Peter Schaar
Überwachung total

aufbau

Peter Schaar

Überwachung total

Wie wir in Zukunft unsere Daten schützen

aufbau

ISBN 978-3-351-03295-1

Aufbau ist eine Marke der Aufbau Verlag GmbH & Co. KG

1. Auflage 2014

Einbandgestaltung hißmann, heilmann, Hamburg
Satz LVD GmbH, Berlin
Druck und Binden CPI – Clausen & Bosse, Leck
Printed in Germany

www.aufbau-verlag.de

Inhalt

Diagnose Totalüberwachung

Am 6. Juni 2013 hat sich unsere Sicht auf das Internet dramatisch verändert. An diesem Tag veröffentlichten die Washington Post und der britische Guardian erste Dokumente, die der ehemalige Geheimdienstmitarbeiter Edward Snowden gesammelt und auf drei tragbaren Computern ins Ausland mitgenommen hatte. Schon diese ersten Veröffentlichungen offenbarten die atemberaubenden globalen Überwachungsaktivitäten des amerikanischen Computergeheimdienstes NSA. Seither wird die Welt immer wieder durch neue Enthüllungen in Atem gehalten.

Es ist nicht mehr zu leugnen: Nicht nur die Geheimdienste autoritärer »Schurkenstaaten«, auch westliche Nachrichtendienste überwachen unsere Kommunikation, und sie sammeln viele Daten über unser Verhalten. Ihre Grenzen werden dabei in erster Linie von den eigenen Fähigkeiten bestimmt, weniger durch Gesetze und schon gar nicht durch moralische Grundsätze. Sie handeln gemäß einer Devise, die dem Minister für Staatssicherheit der verflossenen DDR, Erich Mielke, zugeschrieben wird: »Um wirklich sicher zu sein, muss man alles wissen.«

Solange es Geheimdienste gibt, streben sie nach Informationen, von denen sie annehmen, dass sie für ihre Regierungen nützlich sein könnten. Bisweilen ist die Informationssammlung auch Selbstzweck und dient dem eigenen

Machtgewinn. Auch in der alten, analogen Welt galt für die Geheimdienste nicht das Gebot der Mäßigung – die Grenzen der Nachrichtensammlung waren wie heute überwiegend praktischer Natur. Aber weil es viel mühsamer war, Daten zu sammeln, zu kopieren und auszuwerten, konzentrierte man sich auf »lohnende« Ziele. Das alltägliche Leben der allermeisten Menschen wurde weder registriert noch überwacht. Lediglich in Überwachungsstaaten wie der DDR hatten Geheimdienste die Aufgabe, die Menschen auch in ihrem Alltag soweit wie möglich auszuforschen. Dass dabei riesige Datensammlungen entstanden, zeigen die vielen Kilometer Aktenregale, die in der Stasi-Unterlagenbehörde zu besichtigen sind.

Trotzdem waren selbst die in autoritären Regimen angehäuften Informationsbestände ein Klacks gegen die Datenmassen, die Geheimdienste heute aus der Digitalkommunikation erlangen und in elektronischen Speichern ablegen. Die NSA sieht in der Informationsgesellschaft ein »goldenes Zeitalter«, wie ein im Internet zu findendes Strategiepapier[1] belegt – vermutlich sehen das andere Nachrichtendienste ähnlich.

Dabei haben die Geheimdienststrategen im Blick, wie sich die Informationstechnik weiterentwickelt. Das Zauberwort heißt »ubiquitous computing« – allgegenwärtige Datenverarbeitung. Digitale Informationen entstehen vielfach auch dann, wenn die Betroffenen davon nichts mitbekommen: Technische Daten, die für den Betrieb der Geräte, für den Aufbau von Verbindungen und für viele Dienstleistungen erforderlich sind. Wenn wir den Fernseher einschalten, mit dem Auto oder mit öffentlichen Verkehrsmitteln unterwegs sind oder beim Bezahlen an der Supermarktkasse erzeugen eingebaute Computerchips solche »Metadaten«. Selbst wenn wir keinen PC benutzen und das Handy zu Hause bleibt, hinterlassen

wir so immer mehr digitale Spuren. Einen erheblichen Beitrag zur Datenanhäufung leisten die vermeintlich »kostenlosen« Internetangebote, die wir in Wirklichkeit mit unseren Daten finanzieren. Viele Dienste rechnen sich nur, weil sie unser Verhalten und die Interessen registrieren und die Daten zur möglichst treffsicheren Platzierung personalisierter Werbebotschaften verwenden. Je zahlreicher die angehäuften Nutzerdaten sind, aus denen die Unternehmen Verhaltens- und Interessenprofile ableiten können, desto besser.

Von dem immer weiter perfektionierten Tracking und Targeting, der möglichst umfassenden Verfolgung des Nutzers im Netz, profitieren auch die Geheimdienste. Die aus kommerziellen Gründen eingesetzten Mittel zur elektronischen Wiedererkennung von Nutzern liefern auch ihnen Erkenntnisse über persönliche Interessen und Verhaltensweisen. Internetunternehmen bestellen das Feld für staatliche Überwachung. Wie wir inzwischen wissen, ernten Nachrichtendienste die privatwirtschaftlich bestellten Datenfelder großflächig ab – sei es mit legalen Mitteln, sei es unter Ausnutzung technischer Schwachstellen bei Google, Facebook & Co.

Die im Verborgenen agierenden Nachrichtendienste setzen gewaltige Ressourcen ein, um die bei der digitalen Kommunikation angehäuften Datenbestände auszulesen, zu kombinieren und zu bewerten. Im Mittelpunkt steht dabei natürlich nicht mehr die »Wanze«, die unter dem Bett oder Schreibtisch einer Zielperson versteckt wird. Es geht vielmehr um die Bildung umfassender Kommunikations-, Verhaltens- und Bewegungsprofile von jedermann. Angestrebt wird die Datengewinnung »from anyone, anytime, anywhere«, also die totale Überwachung, wie die NSA unumwunden zugibt. Der Dienst sieht sich dabei als Maschine, als Teil eines »Netzwerks von

Sensoren, die interaktiv messen, reagieren und sich in Echtzeit gegenseitig alarmieren.« Die Überwachung beschränkt sich nicht auf Verdächtige. Erfasst wird jeder, der elektronisch kommuniziert oder sich digitaler Hilfen bedient. Wo Gesetze im Wege stehen, wird versucht, sie im eigenen Sinne umzudeuten und sie zu umgehen. Oder man hält sich nicht an sie.

Dabei sind sich die Nachrichtendienstler durchaus bewusst, dass Unternehmen, Staaten und Nutzer versuchen, sich zu schützen. Um die befürchtete »Erblindung« zu vermeiden, setzt man alles daran, die Datenverschlüsselung und andere Schutzmechanismen auszuhebeln. Während Nachrichtendienste offiziell vor Hackern und feindlichen Mächten warnen, die unsere Daten aus dem Cyberspace bedrohen, suchen sie nach unbekannten Lücken in der Hard- und Software und nutzen sie aus. Zugleich wird daran gearbeitet, die gegen Datenmissbrauch und andere virtuelle Bedrohungen gerichtete Datenverschlüsselung zu schwächen.