Google doch!

ALVERIC

22.09.2026

Einleitung

«Google doch!» Dieser Satz ist so fest im Sprachgebrauch verankert, dass er längst nicht mehr als Markenname wahrgenommen wird. «Etwas googeln» und «im Internet suchen» gelten für die meisten als dasselbe. Tatsächlich sind es aber zwei getrennte Dinge. Der Name wuchs durch Dominanz zum Gattungsbegriff, ein Prozess, den Google seit 2003 vergeblich zu stoppen versuchte. [1/2]

Ein gewöhnlicher Vormittag am Computer genügt, um zu merken, wie tief das geht. Mein eigener Tag lief lange Zeit genau so ab. Der Rechner startete mit Windows. Die Mails kamen über einen Anbieter, dessen Server irgendwo zwischen Irland und Kalifornien standen. Ein Video wurde auf YouTube geschaut, ein Dokument in einer Cloud gespeichert, deren Rechtsgrundlage ebenfalls nicht in der Schweiz lag. Keine dieser Entscheidungen hatte ich je bewusst getroffen. Ich hatte mich nie hingesetzt und gedacht, heute wähle ich die USA. Ich hatte schlicht das genutzt, was funktionierte, was vorinstalliert war, was alle anderen auch nutzten. Genau diese Unauffälligkeit ist der Kern des Problems und darum geht es in diesem Essay.

Wie ein Unternehmen zum Standard wurde

Um zu verstehen, wie tief diese Abhängigkeit sitzt, reicht ein Blick auf die Zahlen. Google Chrome hält im Jahr 2026 je nach Erhebungsmethode zwischen 65 und 71 Prozent des globalen Browsermarkts [3/4]. Entscheidend ist aber nicht der Marktanteil von Chrome allein, sondern dass Chromium-basierte Browser (Chrome, Edge, Brave, Opera, Vivaldi) zusammen rund 80 Prozent aller Browsing-Sessions weltweit ausmachen. Firefox, mit seiner eigenen Gecko-Engine, liegt bei unter drei Prozent. Diese Konzentration hat eine konkrete technische Konsequenz. Websites und Webanwendungen werden primär auf Chromiums Rendering-Engine Blink getestet, zweitens auf Firefox und Safari, seltener auf anderen Engines. Der Standard entsteht nicht durch Konsens, sondern durch Marktanteil. Was auf Blink reibungslos läuft, gilt als Standard. Was auf Gecko abweicht, wird zur Ausnahme erklärt.

Wer versucht, dem Chrome-Kosmos mit Firefox etwas entgegenzusetzen, merkt schnell, wie viel Trägheit dagegen arbeitet. Ich nutze Firefox seit zwanzig Jahren, aus Überzeugung, nicht aus Trotz. Der Grund dafür ist in erster Linie Datenschutz. Firefox blockiert Tracking durch Werbetreibende standardmässig stärker als Chrome, ist quelloffen und wird nicht von einem Konzern kontrolliert, dessen Geschäftsmodell auf dem Sammeln von Nutzerdaten beruht. Das ist mir wichtiger als jede Komfortfrage. Wer noch weiter gehen will, findet mit LibreWolf oder dem Mullvad Browser Optionen, die von Haus aus noch konsequenter auf Datenschutz getrimmt sind. Allerdings mit eigenen Einschränkungen, etwa bei der Update-Geschwindigkeit oder der Kompatibilität mit Banking-Seiten. Umso wichtiger ist es mir, an dieser Stelle nichts zu beschö-

nigen. Websites werden primär auf Blink optimiert und in diesem Umfeld getestet. Das führt bei Firefox gelegentlich zu Darstellungsproblemen, meist bei Randanwendungen, seltener bei grossen Plattformen. Hinzu kommt ein spürbar höherer Arbeitsspeicherbedarf und ein deutlich kleineres Angebot an Erweiterungen. Gut 35′000 gegenüber über 110′000 im Chrome Web Store. [5] Wer sich für Firefox entscheidet, wählt nicht den bequemeren Weg. Man gewinnt Unabhängigkeit von einem datenhungrigen Konzern, zahlt aber mit kleinen, alltäglichen Reibungsverlusten.

