SVRV Sachverständigenrat für Verbraucherfragen

Technologien für und wider Digitale Souveränität

Rüdiger Weis, Stefan Lucks, Volker Grassmuck

Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen

Juni 2017

Berlin, Juni 2017
ISSN 2365-8436

Herausgeber:

Sachverständigenrat für Verbraucherfragen
beim Bundesministerium der Justiz und für Verbraucherschutz
Mohrenstraße 37
10117 Berlin

Telefon: +49 (0) 30 18 580-0
Fax: +49 (0) 30 18 580-9525
E-Mail: info@svr-verbraucherfragen.de
Internet: www.svr-verbraucherfragen.de

Diese Veröffentlichung ist im Internet abrufbar.

Mitglieder des SVRV

Prof. Dr. Lucia Reisch (Vorsitzende)
Professorin für Interkulturelle Konsumforschung und europäische Verbraucherpolitik an der Copenhagen Business School

Dr. Daniela Büchel (stellv. Vorsitzende)
Mitglied der Geschäftsleitung REWE für die Bereiche Human Resources und Nachhaltigkeit

Prof. Dr. Gerd Gigerenzer
Direktor der Abteilung „Adaptives Verhalten und Kognition“ und des Harding-Zentrums für Risikokompetenz am Max-Planck-Institut für Bildungsforschung in Berlin

Helga Zander-Hayat
Leiterin des Bereichs Markt und Recht bei der Verbraucherzentrale Nordrhein-Westfalen

Prof. Dr. Gesche Joost
Professorin für das Fachgebiet Designforschung an der Universität der Künste und Internetbotschafterin der Bundesregierung im Gremium der „Digital Champions“ der EU

Prof. Dr. Hans-Wolfgang Micklitz
Professor für Wirtschaftsrecht am Europäischen Hochschulinstitut in Florenz

Prof. Dr. Andreas Oehler
Professor für Finanzwirtschaft an der Universität Bamberg und Direktor der Forschungsstelle Verbraucherfinanzen und Verbraucherbildung

Prof. Dr. Kirsten Schlegel-Matthies
Professorin für Haushaltswissenschaft an der Universität Paderborn

Prof. Dr. Gert G. Wagner
Professor für Empirische Wirtschaftsforschung und Wirtschaftspolitik an der Technischen Universität Berlin, Vorstandsmitglied des Deutschen Instituts für Wirtschaftsforschung und Max Planck Fellow am MPI für Bildungsforschung

Mitarbeitende des SVRV

Leiter der Geschäftsstelle: Thomas Fischer

Wissenschaftlicher Stab der Geschäftsstelle: Dr. Irina Domurath, Dr. Christian Groß

Studie

Technologien für und wider Digitale Souveränität

Rüdiger Weis, Stefan Lucks, Volker Grassmuck

Berlin im November 2016

im Auftrag des

Sachverständigenrates für Verbraucherfragen

Bundesministerium der Justiz- und für Verbraucherschutz

Technologien für und wider Digitale Souveränität

Rüdiger Weis, Stefan Lucks, Volker Grassmuck

Berlin,im November2016

Zu dieser Studie

Die Digitalisierung und weltweite Verknüpfung der Kommunikationsnetze bilden den tiefsten Einschnitt in der Geschichte seit der industriellen Revolution. Das Zusammenleben der Menschen, das gesamte Wirtschaftsleben, das Verhältnis zwischen Bürger und Staat und das Verhältnis der Staaten untereinander sind dabei, sich grundlegend zu verändern.

Es stellt sich die Frage, mit welchen rechtlichen und technischen Schritten man, trotz der Bildung monopolartiger Strukturen, der real existierenden Massenüberwachungen – nach einer Entscheidung des Bundesverfassungsgerichtes zur Vorratsdatenspeicherung (Beschlüsse vom 8. Juni 2016 1 BVG 42/15 und 1 Bar 229/16) „kann die umfassende und anlasslose Bevorratung sensibler Daten über praktisch jedermann einen erheblichen Einschüchterungseffekt bewirken" – und der rasanten technologischen Entwicklung insbesondere im Bereiche der neuronalen Netze sicherstellen kann, dass fundamentale Menschenrechte, die Demokratie und die soziale Marktwirtschaft weiterhin gewährleistet werden.

Um die verschiedenen Problemlagen möglichst eng aus der Alltagserfahrungen von Verbraucherinnen und Verbrauchern heraus darzustellen, wurde der Ansatz zweier konträrer Zukunftsszenarien gewählt. Aus den Szenarien werden die einzelnen Dimensionen der digitalen Souveränität entwickelt.

Im Weiteren behandelt die vorliegende Studie technische Aspekte, die die digitale Souveränität fördern oder ihr entgegenstehen. Zu den Schwerpunktthemen gehören Scoring, das Internet der Dinge, die Problematik geschlossener Systeme und der Schutz von besonders gefährdeten Personengruppen. Es wird jeweils auf Lösungsansätze und gesetzgeberische Handlungsoptionen eingegangen. Außerdem verweist die Arbeit auf geeignete Instrumente einer datenschutzfreundlichen Kryptographie, zum Beispiel blinde Unterschriften, anonyme Attestate und die Methode der differentiellen Vertraulichkeit.

Inhalt

1. Ein Blick in die Zukunft

Das Buch "Your First Computer" von Rodnay Zaks erschien 1980 (deutsche Übersetzung "Mein erster Computer", 1981). Kapitel 1 schildert das Leben im "Zeitalter der Mikrocomputer" am Beispiel einer Familie: Jens, Linda und mehrere Kinder. Jens ist beruflich immer erreichbar. Noch vor dem Aufstehen checkt er seine elektronische Post und Einträge in seinem Groupware-Terminkalender. Linda isst an einem Architekturbüro beschäftigt. Sie arbeitet offenbar in Teilzeit und meistens zu Hause, am Computer. Für Jens und Linda ist es normal, Bankgeschäfte und Einkäufe online zu tätigen und sich beim Autofahren vom Navi den Weg zeigen zu lassen.

Zaks damals erstaunliche Zukunft ist heute unsere ganz normale Gegenwart. Aber wie werden Jens und Linda in wenigen Jahrzehnten leben? Besser gesagt, wie werden wir dann leben? Wir haben uns zwei verschiedene Zukunftsszenarien überlegt.

1.1. Zukunft A

Morgen

Es ist 6:30 Uhr morgens. Jens wird vom Weckgeräusch seines Smartphones wach. 'Warum weckt mich das dumme Ding so früh?' denkt Jens, doch dann sieht er die Nachricht seines Chefs im Display: "Verkaufsgespräch 9:00 Uhr! Vorher Besprechung!" Ganz leise steht Jens auf, um Linda nicht zu wecken, wäscht sich kurz, zieht sich an, macht sich schnell noch einen Kaffee und ein Toastbrot, und setzt sich ins Auto. Als Lindas Smartphone sie um 7:00 Uhr weckt, ist Jens schon unterwegs.

Weil das Auto die größte Strecke autonom fährt, hat Jens Zeit genug, seinen Toast hinunterzuwürgen, seinen Kaffee zu trinken, und E-Mails zu lesen. Eine Mail leitet er an Linda weiter.

Vormittag

Im Büro angekommen, bespricht Jens mit seinem Chef und einigen Kollegen die Verhandlungsstrategie. Es geht um einen wichtigen Kunden und einen sehr lukrativen Großauftrag. Die Besprechung dauert bis 8:10. Noch fast eine Stunde, bis der Kunde kommt! Jens ärgert sich, weil er heute morgen aus Zeitgründen nicht geduscht hat. Pünktlich um 9:00 Uhr kommt der Kunde. Sie verhandeln einige Stunden, bis der Vertrag endlich unterzeichnet werden kann.

Inzwischen haben auch Linda und die Kinder gefrühstückt, und die Kinder, Timo und Tina, sind zur Schule gegangen.

Linda checkt nun ihre E-Mails. Sie hat vier E-Mails erhalten. Eine Nachricht ist SPAM. Linda löscht die Nachricht. Die zweite Nachricht besteht aus Urlaubsgrüßen von Freunden, zusammen mit ein paar Urlaubsbildern. Die machen genau dort Urlaub, wo Lisa und ihre Familie letztes Jahr Urlaub gemacht haben. Linda freut sich und schickt den Freunden ein eigenes Urlaubsbild vom letzten Jahr.

Die dritte Nachricht ist die, die Jens an sie weitergeleitet hat. Jens wird von einem anonymen Absender aufgefordert, einen bestimmten Betrag in Bitcoins zu bezahlen. Bezahlt Jens nicht, schickt der Erpresser die Beweise an Linda. Allerdings weiß diese bereits Bescheid: Die angebliche Untreue von Jens besteht darin, dass er auf einer Messe war, und sich mit einem Kollegen ein Hotelzimmer geteilt hat, weil in der Nacht nur noch ein Zimmer frei war. Der einzige "Beweis" ist eine Kopie des Buchungsbelegs im Anhang der E-Mail, dem zufolge eben Jens und der Kollege gemeinsam ein Zimmer mit Doppelbett belegt haben. Lächerlich!

Linda ärgert sich. Nicht so sehr über Jens. Klar, die nervige Mail hätte er ihr gar nicht erst weiterzuleiten brauchen. Sie ärgert sich über das insgesamt immer häufigere Auftreten solcher Erpressermails. In der Zeitung stand in dem Zusammenhang etwas von der "neuen Nigeria-Connection", was immer damit gemeint ist. Jeder und jede bekommt irgendwann einmal derartige E-Mails. Zwar verlangen die Erpresser nie größere Beträge, und Linda hat noch nie von jemandem gehört, der tatsächlich bezahlt hat. Aber manchmal muss wohl jemand zahlen, sonst würde sich das Geschäft der Erpresser nicht lohnen. Und wie kommen die Erpresser eigentlich an den Buchungsbeleg aus dem Hotel?

Was Linda nicht weiß: Die meisten Mailservers beruhen auf der Auswertung von Fotos. Und besonders häufig werden Jugendliche erpresst, die beim "fremdknutschen" vor eine Kamera geraten. Gesichtserkennung, Abgleich mit dem "Beziehungsstatus" in sozialen Netzwerken und das Verschicken der Erpresser-Mail – alles geht automatisch. Wer den geforderten (und in der Regel eher kleinen) Betrag auch nach mehrfacher Aufforderung nicht bezahlt, muss damit rechnen, dass das Foto an den festen Freund oder die feste Freundin geschickt wird.

Die vierte Nachricht ist ein Schock für Linda! Sie stammt von der Schule, auf die Tina geht. Tina soll am Ende des Schuljahres die Schule verlassen! Letztes Jahr war Tinas Schul-Score noch bei 495, aber jetzt ist der Score nur noch 325. Schüler mit einem Score unter 335 müssen die Schule verlassen. Linda versteht die Welt nicht mehr. Ausgerechnet Tina! Tina hat gute Noten in der Schule – ganz anders als Timo, dessen Score sich immerhin von 380 im letzten Jahr auf 445 in diesem Jahr verbessert hat,

unter anderem, mit Hilfe einer Nachhilfe-App. Mit einigen Klicks vereinbart sie einen Gesprächstermin mit Tinas Klassenlehrer, Herrn Ärmel, am frühen Nachmittag. Allerdings muss sie dann heute Vormittag arbeiten – eigentlich hatte sie erst ihre Tante Jutta besuchen wollen, die im Krankenhaus liegt.

