JA, ICH HAB WAS ZU VERBERGEN!

AStA-Reader zum Datenschutz

asta.ms

Inhalt

Vorwort

„Aber ich hab doch nichts zu verbergen…“

Datenschutz ist ein Thema, das vielen wichtig erscheint, aber häufig auch zu komplex und weit weg vom persönlichen Alltag. Einerseits finden wir gruselig, was seit Edward Snowden über die Überwachungspraktiken der Geheimdienste bekannt geworden ist. Andererseits kann, was wir tun, auch gar nicht so interessant sein, dass es sich wirklich lohnen würde, uns zu überwachen. Also kleben wir einen Zettel über die Laptop-Kamera, wenn wir diese nicht gerade zum Skypen benutzen, und verdrängen das mulmige Gefühl.

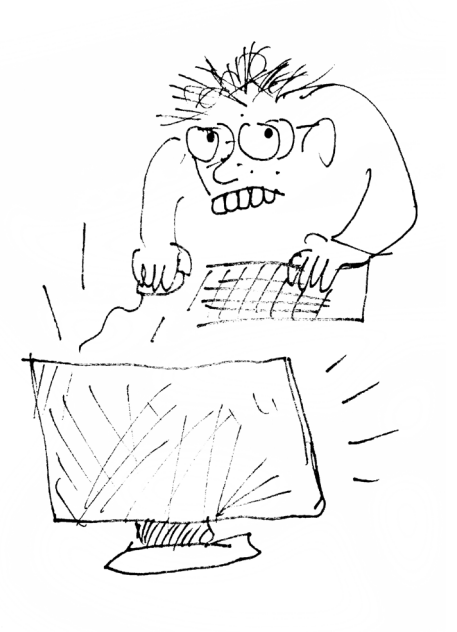
Oft fällt dann auch der Satz „ich habe doch nichts zu verbergen“, der so einfach und schlüssig klingt, dass er unwidersprochen bleibt. Aber stimmt das? Haben wir wirklich nichts zu verbergen? Oder andersherum, gibt es nichts, was wir gerne geheim halten würden? Streng genommen gibt es da schon einiges. Die Geheimzahl für das Bankkonto, kleine Sünden im Alltag, aber vielleicht auch die persönliche Krankengeschichte oder Einzelheiten der sexuellen Orientierung.

Wir verdrängen allzu leicht, dass dieses Wissen auch gegen uns ausgenutzt werden kann, weil wir in einem weitgehend toleranten Umfeld aufgewachsen sind und leben. Aber das heißt nicht, dass niemand Macht über uns ausüben kann. Was wäre, wenn das Prüfungsamt wüsste, dass ich nicht krank die Klausur verpasst habe, sondern weil ich verkatert war? Was sagt mein*e Arbeitgeber*in zu meiner chronischen Erkrankung, die zwar schon länger nicht mehr aufgetreten ist, aber jeden Tag wieder kommen könnte? Würde meine Bank mir weiterhin ein kostenloses Konto zur Verfügung stellen, wenn sie bereits wüsste, dass ich höchstwahrscheinlich in der Zukunft kein*e solvente*r Kund*in sein werde? Wie erreiche ich meine Freund*innen, wenn Facebook mich nicht mehr als Nutzer*in akzeptieren würde?

Häufig denken wir nur an die Staatsmacht, wenn wir sagen, wir hätten doch durch mehr Überwachung nichts zu befürchten. Dabei vergessen wir schnell, dass auch im Kleinen unser Alltag überall von asymmetrischen Machtverhältnissen geprägt ist - und Informationen helfen nun mal der stärkeren Seite.

Im Folgenden wollen wir zunächst noch einmal als Grundlage die historische Entwicklung des Datenschutzes darstellen und feststellen, welche Auswirkungen Überwachung auf die freiheitliche Gesellschaft haben kann. Daran anschließend erörtern wir anhand einiger Beispiele, weshalb man sich schützen sollte und wie dies funktioniert, ohne gleich zum „Computer-Nerd“ zu werden.

Wir wünschen viel Spaß beim Lesen und Ausprobieren!



I.

Warum Datenschutz

1.

Historie des Datenschutzes

„Datenschutz“ ist ein breit gefasster Begriff. Er kann das Sammeln von Daten ebenso betreffen wie deren Verarbeitung, ein positiv gefasstes Recht auf informationelle Selbstbestimmung, und letztlich kann man auch den generellen Schutz der Privatsphäre unter diesen Begriff fassen. Als solcher blickt der Datenschutz auf eine lange Geschichte zurück. So wurde das Beichtgeheimnis, die Verschwiegenheitspflicht des*der Geistlichen bei der Beichte, bereits 1215 formuliert und in Kirchenrecht überführt und entbindet Geistliche bis heute von der Anzeigepflicht selbst für Kapitalverbrechen. Auch andere Berufsgruppen bildeten mit der Zeit Verschwiegenheitspflichten aus.

Mit der Verfassung der Weimarer Republik wurde das Postgeheimnis 1919 erstmals in Deutschland zum Grundrecht erklärt – jedoch, wie das häufig bei Datenschutzrechten der Fall ist, ein Grundrecht mit Einschränkungen: So übten die alliierten Siegermächte des Ersten Weltkriegs abhängig vom Gebiet teils bis 1924 Postüberwachung aus. Mit der kurzen Phase der Freiheit war es am 28. Februar 1933 vorbei, als die NSDAP mit der „Verordnung des Reichspräsidenten zum Schutz von Volk und Staat“ das Postgeheimnis – samt weiterer Grundrechte - restlos aushebelte. Es kehrte mit dem Kriegsende nicht zurück, denn noch gründlicher als nach dem Ersten Weltkrieg wurde das Postwesen 1945 der alliierten Kontrolle unterworfen. Nachdem das Postgeheimnis 1949 im Grundgesetz Artikel 10 verankert wurde, wurde die Kontrolle 1951 aufgehoben.

Einen großen Schritt zurück machte die Bundesrepublik in Sachen Postgeheimnis ausgerechnet 1968, als der Bundestag angesichts des „Deutschen Herbstes“ Notstandsgesetze verabschiedete, inklusive des „Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses“, kurz auch Artikel-10-Gesetz genannt. Das Gesetz erlaubt dem Verfassungsschutz, dem Militärischen Abschirmdienst (MAD) sowie dem Bundesnachrichtendienst (BND), unter bestimmten Umständen Postverkehr und Telekommunikation zu überwachen, wenn Anhaltspunkte zu be-

stimmten Katalogstrafen vorliegen: Hochverrat, Volksverhetzung, aber auch Einschleusen von Ausländer*innen. Bemerkenswert am Artikel-10-Gesetz ist, dass den Betroffenen nicht einmal der Rechtsweg offensteht – eine beispiellose Einschränkung von Artikel 19 Absatz 4 GG, nach dem gegen Rechtsverletzungen grundsätzlich der Rechtsweg offensteht. 2008 hat das Bundesverwaltungsgericht auch flächendeckende Überwachung von Kommunikationsverbindungen anhand des Artikel-10-Gesetzes für zulässig erklärt. Zugleich erlaubt das Gesetz dem BND ausdrücklich, gewonnene Daten an ausländische Geheimdienste weiterzuleiten. Das Vorgehen von BND und Co ist damit kein eindeutiger Rechtsbruch mehr, sondern ausdrücklich im Grundgesetz vorgesehen – was der eigentliche Skandal an der Überwachungsaffäre ist. Ebenfalls 1968 schloss die Bundesregierung mehrere Verwaltungsvereinbarungen mit den Alliierten, die diesen den Zugriff auf die Post der Bundesbürger*innen ermöglichte. Diese Vereinbarungen waren bis 2012 geheim.

Hessen war das erste Bundesland, das sich 1970 ein eigenes Datenschutzgesetz gab. 1977 folgte dann das Bundesdatenschutzgesetz, das Datenverarbeitung ohne gesetzliche Grundlage unter Strafe stellte. Jedoch brauchte es das Bundesverfassungsgericht, um klarzustellen, dass auch gesetzlich angeordnete Datenverarbeitung gegen Grundrechte verstoßen kann: Die im Frühjahr 1983 geplante Volkszählung wurde vom BVerfG gestoppt, da ein massenhaftes Ansammeln von Daten durch den Staat als nicht mit der freiheitlich-demokratischen Grundordnung vereinbar gesehen wurde. „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen“, heißt es treffend in der Begründung. Entsprechend wurde das Bundesdatenschutzgesetz 1990 sowie 2009 umfassend novelliert. Nichtsdestotrotz konzentriert sich das deutsche Datenschutzrecht weiterhin auf staatliche Datenverarbeitung und hält damit nur unzureichend Schritt mit der technischen Entwicklung.

Auch international gab es – zumeist zaghafte – Ansätze. Als einer der ersten ist die 1948 verabschiedete Allgemeine Erklärung der Menschenrechte zu nennen, die dem Individuum ein Schutzrecht vor „willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr“ zugesteht. Aufgrund des Aufkommens von datenverarbeitender Technik beschloss der Europarat 1981 das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“, kurz: die Europäische Datenschutzkonvention. Die 2000 beschlossene Grundrechtecharta der Europäischen Union enthielt ebenfalls einen Schutz für Privatsphäre und Kommunikation. Kein Glanzlicht setzte die EU dagegen mit ihrer Richtlinie 2006/24/EG, die die Mitgliedsstaaten zur Einführung einer Vorratsdatenspeicherung zwingen sollte und 2014 vom Europäischen Gerichtshof für ungültig erklärt wurde.

2.

Jüngste Entwicklungen

In den letzten Jahren wurde durch Enthüllungen immer wieder deutlich, dass die großen Geheimdienste bei ihrer Datensammlung offenbar jedes Maß verloren haben. Gleichzeitig stellten die Untersuchungsausschüsse des Bundestages zum BND (im Zusammenhang mit der NSA-Spionage) sowie zum Verfassungsschutz (im Zusammenhang mit den NSU-Morden) immer wieder massive Schlamperei fest. Die bisher bestehenden Kontrollmechanismen scheinen daher entweder nicht ausreichend zu sein, um einen hohen Grundrechtsschutz zu gewährleisten, oder wurden sogar bewusst umgangen.

Neben den Nachrichtendiensten speichert die Polizei personenbezogene Daten mit teils fragwürdigen Begründungen. Eine zentrale Funktion nimmt für Deutschland dabei das polizeiliche Informationssystem INPOL der Bundes- und Landespolizeien ein. In der INPOL-Datenbank können sog. personengebundene Hinweise ein-

getragen werden. Unter anderem sollen laut Medienberichten in INPOL über 150.000 Deutsche als „Betäubungsmittel-Konsumenten“ festgehalten sein. Auch Kategorien wie „geisteskrank“, „Ansteckungsgefahr“ oder „Straftäter linksmotiviert“ finden sich in der Datenbank. Die Verwendung dieser Kategorien ist umstritten, da um z.B. als Straftäter zu gelten keine Verurteilung vorliegen muss, sondern ein begründeter Verdacht ausreicht. Auch ist fraglich, welchem Zweck eine solche Datenbank dient. Offiziellen Angaben zufolge dienen die Eintragungen der „Eigensicherung“ der Polizeibeamt*innen und stellen keine Grundlage für polizeiliche Maßnahmen dar. In der Praxis lässt sich dies schwer überprüfen. Es liegt aber zumindest der Verdacht nahe, dass die Markierung als „Betäubungsmittel-Konsument*in“ ein Anlass für eine ausführlichere Kontrolle bieten könnte, während die Gefährdung von Polizeibeamt*innen durch Drogenkonsument*innen ein eher geringeres Problem darstellt.

Europaweit wird von allen Polizei-, Grenzschutz-, Zoll-, Visa- und Justizbehörden das sog. Schengener Informationssystem (SIS) genutzt. In SIS werden Personen, Fahrzeuge, Ausweise, Banknoten oder auch Waffen gespeichert, die zur Fahndung ausgeschrieben sind oder vermisst werden. In der neueren Version SIS II sollen auch Lichtbilder, Fingerabdruckdaten und sogar der phonetische Klang eines Namens eingespeichert werden können. Das Ziel der SIS-Datenbank wurde ursprünglich zur Verbrechensbekämpfung eingeführt. Heute behandelt jedoch ein Großteil der Datensätze Personen aus „Drittstaaten“, die ausgewiesen und abgeschoben bzw. an der Wiedereinreise gehindert werden sollen.

Wie Ihr herausfindet, ob Ihr in einer dieser Dateien geführt werden, könnt Ihr im Text zu Auskunftsansprüchen nachlesen.

3.

Warum Datensparsamkeit?

Um zu verstehen, warum man sparsam mit Daten umgehen sollte, muss man zunächst einmal ihren Wert realistisch beurteilen können. Das fällt nicht immer leicht. Deutlich wird dies am Beispiel Face-

book: Stöbert man in seiner „Timeline“, also einem Ausschnitt der Daten, die das Unternehmen über einen gesammelt hat, stößt man auf eine Menge Belanglosigkeiten. Aus der Information, dass man vor Ewigkeiten mal einen bestimmten Ort besucht oder einen peinlichen Kommentar abgegeben hat, lässt sich kein großer Nutzen ziehen. Das könnte zu dem Gedanken verleiten, dass diese Daten auch nichts wert sind.

Leichtfertig lassen wir uns als Facebook-User also auf ein Tauschgeschäft ein: die persönlichen Daten über unsere Kontakte, Aufenthaltsorte und Vorlieben landen bei Facebook. Dafür ermöglicht Facebook es uns dann, unser soziales Umfeld komfortabel zu managen, zum Beispiel mit Party-Einladungen, dem schnellen Kontakt zu Freunden aus dem Ausland oder in einer Uni-Gruppe. Die Daten sind also Währung, mit der wir für Technologie bezahlen, auf die inzwischen keiner mehr verzichten möchte. Wer sich aus den sozialen Netzwerken zurückzieht, wird von Informationen und Kontakten abgeschnitten.

Im Jahr 2014 erzielte Facebook einen Gewinn von 2,94 Milliarden Dollar. Grund dafür ist nicht nur, dass das Unternehmen viele Menschen erreicht. Entscheidend ist, dass durch die riesigen und immer größer werdenden Datenbestände das Verhalten dieser Menschen ganz gezielt analysiert und ausgewertet werden kann, was unter anderem die Zielgenauigkeit von Werbeanzeigen steigertIn den Händen von Facebook sind die Daten, die wir so naiv gegen die kleinen Erleichterungen des Alltags eingetauscht haben, plötzlich eine Menge wert. Auch deswegen verlangen die Internetriesen immer mehr von unseren Daten. Und wir geben sie ihnen gerne: Sogar so etwas Wertvolles wie den eigenen Fingerabdruck lassen wir bei Apple hinterlegen, um im Gegenzug den kleinen Komfort zu haben, das Handydisplay ohne Code entsperren zu können.

