Schwere Kost
[Lesestoff, der nicht leicht zu verdauen ist.]

SIEHT ALLES. HÖRT ALLES. VERRÄT ALLES.

Eine kleine Aufklärung darüber, was ihre geliebte Taschenwanze den ganzen lieben lagen Tag so treibt.

[Matthias Müller]

„Wenn wir die Demokratie in den kommenden Jahrzehnten erneuern wollen, brauchen wir dazu das Gefühl der Entrüstung, ein Gespür für den Verlust dessen, was man uns da nimmt. Und ich meine damit nicht nur unsere ‚persönlichen Daten'.

Was hier auf dem Spiel steht, ist die Erwartung seitens des Menschen, Herr über sein eigenes Leben und Urheber seiner eigenen Erfahrung zu sein. Was hier auf dem Spiel steht, ist die innere Erfahrung, aus der wir den Willen zum Wollen formen, und die öffentlichen Räume, in denen sich nach diesem Willen handeln lässt. Was auf dem Spiel steht, ist das herrschende Prinzip sozialer Ordnung in einer Informationszivilisation und unser Recht als Individuen und Gesellschaften, eine Antwort auf die alten Fragen zu finden: ‚Wer weiß? Wer entscheidet? Wer entscheidet, wer entscheidet?'

Dass der Überwachungskapitalismus so viele unserer Rechte in diesen Sphären an sich gerissen hat, ist ein skandalöser Missbrauch digitaler Fähigkeiten und ihres einst grandiosen Versprechens, das Wissen zu demokratisieren und auf die Erfüllung unserer frustrierten Bedürfnisse eines effektiven Lebens hinzuarbeiten. Die digitale Zukunft ist nicht aufzuhalten, aber der Mensch und seine Menschlichkeit sollten obenan stehen. Die Behauptung der Unabwendbarkeit weise ich zurück, und ich hoffe, Sie tun das auch" (Shoshana Zuboff: „Zeitalter des Überwachungskapitalismus", Seite 596 ff.).

Weisen Sie die Unabwendbarkeit ebenfalls zurück? Entziehen Sie sich dem Sog des Fatalismus?

Vielleicht gehören Sie zu der kleinen Fraktion, die klar ausspricht, dass sie etwas zu verbergen hat. Zumeist heißt es ja von den meisten: „Ich habe ja nichts zu verbergen." Was natürlich nicht stimmt. Jeder Mensch hat etwas zu verbergen. Und das ist sein gutes Recht.

Und Sie, werter Leser, werte Leserin, sind sich sogar dieses Rechts mehr als bewusst. Andernfalls hätten Sie wohl kaum damit begonnen, den vorliegenden Beitrag zu lesen. Aber wie Sie dieses Recht gegen die Übermacht des Überwachungskapitalismus geltend machen könnten, das wissen Sie vielleicht nicht.

Was ist uns lieber — Freiheit oder Gängelung? Verfügbarkeitsstress oder Entspannung? Ein Rest von Intimsphäre oder totale Transparenz? Informelle Selbstbestimmung oder das Gefühl, für kommerzielle Zwecke nur benutzt zu werden? Sich sicher zu fühlen oder ständigen Angriffen auf unseren Geist ausgesetzt zu sein? Die Antwort auf all diese Fragen sollte einfach sein. Dennoch trifft die Mehrheit der Menschen bei diesen Entscheidungen Tag für Tag die für sie jeweils schädliche Wahl. Das Smartphone ist zum Tyrannen im Taschenformat geworden. Für viele ist es ein Suchtfaktor, und den wenigen,

die noch leichten Herzens darauf verzichten könnten, wird das Gerät zunehmend durch strukturelle Zwänge aufgedrängt. Im selben Maß, wie das Smartphone „unentbehrlich“ geworden ist, wachsen die Gefahren und Zumutungen, die mit seiner Benutzung verbunden sind. Programmierer arbeiten auf Hochtouren an Anwendungen, die uns zunehmend nicht nur ausspionieren, sondern unseren Geist auch im Interesse der herrschenden Narrative zu deformieren versuchen. Die von Apple und Google konfigurierten Geräte sind weitaus mehr als nur „nützliche Werkzeuge“ — es sind Wanzen, Überwachungskameras, Datenkraken und Waffen zur psychologischen Kriegsführung in einem.

