

Christian Heller

POST-PRIVACY

Prima leben
ohne Privatsphäre

Verlag C.H.Beck

Google StreetView, Facebook & Co – Privatsphäre als persönlicher Raum, der sich sicher weiß vor fremden Blicken, ist praktisch tot. Schuld ist das Internet. Datenschutz ist ein Kampf gegen Windmühlen, bestenfalls ein Hinauszögern des Unausweichlichen. Wichtiger ist die Frage, wie wir unser Leben ohne die Sicherheiten der Privatsphäre lebenswert machen können. Es gab früher Zeiten ohne Privatsphäre, und es wird wieder Zeiten ohne Privatsphäre geben. Bei genauerem Hinsehen wird klar, dass sie ohnehin nicht der luppenreine Wohltäter ist, den Datenschützer gern aus ihr machen. Ihre Auflösung bringt nicht nur Aufgaben, denen wir uns stellen, sondern Chancen, die wir ergreifen sollten. Hierbei will dieses Buch helfen: durch Aufzeigen neuer Lebensführungsstrategien und alter und neuer Vorbilder hierfür.

Christian Heller ist Blogger und Filmkritiker. Er befasst sich mit Internet-Kultur und Medienkunst und betreibt die Website www.plomlompom.de.

T 44 203



Originalausgabe

© Verlag C.H.Beck oHG, München 2011
Satz, Druck u. Bindung: Druckerei C.H.Beck, Nördlingen
Umschlagentwurf: malsyteufel, Willich
Printed in Germany
ISBN 978 3 406 62223 6

www.beck.de

INHALT

1. DAS ENDE DER PRIVATSPHÄRE

Herr Meyer gibt sich dem Netz Preis 8 – Herr Meyer hätte gern ein bisschen Privatsphäre 11 – Freiwillige und unfreiwillige Entkleidung 14 – Hilfe, das Internet ist überall 17 – Die Ohnmacht des Rechts über das Netz und die Daten 20 – Kapitulation 22 – Und nun? 24

2. EINE KLEINE GESCHICHTE DES PRIVATEN

Loblied auf den öffentlichen Mann 27 – Leben im Maschinenraum 29 – Private Gemeinschaft im Mittelalter 31 – Der Aufstieg der bürgerlichen Familie 33 – Home, Sweet Home 35 – Furcht vor dem bösen Blick 38 – Privatsphäre und Freiheit 42 – Techniken des Selbst 45

3. DIE ENTFESSELUNG DER DATEN

Die ersten Daten-Maschinen 49 – Die Daten-Universal-Maschine 51 – Daten von jedem, Daten für jeden 54 – Daten für das Selbst 57 – Petabytes statt Theorie 61 – Kirche der Re-Simulation 66 – Für die Freiheit der Daten 71

4. DIE FESSELUNG DER DATEN

Deutsche Schule 74 – Datenschutz und Staat 78 – Datenschutz und private Akteure 80 – Digitale Entmündigung 83 – Wem gehören die Daten? 87 – Duldsbarkeit des Datenschutzes 92

5. INFORMATIONSMACHT

Macht und Freiheit 95 – Wissen als Macht 98 – Der Glaube an Wissen als Macht 102 – Transparenz 107 – Die Transparen-

te Gesellschaft 110 – Informationskontrolle und Gesellschaftsform 115 – Privatsphäre und Ordnung 120

6. POST-PRIVACY-TAKTIKEN

Lehren der sexuellen Revolution 124 – Das Ugol'sche Gesetz 129 – Solidarität und Transparenz 133 – Optimierung durch Transparenz 137 – Zurückhaltung oder Filter? 140 – Toleranz 142 – Entgrenzung des Einzelnen 146

7. ABWÄGUNGEN

Im Zweifel für die größere Auswahl 152 – Persönliche Praxis 155 – Die Machtfrage 156 – Risiko 158 – Utopie und Dystopie 160

DANK 162

ANMERKUNGEN 163

1. DAS ENDE DER PRIVATSPHÄRE

Die Privatsphäre ist ein Auslaufmodell. Unser Sein und Handeln, egal wie persönlich oder geheimniskrämerisch, ist zunehmend für andere einsehbar. Wir müssen lernen, damit klarzukommen. Wir treten ein in das Zeitalter der «Post-Privacy»: in ein Leben nach der Privatsphäre.

Dass unsere Privatsphäre empfindlich bedroht sei, hören wir schon länger: Nach verbreiteter Ansicht wird sie angegriffen durch den Überwachungsstaat, durch den Fluss unserer Daten ins Internet, durch kommerzielle Interessen. Exemplarisch seien einige Buchtitel der letzten Jahre genannt: *Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft*.¹ Oder: *Die Überwachungsmafia: Das gute Geschäft mit unseren Daten*.² Oder: *1984.exe*.³ Ein großes Kamera-Auge blickt drohend auf uns herab vom Cover des Bestsellers *Angriff auf die Freiheit: Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte*.⁴

Die zunehmende Einsehbarkeit unseres Lebens und der Kontrollverlust über unsere Daten gelten den meisten Autoren solcher Bücher als eine Bedrohung, gegen die wir uns zur Wehr setzen müssen: *Ausgespäht und abgespeichert: Warum uns die totale Kontrolle droht und was wir dagegen tun können*.⁵ Oder: *Die wissen alles über Sie: Wie Staat und Wirtschaft Ihre Daten ausspionieren – und wie Sie sich davor schützen*.⁶ Oder: *Die Datenfresser: Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückverlangen*.⁷

Eines eint das vorliegende Buch mit den eben genannten Titeln: der Glaube, dass unsere Privatsphäre gerade von allen Seiten heftigst bedrängt wird. Aber daraus folgere ich nicht den Auftrag, die Privatsphäre entschlossen zu verteidigen. Ich halte den Kampf zu ihrer Rettung für längst verloren. Vielleicht lohnt es sich, ihn hier und da noch eine Weile zu führen – aber nur aus taktilen Gründen, und sicher nicht um jeden Preis. Das «Ende der Privatsphäre» bedeutet nämlich nicht unbedingt den Weltuntergang. Was es uns

an Freiheit bringt, nicht beobachtet zu werden, das wird in mancher Weise überschätzt. Hingegen eröffnet uns der Pfad, der uns in die Post-Privacy führt, viele neue Freiheitsräume – und die gilt es, zu erkunden. Die Post-Privacy kommt – und wir sollten lernen, das Beste aus ihr zu machen. Das sind, im Groben, die Ideen, die hinter diesem Buch stecken.

Warum bin ich mir so sicher, dass das Ende der Privatsphäre gekommen ist? Manchem klingt die These vielleicht ein wenig gewagt. In diesem ersten Kapitel werde ich versuchen, sie plausibel zu machen. Für Lesefaulen die Kurzfassung: Schuld ist das Internet.

Herr Meyer gibt sich dem Netz preis

Das «Internet» ist ein Netz (und einfach «Netz» werde ich es im Folgenden oft nennen) aus intelligenten Maschinen: den «Computern». Sie ernähren sich von Informationen, und eben damit füttern wir sie auch. Sie speichern diese Informationen, verarbeiten sie und schicken sie untereinander hin und her.

Im Netz breiten sich Wissen, Intelligenz und Verständigung aus. Es ist ein junges, heranreifendes Gehirn. Es wächst durch alles, was von außen hineingegossen wird. Über den ganzen Planeten streckt es seine Fühler aus. Das Netz will alles lernen über diese Welt, in die es hineinwächst, in der es langsam zu Bewusstsein gelangt. Sein Speicher ist unendlich groß, entsprechend auch sein Hunger nach Erfahrung, Input, Daten. Tabus wie Datenschutz oder Staatsgeheimnisse kennt seine Neugier nicht.

