Die Digitalisierung pocht an das Tor unserer innersten Welt

Autor(en): **Lobsiger, Adrian**

Objekttyp: **Article**

Zeitschrift: **Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur**

Band (Jahr): **97 (2017)**

Heft 1050

PDF erstellt am: **16.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-736591

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

9 Die Digitalisierung pocht an das Tor unserer innersten Welt

Die Verteidigung der Gedankenfreiheit ist nicht nur ein Fall für den Eidgenössischen Datenschützer. Gefordert sind auch die Wirtschaft, die Behörden und jeder einzelne.

von Adrian Lobsiger

Sie machen uns und unser Leben bequemer, fast niemand möchte sie mehr missen: die Rede ist von Sensoren, die im öffentlichen und privaten Raum Bewegungen, Gesichter und Stimmen erfassen, sei dies über Smartphones, Gesundheitsarmbänder oder die Bordelektronik von Autos. Unsere neuen digitalen Assistenten ermöglichen eine Vielzahl von nützlichen Diensten wie die Spracherkennung, den standortbezogenen Fahrplan oder die Navigation in Städten und entlegenen Gebieten. Trotzdem ist der Gedanke an das Bewegungsbild des Smartphones ein unangenehmer. Denn es enthüllt, an welchen Orten wir arbeiten, konsumieren oder speisen und an welchen Adressen wir die Nacht verbringen. Und noch während wir uns fragen, wie wir mit all den Sensoren und Cloud-Diensten klarkommen sollen und wie viel Platz eigentlich noch bleibt für ein privates und selbstbestimmtes Leben, pocht die Digitalisierung bereits an das Tor unserer innersten Welt der Gedanken und Phantasien.

Die Welt des Intimen wird in liberalen Gesellschaften einer von der Verfassung garantierten individuellen Freiheits- und Privatsphäre der Gedanken- und Gewissensfreiheit zugewiesen. Der Rechtsstaat garantiert, dass niemand seine Intimitäten mit Dritten teilen muss. Informationen, die der Psyche durch Spitzel, Lügendetektoren oder Medikamente abgerungen werden, sprechen Verfahrensordnungen jeden Beweiswert ab. Nebst den Gedanken umfasst die Schutzsphäre des Privaten alles, was in den eigenen vier Wänden gesprochen oder geschrieben wird, sowie die dort verfügbaren Erkenntnisquellen wie Bücher oder Bilder. Sind Intimitäten einmal in die mit anderen geteilte Aussenwelt gelangt, muss damit gerechnet werden, dass sie dort gehört, gelesen oder gesehen werden und sodann nicht mehr rückgängig zu machende Wirkungen entfalten. Damit das Intime nicht unkontrolliert, sondern im Sinne einer willentlichen Übertragung nach aussen dringt, schützt das Strafrecht die Privatsphäre vor heimlichen Ausforschungen und Zugriffen Dritter. Und das Personen- und Datenschutzrecht statuieren die fundamentale Regel, dass niemand intime Daten bearbeiten darf, ohne vorgängig eine Einwilligung der Betroffenen eingeholt zu haben – es sei denn, er könne sich auf eine besondere Rechtfertigung wie zum Beispiel eine gesetzliche Pflicht berufen.

Adrian Lobsiger
wurde 2016 von der Vereinigten Bundesversammlung für eine Amtsdauer von vier Jahren zum Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gewählt. Der EDÖB übt seine Funktion unabhängig und ohne Weisung einer Behörde aus.