Die meisten Menschen hegen einen vagen Verdacht. Viele haben das ein oder andere Indiz wahrgenommen, das belegt, das ein solcher Verdacht durchaus begründet sein könnte. Trotzdem schaffen es die wenigsten, ihr Verhalten objektiv zu analysieren und einmal verinnerlichte Verhaltensweisen zu ändern. Gewohnheiten und Routinen sind schwer loszuwerden. Vor allem, wenn diese sich zu Sucht oder Zwang entwickeln. Das passiert nicht nur bei Alkohol und Drogen, sondern in geradezu epidemischer Weise bei etwas, das ich bevorzugt „Taschenspion“ nenne: dem Smartphone.

Während die exzessive Nutzung des Geräts in praktisch allen Lebenslagen fraglos zur sozialschädlichen Unart — um nicht zu sagen Plage oder Seuche — avanciert ist, markiert der Suchtfaktor des kontinuierlich potenter werdenden Begleiters nicht einmal das größte Problem. Denn Abhängigkeiten lassen sich überwinden, wenn auch müh- und langsam; dass die Geräte zur lückenlosen Observation, Manipulation und Transformation der Gesellschaft genutzt werden aber nicht. Denn sie haben sich längst zu tief in die sozioökonomischen Strukturen unserer Zeit gefressen. Einem Großteil der Bevölkerung erscheint der Alltag ohne Smartphone kaum mehr organisierbar. Ob Kommunikation, Nachrichten, Wettervorhersage, Routenplaner, Zahlungen, Zwei-Faktor-Authentifizierung, Fotosammlung, Videostreaming oder Musikarchiv — der mobile Begleiter hilft.

Doch das irreführend positiv und progressiv geprägte Lifestyle-Image des nützlichen Allroundtalents täuscht über dessen sprichwörtlich böse Absichten hinweg. Diese offenbaren sich bei einem Blick auf seine Entwicklung, die dahinterstehenden Konzernstrukturen, ein paar erschreckende Zahlen zu seinen Effekten auf Mensch und Gesellschaft und vor allem auf das, was Smartphones mit Android/Google- oder iOS/Apple-Betriebssystem ganz ohne Zutun oder Wissen des Nutzers treiben.

Zur Kontextualisierung: Über 60 Prozent des gesamten Internetverkehrs sowie 55 Prozent der weltweiten Webseitenzugriffe finden mittlerweile über Mobiltelefone statt (Stand: April 2024). 98 Prozent der Geräte laufen entweder auf Android oder iOS. 92,3 Prozent aller Internetnutzer greifen von ihrem Taschencomputer aus auf das Internet zu. 6,92 Milliarden Menschen nennen ein solches Gerät derzeit ihr eigen. Das sind Ende 2023 gut 86 Prozent der Weltbevölkerung, die damit, je nach Region, zwischen zwei und knapp sechs Stunden pro Tag verbringen. Der alarmierende globale Durchschnitt für Menschen im Alter von 16 bis 64 Jahren liegt aktuell bei sechs Stunden und 58 Minuten Bildschirmzeit pro Tag. Weit über hundert Mal greift man in diesem Zeitraum nach dem Gerät. Tendenz steigend. 35,2 Prozent der Nutzungsdauer verbringen iPhone- und Android-Kunden auf Social Media (Stand: 2021). Zum Telefonieren wurden Smartphones schon seit 2012 kaum noch genutzt. „Smartphone-Penetration“, wie man die Marktdurchdringung im Vertriebsjargon der Telekommunikationsbranche bezeichnet, scheint in Anbetracht dieser Zahlen eine zunehmend zutreffende Beschreibung für die allgemeinen Entwicklungen darzustellen. Denn das Gerät vergewaltigt das Gehirn.

Trotzdem hat das Handy die Welt im Sturm erobert. Zuerst war es die Begeisterung für das Neue, die Freude am mobilen Telefonieren. Am Spielzeug selbst. Es hatte was von Amateurfunk. Oder Gameboy. Dann kam die SMS. Dicht gefolgt von mobiler E-Mail und der Möglichkeit, nun auch unterwegs ins Internet gehen zu können. Dann folgte das erste iPhone.