Gleichzeitig ist das Netz in zunehmendem Maße Unterbau des gesellschaftlichen, kulturellen und persönlichen Lebens von uns Menschen. Nahezu alles ist daran angeschlossen, verewigt sich darin, tauscht sich darüber aus. Wer heutzutage nicht den Anschluss verlieren möchte, der muss am Netz teilnehmen. Und dafür verwandelt er sich in das Blut, in den Lebenssaft des Netzes: in maschinenlesbare Information, also «Daten». Um mitzuspielen, geben wir der Neugier des Netzes das, was sie begeht.

Stellen wir uns einen Herrn Meyer vor. Herr Meyer will ins Netz. Das Kabel ist gelegt, sein Computer mit dem Internet verbunden.

Was macht Herr Meyer jetzt? Er tippt etwas auf der Tastatur oder klickt mit der Maus irgendwo hin. Auf diese Weise erzeugt er Informationen, die für das Netz bestimmt sind: Anfragen, Wünsche, Eingaben. Die schickt er übers Kabel hinaus. Ins Netz gehen heißt also: einen Kommunikationsvorgang mit dem Netz beginnen, etwas sagen und auf Antwort warten.

Dort, im Netz, schauen sich Herrn Meyers Informationen, seine Bitten um Antwort, für ihn um. Sie tauschen sich mit anderen herumvagabundierenden Informationen und Informationsvorgängen aus. Und irgendwann, wenn sie glauben, das zu haben, was Herr Meyer sucht, schicken sie es ihm als Antwort zurück. Während dieses Vorgangs hinterlassen sie allerorten Spuren oder gar Kopien ihrer selbst. Über diese lernt das Netz von den Dingen der Menschen, von Herrn Meyer und seiner Welt. Herr Meyer erlangt Teilhabe am Netz, indem er ihm etwas von sich preisgibt. Und zu solcher Preisgabe bietet das Netz ihm sehr viele Möglichkeiten.

Will unser Herr Meyer fürs eigene Ich im Netz längerfristig eine Vertretung haben, dann muss er sich eine Netz-Identität aufbauen. Vielleicht bastelt er sich eine persönliche Website, eine Art Internet-Visitenkarte mit folgendem Inhalt: «Hallo, das bin ich, ich bin 42 Jahre alt, komme aus Darmstadt, und das sind Fotos meines Hundes.» Oder er legt sich ein «Profil» auf einer Website wie Facebook.com, MeinVZ.de oder wer-kennt-wen.de an: ebenfalls so etwas wie eine Visitenkarte, die Informationen wie seinen Namen, seinen Wohnort, seine Hobbys oder seine schulische Laufbahn dem Netz mitteilt. Vielleicht hört er an dieser Stelle auch schon auf mit der Selbstdarstellung: Man muss dem Internet ja nicht gleich alles von sich preisgeben, oder?

Aber wenn er will, kann Herr Meyer beliebig fortfahren. Weitere Eingabefelder locken – etwa für seine politischen Sympathien, sein Glaubensbekenntnis oder seine sexuellen Neigungen. Je mehr er eingibt, desto plastischer ist er im Netz vertreten, und umso mehr kann das Netz ihm zurückgeben. Mehr Besucher werden in seinem Profil Interessantes finden. Mehr Verbindungslien zu anderen im Netz öffnen sich ihm: «Wer hier wohl noch alles dieselbe Grundschule besucht hat wie ich?» Herr Meyer braucht in seinem Profil bloß auf den Namen seiner Grundschule zu klicken:

Prompt bekommt er alle anderen Nutzer aufgelistet, die sich in ihrem Profil als Absolventen derselben bezeichnen. Genauso läuft es mit anderen Angaben: Wer hier wohl noch alles gerne *Raumschiff Enterprise* schaut? Wer wohl noch so alles mit Frau Müller befreundet ist?

Herr Meyer kann dieses Spiel der Selbstdarstellung im Netz sehr weit treiben. Reichen ihm das Auswählen aus Vorgaben und das Ausfüllen von Beschreibungskästchen, wie es wer-kennt-wen und Facebook bieten, noch nicht? Dann startet er eben ein «Blog», um öffentlich im Netz ein Tagebuch zu führen. Oder er legt sich mit dem Dienst Twitter.com einen persönlichen Nachrichten-Ticker an. Hier kann er im Minutentakt und in SMS-Länge der Welt wirklich jede Kleinigkeit mitteilen, die ihn bewegt: von «mir ist langweilig» bis zur Zimmermücke, die seine Nachtruhe stört.

Nun hat selbst der mitteilungsbedürftigste Mensch am Tag leider nur vierundzwanzig Stunden Zeit, um ausführliche Berichte über seine Lebensführung zu verfassen. Wem der Aufwand zu groß wird, der kann diese Aufgabe an die Automaten des Netzes abschieben. Wenn er will, lässt Herr Meyer solche Protokollierungsdienste durchgängig seinen Aufenthaltsort übers Handy orten und einem beliebig großen Personenkreis mitteilen.⁸ Oder er weist sie an, alle seine Geldausgaben und Einkäufe zu erfassen und zu veröffentlichen.⁹ Rund um die Uhr, ohne Mehraufwand für ihn selbst.

Stellen wir uns vor, Herr Meyer hätte all das schon früher die Welt wissen lassen wollen. Vielleicht wäre er erzählfreudig von Mitmensch zu Mitmensch geeilt, um seine Tagesprotokolle zu verlesen. Sicher wäre ihm irgendwann jemand entgegengetreten und hätte mit strenger Stimme gesagt: «Du, wir wollen das alles gar nicht wissen. Behalte es bitte für dich.» Im Netz dagegen erreicht jede Information nur den, der sich für sie interessiert. Auf Netzbewohner prasselt ständig ein Übermaß an Daten ein. Sie haben deshalb gelernt, auszublenden, was sie nicht wissen wollen. Sie verfügen über unzählige Filter-Verfahren, die dieses Ausblenden leicht machen. So schwindet der Antrieb, jemanden in die Schranken zu weisen, weil er zu viel über sich redet. Es ist einfacher, ein überbordendes Mitteilungsbedürfnis zu ignorieren, als es zu unterbinden.

Herr Meyer hätte gern ein bisschen Privatsphäre

Ein Verteidiger der Privatsphäre könnte angesichts dessen einwenden: «So sind halt Exhibitionisten, sie müssen ihr Leben zwanghaft aller Welt aufdrängen. Normale Menschen aber haben Beseres zu tun.»

Doch wenn wir das als Exhibitionismus verunglimpfen, dann müssen wir einen rapide wachsenden Teil unserer Mitmenschen zu Exhibitionisten erklären. Mehr als neun Millionen Deutsche betreiben Selbstdarstellung auf den Profilen von wer-kennt-wen¹⁰ und doppelt so viele auf denen von Facebook.¹¹ Weltweit verfügen über 200 Millionen Menschen über ein Twitter-Benutzerkonto.¹² Zum Vergleich: Die Bundesrepublik Deutschland zählt gerade einmal etwas über 80 Millionen Einwohner. Lassen wir den ausgestreckten Zeigefinger auf die «Exhibitionisten» also erstmal stecken.

Aber es stimmt: Die meisten Menschen haben tatsächlich Beseres zu tun, als dem Netz jede Kleinigkeit ihres Lebens mitzuteilen. Viele ziehen sogar klare Grenzen, was sie der Welt preisgeben wollen und was nicht: Einige wenige, ausgewählte Daten über mich dürfen ruhig öffentlich sein. Ein paar mehr Daten, weniger streng ausgewählt, darf ein kleiner Kreis von Vertrauten erfahren. Und der Rest bleibt sicher verborgen, in der Privatsphäre der Dinge, die ich offline lasse.

