Datenschutz und Internet – Es ist kompliziert!

Peter Schaar¹

Online publiziert: 14. Mai 2020

© Springer-Verlag GmbH Deutschland, ein Teil von Springer Nature 2020

Zusammenfassung

Angesichts der zunehmenden Bedeutung des Internets für die private, geschäftliche und staatliche Kommunikation werden dessen Datenschutzdefizite systemrelevant. Die damit einher gehenden Risiken lassen sich durch datenschutzrechtliche Vorschriften allein nicht beherrschen. Sie müssen ergänzt werden durch informationstechnische Sicherungen, die bereits beim Systemdesign greifen (Privacy by Design). Zudem müssen das Verbraucher- und Wettbewerbsrecht und die Haftungsregelungen der neuen Situation angepasst werden.

„Datenschutz und Internet passen nicht zusammen“. Leider ist an dieser weit verbreiteten Ansicht mehr als ein Körnchen Wahrheit. Das Internet hat sich rasant zu einem Medium entwickelt, bei dem Überwachung und das Sammeln von Daten über seine Nutzerinnen und Nutzer immer mehr Raum einnimmt. Bei vielen Business-Modellen steht die kommerzielle Verwertung der Nutzerdaten sogar im Vordergrund. Der jeweils angebotene Service wird so gestaltet, dass dabei möglichst viele Daten generiert werden, die sich auswerten und monetarisieren lassen. Die Finanzierungsmechanismen der vordergründig „kostenlosen“ Dienstleistungen sind für die Nutzerinnen und Nutzer weitgehend intransparent, genauso wie der konkrete Beitrag, den ihre Daten dabei leisten. Personenbezogene Daten sind die wichtigste Währung, in der wir für die Inanspruchnahme digitaler Dienste bezahlen, aber es fehlt das Preisschild. Anbieter berufen sich auf Betriebs- und Geschäftsgeheimnisse, wenn wir wissen wollen, wie sie mit unseren Daten umgehen und welchen Mehrwert sie daraus schöpfen.

Spätestens seit den Enthüllungen von Edward Snowden im Jahr 2013 ist zudem allgemein bekannt, dass staatliche Stellen, allen voran Geheimdienste, das Netz zur globalen, umfassenden Überwachung nutzen (vgl. [1–3]). Sie können dabei nahtlos auf die privatwirtschaftliche Datenmaximierung aufsetzen und gelangen zu tiefen Einblicken in unser Verhalten und unsere Persönlichkeit.

Der von Shoshana Zuboff geprägte Begriff „Überwachungskapitalismus“ [4] beschreibt zutreffend unsere heu-

tige, zugleich von Kommerzialisierung, Überwachung und individuellem Kontrollverlust geprägte Gesellschaftsordnung.

Historisches

Rein technisch stand schon in den Frühzeiten des Internets nicht die Vertraulichkeit im Vordergrund. Schon in den 1980er-Jahren wurde der Nachrichtenaustausch über das Netz mit dem Versenden einer Postkarte verglichen, bei der jeder am Transport Beteiligte, etwa der Postbote, nicht nur die Absender- und Empfängeradressen, sondern auch den Inhalt mitlesen kann. Und viele erinnern sich noch an die 1993 veröffentlichte Karikatur, in der einem vor einem Bildschirm sitzenden Hund die Worte in den Mund gelegt werden: „On the Internet, nobody knows you’re a dog“ [5]. Weder die Vertraulichkeit, noch die Integrität und Authentizität der über das Internet übertragenen Informationen waren gesichert.

Standards

Bei der Festlegung der dem Internet zugrunde liegenden Standards haben Datenschutz und Informationssicherheit keine Rolle gespielt. So sieht das TCP/IP Protocol keine Sicherheitsvorkehrungen gegen unberechtigte Kenntnisnahme vor. Dies gilt auch für weitere technische Festlegungen, etwa für das zur Zuordnung von IP-Adressen und Domainnamen verwendete Domain Name Systeme (DNS) und das zur Steuerung des Routing eingesetzte Border Gateway Protocol (BGP) (vgl. [6]). Man kann also sagen, dass die Sicherheitsmängel in den Genen des Internets verankert sind. Die vor Jahrzehnten definierten Standards bilden nach wie vor

✉ Peter Schaar
schaar@caid-berlin.de

¹ Europäische Akademie für Informationsfreiheit und Datenschutz, Berlin, Deutschland

zentrale technische Konventionen der Internetkommunikation. Ohne zusätzliche Sicherheitsmaßnahmen ist es nicht nur möglich, Inhalte mitzulesen und unbefugt zu verändern. Zugleich bieten die Standards Angriffspunkte für das Tracking der Nutzeraktivitäten und das gezielte Abgreifen von gespeicherten Daten.