Wie aber steht es mit den Erkenntnisquellen, die wir gelenkt von unseren inneren Impulsen im Internet ansteuern? Ist deren individuelle Anwahl Privatsache, so wie die Pflege der privaten Bücher- oder Fotosammlung? Dies ist zu bejahen, weil angesurfte Seiten schon nach kurzen Erfassungszeiträumen Persönlichkeitsprofile erzeugen, die über Interessen, Vorlieben oder Kontakte und damit indirekt Gedanken- und Gesinnungsmuster bis hin zu sexuellen Orientierungen und intimen Phantasien mutmassen lassen. Folglich ist die Drittnutzung von individuellen Surfprofilen von einer ausdrücklichen Einwilligung der Betroffenen abhängig zu machen. Ein Erfordernis, das den Betreibern digitaler Geschäftsmodelle, die auf der Bearbeitung grosser Datenmengen beruhen, nicht besonders gelegen kommt. Sie sehen im Surfverhalten der Massenkundschaft ein kommerzielles Gut, das es durch algorithmische Analysen und Personalisierung von Angeboten mit einem Maximum an digitaler Effizienz zu nutzen gilt. So suchen die meisten Big-Data-Modelle denn auch den Aufwand für das Einholen von Zustimmungen ihrer Kunden möglichst tief zu halten, indem sie von deren Identifikation absehen und das zum Zwecke der Personalisierung ihrer Leistungen analysierte Surfverhalten stattdessen aggregierten Konsumgruppen zuordnen. Aus Sicht des Datenschutzes ist der Wegfall der Identifikation als Bearbeitungszweck zu begrüssen. Dennoch bleibt auch eine nicht auf die Identifikation von Einzelpersonen abzielende Personalisierung von Onlineangeboten mit erheblichen Risiken für die Privatsphäre verbunden. Werden Inhalte von Abfrageprotokollen durch Zugriffsbefugte oder -unbefugte zweckwidrig ausgesondert, können aus den ersichtlich werdenden Persönlichkeitsprofilen leicht Identitäten von einzelnen Benutzern herausgelesen werden, womit deutlich wird, dass die oft vorschnell als blosse «Sachdaten» verkannten Abfrageinhalte potenziell besonders

schützenswerte Personendaten darstellen. Die Bearbeitung von Surfprofilen darf demzufolge nie zu einer Aussonderung eines Verhaltens bestimmbarer Personen führen, ohne dass dafür deren ausdrückliche Einwilligung vorliegt.

Selbstverantwortlich einwilligen können Kunden indessen nur, soweit die Unternehmen fair[1] und umfassend[2] darüber informieren, wie und wofür sie Surfprotokolle bearbeiten. Je rascher der Anteil an fairen und umfassenden Informationsangeboten wächst, desto besser stehen die Chancen, dass sich eine digitale Kultur der Transparenz und Selbstverantwortung[3] etablieren kann, von der die Wirtschaft und ihre Kunden gleichermassen profitieren.

Nebst der erwähnten Pflicht zur Transparenz haben die Bearbeitungsverantwortlichen eine Reihe präventiver Massnahmen zu ergreifen, um Informationen zum Surfverhalten vor Missbräuchen durch Dritte zu schützen. Allein das Wissen um die blosse Existenz umfangreicher Surfprotokolle lässt Hacker nach Mitteln und Wegen suchen, um sich Zugang zu diesen Informationen zu verschaffen. Sei es, um die Daten zu verkaufen, sei es, um Firmen oder Einzelpersonen zu erpressen, oder sei es, um letztere und ihre Angehörigen, wie im Fall des Kontaktportals Ashley Madison, öffentlich blosszustellen. Solche Lecks machen denn auch die Bedeutung einer angemessenen Datensicherheit offensichtlich, die nach neuem Datenschutzrecht im Rahmen sogenannter Datenschutz-Folgeabschätzungen nachgewiesen werden muss. Meine Behörde wird das Datenschutzrecht denn auch dahingehend zu interpretieren wissen, dass die Bearbeitung des Nutzungsverhaltens zu unterlassen ist, solange der Verantwortliche nicht hinreichende Massnahmen ergriffen hat, um die Betroffenen vor einer Identifizierung und Offenlegung ihres Surfverhaltens zu schützen.

Grenzen auch für Sicherheitsbehörden

Weiter muss klar sein, dass hinsichtlich des Zugriffs auf Abfrageprotokolle und deren Auswertung auch der Polizei und den Staatsanwaltschaften Grenzen gesetzt sind. Zum einen, weil das schweizerische Polizeirecht kein polizeiliches Einschreiten gegen abstrakte und hypothetische Gefahren zulässt. Zum andern, weil das Strafrecht keine Gesinnungsstrafen kennt und deshalb ausschliesst, dass die Kriminalpolizei zwecks Gewinnung von Verdachtslagen Informationen über die mutmassliche Gedankenwelt der Bevölkerung beschafft.

Klar ist aber auch: der hier unterstrichene Schutz der Freiheitssphäre darf nicht dazu führen, dass wir zu einem sicheren Hafen für Kriminelle werden. Es gibt denn auch keine Informationen, die der schweizerische Rechtsstaat der Strafverfolgung grundsätzlich entziehen würde. Die Erhebung und Verwertung von strafverfolgungsrelevanten Informationen, welche die Privat- und Intimsphäre betreffen, wird aber vom Entscheid eines Richters abhängig gemacht, der die Grundrechte der Betroffenen gegen die Interessen der Öffentlichkeit abwägt. So zum Beispiel, indem er in Würdigung der konkreten Umstände des Einzelfalles sowie nach Massgabe der gesetzlichen Verfahrensordnungen und Rechtsprechung über die Anordnung der technischen Direktüberwachung eines Surf- oder anderen Kommunikationsverhaltens und dessen spätere Verwertung als Beweis entscheidet.