Wie meistens arbeitet Linda zu Hause. Sie lädt die Baupläne, an denen sie schon gestern gearbeitet hat, und ergänzt fehlende Details. Leider ist sie unkonzentriert: Die Sorge um Tinas Schullaufbahn lenkt sie ab. Immer wieder macht sie Pausen bei der Arbeit. Und sie macht Fehler, auf die der Computer sie hinweist. Nach vier Stunden loggt sie sich aus. Doch wegen der vielen kleinen Pausen, und der Fehler, die sie gemacht hat, rechnet der Computer ihr nur drei Stunden Arbeitszeit an. Linda isst schnell eine Kleinigkeit, dann steht der Termin mit Herrn Ärmel an.

Nachmittag

Auf ihrem Bildschirm sieht sie Herrn Ärmel und Tina. Tina hat rote Augen. Sie hat geweint. Der Lehrer kann sich Tinas schlechten Score überhaupt nicht erklären. Er selbst hält Tina für eine ausgesprochen gute Schülerin, und er ist sich sicher, dass sie einen guten Abschluss erzielen würde, wenn sie auf der Schule bleiben dürfte. Aber die Scores, die im Auftrag des Kultusministeriums berechnet werden, berücksichtigen nicht nur die Noten und die Leistungen in der Schule, sondern alle außerschulischen Daten, dies sie finden können: "Die Teilnahme an Sportveranstaltungen und wie gut man dabei abschneidet, die Gesundheitsdaten, die Kommunikation in sozialen Netzwerken, einfach alles. Irgendetwas löst beim Auswertungsalgorithmus rotes Licht aus. Keine Ahnung, was!" "Und nun? Meine Tochter kann doch nicht wegen irgendwelcher Zahlen, von denen keiner weiß, wie sie zustande kommen, von der Schule fliegen!" "Wenn es nach uns Lehrern ginge, dann nicht. Aber das Ergebnis von dem Auswertungsalgorithmus zählt, und unsere Erfahrung als Lehrer ist irrelevant. So steht es im Gesetz. Es tut mir wirklich leid!"

Herr Ärmel will das Gespräch schon beenden, als sich auf einmal die Schuldirektorin in die Konferenz mit einschaltet. Es gibt eine brandneue Verordnung des Kultusministeriums! Weil Tinas Score zwar unter 335 aber über 300 ist, gilt sie, dieser Verordnung zufolge, als Härtefall. Härtefalle dürfen ein Jahr an der Schule bleiben und bekommen noch eine letzte Chance, ihren Score zu verbessern. Bedingung ist allerdings die Nutzung einer zertifizierten Nachhilfe-App. Es gibt bisher genau eine zertifizierte Nachhilfe-App. Anders als die Open-Source Nachhilfe-App, mit der Tinas Bruder Timo zuletzt seine Noten und seinen Score verbessert hat, kostet die zertifizierte App allerdings Geld. Sie ist sogar ausgesprochen teuer! Aber sie ist die einzige Alternative

zum Verlassen der Schule, deshalb stimmt Linda dem Kauf der App zu. Die Familie wird sich in den nächsten Monaten einschränken müssen. Die Video-Konferenz endet.

Was weder Linda noch Tina noch Herr Ärmel noch die Direktorin wissen: Der Hersteller der zertifizierten App ist eine Tochterfirma der gleichen Firma, die im Auftrag des Kultusministeriums die Scores berechnet.

In der Zwischenzeit hat Jens frei. Wie am Vortag besprochen, holt er Timo mit dem Auto ab und bringt ihn zum Fußballtraining. Während er das Fußballtraining beobachtet, sieht er noch ein paar Unterlagen aus dem Büro durch. Dann will er einen Zeitungsartikel lesen, den er vorgestern auf seinem Smartphone abgespeichert hat. Es geht um Geschäftsbeziehungen, die der Ehemann einer Ministerin mit einer Big-Data Firma unterhalten soll. Doch als Jens die Datei mit dem Artikel zu öffnen versucht, erhält er nur eine Fehlermeldung: "Dieser Bericht enthielt Firmengeheimnisse der … Gemäß § … des Urheberrechts- und Geheimnisschutzgesetzbuchs in seiner Fassung vom … wurde die Datei gelöscht. Der Betrag von … Cent, den Sie für den Bericht bezahlt haben, wurde auf Ihr Konto mit der Nummer … zurücküberwiesen." Jens ärgert sich sehr! Auch wenn der Bericht wahrscheinlich maßlos übertrieben ist, hätte er ihn gerne gelesen.

Am Ende des Trainings fordert die Trainerin die Kinder auf, eine spezielle Fußball-App auf ihren Smartphones zu installieren. "Wenn das Training einmal ausfällt, wenn der Termin für ein Spiel sich verschiebt, oder wenn sonst irgendetwas Wichtiges passiert, erfahrt Ihr das über diese App. Die App ist kostenlos, und Ihr tut unserem Verein sogar etwas Gutes! Pro Installation spendet der Hersteller der App … Cent für uns. Allerdings müssen Eure Eltern dem Installieren der App zustimmen." Jens wundert sich nicht! Klar, wenn jemand etwas "kostenlos" anbietet, und dann sogar noch Geld "spendet", dann muss er Daten verhökern, um selbst Geld zu erwirtschaften. Und dem Verhökern dieser Daten muss, laut Gesetz, der Betroffene zustimmen - oder bei Minderjährigen ein Erziehungsberechtigter. Jens liest sich die Nutzungsbedingungen gar nicht erst durch und stimmt zu. Er will gar nicht wissen, welche Daten die App alle sammelt und weiterleitet. Ohne App wäre Timo von dem Informationsfluss in der Mannschaft abgeschnitten – dann könnte er die Fußballschuhe auch gleich an den Nagel hängen. Leise reimt Jens vor sich hin: "Datenschutz, hin und her, ohne App, geht nichts mehr!"

Inzwischen arbeitet Linda wieder. Sie ist etwas müde, aber sie schafft es, ihre Entwürfe ohne weitere Fehler fertigzustellen. Und ihr Computer rechnet ihr die bisher fehlende Stunde auch noch gut.

Abend

Der Rest der Familie trifft fast gleichzeitig ein. Jetzt soll es schnell Abendessen geben. Jens kocht Nudeln, macht ein paar Bockwürste heiß und stellt Tomatenketchup auf den Tisch. Das ist nicht gerade gesunde Ernährung, aber es schmeckt allen und geht schnell.

Nach dem Abendessen, als es langsam dunkel wird, zieht sich Linda eine Stirnlampe auf den Kopf, ein Fitness-Armband ans Handgelenk und zieht Jogging-Schuhe an. "Mama, warum willst Du denn jetzt noch joggen?" Linda erklärt ihren Kindern, dass ihre Krankenkasse jedes Jahr einen neuen Gesundheitsscore berechnet. Davon hängt ab, wie viel sie für die Krankenversicherung bezahlen muss. Und der Score hängt, unter anderem, von Krankheiten ab, an denen Blutsverwandten erkranken. "Und weil Tante Jutta jetzt so eine teure Behandlung bekommt, wird sich mein Score deutlich verschlechtern. Das kann ich wett machen, indem ich pro Woche mindestens drei Stunden Ausdauersport mache. Das Fitness-Armband meldet meine sportliche Tätigkeit an die Krankenkasse. So, und jetzt muss ich los!"

Jens und Timo gucken noch die Zusammenfassung von Fußballspielen, die heute stattgefunden haben. Tina arbeitet für ihr Gefängnisprojekt. Sie "betreut" zwei Gefängnisinsassen mit denen sie regelmäßig chattet und E-Mails austauscht. Zwei- oder dreimal hat ihr das Gefängnis auch schon eine Videokonferenz mit "ihren" Gefangenen erlaubt.

Als Linda nach etwas mehr als zwei Stunden zurückkommt, hat Jens die Kinder ins Bett gebracht, liegt selbst im Bett und schnarcht leise. Auch Timo und Tina schlafen tief und fest. Linda duscht sich und kuschelt sich an Jens. Es dauert lange, bis sie endlich einschläft.

1.2. Zukunft B

Morgen

Es ist 7:00 Uhr morgens. Die Smartphones von Jens und Linda spielen gleichzeitig ihre Weckmusik. Linda dreht sich noch einmal um, aber Jens steht sofort auf und kommt kurz danach mit zwei Tassen Kaffee zurück. Im Bett sitzend, besprechen er und Linda, was heute ansteht. "Wann habt Ihr heute das Verkaufsgespräch?" fragt Linda. "Gestern stand die Uhrzeit noch nicht fest - ich schaue nach, sobald ich kann. Und Du, Linda, hast Du irgend etwas Besonderes vor?" "Heute Vormittag will ich Tante Jutta im Krankenhaus besuchen." "Bestell ihr gute Besserung und viele Grüße von mir!" "Und denkst Du daran, Timo nachher zum Fußball zu bringen?" "Geht Klar!"

Dann folgt die morgendliche Routine: Duschen, Kinder wecken, gemeinsames Frühstück, die Kinder brechen auf zur Schule.

Vormittag

Punkt 8:00 ist Jens Smartphone freigeschaltet für berufliche Nachrichten. Jens liest auf dem Display: "Verkaufsgespräch schon um 9:00 Uhr! Rückruf so schnell wie möglich!" Jens sofort seinen Chef an. "Ich weiß, Sie sind immer kurz vor neun Uhr im Büro. Aber heute müssen wir uns noch über die Verhandlungsstrategie unterhalten. Können wir, während Sie unterwegs sind, an einer Konferenzschaltung teilnehmen?" "Kein Problem!" Jens steigt ins Auto, bestätigt die Ziel-Adresse (sein Büro, bzw. das benachbarte Parkhaus), und, da das Auto keinen menschlichen Fahrer mehr braucht, nutzt Jens sein Smartphone für eine Video-Konferenz mit seinem Chef und einigen Kollegen. In jeder Kurve wackelt sein Bild hin und her, aber die anderen Teilnehmer der Konferenz scheint das nicht zu stören. Einige von ihnen sind selbst unterwegs. Als Jens pünktlich die Firma erreicht, steht die Verhandlungsstrategie fest. Wenige Minuten später kommt der Kunde. Nach einer mehrstündigen Verhandlung wird der Vertrag endlich unterzeichnet.

Linda checkt inzwischen ihre E-Mails. Sie hat drei E-Mails erhalten. Eine Nachricht ist SPAM. Linda löscht die Nachricht. Die zweite Nachricht besteht aus Urlaubsgrüßen von Freunden, zusammen mit ein paar Urlaubsbildern. Die machen genau dort Urlaub, wo Lisa und ihre Familie letztes Jahr Urlaub gemacht haben. Linda freut sich und schickt den Freunden ein eigenes Urlaubsbild vom letzten Jahr.

Die dritte Nachricht stammt von der Schule. Tinas Lehrer, Herr Ärmel, bittet um ein Gespräch, möglichst noch heute. Sie ruft in der Schule an. Herr Ärmel hat gerade Unterricht, aber die Sekretärin ist informiert. Es geht um den Schul-Score von Tina. Der ist unerwartet niedrig. Linda ist sehr beunruhigt. Die Sekretärin weist Linda darauf hin, dass Herr Ärmel gleich eine Freistunde hat und bereit zum Gespräch ist. Linda überlegt, mit Herrn Ärmel eine Video-Konferenz abzuhalten – aber solche Sachen klärt sie lieber im persönlichen Gespräch, und die Zeit reicht noch. Sie ruft mit einer Taxi-App ein Taxi und lässt sich damit zur Schule bringen. Linda ist rechtzeitig vor Beginn der Hofpause in der Schule und wird von der Sekretärin zum Besprechungszimmer gebracht. Kurz danach kommen Tina, Herr Ärmel, und die Datenschutzbeauftragte, Frau Blau. Herr Ärmel erklärt, dass Tinas Schul-Score nach der neuesten Auswertung nur noch 325 beträgt. Linda ist schockiert: Was ist los mit Tina? Tina hat gute Noten in der Schule – ganz anders als Timo, dessen Score sich immerhin von 380 im letzten Jahr auf 445 in diesem Jahr verbessert hat, wohl auch, mit Hilfe einer Nachhilfe-App. "Muss Tina jetzt die Schule verlassen?" Herr Ärmel beruhigt sie. "Wo kämen wir denn hin, wenn wir

unsere Schüler wegen irgendwelcher Zahlen, von denen wir nicht so recht wissen, wie sie zustande kommen, von der Schule werfen? Wir nehmen die Scores zur Kenntnis. Manchmal sind die Scores eine frühe und sinnvolle Warnung vor möglichen Problemen, aber am Ende entscheiden wir Lehrer … und nicht irgend ein Computerprogramm."