Aus unserer Naivität schlagen Facebook & Co. riesige Gewinne. Doch es gibt noch ein größeres Problem, als dass wir uns zum eigenen Nachteil von der Werbeindustrie ausnehmen lassen. Geheimdienste haben ein gewaltiges Interesse an den Datenbeständen. Jedes Wort, das jemals im Facebook-Messenger oder bei Google-Mail eingegeben wurde, ist dort hinterlegt. Geheimnisse und Laster in Ungnade gefal-

lener Menschen lassen sich über Jahre hinweg in die Vergangenheit genauestens nachvollziehen. Gesellschaftliche Gruppen können auf ihre inneren Verbindungen und Schwächen hin untersucht werden. Die Daten werden zur Waffe. Und in der Tat: Seit den Snowden-Veröffentlichungen über das Programm „MUSCULAR“ ist gewiss, dass die NSA Rechenzentren von Google und Yahoo ganz gezielt angezapft hat, um sich Zugang zu deren Datenbeständen zu verschaffen. Nicht jeder Geheimdienst agiert aus einem demokratischen Rechtsstaat heraus und selbst in diesen kommt es vor, dass Geheimdienste außer Kontrolle geraten, wie der Bericht des US-Senats über die CIA-Folter aus dem Jahr 2014 zuletzt wieder gezeigt hat.

Deswegen ist ein Umdenken im Umgang mit unseren Daten erforderlich. Daten, die erst gar nicht anfallen, können auch nicht missbraucht werden. Wenn jeder möglichst wenig Daten und die nur mit gesundem Misstrauen und einer Kosten-Nutzen-Abwägung aus der Hand gibt, dann ist das „Datensparsamkeit“. Sparsam mit Daten geht um, wer nur mit Bargeld bezahlt, keine Bonuskarten hat, sein Smartphone auch mal ausschaltet und sensible Informationen nicht unverschlüsselt durchs Internet schickt. Daten sind etwas wert. Für die Werbeindustrie sind sie das „Öl des 21. Jahrhunderts“ und für die Geheimdienste das Mittel zur Macht. Deswegen sollten wir sie nicht verschenken.

4.

„Es sind doch nur Metadaten!“

Wenn Überwachung kritisiert wird, lautet eine der typischen Antworten von Vertreter*innen der Sicherheitsbehörden, es handle sich lediglich um Metadaten (auch Verkehrs- oder Verbindungsdaten genannt). Für die Inhalte der Gespräche, eMails und Chat-Nachrichten interessiere man sich gar nicht. Ähnlich wird im Zusammenhang mit der Vorratsdatenspeicherung argumentiert. Da lediglich erfasst werde, wer, wann, von wo, mit wem kommuniziert habe, aber keine Speicherung der jeweiligen Inhalte stattfinde, sei die Freiheit der Bürger*innen nicht gefährdet. Erst im konkreten Verdachtsfall werde auf die Daten zugegriffen. Somit handle es sich auch nicht um eine Mas-

senüberwachung – und wer nichts zu verbergen habe, der habe sowieso nichts zu befürchten.

Sind Metadaten wirklich so ungefährlich?

Das Wort Metadaten zeigt, dass es hier um die Meta-Ebene von Daten geht. Metadaten sind also Daten über Daten. Ganz plastisch lässt sich das am Beispiel von Büchern in der ULB erklären. Bei den Metadaten handelt es sich um Informationen über Autor*in, Erscheinungsjahr und Standort des Buches. Noch nicht umfasst sind die eigentlichen Daten selbst – also der Inhalt des Buches. In der Kommunikation werden mit Meta-Daten in der Regel die verwendeten Telefonnummern oder IP-Adressen, der Standort sowie Zeitpunkt und Dauer der Nutzung.

Diese Metadaten sagen jedoch mehr über uns aus, als wir auf den ersten Blick denken. Dies belegt unter anderem die Metaphone-Studie der Stanford University. Dort haben die Probanden freiwillig die Metaphone-App auf ihre Smartphones geladen, die innerhalb eines Zeitraums von drei Monaten alle Metadaten von Anrufen, Chats und auch den Facebook-Profilen der Studienteilnehmer*innen speicherte. Die Kommunikationsinhalte wurden jedoch ausdrücklich nicht mitprotokolliert. Bei 5000 aus dem Gesamtmaterial zufällig ausgewählten Telefonnummern gelang es den Forscher*innen auf Anhieb, die Namen von über 72% der damit verknüpften Teilnehmer*innen herauszubekommen – auch wenn diese nicht selbst an der Studie teilgenommen haben. Dies ist besonders brisant vor dem Hintergrund, dass Geheimdienste, aber auch große Werbefirmen und Telekommunikationsgesellschaften über deutlich weitgehendere Auswertungsmöglichkeiten verfügen als die Wissenschaftler*innen.

Wer hat uns verraten? Metadaten!

Neben der einfachen Identifizierbarkeit aller Kommunikationspartner*innen verraten Metadaten auch viel über unsere Gewohnheiten und konkrete Lebenssituationen. Bei einer Teilnehmerin der Metaphone-Studie wurde beispielsweise gespeichert, dass sie nach einer ausführlichen, in den frühen Morgenstunden geführten Unterredung mit ihrer Schwester mehrfach mit einer Einrichtung für Elternplanung und Schwangerschaftsabbrüche telefoniert hat. An der Verteilung

der Anrufe ließen sich Rückschlüsse ziehen, zu welchem Zeitpunkt die Schwangerschaft entdeckt und wann die Abtreibung durchgeführt wurde. All dies ging, ohne ein Wort der Kommunikation mitgehört zu haben.

Auch im militärischen Bereich nehmen Metadaten eine immer bedeutendere Rolle ein. Anhand von Metadaten werden Bewegungsprofile erstellt, die darüber Aussagen treffen sollen, ob eine Person terroristischen Aktivitäten nachgeht. Im Extremfall geht es sogar soweit, dass die Metadaten dafür herangezogen werden, Menschen in Krisengebieten per Drohnenangriff zu töten. Der ehemalige NSA- und CIA-Chef Michael Hayden hat dies auf den Punkt gebracht, als er auf einem Universitätspodium im April 2014 sagte: „We kill people based on metadata."

5.

Datenschutz und politischer Aktivismus

Auch politischer Aktivismus kann ein Grund dafür sein, ins Visier staatlicher Überwachungsmaßnahmen zu gelangen. Dies bezieht sich insbesondere auf die Maßnahmen des sogenannten Verfassungsschutzes (ein Bundesamt und 16 Landesämter), der zur Aufgabe hat, die freiheitlich-demokratische Grundordnung (FDGO) zu verteidigen. Die Verfassungsschutzämter arbeiten dabei mit einem Extremismusmodell, welches das politische Spektrum in eine gesellschaftliche Mitte und davon abweichende Positionen einteilt. Politische Orientierungen an den Rändern des Spektrums werden dabei als extremistisch bewertet, sofern diese im Gegensatz zur bestehenden Mehrheitsgesellschaft stehen. Sofern jemand einmal als „extremistisch" gekennzeichnet wurde, kann dies zur Überwachung der Person führen. Dabei steht die verwendete Definition von Extremismus sehr stark in der Kritik. Bürgerrechtsorganisationen und Sozialwissenschaft-

ler*innen bemängeln unter anderem, dass lediglich das Abweichen von der Mitte als Indikator für extremistische Positionen herangezogen werde, während die Motivation unbeachtet bleibt. Hier wird insbesondere kritisiert, dass sogenannte linksextremistische Gruppen die herrschende Wirtschaftsordnung ablehnen und bekämpfen, während im Rechtsextremismus Menschen auf Grund ihrer Herkunft, Religion oder sexuellen Orientierung abgelehnt werden. Eine Gleichstellung beider Motivationen erscheint auf Grund der unterschiedlichen Zielrichtung unzulässig und verharmlosend gegenüber der rechtsextremen Menschenfeindlichkeit. Darüber hinaus wird dem Extremismusmodell ebenfalls begriffliche Unschärfe vorgeworfen. [1]

Auch gab es in der Vergangenheit immer wieder Fälle, in denen Aktivist*innen und Journalist*innen wegen ihres Eintretens gegen Nazis und rechte Gewalt durch die Verfassungsschutzämter beobachtet wurden, ohne dass auch nur die Möglichkeit eines Verstoßes gegen die FDGO plausibel erscheint. So wurde unter anderem die preisgekrönte Journalistin Andrea Röpke jahrelang vom Verfassungsschutz beobachtet, weil sie bei einer Veranstaltung gesagt haben soll, sie werde „gegen den Faschismus in jeder Form kämpfen“. [2] Auch der Journalist Ronny Blaschke, der seit Jahren über Gewalt und Diskriminierung im Sport berichtet, wurde jahrelang vom Verfassungsschutz beobachtet, ohne dass dieser einen Grund dafür nennen könnte. [3] Blaschke hält seit Jahren Vorträge in Fanprojekten, an Schulen und Universitäten. Ähnlich erging es dem Rechtsextremismus-Experten und Journalisten Kai Budler. Budler wurde vom Verfassungsschutz beobachtet mit dem Vorwurf, er trete „in gestaltender Funktion bei Veranstaltungen linksextremistischer Gruppierungen auf“. In diesem Fall besonders peinlich: Die Überwachung durch den niedersächsischen Verfassungsschutz dauerte auch noch mehr als ein Jahr an, obwohl Kai Budler gar nicht mehr in Niedersachsen lebte. Dieses Detail war der Behörde offenbar entgangen, was nicht unbedingt ein positiver Beleg für die Qualität der Überwachung ist.

Die Beispiele zeigen, dass auch Personen, die gänzlich unverdächtig sind, die freiheitlich-demokratische Grundordnung zu bekämpfen, immer wieder im Visier der Verfassungsschutzämter landen, weil sie

sich gegen menschenverachtende Ideologien, Diskriminierung und Ausgrenzung einsetzen. Es finden sich zahlreiche weitere Beispiele, die zeigen, dass die Macht der Verfassungsschutzämtern nicht nur gegen Gefahren für eine freiheitliche Gesellschaft, sondern auch gegen politisch nicht gewollte oder ungemütliche Kritiker*innen eingesetzt werden kann.

Insbesondere in der antifaschistischen und globalisierungskritischen Szene, aber auch im Bereich des Tierrechtsaktivismus häufen sich Berichte von verdeckten Ermittler*innen, die die Vorbereitung von Protestaktionen im Zusammenhang mit Großveranstaltungen wie den G8-Gipfeln ausspionieren sollen. Nach der Enttarnung einiger Spitzel stellte sich jedoch wiederholt heraus, dass diese ihre Ermittlungsbefugnisse (z.B. durch das Betreten von Privatwohnungen, das Anstacheln zu kriminellen Handlungen oder auch durch das Eingehen sexueller Beziehungen) erheblich überschritten haben oder ihr Einsatz schon zu Beginn auf äußerst diffuse Begründungen wie eine nicht näher präzisierte Gefahrenabwehr beruhte. [4]

Besonders umstritten war die vom Bundeskriminalamt (BKA) geführte Datenbank „International agierende gewaltbereite Störer“ (IgaSt). Für eine Aufnahme in die Datei soll schon ausreichen, einmal im Zusammenhang mit (G7-, NATO-, EU-) Gipfelprotesten kontrolliert worden zu sein. Auf Basis solcher Dateien werden vor großen Gipfeln regelmäßig Einreiseverbote ausgesprochen. Inwiefern solche Dateien ihre Berechtigung haben, lässt sich nicht abschließend klären, weil die Gründe für eine Aufnahme in die IgaST-Datei unklar sind, zumindest aber ein recht vager Verdacht ausreicht. Aus Datenschutz-Perspektive ist jedenfalls die Gefahr zu sehen, dass hier legitimer politischer Protest mit strafbarem Verhalten vermischt wird, was zu einer Kriminalisierung politischen Engagements führen kann. Die IgaST-Datei wurde 2011 abgeschafft, ihre Inhalte finden sich inzwischen aber größtenteils in der Zentraldatei „politisch motivierte Kriminalität links“ (PMK links-Z) des BKA. [5]

Für Aktivist*innen sollte daher gelten, nicht nur im Zusammenhang mit Demonstrationen oder Aufklärungsveranstaltungen auf die eigene Sicherheit zu setzen, sondern auch bei der Kommunikation unter-

einander auf Datensparsamkeit und Verschlüsselung zu achten. Zum Beispiel sollten in der schriftlichen Kommunikation oder auf öffentlichen Veranstaltungen möglichst keine (Nach-)Namen genannt werden, Mails und Chats sollten verschlüsselt sein und auf Fotos können z.B. mit der App ObscuraCam Gesichter unkenntlich gemacht werden. Datenschutz ist eben immer auch Schutz vor unfreiwilliger Offenbarung der eigenen Identität durch staatliche Stellen und politische Gegner*innen Wenn Ihr vermutet, dass Ihr zu Unrecht in einer Datenbank für politisch motivierte Kriminalität zu finden seid, erfahrt im Text zu Auskunftsansprüchen, wie Ihr dies herausfindet und ggf. die Löschung beantragen könnt.

[1] http://www.pr.uni-freiburg.de/pm/2009/pm.2009-12-04.420
[2] http://www.spiegel.de/spiegel/vorab/journalistin-andrea-roepke-strafanzeige-fuehrte-zur-beobachtung-a-952301.html
[3] http://www.sueddeutsche.de/medien/sportjournalist-von-verfassungsschutz-beobachtet-unter-verdacht-1.1780710
[4] Für weitere Informationen zu dem Thema hilft es einfach mal die Namen Danielle Durand, Mark Stone, Simon Brenner, Lyn Watson oder Marco Jacobs in die Suchmaschine deiner Wahl einzugeben.
[5] https://www.datenschmutz.de/moin/IgaSt

II.

Die Datenschutz-bewegung

1.

Datenschutz

Organisationen in Deutschland

Bewusst mit den eigenen Daten umzugehen ist wichtig – aber es reicht nicht immer. Angesichts der großen Datenschutzskandale, die sich in letzter Zeit häufen, ist es gut und wichtig, dass sich verschiedene Organisationen mit den Themen Datenschutz und informationelle Selbstbestimmung beschäftigen, Tipps verbreiten, Lobbying betreiben und Rechtsverstöße anprangern. In diesem Kapitel möchten wir daher einige der wichtigsten Datenschutz-Organisationen in Deutschland kurz vorstellen.

Arbeitskreis Vorratsdatenspeicherung (AK Vorrat)
www.vorratsdatenspeicherung.de

Der AK Vorrat ist ein deutschlandweiter Zusammenschluss von Verbänden und Personen, der sich gegen die Massenüberwachung durch Vorratsdatenspeicherung ausspricht. Im Kontext des AK werden u.a. die „Freiheit statt Angst"-Demonstrationen organisiert.

Chaos Computer Club (CCC)
www.ccc.de

1981 in Berlin gegründet, ist der Chaos Computer Club ein Zusammenschluss deutscher Hacker*innen und die bekannteste deutsche Datenschutzorganisation. Inzwischen haben sich sogenannte Erfa-Kreise (Erfahrungsaustausch-Kreise) und Chaostreffs in ganz Deutschland gegründet.

Deutsche Vereinigung für Datenschutz
www.datenschutzverein.de

„Datenschutz ist Menschenrecht", betont der DVD e.V. (mit Sitz in Bonn) und arbeitet darauf hin, über die Gefahren von Verstößen gegen dieses Recht aufzuklären. Bereits seit 1978 gibt er dazu die Fachzeitschrift DANA (Datenschutznachrichten) heraus.