Eben diesen Richtervorbehalt hat der Gesetzgeber auch im neuen Nachrichtendienstgesetz eingebaut, das Überwachungen von Individualkommunikation stets von einer verwaltungsrichterlichen Genehmigung abhängig macht. Da die Staatsschutztätigkeit des Nachrichtendienstes indessen auf die Früherkennung und vorbeugende Abwehr ideologisch-politisch motivierter Bedrohungen wie des gewalttätigen Extremismus und Terrorismus abzielt, setzen die Massnahmen des Staatsschutzes im Gegensatz zu jenen der ordentlichen Polizeitätigkeit und Strafverfolgung ein, bevor sich eine konkrete Störung der öffentlichen Sicherheit oder eine Straftat ereignet haben. Anders als Polizei und Staatsanwaltschaften orientiert sich die nachrichtendienstliche Datenbeschaffung und -analyse aufgrund der ideologisch-politischen Natur der abzuwehrenden Gefahren nicht vorab an äusserlich manifestierten Handlungen, sondern an inneren Haltungen und Gesinnungsmustern, womit sie der rechtsstaatlichen Tabuzone der Gedanken- und Gewissensfreiheit in bedrohlichere Nähe rückt als die Strafverfolgung. Aus diesem Grund hat der Gesetzgeber die unter Richtervorbehalt stehende Überwachung von Individualkommunikation durch den Nachrichtendienst denn auch durch das zusätzliche Erfordernis einer Genehmigung durch den oder die Chefin des zuständigen Departements erschwert, welcher eine Konsultation des Sicherheitsausschusses des Bundesrats vorangegangen sein muss. Hinzu kommt ein besonderes Aufsichtsregime durch ein unabhängiges Fachaufsichtsorgan, eine Kontrollinstanz über die Funk- und Kabelaufklärung sowie die parlamentarische Oberaufsicht.

Damit es nicht zu einer Umgehung all dieser besonderen Genehmigungs- und Kontrollmechanismen kommen kann, ist es von höchster rechtsstaatlicher Bedeutung, dass die Polizei die Frühaufklärung von ideologisch-politisch radikalisierten Milieus dem Nachrichtendienst überlässt. Die Datenbeschaffung von Polizei und Staatsanwaltschaften soll diesbezüglich erst einsetzen, nachdem sie der Nachrichtendienst über hinreichend konkrete Gefährdungen der inneren Sicherheit oder Handlungen informiert hat, welche die Schwelle zum strafrechtlich relevanten Tatverdacht überschritten haben. Umgekehrt soll die nachrichtendienstliche Frühaufklärung einen Bogen machen um die Netzwerke der pekuniär motivierten Kriminellen, die sich mit Korruption, Drogen- und Wirtschaftskriminalität sowie Geldwäscherei oder Menschenhandel bereichern. Dass der Nachrichtendienst und die Polizeiorgane des Bundes gegenseitig die Disziplin aufbringen, sich bei der Beschaffung und Analyse ihrer Früherkennungsdaten auf jene Bedrohungsfelder zu konzentrieren, die ihnen vom Gesetzgeber zugewiesen worden sind, ist denn auch eines der zentralen Aufsichtsziele der Datenschutzbehörde des Bundes im Bereich der inneren Sicherheit.

«Je weniger die Menschen an die Meinungs- und Kommunikationsfreiheit im Internet glauben, desto zahlreicher werden sie auf Alternativen setzen.»

Adrian Lobsiger

«Rechtsstaatlichen Speck» loswerden?

Die rechtsstaatlichen Vorgaben der Personendatenbearbeitung und die für Eingriffe in die Privatsphäre durch Sicherheitsbehörden vorbehaltenen Justiz-, Kontroll- und Aufsichtsverfahren sind fraglos zeitaufwendig und teuer. Kritiker des Datenschutzes lassen denn auch nicht selten anklingen, dass aufstrebende Nationen, gerade auch dank umfassender Vorratsdatenspeicherung und automatisierter Daueranalysen aller kollektiv nutzbaren Daten, zu einem beneidenswerten Wirtschaftswachstum gefunden hätten. Ist die Schweiz also schwerfällig geworden, und sollte sie «rechtsstaatlichen Speck» loswerden?