Was dieser technische Fortschritt seit 2007 mit einem im Kern sozialen Wesen angestellt hat, sehen wir heute an Bushaltestellen, Restaurant-Tischen, auf Schulhöfen oder bei gemeinsam einsamen Gruppen von Display-Junkies. Die Auswirkungen sind verheerend. Der spielerisch-leichte Flair des Handfunk-Feelings ging rasch verloren. Was das Gerät heute primär auslöst, sind Stress, Druck, Verwirrung, Zwänge und Ängste.

Selbst eine oberflächliche Suche fördert sofort sechs bis neun „medizinische Errungenschaften“, sprich Zivilisationskrankheiten zutage, die auf unsachgemäße Nutzung des Smartphones zurückzuführen sind. Von der Smartphone-Akne und Video-Schulter bis hin zum Handy-Nacken, PVS (Phantom Vibration Syndrome), FOMO (Fear of missing out), PtSS (Post-textliches Stress-Syndrom) oder MAIDS, dem „Mobile and Internet Dependency Syndrome“. Das unreflektierte Nutzungsverhalten, das Distraktionsdiktat der Plattformökonomie, verändert unser Denken, die Physis, Augen und unsere emotionalen wie sozialen Fähigkeiten. Smartphones und Social Media haben die anatomische Struktur unserer Gehirne verändert. Die Aufmerksamkeitsspanne von Jugendlichen beträgt nur noch einen Bruchteil dessen, was in der älteren Generation „normal“ ist. Junge Menschen sind mehr und mehr gehirnphysiologisch nicht mehr dazu imstande, länger andauernde Konzentrationsleistungen zu erbringen. Stattdessen ist ihre Amygdala abnorm vergrößert – das Angst und Bewertungszentrum im Gehirn. Daher sind junge Menschen so leicht von Weltuntergangsphantasien zu überzeugen und sie sind trotz erbärmlicher Bildungs- und Wissensniveaus zu allen möglichen Themen extrem meinungsstark. All dies sind die Folgen der exzessiven Nutzung von Bildschirmgeräten wie dem Smartphone. Von der „mentalen Gesundheitskrise“, die längst mehr nicht nur bei Teenagern durch intensive Social-Media-Nutzung ausgelöst wird, gar nicht erst zu sprechen. Es dürfte im Lichte nackter Zahlen und sich abzeichnender Langzeiteffekte also unstrittig sein, dass der vermeintlich praktische Alltagshelfer die Spezies Mensch evolutionär nicht wirklich vorangebracht hat.

Im Rausch permanenter Erreichbarkeit geht leider unter, dass Smartphones uns nicht nur massiven physischen und sozialen Schaden zufügen. Nicht umsonst

bezeichne ich sie meist als Waffe. Oder Wanze. Denn Wissen ist Macht — und niemand weiß so viel über den Menschen der Postmoderne wie Google oder Apple.

Die Konzerne kennen nicht nur alle unsere Kontakte, Bewegungsdaten, Songs, Fotos, Videos, Bankverbindungen, Kontostände und E-Mail-Anhänge, sondern auch unsere Suchanfragen, politischen Ansichten, Sorgen, Ängste, unsere sexuellen Präferenzen bis ins Detail, vertraulichen Nachrichten und intimen Gespräche. Diese Informationen zeichnen nicht nur ein detailliertes Bild vom sozialen Netzwerk jedes Nutzers, sondern auch ein ausgesprochen präzises psychologisches Profil, das aufschlussreicher kaum sein könnte. Über 72 Millionen Datenpunkte sammeln Anbieter für Digitalwerbung in den USA pro Kind bis zu dessen 13. Lebensjahr. Facebook hortet mindestens 52.000 Einträge je Nutzer. Das harmloseste Ergebnis dieser Datensammlung ist zielgerichtete Werbung, die uns auf Basis von Daten und Nutzungsverhalten auf Plattformen und Webseiten angezeigt wird. Das könnte man noch als irrelevant abtun. Was jedoch heute schon funktioniert, ist das die Preisbildung auf großen Handelsplattformen auf der Basis von Userdaten individualisiert wird. Heißt: sobald Amazon weiß, dass Sie bei einer bestimmten Produktkategorie ihre Kaufentscheidungen mehr impulsiv als rational treffen, zahlen Sie mehr. Wenn Sie also glauben, Sie hätten im Netz „nichts zu verbergen", sind Sie ein naives Dummerchen. Ihre Daten machen Sie zur leichten Beute für Geschäftemacher.

