C.H.BECK
www.chbeck.de

Unverkäufliche Leseprobe

Christian Heller
Post-Privacy
Prima leben ohne Privatsphäre

174 Seiten, Paperback
ISBN: 978-3-406-62223-6

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 zurückerlangen.*[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 taktischen 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 Lesefaule 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 begehrt.

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 Verbindungslinien 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.

Ein Verteidiger der Privatsphäre könnte angesichts dessen einwenden: «So sind halt Exhibitionisten, sie müssen ihr Leben zwanghaft aller Welt aufdrängen. Normale Menschen aber haben Besseres 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-wen[10] 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 Besseres 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 Schlafrhythmus. 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 grübelt: «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 Dienste[18] 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 angeschaut und bestellt haben, erahnt es unsere literarischen Vorlieben. Googles Suchergebnisanzeige orientiert sich nicht nur an dem Text, den wir ins Suchfeld eingeben, 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 ausgefuchstes «Datamining», also ein möglichst schlaues 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 offenherzig 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]

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 Eifrige[24] 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 weiterverteilt, 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 Augsburg[25] 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?

[…]