Wenn eine einzelne Ausgabe zur Wahrheit wird

Diese Machtverschiebung zeigt sich auch dort, wo man sie zunächst nicht vermutet. In Diskussionen über Geschichte, Politik oder aktuelle Ereignisse. Immer häufiger zitiert jemand eine KI-Antwort als Beleg für eine steile Behauptung. Die Maschine liefert dabei scheinbare Quellenangaben, die der Benutzer aber nicht überprüft. Bei genauerem Hinsehen erweisen sich diese Quellen oft als das Gegenteil von dem, was die KI behauptet. Sie widersprechen der Aussage sogar direkt. Dennoch formuliert die KI ihre Antwort so, dass der Benutzer das erwartete Ergebnis erhält. Sie wählt vage Formulierungen, die sich in beide Richtungen deuten lassen.

Bemerkenswert ist nicht primär der Fehler selbst. KI-Modelle produzieren Fehlinformationen, das ist bekannt und dokumentiert. [6] Bemerkenswert ist, wie schnell diese unbelegte Behauptung von anderen unhinterfragt übernommen und als gesicherte Tatsache weitergereicht wird, obwohl bereits Gegenrecherchen vorliegen. Eine einzelne Modellausgabe eines einzelnen Konzerns wird damit faktisch zur Autorität in einer Debatte, die eigentlich Quellenarbeit verlangt. Genau das ist die Verschiebung, um die es hier geht. Es geht längst nicht mehr nur darum, welches Betriebssystem oder welchen Browser man nutzt. Vielmehr darum, welchem Unternehmen man die Deutungshoheit über das überlässt, was als Fakt gilt.

Interessanter als der Fehler selbst ist der Mechanismus dahinter. Sprachmodelle sagen Text Wort für Wort anhand von Wahrscheinlichkeiten voraus. Sie schlagen keine Fakten in einer Datenbank nach und verifizieren nichts gegen eine Grundwahrheit. Kohärenz und Wahrheit sind für das Modell technisch nicht dasselbe. Eine falsche, aber flüssig formulierte Aussage wirkt oft sogar sprachlich kohärenter als ein ehrliches Eingeständnis von Unsicherheit. OpenAI hat in einer aktuellen Forschungsarbeit dargelegt, dass Standardverfahren beim Training und bei der Bewertung von Modellen das Raten belohnen. Sie belohnen nicht das Eingeständnis von Unsicherheit.[7/8] Das führt strukturell dazu, dass Modelle lieber selbstbewusst falsch antworten, als Unsicherheit einzugestehen.

Ein wirtschaftlicher Anreiz verschärft die Lage. KI-Anbieter müssen Kunden halten, Abonnements verkaufen. Vage Antworten, die Bestätigungen liefern, binden Nutzer stärker als ehrliche Unsicherheit. Verschwörungserzählungen werden so wohlwollend behandelt, indem die KI extra vage bleibt, damit der zahlende Kunde nicht abspringt. Das ist Das ist kein technischer Fehler mehr. Das ist ein Geschäftsmodell. Besonders problematisch ist die Autoritätsvervielfachung. Eine lokale Autorität wie ein Streamer präsentiert eine Behauptung. Die KI bestätigt diese mit scheinbaren Quellen. Die Bubble nimmt beides als doppelte Bestätigung. Die KI wird zur höheren Instanz, die den lokalen Meinungsführer legitimiert. Selbst wenn die Quellen der KI der Aussage widersprechen, zählt die Kombination aus lokaler Autorität plus KI-Autorität als Beweis. Technisch ließe sich die Behauptung widerlegen, doch in der Echo-Kammer wird jede Gegenrecherche

abgewehrt. Das Tückische an dieser Art von Fehler ist, dass sie sich sprachlich in nichts von einer korrekten Antwort unterscheidet. Ein Mensch, der unsicher ist, klingt für gewöhnlich auch unsicher. Er zögert, relativiert, verweist auf Lücken im eigenen Wissen. Ein halluzinierendes Sprachmodell tut das nicht. Es klingt exakt so überzeugt wie ein Modell, das richtig liegt. Es besitzt schlicht keinen eingebauten Mechanismus, um Zweifel auszudrücken. Und das ist kein Kinderkrankheiten-Problem, das mit der nächsten Modellgeneration verschwindet.