Die Globalisierung der Wirtschaft bringt es mit sich, dass schweizerische Unternehmen auch mit Weltregionen in Konkurrenz stehen, in denen kein vergleichbarer Schutz der Privatheit und Selbstbestimmung existiert. Gerade der Umstand, dass manche der sogenannten Internetgiganten aus dem Silicon Valley ihre Marktanteile in autoritär-staatlich gelenkten Volkswirtschaften – wohl auch aus Sorge um ihre Reputation – zurückbinden liessen, sollte alle Unternehmen generell zur Vorsicht mahnen, bei der Bearbeitung von Kundendaten vorschnell rechtsstaatliche Prinzipien über Bord zu werfen. Mit Blick auf die datenschutzrechtliche Verantwortung der öffentlichen Hand sollte bedacht werden, dass jeder Staat, der sich Zugang zum Surfverhalten seiner Bevölkerung verschafft, statt sie vor solchen Zugriffen zu schützen, Gegenreaktionen zu gewärtigen hat. Trotz des Risikos, als Cyberkriminelle verfolgt zu werden, setzen immer mehr anständige Menschen allein der Freiheit ihrer Gedanken, Ideen und Phantasien wegen Instantmessenger, Anonymisierungsdienste oder Geräteverschlüsselungen ein, die es ihnen erlauben, Dritten den Zugriff auf ihre Kommunikationsdaten zu erschweren oder beim Surfen Spuren zu verwischen. Es darf nicht übersehen werden, welcher Schaden entsteht, wenn die Allgemeinheit nicht mehr darauf vertraut, dass Gedanken und Phantasien unantastbar bleiben. Je weniger die Menschen an die Meinungs- und Kommunikationsfreiheit im Internet glauben, desto zahlreicher werden sie auf Alternativen setzen. Je penetranter der sanfte Druck auf mündige Menschen gegen den Einsatz verschlüsselter Kommunikation oder analoger Instrumente wie Bargeld, desto unaufhaltsamer der Vormarsch von Verschlüsselungssoftware oder von Kryptowährungen.

Die alternativen Instrumente von heute prägen die Digitalisierung von morgen, und der Motor dieser eigenwilligen Innovation sitzt nicht (nur) im Silicon Valley. Er sitzt überall auf der Welt, wo es Menschen gibt, die sich ein privates und deshalb selbstbestimmtes Leben wünschen. ‹

[1] Fair ist eine aufgeschaltete Information, wenn sie erstens sprachlich leicht verständlich ist und die Kunden zweitens durch eine bedienungsfreundliche Programmierung direkt auf jene Passagen der Nutzungs- und Geschäftsbedingungen lenkt, die für die informierte Ausübung konkreter Wahl- und Zustimmungsrechte relevant sind. So zum Beispiel, indem die einschlägigen Passagen zur Funktionalität «Kamera» angesteuert werden können, bevor der Kunde entscheidet, ob er diese aktivieren will.

[2] Umfassend zu informieren bedeutet, mehrere Erklärungstiefen anzubieten, welche die unterschiedlich weit gehenden Bedürfnisse von der Online-Laufkundschaft bis hin zu spezialisierten Kreisen wie Investigationsjournalisten oder Datenschutzbehörden abdecken.

[3] Selbstverantwortlich surfen setzt voraus, dass wir uns auch Gedanken über die hinterlassenen Spuren machen. Wer auf sozialen Netzwerken ein Konto mit dem eigenen Namen, einer Mailadresse und Fotos unterhält und eingeloggt surft, versetzt den Anbieter technisch in die Lage, das Surfverhalten im Internet mit seiner Person zu verknüpfen. Weniger Spuren erzeugen diejenigen Nutzer, die sich regelmässig aus ihrem Social-Media-Konto ausloggen. Wer Wert auf die Vertraulichkeit des Surfverhaltens setzt, wird zudem bei der Auswahl von sogenannten Browser-Add-ons darauf achten, dass diese nicht den Verlauf der Seitenbesuche auslesen oder mitschneiden – und schon gar nicht an Dritte weitergeben. Weiter kann das Risiko einer missbräuchlichen Verknüpfung dieser Daten durch regelmässiges Löschen von Cookies und den Verzicht auf das Anlegen eines Surfverlaufs gemindert, wenn auch nicht vollständig gebannt werden.