# Vorsicht!

# 8 Vorsicht!

**Die Digitalisierung ermöglicht neue Dimensionen an Überwachung und Desinformation. Sie kann damit zu einer Gefahr für die Demokratie werden.**

*von Nick Monaco*

Kürzlich wurde bekannt, dass sich Cambridge Analytica illegal Daten von über 50 Millionen Facebook-Nutzern über eine Drittanbieter-App beschafft hat. Sie wurden während der US-Präsidentschaftswahlen 2016 für psychographisches Microtargeting eingesetzt, mit dem Ziel, politische Botschaften – harmloser bis heimtückischer Natur – zu verbreiten. Zu Recht stand Facebook weltweit in der Kritik, und Mark Zuckerberg wurde aufgefordert, vor mehreren Regierungen auszusagen.

Dies ist nur die jüngste vieler Episoden, die informierte Bürger nachdenklich stimmten bezüglich der Auswirkungen der Technologie auf die liberale Demokratie: Die Snowden-Offenbarungen, die jüngsten Ransomware-Angriffe, die Rolle von Bots, Hacking und Desinformation in der Weltpolitik sowie das Hacking der Wahlinfrastruktur in den USA haben gezeigt, dass digitale Technologien eine Bedrohung für die demokratische Regierungsführung darstellen können. Das führt uns zwangsläufig zur Frage: Wird die Digitalisierung der Demokratie weltweit mehr schaden als nützen? Entscheidend sind vier Themen: Privatsphäre und bürgerliche Freiheiten, Desinformation, die Auswirkungen der Automatisierung auf die Arbeit und die Sicherheit der digitalen Infrastruktur.

### Privatsphäre und bürgerliche Freiheiten

Eine der grössten Bedrohungen für die Demokratie ist die Erosion der Privatsphäre, die in den letzten zwanzig Jahren weltweit als Folge einer stärker vernetzten und digitalisierten Welt stattgefunden hat. Mehr von unseren persönlichen Informationen, von unseren Bankgeschäften, Gesundheitsdaten, von unserer Kommunikation ist jetzt online greifbar als je zuvor.

Alle online generierten Daten sind anfällig für die Ausnutzung, das Hacking und die Überwachung durch Unternehmen, Werbe- und Versicherungsagenturen, Regierungen oder Privatpersonen, die genug zu zahlen dafür bereit sind. Das Internet der Dinge wird diesen Effekt noch verstärken. Schlecht durchdachte Gesetzgebung, wie die jüngste Entscheidung der republikanischen Parlamentarier in den USA, den Internetprovidern den Verkauf von Daten privater Verbraucher zu erlauben, gefährdet potenziell zivile Freiheiten.

Regierungen können in ihrer Wahrnehmung von Gut und Böse eine bemerkenswerte Willkür an den Tag legen. Der Nationalheld von heute war in vielen Fällen der Staatsfeind von gestern – oder umgekehrt. Diese Gefahren werden sich in den kommenden Jahren noch verstärken – man braucht sich nur die jüngsten, auf Gesichtserkennungssoftware basierenden Verhaftungen in China oder dessen Pilotprojekt des «Social Credit Score» anzuschauen, um festzustellen, dass solche dystopischen Ergebnisse alles andere als an den Haaren herbeigezogen sind.

Ein Mangel an Rechenschaftspflicht in Verbindung mit einem schleichenden Wachstum der Geheimdienste in den westlichen Demokratien verschärft diese Probleme. Mit der Digitalisierung unseres Lebens und der Verbreitung billiger ziviler Überwachungstechnologien wird eine kluge Regulierung sowohl der staatlichen als auch der privaten Datenerhebung und -überwachung unabdingbar für die Sicherung der Gesundheit der Demokratien sein.

### Desinformation

Eine weitere Bedrohung für die Demokratien ist eine neue Anfälligkeit für Informationsoffensiven. Experten warnen seit langem vor dem Potenzial von Social Media, Autokratien zu zementieren und Demokratien zu schädigen. Seit 2016 ist sich die Welt des Einflusses von Junknews und Desinformation im Internet bewusst geworden. Die Verwendung von Bots zur Verstärkung politischer Botschaften ist ein internationales Phänomen. Während der Brexit-Kampagne generierten auf Twitter weniger als 1% der Konten über 30% der Gespräche zum Thema. Schon 2012 hielt Südkoreas Nationaler Nachrichtendienst die etablierte Partei an der Macht, indem er 1,2 Millionen Nachrichten auf Twitter verbreitete, die Park Geun-Hye bevorzugten und ihre Gegner als nordkoreanische Sympathisanten beschmierten. Park gewann die Präsidentschaftswahl mit wenig mehr als einer Million Stimmen Vorsprung.

Im Jahr 2017 stellte Freedom House fest, dass 30 Regierungen Online-Kommentatoren beschäftigten und dass es online in 18 Ländern zu Desinformation und Manipulationen im Zusammenhang mit Wahlen kam. Von 2012 bis 2016 erlebte die Bevölkerung

in Mexiko, Ecuador, Indien und auf den Philippinen, wie Wahlkampfapparate, die Präsidentschaftskandidaten an die Macht brachten, in staatliche Propaganda- und Trollingmaschinen umgewandelt wurden, um Kritiker mit Online-Hasskampagnen zu treffen.

