BUCH

Die notwendige Revolution

Er ist der Erfinder des Big-Data-Modells – und kämpft gegen die digitale Überwachungswirtschaft. Ein Insiderbericht

Eric Dolatre, Thilo Komma-Pöllath | Ariston © 2021 | 320 Seiten

Buch kaufen

getAbstract-Rating

★ 8 | Meinungsstark | Praktische Beispiele | Insiderwissen

Das lernen Sie

- Wie der Cloud Act die DSGVO aushebelt und US-Behörden Zugriff auf Ihre Daten bekommen
- Was Ihr Smartphone und Smarthome heimlich über Sie verraten und wie Geräte Sie ausspionieren
- Warum datensichere Alternativen trotz Bedarf am Markt kaum eine Chance haben
- Welche paradoxe Rolle Gratisdienste bei der Entstehung der Datenmonopole spielten

Vermittelte Skills

Schützen Sie Ihre Daten und Privatsphäre | Digitalkompetenz aufbauen | Berufliche Kompetenzen

Über die Autoren

Eric Dolatre war einer der Gründer des Webportals GMX. Sein Modell benutzerprofilabhängiger Werbung gilt als Vorläufer von Big Data.

Rezension

Wir brauchen mehr Datenschutz. In dieses Horn stoßen viele Autoren. Doch der Weckruf dieses Autors schallt besonders laut. Kenntnisreich und mit klaren Argumenten zerlegt er die Illusion der hiesigen Digitalpolitik, die sich mit der Datenschutz-Grundverordnung schon auf gutem Weg wähnt. Dennoch gerät der Autor hie und da ins Plaudern über den Aufstieg des Internets in Deutschland, den er aus erster Hand miterlebte. Die Zukunft, die er schildert, scheint düster – doch es gibt Wege, die dystopische Entwicklung zu vermeiden. Ein Buch für alle, die noch nach Gründen suchen, ihre Datensicherheit selbst zu erhöhen.

Take-aways

- Kostenlose Apps und Onlineportale spähen ihre Nutzer aus.
- Die Überwachung von Konsumenten ist werbenden Unternehmen viel Geld wert.
- Die Überwachungspraxis von demokratischen Ländern und die von unfreien nähern sich an.
- Der Cloud Act der USA macht die europäische DSGVO zum Papiertiger.
- Im Jahr 2025 wird Microsoft Office-Nutzer vollständig in seine Cloud gezwungen haben.
- Datensichere Alternativen haben auf dem Markt derzeit keine Chance.
- Europa muss massiv in digitale Infrastruktur investieren, wenn es ein datenschutzkonformes Internet will.
- Die deutschen Digitalpolitiker haben den Ernst der Lage nicht begriffen.
- Merken Sie sich: Was im Internet gratis ist, ist tendenziell gefährlich.

Zusammenfassung

Kostenlose Apps und Onlineportale spähen ihre Nutzer aus.

Die größten digitalen Konzerne der Welt arbeiten nach einem Geschäftsmodell, das für Nutzer scheinbar kostenlos ist. Im Hintergrund sammeln sie jedoch die privaten Daten der Nutzer und verkaufen sie an Werbeunternehmen. Durch immer höhere Geschwindigkeiten im Netz können immer mehr Cookies und werberelevante Daten übertragen werden – ohne dass Nutzer es merken. Die Praxis steht seit 2018 im Widerspruch zur Datenschutz-Grundverordnung

(DSGVO) – dennoch geht sie weiter. Den Grundstein dafür legten deutsche Verlage mit gebührenfreien Digitalangeboten. Statt Geld zu verlangen, stellten sie in Hoffnung auf Reichweite und Werbeerlöse Inhalte kostenlos ins Netz. Das bereitete den Boden für Facebook & Co., die den Verlagen den Werbemarkt aus der Hand nahmen.