Digitalcourage
www.digitalcourage.de

Seit 1987 setzt sich der Bielefelder Verein Digitalcourage, bis 2012 unter dem Namen FoeBuD bekannt, für Datenschutz und weitere Themen ein. Bekannt ist Digitalcourage vor allem für die Ausrichtung der

deutschen BigBrotherAwards. Ein Arbeitsschwerpunkt liegt auf der Ermächtigung zu digitaler Selbstverteidigung.

Digitale Gesellschaft
www.digitalegesellschaft.de

Die auf Kampagnenarbeit ausgerichtete Digitale Gesellschaft hat sich 2010 in Berlin gegründet. Sie arbeitet unter anderem ausführlich zu Verstößen gegen Netzneutralität.

European Digital Rights (EDRi)
www.edri.org

EDRi fungiert als Dachverband für Datenschutz- und Bürgerrechtsorganisationen aus ganz Europa. Aktuell nennt EDRi 33 Mitgliedsorganisationen. Schwerpunkte des in Brüssel angesiedelten Verbands sind Datenschutz-relevante Vorhaben auf EU-Ebene wie die Vorratsdatenspeicherung.

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)
www.fiff.de

Der Bremer FIfF besteht seit 1984 und versteht sich als Informatik-Fachverband, der sich kritisch mit den gesellschaftlichen Folgen von Entwicklungen in der Informationstechnik auseinandersetzt.

Netzpolitik.org
www.netzpolitik.org

Das der Digitalen Gesellschaft nahestehende Blog Netzpolitik.org setzt sich seit 2004 mit digitalen Themen wie Datenschutz und Überwachung auseinander und ist eine wichtige Informationsquelle für politische Entwicklungen in diesem Bereich.

2.

Big Brother Awards

die Oscars für Datenkraken

Big Brother (in der deutschen Übersetzung: Großer Bruder) ist die mysteriöse Führerfigur in George Orwells Roman „1984“. Sie symbolisiert die totalitäre Partei, die absolute Macht über das Großreich Ozeanien und seine Bürger*innen ausübt, indem sie jedwede Privatsphäre abgeschafft hat: Der Große Bruder sieht alles. Ein passender Namensgeber ist er deshalb für den „Big Brother Award“, einen oft auch

als „Oscar für Datenkraken“ bezeichneten Negativpreis, der zum ersten Mal 1998 in Großbritannien vergeben wurde. Seit 2000 findet auch in Deutschland jährlich eine Verleihung der Big Brother Awards (BBAs) statt. Sie wird ausgerichtet von Digitalcourage e.V. in Bielefeld. Eine Jury aus Mitgliedern diverser deutscher Datenschutzorganisationen vergibt Preise in mehreren Kategorien [1], darunter:

Behörden & Verwaltung: Der Bundesnachrichtendienst (BND) erhielt 2015 den Big Brother Award für seine Rolle im NSA-Skandal, da er massenhaft Telekommunikationsdaten von Bundesbürger*innen an NSA und Co. übermittelte und dabei von Seiten der verantwortlichen Politik nicht etwa eingebremst, sondern sogar aufgerüstet wurde.

Politik: Aus demselben Grund fand sich 2014 das Bundeskanzleramt auf der Liste der Preisträger*innen wieder. Ihm obliegt die Aufsicht über den BND und damit die Verantwortung für die massenhaften Bürgerrechtsverletzungen, die ihm Rahmen der Affäre begangen wurden.

Wirtschaft: 2007 wurde hier die Deutsche Bahn ausgezeichnet dafür, dass sie systematisch anonymes Reisen unmöglich macht. Als Beispiele wurden hier „Auflösen von Fahrkartenschaltern, Automaten ohne Bargeldannahme, personalisierter Kauf im Internet, Abfrage des Geburtsdatums und Zwangsabgabe eines Bildes bei Bahncards, flächendeckende Videoüberwachung und ein RFID-Chip in der Bahncard 100 ohne Kunden zu informieren“ zitiert.

Arbeitswelt: In dieser Kategorie werden Datenschutzverstöße von Unternehmen gegenüber Angestellten festgehalten – eine besonders perfide Ausnutzung von Machtpositionen, wie sie etwa 2011 in der Laudatio auf Daimler zu hören war, nachdem das Unternehmen flächendeckend Bluttests von seinen Mitarbeiter*innen forderte.

Kommunikation: 2011 wurden in dieser Kategorie gleich zwei Preise vergeben: An die „Gated Community“ Facebook und an Apple, welches seine Kund*innen zwingt, den zweifelhaften Datenschutzbestimmungen der Firma zuzustimmen. Übrigens: Für Konkurrentin Google wurde 2013 direkt eine eigene Kategorie geschaffen, Globales Datensammeln.

Im Jahr 2014 wurde zum ersten Mal auch ein Positivpreis vergeben. Der Julia-und-Winston-Award, angelehnt an die beiden Hauptfiguren aus „1984“, die sich gegen das totalitäre Regime auflehnen, ging an Edward Snowden für die Aufdeckung der globalen Überwachungsaffäre um die Geheimdienste NSA und GCHQ. Weiterhin wird ein ebenfalls von „1984“ inspirierter Neusprech-Award für Begriffe vergeben, die Überwachung und Datenschutzverstöße verschleiern sollen: So wurde 2015 „Digitale Spurensicherung“ als Euphemismus für die politisch verbrannte Vorratsdatenspeicherung honoriert.

[1] Alle Preisträger*innen und weitere Infos findet ihr unter: bigbrotherawards.de

3.

Post-Privacy

was kommt nach der Privatsphäre?

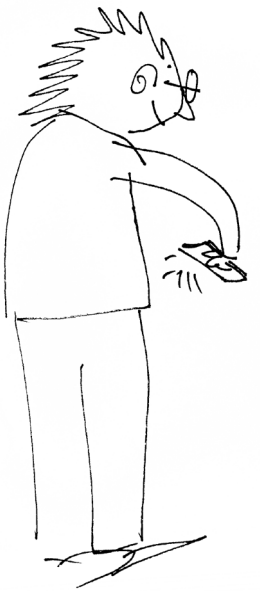
Was kommt nach dem Recht auf Privatsphäre? Massenüberwachung ist längst Realität, darüber machen sich die Autoren dieses Readers keine Illusionen. Die Meinungen darüber, wie damit umzugehen ist, gehen jedoch auseinander. Auf der einen Seite wird um Datenschutz und Privatsphäre gekämpft, und auch, wenn es womöglich niemals einen perfekten Schutz geben wird, können selbst Einzelne einiges dafür tun, um ihr Recht auf informationelle Selbstbestimmung einzufordern – das möchten wir mit diesem Reader dokumentieren. Auf der anderen Seite steht das Konzept der „Post-Privacy“.

„Datenschutz ist konzeptionell implodiert“, meint Blogger Michael Seemann [1] und erklärt ihn zum Rückzugsgefecht gegen die Datenflut. Das massenhafte Sammeln von Daten sei aus der gesellschaftlichen Wirklichkeit nicht mehr wegzudenken und werde mit fortschreitender technischer Entwicklung noch weiter zunehmen. Nicht einmal der Rückzug aus dem Netz helfe da weiter. Stattdessen fordern Vertreter*innen der Post-Privacy die Flucht in die Transparenz. Es müsse unter diesen Umständen um die Schaffung einer Gesellschaft gehen, in der alles über eine Person erfahrbar wird, in der das Konzept der Privatsphäre vollständig aufgegeben wird, ohne dabei in einen Orwell‘schen Totalitarismus zu münden. Datenschützer*innen halten ein solches Vorhaben für gefährlich, Post-Privacy-Vertre-

ter*innen (die sich selbstironisch als „Spackeria“ bezeichnen) für unausweichlich.

Stattdessen, so das Post-Privacy-Konzept, bringe das Ende der Privatsphäre neue Freiheitsräume. Solange das Datensammeln den Geheimdiensten überlassen werde, hätten diese das Monopol auf die Daten. Dieses zu überwinden könne nur durch die Offenlegung der Daten gelingen. Kritik, bei diesem vorauseilenden Gehorsam in Form von völliger Transparenz würden Menschen ihr Verhalten und Handeln radikal anpassen, wird dadurch nicht entkräftet. Allerdings ist diese Veränderung der menschlichen Gesellschaft ein integraler Bestandteil von Post-Privacy. Seine Privatsphäre aufzugeben wird damit zur bewussten Entscheidung zugunsten empfundener Freiheitsgewinne – eine Einschätzung, vor der wir unserer Ansicht nach nur warnen können. Dennoch ist das Post-Privacy-Konzept ein nicht zu leugnender Bestandteil der Debatte um Datenschutz und lohnt deshalb eine Beschäftigung.

[1] http://www.heise.de/ct/artikel/Archaeologie-der-Zukunft-1029002.html



III.

Datenschutz offline

1.

RFID

die Schnüffelchips

Hinter den Buchstaben „RFID“ verbirgt sich die Abkürzung für „Radio Frequency Identification“ - eine Technik im Kommen, wenn es nach den Herstellenden geht. RFID-Chips sind schwer zu findende, nur Millimeter dicke Speicherchips, auf denen eine Identifikationsnummer abgespeichert ist. Gerät der Transponder in die Reichweite eines Lesegeräts, fängt er dessen elektromagnetische Strahlung auf und schickt im Gegenzug seine Nummer zurück. Diese Technik soll als Diebstahlsicherung zunehmend die bekannten Barcodes auf Waren aller Art ersetzen. Ein lobenswertes Ziel – oder?

Das Problem ist, dass sich der Nutzen von RFID-Chips damit nicht erschöpft. Auch nach dem Verlassen des Geschäftes bleiben die Transponder aktiv. Wer Kleidungsstücke bestimmter Marken (z.B. Levi Strauss, Gerry Weber, C&A) kauft, trägt bereits jetzt mit hoher Wahrscheinlichkeit aktive Chips mit sich herum. Das ist solange einigermaßen unproblematisch, wie es noch keine umfassende RFID-Infrastruktur gibt – nur wenige Unternehmen nutzen die Technik bislang im großen Stil. Sollte sich das irgendwann ändern, wird jedes Geschäft die Chips auslesen können – und damit nicht nur unsere präferierten Marken und Produkte auslesen, sondern unter Umständen auch Bewegungsprofile erstellen können. Ein Szenario, das umso realistischer ist, wenn man weiß, dass seit 2005 in allen deutschen Reisepässen und seit 2010 in allen Personalausweisen ein RFID-Chip steckt.

Die Einsatzmöglichkeiten für RFID sind riesig. Ursprünglich als Militärtechnik konzipiert, wird sie heute für Chipkarten oder Zugangskontrollen für Fahrzeuge benutzt. Pläne der Europäischen Zentralbank, Geldscheine mit RFID-Transpondern auszustatten, wurden (bislang) nicht umgesetzt. Das Implantieren von RFID-Chips unter die menschliche Haut wurde bereits erfolgreich getestet – eine Möglichkeit, die an Szenarien aus dystopischen Science-Fiction-Filmen erinnert. Das ist noch kein Grund, in Panik zu geraten. Es gibt durchaus sinnvolle Einsatzmöglichkeiten für RFID. Überall dort jedoch, wo die Chips das Erfassen, Verfolgen und Überwachen von einzelnen

Menschen ermöglichen, stellen sie eine Bedrohung für die Privatsphäre dar, gerade weil noch niemand weiß, wie sich die RFID-Technik in Zukunft entwickelt und verbreitet.

Wie kann ich verhindern, durch die RFID-Technik überwacht zu werden? Im bislang größten Einsatzgebiet, Mode, sind die Chips häufig in den Etiketten angebracht (was sich erkennen lässt, wenn man das Etikett gegen eine starke Lampe hält): Abschneiden oder die Antenne, etwa mit einer Nadel, zerstören. Wird der Chip dagegen etwa im Futter eines Mantels versteckt, ist das Entdecken schon schwieriger. Handelsübliche Chips funken auf der Frequenz 13,56 MHz, was sich potentiell abhören lässt. Eine sichere Methode der Zerstörung ist ein elektromagnetischer Impuls. Den Chip für ein paar Sekunden in die Mikrowelle zu legen funktioniert, birgt allerdings das Risiko, auch den zugehörigen Gegenstand zu beschädigen. Auch das Abschirmen von Funksignalen ist möglich, etwa mit RFID-Schutzhüllen. Langfristig am Wirksamsten ist natürlich, sich über Unternehmen zu informieren, die RFID benutzen, und dort erst gar nicht einzukaufen – oder noch besser, die Verantwortlichen auf die Gefahren von RFID hinzuweisen.

2.

Mein Datenausweis

ePerso und „elektronische Gesundheitskarte“

Auch vor unseren Ausweiskärtchen macht das Thema Datenschutz keinen Halt - seit 2010 gibt es den „elektronischen Personalausweis“, seit 2014 die „elektronische Gesundheitskarte. Der elektronische Personalausweis, der anders als sein Vorgänger-Dokument in Chipkartenform ausgestellt wird, enthält seit 2010 einen RFID-Chip, auf dem digital Name, Geburtsdatum Geburtsort, Anschrift, Seriennummer (des Ausweises) und Lichtbild gespeichert werden. Zusätzlich können freiwillig zwei Fingerabrücke auf dem ePerso gespeichert werden, wovon unter Datenschutzgesichtspunkten jedoch abzuraten ist. Darüber hinaus kann im neuen Personalausweis die so genannte eID-Funktion aktiviert werden, die es ermöglichen soll, sich im Internet (z.B. beim Abschluss von Verträgen, bei der Antragstellung bei Behörden) auszuweisen. Die eID-Funktion muss bei der Ausstellung des Personalausweises von Euch im Bürger*innenbüro der

Stadt verlangt werden, lässt sich also leicht umgehen.

Um die Verbreitung dieser eID-Funktion voranzutreiben, wurden 2010 kostenlose Basislesegeräte durch den Bund verteilt. Versuche des Chaos Computer Clubs haben jedoch gezeigt, dass die kostenlos verteilten Geräte eine Sicherheitslücke darstellen können, da sie über keine eigene Tastatur zur Pin-Eingabe verfügen und die Nutzung der Computertastatur über so genannte Keylogger-Software mitgeschnitten werden kann. Lediglich die teureren Lesegeräte, die auf eigene Kosten beschafft werden müssen, vermeiden durch eine eigene Tastatur diese Gefahr. Letztendlich hat sich die eID-Funktion bisher als nicht besonders relevant herausgestellt – laut aktuellen Erhebungen nutzen lediglich 5% der Deutschen diese ePerso-Funktion. Auch wenn – anders als beim elektronischen Reisepass – die Speicherung biometrischer Daten auf dem Chip des Personalausweises nicht verpflichtend ist, stellt die Art seiner Einführung aus den oben genannten Gründen mindestens ein Sicherheitsrisiko dar.

Auch bei der elektronischen Gesundheitskarte ist der zusätzliche Nutzen umstritten. Die eGK enthält persönliche Daten wie Name, Geburtsdatum, Geschlecht, Anschrift, Versichertenstatus und Krankenversicherungsnummer. Darüber hinaus soll die neue Karte die Möglichkeit von freiwilligen Angaben zu unter anderem der individuellen Arzneimittelverträglichkeit enthalten, aber auch als Identifikationsmerkmal für die geplante elektronische Patientenakte dienen. Hierbei sollen Behandlungsdaten in einer zentralen Datenbank gespeichert werden; für den Zugriff muss die eGK vorliegen. Die elektronische Patientenakte wird seit 2011 in Deutschland als Modellversuch getestet und von Datenschützer*innen heftig kritisiert, da dabei hochsensible Gesundheitsdaten zentral gespeichert würden.