Das Phänomen des staatlich finanzierten Trolling, des Einsatzes von gezielten Online-Hass- und Belästigungskampagnen, um Menschen zum Schweigen zu bringen und einzuschüchtern, untersuche ich eingehend in einer neuen Studie am Digital Intelligence Lab mit Carly Nyst, ehemals Legal Director von Privacy International. In einem Fall wurde eine ecuadorianische Journalistin, Martha Roldós, mit illegaler Spyware angegriffen. Bald darauf wurden ihre privaten E-Mails in irreführenden Artikeln von einer staatlichen Zeitung veröffentlicht, und sie wurde vom damaligen Präsidenten Rafael Correa direkt im nationalen Fernsehen angegriffen. Die Hetze des Präsidenten führte online zu einer massiven Desinformations- und Hasskampagne gegen Roldós, die sie davon abhalten sollte, den investigativen Journalismus und ihr Recht auf freie Meinungsäusserung auszuüben.

Dieser Fall zeigt, dass sich scheinbar isolierte Probleme wie Privatsphäre und Desinformation verbinden und in eine neue Form der Menschenrechtsverletzung ausarten können – eine, für die die westlichen Rechtsstaaten schlecht gerüstet sind.

### Arbeit und Infrastruktur

Wichtige Themen sind auch die Zukunft der Arbeit und der Infrastruktur. Während oft die Globalisierung für den Wegfall von Arbeitsplätzen verantwortlich gemacht wird, zeigt die Forschung, dass die Hauptursache in der Automatisierung liegt, nicht in der Globalisierung. Dieser Trend wird sich mit zunehmender Digitalisierung und Fortschritten in der KI (künstlichen Intelligenz) noch verstärken. Trumps Wahl war zumindest teilweise auf eine Gegenreaktion dieser Arbeiter zurückzuführen, und sie hat die amerikanische und wohl auch die globale Demokratie eindeutig ausgehöhlt.

Kritische Infrastrukturen wie Kernenergieanlagen, Stromnetze und Wahlsysteme werden zunehmend an das Internet angebunden. Das erhöht die Gefahr absichtlicher Angriffe oder unbeabsichtigter Katastrophen. Die WannaCry-Ransomware-Attacken in Grossbritannien und der jüngste SamSam-Angriff in Atlanta sind kleine Beispiele für die Gefahren, die von dieser Anordnung ausgehen. Man braucht sich nur den Reichstagsbrand oder den 11. September anzusehen, um zu erkennen, welche bleibenden Schäden ein grosser Infrastrukturunfall an demokratischen Normen und bürgerlichen Freiheiten verursachen könnte.

### Lösungen

Wir können Massnahmen ergreifen, um es unwahrscheinlicher zu machen, dass der Genuss moderner Telekommunikation die Privatsphäre und die bürgerlichen Freiheiten gefährdet. Die Verwendung von Verschlüsselungstechnologien (vereinfacht durch Apple, Signal und Tor) erschwert die unrechtmässige Massenüberwachung. Tim Berners-Lee, der Erfinder des World Wide Web, hebt die Wichtigkeit hervor, Benutzern mehr Kontrolle über ihre Daten zu geben. Die Missachtung der Verbraucherrechte und das Versäumnis, auf den Schaden aufmerksam zu machen, den ihre Netzwerke der Demokratie zufügen können, macht Technologieunternehmen nicht weniger schuldig als vor einigen Jahrzehnten die Tabakriesen in ihren Kampagnen zur Verschleierung der klaren Gesundheitsschäden des Tabaks oder als die grossen Ölkonzerne in ihrer jahrzehntelangen Ablehnung des Klimawandels.

Im öffentlichen Sektor müssen die Bürger mehr Kontrolle über die Nachrichtendienste verlangen. Die Gewährleistung der Verfassungsmässigkeit ihrer Praktiken ist von grundlegender Bedeutung für die Demokratie. Die EU ist mit ihrer Allgemeinen Datenschutzverordnung und dem «Recht der Bürger auf Vergessenwerden» Vorreiterin, ebenso wie Estland und Taiwan mit ihren offenen Dateninitiativen.

Auch wird das Problem der Desinformation verschiedentlich angegangen. Da es technologischer wie auch gesellschaftlicher Natur ist, erfordert es entsprechend Lösungen in beiden Bereichen. Soziale Initiativen wie Taiwans neue Schulprogramme für digitale Kompetenz, die Zusammenarbeit von Twitter vor Ort mit lokalen NGOs und Experten sind lobenswerte Antworten. Technologische Lösungen, wie z.B. die Transparenz von Bots auf sozialen Plattformen, sind ebenfalls zu begrüssen. Jede öffentliche Regelung zur Desinformation sollte bei der Verwendung der Instrumente (wie der Verwendung von Bots zur Verstärkung politischer Botschaften) und nicht bei den Instrumenten selbst ansetzen.

Auf allen Ebenen ist mehr Kommunikation und Transparenz nötig. Gemeinsame Kommissionen von Führungskräften des privaten Sektors, akademischen Forschern und Gesetzgebern sind ein notwendiger erster Schritt, um sicherzustellen, dass digitale Technologien ein Positivsummenspiel für alle Beteiligten bleiben und dass sie nicht die demokratische Regierungsführung und bürgerliche Freiheiten verringern. Entwickler sollten auch daran arbeiten, die möglichen sozialen Nebenwirkungen ihrer Kreationen vorherzusehen – wie der Journalist John Markoff schreibt: «Wie wir unsere zunehmend autonomen Maschinen gestalten, wird das Wesen unserer Gesellschaft und unserer Wirtschaft bestimmen.» ❮

**Nick Monaco**
ist Researcher für das Computational Propaganda Project am Internet Institute der Universität Oxford.