuständig, sondern vielmehr soll zwischen verschiedenen privaten Anbietern gewählt werden können. Leider sieht das beschlossene E-ID-Gesetz zudem keine elektronische Unterschrift vor. Neben den verschiedenen Anbietern soll es auch verschiedene Sicherheitsstufen geben. Wobei nicht alle Anbieter alle Sicherheitsstufen anbieten müssen. Sämtliche Varianten der E-ID sollen rein online beantragt werden können, wobei sich die Anforderungen leicht unterscheiden. Beim Einsatz setzt die mittlere Sicherheitsstufe dann eine Zwei-Faktor-Authentifizierung voraus. Bei der höchsten Stufe muss diese auf einem biometrischen Merkmal basieren. Typischerweise würde dies ein Fingerabdruck am Smartphone sein. Wer kein passendes Gerät hat oder einsetzen will, droht ausgeschlossen zu werden.

Herausgeber der E-ID

Das Gesetz sieht einen Markt von E-ID-Herausgebern vor. Faktisch dürfte es aber nur eine Firma geben, die E-IDs anbietet: Die SwissSign. Die ehemalige Tochtergesellschaft der Schweizer Post wurde 2017 zuerst in ein Gemeinschaftsunternehmen von Post und SBB ausgelagert. Am Digitaltag 2018 wurde dann mit viel Brimborium die Überführung in ein Joint-Venture verkündet. Dieses besteht aus 20 grossen Schweizer Konzernen, die das grosse Geschäft nicht Facebook, Google und anderen Tech-Giganten überlassen wollen und die Macht haben werden, das E-ID-Monopol erfolgreich zu verteidigen.

Die SwissSign möchte aber nicht nur E-ID-Provider sein, sondern bietet weiter ein zentrales Login für diverse Dienste, wie beispielsweise für die Medien-/Tracking-Allianz, an. So verfliessen die Grenzen zwischen amtlicher Ausweiskontrolle und simplem Anmeldevorgang auf Onlineportalen. Es ist zu erwarten, dass die einfache Verfügbarkeit eines Identitätsdienstes auf Basis der E-ID zu einer Überidentifizierung führt. Die einfache Identifizierung könnte dann für immer mehr Dienste verlangt werden, was wiederum die Verknüpfung mit anderweitig gewonnenen Profilinformationen zu einem eindeutig zuzuordnenden Persönlichkeitsprofil ermöglicht.

Dies ist nicht nur aus Sicht des Datenschutzes problematisch, sondern ergibt auch eine Art digitales Klumpenrisiko: Verliert man das eine Passwort oder wird gar der Login-Provider gehackt, sind gleich alle mit dem Login verbunden Dienste betroffen. Zudem stehen bei einem Login für E-Commerce-Anwendungen die Benutzerfreundlichkeit und nicht die Sicherheit im Zentrum. Diese beiden Anforderungen widersprechen sich. Auch kann ein Grossteil der Logins gar nicht durch eine Schweizer E-ID (und Schweizer Datensammler) abgelöst werden, da es keine internationale Lösung ist. Die Einwohnerinnen und Einwohner der Schweiz werden sich auch in Zukunft weder bei Amazon noch bei anderen internationalen Diensten mit der Schweizer E-ID anmelden können. Für ein sicheres und verteiltes allgemeines Login braucht es kein Schweizer Bundesgesetz – sondern internationale Standards.

Kurz: Gegen die internationalen Datenkraken hilft kein neues E-ID-Gesetz, sondern vielmehr griffige Datenschutzbestimmungen wie beispielsweise ein Koppelungsverbot und die internationale Durchsetzbarkeit, wie sie die EU-DSGVO kennen. Es ist zudem wichtig, dass die Interessenlage der Herausgeber und die Finanzierung der E-ID transparent sind.

Datenschutz?