3.

Video-Überwachung

In London sind es über eine Million, in deutschen Städten zum Glück deutlich weniger: Dennoch sind Überwachungskameras in unserem Alltag allgegenwärtig. Von Bankschaltern und Tankstellen über Kaufhäuser bis zum Personennah-

verkehr gibt es zahlreiche Bereiche, in denen mehr oder weniger auffällig das Verhalten im öffentlichen Bereich gefilmt wird. Neben der staatlichen Überwachung machen den ganz großen Anteil private Kameras von Geschäften aus. Der Ruf nach mehr Kameras folgt regelmäßig auf (versuchte) Terroranschläge oder Gewalttaten im öffentlichen Raum (Stichwort U-Bahnschlägerei).

Dabei ist die Grenze zwischen angemessener Kontrolle, die ja auch dazu dient, Schwächere vor Übergriffen zu schützen, und einer Totalüberwachung des öffentlichen Lebens nur sehr schwer zu ziehen. Video-Aufzeichnungen erleichtern die Arbeit der Polizei, wenn es nach einer Straftat darum geht, die Täter*innen möglichst schnell zu finden. Auf der anderen Seite ist eine präventive Wirkung, also ein Schutz potentieller Opfer bisher nicht nachgewiesen, da auch die beste Kamera bei Affekttaten niemanden aufhalten kann. Auch führt Video-Überwachung nicht automatisch dazu, dass schneller Hilfe zur Stelle ist, weil der ganz überwiegende Teil der Kameras lediglich aufzeichnet, aber niemand live beobachtet, was gefilmt wird. Darüber hinaus haben Studien gezeigt, dass eine Verlagerung von Straftaten an nicht-überwachte Orte stattfindet.

Kameras lösen oft ein diffuses Gefühl der Überwachung aus. Ähnlich wie bei der Vorratsdatenspeicherung werden größtenteils unschuldige Personen überwacht, die davon in der Regel nichts mitbekommen. Auch wecken einmal für einen bestimmten Zweck gespeicherte Daten schnell Begehrlichkeiten aus anderen Bereichen. So wird zum Beispiel immer wieder gefordert, die für die Autobahn-Maut gespeicherten Video-Aufnahmen auch für die Strafverfolgung zu verwenden, also diese zu zweckentfremden. Richtig problematisch werden die Video-Mitschnitte allerdings, wenn man einen Blick in die Zukunft bzw. auf aktuelle Entwicklungen in diesem Bereich wirft. In Forschungsprojekten wie dem von der EU geförderten INDECT-Programm wird bereits an einer automatischen Auswertung der Überwachung gearbeitet, die „abnormales Verhalten“ feststellen soll, zu dem unter anderem langes Sitzen oder schnelle Bewegungen zählen. Es braucht nicht viel Fantasie, um sich vorzustellen, dass solche Maßnahmen schnell zu uniformen Verhalten aus vorauseilendem Gehorsam gegenüber der Software

führen. Störungen im geordneten Ablauf – seien es Obdachlose oder Demonstrant*innen – werden dabei als Abseits der Norm und damit potentiell gefährlich betrachtet. Darüber hinaus ermöglichen immer zuverlässiger arbeitende Gesichtserkennungsprogramme, dass auch große Mengen von Daten verarbeitet, also eine Person in der Vielzahl der Video-Bilder durchgehend verfolgt werden kann.

Nicht jede Form der Video-Überwachung ist schlecht. In Banken oder Spielcasinos sind Kameras sogar gesetzlich vorgeschrieben, was angesichts der großen Geldbeträge auf kleinem Raum unmittelbar einleuchtend ist. Eine Sicherheitspolitik, die auf Grund abstrakter Gefahren ganz konkret die informationelle Selbstbestimmung jeder Person, die sich im öffentlichen Raum bewegt, einschränkt, ist jedoch problematisch!

4.

Bonuskarten: Null Punkte für den Datenschutz

In diesem Jahr feiert das Unternehmen Payback sein 15-jähriges Bestehen – und damit seine Erfolgsgeschichte: Die Payback-Karte ist die am weitesten verbreitete Bonuskarte in Deutschland und wird in Millionen Portemonnaies mitgeführt. Daneben existieren weitere Bonuskarten wie Deutschlandcard, IKEA Family Card, Shell ClubSmart usw. Das Prinzip ist so einfach wie vielversprechend: Der*-Die Kund*in lässt an der Kasse die Karte einscannen und erhält dafür Bonuspunkte, gemessen am Wert des Einkaufs. Diese Punkte können in Prämien oder Preisnachlässe umgewandelt werden. Klingt nach einem guten Geschäft?

Nicht für die Kund*innen, die „häufig nur einen mageren Preisnachlass“ erhalten, wie die Verbraucherzentrale NRW feststellt [1]. Für die Unternehmen dafür umso mehr: Bonuskarten binden an bestimmte Unternehmen, sodass günstigere Angebote bei der Konkurrenz häu-

fig außer Acht gelassen werden – auch, weil Punkte schnell verfallen und man damit quasi gezwungen wird, in kurzen Zeiträumen viel einzukaufen. Unterm Strich bezahlen die Kund*innen damit häufig durch Kundenkarten sogar mehr anstatt weniger. Doch das ist nicht der Hauptgrund, weshalb diese Programme für Unternehmen derart attraktiv sind. Denn auch bei sogenannten Bonuskarten geht es in erster Linie um eines: Das Sammeln von Daten.

Wer beim Einkauf seine Karte vorlegt, gibt gleichzeitig seine Anonymität ab. Gespeichert werden Ort und Zeitpunkt des Kaufs sowie der Preis, bei Zustimmung des*der Kund*in auch die Art der Ware – es lohnt sich unbedingt, das Kleingedruckte zu lesen. Doch auch ohne Produktnamen genügen die gespeicherten Daten in Verbindung mit den vorliegenden Personalien, um bei wiederholtem Einkauf Kund*innenprofile zu erstellen: Wie oft kaufen bestimmte Personen ein? Wie viel Geld geben sie dabei aus? Wo wohnen Menschen, die besonders viel Geld im Laden lassen (und wo sollte deshalb intensiver geworben werden)? Die Daten werden zu Werbezwecken auch an Partnerunternehmen übermittelt. Das heißt, ein Supermarkt, der Payback beauftragt, profitiert auch von den gesammelten Daten anderer Payback-Partner*innen. Auf diese Weise bleiben die Informationen nicht, wie der*die Kund*in vielleicht glaubt, im Supermarkt um die Ecke, sondern werden in ein kommerzielles Netzwerk eingespannt, das mit diesen Daten großes Geld macht. „Immerhin bleiben die Daten in Deutschland“, mag man vielleicht denken. Nun, Payback etwa gehört seit 2011 zur American-Express-Gruppe …

Bereits 2000 erhielt die Payback-Karte den Big Brother Award für „Business & Finanzen“ mit der Begründung, dass hier „die Konsumgewohnheiten von Bürgerinnen und Bürgern ausgeforscht, ausgewertet und auf unabsehbare Zeit gespeichert“ werden [2]. Seitdem wurde Payback mehrmals von deutschen Gerichten dazu gezwungen, seine Formulare anzupassen (auf denen explizit nach Daten gefragt wird, die für die Rabattsammlung unerheblich sind). Am Grundsatz hat das wenig geändert: Bonuskarten – und das bedeutet nicht nur Payback, sondern alle derartigen Karten – sind eine Sammelmaschine, die für Kund*innen kaum geldwerte Vorteile (oder sogar de facto

Nachteile) abwirft. Für die Firmen, die man sich in harmloser Plastikform in die Geldbörse steckt, ist das jedoch eine Goldmine, und der Datenschutz bleibt auf der Strecke.

[1] http://www.vz-nrw.de/Kundenkarten-Wenig-Rabatt-fuer-viel-Information-1
[2] https://bigbrotherawards.de/2000/business-finanzen-payback

5.

Schufa

Die Schufa ist ein Unternehmen, das zum großen Teil Banken gehört. Sie hat Daten von über 66 Millionen Menschen in Deutschland gespeichert. Auf Grundlage dieser Daten werden „Scores“ berechnet, die Aufschluss über die Kreditwürdigkeit der entsprechenden Personen geben sollen. Banken, Handels- und Telekommunikationsunternehmen und Versicherungen beurteilen danach ob und zu welchen Konditionen sie jemandem einen Vertrag anbieten.

Die Daten, darunter zum Beispiel ob und wie viele Girokonten und Kreditkarten jemand hat, ob ein Kredit aufgenommen wurde und dieser rechtzeitig abbezahlt wird oder ob jemand seine Rechnungen nach Mahnung nicht begleicht, erhält die Schufa von ihren Geschäftspartner*innen. Diese können wiederum im Gegenzug bei berechtigtem Interesse auf einzelne Datensätze zugreifen.

Der (aus Datenschutzgesichtspunkten problematische) Datentausch im großen Stil ist mit dem Bundesdatenschutzgesetz vereinbar, weil die betroffenen Personen die sogenannte „Schufa-Klausel“ unterzeichnet haben. Läuft es wirtschaftlich gut, profitiert man meist davon. Denn dadurch, dass man seiner Bank die Zusammenarbeit mit der Schufa ermöglicht, kann man seine Kreditwürdigkeit beweisen. Das ist in aller Regel Voraussetzung, um zum Beispiel ein Girokonto eröffnen zu können.

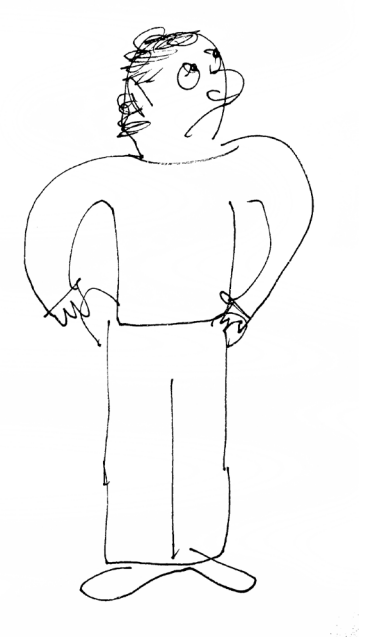
Anders jedoch, wenn man von der Schufa als unzuverlässig bewertet wird: Der Zinssatz, zu dem man einen Kredit aufnehmen kann, fällt höher aus oder Angebote wie ein Girokonto werden ganz verweigert. Solchen drastischen Folgen steht ein undurchsichtiges Verfahren zur Berechnung der „Scores“ gegenüber: So könnte zum Beispiel ein häufiger Wechsel des Wohnorts statistisch ein Indiz für Unzuverläs-

sigkeit sein. Inwiefern auch Daten über Einkommen, Geschlecht, Alter und Familienstand in die Bewertung einfließen, ist unklar. Hieran lässt sich die zunehmende Macht der Daten und Algorithmen erahnen, denen der Einzelne ausgeliefert ist. 2012 wollte die Schufa mit dem Hasso-Plattner-Institut erforschen, wie sich Daten aus sozialen Netzwerken für die Beurteilung der Kreditwürdigkeit nutzbar machen lassen. Nach Protesten wurde die Zusammenarbeit jedoch von Seiten des Instituts aufgekündigt.

Besteht der Grund für eine schlechte Schufa Bewertung nur darin, dass falsche Daten zugrunde lagen, kann man diese nach Einholen einer Auskunft (siehe Rechtliches: Auskunftsansprüche) berichtigen lassen.

Dem Erstellen eines „Scores“ (nicht aber der generellen Datenerhebung und -weitergabe) kann man bei der Schufa schriftlich wiedersprechen. Jedoch ist nicht klar, ob sich daraus negative Folgen für zukünftige Geschäfte ergeben. Bis 2001 war es sogar Praxis der Schufa, Auskunftsersuche nach dem Bundesdatenschutzgesetz als Negativmerkmal zu hinterlegen.

Zudem besteht die Möglichkeit, gar keine „Schufa-Klauseln“ zu unterzeichnen. Es ist jedoch unwahrscheinlich, dass sich die Unternehmen darauf einlassen. Entsprechende Angebote könnte man also nicht wahrnehmen und unterläge so ähnlichen Einschränkungen wie bei einer Schufa-Negativbewertung. Ab 2016 zumindest gibt es infolge eines Beschlusses des Europäischen Parlaments einen Anspruch auf ein Girokonto auf Guthabenbasis für „Jedermann“, das dann auch ohne Schufa-Klausel eröffnet werden kann.



IV.
Datenschutz online

1.

Facebook, die Datenkrake

Jedes Mal, wenn Facebook ankündigt, seine Nutzungsbedingungen zu ändern – und das passiert nicht gerade selten, zuletzt im Januar 2015 – taucht ein regelrechter Sturm von Statusupdates auf, in denen Nutzer*innen den neuen Regeln widersprechen. Ein gewisses Maß an Besorgnis, lässt sich daraus wohl schließen, ist also vorhanden bei den beinahe anderthalb Milliarden Menschen, die sich inzwischen per Facebook vernetzen. Gleichzeitig sprechen diese Widersprüche Bände über die Hilflosigkeit gegenüber der Datenkrake Facebook, denn sie haben schlichtweg keinen Nutzen. Wer Mitglied bei Facebook ist, akzeptiert automatisch sämtliche Einstellungen, die Facebook den Nutzer*innen auferlegt. Der einzige Weg, geänderten Einstellungen zu widersprechen, ist, Facebook zu verlassen – und auch das ist alles andere als einfach, denn selbst wenn du deinen Account stilllegst, bleiben deine Daten auf Facebook-Servern gespeichert.

Viele Datenschützer*innen empfehlen deshalb, Facebook gar nicht erst zu nutzen. Das wäre konsequent, übersieht aber angesichts der (bedenklichen) Monopolstellung des Netzwerks, wie schwer ein solcher Ausstieg für viele von uns ist, welche Folgen er für das soziale Umfeld nach sich zieht. Facebook schafft Abhängigkeiten. Dagegen erscheinen die Datenschutzprobleme als das kleinere Übel, zumal die Wenigsten so genau wissen, welche Einstellungen gerade aktuell sind, was die ganze Welt sehen kann und was mit diesen Daten passiert.

2011 erstellte ein Mädchen aus Hamburg eine Facebook-Veranstaltung – eine kleine, private Geburtstagsparty, die nicht lange klein und privat blieb, weil das Mädchen vergaß, die Veranstaltung als „privat“ zu markieren. In der Folge sagten 15.000 Menschen zu, und ein Polizeieinsatz war nötig, um die Feierwilligen davon abzuhalten, das Haus zu stürmen. Es lohnt sich also, genau darauf zu achten, was man bei Facebook anklickt und was nicht – die Folgen sind nicht immer absehbar, erst recht nicht langfristig.