Infrastrukturdefizite

Zwar wurden derartige Praktiken frühzeitig als „unethisch“ gebrandmarkt, doch bewirkte diese Einordnung zunächst keine Änderungen an den zugrunde liegenden technischen Strukturen, Standards und Prozessen. Die Diskussion über Datenschutz und Datensicherheit konzentriert sich nach wie vor auf die Anwendungsebene, vernachlässigt aber die digitalen Infrastrukturen: Wer eine Ressource oder einen Dienst über das Internet anbietet oder nutzt, soll dafür sorgen, dass die Vertraulichkeit und Integrität der Daten gewährleistet sind. Die zugrunde liegenden Strukturen erfahren immer noch nicht die Beachtung, die sie unter Datenschutz- und IT-Sicherheitsgesichtspunkten verdienen.

Dass Forderungen, elektronisch verarbeitete Daten zu schützen, bei der Gestaltung des frühen Internets keine Rolle spielten, hängt eng mit der Motivation der Entwickler und der sie finanzierenden Einrichtungen zusammen. Treiber der Internetentwicklung war das US-Militär, aus dessen Etat auch die finanziellen Ressourcen stammten. Träger und Begünstigte waren zunächst die Universitäten mit verteidigungsrelevanter Forschung, die ein Netz schaffen sollten, das selbst dann noch funktioniert, wenn Teile des Netzwerks durch nukleare Kriegseinwirkung zerstört würden. Daran, dass einmal massenweise schützenswerte personenbezogene Daten von der Internetkommunikation betroffen sein könnten, war in dieser Frühphase nicht zu denken. Der dezentralen Struktur des Internets entspricht es, dass lediglich für Teilbereiche – etwa die Vergabe von IP-Adressen und Domainnamen – (bisher) weitgehend akzeptierte internationale Strukturen bestehen.

Kommerzialisierung

Erst in den späten 1980er-Jahren öffnete sich das Netz allmählich auch nichtuniversitären Einrichtungen. Dies eröffnete viele Chancen für eine technikaktive Protestszene, deren Ausläufer bis in die Gegenwart reichen – wie etwa den deutschen Chaos Computer Club. Es dauerte aber nicht lange, bis sich das Internet immer weiter von einem nutzerorientierten zu einem von geschäftlichen Interessen geprägten Medium wandelte. Immer stärker in den Vordergrund rückt seither die wirtschaftlich motivierte Bereitstellung von digitalen Informations- und Serviceangeboten. Deren Finanzierung unterschied sich zunächst nicht so sehr von ihren

analogen Vorbildern, bei denen die Kunden für die jeweils in Anspruch genommene Leistung zu zahlen hatten.

Tracking und Profiling

Das 1996 entwickelte Hypertext Transfers Protocol (HTTP) ermöglichte es, physisch verteilte Informationen so zu bündeln, dass sie für den Nutzer einheitlich auf einer Webseite präsentiert werden. Damit entstand die Möglichkeit, von externen Dienstleistern bereitgestellte Werbung einzublenden. Diese Dienstleister – etwa das 1995 gegründete und seit 2007 zum Google-Imperium gehörende Unternehmen DoubleClick – waren damit nicht nur in der Lage, anbieterübergreifend Werbebotschaften zu platzieren, sondern können darüber hinaus die Datenabrufe einzelnen Geräten und Nutzern der jeweiligen Webseiten zuordnen. Mithilfe von Cookies konnten aus unterschiedlichen Bereichen stammende Nutzerinformationen zusammengeführt und in Profilen gespeichert werden.

Heute ist die exzessive Sammlung aller möglichen Daten über unser Verhalten nicht mehr die Ausnahme, sondern die Regel. Sie beschränkt sich nicht mehr auf die virtuelle Welt sondern erfasst zunehmend auch unser wirkliches Leben. Bisher analoge Geräte werden digitalisiert und vernetzt. Der Bereich, in dem unser Verhalten nicht erfasst, vermessen und beurteilt wird, schrumpft in atemberaubendem Tempo.

It's the Economy, Stupid!

Es ist nicht die Digitalisierung an sich und auch nicht die Vernetzung, die unsere Selbstbestimmung beeinträchtigen und die Menschen tendenziell zu Marionetten degradieren. Diese Entwicklung ist das Ergebnis einer wirtschaftlichen Verwertungslogik in Bezug auf unsere Daten, die zu einer ungeheuren Wissens- und Machtkonzentration bei wenigen riesigen Unternehmen geführt hat. Das heutige Internet ist – anders als in seinen Anfängen – das Gegenteil einer dezentralen Informationsinfrastruktur und es steht zunehmend unter Kontrolle weniger hochpotenter Player.