Frau Blau erklärt, wie der Score berechnet wird. Es gehen alle Noten ein, aber auch externe Daten wie "die Teilnahme an Sportveranstaltungen und wie gut man dabei abschneidet, die Gesundheitsdaten, die Kommunikation in sozialen Netzwerken, und so weiter und so weiter." "Und welche Bedeutung hat der Score, wenn er nicht dazu genutzt wird, die Schüler von der Schule zu weisen?" Frau Blau erklärt "Ein niedriger Score bei guten Noten kann ganz belanglos sein, er kann aber, wie schon gesagt, auch eine frühe Warnung sein, sich um ein Problem zu kümmern, das sonst die Schullaufbahn gefährden könnte. Ich habe schon eine Vermutung, warum der Score Ihrer Tochter so niedrig ist. Aber aus Datenschutzgründen müssen Sie einer Detailauswertung zustimmen."

Linda nickt. Frau Blau tippt auf ihrer Tastatur, Linda bekommt auf ihr Smartphone eine Anfrage vom Server des Kultusministeriums, die sie mit "ja" beantwortet, und kurz darauf schauen sich die vier am Bildschirm eine lange Liste an. "Alles grün, ich scrolle herunter". Ein einziger Eintrag ist leuchtend rot und mit einem Ausrufezeichen versehen. "Nicht erschrecken" sagt Frau Blau, und liest vor: "Regelmäßiger Umgang mit Kriminellen!"

Natürlich erschrecken Linda und Tina doch, und wie! Die eine wird knallrot im Gesicht, die andere ganz blass. "Aber ich habe doch keine …" fängt Tina an. "Es ist wegen des Gefängnisprojektes" erklärt Frau Blau. "Du schreibst doch diesen Gefangenen, und Du hast sie sogar schon virtuell besucht, nicht wahr?" Tina nickt. "Nun, der Auswertungsalgorithmus sieht jeden Umgang mit Kriminellen als Hinweis auf ein mögliches Abrutschen in die Kriminalität an und stuft dann den Score entsprechend massiv herab. Bei Anderen mag das zutreffen, aber Eurer Gefängnisprojekt hat natürlich nichts damit zu tun, dass Ihr selbst kriminell werdet!

Im Rahmen des Gefängnisprojektes "betreut" Tina zwei Gefängnisinsassen, mit denen sie regelmäßig chattet und E-Mails austauscht. Zwei- oder dreimal hat das Gefängnis den Gefangenen auch schon eine Videokonferenz mit Tina erlaubt.

Die Pause ist längst vorbei, und Tina kommt zu spät zum Musikunterricht. "Kein Problem, die Kollegin weiß Bescheid" erklärt Herr Ärmel. Trotzdem beeilt sich Tina, schnell zum Musikraum zu kommen … jedenfalls, solange sie noch in Sichtweite ihres Klassenlehrers ist. Linda verabschiedet sich von Herrn Ärmel und Frau Blau. "Vielen vielen Dank, mir ist ein Mühlstein vom Herzen gefallen!"

Nachmittag

Am Kiosk vor der Schule besorgt Linda sich eine Kleinigkeit zu Essen. Dann bestellt sie sich ein Taxi ins Krankenhaus, um ihre Tante Jutta zu besuchen. Die hatte eine schwere Operation. Sie liegt schon eine ganze Weile im Krankenhaus. Inzwischen geht es ihr wieder besser, und sie langweilt sich sehr. Umso mehr freut sie sich über den Besuch von Linda. Zum Glück soll Jutta bald aus dem Krankenhaus entlassen werden.

Weil die Erkrankung von Jutta selten und wenig erforscht ist, und weil die Krankheit erblich bedingt sein kann, hat Linda zugestimmt, sich untersuchen zu lassen. Ihre Daten werden anonymisiert in einer statistischen Datenbank gespeichert. Die Datenbank kann nur für die statistische Auswertung der Daten genutzt werden, wie sie für die medizinische Forschung gebraucht wird. Selbst wer den vollständigen Inhalt der Datenbank kennt, kann keine direkten Rückschlüsse auf Linda und ihren Gesundheitszustand mehr ziehen.

Schließlich bestellt sich Linda wieder ein Taxi und fährt nach Hause. Sie lädt die Baupläne, an denen sie schon gestern gearbeitet hat, und ergänzt fehlende Details. Weil es Jutta wieder gut geht, und weil das Problem mit Tinas Score sich in Luft ausgelöst hat, geht Linda die Arbeit extrem gut von der Hand, und schon nach drei Stunden ist ihr Entwurf fertig. Weil sie noch etwas Zeit hat, bereitet sie eine Minestrone zum Abendessen vor und geht dann eine Runde Joggen.

In der Zwischenzeit hat Jens frei. Wie besprochen, holt er Timo mit dem Auto ab und bringt ihn zum Fußballtraining. Während er das Fußballtraining beobachtet, blättert er ein paar Unterlagen aus dem Büro durch, und liest einen Zeitungsartikel, den er vorgestern auf seinem Smartphone abgespeichert hat. Es geht um Geschäftsbeziehungen, die der Ehemann einer Ministerin mit einer Big-Data Firma unterhalten soll. 'Eine Sauerei – die Partei von dieser Ministerin werde ich bei der nächsten Wahl nicht wieder wählen' denkt Jens bei sich.

Am Ende des Trainings fordert die Trainerin die Kinder auf, eine spezielle Fußball-App auf ihren Smartphones zu installieren. Bei der Installation hat man die Wahl zwischen einer kostenlosen und einer Bezahl-Variante. "Ihr wisst, dass die kostenlose Variante dann Eure Daten verhökert" erklärt die Trainerin. "Dem müssen Eure Erziehungsberechtigten zustimmen." Jens stimmt nicht zu, zumal die Bezahl-Variante nicht teuer ist. Weil Timo noch kein online-Konto hat, bezahlt Jens für ihn. "Das sind nur … Cent pro Woche, die ziehe ich Dir vom Taschengeld ab" kündigt Jens an. "Na gut!" antwortet Timo. Er hat genug Taschengeld. Außerdem weiß Timo aus Erfahrung, dass die Chancen gut stehen, dass sein Vater das schon nächste Woche vergessen haben wird.

Abend

Als Jens und Timo nach Hause kommen, ist Tina auch gerade angekommen, aber Linda ist noch joggen. "Die kommt gleich", sagt Jens und kocht die von Linda vorbereitete Minestrone. Timo hilft seinem Vater und reibt den Parmesan für die Minestrone. Tina schreibt "ihren" beiden Gefangenen jeweils eine E-Mail. Als Lisa kommt, geht sie schnell duschen, dann isst die Familie gemeinsam zu Abend.

Später gucken Jens und Timo noch die Zusammenfassung von Fußballspielen, die heute stattgefunden haben.

Währenddessen fragt Linda ihre Tochter, ob sie versteht, wie der Schul-Score berechnet wird. "Nun ja, wir lernen im Digitalunterricht, wie man Daten sammelt und auswertet. Bei der Auswertung sucht man nach statistischen Zusammenhänge zwischen bestimmten Datenwerten und zukünftigen Verhaltensmustern." "Und wie macht man das genau?" "Zum Beispiel mit neuronalen Netzen, oder einfach mit Bayes'sche Schätzern." "Mit was, bitte?" Noch eine Weile erklärt Tina ihrer Mutter, wie das funktioniert, was man vor zehn oder zwanzig Jahren "Big Data" genannt hatte. "Aber woher weiß der Computer, der deinen Score berechnet, eigentlich, dass du Kontakt zu Gefängnisinsassen hast?" "Ein paar Jahre vor meiner Geburt hat man in unserem Land die Vorratsdatenspeicherung eingeführt. Vielleicht erinnerst du dich?" "Ja, es ging damals darum, Terroristen zu fangen. Ich weiß nicht, ob das sehr hilfreich war." "Jedenfalls, weil man die Daten schon einmal auf Vorrat hat, kamen die Leute nach ein paar Jahren auf die Idee, sie noch für andere Dinge einzusetzen, die irgendwie 'wichtig' oder 'gesellschaftlich sinnvoll' waren. Zuerst kam das Suizidverhinderungsprogramm." "Ah, ja, ich erinnere mich daran. Durch die Analyse der Daten konnte man feststellen, ob jemand selbstmordgefährdet war. Dem hat man dann irgendwie geholfen." "Genau. Danach kamen weitere derartige Programme. Und seit kurzem regelt das Gesetz eben auch die Nutzung der Vorratsdaten für den Schul-Score."

Noch etwas später bringen Jens und Linda ihre Kinder ins Bett, trinken zusammen noch ein Glas Wein, und gehen dann selbst ins Bett.

In Zukunft A genießen Jens, Linda und ihre Kinder deutlich weniger digitale Souveränität, als Zukunft B. Dabei ist Zukunft A nicht die schlechteste denkbare Zukunft - mit den technischen Möglichkeiten, die Google, Facebook und Co heute haben, könnte man den Überwachungsstaat, den sich George Orwell einmal ausgedacht habe, wie eine Anfängerübung aussehen lassen. Umgekehrt ist auch Zukunft B keineswegs ideal! So ist die Vorratsdatenspeicherung eine gravierende Einschränkung der digitalen Souveränität. Wenn Daten einmal gespeichert werden, entsteht

gesellschaftlicher und politischer Druck, sie auch für gerade wichtig erscheinende Dinge einzusetzen, derentwegen man die Daten ursprünglich nicht gespeichert hatte. Vielleicht ist es wünschenswert, im Vorfeld bereits erkennen zu können, wenn Jugendliche dabei sind, in eine kriminelle Szene abzudriften. Die Folge in Zukunft B ist, dass Jugendliche, die, wie Tina, einfach nur Kontakt zu Gefängnisinsassen haben, diskriminiert werden. Immerhin hat Tina selbst Glück, denn ihre Lehrer sind gut informiert und verständnisvoll. Ebenfalls nicht ideal in Zukunft B ist, dass man im Fußballverein aus Bequemlichkeit den Sportlern eine App aufnötigt, die irgendwie bezahlt werden muss, mit Daten, oder mit Geld. Das mag besser sein, als in Zukunft A, wo man nur mit Daten bezahlen kann. Doch eigentlich sollte ein Sportverein in Lage sein, einen derartigen Service für seine Mitglieder tatsächlich kostenlos anzubieten.

2. Digitale Souveränität

Der Begriff der “Digitalen Souveränität” wird in den letzten Jahren immer häufiger verwendet. Den Eindruck, Europa sei zunehmend nur noch Konsumenten von Hardware aus Asien und Software und Internetdiensten aus den USA, gab es schon länger. Umlaufgeltung erlangte der Begriff spätestens 2013, ausgelöst durch die Snowden-Enthüllungen über die umfassenden Abhöraktivitäten der NSA. In diesem Sinne fand er Eingang in den Koalitionsvertrag von CDU, CSU und SPD vom 27.11.2013. Dort heißt es:

> „Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings. … Zur Wahrung der technologischen Souveränität fördern wir den Einsatz national entwickelter IT-Sicherheitstechnologien bei den Bürgerinnen und Bürgern.“ (Koalitionsvertrag 2013: 147 f.)