Besonders gravierende Veränderungen haben die Facebook-Stan-

dardeinstellungen im Laufe der Jahre durchgemacht. War früher der bestmögliche Schutz die übliche Einstellung, und Daten öffentlich freizugeben musste manuell eingestellt werden, so sind inzwischen die meisten Standardeinstellungen erst einmal so öffentlich, also datenschutz-unfreundlich, wie möglich. Natürlich mag es sein, dass zu dem Zeitpunkt, an dem du diesen Reader liest, schon die nächste Änderung der Nutzungsbedingungen ins Land gezogen ist und das nächste Datenloch aufgerissen hat. Es lohnt sich also, die Augen offen zu halten und gelegentlich mal einen Blick in deine Einstellungen zu werfen. Hier ein paar Beispiele für Einstellungen, die anzuschauen sich lohnen.

Profil-Informationen

Das offensichtlichste Problem: Fast alle Angaben, die Facebook von dir möchte, sind per Standard öffentlich, vom Wohnort bis zu sexueller Präferenz und politischen Einstellungen, Dinge also, die du vielleicht nicht mit jedem teilen möchtest. Das lässt sich zum Glück über den Button „Informationen aktualisieren“ im eigenen Profil leicht ändern. Inzwischen geht Facebook aber noch perfider vor: Änderst du, sagen wir, deinen Arbeitsplatz, so möchte Facebook häufig wissen, wer von deinen Freund*innen noch dort gearbeitet hat. Selbst wenn du diese Info unbedenklich findest, geht das anderen Menschen vielleicht anders. Jeder Mensch muss selbst entscheiden dürfen, wie er*sie mit seinen*ihren eigenen Daten umgeht! Einer der wichtigsten Hinweise also: Gib keine Informationen über andere preis!

Markierungen

Wenn ein*e Freund*in dich auf einem Foto markiert, wird dieses sofort in deiner Chronik angezeigt und ist also auch für andere sichtbar – sei es dein Urlaubsfoto im Bikini oder der Schnappschuss von der letzten Party, auf dem du schon nicht mehr völlig nüchtern zu sehen bist. Was tun? Oben in deiner Chronik findest du den Button „Aktivitätenprotokoll anzeigen“. Geh auf „Markierungen überprüfen“ und anschließend rechts oben auf das kleine Zahnrad. Dort kannst du aktivieren, dass du jedes Mal, wenn dich jemand markiert, erst einmal überprüfen kannst, ob du wirklich möchtest, dass die ganze Welt das zu sehen bekommt.

Werbeanzeigen

„Facebook berechtigt Anwendungen Dritter bzw. Werbenetzwerke weder zur Nutzung deines Namens noch zur Nutzung deines Bildes für Werbeanzeigen. Sollten wir dies in Zukunft gestatten, so wird die von dir ausgewählte Einstellung die Nutzung deiner Informationen regeln.“ Ein schönes Beispiel für die perfide Arbeitsweise von Facebook: Man bereitet schon einmal Datenschutzverstöße von übermorgen vor. Bearbeiten kannst du diesen Standard unter „Einstellungen“ oben rechts, dann „Werbeanzeigen“.

Apps

Inzwischen gibt es unzählige Facebook-Apps, und die meisten davon wollen vor allem eines: Ein großes Stück vom Datenkuchen. Das wird insbesondere dann problematisch, wenn du eine App verwenden möchtest und diese von dir verlangt, auch auf die Daten deiner Freund*innen zugreifen zu können, darunter zum Beispiel auf Fotos. Natürlich können auch deine Daten auf diese Weise eingesehen werden, ohne dass du davon etwas erfährst. Gehe oben rechts auf „Einstellungen“ und dann links auf „Apps“. Bei „Von anderen Nutzern verwendete Apps“ kannst du einsehen und ändern, welche deiner Daten deine Freund*innen womöglich weitergeben.

Suchmaschinen

Schon mal über eine Suchmaschine deinen Namen gesucht? Die Chancen stehen gar nicht so schlecht, dass du dabei über dein Facebook-Profil gestolpert bist. Das können aber auch, sagen wir mal, deine potentiellen Arbeitgeber*innen vor deinem Bewerbungsgespräch. Geh auf „Einstellungen“, dann auf „Privatsphäre“ und stelle die Standardeinstellung auf „nein“.

Veranstaltungen

Bei den meisten Veranstaltungen ist öffentlich einsehbar, wer daran teilnimmt. Was aber oft vergessen wird: Veranstaltungen bleiben bestehen, auch nachdem das Event vergangen ist! Das bedeutet, unter Umständen lässt sich noch Jahre später herausfinden, auf welcher Demo du damals mitgelaufen bist. Wenn du das nicht willst, hilft nur eines: Jede Veranstaltung einzeln manuell verlassen bzw. absagen. Dazu musst du über dein Profil auf „Veranstaltungen“ und dann „Vergangene Veranstaltungen“ gehen.

2.

Social Media: Alternativen?

Seit in den neunziger Jahren die ersten sozialen Netzwerke aufkamen, hat das Konzept eine beispiellose Erfolgsgeschichte hinter sich. Gegenwärtig sind rund 1,5 Milliarden Menschen bei Facebook registriert, etwa ein Fünftel der Weltbevölkerung. Auch andere Portale wie Instagram, Twitter oder Google+ zählen zu den am stärksten frequentierten Seiten im Netz. Zugleich häuft sich die Kritik an ebendiesen Seiten. Immer mehr User sind unzufrieden vor allem damit, wie die Netzwerke mit ihren Daten umgehen. Häufig wechselnde Bestimmungen, Weitergabe von Daten an Geheimdienste und allgemeine Intransparenz tragen mit dazu bei, die Benutzer*innen zu verunsichern. Dabei gehört genau das zur Geschäftsstrategie der Netzwerke: Die Benutzung der Seiten ist in der Regel kostenlos. Das bedeutet, die dahinter stehenden Unternehmen machen ihre Gewinne auf eine andere Weise – im Geschäft mit den Daten der Nutzenden.

Gibt es Alternativen? Zunächst ist festzustellen, dass es schwer ist, die Marktmacht von Facebook und Co zu brechen, weil diese stark auf Exklusivität ausgelegt sind. Wer auf der Suche nach einem sozialen Netzwerk ist, wird sich in der Regel für das entscheiden, bei dem die meisten Freund*innen und Bekannte aktiv sind – so werden bereits große Netzwerke größer, während kleinere Netzwerke nur dann eine Chance haben, wenn sie sich spezialisieren. (So kann sich Twitter deshalb am Markt halten, weil es deutlich anders funktioniert als Facebook. Die deutschsprachigen Alternativen meinvz und studivz sind dagegen genau daran gescheitert.) Eine Ablösung des Marktriesen Facebook ist damit schwierig – und Facebook weiß das und nutzt diese Machtposition bewusst aus.

In dieser vermeintlichen Schwäche neuer Netzwerke liegt jedoch zugleich auch eine Chance. Mit jedem neuen Datenskandal wächst das Misstrauen gegenüber Facebook und Co. Wir möchten mit diesem Reader dazu beitragen, dass Datenschutzprobleme nicht hilflos hingenommen werden. Wir möchten Diskussionen anstoßen. Für die*den einzelne*n Benutzer*in fehlt womöglich der Anreiz, von Facebook

zu einer Alternative zu wechseln. Für einen ganzen Freundeskreis dagegen, der sich mit dem Thema beschäftigt und darüber Lust bekommt, etwas Neues zu probieren, kann die Suche nach Alternativen zu einem spannenden Experiment werden.

2010 sorgte das neu gegründete Netzwerk Diaspora für einige Aufmerksamkeit. Funktional an Facebook und Google+ erinnernd, bricht Diaspora mit dem Datensammelwahn, indem das Netzwerk nicht über einen zentralen, firmeneigenen Server läuft. Stattdessen werden weltweit dezentrale Server aufgebaut, und via podupti.me kann jede*r Nutzer*in selbst entscheiden, über welchen davon sie*er sein Diaspora-Profil laufen lässt - oder sogar einen eigenen Server aufsetzen. Natürlich fehlen zu Letzterem häufig technisches Know-How und Hardware, und so wird man seine Daten weiterhin außerhalb der eigenen Reichweite lagern müssen, wenn auch in diesem Fall nicht in den Händen eines Konzerns, der Profit daraus schlagen will.
Ähnlich und nutzer*innenfreundlicher ist das dezentrale Netzwerk Friendica. Großer Wert wird auf Dezentralität gelegt; so können Diaspora/Friendica-Profile etwa mit Facebook verknüpft werden, damit Status-Updates von Kontakten dort auch im neuen Profil angezeigt werden. Beide Seiten benötigen eine gewisse Einarbeitung und laden gerade deshalb zum Probieren im Freundeskreis ein. Wichtig ist: Es gibt Alternativen zur Datensammelwut von Facebook, sie müssen nur genutzt werden!

3.

Tracking-Cookies

Hilfe, ich werde verfolgt

Wenn ich eine Website aufrufe, merke ich immer häufiger, dass diese Seite mich wiedererkennt. In sozialen Netzwerken bleibe ich eingeloggt; Shoppingseiten halten mir vor, was ich mir bei meinem letzten Besuch angeschaut habe. Diese Wiedererkennung funktioniert über so genannte Cookies – kleine Textdateien, die die Website in meinem Browser ablegt und dort beim nächsten Besuch wieder abrufen kann – und sie ist nützlich, aber auch bedenklich. Eine Seite wie Amazon kann auf diese Weise jeden Artikel, den ich mir dort jemals angeschaut habe, festhalten

und dadurch ein Profil für mich erstellen, das meine Interessen und Vorlieben berechnet und daraus Kapital schlägt.

Doch das „Verfolgen“ im Netz durch Tracking-Cookies geht noch darüber hinaus. Cookies übermitteln Daten in der Regel nur an die Website, auf der ich mir das Cookie eingefangen habe: Amazon verfolgt so meinen Browserverlauf auf Amazon, Ebay den Verlauf auf Ebay und so weiter. Jedoch ist es den Unternehmen möglich, ihr Ausspähen auszuweiten, indem die Webadresse der Seite in andere Seiten eingebettet wird. Eine beliebte Methode, das zu tun, sind Werbebanner. Inzwischen kommt kaum noch eine Seite ohne externe Werbung aus – zum Beispiel für Amazon. Natürlich zeigen diese Werbebanner häufig nicht irgendwelche Werbung, sondern Anzeigen, die genau auf mich zugeschnitten sind, eben indem sie auf den entsprechenden Cookie zugreifen. Zugleich registriert der Tracking-Cookie damit jeden Besuch auf einer Website, auf der Amazon-Werbung zu sehen ist. Auf diese Weise kann das Surfverhalten im Netz mittels Tracking-Cookies umfassend nachverfolgt werden.
Was kann ich dagegen tun? Jeder Browser lässt verschiedene Optionen im Umgang mit Cookies zu. Bei Firefox etwa gehe ich über „Einstellungen → Datenschutz → Chronik“: Lasse ich Firefox eine Chronik „nach benutzerdefinierten Einstellungen“ anlegen, so habe ich die Option, Cookies von Drittanbietern grundsätzlich abzulehnen. Natürlich kann ich Cookies auch generell ausschalten, oder einstellen, dass sie nach jeder Browser-Session gelöscht werden – das bedeutet dann allerdings, dass meine LogIn-Daten in Mail-Konten, sozialen Netzwerken usw. ebenfalls nicht mehr gespeichert werden. Auch kann ich bereits in meinem Browser gespeicherte Cookies anzeigen lassen und diese, wenn ich möchte, einzeln oder auch alle entfernen. So kann ich selbst darüber bestimmen, was ich Websites gegenüber preisgeben – und was ich lieber für mich behalten möchte.

Um das Tracking über Werbeanzeigen zu verhindern, bietet sich die Browser-Erweiterung „AdBlock Edge“ (Firefox) bzw. „AdBlock“ (Opera, Safari, Chrome) an. Diese blockiert standardmäßig Werbeanzeigen und damit die Möglichkeit, über diese Anzeigen Cookies im Browser abzulegen. Nicht empfehlenswert ist dagegen die häufig verwendete Erweiterung „AdBlock

Plus“, da diese eine Whitelist so genannter „Acceptable Ads“ zulässt. Vorwürfen zufolge lässt sich AdBlock Plus die Aufnahme marktstarker Unternehmen in diese Whitelist fürstlich entlohnen [1].

Eine andere Möglichkeit bietet die Browser-Erweiterung „Ghostery“, die derzeit für Firefox, Safari, Opera und Chrome existiert. Einmal installiert, zeigt Ghostery, symbolisiert durch ein kleines blaues Gespenst in der Menüleiste des Browsers, beim Aufruf einer Website jedes auf dieser Website aktive Programm an, das potentiell Daten weitergibt – von einfachen Share-Buttons bis zu Werbebannern und Tracking-Cookies. Ghostery ermöglicht es, einzelne dieser Programme (oder zum Beispiel auch generell Werbeprogramme) auszuschalten. Derzeit kennt Ghostery etwa 2000 Programme, die erkannt werden. Natürlich werden aber mit der Zeit neue Tracker entwickelt, die Ghostery nicht automatisch blockiert, deshalb empfehlen sich gelegentliche Updates. Besonders wichtig ist es, bei der Installation nicht die Funktion „GhostRank“ zu aktivieren, denn diese gibt selbst Nutzungsdaten weiter und sollte deshalb vermieden werden. Richtig benutzt ist Ghostery ein interessantes und nützliches Werkzeug, schon weil es offenlegt, wie unfassbar viele Programme und Dienste eigentlich scharf auf unsere Daten sind – und damit zeigt, wie wichtig es ist, beim Surfen im Netz den Datenschutz immer im Hinterkopf zu behalten.

[1] http://www.heise.de/newsticker/meldung/Schwere-Vorwuerfe-gegen-Werbeblocker-AdBlock-Plus-1897152.html

4.