Dieser Plan scheitert jedoch schon heute an den Möglichkeiten der Datenwelt. Ein Beispiel:

Wie erwähnt, können wir bei Facebook persönliche Profile einrichten und dort vieles reinschreiben – müssen es aber nicht. Beispielsweise: Wer sind meine Freunde? Was sind meine Lieblings-Musikgruppen? Bin ich hetero, bi oder schwul? Die letzte Frage betrachten viele Menschen sicher als Privatsache. Je nach Umfeld kann es sogar fürs eigene Wohl sehr ratsam sein, die eigene Homosexualität geheim zu halten.

Nehmen wir mal an, Herr Meyer sei homosexuell. Er will nicht, dass sein Facebook-Umfeld davon erfährt. So exhibitionistisch ist er nämlich gar nicht, wie eben noch angedacht. Er zieht klare Grenzen, was er der Welt mitteilen möchte und was nicht. Die

Angabe, homosexuell zu sein, wird er in seinem Profil sicher nicht machen.

Herr Meyer geht sogar noch weiter: Er versucht, gar nicht erst einen Eindruck von möglicher Homosexualität aufkommen zu lassen. Er wird sich hüten, Fotos vom letzten Christopher Street Day auf Facebook einzustellen oder andere Vorlieben publik zu machen, von denen er glaubt, sie könnten in dieses oder jenes Schwulen-Klischee passen. Mit solchen Vorsichtsmaßnahmen glaubt er sich einigermaßen sicher. Seine sexuelle Orientierung ist privat, und das soll sie auch bleiben.

Er hat seine Rechnung allerdings ohne die Tüftler vom «Massachusetts Institute of Technology» (MIT) gemacht. Dort hat man ein Verfahren entwickelt, um die Homosexualität von Männern mit Facebook-Profil mit hoher Wahrscheinlichkeit zu ermitteln, selbst wenn sie weder Fotos einstellen noch Vorlieben egal welcher Art verkünden. Alles, was man dafür braucht, ist eine Analyse ihres sozialen Umfelds auf Facebook: Dort ist man ja vor allem, um mit Freunden, Verwandten und Bekannten in Kontakt zu bleiben. Oft genug (es lässt sich abstellen, aber so besorgt sind nur wenige) führt man sie sogar in einer für alle Welt sichtbaren Freundesliste auf. Am MIT fand man nun heraus: Ob ein Student schwul ist, lässt sich näherungsweise vorhersagen über einen bestimmten Anteil von Männern unter seinen Facebook-Freunden, die sich auf ihren eigenen Profilen als schwul outen.¹³

Herr Meyer hat seine Freundesliste nicht geheim gehalten. Jetzt ist er entdeckt. Seine Privatsphäre im Netz hört eben nicht erst dort auf, wo er ausdrücklich etwas von sich mitteilt. Das bisschen Leben, das er von sich öffentlich macht, gibt genug Anhaltspunkte, um noch viel mehr davon freizulegen.

Das Netz wird durchstreift von Computer-Intelligenzen, die Experten sind in Detektivarbeiten wie der eben beschriebenen. Das obige Beispiel ist trivial, verglichen mit ihrem übrigen Können: In ihrer Kombinationsgabe erwecken sie oft den Eindruck eines digitalen Sherlock Holmes. Trainiert werden sie von den allerbesten Mathematikern und Statistikern. Gefüttert werden sie mit einem Daten-Weltwissen, das ausgedruckt und in Buchform gebunden in kein Bibliotheksgebäude der Welt passen würde.

Viele Dienste im Netz bieten uns direkten Zugriff auf solche Intelligenzen. So brauche ich mein Schlafverhalten nicht laut auszusprechen – die Seite SleepingTime.org wirft kurz einen Blick auf meinen persönlichen Nachrichtenticker bei Twitter und schließt daraus beängstigend genau auf meinen Schlafrythmus. Oder ich schenke dem Empfehlungsportal Hunch.com ein bisschen Lebenszeit. Das stellt mir am laufenden Band Fragen wie zum Beispiel: «Wie rum hängst du dein Klopapier auf?» Nach einer Weile kennt Hunch mich so gut, dass es errät, welches Automodell ich fahre und welche Partei ich wähle. Ähnliche Fragenkataloge kann ich bei der Online-Partnervermittlung OkCupid.com durcharbeiten. Die verspricht, Leute aus meiner Umgebung zu finden, die bezüglich Charakter und Interessen zu mir passen. OkCupids Formeln erweisen sich nicht nur als treffsicher, sondern sogar für Dating-Zwecke als viel zu treffsicher: Aus einer regionalen Auswahl von Hunderten oder Tausenden schlägt es mir zuvorderst Menschen vor, die ich sowieso schon dem eigenen Freundeskreis zurechne. OkCupid kann also recht gut voraussagen, wer wem in einer Stadt über den Weg läuft und dann bei dieser Person hängen bleibt.

Dass Schwule im Durchschnitt mehr schwule Freunde haben als Nicht-Schwule, ist vielleicht nicht überraschend. Herr Meyer grüßt: «Das hätte ich mir denken können, dass meine Freundesliste Hinweise auf meine sexuelle Orientierung gibt.» Aber so offensichtlich scheinen die Zusammenhänge nicht immer. Genug Statistik und Datenmengen vorausgesetzt, lassen sich auch ganz andere Muster erkennen. OkCupid bietet hierfür viele weitere Beispiele. Die Tausenden von Fragen, die man dort beantworten kann, umfassen jedes denkbare Thema: von Politik über Mathematik bis zur persönlichen Hygiene. Bei sieben Millionen Mitgliedern,¹⁴ die diese Fragebögen ausfüllen, kommt so einiges an bemerkenswerter Statistik zusammen, vor allem über die amerikanische Nutzerschaft. Interessante Entdeckungen werden regelmäßig im Firmen-Blog veröffentlicht. So scheinen etwa Anhänger der Republikaner in sich harmonischere Gruppen zu bilden als Anhänger der Demokraten: Zwei Republikaner, die bei OkCupid aufeinander treffen, haben eine höhere Paarungs-Chance als zwei Demokraten.¹⁵ Und die meisten OkCupid-Nutzer mit der Bereitschaft, auf Wunsch des

Partners Vergewaltigungsfantasien auszuspielen, kommen aus den US-Bundesstaaten Nevada, Wyoming und Florida.¹⁶

Auf dieselbe Weise sammelt OkCupid statistische Auffälligkeiten entlang der Achse zwischen Hetero- und Homosexualität.¹⁷ Herr Meyer kann diese Parameter unmöglich alle abschätzen und zwecks Verschleierung vorausahnen. Jede noch so harmlos anmutende Auswahl an Informationen könnte zu Tage fördern, was er geheim halten möchte.

Freiwillige und unfreiwillige Entkleidung

Wer weiß, was in den Mathematikerköpfen und Computerprozessoren von Internetunternehmen und Geheimdiensten noch so an Rechenverfahren wartet, um unser Intimstes zu enthüllen? Wer sich dagegen absichern will, dem kann man wohl nur zur Paranoia raten: am Besten überall nur das Allernötigste angeben; das Facebook-Profil so karg wie möglich halten; nirgendwo im Netz sich zu irgendwas unter dem eigenen Namen äußern; nur keine Daten eingeben – alles kann dich verraten.

Die Datensparsamkeit, die der Einzelne sich leisten kann, ist aber beschränkt. Er hat oft genug nur die Wahl, am Sozialkosmos des Internets teilzunehmen – oder eben nicht. Wer ein Nutzerkonto bei den gefragtesten Internet-Diensten wie zum Beispiel Amazon, Facebook oder Google hat, der hat diesen bereits den Schlüssel für das Innerste seiner Privatsphäre gegeben. Der kann sich zwar zurückhalten im bewussten, eigenwilligen Verbreiten von Bildern, Äußerungen oder Selbstbeschreibungen. Aber auch so protokollieren und archivieren diese Dienste¹⁸ jeden seiner Klicks; auf welchen ihrer Inhalte er wann und wie lange verweilt; von welchen anderen Seiten im Netz er auf sie gelangt und in Richtung welcher anderen Seiten er sie wieder verlässt; mit welchen ihrer Nutzer er sich unterhält oder auf denselben Fotos landet; nach welchen Begriffen er mit ihren Suchmaschinen fahndet; welchen ihrer Empfehlungen er folgt und welchen nicht.