Kurz darauf verwendete Infrastrukturminister Dobrindt den Begriff in einem Interview mit der Bild am Sonntag. Die Frage lautete nach der Sicherheit der digitalen Infrastruktur angesichts des NSA-Spähskandals. Dobrindts Antwort: „Wir müssen wieder Vertraulichkeit im Netz garantieren können und als Deutsche und Europäer unsere digitale Souveränität zurückgewinnen. Dafür werden wir viel Geld ausgeben müssen.“ (BamS 22.12.2013) Hier meint der Begriff also die nationale und europäische Souveränität im Sinne von Sicherheit, Unabhängigkeit und Wettbewerbsfähigkeit, insbesondere, was die kritischen Infrastrukturen betrifft, deren Kontrolle den deutschen Behörden zunehmend entgleitet (Schulzki-Haddouti, 21.08.2015).

Auch das Wirtschaftsministerium registriert in einer weiteren TNS Infratest-Erhebung unter deutschen Unternehmen das wachsende Gefühl der technische Abhängigkeit von US-amerikanischen Anbietern wie Google. “Die digitale Souveränität der deutschen Wirtschaft gilt als bedroht.“ (BMWi 2015: 127) Statt eines Verbrauchers, der die Souveränität über seine Daten zunehmend auslagert, wird hier der mündige Bürger gefordert, „der informiert und bewusst festlegt, wie mit seinen Daten verfahren wird.“ Mit individueller Bildung allein wird es nicht gehen, daher müssten „die Unternehmen offenlegen, was mit den Daten ihrer Verbraucher geschieht.“ (ebd.: 132)

Die ebenfalls 2013 erschienene Untersuchung Zukunftspfade Digitales Deutschland 2020 des TNS Infratest für den IT-Planungsrat beim Bundesministerium des Innern nimmt eine stärker individuelle Perspektive ein. Die Bedeutung von Digitaler Souveränität sehen die Experten fast gleichauf mit der von Sicherheit/Datenschutz und Infrastruktur (Breitband). Die zentrale Aussage: „Der souveräne Einsatz von Informations- und Kommunikationstechnik (IKT) ist eine wesentliche Voraussetzung für den mündigen digital-souveränen Bürger.“ (BMI 2013: 34) Digitale Souveränität wird hier als Bildung von Medienkompetenz aller Bürgerinnen und Bürger verstanden. Der Staat müsse Digitale Souveränität als Kernkompetenz in die Lehrpläne der Schulen aufnehmen. Auch Unternehmen müssten ihr Mitarbeitern systematisch in Digitaler Souveränität schulen (ebd.: 10). Zudem sieht die Studie eine hohe Notwendigkeit wissenschaftlicher Politikberatung, „damit digital souveräne Politiker in der Lage sind, Digitalisierungspolitik jeweils auf Höhe der Zeit bewerten und gestalten zu können.“ (ebd.: 11). Vor allem betont die Studie aber ohne Unterlass: „Nahezu alle befragten Experten vertreten die Ansicht, dass jeder Bürger für den Aufbau seiner digitalen Souveränität selbst verantwortlich ist.“ (ebd.: 35)

Der Bundesverband Informationswirtschaft Bitkom merkt zurecht an, dass der Begriff „Digitale Souveränität“ bislang weder definiert noch inhaltlich differenziert sei (Bitkom 2015: 3). Natürlich nur, um eine eigene Definition vorzuschlagen. Die richtet sich vor allem auf die wirtschaftliche Leistungsfähigkeit von Deutschland und der EU im Wettbewerb mit den USA und China. Diese können selbstbestimmt handeln und entscheiden nur, wenn sie bei digitalen Schlüsseltechnologien und Diensten und Plattformen über eigene Fähigkeiten auf internationalem Spitzenniveau verfügen (ebd.: 9).

Eine neue Wende brachte das Papier Leitplanken Digitaler Souveränität, das das BMWi zum 9. IT-Gipfel im November 2015 vorlegte. Es spielt eine wirtschaftlich verstandene Souveränität gegen den Datenschutz aus. „Bisherige Grundprinzipien des Datenschutzes wie Datensparsamkeit und Zweckbindung müssen überprüft und durch Prinzipien der Datenvielfalt und des Datenreichtums ergänzt und ersetzt werden.“ (BMWi 2015a: 5)

Der Begriff „digitale Souveränität“ ist wissenschaftlich undefiniert und als politischer changiert er zwischen einem nationalen Sicherheits- und Wirtschaftskonzept und einer erweiterten Medienkompetenz, die sich anzueignen weitgehend in der Verantwortung der Bürger liegt und die in der Zeit des Datenreichtums den Datenschutz ersetzen soll.

In dieser Begriffsverwirrung haben die Autoren dieser Studie keine Quellen gefunden, die überzeugend auflisten, welche rechtlichen oder gesellschaftlichen Gegebenheiten aus Verbrauchersicht erfüllt sein müssen, damit die Mitglieder einer Gesellschaft als “digital souverän” gelten können. Daher haben die Autoren die beiden

Zukunftsszenarien zum Ausgangspunkt genommen, um eine Liste der ihrer Ansicht nach wesentlichen Aspekte der Digitalen Souveränität zusammenzustellen.

2.1. Entscheidungsfreiheit und Selbstbestimmung

In Zukunft A haben die Lehrer nicht die Entscheidungsfreiheit darüber, einen Schüler oder eine Schülerin mit guten Noten aber schlechtem Score an der Schule zu lassen. Sogar Tina, die tatsächlich eine gute Schülerin ist, darf nur wegen einer Härtefallregelung an der Schule bleiben – und weil ihre Eltern bereit und in der Lage sind eine teure zertifizierte Nachhilfe-App zu bezahlen.

Bei der Fußball-App zeigt sich ebenfalls die Entscheidungsfreiheit – oder ihr Fehlen. Ohne die App wäre Timo bald vom Geschehen im Fußballverein ausgeschlossen. In Zukunft A hat Jens deshalb eigentlich keine andere Wahl, als dem Installieren der App zuzustimmen, mit dem entsprechenden Verlust an Vertraulichkeit. In Zukunft B hat er zumindest die Freiheit, statt mit seinen Daten mit einem überschaubaren Geldbetrag zu bezahlen, und damit mehr digitale Souveränität. Trotzdem ist der faktische Zwang, ein Smartphone besitzen und die App installieren zu müssen, auch in Zukunft B eine Einschränkung der digitalen Souveränität.

Eng mit der Entscheidungsfreiheit verknüpft ist die Transparenz (siehe unten). Rationale Entscheidungen brauchen Information als Entscheidungsgrundlage. Entscheidungsträger, die keine Ahnung haben, wie der Score einer Person zustande kommt, haben eigentlich nur die Wahl zwischen zwei Übeln: Den Score ignorieren, oder die eigene Entscheidung dem Score unterwerfen. Nur wer, wie die Lehrer in Zukunft B, nachvollziehen kann, wie ein Ergebnis zustande kommt, kann tatsächlich rational entscheiden.

In Zukunft A wird Jens um 6:30 von seinem Chef geweckt und ins Büro beordert. In Zukunft B ist das Smartphone von Jens bis 8:00 Uhr für dienstliche Nachrichten gesperrt.

Die Freiheit, nicht immer erreichbar sein zu müssen – ohne seinen Arbeitsplatz zu gefährden - ist auch ein Aspekt digitaler Souveränität.

2.2. Gleichbehandlung

Gleichbehandlung bedeutet, dass man für seine Entscheidungen, Einstellungen und Wesensmerkmale keine willkürlichen Vor- oder Nachteile haben darf. Das kann Menschen mit einer bestimmten sexuellen Orientierung betreffen, Angehörige von bestimmten Religionen, Personen, die bestimmte Berufe ausüben oder bestimmte politische Ansichten vertreten etc. Diese Problematik ist natürlich nicht neu, man denke

an die Situation von Juden, Schwulen, überzeugten Christen, Kommunisten oder sogenannten "Zigeunern" im Nationalsozialismus.

In einer digitalen Zukunft werden die Verbraucher aber so viele Daten von sich preisgeben, dass es extrem leicht fallen wird, Gruppen ungleich zu behandeln. Ein – im Vergleich zur NS-Zeit natürlich harmloses – Beispiel in Zukunft A ist der Schulausschluss von Tina, der beinahe stattgefunden hätte, und der Zwang, ein teures Nachhilfeprogramm zu verwenden, der dann stattdessen ausgeübt wird. Der Grund ist der schlechte Schul-Score, und den Grund für den schlechten Schul-Score erfährt in Zukunft A niemand. Die Benachteiligung von Tina ergibt sich aus einer eigentlich guten Absicht und einem naiven Vertrauen in einen ebenso naiven Algorithmus, nicht aus der Absicht, eine bestimmte Gruppe zu diskriminieren. Mit ähnlichen Mechanismen kann man jedoch auch die Diskriminierung von Gruppen ermöglichen.

Vor allem wird es in der digitalen Zukunft grundsätzlich einfacher, Personen und Gruppen zu diskriminieren, ohne dass diese überhaupt merken, dass sie diskriminiert werden. Um das zu verhindern, braucht man **Transparenz** (siehe unten). Ohne Transparenz wird es für die Betroffenen dann schwierig, wenn nicht unmöglich, sich gegen eine Diskriminierung zu wehren – selbst dann, wenn die Betroffenen in einem Rechtsstaat leben und das Recht hätten, sich gegen die Diskriminierung zu wehren.

2.3. Vertraulichkeit

In Zukunft A sind digitale Erpressungen an der Tagesordnung. Besonders häufig und manchmal erfolgreich sind Erpressungen mit öffentlichem Bildmaterial – sehr einfach und effektiv dank einer vollautomatischen Gesichtserkennung. In Zukunft B sind derartige Erpressungsversuche deutlich seltener, weil die Erpresser nicht so leicht an das Datenmaterial herankommen.

Vertraulichkeit bedeutet, dass man selbst bestimmen kann, wer Daten bekommt, Bilder nutzen darf, und wofür, und, vor allem, wer diese Daten nicht bekommt.

In Zukunft B muss Linda als Erziehungsberechtigte auch explizit zustimmen, dass Einzeldaten für den Schul-Score vom Klassenlehrer und der Datenschutzbeauftragten eingesehen werden können.

Welche Daten sollten eigentlich vertraulich sein? Sollten bei E-Mails und Chats und dergl. nur die Inhalte der Kontakte vertraulich sein (also was jemand geschrieben hat)? Sind nicht die Verbindungsdaten (also wer wem wann geschrieben hat) genauso vertraulich? Sowohl in Zukunft A, als auch in Zukunft B steht es schlecht um die Vertraulichkeit der Verbindungsdaten: Die Tatsache, dass Tina Kontakt zu Strafgefangenen hat, führt zu einer massiven Abwertung ihres Schul-Scores. Im Sinne

der digitalen Souveränität sollten Verbindungsdaten gar nicht gespeichert bzw. ausgewertet zu werden.

2.4. Authentizität

Die oben genannte Zustimmung holt sich der Server des Kultusministeriums über Lindas Smartphone. Wir gehen davon aus, dass Linda sich zuvor dem Smartphone gegenüber als rechtmäßige Besitzerin des Smartphones ausgewiesen hat, z.B. durch Eingabe eines Passwortes, durch einen Fingerabdruck etc.

Authentizität bedeutet, dass man weiß, ob der Kommunikationspartner, mit dem man redet, der ist, den er vorgibt, zu sein, bzw. ob er bestimmte Zugriffs- oder Bestimmungsrechte hat. Authentizität ist eine entscheidende Komponente der digitalen Souveränität, die leider oft vergessen wird. Wenn man nicht überprüfen kann, ob jemand auf bestimmte Daten zugreifen darf, oder ob jemand bestimmte Einstellungen ändern darf, dann kann man digitale Souveränität nicht realisieren. Authentizität kann sogar lebenswichtig sein – zum Beispiel im Fall eines per Fernsteuerung regelbaren Herzschrittmachers oder einer Insulinpumpe.