Deutlich gravierender sind die Auswirkungen durch Datenmissbrauch — siehe Cambridge Analytica Skandal —, mentale Manipulation, elektronische Ausweise, digitale Währungen, algorithmisierte Zensur, Sozialkreditsysteme, CO2-Budgetierung und Geofencing. Alles Projekte, die ohne Smartphone überhaupt nicht möglich wären. Wer permanent seinen Standort an eine Zentrale übermittelt, ist leicht zu kontrollieren. So werden bereits heute viele Inhalte, die in der Schweiz oder anderen Nicht-EU-Ländern angezeigt werden, in EU-Staaten unterdrückt. Informationen, die über einen VPN-Service oder eine trackingfreie Suchmaschine im Internet leicht zu entdecken sind, sind bei Google vollständig unauffindbar. Auch manch ein Musiktitel lässt sich nicht mehr abspielen, wenn man auf Reisen ist. „In Ihrer Region nicht verfügbar", heißt es da. Geofencing-Exklusion light. Zum Nachdenken sollte es jeden Leser, wenn er sich klar macht, dass die Auswertung dieser Datenströme zunehmend speziellen KI-Anwendungen überlassen wird. Die große Stärke von KI ist es, „Cluster" in großen Datenmengen erkennen zu können. Sie werden auf der Basis ihrer Bewegungen im Datennetz als Bürger „kategorisiert" - mit allen möglichen Folgen. Was die KI über Sie behauptet, wird als wahr erachtet werden, denn KI „macht keine Fehler" – glauben zumindest viele. Die KI-Gläubigkeit insbesondere bei Politikern ist immens, dabei wissen IT-Fachleute, dass KI nicht mehr als ein aufgeblasenes Statistiktool ist und immer bleiben wird. Dennoch überträgt man mehr und mehr Entscheidungsverantwortung an diese unmenschlichen, seelenlosen Systeme.

Smartphones überwachen und dokumentieren die Position ihres Besitzers natürlich auch, wenn alle GPS-Funktionen deaktiviert sind oder das Gerät komplett ausgeschaltet ist, wie ein Artikel zu NSA-Überwachungstechniken von 2013 oder ein Bericht der Princeton University von 2017 zeigen. Das optionale Abschalten von Standort- und Ortungsdiensten oder der Hintergrundaktualisierung in den Smartphone-Menüs bezieht sich nur auf Dienst- und Drittanbieter-Apps. Wobei viele davon unbeeindruckt trotzdem Daten übertragen. Verkauft werden solche Lokationsdaten bevorzugt an Regierungen und Geheimdienste.

Und die Ortungsdienste von Google und Apple lassen sich weder abschalten, noch ist klar, was mit den Daten geschieht. So war beispielsweise meine gesamte Reiseroute kreuz und quer durch Südafrika auf den Meter genau bei Google Maps dokumentiert, obwohl ich alle Tracking-Funktionen deaktiviert hatte und sich in der Savanne mit dem Smartphone keine Datenverbindung herstellen lässt, wenn man sich nicht gerade in der Nähe eines Hotel-Hotspots befindet und lokal erhältliche Guthabenkarten für Daten freischaltet. Dieser Programmatik folgend ist es ein Leichtes, digitales Geld oder moderne PKW demnächst so zu programmieren, dass sie nur in einem vordefinierten Radius funktionieren. So wird das Smartgrid zum unsichtbaren Käfig.

Welche Ziele der digital-finanzielle Komplex des Korporatismus verfolgt, zeigt sich exemplarisch an den jüngsten Entwicklungen für Android-Smartphones. Beispiel Google Play Protect, eine Betriebssystemsoftware, die vor „schädlichen", oder „unbekannten" Drittanbieter-Apps warnen, sie scannen und deren Installation verhindern soll. Vorgeblich zur Sicherheit des Nutzers. Es braucht jedoch nicht viel Fantasie, um sich vorzustellen, dass auch unliebsame Applikationen von Odysee, Rumble, RT, Al Jazeera oder anonyme Krypto-Wallets rasch auf der Liste schädlicher Software landen und so nicht mehr verwendbar sind.