Die Rechenverfahren von Amazon, Facebook und Google wälzen sich wie wild durch die so entstandenen Daten-Berge. Amazon

empfiehlt uns Bücher, von denen es glaubt, dass sie uns interessieren: Aus dem Wissen, was für Bücher wir uns auf seinen Seiten angesehen und bestellt haben, erahnt es unsere literarischen Vorlieben. Googles Suchergebnisanzeige orientiert sich nicht nur an dem Text, den wir ins Suchfeld eingegeben, sondern auch an Googles Einschätzung unserer Interessen – nach einer Auswertung unserer früheren Suchanfragen und unserer früheren Entscheidungen, bestimmte Suchergebnisse anzuklicken oder nicht. Und Facebook macht oft schaurige Vorschläge, mit wem aus seiner großen Nutzerschaft wir uns noch anfreunden sollten: zum Beispiel verstoßene frühere Affären oder andere Menschen aus verdrängten Vergangenheiten. Wie kommt Facebook auf diese Verbindungen? Durch ausgefuchtes «Datamining», also ein möglichst schlau Umgraben der Daten, die über uns selbst und all die anderen in seinen Datenbanken schlummern.

Gelegentlich wissen die Denkmaschinen des Netzes mehr über uns als wir selbst, unsere Eltern und unsere Freunde zusammengenommen. Was wir dem globalen Gehirn Internet nicht direkt über uns mitteilen, das erfasst und folgert es eben selber – notfalls, ohne uns um Erlaubnis zu bitten.

Nicht jedem gefällt das. Der Verteidiger der Privatsphäre fragt zornig: «Was erlauben diese Dienste sich?» Es gibt viel öffentliche Empörung und Klagen über mangelhaften «Datenschutz» bei all den eben genannten Internet-Riesen. Datenschützer fordern (sinngemäß): «Wissen über uns, unsere Persönlichkeit, unser Umfeld, unser Verhalten gehört unter unsere Kontrolle. Daten, die uns betreffen, sollten nicht ohne unsere ausdrückliche Erlaubnis gesammelt, ausgewertet oder gar mit anderen Daten zusammengeführt werden. Wer das tut, so wie Google oder Facebook, der gehört als Datenverbrecher an den Pranger gestellt.»

Die öffentliche Debatte darüber wird mit beträchtlicher Lautstärke geführt. Ein Großteil der Nutzer etwa von Google oder Facebook dürfte sie inzwischen mitbekommen haben – oder hat sich sogar daran beteiligt. Aber kaum jemand verzichtet deshalb auf Google oder löscht sein Facebook-Profil. Im Gegenteil: Facebook kann sich regelmäßig mit Google um den Titel des Datenschutz-Gefährders Nummer Eins streiten und ist trotzdem in den sieben

Jahren seines Daseins auf knapp 700 Millionen Nutzer angewachsen.¹⁹ Das heißt: Grob ein Zehntel der Menschheit teilt Facebook inzwischen freiwillig mindestens Name und Alter (zu einem gewissen Prozentsatz wahrscheinlich nicht ganz korrekt), Geschlecht, Freundeskreis und das eigene Klick-Verhalten mit. In westlichen Ländern beträgt der Bevölkerungsanteil mit Facebook-Profil wenigstens ein Fünftel (Deutschland) und oft genug schon die Hälfte (USA, Kanada, Großbritannien).²⁰ Und selbst wer kein Benutzerkonto hat, muss damit rechnen, dass er dennoch irgendwo in den Datensätzen von Facebook Erwähnung findet: Freunde tratschen bei Facebook über abwesende Dritte und benennen deren Gesicht auf den Gruppen- und Partyfotos, die bei Facebook lagern. Eigentlich brauchen unsere Regierungen gar keine Volkszählungen mehr – sie müssen einfach nur höflich bei Facebook anfragen.

Und wer will es all diesen Menschen verdenken, dass sie so offenerherzig mitspielen? Unterm Strich scheinen die meisten Gutes und Nützliches aus ihren Verhältnissen zu den bösen «Datenkraken» zu ziehen: Unterhaltung, Sozialleben, Selbstbehauptung. Nicht nur für die Internet-Riesen ist Datenschutz nur ein Lippenbekenntnis, sondern auch für die meisten ihrer vermeintlichen Opfer. Ein lockerer Umgang mit Informationen über andere ist längst nicht nur die Norm bei den Betreibern datensammelnder Webseiten, sondern auch bei den Nutzern untereinander.²¹ Datenschützer hoffen, irgendwann würde die Masse ihre Lektion lernen, irgendwann wäre der Bogen überspannt, irgendwann hätten alle die Nase voll von Erfassung, Durchrasterung und Verknüpfung ihrer Daten. Vor die Wahl gestellt zwischen dem Schutz ihrer Privatsphäre und einem Platz in der Neuen Welt, scheinen sich aber mehr und mehr Menschen für Letzteres zu entscheiden. So wurde im Mai 2010, aus Protest gegen die Datenschutz-Politik von Facebook, die bisher vermutlich größte öffentliche Kampagne zum Facebook-Austritt gestartet: der «Quit Facebook Day». Wie viele hatten am Ende dieses Tages geschworen, ihr Facebook-Profil zu löschen? Nicht einmal ein Zehntausendstel der Gesamt-Nutzerschaft.²²

Hilfe, das Internet ist überall

Ob den Verdateten wirklich bewusst ist, worauf sie sich einlassen? Vielleicht nicht. Aber wie sähen die Alternativen aus? Ein vehementer Verteidiger der Privatsphäre könnte vorschlagen: «Weigere dich einfach, das Internet-Spiel mitzuspielen. Halte dich konsequent raus. Bleib in der schönen Welt da draußen, fern von Internet-Eingabe-Geräten. So wahrst du deine Privatsphäre.»

Nun besteht aber einerseits ein enormer gesellschaftlicher Druck, am Netz teilzunehmen. Fernsehsendungen enden regelmäßig so: «Wenn Sie mehr erfahren möchten, besuchen Sie unsere Website unter ...» Kommentare, Wettbewerbsbeiträge und Bewerbungen sollen eingereicht werden per Online-Formular oder E-Mail. (E-Mails an Google-Mail-Adressen werden übrigens von Googles Algorithmen durchforstet, die im Text-Inhalt nach Hinweisen für passende Werbeanzeigen suchen.²³) Einladungen zu Veranstaltungen lassen sich verführerisch einfach über Facebook oder ähnliche Dienste abwickeln, was Außenstehende leicht ausschließt. Ein Verweigerer müsste nicht nur Selbstdisziplin üben, sondern vor allem wachsenden Verzicht am gesellschaftlichen Leben.

Andererseits gibt es ein solches «Außerhalb» des Internets gar nicht mehr. Das scheint vielen in Deutschland schlagartig im Sommer 2010 bewusst geworden zu sein, als die Debatte über Googles Dienst «Street View» entbrannte.

Seit 2005 erfasst und veröffentlicht Google in seinen Diensten «Google Maps» und «Google Earth» fotografisch die Erdoberfläche. Angefangen hat alles mit Satellitenfotos sämtlicher Erdregionen, von der Antarktis bis nach Garmisch-Partenkirchen. Über die Jahre wuchs die Bildauflösung dieser Fotos beständig: Konnte man früher gerade einmal das eigene Haus ausmachen, so klappt das heute fürs eigene Auto. Menschen sind zwar bisher nur als Punkte mit Schattenwurf erkennbar. Einen interessierten Blick in Nachbars Garten kann man aber trotzdem werfen.

