Freitag, 11. Juli 2025, 14:00 Uhr
~4 Minuten Lesezeit

Nichts zu verbergen

Die Leichtfertigkeit, mit der viele Menschen ihre Daten im Internet hinterlassen, könnte sie langfristig in unangenehme Situationen bringen, auch wenn sie nichts verbrochen haben.

von Günther Burbach
Foto: Pla2na/Shutterstock.com

Es gibt kaum eine Aussage, die dem Prinzip des Datenschutzes drastischer zuwiderläuft als „Ich habe doch nichts zu verbergen“. Für viele klingt das

beruhigend. Aber was, wenn genau dieser Satz der Anfang vom Ende der eigenen Selbstbestimmung ist? Was, wenn unsere Daten, unsere Kontakte, unsere Vergangenheit oder sogar die Vergangenheit anderer, mit denen wir nur am Rande zu tun haben, plötzlich gegen uns verwendet werden? In einer Welt, in der Konzerne wie Palantir ganze Bevölkerungen durchleuchten können, reicht es als Verdachtsgrund oft schon, dass man überhaupt existiert. Wer wissen will, wie weit wir unsere Freiheit bereits verloren haben, muss nicht auf dystopische Zukunftsromane warten. Die Zukunft ist längst da, sie heißt: Datenschatten.

Die neue Währung heißt Kontrolle

Palantir wurde einst als Datenanalyse-Startup mit „guten Absichten“ gegründet. Heute ist es ein Milliardenkonzern, dessen Software von US-Geheimdiensten, europäischen Polizeibehörden, Migrationsdiensten und Finanzinstitutionen genutzt wird. Was Palantir liefert, ist kein Rohdatenzugang: Es liefert Erkenntnisse, Profile, Prognosen. Wer mit wem Kontakt hatte. Wer wann wo war. Wer welche Risikobewertung erhalten sollte.

> ***Dabei geht es nicht mehr darum, ob jemand ein Verbrechen begangen hat. Es geht darum, ob jemand in einem Netzwerk auftaucht, das möglicherweise als „auffällig“ kategorisiert wird. Und dazu reicht schon eine digitale Verbindung: ein Like, ein gemeinsames Foto, ein Standort zur selben Zeit.***

Menschen werden nicht mehr nach ihren Handlungen beurteilt,

sondern nach ihrer rechnerischen Wahrscheinlichkeit.

Der Freund eines Freundes ist das Risiko

Stell dir vor, du lernst jemanden kennen. Vielleicht auf der Arbeit, vielleicht bei einem politischen Treffen. Du verstehst dich gut, ihr schreibt euch. Du hast nichts zu verbergen. Aber was, wenn dein neuer Bekannter vor Jahren an einer Demonstration teilgenommen hat, die auf einer geheimen Watchlist stand? Was, wenn er früher in einer Gruppe war, die heute als „extremistisch“ eingestuft wird? Was, wenn seine Cousine einmal mit einer Person gesprochen hat, die unter Beobachtung steht?

Schon bist du in einem System wie Palantir möglicherweise als Risikoverbindung markiert. Nicht, weil du etwas getan hast. Sondern weil du existierst und dich mit jemandem verbunden hast. Die Software macht keine Fehler, sie folgt nur der Logik der Wahrscheinlichkeit. Aber die Konsequenzen sind real: keine Einladung mehr zu einer Stelle, keine Einreise mehr in ein Land, eine plötzliche Prüfung deines Steuerprofils.

Datenschutz als Nebelwand

Es heißt immer: „Wir haben doch Datenschutz in Europa.“ Aber Datenschutz ist oft nichts weiter als ein juristischer Schleier. In Wahrheit klicken wir täglich Nutzungsbedingungen weg, die länger sind als jede Kurzgeschichte. Kaum jemand liest sie. Und wenn, versteht er sie nicht. Genau das wissen die Anbieter. Wer sich mit der Datenschutz-Grundverordnung (DSGVO) brüstet, weiß oft genau, wie er sie umgehen kann: mit Intransparenz, mit Standardvertragsklauseln, mit technischen Schlupflöchern.