Apple machte 2021 Schlagzeilen mit der Bekanntgabe, „Client Side Scanning" auf iPhones und iPads installieren zu wollen. Diese Erweiterung sollte es dem Tech-Konzern ermöglichen, sämtliche Fotos zu scannen, die auf iCloud hochgeladen werden. Damit sollte die Verbreitung von Kinderpornografie — CSAM (Child Sexual Abuse Material) — erschwert werden. Das Internet Architecture Board (IAB) warnte damals eindringlich vor diesem skandalösen Paradigmenwechsel in puncto Privatsphäre und Datenverschlüsselung. Nach einigem Tumult nahm Apple offiziell Abstand von diesem Vorhaben. Installiert wurde die Software allerdings trotzdem. Das Programm befindet sich also heute auf jedem Apple-Gerät mit aktuellem Betriebssystem. Es sei jedoch nicht aktiv, teilen Apple, die Faktencheck-Industrie und diverse Tech-Blogger mit.

Das ist allerdings nicht korrekt, wie man anhand der Ausführungen des Cybersicherheitsexperten Rob Braxman erkennen kann. Die Funktion ist nur gut getarnt. Bei genauerer Betrachtung wird klar: Jedes Foto, das man mit einem iPhone, iPad oder Mac aufnimmt, wird lokal gescannt. Wie sonst sollte das Gerät Gesichter identifizieren und für spezielle Alben vorschlagen können. Dabei wird jedes Bild mit sogenannten Neural Hashes versehen, mit eindeutigen Identifikatoren, die beim Upload in die Cloud übertragen und katalogisiert werden. Privatsphäre für Fotos gibt es nicht mehr. Denn auch wenn die Cloud-Dienste deaktiviert sind, übertragen Apple-Geräte die Transkripte der Neural-Hash-

Datenbank nachts heimlich an die Zentrale. Und löschen lassen sich Bilder in der Cloud auch nicht so einfach. Klickt man im Kontextmenü eines Fotos auf „Delete“, wird das Foto nicht wirklich gelöscht, sondern nur in der User-Ansicht ausgeblendet. Wie lange Apple und Google die Daten auf ihren Servern belassen, ist nicht bekannt. Vermutlich lange. Denn wie ein Versuch von „CopyTrans“ zeigt, lassen sich aus der iCloud auch Fotos herunterladen, die vermeintlich bereits vor Jahren gelöscht wurden.

Google geht noch einen Schritt weiter. Wie das „Medium für digitale Freiheitsrechte“ Netzpolitik.org am 16. Mai 2024 ausführt, plant das Unternehmen, künftig alle Anrufe seiner Nutzer zu scannen — und zu speichern —, um seine Kunden so vor Telefonbetrügern warnen zu können. Vorratsdatenspeicherung war gestern. Mittlerweile arbeiten neben den Tech-Konzernen selbstverständlich auch die transatlantisch bewegten Überwachungszirkel in EU, Großbritannien und den USA an Gesetzen, die Client Side Scanning und anlasslose Totalüberwachung legalisieren. Auch wenn derartige Unterfangen das Recht auf den Schutz persönlicher Daten oder die Unschuldsvermutung ad absurdum führen und Projekte wie die sogenannte Chatkontrolle nach allgemeinem Rechtsverständnis illegal sind.

Doch schlimmer geht immer. Smartphones, die sich mit Gesichtserkennungssoftware wie „Face ID“ entsperren lassen — als wäre der an polizeidienstliche Erfassung erinnernde Fingerabdruck nicht schon genug gewesen —, fertigen alle fünf Sekunden ein Infrarotbild von ihrer Umgebung an. Selbst dann, wenn der Bildschirm gesperrt oder verdeckt ist. Nach Angaben von Apple ist das nötig, um das Gerät zügig per Blick auf den Bildschirm entsperren zu können. Die von Face ID angefertigten Fotos werden in mathematische Strukturen umgewandelt und auf dem Telefon abgelegt. Einem Gerät, das jede Nacht gegen drei Uhr unaufgefordert nicht einsehbare Datenpakete „nach Hause“ schickt.