Daten sind in ungeheurem Umfang außerhalb der Kontrolle der einzelnen Nutzerinnen und Nutzer konzentriert. Die nicht ganz ernst gemeinte Definition, dass sich Cloud-services vor allem darin von klassischen IT-Strukturen unterscheiden, dass die Daten nicht mehr auf dem eigenen, sondern auf einem fremden Computer verarbeitet würden, beschreibt zutreffend einen wichtigen Aspekt der heutigen informationstechnischen Realität, wobei die Kontrolle immer stärker bei wenigen, international tätigen Unternehmen liegt.

Allerdings werden auch solche Daten im Interesse der Datenoligopolisten verwendet, die auf dezentralen Geräten gespeichert sind. Die Betreiber von Anwendungsplattformen bestimmen weitgehend, welche Apps zur Nutzung

freigegeben werden und welche Informationen sie an wen ausspielen können. Deutlich wurde deren Einfluss jüngst bei der Festlegung der Standards für die Nachverfolgung von Kontakten im Zusammenhang mit der Bekämpfung der COVID-19 Pandemie. Apple und Google – und nicht die Weltgesundheitsorganisation – legten die weltweit für das Contact Tracing gültigen Standards fest. Mag sein, dass das von den Konzernen favorisierte „dezentrale“ Verfahren gegenüber dem konkurrierenden „zentralen“ Modell datenschutzrechtliche Vorteile ausweist. Problematisch war aber gleichwohl, dass die entsprechenden Weichenstellungen nicht durch demokratisch oder völkerrechtlich legitimierte Akteure, sondern durch allein über die Marktmacht der Konzerne vorgenommen wurden.

Noch bedeutsamer sind die Bemühungen der Internetkonzerne, auch die Kontrolle über die Basisinfrastrukturen des Netzes zu übernehmen, etwa indem sie – und nicht die Telekommunikationsunternehmen – die Nutzer mit dem Netz verbinden. Hinzuweisen ist hier etwa auf das Projekt „Loon“ der Google-Mutter-Alphabet [7] zur Versorgung abgelegener Gegenden mit Internet oder das Vorhaben von Amazon, eine globale Internetversorgung über mehr als 3000 Satelliten zu gewährleisten („Projekt Kuiper“) [8]. Auch Facebook ist dabei, wenn neue Märkte erschlossen werden: Das Unternehmen setzt dabei auf Internetdrohnen, die auch in der Wüste und im Dschungel einen Internetzugang ermöglichen sollen [9]. Auch weniger sichtbar, – aber nicht weniger wirksam – erweitern die Konzerne ihre Kontrolle über die Internetinfrastrukturen. So ist der Alphabet im Begriff, sich über den Service „Google Public DNS“ [10] noch tiefer in der Infrastruktur des Internets zu verankern.

Letztlich versuchen global tätige Unternehmen, ihre jeweiligen Ökotope zu Synonymen des Internets zu entwickeln, eines proprietäre „Internets“, in der letztlich nur eine Instanz die vollständige Kontrolle ausübt und damit über den Umgang mit Informationen im wirtschaftlichen Eigeninteresse entscheidet.

Datenschutz

Das in den 1970er-Jahren in seinen Grundzügen entwickelte moderne Datenschutzrecht sollte negativen Folgen der Digitalisierung entgegenwirken. Ausgehend von dem bereits im 19. Jahrhundert geforderten Privatsphärenschutz (Privacy) [11] und dem Schutz vor Datenmissbrauch¹ wurde er 1983 ergänzt um das Grundrecht auf informationelle Selbstbestimmung:

Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig².

Der Schutz personenbezogener Daten wurde mit der 1981 in Kraft getretenen Datenschutzkonvention des Europarats [12] zu internationalem Recht und er wird durch die EU-Grundrechtecharta geschützt.

Der Einzug digitaler Technik und des Internets in den modernen Alltag verursachte vielfältige neue Datenschutzprobleme und verschärfte bestehende Risiken. Die von den Parlamenten vieler Länder und seit Mitte der 1970er-Jahre beschlossenen Datenschutzgesetze und die EG-Datenschutzrichtlinie von 1995³ trugen diesen besonderen und teils neuartigen Risiken nur unzureichend Rechnung. Das Datenschutzrecht musste dementsprechend um Regelungen ergänzt werden, die der neuen Gefahrenlage entsprechen.