Dann kam «Street View»: Google fährt weltweit die Innenstädte mit Autos ab, auf deren Dach Kameras montiert sind, und zwar solche mit Rundum-Ansicht: Für alle abgefahrenen Straßen entste-

hen Panoramaaufnahmen aus Sicht eines Auto-Dachs. Diese Bilder sind jetzt, neben der Draufsicht von oben, als zusätzliche Perspektive auf Google Maps und Google Earth anwählbar. Bekamen wir vorher also nur Einblick in Bereiche, die uns und unseren Augen meist unzugänglich sind – Dächer, Innenhöfe, Gärten –, werden nun die Anblicke nachgereicht, die sich auch jedem normalen Fußgänger bieten: Hausfassaden, Werbeplakate, andere Passanten – der öffentliche Raum, wie ihn jeder sieht, nicht nur der Spionagesatellit.

Umso erstaunlicher war, dass sich gerade daran eine Welle der Empörung entlud. Street View macht nichts öffentlich, was nicht schon vorher öffentlich war. Aber es macht deutlich, dass die Tentakel des Netzes inzwischen den gesamten öffentlichen Raum erfassen und nicht nur ausgewählte Punkte, die man leicht meiden kann. Befeuert durch eine skandalisierende Medienberichterstattung erkannten viele Betroffene ganz richtig: Ohne mein Zutun oder meine Einwilligung reicht der Raum, der ins Internet eingespeist wird, inzwischen bis zu meiner Wohnungstür und meinem Küchenfenster.

Die Gegner von Street View fanden viele gute und schlechte Argumente gegen den Dienst. Was sie nicht fanden, war eine wasserdichte rechtliche Handhabe: An öffentlichen Straßen gelegene Hausfassaden lassen sich schwerlich dem öffentlichen Raum entziehen, den jeder fotografieren und publizieren darf. Ins Bild geratene Passanten werden verpixelt – individuelle Persönlichkeitsrechte bleiben gewahrt. Google hatte aber ein Image als freundlicher Riese zu verlieren. Also schenkte es dem deutschen Datenschutz eine Geste der Demut: Bewohner und Besitzer von Häusern erhielten ein Einspruchsrecht zur Unkenntlichmachung ihrer Fassaden in Street View.

An der Netz-Bekanntheit dieser Fassaden ändert das wenig. Googles Rücksichtnahme reicht nur bis zur Zensur der Fassaden-Fotos, die es selbst geschossen hat – nicht aber bis zur Zensur dessen, was Google-Nutzer aus ihren eigenen Fotoapparaten heraus in den Dienst hochladen. Nutzer von Street View haben die Wahl, sich Googles Fassadenbilder überlagert von den Fassadenbildern der Nutzer anzeigen zu lassen – und einige besonders Eifrig²⁴ füllen

mit ihrer eigenen Arbeit systematisch die Bilderlücken auf, die Hausbewohner-Einsprüche in die Straßenzüge deutscher Städte gerissen haben. Und was sich an Fassaden nicht bei Google findet, findet sich vielleicht bei der Konkurrenz: Zum Beispiel bietet Sightwalk.de Panorama-Straßenansichten der wichtigsten deutschen Innenstädte an – und zwar ohne große Aufregung bereits seit 2009. Microsofts Dienst «StreetSide» macht dasselbe und befindet sich im Jahr 2011 in einer ähnlichen Kompromisssuche mit deutschen Datenschützern wie Street View. Fassaden anschauen kann man aber unzensiert schon seit Längerem bei Microsofts «Bing Maps». Das bietet im Gegensatz zu «Google Maps» nicht nur die reine Vogelperspektive in direktem Lot von oben nach unten, sondern auch in 45°-Schrägen nach allen vier Himmelsrichtungen.

All das ist nur ein Beispiel für einen allgemeineren Trend: Ob nun durch Google-Autos oder Überwachungskameras, durch staatliche Abhörwanzen oder Handyfotos, durch Webcams oder WLAN-Ortungswagen – langsam nähert sich die Erfassung unserer Welt durch Mess- und Aufzeichnungsgeräte einer Totalität an. Und was erfasst wird, wird oft genug breit weiterversetzt, vielleicht sogar jedermann zugänglich gemacht.

Allein mit einem modernen Mobiltelefon trägt bald jeder eine Foto- oder Videokamera, ein Ton-Aufzeichnungsgerät und einen Peilsender mit sich herum. Auch Internet haben diese Geräte inzwischen stets eingebaut: Die persönlichen Nachrichtenticker, die sich Twitterer nennen, berichten via Handy heute aus scheinbar jeder noch so geschlossenen Veranstaltung live. So fällt es immer schwerer, Räume gegen einen Informationsfluss nach innen oder außen abzuschotten. Man bemüht sich um ausdrückliche Twitter-Verbote, wie etwa in den geschlossenen Sitzungen des Stadtrats von Augsburg²⁵ oder der SPD-Bundestagsfraktion.²⁶ Doch selbst deutsche Gerichte sind verunsichert: Wie etwa soll während einer Gerichtsverhandlung die Echtzeit-Kommunikation des Publikums mit der Weltöffentlichkeit wirksam unterbunden werden? Das Recht scheint darauf keine saubere Antwort zu wissen.²⁷

Kaum noch ein Raum oder eine Situation scheint sicher vor den Maschinen, die die äußere Welt in Datenfutter fürs Netz verwandeln. Langfristig wirksame Abwehrmöglichkeiten gegen die Ver-

vielfältigung der Augen und Ohren um uns herum sind nicht in Sicht. Wenn morgen in jeder Brille und übermorgen in jedem Augen-Implantat eine Kamera mit Echtzeit-Übertragung in die globalen Infoströme eingebaut ist, wollen wir dann Brillen und Augen verbieten?

Die Ohnmacht des Rechts über das Netz und die Daten

Verbote – ja, warum eigentlich nicht? Der Verteidiger der Privatsphäre könnte einwenden: «Dass Technik möglich oder sogar schon da ist, heißt nicht, dass sie eingesetzt werden sollte. Diese Entscheidung hat sich dem gesellschaftlichen Wohl zu beugen. Jenes setzt sich notfalls durch den Zwang der Gesetze durch. Privatsphäre halten wir für einen Bestandteil des gesellschaftlichen Wohls. Notfalls müssen wir das Netz zum Respekt davor zwingen.»

Es kann nicht sein, was nicht sein darf: «Das Internet darf kein rechtsfreier Raum sein.»²⁸ Tatsächlich erweisen sich Gesetze aber oft genug als unfähig, dem Netz wirksam etwas vorzuschreiben.

Das Recht setzt auf die Durchsetzungsmacht einzelner Staaten in ihren Territorien. Das Netz aber greift über einzelne staatliche Machtgebiete hinaus. Erlässt Deutschland Gesetze, die das Netz regeln sollen, finden die Regelverstöße halt auf Computern im Ausland statt. Dort können sie trotzdem noch von Deutschen abgerufen oder beliefert werden, denn die Verbindungen des Netzes überschreiten Staatsgrenzen. Es bräuchte also globale Rechtslösungen. Die aber kommen nur zäh voran: Weltweit gibt es zu große Unterschiede und Widersprüche zwischen den verschiedenen Rechtsnormen und -interessen. Ehe sich hier die Kräfte sammeln, hat das Netz bereits Fakten geschaffen. Politische und bürokratische Vorgänge alter Form kommen da kaum hinterher.