Die Kameras moderner Smartphones können aber noch ganz andere Dinge. Sie folgen zum Beispiel dem Blick des Besitzers, um dessen Handlungen antizipieren oder Befehle empfangen zu können. Analysieren seine Mimik. „Aufmerksamkeitssensible Funktionen“, nennt das die Firma mit dem Apfel-Logo. Wem bei der immer öfter biometrisch gehandhabten Einreisekontrolle an Flughäfen mulmig zumute ist, sollte demnach wohl kein Smartphone nutzen.

Der Taschenspion hört natürlich auch zu. Und zwar permanent. Wie sonst sollte „Siri“ wissen, wann man etwas von ihr will. Doch auch hier wiegeln „Experten“ und leitmedialer Komplex vehement ab und behaupten, es sei reiner Zufall, dass Werbeanzeigen und Social-Media-Inhalte exakt das widerspiegeln, was im Umfeld des Gerätes in den letzten Stunden besprochen wurde. USA Today räumt in diesem Kontext zwar ein, dass das Telefon zuhöre, diese Daten aber nur lokal verarbeitet würden und keine Sprachaufzeichnungen an Apple, Google oder Amazon übertragen würden. Und das ist sogar korrekt. Denn die Datenmenge wäre zu groß. Stattdessen übertragen die Smartphones Textdateien mit Transkripten, die heute jeder sehen kann, wenn er mit iMessage eine Voicemail aufnimmt und diese umgehend als Text erscheint. Diesen Aspekt sparen die Faktenchecks beflissentlich aus.

Zudem werden die KI-basierten Anwendungen „zur Vermeidung häuslicher Gewalt“ oder präventiver „Gefahrenabwehr“, von denen eine im März 2023 veröffentlichte Studie 136 Stück untersuchte, nur dann wie in Aussicht gestellt funktionieren, nämlich autonom, wenn das Smartphone seine Kameras, Mikrofone und Bewegungssensoren permanent nutzt, um seine Umgebung zu überwachen.

Dabei stellt das einzelne Gerät künftig nicht mehr das größte Problem für freiheitsaffine Zeitgenossen dar. Denn die Taschenspione überwachen seit geraumer Zeit nicht mehr nur ihren jeweiligen Besitzer, sondern auch dessen gesamtes Umfeld.

Dazu kommunizieren die Geräte untereinander, tauschen Informationen wie IMEI-Nummern, IP-Adressen und Kontaktdaten aus. iPhones bieten diese Funktion seit September 2020 (iOS 13.7) flächendeckend über das Betriebssystem an. Die über Bluetooth Low Energy (BLE) gesammelten Informationen bildeten die Grundlage für die Contact-Tracing-Apps während der Coronakrise. Auch die deutsche Corona-Warn-App nutzte den intransparenten Datenpool. Dafür konnte das Programm über eine Schnittstelle alle Begegnungen der vergangenen 14 Tage auslesen. Ende 2020 entwickelten bereits über 20 Länder Tracking-Applikationen, um die von Big Tech gesammelten Bewegungs- und Begegnungsdaten auslesen und in ihren COVID-Apps darstellen zu können.

Meint: iPhones zeichnen seit knapp vier Jahren jeden Kontakt mit einem anderen iPhone auf und bilden daraus Netzwerkkarten zu Bewegungen und Begegnungen ihrer Besitzer. Im Menü des Smartphones lässt sich diese Funktion zwar deaktivieren – anzunehmen, das Gerät sammle deshalb nicht trotzdem die entsprechenden Daten, ist allerdings naiv. Nach Angaben von Apple sollten diese Informationen übrigens nur lokal gespeichert und nach 14 Tagen automatisch gelöscht werden. Was von solchen Statements zu halten ist, zeigt das vorgängig angeführte Beispiel mit den vermeintlich gelöschten, aber auch nach Jahren wiederherstellbaren iCloud-Fotos.