Dieses Problem ist bei meinen Tests am deutlichsten bei Gemini aufgetreten. Bei mehreren Vergleichstests lieferte das Modell fast immer eine Mischung aus Fakten und Halluzinationen, ohne dass sich beides unterscheiden liess. Vielleicht liegt das an meinem Prompting-Stil, vielleicht an der Architektur selbst. Für mich ist es jedenfalls ein Grund, Gemini nicht zu nutzen. Bei ChatGPT mag sich das in eine ähnliche Richtung bewegen. Dazu kann ich aber schon länger nichts mehr aus eigener Erfahrung sagen, da ich OpenAI meinerseits längst den Rücken gekehrt habe.

Drei Abhängigkeiten, ein Muster

Diese Verschiebung von der reinen Marktmacht zur Deutungshoheit darüber, was als Fakt gilt, wäre schon für sich genommen Grund genug zur Vorsicht. Sie wird aber erst dann wirklich beunruhigend, wenn man sich vor Augen führt, wem diese Macht eigentlich untersteht. Es handelt sich nicht um neutrale, staatenlose Infrastruktur, sondern um Unternehmen, die einem einzigen Rechtsraum unterliegen. Und dieser Rechtsraum hat in den letzten Jahren wiederholt gezeigt, dass er bereit ist, genau diese Abhängigkeit politisch einzusetzen.

Damit landet man fast zwangsläufig bei einem Vergleich, der auf den ersten Blick steil wirkt, die USA in einer Reihe mit Russland und China. Bei genauerem Hinsehen zeigt sich aber, dass es sich nicht um drei identische Fälle handelt. Es ist dasselbe Grundmuster mit unterschiedlichem Material.

Russland spielt für die zivile IT-Abhängigkeit der Schweiz kaum eine Rolle. Zwar gibt es eigene Sprachmodelle wie YandexGPT und GigaChat, die inzwischen sogar breite Nutzerzahlen erreichen. Sie sind aber vor allem auf den russischen Markt zugeschnitten und technologisch klar hinter den grossen westlichen und chinesischen Modellen zurück. Für den Westen ergibt sich daraus keine praktische Alternative und auch keine Abhängigkeit. Ausserhalb der Energiefrage bleibt der Berührungspunkt gering.

Bei China sieht das anders aus. Dort geht es nicht um Software, sondern um Hardware und Billigproduktion. Wie real und gleichzeitig politisch ausnutzbar das werden kann, zeigte die Corona-Pandemie. Rund 80 Prozent der Schweizer Maskenimporte stammten damals aus China.[9] Als die globale Nachfrage im März 2020 explodierte, wurde die Beschaffung zum Problem. Verschärft wurde dies dadurch, dass zeitweise selbst Nachbarstaaten wie Frankreich und Deutschland Lieferungen in die Schweiz blockierten. Der Zürcher Kantonsapotheker Andreas Hintermann brachte es damals auf den Punkt: Man sei bezüglich Schutzausrüstung vollständig von China und anderen Ländern abhängig gewesen.[10] Bemerkenswert ist, was danach geschah: nichts. Kaum hatte sich die Lage entspannt, kauften Kantone, Gemeinden und Alters- und Pflegeheime wieder überwiegend die günstigeren China-Masken. Statt die neu aufgebaute Schweizer Produktion zu stützen. Die Folge war, dass Schweizer Hersteller ihre Kapazitäten erneut herunterfahren und

Personal entlassen mussten.[11] Damals habe ich bereits vermutet, dass wir aus diesem Fehler nichts lernen würden. Ich hätte mich gerne geirrt.