Mit dem beschlossenen E-ID-Gesetz fallen an drei nennenswerten Berührungspunkten personenbezogene Daten an: Beim Bundesamt für Polizei, dem Fedpol, wird eine neue, zentrale Datenbank geschaffen. Diese wird für die Ausstellung der E-ID durch die Identitäts-Provider und für die laufende Aktualisierung der Personendaten bei den Onlinediensten verwendet, welche die E-ID zur Authentifizierung einsetzen. Das Fedpol soll die verschiedenen Personenidentifizierungsdaten aus unterschiedlichen Registern zusammenführen können.

Bei den privaten Anbietern der E-ID fallen bei jedem Login Daten an. Laut dem E-ID-Gesetz dürfen die Identitäts-Provider zwar «die Daten, die bei einer Anwendung der E-ID entstehen, und darauf basierende Nutzungsprofile» nicht kommerziell verwerten. Die Daten dürfen jedoch für sechs Monate gespeichert werden. Würde dem Prinzip der Datensparsamkeit gefolgt, wären sie hingegen unverzüglich zu löschen. Eine wirklich datenschutzfreundliche Lösung würde dem Prinzip «Privacy by Design» folgen und eine Systemarchitektur wählen, bei der diese Daten gar nicht erst bei einer zentralen Stelle anfallen. Eine angemeldete Person kann einfach und lückenlos getrackt werden. Es besteht daher die Gefahr, dass für alltägliche Vorgänge eine Anmeldung mehr und mehr nötig wird, um beispielsweise beim Stöbern im Onlineshop über einen individuellen Rabatt informiert zu werden. Der Weg zu einem gläsernen Kunden und dem personalisierten Preis ist so nicht mehr weit. Wirkungsvolle Schranken könnte auch hier erst das totalrevidierte Datenschutzgesetz bringen.

Bevölkerung möchte eine staatliche E-ID

Eine repräsentative Umfrage von Demoscope aus dem Mai 2019 zeigt, dass 87% der Bevölkerung die E-ID vom Staat beziehen wollen. Nur gerade 2% möchten die geplante E-ID von privaten Unternehmen ausgestellt erhalten. Insbesondere beim Datenschutz fehlt der Bevölkerung das Vertrauen in private Unternehmen. 81% der befragten Personen erachten zudem die rechtsverbindliche elektronische Unterschrift als wichtig. Auch die neuste repräsentative Studie der Universität Zürich hat aufgezeigt, dass rund 81% der Bevölkerung die E-ID vom Staat beziehen wollen. Diese Umfragen zeigen sehr deutlich, dass bei den gewünschten Anwendungen Behördengänge und die politische Teilhabe ganz vorne stehen. Das Ausstellen einer E-ID ist ein zentrales Element von E-Government und auch der digitalen Demokratie. Entsprechend ist es wichtig, dass diese Aufgabe vom Staat wahrgenommen wird. Der Staat darf sich nicht aus der Verantwortung stehlen. Im Gegenteil: Er muss für das nötige Vertrauen sorgen.

Im Kanton Schaffhausen ist bereits eine staatliche, smartphonebasierte E-ID erfolgreich im Einsatz. Andere Kantone wollen nachziehen.

Beglaubigte Identifikationsmerkmale und ein qualifiziertes Zertifikat für die Unterschrift könnten aber auch sicher auf ID, Pass oder Ausländerausweis gespeichert werden. So würden die amtlichen Ausweise zu Smartcards, die auch gleich als zweiter Faktor bei der Authentifizierung verwendet werden könnten. Das Hantieren mit biometrischen Merkmalen wäre nicht notwendig. Um einen gesunden Markt zu fördern, wären weiter offene Schnittstellen und Standards einzusetzen, damit – neben den Behörden für E-Government – Private die E-ID mit Einverständnis der InhaberInnen ebenfalls nutzen können.