Google zog natürlich nach und implementierte eine ähnliche Datenkrake. So zeichnen auch Android-Geräte seit Ende 2020 jede Begegnung mit anderen Android-Geräten auf. Damit entstanden zwei riesige Mesh-Netzwerke, in denen Maschinen ohne Zutun ihres Besitzers untereinander kommunizieren. In Deutschland verwenden 66,1 Prozent der Smartphone-Nutzer Android – 33,2 Prozent iOS von Apple (Stand: März 2024). Damit sind 99,3 Prozent der Bevölkerung kartografiert. Denn seit gut einem Monat verstehen sich die beiden bisher getrennt voneinander spionierenden Betriebssysteme nun auch gegenseitig.

Das läutet nicht nur klammheimlich einen Paradigmenwechsel in Sachen Totalüberwachung ein, ein solches Mesh-Netzwerk schafft darüber hinaus die Grundlage für die Militarisierung der Smartphone-Infrastruktur, weil dieses Netzwerk nicht nur Daten sammeln und senden, sondern auch Befehle empfangen kann.

So könnte auf Knopfdruck für 99,3 Prozent der Bevölkerung Malware installiert, ein Blackout simuliert oder eine bestimmte Funkfrequenz generiert werden. Diese könnte — wie in meinem Text „Die sechste Dimension“ beschrieben

— Nanopartikel und Smartdust zu bestimmten Reaktionen anregen.

In diesem Kontext ist bemerkenswert, dass das iPhone mitnichten auf einen genialen Erfinder zurückzuführen ist — auch wenn sich Steve Jobs gerne als solcher gerierte —, sondern auf Militärtechnologie. Jobs hat sie nur clever verwendet und vermarktet. Mariana Mazzucato widmete dieser Geschichte ein ganzes Kapitel ihres 2013 publizierten Buches „The Entrepreneurial State". Auf 261 Seiten zeigt die Autorin, dass viele der gemeinhin als privatwirtschaftliche Meisterleistung gefeierten Innovationen unserer Zeit eigentlich auf einen interventionistischen Staat zurückzuführen sind. Batterien, Sensoren, Chips, Siri, Touchscreen — allesamt finanziert und entwickelt von US-Regierung und US-Militär. Eine 2014 von Business Insider veröffentlichte Grafik verdeutlicht das Ausmaß. Noch 2012 warnte die DARPA selbst davor, dass Mobiltelefone bei flächendeckender Verbreitung eine ideale Waffe für verdeckte Angriffe auf die Bevölkerung darstellen.

Google existiert gleichsam nur dank Forschungsbudgets, die von CIA und NSA zur Entwicklung von Massenüberwachungswerkzeugen zur Verfügung gestellt wurden. Ein firmeninternes Video aus dem Jahr 2016 verdeutlicht die Vision von Google, mit „totaler Datensammlung die Gesellschaft verändern" zu können. Wie von Yasha Levine in seinem 2018 publizierten Buch „Surveillance Valley" dargelegt, gilt das aber nicht nur für Google, sondern für alle Big-Tech-Konzerne. Selbst bei CBS News konnte man 2011 nachlesen, wie intensiv In-Q-Tel, das Investmentvehikel der CIA, bei der Gründung von Google, Facebook, Twitter und Co. mitmischte und wie der Geheimdienst die Unternehmen seither für seine Zwecke missbraucht. Überschrift des CBS-Artikels: „Social Media is a tool of the CIA. Seriously." Übersetzt: Soziale Medien sind ein Werkzeug der CIA. Ernsthaft.

Dass man dieser permanenten Smartphone-Überwachung durch Google und Apple auch durch die Verwendung verschlüsselter Messenger-Dienste nicht mehr entkommt, veranschaulicht das unlängst von Microsoft vorgestellte KI-Dienstprogramm Recall. Es soll demnächst für Windows ausgerollt werden und dem Benutzer bei der Suche nach Dateien helfen. Dafür macht Recall alle paar Sekunden Screenshots und zeichnet damit alles auf, was auf dem Computer geschieht. Die umgehend Sturm laufenden Datenschützer versuchte Microsoft-CEO Satya Nadella damit zu beruhigen, dass die Daten nur lokal gespeichert würden, verschlüsselt seien und nach drei Monaten gelöscht werden sollen. Wenig beruhigend. Denn verschafft sich ein Hacker Zugriff auf einen Computer, muss er nur Recall aufrufen, um Zugang zu Passwörtern oder anderen sensiblen Daten zu erhalten. Ob die Daten nur lokal gespeichert und nach drei Monaten gelöscht werden, ist wie immer bei solchen Aussagen höchst fraglich. Vor allem aber zeigt ein Programm wie Recall, dass auch technisch sichere Messenger ganz simpel überwacht werden können. Dazu muss man deren Nachrichten nicht auf dem Server abfangen und entschlüsseln, sondern einfach nur durchgängig auf dem Smartphone fotografieren und zur Übertragung in Textdateien umwandeln.