> *„Google, Amazon, Facebook, Apple und Microsoft sind die größten Influencer der Gegenwart, sie haben ein Beeinflussungsmonopol geschaffen, das einer freien Welt zuwiderläuft."*

Dieses Geschäftsmodell verletzt nicht nur Postgeheimnis und Privatsphäre. Es monopolisiert auch das Wissen über die Nutzer bei wenigen US-Konzernen. Dass wir ihnen blindes Vertrauen entgegenbringen, unserem Rechtsstaat hingegen misstrauen, wenn er zur Kriminalitätsbekämpfung unsere Daten einsehen will, scheint paradox.

Der Markt für Kostenlosdienste wäre kleiner, wenn ihm ein seriöses Marktsegment gegenüberstehen würde, bei dem Nutzer bezahlen würden. Leider hat sich im Internet eine „Kostenloskultur" durchgesetzt.

Die Überwachung von Konsumenten ist werbenden Unternehmen viel Geld wert.

Anzeigen in Zeitungen erreichen massenhaft Leute, die sie als Käufer eigentlich gar nicht ansprechen wollen – etwa Männer bei Damenbindenwerbung. Digitalkonzerne bieten der Werbewirtschaft Zielgenauigkeit ohne Streuverluste. Den digitalen Handel mit Nutzerdaten betreiben Adresshändler wie Deutsche Post Direkt, die über 37 Millionen Adressen mit einer Milliarde Einzelinformationen über Personen verknüpft. Dafür interessieren sich Datenbroker. Die weltgrößten sind die Konzerne Adobe und Oracle. Oracle reichert permanent drei Milliarden Personenprofile mit tagesaktuellen Informationen aus 700 Millionen Social-Media-Posts, 15 Millionen Webseiten und Tausenden Onlineshops an.

Die aufbereiteten Daten werden dann verkauft – an Werbeindustrie, Unternehmen, Parteien oder zurück an die Quelle, Google und Facebook. Google besitzt den weltgrößten Vermarkter von Onlineanzeigen. DoubleClick, eine von Google übernommene Werbefirma, verdiente 2018 mit Werbung 116 Milliarden Dollar. Insgesamt ist der Datenhandel ein weltweiter Markt von mehreren Hundert Milliarden Dollar. Eine einfache Adresse kostete 2018 beim Adresshändler Schober 1,16 Euro, ein angereicherter Basisdatensatz rund 40 Euro. Die Datenbestände sind beliebte Ziele von Hackern.

Die Überwachungspraxis von demokratischen Ländern und die von unfreien nähern sich an.

Bei der Überwachung geht es nicht nur um uns als Konsumenten, sondern auch als Bürger. Konzerne und Sicherheitsbehörden arbeiten zusammen. Die Überwachungspraxis in demokratischen und die in unfreien Ländern nähern sich an. Wie in China gilt auch bei Geheimdiensten Europas und der USA eine sichere Verschlüsselung als Bedrohung, die es zu verhindern gilt. Die Überwachungsmöglichkeiten sind heute weit vielfältiger als damals bei der DDR-Staatssicherheit. Dafür gibt es einige Beispiele:

- Ein im iPhone verbautes Barometer misst präziser als GPS, in welchem Stockwerk Sie sich gerade befinden und wie lange Sie sich wo aufhalten.
- Die Sprachassistenz Alexa hat sieben eingebaute Mikrofone, die bei Ihnen zu Hause permanent zuhören und sich nicht ausschalten lassen. Wie viele Mikrofone in einem iPhone stecken, ist Betriebsgeheimnis; in neuen Autos sind es bis zu fünf.
- In den meisten in China hergestellten Laptops überwachen Keylogger-Chips jeden Buchstaben der Tastatur und übermitteln das Getippte.
- Der Messenger WhatsApp transferiert bei jeder Änderung von Einträgen das komplette Adressbuch Ihres Smartphones auf seine Server – auch die Kontaktdaten Ihrer Bekannten, die weder bei Facebook noch WhatsApp sind.
- Der chinesische Staat verwendet für sein berüchtigtes „Social Scoring“ die Daten der in China omnipräsenten App WeChat, um die Bürger zu kontrollieren.
- Ein Tesla sammelt in einer Fahrtstunde so viele Daten wie ein Flugzeug in drei.