Als Gesetzesgrundlage ist kein neues E-ID-Gesetz nötig. Es kann das bestehende Ausweisgesetz herangezogen werden: Art. 2 Abs. 2quater AwG: «Der Ausweis kann zudem elektronische Identitäten für Authentisierungs-, Signatur- und Verschlüsselungsfunktionen enthalten.» Als Kartenleser für die E-ID könnte ein Smartphone mit Funk-Schnittstelle zur Smartcard dienen. Die quelloffene AusweisApp2 bietet dies in Deutschland für den Personalausweis und den Aufenthaltstitel für nicht EU-Bürgerinnen und Bürger an.

Referendum

Gegen das beschlossene Gesetz wurde erfolgreich das Referendum ergriffen. Hinter dem E-ID-Referendum steht ein breiter Zusammenschluss von Organisationen und Netzwerken. Das sind unter anderem die Digitale Gesellschaft, die Kampagnenorganisation Campax, die Demokratie-Plattform WeCollect und der Verein PublicBeta. Unterstützt werden sie von der SP Schweiz, den Grünen und der Piratenpartei, VPOD, Internet Society Switzerland, Grundrechte.ch, dem Schweizer Seniorenrat (SSR), der Vereinigung aktiver Senioren- und Selbsthilfeorganisationen der Schweiz (VASOS) sowie engagierten Mitgliedern aus allen Parteien. Die Volksabstimmung wird voraussichtlich am 27. September 2020 stattfinden.

Von Daniel Donatsch und
Erik Schönenberger, Digitale Gesellschaft

Erik Schönenberger ist Informatiker und Geschäftsleiter der Digitalen Gesellschaft. Es setzt sich seit vielen Jahren für Freiheitsrechte in einer vernetzten Welt ein.

Die Digitale Gesellschaft ist ein gemeinnütziger und breit abgestützter Verein für Bürger- und Konsumentenschutz im digitalen Zeitalter. Die NGO setzt sich seit 2011 als zivilgesellschaftliche Organisation für eine nachhaltige, demokratische und freie Öffentlichkeit ein. Sie verteidigt die Grundrechte in einer digital vernetzten Welt.

NOW HAVE SOME COOKIES

THE RIGHT TO DIGITAL INTEGRITY OF THE HUMAN PERSON

Data protection as we have known it for the past 25 years has failed. We have lost control over our personal data. We are of course responsible of this situation. We accept using services that are designed to provide us comfort through processing and reselling our personal data that we fail to value. But when we try to use tools to protect ourselves, like anonymity tools, we are tagged as potential criminals. When we solicit assistance of the public authorities, we are often left in despair. Data protection offices haven't seen their financial means really evolve while the amount of personal data being produced, recorded and shared has skyrocketed. Regulation itself cannot efficiently protect the interests of individuals. We are facing an industry that mistakenly defined personal data as the "new oil of the 21st century". Presenting themselves as innovative, governments are promoting the development of a big-data driven industry while participating themselves actively in massive data collection and processing for security reasons. The actual paradigm is comparable to a form of slavery, if we consider that whoever is controlling personal data is able to influence the individuals without them being aware of the manipulation.

Today our digital existence does not depend anymore on our actions alone. While some of the oldest of us were digitally born the day we touched our first computer, our children are born with a digital existence without them being conscious of it. Even if we are not registered on a social network, the mere fact that our friends are using one makes it most probably aware of our existence. Analysis of personal data is so refined that an individual profile can be created without the targeted person having willingly provided any information. It only takes one person to casually share their address book within a social network to trigger the shadow profile creation process. This is not science-fiction anymore. We witness the emergence of generations that have a digital existence before they are actually born. Sharing ultrasound pictures of unborn babies is now a trend. You merely need to mention a pregnancy on a social network for this human being to digitally exist. The medical data generated by a birth and the monitoring of the mother and child is itself impressive. Whether we like it or not, a part of our life is digital. This is why personal data cannot simply be an object that can be owned by someone else. Personal data is part of our individuality, it defines us, tells so much about us. "We" are our personal data and this personal data is "us".