Datenschutz-Grundverordnung

Ein wichtiger Anstoß für ein effektiveres Datenschutzrecht kam erneut aus Europa: Die 2016 vom Europäischen Parlament gebilligte und seit dem 25. Mai 2018 wirksame EU-Datenschutz-Grundverordnung (DSGVO) ist in allen Mitgliedstaaten direkt anwendbares Recht. Neben dieser Harmonisierung bedeutsam ist die Tatsache, dass die Datenschutzaufsichtsbehörden endlich wirksame Instrumente bekamen, Datenschutzverstöße wirksam zu ahnden. Sie können unzulässige Verarbeitung untersagen und sie können Geldbußen in erheblicher Höhe erheben (bis zu 20 Mio. € oder – darüber hinausgehend – bis zu 4 % des Konzernjahresumsatzes).

Der durch die DSGVO ausgelöste Impuls zeigt Wirkung. Inzwischen wird die Terra Incognita des Datenschutzes, also diejenigen Staaten, in denen personenbezogene Daten keinen oder nur minimalen Schutz genießen, zum Glück kleiner. Selbst im Ursprungsland des Internets, den USA, gibt es inzwischen Datenschutzgesetze, die die Verarbeitung durch Unternehmen schützen, allerdings nur auf Ebene von Bundesstaaten. Hervorzuheben ist in diesem Zusammenhang der am 1. Januar 2020 in Kraft getretene California Consumer Privacy Act.

Kritisch ist allerdings anzumerken, dass die neuen Gesetze noch weit davon entfernt sind, die von den Gesetzgebern beabsichtigten Wirkungen zu entfalten. Angesichts der un-

¹ § 2 Hessisches Datenschutzgesetz v. 07.10.1970, Hessisches GVBl. 1970, S. 625.

² Bundesverfassungsgericht, Volkszählungsurteil vom 15.12.1983, BVerfGE 65,1,1.

³ Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

geheuren Marktmacht einiger weniger digitaler Unternehmen und der Einschließungs-(Lock-in-)Effekte erweist sich insbesondere die Einwilligung als (aus Datenschutzsicht) weitgehend stumpfes Schwert, den exzessiven Umgang mit persönlichen Daten einzuschränken. Allerdings ist hier das letzte Wort noch nicht gesprochen, denn zahlreiche Einwilligungstexte werden von den Datenschutzbehörden als unwirksam angesehen.

So hat die französische Datenschutzbehörde CNIL den von Google verwendeten Einwilligungstext beanstandet und das Unternehmen mit einem Bußgeld in Höhe von 50 Mio. € belegt [13]. Das Unternehmen hat den Bußgeldbescheid angefochten, sodass diese Angelegenheit – wie andere Verfahren auch – einer gerichtlichen Klärung harren. Bedauerlich ist, dass die für die Überwachung der Einhaltung der DSGVO gegenüber den meisten US-Internetgiganten federführende irische Datenschutzbehörde in den 18 Monaten seit dem Wirksamwerden der DSGVO keine Entscheidung über eine der vielen ihr vorliegenden Beschwerden gegen die Internetkonzerne getroffen hat und dass sie nicht eine einzige Sanktionsmaßnahme gegen ein Unternehmen ergriffen hat.

E-Privacy

Die 2001 vom Europäischen Parlament beschlossene und 2009 ergänzte E-Privacy-Richtlinie⁴, die den Datenschutz bei elektronischer Kommunikation sicherstellen sollte, war von Anfang an hart umstritten. Der Widerstand gegen ein schärferes Datenschutzrecht für das Internet kam ursprünglich hauptsächlich von denjenigen Unternehmen, die den geschäftlichen Nutzen personenbezogener Daten erkannt hatten. Bis heute wurden zentrale Regelungen der Richtlinie nicht in nationales Recht umgesetzt, etwa die Vorgaben zur Einwilligung bei der Verwendung von Tracking-Cookies.

Auch die nach dem Inkrafttreten der DSGVO erforderliche Weiterentwicklung der Regeln für den Datenschutz im Internet ist heftig umstritten. Speziell das von der Europäischen Kommission angestoßene Verfahren zur Schaffung einer verbindlichen, in allen Mitgliedstaaten direkt anwendbaren E-Privacy-Verordnung ist ins Stocken geraten. Der Rat der EU-Telekommunikations- und Transportminister hat am 3. Dezember 2019 das vorläufige Scheitern seiner fast drei Jahre währenden Bemühungen um einen Konsens über den von der Europäischen Kommission vorgelegten

Entwurf einer E-Privacy-Verordnung⁵ festgestellt. Während sich das Europäische Parlament bereits mit seiner im Oktober 2017 beschlossenen Stellungnahme [14] positioniert hatte, erwiesen sich die Regierungen als Bremser in diesem für die Zukunft der Europäischen Union, ihre Bürgerinnen und Bürger und die europäische Wirtschaft äußerst wichtigen Projekt.