2.5. Verfügbarkeit

In Zukunft A hat Jens einen Zeitungsartikel gekauft, der dann, ohne seine Zustimmung, wieder von seinem Smartphone gelöscht wurde. Zwar bekommt Jens sein Geld erstattet, aber er kann diesen Artikel nicht mehr lesen. In Zukunft B kann niemand ohne explizite Zustimmung von Jens den Artikel löschen, wenn er einmal auf dem Smartphone von Jens ist.

Verfügbarkeit bedeutet, dass man sich darauf verlassen kann, einen Dienst, eine Sache oder irgendwelche Daten nutzen zu können.

2.6. Transparenz

Transparenz bedeutet im weitesten Sinne, dass Vorgänge und Entscheidungen nachvollziehbar sind. Im Sinne der digitalen Souveränität bedeutet es insbesondere, dass die Betroffenen wissen und verstehen, wozu ihre Daten genutzt werden, und dass Entscheidungsträger wissen und verstehen, wie die Daten, aufgrund derer sie eine Entscheidung fällen, zustande kommen. Wir erläutern die Bedeutung der Transparenz am Beispiel des Scoring.

Scoring ist keine neue Erfindung. Zum Beispiel ist es schon seit Jahrzehnten in Deutschland üblich, von Bankkunden, Schuldnern, Mietern etc. eine sogenannte "SCHUFA-Auskunft" einzuziehen. Das Ergebnis ist im Prinzip ein Score, also ein Zahlenwert, der Auskunft darüber gibt, wie kreditwürdig oder zahlungsfähig jemand ist.

Der Auftraggeber kennt das Verfahren nicht. Er muss es auch nicht kennen. Er muss sich allerdings darauf verlassen, dass der Score mit der tatsächlichen Zahlungsfähigkeit korreliert.

Scoring ist zwar nicht neu, doch wird in immer größerem Ausmaß betrieben. Vor allem sind immer mehr Daten verfügbar, die (ob im Einzelfall sinnvoll oder nicht) zur Berechnung eines Scores herangezogen werden. So ist der Schul-Score, mit dem abgeschätzt werden soll, wie gut sich ein Schüler oder eine Schülerin in den nächsten Jahren entwickelt, und wie wahrscheinlich es ist, einen angepeilten Schulabschluss zu erreichen, eine durchaus realistische Zukunftsvision. Inwieweit ein Schul-Score tatsächlich dazu beitragen kann, gefährdete Schulkarrieren zu retten, sei dahingestellt.

Psychologisch ist es verführerisch, eine einzige Zahl zu haben, und, auf der Basis dieser Zahl, klare und nachvollziehbare Entscheidungen zu fällen. Wie sich bei Tina zeigt, bildet eine einzige Zahl die Realität aber oft falsch ab.

Für Entscheidungsträger bedeutet Transparenz, die Einzelpunkte nachvollziehen zu können, aus denen der Score zusammengesetzt ist - so wie in Zukunft B. Für die Betroffenen bedeutet Transparenz, dass sie die Gründe, die zu der Entscheidung geführt haben, selbst nachvollziehen können.

In Zukunft A zeigt sich das Fehlen an Transparenz am Umgang mit dem Schul-Score. Tina hatte keinen Grund, im Vorfeld mit einem schlechten Score zu rechnen. Selbst als sie erfährt, dass ihr Score derart schlecht ist, kann ihr niemand den Grund oder die Ursache für den schlechten Score erklären.

2.7. Digitale Bildung

Wissen ist Macht. Bildung ist mächtiger. Nur wer versteht, wie die digitale Welt funktioniert, kann die Freiheit, über seine Daten entscheiden zu dürfen, wirklich nutzen. Neben der oben erwähnten Transparenz ist auch digitale Bildung wichtig. Wer nicht im Ansatz versteht, wie Scoring-Methoden funktionieren, oder wie Algorithmen aus vielen scheinbar harmlosen Einzeldaten detaillierte Aussagen über Personen ableiten, wird seine eigene digitale Souveränität nur sehr eingeschränkt nutzen können.

Wir stellen uns den "Digitalunterricht", den Tina in Zukunft B genießt, als eine Art erweiterten "Informatikunterricht" vor. Tina und ihre Mitschüler lernen die Grundlagen, wie man einfache Programme schreibt, wie man große Datenmengen auswertet etc.

Der "Medienkompetenz"-Unterricht, den es heute in vielen Bundesländern gibt, mag für sich sinnvoll sein – er liefert aber bei weitem nicht das, was wir unter digitaler Bildung verstehen. Umgekehrt soll der Digitalunterricht nicht vordringlich dazu dienen, Informatiker auszubilden oder die nächste Hackergeneration hervorzubringen. Digitale

Bildung vermittelt vielmehr die Kenntnisse und Fähigkeiten, die man braucht, um kompetent seine digitale Souveränität ausüben zu können.

2.8. Privacy by Design / by Default / by Option

Linda hat der Speicherung ihrer medizinischen Daten in einer statistischen Datenbank zugestimmt. Die Datenbank kann nur für die statistische Auswertung der Daten genutzt werden, wie sie für die medizinische Forschung gebraucht wird. Direkte Rückschlüsse auf Linda und ihren Gesundheitszustand sind unmöglich.

Vertraulichkeit ("Privacy") und andere Sicherheitseigenschaften können entweder natürliche Bestandteile von Kommunikationssystemen sein, die eben entwickelt wurden, um die gewünschte Funktionalität zu realisieren. Das ist "by Design". Oder sie können die Wahl zwischen einem mehr und einem weniger sicheren Modus lassen. Muss man, um in den weniger sicheren Modus zu gelangen, spezielle Aktionen ausführen, die bei dem sicheren nicht nötig sind, ist die Sicherheit "by Default", also voreingestellt. Ist man, ohne weitere Aktion, bereits im weniger sicheren Modus und muss selbst aktiv werden, um in den sicheren Modus zu gelangen, liegt Sicherheit "by Option" vor.

3. Es ist noch nicht soweit. Aber es fängt schon an.

Erscheint Ihnen das Löschen des Zeitungsartikels aus Jens Smartphone in Zukunft B unrealistisch? Bereits 2009 hat Amazon ein elektronisches Buch, das an zahlreiche Kunden verkauft wurde, von deren E-Book-Readern **ohne Vorwarnung oder gar Zustimmung gelöscht** (Spiegel 20.07.2009). Den Kunden wurde, genau wie Jens in unserer Geschichte, der Kaufpreis zurückerstattet. Besonders ironisch ist, dass es sich dabei um das Buch "1984" handelt, in dem George Orwell jene beklemmende Zukunftsvision ausbreitet, mit der elektronischen Überwachung aller Menschen und der systematischen Manipulation aller Medien.

Hier noch einige willkürlich ausgewählte Ereignisse der letzten Monate:

- Snapchat ist eine scheinbar recht datenschutzfreundliche App, weil "Snaps" nach dem Betrachten automatisch gelöscht werden. Im Juni 2016 gibt Snapchat allerdings bekannt, ein Verfahren zum **Auswerten der Inhalte** von Snaps patentiert zu haben. Selbst wenn die Snaps selbst längst gelöscht wurden, wird Snapchat immer noch wissen, wofür sich ein Nutzer besonders interessiert.
- Nutzer der SwiftKey-App erhalten im Juli 2016 Wortvorschläge, die **aus den Daten anderer Nutzern** erzeugt wurden. Unter anderem werden fremde E-Mail-Adressen als Wortvorschläge gemacht.
- Der Digitalkünstler Dennis Cooper hat seit 14 Jahren seine gesamte Kunst in seinen Blog bei Google hochgeladen. Im Juli 2016 ist die digitale Kunst weg: Google hat sie **gelöscht**.
- Im August 2016 wird bekannt, dass Facebook **Patienten einer Psychiaterin** andere Patienten der Psychiaterin als mögliche Freunde vorschlägt. Vermutlich hatten die Patienten Facebook den Zugang zu ihren Smartphones erlaubt, und Facebook hat die Telefonnummer der Psychiaterin als Nummer eines gemeinsamen Freundes identifiziert.
- WhatsApp – einige Jahre zuvor von Facebook aufgekauft – kündigt im August 2016 eine Änderung seiner Nutzungsbedingungen an. Zwar kann man der Nutzung der Daten durch Facebook zu Werbezwecken widersprechen (Privacy by Option), aber **die Daten werden trotzdem an Facebook weitergegeben** und dürfen von Facebook für andere Zwecke genutzt werden. Das kann man nur dadurch verhindern, dass man den neuen Nutzungsbedingungen nicht zustimmt und damit auf die Nutzung von WhatsApp verzichtet. Im September 2016

drohten Verbraucherschützer wegen dieser Praxis mit einer Klage gegen WhatsApp.

- Forscher der Universität Texas in Austin demonstrieren im September 2016 eine Gesichtserkennungssoftware, die auch bei **verpixelten Gesichtern** eine gute Erkennungsleistung hat.
- Im September 2016 **zensiert** Facebook eines der berühmtesten Kriegsfotos der Welt (das Pressefoto des Jahres 1972). Weil auf dem Foto ein nacktes Kind abgebildet ist, das vor Napalm-Bomben fortläuft, betrachten die Facebook-Zensoren das Bild als Kinderpornographie. Sogar Proteste gegen diese Entscheidung werden von Facebook zensiert. Aufgrund der massiven Kritik nimmt Facebook die Entscheidung nach einigen Tagen zurück. Wäre dieses Bild jemals so bekannt geworden, wenn es Facebook schon 1972 gegeben hätte?
- Am 13. September 2016 sorgt ein Firmware-Update des Drucker-Herstellers HP dafür, dass der Drucker Tintenpatronen von Fremdherstellern, die bis dahin funktionierten, ab sofort ablehnt. Dabei war das letzte Firmware-Update von HP schon im März 2016 - die Funktion wurde offenbar an einem bestimmten Stichtag aktiviert, nachdem viele Kunden die HP-Firmware installiert hatten. Das **verzögerte Aktivieren einer Schadensfunktion**, einige Zeit nach der Installation der Software, ist ansonsten eher typisch für bösartige Malware.
- Im Oktober 2016 kündigt das Unternehmen Score Assured in Großbritannien eine neue Dienstleistung an: **Scoring anhand der Teilnahme an sozialen Netzwerken** (aktuell Twitter, Instagram, Facebook und LinkedIn). Score Assured will ausdrücklich nicht nur den gegenwärtigen Status einer Person bewerten, sondern auch deren dessen zukünftige Entwicklungen prognostizieren. Score Assured macht auch Aussagen zu Persönlichkeitsmerkmalen (Offenheit, Extrovertiertheit, …) und sogar darüber, wie neurotisch eine Person ist. Die erste Zielgruppe von Score Assured sind Mietinteressenten. Die Teilnahme am Scoring ist grundsätzlich "freiwillig". Aber wer die Teilnahme verweigert, wird eine begehrte Wohnung wahrscheinlich nicht bekommen. In naher Zukunft will Score Assured auch das Scoring von Stellenbewerbern für potentielle Arbeitgeber vermarkten.
- Im Oktober 2016 weist ProPublika darauf hin, dass Google bereits einige Monate vorher seine "privacy policy" geändert hat. Die bisherigen Regeln verboten es Google explizit, die Informationen über das Surfverhalten, das Google über den DoubleClick Dienst gesammelt hat, mit persönlich identifizierbaren Informationen zu verknüpfen. Nunmehr ist es Google

grundsätzlich erlaubt, **persönliche Informationen**, zum Beispiel über die Nutzer des E-Mail-Dienstes gmail, **mit dem beobachteten Surfverhalten im WWW zu verknüpfen**, das mit Hilfe von DoubleClick gewonnen wird. Nutzer die das nicht wollen, müssen die Voreinstellung der Google Dienste ändern (Privacy by Option).