Previous attempts to take back control of personal data have failed. Defining personal data as an object subject to property laws, as intellectual property subject to copyright law, or even to define them as common good owned by the society instead individuals, all these concepts are hoping to create a tool for the society to gain control of personal data over data-driven companies. But all these concepts are failing to see the human in the data.

Our human rights are built on one overarching right: the "right to life". This is the most important right. Without it, we cannot benefit of any other right. When this right is present in Human Rights declaration or in Constitutions, it is often followed by the right to respect to physical and mental integrity. It is believed that in order for a human to remain free and autonomous in its actions, it must not fear the society to kill it or harm its integrity in any way. If human beings enjoy a digital existence, we must consider that their right to integrity also expands to the digital dimension. If there is a right to physical integrity and to mental integrity, there must be a right to digital integrity. Exploiting someone's personal data must be considered a violation of their digital integrity. The simple fact of collecting data could be criminalized.

The consequences of the enforcement of a right to digital integrity are profound. Gathered within the AFAPDP association, the french speaking data protection agencies adopted, on October 18th 2018, a very important resolution on data ownership: personal data are constituting elements of the human person. A human person has inalienable rights over its personal data. This resolution is visionary. The implications are game changing. Personal data is like a part of your body. Personal data cannot be sold.

The article 10 of our Swiss Constitution already gives us the rights to be respected for our physical and mental integrity. We can add the digital integrity to our Constitution. When added, the right will impose itself to our institutions. It will be given to all individuals, even those unaware of their digital-self. Our institutions will be compelled to treat all with respect their integrity, is it physical, mental or digital. It should not be the burden of an individual to prove that a mistreatment is indeed a violation of its rights.

The existing laws, like GDPR, are complementary. They provide detailed tools and subsequent rights that can be used to enforce the right to the digital integrity. However, the GDPR is incompatible to this right in its article 2 relating to the material scope. Article 2 excludes public institutions to be subject to the GDPR when the data processing is related very loosely to a security related matter. A right to digital integrity cannot allow such large exception.

For Mikuláš Peksa, Member of the European Parliament, the "New Iron Curtain" will divide the world between countries embracing surveillance capitalism and those embracing digital self-determination. True to our humanist traditions, respecting all our own physical, mental and digital integrity, our society can become a strong digital free society with educated individuals autonomous in their choices. Our society should develop and adopt privacy friendly tools and protocols for its interactions available and usable by all. The digital revolution should benefit humanity as a whole. It should not for a privileged few to benefit most from it.

We are at the dawn of a new era. It is still possible to make the decisions that will make these innovations respect individual rights and autonomy. Recognizing and protecting our right to digital integrity is an important first step to make sure that human beings are not the subject of technology. This is definitely a humanistic battle.

By Alexis Roussel

Alexis Roussel is the Chairman of Bity, a Swiss bitcoin broker company that he co-founded in 2014. He holds a Masters in New Technology public law and has served as E-Governance specialist for the United Nations. Alexis was also the president of the Pirate Party of Switzerland to promote a human-centric and distributed approach of a technological society.

SITZSTREIK IM INTERNET

Während bürgerliche Freiheiten auch offline immer weiter eingeschränkt werden, sollen manche fundamentalen Rechte wie Demonstrations- und Versammlungsrecht im Internet schon gar nicht eingeführt werden.

Bereits in den Anfängen des World Wide Web beunruhigte der neue Raum, der sich für Internetuser auftat, die staatstragenden Mächte und Sicherheitsbehörden. Als ab Mitte der 1990er Jahre das Internet langsam aber sicher zu einem neuen Massenmedium wurde, nahmen die Warnungen vor einem Cyberwar und dem Cyberterrorismus ebenso zu wie jene vor einem neuen Wilden Westen, in dem es keine Regeln gebe, vor allem da die Anonymität im Netz den gesellschaftlichen Zusammenhang bedrohe.