Von besonderer Dringlichkeit ist ein Update der Bestimmungen zum Nutzer-Tracking, denn die auf den Umgang mit Cookies beschränkten Vorgaben der Richtlinie entsprechen immer weniger dem technischen Stand. Die neuen Tracking-Mechanismen, speziell das „Browser-Fingerprinting“, waren noch unbekannt, als die E-Privacy-Richtlinie formuliert wurde. Zudem ist nicht zu bestreiten, dass das wiederholte Abfragen von Einwilligungen zur Verwendung von Cookies nicht etwa den Datenschutz stärkt, sondern zu einer „Einwilligungs-Fatigue“ geführt hat.

Angesichts der immer größeren Komplexität der Verarbeitungsmöglichkeiten müssen die Nutzerinnen und Nutzer ein ausdrückliches Recht erhalten, ihre Datenschutzpräferenzen mittels entsprechender Programme und Einstellungen elektronisch festzulegen. Die Anbieter müssen verpflichtet werden, diese Präferenzen zu befolgen und nicht – wie es bisher vielfach geschieht – sich vor deren Einhaltung durch Klauseln in ihren Nutzungsbedingungen zu drücken.

Zunehmende Kontrolle und Überwachung

Auch wenn das Internet bis heute ein globales Netz ist, bestimmen doch nationale Interessen zunehmend seine Realität. Viele wichtige Entscheidungen waren in Wirklichkeit maßgeblich durch Regierungen und staatliche Institutionen beeinflusst. Das Internet ist nicht nur amerikanischen Ursprungs. Amerikanische Unternehmen und staatliche Akteure haben bis heute erheblichen Einfluss auf nahezu alle wichtigen, die Weiterentwicklung des Internets betreffenden Entscheidungen. Beispielhaft sei hier auf die Zuteilung von IP-Adressen und von Top-Level-Domains hingewiesen, die ursprünglich durch die Internet Assigned Numbers Authority (IANA) vorgenommen wurde, eine bei der US-Regierung unter Vertrag stehenden Behörde. Der faktische Einfluss der US-Regierung, wurde durch verschiedene Vorfälle deutlich, etwa durch die Aussetzung der Verwaltung der afghanischen Top-Level-Domain während des Afghanistankriegs. Die Aufgabe wurde zwar 2009 auf die Internet Corporation for Assigned Names and Numbers (ICANN)

⁴ Richtlinie 2009/136/EG vom 25.11.2009 zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (E-Privacy-Richtlinie).

⁵ Vorschlag für eine EU-Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (Verordnung über Privatsphäre und elektronische Kommunikation) – COM/2017/010 final – 2017/03 (COD) v. 10.01.2017.

übertragen. Allerdings behielt sich die US-Regierung beim Übergang der Verwaltung auf ICANN vor, den Vertrag über die Administration der zentralen Rootzone (IANA-Vertrag) neu auszuschreiben [8]. Angesichts der fortbestehenden US-amerikanischen Dominanz bei der Festlegung der Internetstandards verfolgen verschiedene Staaten – allen voran China – eine Neuordnung der Internet-Governance. Die zentralen Entscheidungen über die Internetstandards sollen bei der Internationalen Fernmeldeunion (ITU) gebündelt werden. Unter dem Stichwort „New IP“ sollen zudem staatliche Durchgriffsmöglichkeiten auf nationale Internetsegmente gestärkt werden.

In der letzten Dekade ist ohnehin eine Reihe virtueller „Ökosysteme“ entstanden, die zwar nicht vollständig autonom agieren, bei denen die Kommunikation und sonstige elektronische Aktivitäten zensiert und überwacht werden. Die Kontrolle der Interaktion von Teilnehmern an einem virtuellen Ökosystem untereinander und mit Akteuren in der Außenwelt unterliegt der Kontrolle durch die Eigentümer bzw. in staatlich kontrollierten Teilnetzen durch staatliche Bürokratien. Es ist zu befürchten, dass sich diese Tendenz weiter verfestigt.

Staatliche Einflussnahme

Der schon in den 1990er-Jahren feststellbare staatliche Überwachungsdruck auf das Internet verstärkte sich insbesondere nach den islamistisch motivierten blutigen Terrorattacken von 2001 (New York), 2004 (Madrid) und 2005 (London), in deren Folge 2006 die Einführung einer EU-weiten, 2014 allerdings vom Europäischen Gerichtshof annullierten Vorratsdatenspeicherung beschlossen wurde⁶. Für Geheimdienste und andere Sicherheitsbehörden wurde das Internet seither zu einem zentralen Operationsfeld. Sie nutzten und nutzen technische Überwachungsmöglichkeiten – vielfach über ihre gesetzlichen Befugnisse hinaus.