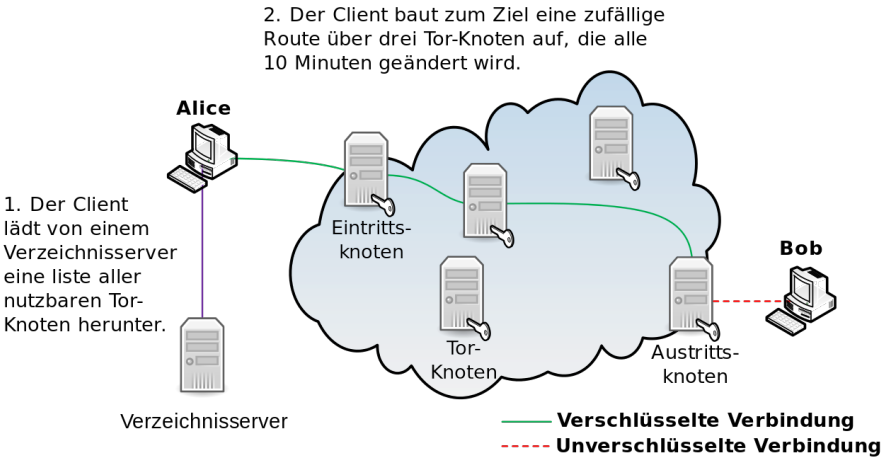
Anonym Surfen

IP-Verschleierung mit Tor

Sicherheitsbehörden und Werbefirmen versuchen das Verhalten Einzelner im Internet möglichst genau zu verfolgen. Als Erkennungsmerkmal dient dabei unter anderem die IP-Adresse, die sich einzelnen Nutzer*innen zuordnen lässt, um deren Surfverhalten zu analysieren. Wer sich im Internet anonym bewegen will, muss daher die IP-Adresse verschleiern. Hierfür eignet sich die freie Software Tor (The Onion Router), die von der Electronic Frontier Foundation (EFF, siehe: B. Die Datenschutzbewegung) entwickelt wurde. Tor funktioniert nach dem Prinzip des Onion-Routing. Die Nutzer*innen wählen sich

dabei über einen Client ein, der zum Ziel (also z.B. der aufgerufenen Seite) eine zufällige Verbindung über drei Tor-Knoten aufbaut, die alle zehn Minuten wechselt. Knoten 1 wird dabei als Eintrittsknoten bezeichnet, Knoten 3 als Austrittsknoten, dazwischen steht ein zufälliger Tor-Knoten. Während Knoten 1 den Kontakt zum Tor-User aufbaut und Knoten 3 den Kontakt zur Ziel-Homepage, wird jeglicher Datenverkehr zwischen User und Homepage durch den zufällig gewählten Tor-Knoten geschleust, sodass User und Zielseite nicht miteinander in Verbindung gebracht werden können.
Tor verschleiert dabei die Herkunft, nicht aber die Inhalte der Daten. Deshalb sollte zusätzlich immer HTTPS zur Verschlüsselung verwendet werden, wenn z.B. Login-Daten eingegeben werden. Darüber hinaus gibt es neben den IP-Adressen noch andere Identifizierungsmerkmale wie Cookies, für die man entsprechende Plug-Ins installieren sollte (s. Tracking). Mittels Tor lassen sich nicht nur IP-Adressen beim Surfen verschlüsseln; auch der eMail-Versand und Instant Messaging (z.B. über Jabber und Chatsecure) können „torifiziert“ werden.

Auf torproject.org kann die Software für Windows, Mac und Linux herunter geladen werden. Wer auf



Quelle: Saman Vosoghi, TOR Arbeitsweise.
Url: de.wikipedia.org/w/index.php?title=Datei:TOR_Arbeitsweise.svg&filetimestamp=20141103182401&

dem aktuell genutzten Rechner keine Software installieren darf (z.B. in der Uni oder im Internet-Café) kann die Version „Torpark“ verwenden, die auf einen USB-Stick kopiert und von dort gestartet werden kann. Für den Firefox-Browser gibt es die Möglichkeit, den so genannten Tor-Button zu installieren, mit dem sich Tor beliebig an- und ausschalten lässt. Letzteres kann durchaus sinnvoll sein, weil die Surfgeschwindigkeit gegenüber dem Betrieb ohne Tor deutlich verlangsamt ist.

Anonymes Surfen für Fortgeschrittene bietet das freie Betriebssystem Tails (The Amnesic Incognito Live System). Tails ist ein auf Linux basierendes Programm, das unabhängig vom Betriebssystem des Computers direkt von einem USB-Stick, einer DVD oder einer SD-Karte gestartet werden kann. Tails schleust jede ausgehende Verbindung durch das Tor-Netzwerk und sorgt dafür, dass Daten nicht auf der Festplatte des Rechners, sondern nur im Arbeitsspeicher festgehalten und damit nach dem Herunterfahren des Gerätes gelöscht werden.
Tor gilt als relativ sicherer Weg der Verschleierung von IP-Adressen und wurde unter anderem vom NSA-Whistleblower Edward Snowden genutzt. In der Vergangenheit wurden von Sicherheitsforscher*innen jedoch mehrfach Schwachstellen in der Software aufgezeigt, wie in Einzelfällen mit dem Aufwand großer Ressourcen teilweise eine De-Anonymisierung erreicht werden konnte. Wie auch bei Verschlüsselung gilt bei der Verschleierung von IP-Adressen, dass es niemals 100%ige Sicherheit geben wird, die Wahrscheinlichkeit unerkannt zu bleiben aber durch die Nutzung von Tor erheblich gesteigert wird.

5.

Mail-Verschlüsselung mit PGP

Wenn über Verschlüsselung gesprochen wird, muss erst einmal grundsätzlich unterschieden werden, ob es um eine Transport- oder eine Ende-zu-Ende-Verschlüsselung geht. Transport-Verschlüsselung bedeutet, dass der Kontakt zwischen Absender und Server verschlüsselt wird, während auf dem Server die Mails wiederum unverschlüsselt gespeichert werden, bevor sie weiter versandt werden.

Wirklich sicher ist hingegen nur die Ende-zu-Ende-Verschlüsselung, bei der eine Nachricht, in diesem Fall eine eMail, während des gesamten Sendevorgangs verschlüsselt ist und erst bei dem*der Empfänger*in wieder entschlüsselt wird. Eine Ende-zu-Ende-Verschlüsselung lässt sich am Besten mit dem Programm Pretty Good Privacy (PGP) erreichen, an der sich nach aktuellem Kenntnisstand auch die NSA noch die Zähne aus beißt.

Die Verwendung von PGP unterscheidet sich geringfügig zwischen den verschiedenen Betriebssystemen und eMail-Programmen. Allgemein kann jedoch gesagt werden, dass die meisten Webmailer (Googlemail, Yahoo, Gmx, Web.de etc.) die Verschlüsselung im Browser nicht unterstützen, weshalb die Mail-Konten am Besten in das Desktop-Programm Thunderbird importiert werden sollten. Thunderbird ist open source-Software und bietet den gleichen Umfang wie das Microsoft-Programm Outlook.

Zunächst muss in Thunderbird das Add-on „Enigmail“ installiert werden, das sich unter Extras → Add-ons findet. Zusätzlich muss die eigentliche Verschlüsselungssoftware OpenPGP installiert werden, worauf allerdings auch direkt bei der Installation des Add-ons hingewiesen wird.

Ist die Software installiert, muss ein so genanntes Schlüsselpaar erstellt werden. PGP arbeitet mit einem System, das aus einem öffentlichen und einem privaten Schlüssel besteht. Der öffentliche Schlüssel dient meinen Kommunikationspartner*innen dazu, die Mail an mich zur verschlüsseln. Die verschlüsselte Mail kann wiederum nur öffnen, wer sich im Besitz des privaten Schlüssels befindet. Das Erstellen der Schlüssel funktioniert ganz einfach unter der Option „Schlüssel verwalten“.

Der öffentliche Schlüssel muss danach den Kommunikationspartner*innen mitgeteilt werden, indem er per Mail verschickt wird oder auf einen Schlüsselserver hochgeladen wird. Wenn ihr die öffentlichen Schlüssel eurer Kommunikationspartner*innen habt, kann die Mail nun mit einem Mausklick verschlüsselt werden. Bedenkt dabei, dass ihr eure privaten Schlüssel nicht verlieren solltet, weil sich die eMails ohne den eigenen Schlüssel nicht wieder entschlüsseln lassen – genau das ist ja das Prinzip von PGP.

6.

Zu datenschutzfreundlichen Mailprovidern wechseln

sinnvoll und einfach

Große Datensammlungen entstehen nicht nur durch unsere Facebook-Aktivitäten, sondern auch bei unseren eMail-Anbietern. Viele eMail-Anbieter erheben keine Gebühren, sondern finanzieren sich durch die Nutzung unserer Nachrichten zu Werbezwecken. Googlemail rastert zum Beispiel alle Mails nach Schlagworten, um passgenaue Werbung anzuzeigen. Anders als bei Social Networks ist es jedoch relativ leicht, den eMail-Anbieter zu wechseln, ohne seine Kontakte oder die zurückliegende Korrespondenz zu verlieren.

Um die eigenen eMails vor sammelwütigen Konzernen zu schützen, bietet sich der Wechsel zu einem Provider mit hohen Datenschutzstandards an. In Deutschland kommen hier vor allem posteo.de, mailbox.org und tutanota.com in Frage. Auch in anderen Staaten gibt es datenschutzfreundliche Anbieter*innen – eine gute Übersicht hierzu gibt es auf: https://www.prxbx.com/email/

Posteo.de und mailbox.org verlangen dafür eine Gebühr von einem Euro pro Monat – also in etwa so viel wie ein Kaffee in der Mensa. Tutanota.com ist dagegen kostenlos und finanziert sich über Spenden. Alle drei Angebote bieten verschlüsselte Mailspeicher, unterscheiden sich jedoch im Einzelnen. Mailbox.org schneidet in vielfach als Testsieger ab, während posteo.de aktuell als erfolgreichster Anbieter gilt. Wir möchten an dieser Stelle keine Empfehlung für den ein oder anderen Dienst aussprechen, aber allen empfehlen durch einen Wechsel für mehr Sicherheit bei den eigenen Mails zu sorgen! Neben dem Wahl des „richtigen“ Providers sollten eMails natürlich auch Ende-zu-Ende verschlüsselt werden (siehe voriges Kapitel).

7.

Suchmaschinen

Alternativen zu Google und Co

Heute schon gegoogelt? Weltweit laufen beinahe drei Viertel aller Suchanfragen, in Deutschland sogar fast 95%[1], über Google. Damit hat Google Inc. Zugriff auf ein nahezu unvorstellbares Datenvolumen, zumal der Konzern neben seiner Suchmaschine auch noch über seinen Mail-Dienst Gmail, sein soziales Netzwerk Google+, über Youtube, seine Betriebssysteme und Browser wie Android und Google Chrome und viele weitere Dienste im Web unterwegs ist und Daten einsaugt wie kein anderer Konzern. Diese Marktmacht ist bedenklich.

Google ist für viele der zentrale Zugangspunkt zum Internet. Man ruft Websites nicht direkt auf, sondern googelt sie - „Googeln“ ist inzwischen zum Synonym für „im Internet suchen“ geworden. Damit weiß Google zunehmend Bescheid über jeden Schritt, den wir im Internet unternehmen. Und das ist auch genau die Strategie: „Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht tun“, hat besagter Larry Page seine Einstellung zum Datenschutz prägnant zusammengefasst [2]. Gmail liest automatisch sämtliche empfangene Mails mit, um dazu passende Werbung einblenden zu können. Und viele Websites nutzen Dienste wie Google Analytics, die bei jedem Besuch einer Seite Daten erheben und an den Konzern weiterleiten.

Google ist mittlerweile derart omnipräsent, dass es gar nicht so leicht ist, den Konzern zu vermeiden. Eine Sache dagegen ist einfach: Alternative Suchmaschinen nutzen. Die Rede ist hier nicht von Anbietern wie Bing (Microsoft) oder Yahoo, die genauso datensammelwütig sind wie der große Bruder Google. Stattdessen lohnt es sich, zu Alternativen wie DuckDuckGo.com oder Ixquick.com zu greifen, die keinerlei Suchanfragen speichern. Ebenfalls eine Empfehlung wert: Metager.de, eine deutsche Meta-Suchmaschine mit hohen Datenschutzstandards. Wer also weiterhin im Internet suchen möchte, ohne dass jemand davon erfährt, wonach – Finger weg von Google!

Noch ein Hinweis: Schon längst ist wissenschaftlich belegt, dass Sprache Handeln und Verhalten formt [3]. Hier wird das mehr als

offensichtlich: Wen über Suchen im Internet gesprochen oder geschrieben wird und dabei nur von „googeln“ die Rede ist, dann wird auch weiterhin Google das Mittel der Wahl bleiben. Das freut Larry Page, weil damit garantiert ist, dass er auch in Zukunft mit Datenbergen jonglieren kann – deinen Datenbergen. Warum also nicht mal wieder „nachschlagen“ statt „googeln“ - oder wie wäre es mit „ixquicken“? Das sorgt garantiert für Nachfragen, und damit hast du direkt die Gelegenheit, einfache Tipps zum Datenschutz an Freund*innen und Bekannte weiterzugeben.

[1] http://www.seo-united.de/suchmaschinen.html
[2] https://bigbrotherawards.de/2013/globales-datensammeln-google
[3] Siehe ein Artikel in der AStA-Zeitung Links vorm Schloss Juli 2014 zu geschlechtergerechter Sprache: http://www.asta.ms/dokumente-und-downloads/publikationen/links-vorm-schloss/4153-links-vorm-schloss-2014-07

8.

Sichere Kurznachrichten

Alternative Messenger neben WhatsApp

Ein mulmiges Gefühl mit WhatsApp

Mit über 450 Millionen Nutzer*innen ist WhatsApp der mit Abstand beliebteste Messenger-Dienst, den es zurzeit gibt. Dass jemand ein Smartphone besitzt, aber WhatsApp nicht nutzt, ist eine Seltenheit und auch wenig verwunderlich angesichts der praktischen Bedeutung von Kurznachrichten in unserem Kommunikationsverhalten. Darüber hinaus hängt der Nutzen eines Messenger-Dienstes sehr stark von dessen Verbreitungsgrad ab, da die meisten Messenger als ein geschlossenes System fungieren. Wenn mein Mailprovider meine Kommunikation durchleuchtet, kann ich relativ einfach zu einem datenschutzfreundlicheren Alternativangebot wechseln und behalte alle meine Kontakte. Wenn hingegen ein Messenger wie WhatsApp in Sachen Datenschutz in der Kritik steht, bedeutet der Wechsel zu einem anderen Anbieter ein Verzicht

auf alle meine Kontakte, was viele trotz erheblicher Kritik am Marktführer dazu bewegt, trotz eines mulmigen Gefühls weiter die App mit dem grünen Logo zu verwenden.

Nach der Übernahme von WhatsApp durch Facebook im Februar 2014 gab es medial viel Wirbel um die Macht des Anbieters (und damit auch den Einfluss des Zuckerberg-Konzerns auf die globale Kommunikation). Online findet sich eine Vielzahl von Einschätzungen, welche Messenger-Dienste bestimmte Verschlüsselungsstandards erfüllen und wo jeweils Sicherheitsprobleme liegen.

Was sind die Alternativen?

Im Folgenden soll daher nur kurz ein Überblick gegeben werden, worauf bei der Wahl des Messengers meines Vertrauens geachtet werden sollte. In jedem Fall solltest du neben diesem Reader noch weitere Informationen im Internet einholen, da die Diskussion um Sicherheitstechnologie eine sehr dynamische ist und vielleicht in einem Jahr gravierende Sicherheitslücken bei einem Dienst entdeckt werden, der heute noch als absolut vertrauenswürdig gilt. Die bekanntesten Alternativen zu WhatsApp sind Threema, Telegram, Surespot und Chatsecure. Als Kriterien haben wir die Praxistauglichkeit des jeweiligen Messengers, den genutzten Verschlüsselungsstandard und die Frage, ob es sich um quelloffene Software (Open Source) handelt, angelegt.

Threema:

Bei Threema handelt es sich um die App eines Schweizer-Unternehmens, die im Frühjahr 2014 nach der Übernahme von WhatsApp durch Facebook großen Zulauf hatte und zeitweise zu den beliebtesten Downloads im itunes-Store zählte. Die App gibt es sowohl für iOS als auch für Android und Windowsphone. Threema erkennt Kontakte anhand der verwendeten Handy-Nummer und erstellt darüber hinaus eine Threema-ID mit der Kontakte gesucht werden können. Threema nutzt ein Authentifizierungsverfahren, bei dem Nutzer*innen, wenn sie sich persönlich begegnen, ihre jeweiligen Barcodes scannen können und so die Echtheit des virtuellen Gegenübers verifizieren. Threema kostet für Android 1,60€ und für iOS 1,79€. Threema verspricht den Nutzer*innen eine sichere Ende-zu-Ende-Verschlüsse-

lung, deren technische Grundlagen auch offen gelegt wurden. Der restliche Teil von Threemas Quellcode wurde jedoch nicht offen gelegt, sodass niemand überprüfen kann, wie die Datenverarbeitung genau auf Threemas Servern erfolgt. Nach allem, was bisher bekannt ist, gilt Threema jedoch als relativ sicher.