Zwar sollte das globale, grenzenlose Internet, das noch weitgehend in den Händen des Westens lag, aus politischen und ökonomischen Interessen heraus erhalten bleiben, aber es stellte auch die nationale Sicherheit etwa der USA in Frage, wie 1997 die von Bill Clinton einberufene Presidential Commission on Critical Infrastructure Protection warnte: «Die Cyberdimension stützt sich zunehmend auf unsere Infrastrukturen und erlaubt den Zugang zu diesen aus der ganzen Welt», was aber auch «traditionelle Grenzen und Rechtsprechungen» unterläuft. So wird nun innere Sicherheit von aussen und aus der Ferne bedroht. Der Schutz der wo auch immer verlaufenden Cybergrenzen, die Bekämpfung des Cyberterrorismus und der Einstieg in den Informationskrieg, die Angst vor neuer Kriminalität und einer unkontrollierten Meinungsfreiheit führte in den Nationalstaaten zu hektischen Massnahmen, während gleichzeitig internationale Abkommen blockiert wurden. Wie immer gehen Sicherheit und Wirtschaftsinteressen vor Menschenrechten und Demokratie.

Die Bedrohungskulisse wurde in der Folge weiter aufgebaut und die gesetzlichen Regelungen verschärft. Länder versuchen zunehmend, den Internetverkehr mit Überwachung und Filtern zu kontrollieren. Immer öfter wird das Internet blockiert oder ein nationales Netz aufgebaut, um einen Staat im Notfall aus dem Internet auszuklinken, es aber auf nationaler Ebene in Betrieb zu halten.

Was in der gesamten Entwicklung, nach 9/11 verstärkt und zunehmend durch die Cyberwar-Aktivitäten und -Ängste der Staaten, aus dem Blick gefallen ist, sind Bemühungen darum, das Internet demokratisch zu gestalten. Noch sind Demonstrationen, freie Meinungsäusserung, Kundgebungen und auch ziviler Ungehorsam möglich. Nicht nur, weil sie in demokratischen Rechtstaaten verfassungsgemäss eingefordert werden können, sondern weil es auch faktisch einen öffentlichen Raum gibt, der von Gemeinden, Ländern und Staaten etwa in Form von Strassen und Plätzen vorgehalten wird. Im Internet sind die Strassen und Plätze (Backbones, Internetknoten, Erd- und Seekabel, Richtfunk, Satelliten, Telefon-, Kabel- oder Mobilfunknetze) hingegen in privater Hand.

In den 1990er Jahren wurde noch um die Einrichtung von öffentlichen virtuellen Räumen gekämpft. Man wollte, wie es die frühe Internetkultur vorgelebt hatte, selbstorganisierte Gemeinschaften und eine eigentumslose Geschenkökonomie. Aber es ging auch darum, sich der öffentlichen privaten Räume zu bemächtigen, parallel zur Reclaim-the-Streets-Bewegung. Daraus entstand die Idee, die Sit-ins als Form des zivilen Ungehorsams aus den Protestbewegungen in den Cyberspace zu übertragen. Den Zugang zu einer Website zu blockieren, ist vergleichbar damit, eine Strasse, einen Platz oder ein Gebäude durch eine Sitzblockade zu blockieren. Die Bewegung der anderen Verkehrsteilnehmenden wird auch hier eingeschränkt, weil es der Sinn einer Demonstration ist, Aufmerksamkeit für ein Anliegen zu erzeugen.

1989 hatte eine italienische Gruppe, die sich Anonymous Digital Coalition nannte, nach einem Massaker an Indios in Chiapas zu einer neuen Form des kollektiven Protestes im Netz aufgerufen, die von Ricardo Dominguez und Stefan Wray vom Electronic Civil Disobedience (EDC) weitergeführt wurde: das gleichzeitige automatisierte Aufrufen einer Website durch massenhaftes Klicken des Reload Buttons als eine Strategie des «elektronischen zivilen Ungehorsams». Daraus entwickelten sich im Vorlauf zu den später praktizierten DoS- oder DDoS-Angriffen mit vielen Zombie-Rechnern Programme wie FloodNet, die man nur anklicken musste, um permanent eine Website zu einer bestimmten Zeit aufzurufen. Andere Programme versuchten durch massenhaftes Versenden von Spam-Emails ebenfalls eine Website lahmzulegen – sogenannte «Email-Bomben».