4. Datenmanagement

4.1 Recht auf Vergessenwerden versus Verfügbarkeit

Wer digitale Informationen über sich preisgibt, will oft nicht, dass diese für immer verfügbar sind. Deshalb wurde die Idee entwickelt, elektronisch gespeicherte Daten mit einem „Verfallsdatum“ auszustatten. Nach Ablauf soll die Information automatisch gelöscht werden. Die EU-Datenschutzgrundverordnung sieht stattdessen eine Art **Recht auf Löschen** vor. Ist der Zweck der Speicherung nicht mehr gegeben oder widerruft die betroffene Person ihre Zustimmung zur Speicherung, müssen die Daten gelöscht werden. Die praktische Umsetzung des Rechtes stößt allerdings auf **grundsätzliche, rechtliche und technische Probleme**.

Grundsätzlich steht das Recht auf Löschen bestimmter Daten im Konflikt mit dem Recht Anderer, auf diese Daten zuzugreifen. Das peinliche Foto einer Privatperson muss offenbar anders behandelt werden als der kritische Bericht über eine öffentliche Person.

Ein nationales oder europäisches Recht auf Löschen ist international kaum durchsetzbar. So setzt Google das Recht auf Löschen nur auf seinen europäischen Domains um. Wer also bestimmte Daten auf „google.de“ erfolglos sucht, findet sie oft auf „google.com“.

Technisch verschwinden Daten, die einmal irgendwo gespeichert wurden, nicht mehr. Metaphorisch ausgedrückt: Ist der Geist erst einmal aus der Flasche, will er nicht wieder hinein. Nehmen wir an, Alice verbreitet ein Bild von sich. Bob betrachtet es auf seinem Gerät. Nach Ablauf des Verfallsdatums soll das Bild (auch) von Bobs Rechner gelöscht werden. Daten sind Folgen von Bits, die beliebig kopiert und überall abgespeichert werden können. Daran scheiterte auch die X-pire! Software, die als „digitaler Radiergummi“ in der Presse Aufsehen erregte. Mit X-Pire! wurden die Daten verschlüsselt verschickt. Zum Betrachten besorgte die X-Pire! Software den Schlüssel vom Server und entschlüsselte das Bild. Das Löschen des Schlüssels vom Server führte dazu, dass das Bild nicht mehr betrachtet werden konnte. Leider kann man Verfahren wie X-pire! dadurch umgehen, dass man den Schlüssel, wenn man das Bild erstmals betrachtet, selbst speichert.

Technisch möglich ist eine Hardwarelösung, bei der ein Teil (das „Trusted Plattform Module“, TPM) von Bobs Computer unter der Kontrolle von Alice oder einer anderen Partei steht. Das TPM sorgt dafür, dass das Bild gelöscht wird oder zumindest nicht mehr angezeigt werden kann. Leider kann nun Alice oder jene andere Partei alles kontrollieren, was Bob je zu sehen bekommt (das bereits erwähnte grundsätzliche Problem). Die digitale Souveränität von Alice, ihre Daten „löschen“ zu können, geht zu Lasten von Bob, der wichtige Aspekte seiner digitalen Souveränität verliert.

Trotzdem kann das Recht auf Vergessenwerden (bzw. auf Löschen) **plausibel durchgesetzt** werden, wenn man annimmt, das Bob das System nicht aktiv unterläuft. Man kann Daten mit Verfallsdatum verbreiten, und Bob kann freiwillig Software einsetzen, die diese Daten nach ihrem Ablauf löscht. So werden im Snapchat-Netzwerk Daten verschickt, die sich kurz nach dem Anschauen wieder löschen. Snapchat weist selbst darauf hin, dass es ohne weiteres möglich ist, die Löschfunktion auszuhebeln. Doch weil der wesentliche Sinn des Netzwerkes im Verschicken und Empfangen flüchtiger „Snaps“ besteht, haben die Nutzer kaum Bedarf, diese Daten dauerhaft zu speichern. Inwieweit sich dieser Ansatz allerdings auf andere soziale Netzwerke übertragen lässt, ist unklar.

4.2 Bezahlen mit Daten

Viele Verbraucher wissen, dass ihre Daten von den Anbietern „kostenloser“ Dienste im Internet für gezielte Werbung genutzt werden. Das wird von manchen sogar positiv gesehen: Wenigstens bekommt man Werbung für Dinge, für die man sich interessiert. **Leider ist die Vermutung falsch, dass die Daten nur für gezielte Werbung genutzt werden.** Tatsächlich kann man Kundendaten auch ohne Werbung zu Geld machen. Deshalb erlaubt zum Beispiel WhatsApp seinen Kunden, der Nutzung ihrer Daten für Facebook-Werbung zu widersprechen. Die Daten werden trotzdem an Facebook weitergegeben – um sie zwar nicht zur Werbung, aber für andere Zwecke zu nutzen.

Unter anderem nutzen soziale Netzwerke die Daten ihrer Nutzer natürlich auch zur Vergrößerung des Netzwerkes. Das ist nicht immer harmlos. So waren nicht alle Patienten einer Psychiaterin davon begeistert, dass sie von Facebook eingeladen wurden, sich untereinander zu befreunden. Aber die Telefonnummer der Psychiaterin war in den persönlichen Telefonbüchern der Patienten und konnte von Facebook ausgewertet werden.

Ansonsten gilt: Daten sind Macht! Die Macht der Daten erlaubt (oder erleichtert) unter anderem **Algorithmic Pricing**: Ein Online-Shop kann verschiedenen Kunden die gleiche Ware (oder Dienstleistung) zu unterschiedlichen Preisen anbieten. Dem passionierten Käufer von Apple-Produkten könnte man das neueste iPhone teurer anbieten. Kunden, die in der Vergangenheit offenbar Preisvergleiche betrieben haben, ohne auf die Versandkosten zu achten, könnte man entsprechend ein „billiges“ Angebot mit einer besonders großen Versandkostenpauschale machen.

Die Macht der Daten ermöglicht auch **Scoring**. Unternehmen nutzen Daten, um Personen zu bewerten, z. B. für die Kreditvergabe, für Versicherungen usw. Sogar potentielle Arbeitgeber könnten ein Scoring der Bewerber einfordern. Mit Scoring ist Geld zu verdienen, also werden Daten zum Scoring genutzt. Das Pikante am Scoring ist,

dass die Betroffenen fast nie wissen, dass sie betroffen sind! Warum hat die Lebensversicherung ihnen kein Angebot gemacht oder nur eines mit Risikozuschlag? Warum hat ein potentieller Arbeitgeber die Bewerbung abgelehnt?

Schließlich bringen die Daten auch **politische Macht**. Egal, ob Internet-Konzerne wie Google oder Facebook diese Macht zur Zeit anstreben oder nicht: Wer die Vorlieben einer Person kennt, wer weiß, worüber sich die Person aufregt und worüber nicht, … der hat einiges an Macht über diese Person. Diese Macht birgt ein erhebliches Missbrauchspotential.

4.3 Lösungsvorschlag: Das Recht auf Vergessenwerden in sozialen Netzwerken

Grundsätzlich sollte es in allen sozialen Netzwerken möglich sein, Daten zu verschicken (Bilder, Filme oder Texte), die ein **Verfallsdatum** haben und danach von der Software (also der App) automatisch gelöscht werden. Dabei sollte man allerdings kein hohes „Sicherheitsniveau“ erwarten oder anstreben. Wer die Löschfunktion aushebeln und die Daten kopieren kann, kann es tun. Wir gehen davon aus, dass typische Nutzer wenig Bedarf haben, Bilder, Filme oder Texte dauerhaft zu speichern, von denen der Absender nicht will, dass sie dauerhaft gespeichert werden. Technisch wäre es sehr einfach, eine solche Lösung umzusetzen.

Bleibt die Frage, wie man mit Dateien umgeht, bei denen man nicht a priori ein Verfallsdatum nennen, bei denen man aber auch nicht sofort, wenn man sie verbreitet, für immer auf das Recht auf Löschen verzichten möchte. Wir schlagen vor, ein Standard-Verfallsdatum zu wählen, z. B. ein Jahr nach Veröffentlichung. Dies entspricht der Idee der **privacy by default**. Für diese Dauer können die Dateien dann auf dem Rechner des Empfängers gespeichert werden. Das Verfallsdatum verlängert sich automatisch, wenn der Absender beim Erreichen des Standard-Verfallsdatums die Datei nicht selbst von seinem eigenen Gerät gelöscht hat.

5. Recht auf Wahl der Darstellung

Bei klassischen Medien gibt es nur eine mögliche Darstellung für den Konsumenten. Einen Text, der auf Papier geschrieben ist (oder auf auch Papyrus, Pergament, …) kann man nur in genau der Qualität lesen, in der der Text geschrieben ist (Schriftart, Größe, …). Immerhin ist es dem souveränen Leser eines geschriebenen Textes möglich, beim Lesen Zeilen, Absätze oder Seiten des Textes zu überspringen oder zu bereits gelesenen Teststellen zurückzukehren.

Mit der Digitalisierung von Texten – und anderen medialen Inhalten – geht potentiell eine Stärkung der Souveränität des Medienkonsumenten einher. Digitale Texte kann man sich grundsätzlich in der Schriftart und -größe anzeigen lassen, die den eigenen Sehgewohnheiten und den Möglichkeiten des Anzeigegerätes entspricht. Das ist ein wesentlicher Beitrag zur Barrierefreiheit der digitalen Medien, aber auch ein Ausdruck der digitalen Souveränität der Verbraucher überhaupt.

Rechtliche oder technische Maßnahmen, die dazu dienen, den Nutzern digitaler Medien die so gewonnene Freiheit der Darstellung wieder zu nehmen, sind verbraucherfeindlich und schränken massiv die Barrierefreiheit ein. Einschränkungen bei der Wahl der Darstellung enthalten den Verbrauchern wichtige Vorteile vor, die die Nutzung digitaler Medien gegenüber der Nutzung analogen Medien mit sich bringt. Unter Umständen sind die Verbraucher bei der Nutzung digitaler Medien dann sogar schlechter gestellt, als bei der Nutzung analoger Medien. Deshalb darf es grundsätzlich keine künstlichen Einschränkungen für die Wahl der Darstellung bei digitalen Medien geben!

Dieser Grundsatz gilt auch für Werbung. Natürlich haben Medienanbieter das Recht, ihr Angebot mit Werbung zu finanzieren. Umgekehrt haben Verbraucher aber das Recht, diese Werbung zu ignorieren. Das ist zum Beispiel bei gedruckten Zeitungen selbstverständlich: Entweder der Zeitungsleser findet die Werbung interessant. Oder er blättert weiter. Technisch ist es ohne weiteres möglich, beim Lesen einer digitalen Zeitung den Nutzer praktisch dazu zu zwingen, die Werbung zur Kenntnis zu nehmen. Zum Beispiel kann man den nächsten Artikel erst anzeigen, wenn die Werbung eine angemessene Zeit lang angezeigt wurde. Oder man kann einen Teil des Bildschirms für Werbung reservieren, die der Verbraucher nicht „weg-klicken“ kann. Tatsächlich ist das heute bereits die Arbeitsweise aggressiver „Pop-Ups“ auf manchen Webseiten.