Schutz durch neue Software? Auch das kann Illusion sein

Selbst wenn du versuchst, dich zu schützen, mit VPN, mit Linux, mit kryptografischen Tools, bleibst du in vielen Fällen auf die Integrität der Anbieter angewiesen.

> ***Jede Schutzsoftware braucht Updates. Jedes Sicherheitstool wird irgendwann von jemandem gepflegt, der entscheiden kann, was „sicher“ ist.***

Selbst Open-Source-Lösungen können kompromittiert werden. Die Idee vollständiger digitaler Kontrolle über die eigenen Daten ist in einer Cloud-Welt ein Mythos.

Was Palantir heute schon kann

Palantir erstellt im Auftrag von Behörden Bewegungsprofile, kombiniert Daten aus Gesundheitsakten, Social Media, Steuerdaten und Telefondiensten. Es kann auf Basis von Metadaten erkennen, wer sich mit wem wann wo getroffen hat. Es analysiert Muster, erstellt Verhaltensprognosen und liefert Risikobewertungen. Für Polizeibehörden, Nachrichtendienste, Auslandsgeheimdienste, aber auch für Konzerne.

Der Einsatz dieser Technologie erfolgt oft ohne Wissen der Betroffenen. Und mit jeder staatlichen Kooperation wächst die Reichweite. Die Grenze zwischen Strafverfolgung, Gefahrenabwehr, Wirtschaftsanalyse und politischer Kontrolle verschwimmt.

Was passieren könnte, wenn …

Was, wenn kriminelle Kartelle sich Zugang zu solchen Plattformen verschaffen? Was, wenn ausländische Mächte, skrupellose Unternehmen oder korrupte Beamte Profile über Richter, Abgeordnete, Journalisten, Gewerkschafter oder Aktivisten erstellen lassen? Was, wenn plötzlich Erpressungen stattfinden, nicht wegen Taten, sondern wegen persönlicher Schwächen, Familienkonstellationen oder politischen Neigungen? Was, wenn man gar nichts mehr „falsch“ machen muss, um ein Problem zu werden? Reicht es dann, unbequem zu sein?

Es geht um mehr als Daten. Es geht um Macht.

Wir leben in einer Gesellschaft, in der die Kontrolle über Informationen zur Kontrolle über Menschen geworden ist.

> ***Die Macht, Daten zu besitzen, zu verknüpfen und auszuwerten, ist längst mächtiger als die meisten staatlichen Instrumente. Palantir ist nur ein Beispiel. Doch es steht für eine Entwicklung, die wir nicht mehr stoppen, sondern nur noch verstehen und begrenzen können.***

Wer heute sagt „Ich habe nichts zu verbergen“, hat vielleicht einfach nicht verstanden, wie wenig es braucht, um in den Fokus zu geraten. Und wie wenig es braucht, um aus einem freien Bürger einen gläsernen Menschen zu machen, dessen Leben algorithmisch berechnet wird.

Das Netz der Schattenmacht ist bereits gespannt. Die Frage ist nur, wer es bemerkt. Und wer es durchschneidet, bevor es zu eng wird.

Günther Burbach, Jahrgang 1963, ist Informatikkaufmann, Publizist und Buchautor. Nach einer eigenen Kolumne in einer Wochenzeitung arbeitete er in der Redaktion der Funke Mediengruppe. Er veröffentlichte vier Bücher mit Schwerpunkt auf Künstlicher Intelligenz sowie deutscher Innen- und Außenpolitik. In seinen Texten verbindet er technisches Verständnis mit gesellschaftspolitischem Blick — immer mit dem Ziel, Debatten anzustoßen und den Blick für das Wesentliche zu schärfen.