Traurige Zeugen dieser Entwicklung sind die Musik- und Filmindustrie sowie ihre Brüder und Schwestern der Rechteverwertungsbranche. Lange Zeit lebten sie glücklich davon, dass ihre Produkte – Musik, Bild, Film, Text – nur auf knappen, kontrollierbaren Datenträgern aus Papier oder Kunststoff verbreitet werden konn-

ten. Dann landeten diese Produkte nach und nach als entkörperliche Information im Netz. Dabei halfen viele Millionen Netz-Nutzer: Achselzuckend verstießen sie gegen undurchsetzbare Gesetze, als sie die Inhalte gekaufter oder auch nur geliehener Datenträger in ihre Internet-Leitungen kopierten.

Findet eine begehrte Information einmal den Weg ins Netz, dann ist sie dort nur schwer wieder herauszubekommen oder sonstwie unter Kontrolle zu bringen. Das Netz ist eine Verbreitungs-, Kopier- und Gedächtnismaschine sondergleichen. Wenn ich hier irgendwo etwas lösche, kann ich mir nie sicher sein, dass nicht andernorts bereits eine Kopie gezogen wurde. Jede Information durchquert auf ihren Wegen Dutzende Vervielfältigungs-Stationen verschiedenster Betreiber. Jeder Einzelne davon kann entscheiden, ob er sich die Information kopiert, insgeheim an Dritte weiterreicht oder gar für jedermann öffentlich macht. Aussichtslos ist die Absicht, Informationen zu entfernen, die einmal durch die Tiefen des Netzes gejagt wurden. Wer gezielt eine Information im Netz zu löschen versucht, der provoziert eher Aufmerksamkeit für das, was er unterdrücken will – und damit dessen Vervielfältigung.²⁹

Die Produkte der Musik- und Filmindustrie sind ins Netz gefallen. Sie lassen sich nicht einfach wieder herausfischen. Sie entziehen sich hier der Kontrolle, die das Gesetz ihren Eigentümern eigentlich garantiert. Wild werden sie im Netz konsumiert, getauscht, verschenkt, vermischt und umgestaltet – unter Millionen von Gesetzesverstößen täglich. Um nur einen relevanten Bruchteil davon zu ahnden, müssten ganze Bevölkerungsschichten vor Gericht gezerrt werden. Dieser Kampf gegen «Raubkopierer» und «Internetpiraterie» ist so verzweifelt wie aussichtslos. Wer ihn gewinnen will, der müsste das Internet abschalten.

Genauso wie mit den Daten der Rechteverwertungsbranche verhält es sich mit unseren persönlichen Daten. Nicht nur Unternehmen wie Google oder Facebook, sondern Millionen unserer Mitmenschen befördern sie ins Netz. Geraten sie einmal in dessen Sog, dann haben wir jede Kontrolle über sie verloren. Als unbeschwerete Einsen und Nullen vervielfältigen sie sich mit Leichtigkeit, passen in jede Tauschbörsen und durchqueren mühelos jedes Einfang-Gatter, das sie stoppen sollte. Wir können natürlich weiter Gesetze er-

lassen, die diese Wirklichkeit kriminalisieren. Das heißt aber nicht, dass diese Gesetze das Gewünschte bewirken.

Kapitulation

Unser Leben lässt sich heute aufteilen in zwei Berge von Daten: solche, die jetzt bereits in irgendeinem digitalen Speicher, in irgend einer Datenbank lagern; und solche, die bald in einer solchen lagern werden.

Sind unsere Daten bereits irgendwo gespeichert, dann haben wir die Kontrolle über sie verloren – egal, was die versprechen, denen wir sie anvertraut haben. Wird nicht böswillig hinter unserem Rücken mit ihnen gehandelt, dann werden sie eben von Dritten gestohlen. Dass 2010 auf dem Schwarzmarkt angeblich anderthalb Millionen gehackte Facebook-Profilen zirkulierten,³⁰ erscheint angesichts der riesigen Facebook-Gemeinde fast schon wie eine statistische Zwangsläufigkeit. Aber selbst moderne Staaten «verlieren» schon mal das eine oder andere: So sind etwa im Jahr 2007 Großbritannien Datenträger mit insgesamt 37 Millionen Datensätzen über seine Bürger abhanden gekommen: CD-ROMs und Festplatten, die man aus Versehen frei herumliegen ließ.³¹ Doch was die unbeabsichtigte Freigabe sensibler Personen-Datensätze betrifft, hat vermutlich Sony im Frühjahr 2011 einen neuen Rekord aufgestellt: Als Opfer einer Hacker-Angriffswelle musste das Unternehmen beinahe wöchentlich eingestehen, Kundendaten wie Passwörter und Kreditkarteninformationen an Hacker verloren zu haben – die Zahl der betroffenen Kunden lag bei ungefähr 100 Millionen.³²

Wer heute Daten sammelt, speichert oder gar auswertet, kann nicht für ihre Sicherheit garantieren. Egal wie gut der Daten-Käfig aus Geheimhaltung, Verboten oder Verschlüsselung geschmiedet sein mag: Es gibt kein perfektes Sicherheitssystem. Jeder Plan hat seine Schwächen, jede Technik ihre Mängel, jede Behörde ihre Korruption. Jeder Informationsvorgang oder -speicher ist nur so vertraulich wie die fahrlässigste oder böswilligste Hand, in die er gelangen könnte. Es ist ein Merkmal des digitalen Zeitalters, dass oft

kleinste Verwundbarkeiten oder Lecks ausreichen, um die stolzesten Sicherheitsmauern vollständig zu Fall zu bringen. Und was einmal an Wissen ausläuft ins digitale Weltmeer, das lässt sich nicht wieder zurückpumpen.

Diese Lektion lernten im Jahr 2010 zum Beispiel amerikanische Militärs und Diplomaten – und weltweit Politiker, die vertraulich mit ihnen zu tun hatten. Ein einziger Saboteur scheint zu genügen, um die Datensicherheit der Vereinigten Staaten zu zerstören: Aus einem geschlossenen militärischen Netz soll sich der Soldat Bradley Manning heimlich vertrauliches Material auf eine CD-ROM kopiert, diese mit nach Hause genommen und das Ganze von dort ans Internetportal WikiLeaks.org weitergeleitet haben.³³ Kurz darauf wanderten Videoaufnahmen von einer fragwürdigen Militäroperation durchs ganze Netz und danach weltweit durch Fernsehnachrichten und Zeitungen. Genauso verhielt es sich wenig später mit der Veröffentlichung von über 90 000 internen, geheimen Dokumenten zum Afghanistankrieg³⁴ und einer Viertelmillion vertraulicher Depeschen amerikanischer Botschaften.³⁵ Wenn nicht einmal der US-Sicherheitsapparat seine Datenbanken dicht bekommt, wer dann?

Was aber ist mit dem Teil meines Lebens, der noch in keiner Datenbank steht? Nun, wir haben gesehen: Die Intelligenzen des Netzes müssen etwas nicht direkt gesagt bekommen, um es trotzdem mit guter Trefferquote vorherzusagen. Auch Daten, die für sich genommen harmlos wirken, erlauben unter Hinzunahme von Weltwissen bemerkenswerte Schlüsse. Dieses Vermögen steigt, je mehr Daten als Statistikfutter verfügbar sind. Die Kenntnisse des Netzes über uns werden fortwährend umfangreicher und tiefgehender. Zugleich wächst die Computerintelligenz, sie auszuwerten und entlegene Stellen miteinander in Beziehung zu setzen: die Befähigung, Bekanntes zum Hebel fürs Hervorkehren von bisher Unbekanntem zu machen. Eine positive Rückkopplung: Je mehr ich weiß, desto leichter fällt es mir, das zu erhellen, was ich noch nicht weiß – also: noch mehr zu wissen. Hinzu kommt, dass die maschinellen Rechen- und Speicherkapazitäten, die all dem zugrunde liegen, seit Jahren immer weiter wachsen – und damit wohl noch einige Jahrzehnte fortfahren werden.³⁶

Fassen wir zusammen: Die Zahl der Augen und Ohren um uns herum steigt. Ebenso steigt die Zahl der freiwilligen oder unfreiwilligen, böswilligen oder einfach nur fahrlässigen Informanten. Das Verbreiten von Daten fällt immer leichter. Die Menge an Daten über unsere Welt explodiert und ist immer mehr Interessierten zugänglich. Ebenso schnell wächst die Intelligenz, sämtliche Puzzleteile zusammenzufügen, um aufzudecken, was noch geheimgehalten wird. All das staut sich auf zu einem gewaltigen Druck gegen die Privatsphäre als Raum des Verborgenen. Die Orte, Gelegenheiten und Sachverhalte, die sich vor diesem Druck sicher glauben können, schrumpfen in Zahl und Größe. Es fällt immer schwerer, sie zu verteidigen.