Im Unterschied zu Hackern, die in Websites eindrangen und diese beispielsweise mit Botschaften überschrieben, legte der «elektronische zivile Ungehorsam» ohne Vermummung nur den Zugang zu einer Website lahm oder machte sie durch wiederholte Aufrufe langsamer. Der Unterschied zu Sit-ins im realen Raum ist, dass Menschen weltweit an solchen Protesten teilnehmen können, ohne vor Ort sein zu müssen, aber eben auch, dass es keinen öffentlichen Raum gibt. Die Staaten haben unter der neoliberalen Ideologie, der auch viele antistaatliche und anarchistische oder libertäre CyberaktivistInnen anhingen, keine Plattformen aufgebaut, die nationale oder globale öffentliche Räume mit den bürgerlichen Freiheiten garantierten. Deswegen wurden und werden Protestformen, die im realen Raum geschützt sind, im Cyberspace als Kriminalität oder als Terrorismus verfolgt. Sitzblockaden sind gerechtfertigt, wenn die menschlichen Körper die freie Bewegung der anderen gewaltlos verhindern. Das Aufrufen einer Website durch ein Programm wird hingegen als eine Waffe oder als Gewalt subsummiert, um solche Aktionen zu kriminalisieren.

Es gab in Deutschland im Juni 2001 eine Aktion, die das Problem deutlich gemacht hatte, aber weitgehend dem Vergessen anheimfiel. AktivistInnen von «kein mensch ist illegal» und «Libertad», die gegen Abschiebung von Geflüchteten protestierten, hatten zu einer zweistündigen Blockade der Website der Lufthansa aufgerufen. Über eine Mail wurde das virtuelle Sit-in gegen die Website Lufthansa.com auch bekannt gegeben und dem Ordnungsamt in Köln – dem Hauptsitz der Lufthansa – mitgeteilt. MitstreiterInnen sollten sich ein Programm des Electronic Disturbance Theatre herunterladen, das die Website immer wieder aufruft. Schon im Vorfeld des virtuellen Sit-ins gegen die Lufthansa, das als «Sitzblockade am Eingang des Internetauftritts der Lufthansa» ausgegeben wurde, hatte das Bundesjustizministerium erklärt, dass solche Aktionen kein legitimes Mittel zur politischen Meinungsäusserung seien und gleich mehrere Straftatbestände erfüllen könnten. Apodiktisch hiess es, dass das Versammlungsrecht im Netz nicht gültig sei: «Unser Haus hält es für zweifelhaft, dass sich die Initiatoren auf das Demonstrationsrecht berufen können.» Die im Artikel 8 Grundgesetz garantierte Versammlungsfreiheit beziehe sich nur auf die physische Anwesenheit «im realen öffentlichen, und nicht im virtuellen Raum». Das Ordnungsamt habe sich daher als «nicht zuständig» erklärt, sagte Strasser, und die AktivistInnen auf den Unterschied zwischen körperlichen und virtuellen Versammlungen hingewiesen und ihnen eine Rechtsberatung empfohlen.

Die Lufthansa sprach von «terroristischen Hackerschlägen» – und das war noch vor 9/11. Das virtuelle Sit-in, das von 150 Organisationen unterstützt wurde, war am Tag der Aktionärsversammlung insofern ein bisschen erfolgreich, als die Website trotz der Bemühungen der Lufthansa angeblich mehrmals für kurze Zeit schwer zu erreichen war. Dazu trugen freilich auch Internetuser bei, die zufällig zur Zeit des virtuellen Sit-ins auf die Website zugriffen. Das Ziel der Demo sei, so sagten Organisatoren, sowieso «nicht ein technisches Knockout des Servers gewesen, sondern durch eine massive Beteiligung und Berichterstattung die Kritik an den Abschiebefügen zu verstärken». Es sollen sich allerdings nur 13.000 Menschen beteiligt haben.