Die Machthaber autoritärer Regimes – etwa des Iran oder Chinas – unterschätzten zunächst die Möglichkeiten zur zivilgesellschaftlichen Selbstorganisation, welche die neuen, internetbasierten Kommunikationstechniken für ihre Bevölkerung boten. Insbesondere Oppositionelle nutzten die Chancen der unzensierten und weitgehend nicht überwachten Internetkommunikation. Weder der „arabische Frühling“ (vgl. [15]), der zum Sturz mehrerer autokratischer Herrscher führte, noch das zeitgleiche Aufbegehren der iranischen Jugend [16] wären ohne Internet, Facebook und Twitter denkbar gewesen. Andererseits erkannten die Regierenden – sofern sie nicht aus dem Amt gejagt wurden – bald die Überwachungs-, Zensur- und Kontrollmöglichkeiten, die das Netz bietet und sie zögerten nicht, davon

Gebrauch zu machen. Deshalb ist kaum damit zu rechnen, dass das Internet in absehbarer Zeit wieder zu einem subversiven Medium wird, das es früher bisweilen war.

So hat die chinesische Regierung im Rahmen des „Golden Shield Projekts“ das eigene Internet durch eine virtuelle Mauer weitgehend nach außen abschottet. Ausgangspunkt waren Proteste anlässlich des 20. Jahrestags des Massakers auf dem Platz des Himmlischen Friedens im Juni 2009, bei denen sich Protestler über das Internet vernetzt hatten. Heute ist das chinesische Internet durch eine „Great Chinese Firewall“ abgeschottet, die alle unliebsamen Inhalte herausfiltert. Auch die sozialen Netzwerke und Messengerdienste werden vollständig überwacht. Kritische Beiträge werden zensiert, wie etwa kürzlich unliebsame Berichte über den Umgang der Regierung mit der Corona-Epidemie Anfang 2020 [17].

Andere Staaten – Russland, Indien und der Iran, um nur die wichtigsten zu nennen – sind dabei, diesem Beispiel zu folgen. Auch dort wird versucht, vollständige Kontrolle über die elektronische Kommunikation zu erlangen, allerdings bisher noch nicht mit so durchschlagendem Erfolg wie China. Auch in Demokratien – etwa in Frankreich, Deutschland und den Vereinigten Staaten – wurden gesetzliche Bestimmungen erlassen, die Betreiber von Internetdiensten zur Ermöglichung staatlicher Überwachung verpflichten, etwa zur Ausleitung der Kommunikation mithilfe von Sicherheitsbehörden kontrollierten Überwachungsschnittstellen. Hinzu kommt ein immer rigideres, zumeist durch nationales Recht bestimmtes Regelwerk, das Dienstanbieter zur Inhaltskontrolle verpflichtet (zur Durchsetzung des Copyrights, zur Unterbindung unzulässiger Informationsweitergabe und zur Verhinderung von „Hasskommentaren“).

Segmentierung

Die technisch und politisch motivierten Eingriffe in die Internetkommunikation haben dazu beigetragen, dass sich die Aufteilung der Verantwortlichkeiten im Internet verschoben hat. Früher hatten die Betreiber der Infrastruktur für die Verfügbarkeit zu sorgen, während die anderen Akteure für die Integrität, Vertraulichkeit und den Datenschutz verantwortlich waren. Heute bestimmen wenige globale Konzerne zunehmend die Funktionsweise des Internets. Google, Facebook, Microsoft, Amazon und Apple – um nur die wichtigsten und „westlichen“ Internetunternehmen zu nennen – betreiben sowohl Infrastrukturen und bieten zugleich zahlreiche eigene Dienste an. Sie bestimmen als Plattformbetreiber darüber, welche anderen Unternehmen nach welchen Konditionen mitspielen können. Standards werden bewusst so definiert, dass sie die Kommunikation über Systemgrenzen hinweg erschweren oder unmöglich machen.

⁶ Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten. Urteil des EuGH v. 08.04.2014 (C-293/12 und C-594/12).