Der Cloud Act der USA macht die europäische DSGVO zum Papiertiger.

2018 hat die US-Regierung unter Donald Trump ein Gesetz verabschiedet, das US-Konzerne verpflichtet, Kundendaten an US-Behörden auszuliefern, selbst wenn diese auf Servern in Europa gespeichert sind. Es ist der Clarifying Lawful Overseas Use of Data Act oder kurz Cloud Act. Jedes Rechenzentrum eines US-Unternehmens unterliegt dem Cloud Act, auch wenn es in Castrop-Rauxel steht. Er verbietet auch effektive Verschlüsselungen, die Geheimdienste außen vor lassen.

> *„Der Cloud Act höhlt die DSGVO aus und reduziert sie zu einer reinen Formalie.“*

Der Cloud Act ist hierzulande kaum bekannt. Er lässt sich nicht mit der DSGVO vereinbaren. Es gibt keine Möglichkeit, sowohl die europäische Norm als auch die amerikanische zu erfüllen. Die Folge: US-Digitalkonzerne verstoßen bei europäischen Kunden gegen hiesige Gesetze. Fast alle Apps in deutschen App-Stores sind nicht datenschutzkonform. Jeder Handwerker, der

mit Ihnen per WhatsApp kommuniziert, missachtet die DSGVO. Jede Lehrerin, die Office 365 verwendet, ebenfalls. Auch nachdem der Europäische Gerichtshof 2020 feststellte, dass der Abfluss persönlicher Daten nach Amerika den Datenschutz aushebelt, geht es damit weiter. Somit ist nicht die DSGVO, sondern der Cloud Act der beherrschende Datenschutzstandard in Europa – und zwar ein niedriger.

Im Jahr 2025 wird Microsoft Office-Nutzer vollständig in seine Cloud gezwungen haben.

Der Konzern Microsoft hat bei Bürosoftware und Betriebssystemen eine Monopolstellung. Diese Abhängigkeit wird durch den Cloud Act noch heikler. Das Kernforschungszentrum CERN in Genf möchte jegliche Software des Konzerns verbannen. Die Stadt München hat es ab 2006 mehrere Jahre lang versucht und stieg auf Linux um. Als der US-Konzern daraufhin seine Deutschlandzentrale nach München verlegte, revanchierte sich die Lokalpolitik und führte seine IT zurück zu Microsoft.

> *„Von Microsoft ist Deutschland heute abhängiger als von russischem Öl oder Gas.“*

Für das Jahr 2025 hat der Konzern angekündigt, den weltweit wichtigsten Mailserver, Microsoft Exchange, in seine Cloud zu verlagern. Es wird auch nicht mehr möglich sein, Microsoft-Programme wie Office auf dem lokalen Rechner, also ohne Cloud-Anschluss zu betreiben. In dem Jahr werden zudem der ultraschnelle 5G-Standard etabliert sein sowie die digitale Kommunalverwaltung. Für den Datenschutz sind das alarmierende Aussichten.

Datensichere Alternativen haben auf dem Markt derzeit keine Chance.

Datenschutz hat auf dem freien Markt kaum eine Chance. Die dominanten werbefinanzierten Monopole drängen sichere Alternativen beiseite. Das Investitionsklima für datenschutzbewusste Gründer ist frostig. Start-up-Finanzierer finden Datenschutz nicht sexy. Lieber finanzieren sie einen weiteren E-Roller-Anbieter als den ersten sicheren Messenger. Aussichtsreiche Gründer gehen dank der besseren Finanzierung ohnehin lieber gleich ins Silicon Valley.