Bei den USA schliesslich geht es um die Kontrolle über Hardware (Nvidia, Intel, AMD), Software, Cloud-Infrastruktur und zunehmend künstliche Intelligenz, also um die Entwicklung und den Besitz der Technologien selbst. Der entscheidende rechtliche Hebel dafür ist der CLOUD Act von 2018. Er verpflichtet US-Unternehmen, auf Anforderung amerikanischer Behörden Daten herauszugeben. Unabhängig davon, wo diese physisch gespeichert sind. Ob ein Rechenzentrum in Frankfurt, Dublin oder sonstwo steht, spielt keine Rolle. Entscheidend ist einzig, wer das Unternehmen kontrolliert.[12] Das betrifft keine Randgruppe. Amazon, Microsoft und Google kontrollieren zusammen rund 70 Prozent des europäischen Cloud-Markts. [13] Dass dieses Risiko nicht bloss theoretisch ist, zeigt ein Fall aus jüngerer Zeit. Im Zuge von US-Sanktionen wurde das Konto des Chefanklägers des Internationalen Strafgerichtshofs gesperrt.[14]

Bei künstlicher Intelligenz wiederholt sich dasselbe Muster. Nur gefühlt noch alternativloser. Man muss dafür nicht einmal Statistiken bemühen. Ein Blick auf zehn beliebige Smartphones würde vermutlich reichen. Auf den meisten davon fände sich ChatGPT, Gemini oder Claude, kaum je Vibe (Mistral, Frankreich), Lumo (Proton, Schweiz), Euria (Infomaniak, Schweiz) oder Aleph Alpha (Deutschland). Diese Beobachtung lässt sich inzwischen auch mit Zahlen unterlegen. Mitte 2026 hielten ChatGPT und Gemini zusammen rund 74% des Marktanteils bei KI-Assistenten.[15] Europäische Anbieter existieren. Mistral aus Frankreich ist mit einer Bewertung, die 2026 in Verhandlungen auf rund 20 Milliarden Euro steigen sollte, sogar Europas wertvollstes KI-Start-up.[17] Sie sind nur schlicht nicht im Bewusstsein der meisten Nutzer angekommen. Die gefühlte Alternativlosigkeit ist damit weniger ein technisches als ein Bekanntheitsproblem.

In allen drei Fällen zeigt sich dieselbe Logik: Wer abhängig ist, macht sich verletzlich. Ob Rohstoffe, Hardware oder Software, im Moment der Krise wird das zur politischen Waffe.

Die Grenzen des Vergleichs

So schlüssig dieses gemeinsame Muster auch wirkt, es wäre unredlich, dabei stehen zu bleiben. Wer die USA ernsthaft in eine Reihe mit Russland und China stellt, muss auch benennen, wo dieser Vergleich an seine Grenzen stösst. Sonst wird aus einer strukturellen Beobachtung eine bequeme Gleichsetzung, die den eigentlichen Unterschieden nicht gerecht wird.

In den USA existiert nach wie vor eine unabhängige Justiz. Sie kann den CLOUD Act oder vergleichbare Eingriffe im Einzelfall auch zurückweisen. Der jahrelange Rechtsstreit zwischen Microsoft und der US-Regierung hat das gezeigt, der überhaupt erst zur Verabschiedung des Gesetzes führte. [16] Es gibt eine freie Presse, die genau solche Fälle öffentlich macht. Und eine Zivilgesellschaft, die Konzerne und Behörden zur Rechenschaft ziehen kann. Auch wenn das im Einzelfall Jahre dauert und nicht immer gelingt. Nichts von alledem lässt sich in vergleichbarer Form für Russland oder China behaupten. Dort existieren diese Kontrollmechanismen entweder nur auf dem Papier oder gar nicht.

Doch dieser Rechtsschutz gilt in erster Linie für US-Bürger. Für alle anderen ändert sich das Bild grundlegend. Der CLOUD Act verpflichtet US-Anbieter zur Herausgabe von Daten, unabhängig vom Standort. Die Entscheidung fällt in US-Gerichten, nach US-Recht. Ausländer haben dort