Auch wenn die entsprechenden Mechanismen bei den privatwirtschaftlich betriebenen Subnetzen/Ökosystemen weniger strikt sind als etwa bei staatlich vollständig kontrollierten Netzsegmenten, ist es für deren Nutzer vielfach schwierig, mit Außenstehenden zu kommunizieren. Dies gilt etwa für Messengerdienste, die jeweils mit eigenen („proprietären“) Standards funktionieren. Während ein Telefonnutzer ohne Weiteres mit den Kunden eines anderen Anbieters telefonieren oder per SMS Nachrichten austauschen kann, ist der Informationsaustausch bei WhatsApp auf die dort registrierten Teilnehmer begrenzt. Auch bei vielen anderen Diensten gibt es entsprechende Beschränkungen. Einschließungseffekte („lock-in“) sind die Folge: Nutzer haben – auch wenn es andere vergleichbare Angebote gibt – keine praktikable Alternative, weil die anderen Familienangehörigen, Kollegen, usw. ebenfalls mithilfe dieses Dienstes kommunizieren oder diese Plattform nutzen.

Was sich ändern muss

Bei der Gestaltung der Informationsgesellschaft der Zukunft geht es um die Frage, wie die Menschen ihre Selbstbestimmung zurückgewinnen können, die im Überwachungs-kapitalismus immer weiter eingeschränkt wird. Allerdings ist die Vorstellung völlig unreal, moderne Gesellschaften könnten Computer und Internet einfach abschalten und zur analogen Informationsverarbeitung zurückkehren. Die Frage nach der Zukunft des Internets und – allgemeiner – nach unserem zukünftigen Umgang mit Informationstechnik ist höchst politisch, denn es geht dabei um die fundamentale Herausforderung, ob es den demokratischen Rechtsstaaten gelingt, ihre zentralen ethischen und rechtlichen Prinzipien zu verteidigen und mit Leben zu füllen, welche die Menschheit in ihrem Jahrtausende langen zivilisatorischen Prozess unter vielen Schmerzen entwickelt hat. An erster Stelle steht dabei die Aufgabe, die Grund- und Menschenrechte im digitalen Zeitalter zu gewährleisten und zu stärken.

Datenschutz ist dabei ein zwar wichtiger, aber eben nur ein Aspekt [4, S. 29]. Er ist eine notwendige, aber keine hinreichende Bedingung, wenn es um die digitale Selbstbestimmung geht. Zu entscheiden ist nicht allein über den Umgang mit personenbezogenen Daten, sondern darüber hinaus auch über „die selbstbestimmte wirtschaftliche Verwertung der eigenen Datenbestände sowie den selbstbestimmten Umgang mit nicht-personenbezogenen Daten, die etwa durch den Wirkbetrieb eigener Geräte generiert werden“, wie die deutsche Datenethikkommission einfordert [18]. Zum einen sind deshalb weitere Rechtsgebiete gefordert, etwa das Kartell- und Wettbewerbsrecht, Transparenzanforderungen, wie sie etwa durch Informationsfreiheits- und Transparenzgesetze formuliert werden und die

Verbesserung der im Zivilrecht vorgesehenen Gewährleistungs- und Haftungsansprüche für die Hersteller von Hard- und Software.

Zum anderen geht es um die technische Gestaltung von digitalen Produkten, Dienstleistungen und Infrastrukturen, also um Ansätze, die gewährleisten, dass die ethischen und rechtlichen Anforderungen tief in der Technik verankert werden, wie es ansatzweise schon im Datenschutzrecht unter den Stichworten „Privacy by Design“ und „Datenminimierung“ geschehen ist, etwa in der EU-Datenschutz-Grundverordnung⁷.

Die DSGVO kann kein Endpunkt der Entwicklung sein. Im Hinblick auf ihre Weiterentwicklung stärker in den Blick genommen werden müssen Systeme, die für den einzelnen Menschen oder für die Gesellschaft wichtige Entscheidungen selbst treffen oder vorbereiten. Von besonderer Bedeutung ist dabei die Zusammenführung und Auswertung von Daten zum Zwecke der Bewertung (Profilbildung) und der Einsatz algorithmischer Entscheidungssysteme, etwa im Zusammenhang unter Verwendung „Künstlicher Intelligenz“ (KI) (vgl. [19]). Dringend erforderlich ist darüber hinaus die E-Privacy-Verordnung (vgl. 3.2).

Bei aller Bedeutung des europäischen Rechts dürfen wir nicht aus dem Blick verlieren, dass Europa – schon allein aufgrund der digitalen Technologieführerschaft der USA und Chinas – das notwendige Umsteuern nicht im Alleingang bewältigen kann. Verfehlte industriepolitische Weichenstellungen und die Unterschätzung der Bedeutung des technologischen Fortschritts durch das Management der meisten großen europäischen Unternehmen haben dazu beigetragen, dass die weitaus meisten global bedeutsamen Digitalunternehmen in den USA und in Asien angesiedelt sind. Zur Hoffnung Anlass gibt aber, dass inzwischen auch in vielen außereuropäischen Staaten eine Datenschutzregulierung erfolgt, die sich an der DSGVO orientiert, wie etwa der am 1. Januar 2020 in Kraft getretene California Consumer Privacy Act (CCPA). Auch das am 1. Februar 2019 zwischen der EU und Japan in Kraft getretene Freihandelsabkommen (EU-Japan Economic Partnership Agreement) garantiert in dem so entstandenen gemeinsamen Wirtschaftsraum ein der DSGVO entsprechendes Datenschutzniveau.