> *„Ist der Gedanke wirklich so abwegig, dass wir unsere sensibelsten Daten schützen müssen?“*

Die Misere zeigt sich unter anderem bei zwei Start-ups deutlich. GMX war Ende der 1990er-Jahre eins der meistgenutzten E-Mail-Portale. Die vier Gründer finanzierten den Dienst auch über Werbung. Diese wurde den Nutzern nach Benutzerprofil zugeschaltet. Das Ausfüllen der Nutzerprofile war jedoch freiwillig. GMX war ein Pionier auf dem Weg zur individuellen Onlinewerbung, dem sogenannten Targeting, und dem Auswerten von Nutzerdaten, sprich Big Data. Vor der Privatsphäre der Nutzer zogen die Gründer jedoch eine Grenze. Heimliches Mitlesen von Mailinhalten oder Chats, um die Zielgenauigkeit der Werbung zu erhöhen, wurde diskutiert, aber abgelehnt. Nach der Übernahme durch United Internet und dem Ausscheiden der vier Gründer bis 2002 folgte GMX der Branche auf dem Weg in die ausufernde Datensammlung zu Werbezwecken.

Ein anderes Start-up, der deutsche Messengerdienst ginlo, bietet datenschutzrechtlich alles, was es braucht. Dessen App ist vollverschlüsselt: Daten werden sowohl beim Speichern als auch beim Versenden unlesbar gemacht. Doch die App hat sich kommerziell nicht etabliert.

Europa muss massiv in digitale Infrastruktur investieren, wenn es ein datenschutzkonformes Internet will.

Datenschutz im digitalen Netz herzustellen, ist eine gesamtgesellschaftliche Aufgabe. Europa sollte sich dabei durch Investitionen im digitalen Raum von den USA emanzipieren. Bislang gibt es weder bei Hardware noch bei Software, Betriebssystemen, Mikrochips oder Apps europäische Alternativen. Die Entwicklung einer unabhängigen Digitalinfrastruktur würde die EU rund eine Billion Euro kosten. Behörden können aber einen wichtigen Schritt tun, indem sie durch ihre Beschaffungspolitik Anbieter datenschutzkonformer Lösungen unterstützen. Daneben ist eine Digitalsteuer ein sinnvolles Instrument gegen die Steuervermeidung der US-Digitalkonzerne. Frankreich und Österreich haben sie eingeführt. Google gab die Steuer durch höhere Werbepreise an seine Werbekunden weiter.

> *„Was wir brauchen, ist ein Internet ohne Risiken und Nebenwirkungen.“*

Jeden Tag entstehen 2,5 Trillionen Byte an Daten, die entsprechend zusätzlichen Speicherplatz benötigen. Neun der zehn größten Cloud-Anbieter der Welt sind US-Unternehmen; ihr Marktanteil in Europa liegt bei mehr als 80 Prozent. Auch mangels eigener Kapazitäten zur Datenspeicherung liegt eine europäische Datensouveränität also in weiter Ferne. Staatliche

Cloud-Projekte wie Gaia-X kommen spät und nur mühsam in Gang. Der Ansatz ist jedoch richtig: Eine sicher verschlüsselte Cloud ist kostengünstiger als viele einzeln verschlüsselte Apps. Voraussetzung ist, dass Firmen, die nicht datenschutzkonform arbeiten, von der Plattform ausgeschlossen bleiben – das beinhaltet vor allem auch US-Anbieter.

Die deutschen Digitalpolitiker haben den Ernst der Lage nicht begriffen.

Voraussetzung dafür, dass der „Marshall-Plan für die Digitalisierung“ umgesetzt werden kann, ist ein radikales Umdenken der Entscheider. Es gibt den Posten der Staatsministerin für Digitalisierung im Bundeskanzleramt, über Jahre bekleidet von Dorothee Bär. Die scheint sich nicht daran zu stören, dass ihr iPhone abgehört werden kann und ihre Apple Watch ihre Gesundheitsdaten überträgt. Dem Amt fehlt es, nicht nur in Sachen Datenschutz, an Durchschlagskraft, Ernsthaftigkeit und Geld. Nötig ist ein vollwertiges Bundesministerium für Digitalisierung.