kaum Möglichkeiten zur Anfechtung. Eine vorherige richterliche Prüfung nach dem Massstab des vierten Verfassungszusatzes ist nicht vorgesehen, und Betroffene werden nicht benachrichtigt. Besonders kritisch ist Section 702 des Foreign Intelligence Surveillance Act (FISA). Sie erlaubt Nachrichtendiensten den Zugriff auf Daten ausländischer Staatsbürger, ohne deren Wissen und ohne Möglichkeit zur Anfechtung. Zielpersonen werden dabei nicht einzeln durch ein Gericht bewilligt, das Gesetz erlaubt eine programmatische Überwachung anhand allgemeiner, jährlich genehmigter Richtlinien.[18] Sowohl die EU als auch die Schweiz haben inzwischen eigene Datenschutzabkommen mit den USA: das EU-US Data Privacy Framework (seit Juli 2023) und das Swiss-US Data Privacy Framework (seit September 2024).[19/20] Wie belastbar dieser Schutz tatsächlich ist, bleibt allerdings umstritten, da er auf US-Zusicherungen beruht, die eine künftige US-Regierung wieder zurücknehmen könnte. Serverstandorte in der Schweiz oder der EU schützen ohnehin nicht vor Zugriff durch US-Behörden, wenn der Anbieter US-Jurisdiktion untersteht.

Dass diese Strukturen existieren, bedeutet jedoch nicht, dass sie stabil sind. In den ersten 15 Monaten der zweiten Trump-Amtszeit stellten Bezirksgerichte mindestens 31 Mal fest, dass die Bundesregierung gegen gerichtliche Anordnungen verstossen habe. Von Massen-Entlassungen über Deportationen bis zu Immigrationspraktiken.[21] Ein Bundesrichter in Minnesota dokumentierte allein für den Januar 2026 96 Verstösse von ICE gegen Gerichtsanordnungen in 74 Fällen und hielt fest, die Behörde habe in diesem einen Monat wahrscheinlich mehr Gerichtsurteile verletzt, als manche Bundesbehörden in ihrem gesamten Bestehen.[22] 69 Richter, darunter elf von Trump selbst ernannte, beschreiben in 77 von CNN analysierten Urteilen die Administration als verfassungswidrig handelnd oder als Behörde, die ihre exekutiven Befugnisse missbräuchlich überdehnt.[23] Das ist kein theoretisches Risiko. Es ist beobachtbares Verhalten.

Ob daraus bereits der Schluss zu ziehen ist, die USA seien eine Autokratie im Sinne von Russland oder China, ist eine andere Frage. Dieses Essay will und kann das nicht abschliessend beantworten. Es wäre aber ebenso unredlich, die bestehenden Kontrollmechanismen als gegeben vorauszusetzen, ohne zu erwähnen, dass sie gerade unter erheblichem Druck stehen. Für die eigentliche Frage dieses Essays, wie abhängig man sich von US-Infrastruktur machen will, ändert das ohnehin wenig. Ein System, dessen Schutzmechanismen aktiv untergraben werden, bietet noch weniger Grund zur Beruhigung als eines, das bloss theoretisch eine Hintertür offenlässt.

Wo keine Wahl besteht

So unterschiedlich die drei besprochenen Fälle im Detail auch sind, sie alle spielen sich auf einer Ebene ab, die der Einzelne kaum beeinflussen kann. Gesetzgebung, Konzernstrategie, geopolitische Spannungen. Auf der privaten Ebene sieht das anders aus. Dort hat man tatsächlich eine Wahl, wie der Rest dieses Essays noch zeigen wird.

Bei Institutionen ist das Bild umgekehrt, und genau das macht die Sache kompliziert. Vorschnelle Unterstellungen von Bequemlichkeit greifen zu kurz. Der gesamte tertiäre Bildungsbereich der Schweiz nutzt US-Cloud-Infrastruktur, von der Universität Zürich über die ETH bis zu den Fachhochschulen. Microsoft Teams dient als Gruppentool und Office 365 als Standard.[24] Eine solche Institution könnte technisch zwar auf eigene Software oder Linux-basierte Lösungen umsteigen. Das würde aber eine Neugestaltung von Grund auf bedeuten, mit entsprechender Einarbeitungszeit für tausende Mitarbeitende und Studierende. Und mit Kosten, die schnell in die Millionen

gehen. Kaum ein Unternehmen, und schon gar keine Hochschule, kann sich das leisten, selbst wenn der Wille dazu vorhanden wäre.