Wir müssen verstehen, dass die Herausforderungen der Digitalisierung eine ähnliche Dimension haben wie die Herausforderungen der Ökologie, wobei durchaus Berührungspunkte zwischen beiden Bereichen bestehen, etwa hinsichtlich des ungeheuren Energieverbrauchs (und der damit verbundenen CO₂-Emissionen) der riesigen Datenzentren, die für die Bereitstellung globaler Cloud- und Streamingdiens-

⁷ Art. 5 Abs. 1 lit. c) der Verordnung (EU) 2016/679 zum Schutz personenbezogener Daten und zum freien Datenverkehr v. 27.04.2016 (DSGVO).

te eingesetzt werden. Auch weil die ökologische Umorientierung nur unter Einsatz digitaler Techniken erfolgversprechend ist, liegt eine enge Verknüpfung beider Bereiche nahe. Vielleicht hilft ja ein neuer Gesellschaftsvertrag: ein „Green New Deal“, erweitert um die digitale Selbstbestimmung!

Literatur

1. Beckedahl M, Meister A (2013) Überwachtes Netz. newthinking, Berlin
2. Greenwald G (2014) Die globale Überwachung. Droemer, München
3. Schaar P (2014) Überwachung total. Aufbau, Berlin
4. Zuboff S (2018) Das Zeitalter des Überwachungskapitalismus. Frankfurt, New York
5. Karikatur von Peter Steiner im New Yorker. (5. Juli 1993)
6. Voelsen (2019) Risse im Fundament des Internets, SWP-Studie. https://www.ssoar.info/ssoar/bitstream/handle/document/62982/ssoar-2019-voelsen-Risse_im_Fundament_des_Internets.pdf?sequence=1&isAllowed=y&lnkname=ssoar-2019-voelsen-Risse_im_Fundament_des_Internets.pdf. Zugegriffen: 29. Jan. 2020.
7. <https://loon.com>. Zugegriffen: 9. Febr. 2020
8. Heise online (2019) Jetzt auch Amazon: Mit mehr als 3000 Satelliten Internet für fast alle Menschen. <https://www.heise.de/newsticker/meldung/Jetzt-auch-Amazon-Mit-mehr-als-3000-Satelliten-Internet-fuer-fast-alle-Menschen-4362295.html>. Zugegriffen: 9. Febr. 2020.
9. DW (2015) Per Facebook-Drohne: Internet aus der Luft. <https://www.dw.com/de/per-facebook-drohne-internet-aus-der-luft/a-18620144>. Zugegriffen: 9. Febr. 2020 (v. 31.7.2015)
10. <https://developers.google.com/speed/public-dns>. Zugegriffen: 9. Febr. 2020
11. Brandeis LD, Warren S (1890) The right to privacy. Harv Law Rev 4(5):193–220
12. (1981) Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten v. 28.1.1981. <https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108>. Zugegriffen: 9. Febr. 2020
13. CNIL (2019) The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21.1.2019. <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>. Zugegriffen: 1. Febr. 2020.
14. Europäisches Parlament (2017) Bericht v. 20.10.2017. http://www.europarl.europa.eu/doceo/document/A-8-2017-0324_DE.html. Zugegriffen: 7. Febr. 2020.
15. Steinschaden J (2012) Digitaler Frühling. Carl Ueberreuter, Wien
16. Kreye A (2010) Die Neda-Revolution. Süddeutsche Zeitung Online v. 17.05.2010. <http://www.sueddeutsche.de/politik/proteste-in-iran-die-neda-revolution-1.116965>. Zugegriffen: 9. Febr. 2020
17. Zeit Online (2020) Coronavirus, bloß nichts durchsickern lassen. <https://www.zeit.de/kultur/2020-01/coronavirus-china-regierung-vertuschung-social-media/komplettansicht>. Zugegriffen: 9. Febr. 2020 (v. 3.2.2020)
18. Datenethikkommission (DEK), Gutachten. Berlin (2019) <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf>. Zugegriffen: 2. Febr. 2020 (v. 23.10.2019, S.17)
19. Europäische Akademie für Informationsfreiheit und Datenschutz, Evaluation der Datenschutz – Grundverordnung – Vorschläge zur Weiterentwicklung des Datenschutzrechts v. 27.1.2020, S 4