> *„Mit jeder Apple Watch kann sich die NSA drei Mitarbeiter sparen.“*

Daneben brauchen wir eine Regulierungsbehörde, die Verbraucher vor Produkten mit vorinstallierter Spionagetechnik schützt, etwa Fernsehern mit integrierter Alexa. Wer für digitale Dienste bezahlt, etwa per Abo, muss damit effektiv vor Werbung geschützt sein. Heute gibt es Anbieter wie Sky, die trotz Aboservice mit Kundendaten Geld verdienen. Die Datenschutzbehörden der Länder sollten die Sicherheitsstandards in Unternehmen, Behörden und Verbänden prüfen und zertifizieren. Ein digitales Prüfsiegel wäre ein Standard, der Sicherheit signalisieren könnte. Wenn deutsche Nutzer US-Software aufrufen, müssten Warnhinweise erscheinen, die auf den möglichen Zugriff durch US-Behörden hinweisen. Apps sollten wie Filme eine Altersfreigabe erhalten. Es bräuchte sowohl eine Weltsicherheitsbehörde und eine eigene Polizei für das Internet als auch eine digitale Gerichtsbarkeit, um Hetze und Beleidigungen verfolgen und ahnden zu können. Die Plattformbetreiber müssen für Inhalte haften. Schulen benötigen ein Budget für Digitalisierung und Weiterbildung. Ansonsten greifen Lehrer aus finanzieller Not weiterhin zu den billigen Lösungen aus USA und Fernost.

Merken Sie sich: Was im Internet gratis ist, ist tendenziell gefährlich.

Lesen Sie die AGBs, bevor Sie Software oder Apps installieren. Was da steht – vom Haftungsausschluss bis zur Anzahl und Tiefe der abgegriffenen Daten –, wird Sie misstrauisch machen. Der wichtigste Schritt ist, dass Sie erkennen: Was im Internet nichts kostet, ist gefährlich. Bezahlen Sie besser für digitale Dienstleistungen, anstatt sie scheinbar kostenlos

in Anspruch zu nehmen. Abgesehen davon können Sie noch mehr tun, um Ihre Daten zu schützen:

- Nutzen Sie Qwant oder MetaGer als Suchmaschine. Damit umgehen Sie US-Server.
- Als berufliches Netzwerk verwenden Sie eher Xing als LinkedIn. Beschränken Sie sich bei den Daten, die Sie dort preisgeben, strikt aufs Geschäftliche. Auch sollten Sie sich von Facebook oder TikTok fernhalten.
- Neben dem sicheren Messenger ginlo ist der Schweizer Dienst Threema empfehlenswert. WeChat sollten Sie dagegen auf keinen Fall installieren.
- Schalten Sie WLAN und Bluetooth unterwegs aus, um Tracking zu vermeiden, und aktivieren Sie Ortungsdienste nur, wenn Sie sie benötigen. Überprüfen Sie auf panopticlick.eff.org, ob Ihr Browser Sie vor Tracking schützt.
- Wollen Sie im Netz anonym surfen, nutzen Sie ein Prepaid-Zweithandy, das Sie nie zu Hause benutzen. Auch den App-Store nutzen Sie mit anonymem Mail-Account und zahlen mit Guthabenkarte.
- Für die Gebäudeautomation – Smarthome genannt – halten Sie sich an den europäischen KNX-Standard. Er stellt sicher, dass bei der Soft- und Hardware für das Smarthome keine Daten abfließen.
- Sagen Sie konsequent Nein zu Sprachassistenten.
- Verschleiern Sie die MAC-Adresse Ihres MacBooks. Die outet Sie in Onlineshops als zahlungskräftigen Apple-Kunde und Ihnen werden höhere Preise angezeigt.