Telegram:

Hinter der App Telegram steht der Beitreiber des größten Sozialen Netzwerks in Russland VK. Telegram sieht im Layout Whatsapp sehr ähnlich, ist kostenfrei und steht für Android und iOS zur Verfügung. In der App kann aktiviert werden, dass Chats verschlüsselt werden sollen, was an einem Schloss-Symbol zu erkennen ist. Allerdings war die Qualität dieser Verschlüsselung lange Zeit umstritten – erst im Februar 2015 erhielt Telegram jedoch im Check der Electronic Frontier Foundation die volle Punktzahl für seine Verschlüsselung. Der Quellcode der App ist bekannt, die dahinter stehende Server-Struktur jedoch nicht. Telegram erkennt andere Kontakte anhand ihrer Telefonnummer und importiert dabei automatisch alle Kontakte aus dem Adressbuch, was u.a. von der Stiftung Warentest ziemlich heftig kritisiert wurde. Insgesamt konnte die App zwar nach ihrer Veröffentlichung einige Schwachstellen ausbessern, es bleiben aber weiterhin offene Fragen.

Surespot:

Die App Surespot gibt es kostenlos für Android und iOS. Der Quellcode ist offen gelegt und zeichnet sich durch einen hohen Verschlüsselungsstandard aus. Für Surespot muss sich allerdings jede*r Nutzer*in einen neuen Nickname erstellen, was die Hemmschwelle für die Nutzung am Anfang sehr hoch legt und das Finden von Freund*innen erschwert. Unter Datenschutzgesichtspunkten ist diese App sehr zu empfehlen, in der Praxis mangelt es jedoch an der schweren Auffindbarkeit anderer Kommunikationspartner*innen.

Chatsecure:

Chatsecure ist eine App des Guardian Project, die auf quelloffener Software basiert und allgemein als sicher gilt. Chatsecure basiert auf dem XMPP-Protokoll, dass sich auch mit anderen Chat-Clients nutzen lässt. Mit dem sogenannten OTR-Protokoll kann Chatsecure in Verbindung mit TOR (s. Anonymes

Surfen) genutzt werden, sodass beim Chatten auch die IP-Adresse verschleiert wird. Für Chatsecure muss ebenfalls ein neuer Benutzer*innenname erstellt werden. Der große Vorteil am XMPP-Protokoll ist, ist dass sich dieses auch auf dem heimischen PC mit dem Jabber-Client Pidgin verwenden lässt. Chatsecure/Jabber ist eine von vielen Sicherheitsexpert*innen empfohlene Lösung, birgt allerdings auch den Nachteil, dass alle Kontakte sich die entsprechende Software installieren müssen. Chatsecure und Jabber werden von vielen Sicherheitsexperten, unter anderem dem Journalisten Glenn Greenwald und Edward Snowden verwendet. Die Bedienung der App ist für ungeübte User jedoch manchmal eine Herausforderung.

Und was ist mit der Verschlüsselung bei WhatsApp?

WhatsApp hat nach einiger Kritik angefangen, den Sicherheitsstandard seiner Chats zu erhöhen. Allerdings ist die Ankündigung, zumindest die Chats zwischen Android-Nutzer*innen mit einer Ende-zu-Ende-Verschlüsselung zu versehen, immer noch nicht umgesetzt. Gruppenchats und Nachrichten zwischen Android- und iOS-Nutzer*innen waren sowieso von Beginn an ausgeklammert. Das große Problem bei WhatsApp ist, dass die Nutzer*innen keinerlei Wissen und noch weniger Kontrolle darüber haben, wie ihre Chatsoftware arbeitet.

Wer dies nicht mehr mitmachen will, aber gleichzeitig nicht auf WhatsApp verzichten kann, sollte zumindest zusätzlich eine der oben genannten Alternativen installieren, um mit anderen datenschutzbewussten Kommunikationspartner*innen über eine sichere App die Verbindung zu halten. Nur wenn viele Personen alternative Angebote verwenden, haben diese auch eine Chance sich zu etablieren.

9.

GPS Im Handy

In jedem Smartphone ist ein GPS-Empfänger verbaut. Er empfängt Radiosignale von Satelliten und kann so bestimmen, wo man sich befindet. Apps können darauf zugreifen. Einen praktischen Nutzen hat das bei Navigationsdiensten: Sie laden das entsprechende Kartenmaterial aus dem Internet herunter und weisen so den Weg zum Ziel.

Daneben gibt es aber auch Apps, die ganz nebenbei darauf zugreifen, ohne dass man als Anwender*in davon profitiert. So zum Beispiel die Facebook-App: Sie läuft oft im Hintergrund und übermittelt dem Unternehmen ständig den Standort. Dort wird er gespeichert und ermöglicht eine noch umfassendere Analyse des Nutzers zur zielgerichteten Werbung. Unter anderem können so Anzeigen von Werbekund*innen in der Umgebung geschaltet werden.

Fallen Standortdaten über einen längeren Zeitraum an, lässt sich daraus ein Bewegungsprofil erstellen, das viel über den Menschen verrät. Neben dem Wohnort und Freizeitgewohnheiten kann das auch etwas über die sozialen Kontakte sein.

Besser also, die Daten werden gar nicht erst erfasst. Den GPS-Empfänger kann man in den Einstellungen ausschalten, wenn er nicht benötigt wird. Das spart zudem Akkulaufzeit. Alternativ kann man auch den Zugriff auf den GPS-Standort für einzelne Apps sperren.

V.

Rechtliche Aspekte

1.

Vorratsdaten-speicherung

Wenn man elektronische Infrastruktur nutzt, fallen Daten an. Beim Telefonieren und im Internet sind das die sogenannten Verkehrs- oder Metadaten, also zum Beispiel wer wen angerufen hat, wo sich jemand dabei befand oder welche Internetseite aufgerufen wurde. Die Vorratsdatenspeicherung wendet sich an die Internetanbieter, die diese Kommunikation organisieren. Sie sollen dazu verpflichtet werden, alles festzuhalten und den Behörden zur Verfügung zu stellen. Mit den Daten sollen Straftaten einfacher verhütet und besser verfolgt werden können und den Nachrichtendiensten die Arbeit erleichtert werden.

Jedoch ist die Vorratsdatenspeicherung nicht unproblematisch. Behörden könnten die Daten missbrauchen. In der klassischen Polizeiarbeit müssen mehr finanzielle Mittel und Personal aufgewendet werden, je mehr Menschen betroffen sind. Schon allein dadurch besteht ein Anreiz, „nicht über die Stränge zu schlagen“. Anders ist es jedoch, wenn im „Datenschatz“ ermittelt wird: Ein einzelner Beamter kann in den Angelegenheiten von tausenden Menschen herumstöbern, unterstützt durch Computerprogramme und mit geringem Arbeitsaufwand. Eine Polizistin, die in die Wohnung eines Verdächtigen eindringt, um dort eine Abhöranlage zu installieren oder Unterlagen zu durchsuchen, muss dafür eine persönliche Hemmschwelle überwinden. Auch diese Hemmschwelle beugt einem Überschreiten der Befugnisse vor; ist aber beim komfortablen Zugriff auf die Vorratsdaten des Verdächtigen vom Amts-PC aus kaum noch vorhanden. Die digitale Durchsuchung wird nicht einmal vom Betroffenen bemerkt. Wer schon nicht erfährt, dass ein Zugriff stattfand, dem ist es unmöglich, einen eventuellen Missbrauch geltend zu machen. Dadurch dass die Polizeiarbeit unsichtbar wird, kann sie viel eher außer Kontrolle geraten.

Auch Kriminelle können sich unerlaubt Zugang zu dem „Datenschatz“ verschaffen, der bei den Internetanbietern lagert. Datenklau im großen Stil passiert häufig und Vorkehrungen dagegen sind teuer. Würden die Internetanbieter Vor-

fälle öffentlich machen oder blieben auch sie aus geschäftlichem Interesse im Verborgenen?

Es besteht zudem das Risiko, dass die Vorratsdatenspeicherung ausgeweitet wird. Ist die Infrastruktur zur Überwachung erst einmal aufgebaut, werden in der Politik schnell Forderungen laut, sie auch für andere als die ursprünglich definierten Zwecke einzusetzen. Nicht auszuschließen also, dass die Analyse des persönlichen Umfelds dann nicht nur nach dem Raubüberfall droht, sondern auch für politischen Aktivismus oder Urheberrechtsverletzungen im Internet. Mit Sicherheit kommt es auch zu einer faktischen Ausweitung durch den technischen Fortschritt. Das Auto mit Internetverbindung, neue mobile Gadgets oder die vernetzte Wohnung produzieren immer mehr Metadaten, aus denen sich ein immer umfassenderes Persönlichkeitsprofil erstellen lässt.

Handeln und Kommunikation hinterlassen zunehmend digitale Spuren. Schon dass diese bei Werbe- und Internetfirmen vielleicht für die Ewigkeit gespeichert werden, kann ein gewisses Unbehagen auslösen. Eine neue Qualität erreicht es jedoch, wenn auch der Staat darauf zugreifen kann. Es besteht das Risiko, dass die Bürger*innen sich dadurch bewusst oder unbewusst im „vorauseilenden Gehorsam“ konformer verhalten, als sie das eigentlich tun würden. Der Austausch von kritischen Gedanken ist jedoch Grundlage unserer Demokratie und darf nicht durch einen Staat, der alles festhält und analysiert, gehemmt werden.

Somit müsste die Vorratsdatenspeicherung schon einen großen Nutzen haben, um noch verhältnismäßig zu sein. Eine Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht aus dem Jahr 2012 konnte jedoch keine Relevanz der Vorratsdatenspeicherung für die Aufklärungsquoten in der Strafverfolgung zwischen 2008 und 2009 feststellen. Menschen, die eine schwere Straftat, wie zum Beispiel einen Terroranschlag, planen, treffen auch im digitalen Raum Vorkehrungen um unentdeckt zu bleiben.

Auch das Bundesverfassungsgericht kam 2010 zu dem Schluss, dass die Vorratsdatenspeicherung tiefe Einblicke in das soziale Umfeld aller Bürger*innen ermöglicht, obwohl ihnen konkret nichts vorzuwerfen ist. Sie sei in ihrer damaligen Ausgestaltung nicht mit dem Grundgesetz vereinbar, da ein „dif-

fus bedrohliches Gefühl des Beobachtetseins“ die Menschen daran hindern könne, ihre Grundrechte wahrzunehmen. Ähnlich sah es 2014 der Europäische Gerichtshof.

Dennoch landet die Vorratsdatenspeicherung immer wieder auf der politischen Tagesordnung. Ob sie eine angemessene Reaktion eines freiheitlich-demokratischen Staates auf die abstrakte Bedrohung durch Terrorismus ist und nicht bloß politischer Aktionismus, bleibt mehr als zweifelhaft.

Quellen:
http://vds.brauchts.net/MPI_VDS_Studie.pdf
BVerfGE 125, 260 http://www.servat.unibe.ch/dfr/dfr_bvbd120.html

2.

EU-Datenschutzverordnung

Wenn ich eine eMail an einen der anderen beiden Autoren dieses Readers verschicke und wir uns alle in Münster aufhalten, wandert die eMail auf Grund der dezentralen Struktur des Internets durch die ganze Welt. Vor diesem Hintergrund ist klar, dass Datenschutzregeln auf nationaler Ebene nur begrenzt wirksam sind. Deshalb hat die EU schon im Jahre 1995 eine Richtlinie für den Datenschutz erlassen, die in den EU-Mitgliedstaaten Eingang in die nationalen Datenschutzgesetze gefunden hat. Seit dem Jahre 1995 hat sich jedoch viel geändert – die Google-Suche gibt es seit 1998, Facebook seit 2004 und mobile Endgeräte wie Smartphones und Tablets sind erst in den letzten fünf Jahren populär geworden. Deshalb gibt es aktuell die Bestrebungen, auf europäischer Ebene eine sogenannte Datenschutzgrundverordnung zu beschließen, die unmittelbar geltendes Recht in allen EU-Staaten wird.

Bei der Datenschutzverordnung geht es zunächst um Unternehmen sowie um die Rechtsansprüche, die wir gegenüber den datenspeichernden Unternehmen haben. Diese Regelungen gelten erst mal nicht für Sicherheitsbehörden, aber wie im Kapitel Datensparsamkeit dargelegt, hängen Möglichkeiten der Behörden und Datensammlungen der Unternehmen eng miteinander zusammen.

Die Datenschutzverordnung orientiert sich an verschiedenen Prinzipien. So soll z.B. die informierte Einwilligung der Nutzer*innen als Grundvoraussetzung für die wei-

tere Speicherung und Verarbeitung dienen. Unternehmen dürfen Daten erst nach einer Zustimmung verarbeiten und dürfen diese auch nur für mit der Zustimmung verbundene Leistungen verwenden – bei der Bestellung eines Buches zum Beispiel für das Zusenden des Buches oder der Rechnung. Vor allem Lobbyist*innen datenverarbeitender Unternehmen versuchen diesen Grundsatz zu schwächen, um die auch für andere „berechtigte Interessen“ der Unternehmen nutzbar zu machen. Außerdem sollen Nutzer*innen das Recht erhalten, von den Unternehmen eine verständliche Auskunft zu bekommen, wie die eigenen Daten verarbeitet werden und ob diese an Strafverfolgungsbehörden und Geheimdienste weitergegeben wurden. Eine solche Datenweitergabe soll nur auf Basis des europäischen Rechts, insbesondere auf sog. Rechtshilfeabkommen zulässig sein. Auch sollen Nutzungsbedingungen leichter verständlich werden, in dem standardisierte Symbole die langen komplizierten Texte ersetzen. Damit Unternehmen effektive Schutzmaßnahmen ergreifen, um die bei ihnen gespeicherten Daten wirksam zu schützen, sind in der Verordnung empfindliche Strafzahlungen bei Verstößen vorgesehen.

Um eine einheitliche Rechtsanwendung sicherzustellen, soll ein europäischer Datenschutzausschuss geschaffen werden, der sich aus allen nationalen Aufsichtsbehörden zusammensetzt und in Fällen von europaweiter Bedeutung bindende Entscheidungen trifft. So soll verhindert werden, dass einzelne Staaten eine möglichst schwache Rechtsanwendung als Standortfaktor nutzen, um internationale IT-Konzerne anzulocken.
Viele Einzelfragen sind noch in der Diskussion zwischen den verschiedenen Institutionen der EU. Aktuell ist geplant, die Datenschutzverordnung Ende 2015 zu beschließen, damit diese nach einer zweijährigen Übergangsphase, also im Januar 2018 in Kraft treten kann.

3.