Zusammenfassend muss man konstatieren: Wer seine Privatsphäre schützen möchte, sollte sein Smartphone abschalten. Oder abschaffen. Denn die von Apple und Google konfigurierten Geräte sind Wanzen, Überwachungskameras, Datenkraken und Waffen zur psychologischen Kriegsführung – keine nützlichen Werkzeuge.

In diese Kategorie fallen eher die sogenannten Dumb-Phones, mit denen man eigentlich nur telefonieren und SMS versenden kann. Die an die frühen 2000er erinnernden Geräte belästigen den Besitzer weder mit unzähligen unnötigen Applikationen noch mit nie enden wollenden Benachrichtigungen. Keine Dopamin-Shots. Keine Updates. Zudem führen die Geräte kein heimliches Eigenleben. Wenn sie aus sind, sind sie aus. Meist lässt sich sogar der Akku herausnehmen. Darüber hinaus melden solch rustikale Handys nicht permanent den eigenen Standort an eine Zentrale. Diese Argumente scheinen mehr und mehr Menschen zu überzeugen. Das 2017 neu aufgelegte Nokia 3310 verkaufte sich 2023 bereits doppelt so oft wie im Vorjahr. Versuchen Sie ihr Smartphone nur noch zwei- oder dreimal am Tag zu checken, die restliche Zeit bleibt es auf Flugmodus oder stummgeschaltet an einem fixen Ort. Kommunikation und Aufgaben, die man zuvor über das Smartphone abgewickelt hat, könnte man wieder zurück auf den PC verlagern. Die unmittelbaren Auswirkungen dieses Vorgehens auf Tagesablauf und Lebensqualität sind beachtlich. Befreiend.

Wer nicht auf ein Smartphone verzichten will oder kann, sollte sich nach Alternativen zu Google und Apple umschauen. Das iPhone fällt dabei aus, da sich das iOS-Betriebssystem nicht verändern oder ersetzen lässt. Android kann allerdings angepasst und ohne Google-Dienste genutzt werden. Zudem lassen sich Smartphone-Alternativen auch mit anderen Betriebssystemen wie GrapheneOS betreiben, die die Privatsphäre des Nutzers respektieren – solange man auch seine Apps nicht mehr aus dem Google Play Store, sondern zum Beispiel von F-Droid, Aurora oder APKPure herunterlädt.

Als Endgerät bietet sich in unseren Breiten beispielsweise ein Murena Fairphone oder Volla Phone an. In den USA ein Above Phone. Das Volla Phone wird ab Werk optional mit zwei Betriebssystemen ausgeliefert, einer Eigenentwicklung sowie GrapheneOS. Damit hat man Kontrolle über die eigenen Daten. Und nach einer kurzen Einarbeitungsphase stellt auch der Verzicht auf Google-Dienste kein Problem mehr dar — denn für praktisch jede Google-App gibt es eine überwachungsfreie Open-Source-Alternative. Tipps, Tools, Tutorials und weiterführende Informationen zum Schutz der Privatsphäre auf PC oder Telefon finden sich unter anderem bei Rob Braxman oder im Shop der „Privacy Academy".

Will man im Mediazän nicht Sklave seiner Geräte sein, muss man sich aktiv mit diesen Themen auseinandersetzen, seine Routinen ändern. Was auch immer man dahingehend gedenkt zu tun, man sollte es jetzt tun. Man muss sich diesem Netzwerk der Totalüberwachung entziehen, die Matrix verlassen, solange es noch geht. Denn die verführerische Bequemlichkeit der Observationsökonomie hat einen hohen Preis: die Freiheit. Und Smartphones sammeln längst mehr Daten über ihre Besitzer, als ein Geheimdienst es mit konventionellen Mitteln je könnte.