Die Lufthansa stellte Strafanzeige wegen Nötigung, die Polizei sah einen «Aufruf zu einer Straftat», die Staatsanwaltschaft ermittelte wegen Computersabotage und Nötigung; der Staatsschutz durchsuchte die Räume des Mitorganisators «Libertad!» in Frankfurt am Main und beschlagnahmte die Computer. Das Frankfurter Amtsgericht verurteilte 2005 ein Mitglied von «Libertad!» wegen «Anstiftung zur Nötigung». Die Strafe von 900 Euro war zwar symbolisch, aber das Gericht wollte klar machen, dass es solche Protestformen im virtuellen Raum nicht geben darf. Die Richterin sprach von der «Kraftentfaltung des Mausklicks», durch den der Tatbestand der Gewalt «in seiner stärksten Form erfüllt» und «der Wille Anderer gebeugt» worden sei. Umstritten war juristisch, ob Online-Demonstrationen oder virtuelle Sit-ins nach dem Grundgesetz als Versammlungen gelten können. Juristinnen schlugen vor, solche Aktionen wie virtuelle Sit-ins als «massenhafte Inanspruchnahme der Meinungsfreiheit» zu sehen, wenn Versammlungen physische Anwesenheit vor Ort erfordern. Allerdings wäre auch das kollektiv wiederholte Aufrufen einer Website physisch im Sinne der Telepräsenz oder -motorik.

2006 sprach dann das Oberlandesgericht Frankfurt den Angeklagten frei. Onlinedemos seien keine Gewalt und Nötigung, auch keine Datenveränderung, sondern der Versuch einer «Meinungsbeeinflussung». Unentschieden bleib der Vorwurf der Ordnungswidrigkeit, die zum Zeitpunkt des Urteils bereits verjährt wäre. Die Begründung ist allerdings interessant: «Die Wirkung beim Opfer, dem User, erschöpft sich in dem Umstand, dass er die Website der A nicht aufrufen kann. Eine physische Beeinträchtigung ist damit nicht verbunden.»

Es wird also gegen das Amtsgericht argumentiert, dass eine Onlineblockade keine physische Blockade ist, wie das bei der Sitzblockade der Fall ist. Das Amtsgericht habe ausgeführt, «dass die technischen Vorgänge in der Summe dazu führen, dass es unmöglich werde, die entsprechende Homepage aufzusuchen. Diese Ausführungen sind bereits im Ansatz verfehlt, da im Falle der Sitzblockade die Opfer in ihrer Bewegungsfreiheit eingeschränkt werden, was im Fall der ‹Onlineblockade› nicht gegeben ist. Die Internetuser können sich weiterhin uneingeschränkt bewegen und fortbewegen.»

2012 erklärte die Bundesregierung auf eine Anfrage der Linken, dass bei «einer Nutzung von Computerprogrammen zur Herbeiführung einer ‹Denial-of-Service-Attacke›» eine Strafbarkeit wegen «Computersabotage» in Frage komme. Auch wer solche Programme verbreite, könne strafbar werden. Entlarvend ist jedoch schon die Terminologie, von einer «Attacke» zu sprechen. «Massen-Email-Proteste» seien aber legitim und würden nicht mit der Absicht einhergehen, anderen Schaden zuzufügen. Sie sind von der Meinungsfreiheit gedeckt. Betont wird aber, dass im Sinne des Artikels 8 des GG virtuelle Versammlungen keine verfassungsrechtlichen «Versammlungen» seien. Denn solche würden eben «die gleichzeitige körperliche Anwesenheit mehrerer Personen an einem Ort» voraussetzen.