Gesetzgeberisch sehen wir in diesem Punkt keinen aktuellen Handlungsbedarf. Jede Technologie, die die Digitale Souveränität der Verbraucher behindert, kann durch eine andere Technologie gekontert werden, die die Digitale Souveränität der Verbraucher wiederherstellt. Gegen aggressive „Pop-Up“ Werbung, zum Beispiel, helfen „Add-Blocker“. Technologien wider Digitale Souveränität und Technologien für Digitale

Souveränität schaffen in diesem Fall einen vernünftigen Interessenausgleich zwischen den Anbietern von Medien und den Verbrauchern.

Wichtig ist es jedoch, mögliche gesetzgeberische Initiativen zum Verbot jener Technologien zu verhindern, die der Digitalen Souveränität der Verbraucher dienen. Neben den bereits genannten „Ad-Blockern“ könnte dies zum Beispiel Software betreffen, die den Kopierschutz von Medien umgeht oder entfernt, um Soft- oder Hardware, um Werbeblöcke bei aufgezeichneten Fernsehsendungen zu überspringen . **Die Nutzung derartiger Technologien für die Digitale Souveränität der Verbraucher darf nicht eingeschränkt oder gar verboten werden.**

Angesichts einer kontinuierlichen (und grundsätzlich legitimen) Lobby-Arbeit zugunsten der Medienarbeiter, mit dem Ziel, die Nutzung derartiger Technologien zu verbieten, könnte die Aufgabe, derartige Verbote zu verhindern, zu einer Daueraufgabe für den Verbraucherschutz werden.

6. Scoring

Beim Scoring werden Massendaten früherer Fälle von Kredit- oder Versicherungsverläufen auf statistische Korrelationen zwischen Input (Alter, Geschlecht, Einkommen usw.) und Output (z.B. Kreditrückzahlung, Versicherungsfall) hin untersucht. Dafür wird eine Fülle von zumeist qualitativen Faktoren auf ein Punktesystem abgebildet und auf einer standardisierten Skala vergleichbar und berechenbar gemacht. Aus einer großen Zahl empirischer Daten werden statistisch Gruppen gebildet, die mit einer bestimmten Eintreffenswahrscheinlichkeit des fraglichen Ereignisses korreliert sind. Die Kunst bei dieser Risikoabschätzung liegt somit in der Identifikation von relevanten Faktoren und in ihrer Gewichtung für die Korrelation mit zukünftigen Ereignissen. Die Daten eines zu prüfenden Einzelfalls werden dann einer dieser standardisierten Gruppen zugeordnet, in der Erwartung, dass das Ereignis sich in diesem Einzelfall mit der gleichen Wahrscheinlichkeit einstellt, wie im Fall dieser Gruppe.

In einem dritten Schritt werden aus dieser errechneten Risikoabschätzung Entscheidungen abgeleitet, ob das Risiko eingegangen und wie es ggf. abgesichert werden soll. Die Schufa sagt nur: 'Das Risiko ist x von 100.' Die Vergabeentscheidung trifft der Sachbearbeiter einer Bank. Scoring verhindert also keine Kredite oder Versicherungen, entscheidet aber über ihren Preis. Während Sparkassen risikoarm vergeben, spezialisieren sich andere Geldinstitute auf Risikokunden und nehmen entsprechend hohe Zinsen. Scoring dient als Entscheidungshilfe. Die Entscheidungen treffen bislang meist noch Menschen, jedoch zunehmend Algorithmen. Mit der Digitalisierung nehmen Quellen, Mengen und Verknüpfbarkeit von Daten, die für eine Risikoabschätzung relevant sein können, unaufhörlich zu. Statt weniger statischer Datenpunkte kann Scoring jetzt auf umfassende Datenströme in Echtzeit angewendet werden. Folglich nimmt der Einsatz von Scoring in unterschiedlichen Feldern zu.

Am bekanntesten ist das Kredit-Scoring, das Vorhersagen über die Wahrscheinlichkeit einer Kreditrückzahlung treffen soll. Diese Form der Bonitätsprüfung wird aber auch für Kauf auf Rechnung im Online-Versandhandel, Ausstellung einer Kreditkarte, Mobilfunk- und Mietverträge vorausgesetzt. Banken, Kreditkartenunternehmen, Versandhändlern, Telekommunikationsunternehmen erstellen ihre eigenen Scores oder greifen auf die Dienstleistungen von Wirtschaftsauskunfteien wie der Schufa zurück.

Versicherungsgesellschaften versuchen bereits seit der Verbreitung von Personenwaagen in den 1860er Jahren, Normwerte für ein gesundes Körpergewicht für die Risikoabschätzung und Kostenkalkulation zu verwenden. Im Zuge des aktuellen Selbstvermessungs-Trends für Gesundheit, Fitness, Ernährung, auch bekannt als

mHealth, werden immer häufiger Smartphone-Apps verwendet als Schrittzähler, Laufprogramme, Body-Mass-Index-Rechner, Diet Tracker, Mood-Manager oder Selbstdiagnose-Tool. Neben den hauseigenen Ortungs-, Bewegungs- usw. Sensoren von Smartphones erweitern Smartwatches, Fitnessarm- und Brustbänder, Schlafsensoren und andere Wearables bis hin zu Implantaten die Messmöglichkeiten.

Auch Kraftfahrzeugversicherungen bieten sogenannte Telematik-Tarife an, bei denen aus gemessenen Verhaltensdaten Risiko-Scores für Unfälle und damit der Versicherungspreis berechnet wird. Auch hier sammeln und versenden Sensoren im Smartphone oder in speziellen im Auto montierte Blackboxen Daten über die Geschwindigkeit auf der jeweiligen Straße, schnelles Bremsen und Beschleunigen, Pausen auf langen Fahrten usw.

Eine Strategie für das Scoring junger Neukunden, die noch keine Fahr- bzw. Kreditgeschichte haben, beruht nicht auf Verhaltensmerkmalen, sondern auf Charaktereigenschaften. Diese sollen mit Hilfe von linguistischen Analysen der Äußerungen auf Social-Media-Plattformen erhoben werden. Admiral, eines der größten britischen Versicherungsunternehmen, plant mit Firstcarquote, sich von Anwärtern den Zugriff auf ihre Facebook-Accounts geben zu lassen. Ihre Textäußerungen werden dann nach Anzeichen untersucht, ob sie gewissenhaft und gut organisiert sind oder allzu selbstsicher auftreten. Diese Charakterdaten werden dann mit älteren Versicherungsfällen verknüpft, um Risikowahrscheinlichkeiten zu berechnen und das Risiko, d. h. die Versicherungsprämie, einer Antragstellerin zu kalkulieren. Wer sich auf den Charaktertest einlässt, könne bis zu 400 Euro im Jahr sparen (Ruddick, Guardian 02.11.16). Auch das britisches Startup Tenant Assured schätzt die Bonität von Mietern anhand ihres Social Media Verhaltens ein (Wagener, Nerdwärts 22.06.2016).

Die Markteinführung eines Score-basierten Produktes wird in der Regel von einem Fairness-Diskurs begleitet. Scoring schütze Verbraucher vor Überschuldung. Es sorge für niedrigere Preise, da es Unternehmen vor Zahlungsausfällen schütze. Eine verhaltensbezogene Preisdifferenzierung verhindere, dass z. B. vorsichtige Autofahrer Risikogruppen quersubventionieren. Schließlich erlaube Scoring, dass junge Kunden ohne Kreditgeschichte und andere Risikogruppen überhaupt einen Kredit oder eine Versicherung erhalten. Und natürlich ist die Selbstüberwachung strikt freiwillig und werde ausschließlich für Boni für risikominderndes Verhalten, nie aber für Strafzahlungen für riskantes Fahren oder zu langes Sitzen am Schreibtisch verwendet.

Überdies suggerieren Quantifizierung und Statistik Objektivität. Menschen mögen ihre Vorstellungen haben über den Zusammenhang von Geschlecht und Fahrsicherheit, Migrationshintergrund und Kreditrückzahlung, Armut und Krankheitsrisiko. Algorithmen dagegen haben keine Vorstellungen. Sie suchen nach statistischen

Korrelation verschiedener Datenpunkte. Die Verfahren, wird stets betont, basierten auf wissenschaftlich fundierten Analysen und der „Unterstützung durch führende akademische Einrichtungen“ (Generali, Pressemitteilung zur Einführung der Telematik-Versicherung Vitality). Auch die Schufa hebt hervor: „Kreditscores sind frei von subjektiven – und daher möglicherweise diskriminierenden – Faktoren, wie z. B. Herkunft, Religion oder Behinderung.“ (Schufa: Was ist Scoring?)

6.1 Datensparsamkeit und Zweckbindung

Scoring bildet seiner Natur nach

> „ein Spannungsverhältnis zwischen Informationsbedürfnissen für die Prognose von Kreditrisiken auf der einen Seite und dem Datenschutz auf der anderen: Je detailliertere Informationen über einzelne Verbraucher vorliegen, desto besser wird die Krediterfüllungsprognose, aber desto mehr wird auch in die Privatsphäre eingegriffen.“ (Schröder/Taeger 2014: 15)

Je mehr Informationen, desto besser die Prognose – dieser Zusammenhang liegt der Methode Scoring systematisch zugrunde. Scoring zielt also seinem Wesen nach auf das Gegenteil von Datensparsamkeit. Auch den verfassungsrechtlich begründeten Grundprinzipien der Erforderlichkeit und der Zweckbindung widerspricht Scoring systematisch. Fahrzeug-, Trainingsdaten, Posts auf Social Media werden nicht zu dem Zweck produziert, Prädiktoren für Risiken, d.h. Faktoren für die Preisdifferenzierung zu liefern. Was technisch machbar und wirtschaftlich erfolgversprechend ist, dem soll der Datenschutz nicht im Weg stehen, so sehen es Teile der Bundesregierung. Kanzlerin Merkel (Weichert/Schuler 2015: 3), Wirtschaftsminister Gabriel (Krempl 19.11.2015) und Infrastrukturminister Dobrindt (Krempl 17.11.2016) singen das gleiche Lied wie der Bitkom: Die Deutschen sollten ihre Datenschutz-Bedenken fallen lassen. Big Data sei der Rohstoff der Zukunft. Wertschöpfung entstehe künftig aus der Nutzung von Kundendaten. Datensparsamkeit und Zweckbindung hätten sich überholt. Stattdessen müsse „Datenreichtum“ und „Datensouveränität“ statt Datenschutz der Maßstab der Politik sein.

- Die Rhetorik vom Datenschutz als Innovationshindernis muss einem klaren Bekenntnis zur Sicherung von informationellen Grundrechten weichen. Die wirtschaftliche Erschließung des Rohstoffs Nutzerdaten darf nicht auf Kosten von unverzichtbaren Schutz- und Freiheitsrechten gehen. Justizminister Maas hat vor einem Jahr die Debatte über eine Charta der digitalen Grundrechte (Maas 10.12.2015 eröffnet. Nach dem brasilianischen Vorbild der breiten gesellschaftlichen Debatte über den Marco Civil da Internet (24.04.2014) geführt, bietet sie die Chance, die Grundrechteorientierung der Bevölkerung wie der Bundesregierung zu stärken.