Auskunfts-ansprüche

Welche Daten sind über mich gespeichert, wo kommen sie her, an wen werden sie weiter gegeben und warum wurden sie gespeichert? Laut Bundesdatenschutzgesetz müssen öffentliche Stellen (§ 19)

und Unternehmen (§ 34) Auskunft darüber erteilen. Es ist eine Ausprägung des Grundrechts auf informationelle Selbstbestimmung: Nur wer von seinen Daten weiß, kann sie anschließend berichtigen oder löschen lassen sowie die Rechtmäßigkeit ihrer Erhebung in Frage stellen.

Nicht nur unliebsame Werbeanrufer kann man so loswerden. Eine Anfrage bei der Schufa ermöglicht zum Beispiel Einblick in die Daten, mit denen Banken und Versicherungen die Kreditwürdigkeit beurteilen. Dazu genügt ein formloses Schreiben mit Hinweis auf die Auskunftspflicht. Wurden durch die Verarbeitung der Daten Persönlichkeitsrechte verletzt, kann man das bei der Datenschutzaufsichtsbehörde anzeigen.

Möchte man erfahren, ob man auf dem „Radar“ einer Behörde wie des Bundeskriminalamtes oder des Verfassungsschutzes aufgetaucht ist, genügt theoretisch auch ein solches Schreiben. Es gelten jedoch einige Ausnahmen von der Auskunftspflicht: Zum Beispiel informiert die Staatsanwaltschaft nach der Strafprozessordnung (§ 491) nicht über Ermittlungen in jüngster Vergangenheit. Ob und in welchem Maße dem oder der Auskunftssuchenden Steine in den Weg gelegt werden, hängt auch davon ab, wie gut der zuständige Landesbeauftragte für Datenschutz seine Arbeit macht.

Gegenüber Geheimdiensten besteht kein Anspruch auf Auskunft nach dem Bundesdatenschutzgesetz. Ein Auskunftsanspruch nach dem Bundesverfassungsschutzgesetz (§ 15) läuft praktisch ins Leere, da er den Geheimdiensten schon eine Verweigerung der Auskunft erlaubt, wenn dadurch Informanten gefährdet werden könnten oder Interesse an der Geheimhaltung besteht. Auch über die Herkunft der Daten und weitere Empfänger lässt sich nichts erfahren.

Insbesondere gegenüber privaten Unternehmen können die Auskunftsansprüche also helfen, einen Teil der „Herrschaft“ über die eigenen Daten wieder zu erlangen. Es kostet sie Arbeit, eine Anfrage zu beantworten. Werden die Unternehmen mit zahlreichen Anfragen konfrontiert, achten sie vielleicht in Zukunft ein bisschen genauer darauf, korrekt mit den Daten umzugehen.

VI.

Datenschutz an der Uni

1.

„Krank? Können Sie das beweisen?“

Qualifizierte Atteste und Anwesenheitslisten

Zentrale Datenschutzprinzipien sind die Zweckbindung der gesammelten Daten und die Datensparsamkeit, also dass lediglich die unbedingt nötigen Informationen gespeichert werden. Beide Prinzipien spielen auch in der Hochschulverwaltung eine Rolle. Grundsätzlich besteht an diesem Umstand ein beiderseitiges Interesse – die Studierenden wollen keine unnötigen Angaben machen müssen, während die Uni aus Kostengründen auch kein Interesse daran hat, zusätzliche Daten zu speichern und zu verarbeiten.

Es gibt jedoch Entwicklungen, bei denen sich Hochschulen nicht mehr an dieses Prinzip gebunden sehen. Besonders besorgniserregend ist dieses Verhalten bei ärztlichen Daten, die zum sensibelsten Bereich der Persönlichkeitsschutzes gehören. So gab es bereits an verschiedenen Hochschulen Bestrebungen, im Falle der Prüfungsunfähigkeit von Studierenden genaue Informationen über das Krankheitsbild zu erfahren, anstatt sich - wie auch im Berufsleben üblich – auf das ärztliche Attest zu verlassen. Einige Hochschulen verlangen dabei, dass dem zuständigen Prüfungsausschuss konkrete Symptome beschrieben werden, während andere Universitäten Informationen über „Art und Verlauf der Erkrankung“ vorgelegt bekommen wollen. Die TU Darmstadt ging sogar so weit, von den Studierenden zu verlangen, die zuständigen Ärzt*innen gänzlich von der Schweigepflicht zu entbinden.

Unabhängig von der Frage, weshalb Prüfungsausschüsse zur Deutung medizinischer Befunde befähigt sein sollten, wird mit derartigen Maßnahmen massiv in die informationelle Selbstbestimmung der Studierenden eingegriffen. Vor allem bei sozial nach wie vor stigmatisierten Krankheiten wie Depressionen kann es erhebliche Nachteile für die Studierenden haben, ihre gesundheitliche Situation gegenüber der Hochschule offen zu legen, die ja zugleich auch der zukünftige Arbeitsplatz sein kann. Darüber hinaus entscheidet der nicht fachkundige Prüfungsausschuss, dass eine

Klausur geschrieben werden muss, während Ärzt*innen dies für unmöglich halten. In jedem Fall wäre der sachlich angemessene und datenschutzkonforme Weg, sich auf die Bescheinigung des medizinischen Fachpersonals zu verlassen.

Ein anderer Bereich, in dem personenbezogene Daten unnötig erhoben werden, sind Anwesenheitslisten in Seminaren und Vorlesungen. Zunächst einmal ist problematisch, wenn Listen herum gegeben werden, auf denen für alle sichtbar die persönlichen Daten jeder*s Studierenden zu sehen ist. Dies erscheint auf den ersten Blick trivial. Allerdings sind Name, Studienfach und Semesterzahl, Matrikel-Nummer, ZIV-Kennung sowie Postanschrift die üblichen Authentifizierungskriterien der Hochschule, um festzustellen, ob eine Person auch wirklich diejenige ist, die sie vorgibt zu sein. Dass diese Daten Missbrauchspotential bieten, wenn sie mit bösen Absichten verwendet werden, liegt auf der Hand.

Zudem werden Anwesenheitspflichten in m §64 Abs. 2a des Hochschulgesetzes NRW für den ganz überwiegenden Teil der Lehrveranstaltungen abgeschafft. Dennoch gibt es weiterhin Dozent*innen, die Anwesenheitslisten führen, obwohl die Anwesenheit der Studierenden nicht verpflichtend ist. Natürlich ist den betreffenden Dozent*innen auch klar, dass sie niemanden zum Unterschreiben zwingen können. Dass die Anwesenheitsquote aber beispielsweise bei der Notenvergabe herangezogen wird, kann nicht ausgeschlossen werden – weshalb eine derartige Liste von Beginn an boykottiert werden sollte. Rechtswidrig erhobene Anwesenheitspflichten sind auch ein Thema, das den AStA seit Jahren beschäftigt. Mehr Infos dazu findet Ihr auf asta.ms.

2.

Datenschutzfragen bei der Vereinheitlichung unserer Uni-Karten

Datenschutz spielt in der Hochschulpolitik immer dann eine Rolle, wenn es um die Vielzahl an Karten geht, die wir mit uns herumtragen. Aktuell sind das der Studierendenausweis, der auch als Ausleihkarte für die Bibliotheken dient, die Mensakarte und das Semesterti-

cket. Eine Vereinheitlichung wird von vielen Studierenden und auch den hochschulpolitischen Listen gefordert, gestaltet sich allerdings schwierig, weil die Karten von unterschiedlichen Stellen ausgegeben werden (Universität, Studierendenwerk, Bahn).

Sollte es zu einer Vereinheitlichung kommen, darf das Datenschutzniveau dadurch nicht verringert werden. Insbesondere die Mensa-Karte und das Semesterticket weisen Datenschutzprobleme auf. In der Mensakarte befindet sich ein RFID-Chip, der das kontaktlose Bezahlen ermöglicht. Die Verschlüsselung der bestehenden Chips steht jedoch immer wieder in der Kritik, hoffnungslos veraltet zu sein. Da sich auf den Mensakarten nur relativ geringe Beträge befinden, wird dagegen seit Jahren nichts unternommen. Diesen Chip zum Speichern zusätzlicher personenbezogener Daten, beispielsweise von Namen oder Matrikelnummern, zu verwenden, ist deshalb keine gute Idee.

Das aktuell verwendete Semesterticket ist ein Papierzettel, der von den Zugbegleiter*innen lediglich einer Sichtkontrolle unterzogen wird. Somit kann keine Massenerfassung unserer Zugfahrten erfolgen. Seitens der Bahn gab es jedoch mehrfach den Versuch, andere Ticketvarianten einzuführen, die datenschutztechnisch zumindest fragwürdig erscheinen. So wurde versucht, den AStA zu einem eTicket mit RFID-Chip zu überreden. Sollte der Chip einmal nicht vom Kartenlesegerät erkannt werden, haben die betroffenen Studierenden halt Pech gehabt und müssen sich einen Fahrschein kaufen. Auch eignet sich diese Technik dazu, Bewegungsprofile über das Fahrverhalten einzelner Studierender zu erstellen.

Der Anfang 2015 unternommene Versuch, in Zusammenarbeit mit der Universitätsverwaltung über die Studierenden hinweg ein Semesterticket-2-Print (ähnlich wie online gebuchte Bahntickets) einzuführen, kann aus Datenschutzperspektive noch nicht abschließend bewertet werden. Hier muss sichergestellt werden, dass der vom Bahnpersonal gescannte QR-Code nur zur Verifizierung des Tickets verwendet, nicht aber abgespeichert oder statistisch ausgewertet wird. Darüber hinaus muss es möglich sein, das Semesterticket auch ohne QR-Code nutzen zu können.

Dabei bedeuten die Datenschutzbelange jedoch nicht, dass keine

Verbesserung bei unseren drei Karten möglich ist. Es wäre ein Leichtes, unseren Studierendenausweis auf Vorder- und Rückseite der Mensakarte zu drucken, ohne den Chip für weitere Daten verwenden zu müssen. Der Haken: Dazu müssten sich Universitätsverwaltung und Studierendenwerk auf eine einheitliche Karte einigen.

3.

Sciebo

Die Uni-Cloud

Heute schon in der Cloud gewesen? Cloud Computing bezeichnet das Benutzen von Speicherplatz auf fremden Servern, ein Service, der immer beliebter wird und im Web 2.0 inzwischen allgegenwärtig ist. Fotos auf Facebook hochzuladen bedeutet nichts anderes, als sie in die Cloud zu schicken. Kommerzielle Anbieter wie Apple, Amazon oder Dropbox stellen beliebigen Speicherplatz zur Verfügung und treffen damit einen Nerv. Denn wie schon Reinhard Mey wusste: „Über den Wolken muss die Freiheit wohl grenzenlos sein“ … zumindest die Freiheit für Datenkraken. Denn die Cloud zu benutzen heißt nichts anderes, als seine Daten undurchsichtigen Unternehmen außerhalb der Reichweite deutscher Datenschutzgesetze anzuvertrauen, mit komplizierten Datenschutzbestimmungen, die oftmals nicht richtig gelesen werden. So haben etwa Microsoft und Google bereits 2011 zugegeben, dass europäische Daten an US-Regierungsbehörden weitergegeben werden [1] – Datenschutz und „Safe Harbor“ hin oder her.

Einundzwanzig nordrhein-westfälische Universitäten unter Projektleitung der Universität Münster haben sich zu Sync & Share NRW zusammengeschlossen, um diesem Missstand „zu Zwecken von Studium, Lehre, Forschung oder Hochschulverwaltung“ Abhilfe zu schaffen. Im Februar 2015 wurde so der Cloud-Dienst Sciebo in Betrieb genommen [2]. Sciebo soll „Studierenden und Wissenschaftlern einen sicheren Umgang auch mit großen Datenmengen“ ermöglichen, so die Universität in einer Pressemitteilung [3]. Die Registrierung ist nur mit einer Uni-Kennung möglich. Teilnehmende erhalten jeweils 30 GB zur universitätsbezogen freien Verwendung. Daten würden hauptsächlich an den Universitäten Münster, Bonn und Duisburg-Essen

verarbeitet. „Insbesondere werden Daten nicht an Privatunternehmen weitergegeben, nicht durch diese verarbeitet und auch nicht außerhalb des Gebietes der Bundesrepublik Deutschland abgespeichert“ [4], bringen die AGB den Vorteil von Sciebo gegenüber Dropbox und Co auf den Punkt. Jedoch sollte beachtet werden, dass die Nutzung von Sciebo eben an die Hochschulzugehörigkeit gebunden ist. Nach Studienende (oder Kündigung) bleibt Nutzenden eine Übergangsfrist von sechs Monaten, um ihre Daten wieder anderweitig unterzubringen.

Beispielhaft ist die klare, auch für Laien einfach zu erschließende Datenschutzregelung von Sciebo. Das ist leider nicht überall der Fall. Die Datenschutzbestimmungen der Zentrums für Informationsverarbeitung (ZIV) etwa muss man sich aus dessen diversen Ordnungen zusammensuchen [5], was selbst für interessierte Studierende eine hohe Hemmschwelle sein dürfte. Zum Teil sind diese Ordnungen eingescannt und lassen sich damit leider nicht per Suchfunktion nach Begriffen durchstöbern. Dabei sollte doch gerade einer Universität daran gelegen sein, ihren Studierenden, auch denen ohne juristische oder technische Vorkenntnisse, eine kritische Auseinandersetzung mit den Rahmenbedingungen ihres Studiums zu ermöglichen!

[1] http://www.heise.de/newsticker/meldung/Auch-Google-uebermittelt-europaeische-Daten-an-US-Behoerden-1319347.html
[2] Zur Registrierung:
Serveradresse der WWU: https://uni-muenster.sciebo.de
Serveradresse der FH Münster: https://fh-muenster.sciebo.de
[3] http://www.uni-muenster.de/news/view.php?&cmdid=2602
[4] http://www.sciebo.de/agb/index.html
[5] http://www.uni-muenster.de/ZIV/DasZIV/Ordnungen/]

VII.

tl;dr

Tipps in Kürze

- offene Software nutzen
- gute Passwörter ausdenken, regelmäßig wechseln,
  evtl. einen Passwortmanager nutzen
- ixquicken und duckduckgoen statt googlen
- https zum Standard machen
- eMails verschlüsseln
- Updates installieren
- Standard-Privatsphäre-Settings überprüfen
- Tracker blockieren - mit Adblock Edge, Ghostery, NoScript ...
- offene Alternativen statt Monopole benutzen
- nicht das eigene Kaufverhalten für kleine Rabatte offen legen
- Nachfragen: Warum muss ich diese Daten angeben?
- GPS im Smartphone ausschalten,
  wenn es nicht gerade gebraucht wird.
- Überlege, welche Dienste du nutzt
  und ob es Alternativen dazu gibt.

Impressum

Redaktionsleitung:
Sebastian Illigens, Marius Kühne & Philip Steitz
(Projektstelle „Datenschutz-Reader“)

Schlussredaktion:
Marieke Reiffs
(Referat für Soziales und Bildung)

Layout, Satz, Bilder:
Johann Edelmann
(Projektstelle für Layout & Design)

Druck:
AStA Druckerei, Schlossplatz 1, 48149 Münster

Auflage: 150

Erscheinungsdatum: 02/2016

Alle Angaben beziehen sich auf den Stand vom Oktober 2015.


astalms