Art. 8 GG lautet: «Alle Deutschen haben das Recht, sich ohne Anmeldung oder Erlaubnis friedlich und ohne Waffen zu versammeln.» Hier ist keine Rede von physischer Anwesenheit; die einzige offene Frage ist, ob eine Online-Blockade als «Waffe» zu werten ist. Wenn man von «Attacke» spricht, tendiert man dazu, kollektive DDoS als Gewalt zu betrachten. Versammlungen und Demonstrationen im realen Raum schränken die Bewegungsfreiheit anderer Menschen ebenfalls ein und fügen kommerziellen Interessen womöglich Schaden zu. Es wäre also höchste Zeit, dass Regierungen von demokratischen Rechtsstaaten die Räume juristisch und virtuell schaffen oder freigeben, um Versammlungen, Demonstrationen oder Sitzblockaden online zu ermöglichen.

Ein Grundproblem ist freilich, dass sich das deutsche Grundgesetz auf deutsche StaatsbürgerInnen bezieht. Das deutsche Versammlungsgesetz räumt aber die Versammlungsfreiheit «jedermann» unabhängig von der Staatsangehörigkeit ein. Nachdem man seit einigen Jahren die Angst vor Destabilisierungs- und Desinformationskampagnen schürt und Informationen als Waffen (weaponized information) bezeichnet, werden hier wohl weitere Beschränkungen aufgebaut. Auffällig ist vor allem, dass die Parteipolitik dieses wichtige Thema in einer digitalen Gesellschaft vermeidet. Auch die neuen Protestformen wie die Gelben Westen, Fridays for Future oder Extinction Rebellion sind auf diesem Auge blind.

Von Florian Rötzer

Florian Rötzer ist ein deutscher Journalist. Er studierte in München Philosophie, Pädagogik sowie Psychologie und ist Chefredakteur beim Online-Magazin Telepolis, zu dessen Gründern er gehört.

A Declaration of the Independence of Cyberspace

by John Perry Barlow <barlow@eff.org>

Governments of the Industrial World, you weary giants of flesh and steel, I com
e from Cyberspace, the new home of Mind. On behalf of the future, I ask you of
the past to leave us alone. You are not welcome among us. You have no sovereign
ty where we gather.

We have no elected government, nor are we likely to have one, so I address you
with no greater authority than that with which liberty itself always speaks. I
declare the global social space we are building to be naturally independent of
the tyrannies you seek to impose on us. You have no moral right to rule us nor
do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have
neither solicited nor received ours. We did not invite you. You do not know us
, nor do you know our world. Cyberspace does not lie within your borders. Do no
t think that you can build it, as though it were a public construction project.
You cannot. It is an act of nature and it grows itself through our collective
actions.

You have not engaged in our great and gathering conversation, nor did you creat
e the wealth of our marketplaces. You do not know our culture, our ethics, or t
he unwritten codes that already provide our society more order than could be ob
tained by any of your impositions.

You claim there are problems among us that you need to solve. You use this clai
m as an excuse to invade our precincts. Many of these problems don't exist. Whe
re there are real conflicts, where there are wrongs, we will identify them and
address them by our means. We are forming our own Social Contract . This govern
ance will arise according to the conditions of our world, not yours. Our world
is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed
like a standing wave in the web of our communications. Ours is a world that is
both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accor
ded by race, economic power, military force, or station of birth.
We are creating a world where anyone, anywhere may express his or her beliefs,
no matter how singular, without fear of being coerced into silence or conformit
y.

Your legal concepts of property, expression, identity, movement, and context do
not apply to us. They are all based on matter, and there is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physic
al coercion. We believe that from ethics, enlightened self-interest, and the co
mmonweal, our governance will emerge . Our identities may be distributed across
many of your jurisdictions. The only law that all our constituent cultures wou
ld generally recognize is the Golden Rule. We hope we will be able to build our
particular solutions on that basis. But we cannot accept the solutions you are
attempting to impose.

In the United States, you have today created a law, the Telecommunications Refo
rm Act, which repudiates your own Constitution and insults the dreams of Jeffer
son, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must n