Das ändert nichts daran, dass genau diese strukturelle Gefangenschaft ein Teil des Problems ist, das dieses Essay beschreibt. Die Verantwortung liegt weniger bei einzelnen trägen Entscheidungsträgern als bei einem System, das sich über Jahrzehnte in eine Abhängigkeit hineinmanövriert hat. Aus der ein Ausstieg inzwischen so teuer geworden ist, dass er kaum mehr realistisch erscheint. Für den privaten Bereich gilt das nicht in diesem Ausmass. Und genau deshalb lohnt es sich, dort anzusetzen, wo tatsächlich noch eine Wahl besteht.

Was sich privat ändern lässt

Was auf institutioneller Ebene kaum mehr rückgängig zu machen ist, sieht im privaten Bereich anders aus. Niemand zwingt eine Einzelperson dazu, ein über Jahrzehnte gewachsenes System aus tausenden Abhängigkeiten zu akzeptieren. Die eigene Infrastruktur lässt sich, Schritt für Schritt, tatsächlich verändern. Ich schreibe das aus eigener Erfahrung. Ich gehe diesen Weg seit Jahren. Mit allen Umständlichkeiten, die das mit sich bringt. Der Umstieg begann für mich nicht erst kürzlich. Seit über sieben Jahren nutze ich DuckDuckGo als Suchmaschine, gelegentlich ergänzt durch Startpage oder Qwant. Firefox ist seit zwanzig Jahren mein Browser. Für die Internetverbindung selbst kommt ProtonVPN zum Einsatz, ein europäisches Produkt. Das bedeutet zumindest bei der Frage, wer meinen Datenverkehr sieht, eine andere Antwort als ein US-amerikanischer Anbieter. Der grössere Schritt kam erst kürzlich, mit dem Wechsel des Betriebssystems selbst. Nach Jahrzehnten als Windows-Nutzer bin ich auf Pop!_OS umgestiegen. Eine Linux-Distribution, die zumindest im Alltag inzwischen überraschend reibungslos funktioniert. Auch wenn es an einzelnen Stellen noch an der eigenen Umgewöhnung hapert, etwa bei Kommandozeilen-Werkzeugen, die man unter Windows nie gebraucht hat. Parallel dazu läuft die Migration meiner Daten weg von Google. Meine Fotos wandern derzeit zu Infomaniak kDrive, einem Schweizer Anbieter.

Bei Social Media war die Entscheidung für mich ähnlich unkompliziert wie bei der Suchmaschine. Praktisch nutze ich keines, mit zwei Ausnahmen: Bluesky und Mastodon. Beide sind Microblogging-Dienste, keine Social-Media-Plattformen im engeren Sinne. Kein Instagram, kein TikTok, kein Facebook, kein X. Keine der grossen Plattformen, die ihr gesamtes Geschäftsmodell auf das Sammeln und Verkaufen von Aufmerksamkeit aufgebaut haben. Mastodon nehme ich bewusst aus. Das Netzwerk basiert auf dem Fediverse, einem dezentralen System ohne zentralen Konzern. Die Regeln legt keine Firma fest, sondern die Community selbst. Damit steht Mastodon der Denkweise dieses Essays näher als dem, wovor es warnt.

Beim Messenger ist die Situation ähnlich. WhatsApp ist in der Schweiz nach wie vor der meistgenutzte Dienst. [25/26] Selbst wer wie ich die App längst verlassen hat, wird ständig nach ihr gefragt. Fast jede Kontaktperson auf meinem Handy nutzt sie. Doch Meta, der Betreiber, verdient am Datenhandel, nicht am Service. Stattdessen nutze ich Signal und Threema. Signal ist quelloffen, verschlüsselt standardmässig und sammelt praktisch keine Metadaten, stammt aber ebenfalls aus den USA. Threema kommt aus der Schweiz, ist kommerziell aber datenschutzfreundlich. Der Umstieg ist für viele nicht vorstellbar, weil ja ohnehin alle WhatsApp nutzen. So blieb mir anfangs

nur die alte SMS. Das ist die eigentliche Falle. Die technische Alternative existiert, das soziale Geflecht nicht.