Die Kämpfe um Datenschutz und Privatsphäre sind Rückzugsgefechte. Privatsphäre, die einmal ans Netz verloren ist, lässt sich nicht wieder zurückgewinnen. Es geht nicht mehr darum, ihr irgendeinen Gebietsanspruch dauerhaft zu sichern. Es geht nur noch darum, den Rückzug möglichst unblutig zu gestalten – und das Unabwendbare vielleicht lange genug hinauszögern, damit wir uns ein wenig darauf einstellen können: Es wird keinen Bereich mehr geben, in dem wir uns vor fremden Blicken sicher glauben können.

Und nun?

Gebe ich damit nicht etwas vorschnell auf? Ein Verteidiger der Privatsphäre könnte einwenden: «Auch wenn der Kampf schwierig bis aussichtslos erscheint – haben wir denn eine andere Wahl, als ihn zu führen? Schließlich geht es hier um die Grundlage persönlicher Freiheit in unserer Gesellschaft. Wenn der Kampf dafür sinnlos geworden sein soll, dann können wir das Menschengeschlecht ja gleich ganz abschreiben.»

Sicher, die Privatsphäre kann förderlich sein für viele wünschenswerte Dinge. Wer sich schützend vor sie stellt, bringt dafür meist hehre Gründe vor: Geschichten über Privatsphäre als Bündnispartner von Menschenwürde, Demokratie, Bürgerrechten, Freiheit, Selbstbestimmung des Einzelnen – und so weiter.

Wenn wir im Namen dieser Bündnis-Geschichten kämpfen sollen, sollten wir sie aber vorher kritisch prüfen. Im Wandel der Zeiten müssen auch die großen politischen Erzählungen immer wieder neu hinterfragt werden. Denn sie haben kein Abonnement auf immerwährende Wahrheit. Worin besteht heute, gerade auch unter sich stark verändernden Umständen, das konkrete Verdienst von Privatsphäre? Ist sie wirklich unser großer Verbündeter im Kampf für unsere Freiheit?

Das ist eine der Fragen, der dieses Buch nachgehen möchte. Eine andere lautet: Wie können – vielleicht sogar: sollen – wir uns in der Zeit des Wandels verhalten, der in diesem Kapitel skizziert wurde? Sollen wir ihn mit offenen Armen empfangen oder uns so lange wie möglich gegen ihn stemmen? Was sind wir bereit, uns die Verteidigung der Privatsphäre kosten zu lassen, vielleicht sogar für sie zu opfern? Oder sollten wir besser gleich aufgeben, nur weil der Kampf aussichtslos erscheint?

Wenn die Privatsphäre langfristig ohnehin verloren ist, zieht das eine dritte Frage nach sich: Wie könnte eine Welt ohne Privatsphäre aussehen? Aus großen liberalen Erzählungen kennen wir eine mögliche Antwort: Eine solche Welt wäre grauvoll und nicht lebenswert. Aber ist das so sicher? Könnte an der Post-Privacy nicht auch manches gewinnbringend sein? Ohne Zweifel schafft der Niedergang der Privatsphäre viele neue Probleme und Gefahren. Vielleicht bringt er aber auch ganz neuartige Lösungen und Chancen mit sich – nach denen soll in diesem Buch Ausschau gehalten werden.

DANK

Dieses Buch entstand unter Hilfe und Input durch viele. Ich kann hier nur wenige nennen. Ich danke meinen Eltern für größte praktische und moralische Unterstützung; und dafür, wie sie den wendenden Text mit ihren eigenen Erfahrungshintergründen begleiteten. Für Ermutigung, überhaupt anzufangen, danke ich Anja Krieger, Moritz Metz und vor allem Kathrin Passig, die mir bei meinen ersten Schritten Richtung Buchmarkt half und das Werden des Textes mit viel Probelesen und einflussreichen Hinweisen begleitete. Für umfangreiches Probelesen, Kommentieren und Kritisieren danke ich auch Nils Dagsson Moskopp, Geraldine Arndt und Jens Ohlig. Hilfreiche Blicke auf entstehende Teile des Textes warfen zudem Julia Seeliger, Änne Nehls, Fiona Krakenbürger, Katrin Wagner und Matthias Rampke, der mir mit strenger Kritik half, eine besonders kritische Stelle halbwegs tauglich zu klopfen. Ich danke meinem Agenten Uwe Heldt, der mich von meiner ersten Konzeptskizze über eine Rohfassung des ersten Kapitels bis zum Kontakt mit dem Verlag C. H. Beck begleitete; dort danke ich vor allem Raimund Bezold und Andreas Wirthensohn fürs Lektorat. Kathrin Ganz und Kai Denker gaben mir wichtige Literaturhinweise. Carmen von der Uni Bielefeld ermahnte mich, hoffentlich rechtzeitig, bei aller Mühe um Vernünftigkeit das Utopisieren nicht zu vergessen. Wichtige Denkprozesse steuerte der Austausch mit der «Post-Privacy-Späckeria» bei, sowie mit Michael Seemann, der hoffentlich bald sein eigenes Buch schreibt. Mirjam Schaub's Seminar «Intimität und der Wert des Privaten» im Wintersemester 2005/06 an der FU Berlin legte Grundsteine, von denen aus das Thema in mir reifte. Außerdem danke ich Gesprächspartnern aus dem Datenschutzumfeld, vor allem Ralf Bendorath und Christian Pfeiffer; ich hoffe, bei aller Verschiedenheit der Sichtweisen findet sich auch für sie Interessantes im Text.

ANMERKUNGEN

1. Das Ende der Privatsphäre

- 1 Peter Schaar, *Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft*, München 2009.
- 2 Pär Ström, *Die Überwachungsmafia. Das gute Geschäft mit unseren Daten*, München 2005.
- 3 Sandro Gaycken, Constanze Kurz (Hrsg.), *1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien*, Bielefeld 2008.
- 4 Ilija Trojanow, Juli Zeh, *Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte*, München 2009.
- 5 Anne-Catherine Simon, Thomas Simon, *Ausgespäht und abgespeichert. Warum uns die totale Kontrolle droht und was wir dagegen tun können*, München 2008.
- 6 Franz Kotteder, *Die wissen alles über sie. Wie Staat und Wirtschaft ihre Daten ausspionieren – und wie Sie sich davor schützen*, München 2011.
- 7 Constanze Kurz, Frank Rieger, *Die Datenfresser. Wie Internetfirmen und Staat sich unsere Daten einverleiben und wir die Kontrolle darüber zurückverlangen*, Frankfurt/M. 2011.
- 8 Google bietet diese Dienstleistung unter dem Namen «Google Latitude» an: <http://latitude.google.com>
- 9 Siehe «Blippy»: <http://blippy.com>
- 10 Selbstdarstellung von wer-kennt-wen, Stand Juni 2011: <http://www.wer-kennt-wen.de/static/presse/>
- 11 «Facebook: Die Welt im Überblick (April 2011)», *SocialMediaSchweiz*: http://www.socialmediaschweiz.ch/Facebook_-_Die_Welt__Update_April_2011_.pdf
- 12 Selbstdarstellung von Twitter, Stand Juni 2011: <http://business.twitter.com/basics/what-is-twitter>
- 13 Carolyn Y. Johnson, «Project ‘Gaydar’», *The Boston Globe*, 20. 9. 2009: http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/
- 14 Selbstdarstellung von OkCupid, Stand Juni 2011: <http://blog.okcupid.com/>
- 15 Christian Rudder, «The Democrats Are Doomed, or How A ‘Big Tent’ Can Be Too Big», *oktrends*, 30. 3. 2010: <http://blog.okcupid.com/index.php/the-democrats-are-doomed-or-how-a-big-tent-can-be-too-big/>
- 16 Chris Coyne, «Rape Fantasies and Hygiene By State», *oktrends*, 25. 6. 2010: <http://blog.okcupid.com/index.php/rape-fantasies-and-hygiene-by-state/>