Konsequenter wurde ich dabei auch bei der eigenen Website. Ich habe alveric.ch so weit wie möglich auf das umgestellt, was gemeinhin als Small Web bezeichnet wird. Unabhängig, werbefrei, ohne Tracking, ohne die üblichen Drittanbieter-Abhängigkeiten, die auf den meisten Websites längst zum Standard gehören. Vollständig lässt sich das nicht durchhalten. Mein Hoster sieht natürlich weiterhin, welche Anfragen auf seinen Servern eingehen. Eine gewisse Restabhängigkeit bleibt also bestehen. Aber ich biete den grossen, meist amerikanischen Datenkraken keine zusätzliche Plattform mehr, über die sie meine Besucher weiterverfolgen könnten. Der Preis dafür ist real. Ohne Tracking und ohne Reichweiten-Algorithmen schreibt man im Grunde blind. Ich weiss nicht genau, was gelesen wird, was funktioniert, was niemanden interessiert. Das kostet Sichtbarkeit, in einem Umfeld, das sich fast ausschliesslich über Klickzahlen und Algorithmen organisiert. Gleichzeitig ist genau das auch die Befreiung an der Sache. Wer sich aus der Aufmerksamkeitsökonomie herausnimmt, muss auch nicht mehr nach ihren Regeln schreiben. Ganz ohne Wermutstropfen geht es allerdings nicht, und ich will das nicht verschweigen. Bei YouTube sehe ich schlicht keine gute Alternative, jedenfalls keine, auf der sich der Content finden liesse, den ich tatsächlich konsumiere. Hier endet meine eigene Konsequenz an der schlichten Realität. Eine Plattform hat manchmal so viel Inhalt und so viele Ersteller an sich gebunden, dass ein Ausstieg gleichbedeutend mit einem Verzicht auf die Inhalte selbst wäre. Nicht nur auf die Plattform.

Wo es wirklich keine Wahl gibt

Doch eine Grenze bleibt: die Hardware. Hier gibt es kaum Alternativen. Mein Computer läuft mit einer Nvidia-Grafikkarte, das Mainboard stammt letztlich ebenfalls aus einem von amerikanischen Architekturen und Patenten geprägten Ökosystem. Hier sehe ich, im Gegensatz zu Software oder Diensten, tatsächlich keine ernsthafte Alternative. Europäische Hersteller wie Infineon, STMicroelectronics und NXP decken zusammen nur etwa 8–9% der globalen Halbleiter-Fertigung ab.[27] Und selbst wenn irgendwann mehr in Europa gefertigt würde, bliebe man weiterhin von den Entwurfswerkzeugen für solche Chips abhängig, die grösstenteils von US-Unternehmen kontrolliert werden.[28] Bei Software kann man sich für eine Alternative entscheiden. Bei der Hardware darunter entscheidet man sich höchstens dafür, mit welchem Anbieter aus einem sehr überschaubaren, fast ausschliesslich amerikanisch oder asiatisch geprägten Feld man zusammenarbeitet.

Schluss

Am Anfang dieses Essays stand ein Satz, der so beiläufig daherkommt, dass man ihn kaum mehr hinterfragt, «Google doch!». Am Ende steht die Erkenntnis, dass genau diese Beiläufigkeit das eigentliche Problem ist. Niemand entscheidet sich morgens bewusst für eine Abhängigkeit. Man wächst einfach in sie hinein, mit jedem vorinstallierten Programm, jedem Standardkonto, jeder App, die alle anderen auch schon haben.

Meine Skepsis gegenüber den USA ist dabei nicht neu und schon gar nicht auf eine einzelne Regierung zurückzuführen. Sie bestand lange vor Trump und wird auch nach ihm nicht verschwinden. Sie richtet sich gegen ein System, nicht gegen eine Person. Das seine wirtschaftliche und technologische Macht wiederholt und unabhängig von der jeweiligen Administration politisch

eingesetzt hat. Die Vergleiche mit Russland und China in diesem Essay sollen das nicht relativieren, sondern einordnen. Es handelt sich um dasselbe strukturelle Muster, an unterschiedlichen Stellen mit unterschiedlichem Material, Rohstoffe, Hardware, Software und Daten. Was alle drei Fälle verbindet, ist dieselbe strukturelle Erkenntnis.

Was ich zeigen wollte, ist ein Weg, den ich selbst seit Jahren gehe, in kleinen Schritten, mit Kompromissen und offen benannten Grenzen. Bei Suchmaschine, Browser, Betriebssystem, Cloud-Speicher und sozialen Netzwerken lässt sich im privaten Bereich einiges verändern. Ohne dass man dafür Held oder Aussteiger werden müsste. Bei Hardware und bei manchen Inhalten, YouTube allen voran, bleibt man dagegen realistischerweise angewiesen auf das, was es nun mal gibt. Und selbst bei der KI bin ich noch nicht dort, wo ich eigentlich hinwill.

Ethische Risiken autonomer Agenten oder intransparenter Algorithmus-Entscheidungen sind wichtig genug für eine eigene Abhandlung. Hier steht etwas anderes im Zentrum. Die einfache Rechnung, dass man sich nicht vollständig in die Hand eines einzelnen Akteurs begeben sollte, wenn Alternativen bestehen.

Es ist Risikomanagement im Kleinen. Man muss diesen Weg nicht zu Ende gehen, um anzufangen. Es reicht, an der einen oder anderen Stelle nicht mehr automatisch ‹Google doch!› zu denken, sondern sich zu fragen, ob es das wirklich sein muss.

Quellen und Belege

- 1. Google (verb) - *Wikipedia*
- 2. Google Defends Its Trademark From Genericide - *Illinois Business Law Journal*
- 3. Die besten Webbrowser 2026 im Vergleich - *Tech Insider Deutschland*
- 4. Browser-Marktanteil-Statistiken (2026) - *VoxBooster*
- 5. Add-on (Mozilla) - *Wikipedia* und Chrome Web Store - *Wikipedia*
- 6. AI hallucination: towards a comprehensive classification of distorted information in artificial intelligence-generated content - *Nature.com*
- 7. Why language models hallucinate - *OpenAI*
- 8. Why Language Models Hallucinate - Kalai, Nachum et al., *arXiv*
- 9. Gueterversorgung in der Krise - *economiesuisse*
- 10. Knappheit in der Corona-Krise - Schweiz produziert ab Mitte April eigene Schutzmasken - *SRF*
- 11. Schweizer Maskenhersteller werden von China und Schweizer Armee verdraengt - *Blick*
- 12. The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data - *Electronic Frontier Foundation*
- 13. European Cloud Providers' Local Market Share Now Holds Steady at 15% - *Synergy Research Group*
- 14. Trump's sanctions on ICC's chief prosecutor have halted tribunal's work, officials and lawyers say - *PBS NewsHour (AP)*
- 15. ChatGPT's market share slips below 50% for first time - *TechCrunch*
- 16. Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0 - *stanfordlawreview.org*
- 17. Mistral is rumored to be raising €3B at €20B valuation - *TechCrunch*
- 18. Decoding 702: What is Section 702? - *Electronic Frontier Foundation*

- 19. EU-US Data Privacy Framework: Adequacy decision of the EU - *EDOEB*
- 20. Swiss-U.S. Data Privacy Framework: Zertifizierte US-Unternehmen bieten einen angemessenen Schutz fuer Personendaten - *admin.ch*
- 21. Trump administration defied federal court orders at least 31 times, review finds - *Scripps News (AP)*
- 22. Holding the Trump Admin Accountable for Violating Court Orders - *Just Security*
- 23. Trump's Own Judges Turn on Him in Blizzard of Blistering Rulings - *The Daily Beast*
- 24. 13 Fragen und Antworten zur Microsoft 365-Einfuehrung an der ETH Zuerich - *IOZ AG*
- 25. Signal vs WhatsApp vs Threema: 3 Mrd. Nutzer (2026) - *Shattered*
- 26. Social-Media-Nutzung stagniert in der Schweiz - *IT-Markt*
- 27. Europas Halbleiterindustrie - *Germany Trade & Invest (GTAI)*
- 28. Synopsys, Cadence Shares Surge After EDA Controls Lifted - *Silicon UK*