- 17 Christian Rudder, «Gay Sex vs. Straight Sex», *oktrends*, 12. 10. 2010: <http://blog.okcupid.com/index.php/gay-sex-vs-straight-sex/>
- 18 Siehe die jeweiligen Datenschutzerklärungen.
Google: <http://www.google.de/intl/de/privacy/privacy-policy.html>
Amazon: http://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=3312401
Facebook: <http://www.facebook.com/policy.php>
- 19 Susan Su, «Facebook Now Reaches 687 Million Users – Traffic Trends, and Data at Inside Facebook, June 2011 Edition», 10. 6. 2011: <http://www.insidefacebook.com/2011/06/10/facebook-now-reaches-687-million-users-traffic-trends-and-data-at-inside-facebook-gold-june-2011-edition/>
- 20 Nick Burcher, «Facebook usage statistics 1st April 2011 vs April 2010 vs April 2009», *NickBurcher.com*, 5. 4. 2011: <http://www.nickburcher.com/2011/04/facebook-usage-statistics-1st-april.html>
- 21 James Grimmemann, «Facebook and the Social Dynamics of Privacy», 2008: <http://www.scribd.com/doc/9377908/Facebook-and-the-Social-Dynamics-of-Privacy>
- 22 «We're quitting Facebook»: <http://www.quitfacebookday.com/>
- 23 «FAQ about Gmail, Security & Privacy»: <http://mail.google.com/support/bin/answer.py?hl=en&answer=1304609>
- 24 Kai Biermann, «Wir müssen den öffentlichen Raum im Netz verteidigen», *ZEIT ONLINE*, 10. 8. 2010: <http://www.zeit.de/digital/datenschutz/2010-08/streetview-jens-best>
- 25 Christian Moravcik, «Twittern im Augsburger Stadtrat verboten», *Politisches aus dem Augsburger Stadtrat*, 18. 12. 2009: <http://moravcik.wordpress.com/2009/12/18/twittern-im-augsburger-stadtrat-verboten/>
- 26 Florian Kalenda, «SPD erteilt Abgeordneten Twitter-Verbot», *ZDNet.de*, 28. 5. 2009: http://www.zdnet.de/news/digitale_wirtschaft_internet_ebusiness_spd_erteilt_abgeordneten_twitter_verbot_story-39002364-41004664-1.htm
- 27 Marcel Berndt, «Twittern im Gerichtssaal ist juristische Grauzone», *Wirtschaftswoche*, 15. 9. 2010: <http://www.wiwo.de/politik-weltwirtschaft/twittern-im-gerichtssaal-ist-juristische-grauzone-441472/>
- 28 Jürgen Rüttgers im Jahr 1996, laut: Konrad Lischka, «Phrasen-Kritik: Das Internet ist kein rechtsfreier Raum», *SPIEGEL ONLINE*, 26. 6. 2009: <http://www.spiegel.de/netzwelt/web/0,1518,632277,00.html>
- 29 Diese Dynamik wird in der Netzkultur «Streisand-Effekt» genannt. Für eine Erläuterung, siehe Wikipedia: <http://de.wikipedia.org/wiki/Streisand-Effekt>
- 30 Riva Richmond, «Stolen Facebook Accounts for Sale», *The New York Times*, 2. 5. 2010: <http://www.nytimes.com/2010/05/03/technology/internet/03facebook.html>
- 31 David Harrison, «Government's record year of data loss», *Telegraph.co.uk*, 6. 1. 2008: <http://www.telegraph.co.uk/news/newstopics/politics/1574687/Governments-record-year-of-data-loss.html>

- 32 Kevin Poulsen, «Chat Log: What It Looks Like When Hackers Sell Your Credit Card Online», *Wired*, 4. 5. 2011: <http://www.wired.com/threatlevel/2011/05/carders/>
- 33 Kevin Poulsen, Kim Zetter, «U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe», *Wired*, 6. 6. 2010: <http://www.wired.com/threatlevel/2010/06/leak/>
- 34 Matthias Gebauer, John Goetz, Hans Hoyng, Susanne Koelbl, Marcel Rosenbach, Gregor Peter Schmitz, «Enthüllungbrisanter Kriegsdokumente: Die Afghanistan-Protokolle», *SPIEGEL ONLINE*, 25. 7. 2010: <http://www.spiegel.de/politik/ausland/0,1518,708311,00.html>
- 35 Scott Shane, Andrew W. Lehren, «Leaked Cables Offer Raw Look at U.S. Diplomacy», *The New York Times*, 28. 11. 2010: <http://www.nytimes.com/2010/11/29/world/29cables.html>
- 36 Diesen Trend bezeichnet man als das «Mooresche Gesetz». Für eine Erläuterung, siehe Wikipedia: http://de.wikipedia.org/wiki/Mooresches_Gesetz
- ## 2. Eine kleine Geschichte des Privaten
- 1 Zu Bedeutung und Verhältnis beider Begriffe siehe «Res Publica» in: Raymond Geuss, *Public Goods, Private Goods*, Princeton 2001. Sowie: Georges Duby, «Private Macht, öffentliche Macht», vor allem S. 19–20, in: Georges Duby (Hrsg.), *Geschichte des privaten Lebens*, Bd. 2: *Vom Feudalzeitalter zur Renaissance*, Frankfurt/M. 1990.
- 2 Paul Veyne, «Das Private im Öffentlichen» in: Paul Veyne (Hrsg.), *Geschichte des privaten Lebens*, Bd. 1: *Vom Römischen Imperium zum Byzantinischen Reich*, Frankfurt/M. 1989.
- 3 Paul Veyne, «Arbeit- und Muße» in: Veyne.
- 4 Zur Beschreibung der römischen Familie und ihres Haushalts, siehe Paul Veyne, «Von der Wiege bis zur Bahre», «Ehe», «Hausgemeinschaft und Freigelassene» in: Veyne.
- 5 Zur öffentlichen Funktion des «privaten» Lebens in Rom, siehe Paul Veyne, «Zensur und Utopie» in: Veyne.
- 6 Zur Vermischung von Öffentlichem und Privatem in Haushalt und Architektur römischer Familienhäuser, siehe Yvon Thebert, «Privates Leben und Hausarchitektur in Nordafrika» in: Veyne.
- 7 Paul Veyne, «Vergnügen und Exzess» in: Veyne.
- 8 Yvon Thebert, «Öffentliche und private Räume» in: Veyne.
- 9 Veyne, S. 81.
- 10 Peter Brown, «Die vornehmen Wenigen» in: Veyne.
- 11 Zum Unterschied zwischen dem lateinischen Begriff des Privaten und der daneben aufkommenden christlichen Innerlichkeit, siehe «The Spiritual and the Private» in: Geuss.
- 12 Peter Brown, «Person und Gruppe in Judentum und Frühchristentum», «Das Wagnis der Wüste» in: Veyne.