- Akademische Datenforschung muss möglich bleiben, unter besonderes gesicherten Laborbedingungen. Die wissenschaftliche Anerkennung mathematisch-statistischer Verfahren und der Nachweis, dass die genutzten Daten für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind, ist Bedingung für die Zulässigkeit von Scoring (§ 28b BDSG).
- Bevor jedoch aus einer Laborerkenntnis ein Produkt werden kann, das im Freilandversuch getestet werden darf, hat eine Ethikkommission darüber zu befinden. Genauso, wie über den Einsatz von möglicherweise hilfreichen, sicher aber einschneidenden Technologien wie Gen- oder Reproduktionstechnik die Gesellschaft entscheidet und nicht der Markt.
- Dabei werden Grenzen auszuhandeln sein. In der Facebook Platform Policy schreibt das Unternehmen App-Entwicklern vor: „3.15. Don't use data obtained from Facebook to make decisions about eligibility, including whether to approve or reject an application or how much interest to charge on a loan.“ Die Vermutung liegt nahe, dass Facebook damit nicht die Interessen von Verbrauchern schützen, sondern dieses Geschäftsmodell sich selber vorbehalten will. Andererseits gibt es gute Gründe, dass auch eine verfassungsrechtliche Abwägung der Auswirkungen von Social-Media-Scoring auf das Grundrecht der freien Meinungsäußerung ein solches Verwertungsverbot normieren würde.
- Opt-In ist eine unumgängliche Voraussetzung, aber nur ein Teil der Lösung. Die Bereitschaft, Daten gegen Rabatte preiszugeben, ist bei etwa 30% der deutschen Bevölkerung vorhanden (YouGov 2015). Sie müssen sich darauf verlassen können, dass auch in dem Fall Privacy by Design als digitale Daseinsvorsorge öffentlich gewährleistet wird.
- Ein Mittel dafür ist die Zertifizierung durch unabhängige Stellen: Nur so haben Verbraucher die Chance, sich darauf verlassen zu können, dass da, wo „vertrauenswürdig“ draufsteht, auch Vertrauenswürdiges drin steckt (anders als bei der Browser-Erweiterung „Web of Trust“, die vorgibt, dem Nutzer dabei zu helfen, sicher zu surfen (NDR 01.11.2016)).

6.2 Datenqualität

Ohne aktuelle und richtige Daten kann eine Datenanalyse keine brauchbaren Ergebnisse liefern. Was in der Informatik als false positives und false negatives bekannt ist, sind für die Wirtschaft entgangene oder getätigte, aber gescheiterte Geschäfte. Wenn öffentliche und nicht-öffentliche Stellen Daten ohne Kenntnis des Betroffenen erheben, muss dieser über die Speicherung, die verantwortliche Stelle sowie die Zweckbestimmungen der Datenverarbeitung unterrichtet werden (§§ 19a, 33 BDSG). Überdies hat die

verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, die Herkunft dieser Daten, die Empfänger, an die Daten weitergegeben werden, und den Zweck der Speicherung (§§ 19, 34 BDSG). Unrichtige Daten sind zu berichtigen; unzulässig gespeicherte und für den Zweck nicht mehr erforderliche Daten sind zu löschen oder, soweit ihre Richtigkeit vom Betroffenen bestritten wird, sich aber weder die Richtigkeit noch die Unrichtigkeit feststellen lässt, zu sperren (§§ 20, 35 BDSG). Beim Scoring schließt der Auskunftsanspruch die innerhalb der letzten sechs Monate erhobenen Wahrscheinlichkeitswerte sowie die zu ihrer Berechnung genutzten Datenarten ein, nicht aber die Daten selbst (34 Abs. 2 BDSG).

- Um aufgrund falscher Daten zustande gekommene Entscheidungen anfechten und Daten korrigieren zu können, muss ein Betroffener Auskunft über alle in den Score eingegangenen Daten erhalten, nicht nur über Datenarten. Der Anspruch richtet sich an die für die Berechnung des Wahrscheinlichkeitswertes verantwortliche Stelle.

6.3 Algorithmenqualität

Bei Verbrauchern stellt sich zunehmen das Gefühl ein, vollkommen transparent für Institutionen zu sein, die selber vollkommen intransparent Entscheidungen über sie treffen. Die Datenmodelle und die Gewichtung der Faktoren beim Scoring sind geheim. Kanzlerin Merkel äußerte jüngst bei den Medientagen in München, „dass Algorithmen transparenter sein müssen, sodass interessierten Bürgern auch bewusst ist, was eigentlich mit ihrem Medienverhalten und dem anderer passiert.“ Der netzpolitische Sprecher der Unionsfraktion, Thomas Jarzombek, korrigierte: „Die Kanzlerin meint sicher nicht, dass die Firmen ihre Geschäftsgeheimnisse offenlegen sollen. Aber wir brauchen mehr Informationen von Betreibern wie Facebook darüber, wie ihr Algorithmus im Großen und Ganzen funktioniert.“ (Reinbold, 26.10.2016). Rechtlich muss die für eine auf Scoring basierende Entscheidung verantwortliche Stelle Auskunft erteilen über „das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.“ (34 Abs. 2 Pkt. 3 BDSG).

Die Schufa erklärt, warum sie ihren Gewichtungsalgorithmus grundsätzlich nicht transparent machen kann: Seine Kenntnis würde 1. betrügerische Manipulationen ermöglichen und 2. Konkurrenten erlauben, das Verfahren zu kopieren. Sie verweist dazu auf eine Studie über die Gefahren transparenter Scores, (Róna-Tas/Hiß 2008) die einen Zusammenhang zwischen der Subprime-Hypothekenkrise und manipulierbaren Scores in den USA zeigt.

- Vertrauliches In Camera Auditing: Eine Überprüfung unter Geheimhaltungsauflagen ist prinzipiell möglich, aber selbst mit vollem Zugriff auf alle Datensätze und Algorithmen ist es schwierig nachzuvollziehen, wie sie zusammenspielen, ob sie systematischen Bias enthalten und welche Ergebnisse sie im Einzelfall produzieren.

6.5. Diskriminierung

Selbst wenn Merkmale wie Geschlecht, Rasse, sexuelle Orientierung, Einkommen nicht direkt erhoben werden, erlauben Kombinationen aus scheinbar unverfänglichen Daten darauf zu schließen. Facebook beschloss aufgrund massiver Kritik vor Kurzem seine „Ethnic Affinity“ Werbung einzustellen (Hern 22.03.2016). Das Unternehmen, das im vergangenen Jahr rund 18 Mrd. US-Dollar mit Werbung einnahm, betonte, es habe keine Möglichkeit, die Ethnizität seiner Nutzer zu erkennen. Die Zielgruppen würden nicht nach Identität, sondern nach Affinität ermittelt, z. B. zu afro-amerikanischen Inhalten. Bis zur Einstellung konnten Werbetreibende Afro-Amerikaner, asiatischstämmige Amerikaner und vier Arten von Hispanics nicht aber Weiße in ihre Zielgruppe ein- oder ausschließen (Maheshwari/Isaac 11.11.2016). Facebook verteidigt sich damit, dass „multikulturelles Marketing“ gängige Praxis in der Werbeindustrie sei (Heath 07.11.2016).

Oft führt aber auch die Auswahl der Trainingsdaten für den Algorithmus zu gänzlich unbeabsichtigten Verzerrungen. So klassifizierte Googles Gesichtserkennung, die an weißen Gesichtern trainiert worden war, Schwarze als „Gorillas“ (Barr 01.07.2015).

Die Markteinführung von Scoring-basierten Produkten erfolgt immer freiwillig und mit dem Versprechen einer tariflichen Belohnung für risikominderndendes Verhalten. Das hat nicht nur marketingpsychologische, sondern rechtliche Gründe. Das Allgemeine Gleichbehandlungsgesetz (AGG) verbietet „eine Benachteiligung aus Gründen der Rasse oder wegen der ethnischen Herkunft, wegen des Geschlechts, der Religion, einer Behinderung, des Alters oder der sexuellen Identität“ im Zusammenhang mit zivilrechtlichen Schuldverhältnissen im Massengeschäft und ausdrücklich bei privatrechtlichen Versicherungen (§ 19 Abs. 1 AGG). Es erlaubt Ungleichbehandlung nur in wenigen Ausnahmen, u. a. wenn sie „besondere Vorteile gewährt” (§ 20 Abs. 1 Pkt. 3 AAG). Seniorenrabatte oder Boni für Frauen, die ein geringeres Unfallrisiko darstellen, sind daher zulässig.

Grundrechte gehen vor Machbarkeit. Die Gleichstellung von Männern und Frauen, bekräftigte der EuGH im März 2011 (C-236/09), bedinge geschlechtsneutrale Versicherungsprämien und Leistungen. Eine Übergangsregelung, die Mitgliedsstaaten

eine geschlechtsspezifische Preisdifferenzierung erlaubte – von der Sache her nachvollziehbar, ist doch für eine Rentenversicherungen relevant, dass Frauen länger leben – erklärt das Gericht mit Wirkung vom 21. Dezember 2012 für ungültig. Seither dürfen in der EU nur noch Unisex-Tarife angeboten werden.

- Es braucht eine gesellschaftliche Debatte darüber, welche Grundrechte durch Scoring-Verfahren bedroht sind und welche Merkmale, wie im Unisex-Urteil, grundsätzlich für Preisdifferenzierung ausgeschlossen werden sollen.
- Beim (in camera) Auditing von selbstlernenden Algorithmen müssen die Trainingsdaten vorgelegt werden, um sie auf versteckte Verzerrungen hin untersuchen zu können.
- Es ist grundsätzlich möglich, Datenanalysealgorithmen – vor allem selbstlernende Algorithmen – auf eine Weise zu implementieren, die ein Auditing praktisch unmöglich macht. Das Vorhandensein einer geeigneten Auditing-Schnittstelle ist grundsätzlich auch im eigenen Interesse des Scoring-Anbieters – außer, wenn er sich bewusst einer unabhängigen Kontrolle entziehen will. Deshalb sollte der Gesetzgeber das Vorhandensein einer Auditing-Schnittstelle verlangen.
- Einspruchsrecht: Gegen fragwürdige Entscheidungen müssen Verbraucher niederschwellig Einspruch erheben und eine Einzelfallprüfung fordern können, bei der die in die Entscheidung eingegangenen Daten überprüft und mit den lokalen Logbuch-Daten abgeglichen werden können.

7. Datensicherheit

Hersteller von IT-Produkten haben selten Interesse an Datenschutz und Datensicherheit. Early Movers wollen den Markt erobern, Sicherheit kostet Zeit in der Entwicklung. Wenn sich einmal implementierte naive Sicherheitslösungen als unsicher erweisen, weigern sich Hersteller oft, neue verbesserte Sicherheitslösungen zu implementieren. Meistens verweisen die Hersteller darauf, dass ihre Kunden nicht bereit sind, die zusätzlichen Kosten zu tragen. Zum Beispiel weisen Telematik-Systeme in Autos regelmäßig Sicherheitslücken auf (Greis 07.09.2015). Wo der Markt systematisch versagt, ist öffentliche Intervention geboten – vor allem, wenn Grundrechte betroffen sind.

- Privacy by Design (PbD), das Kernelement der EU-DSGVO, darf nicht als Kostenfaktor und Innovationsbremse verpönt werden, sondern muss gesetzlich unabdingbar und überprüfbar vorgeschrieben werden.
- PbD in die Informatikausbildung: Technischer Datenschutz muss bei denen ansetzen, die Systeme bauen. Nicht nur PbD, sondern ein umfassendes Verständnis von technischen als sozialen Systemen muss der gesamten Informatikausbildung zugrunde liegen.
- Ein PbD-Prinzip ist, dass Daten grundsätzlich lokal beim Verbraucher verarbeitet und nur in der für den Score erforderlichen aggregierten Form übermittelt werden. Übermittlungen gehen vom lokalen Telematik-Gerät aus, das von außen nicht abgerufen werden kann. Die weitere Verarbeitung von Verhaltens- und Charakterdaten für den Score ist technisch zu trennen von der Stelle, die die eigentliche Entscheidungen (über Versicherungen, Kredite usw.) trifft. Alle Übermittlungs- und Verarbeitungsschritte sind zu jeder Zeit für den Verbraucher sichtbar und nachweisbar und werden in einem lokalen Logbbuch protokolliert, sodass der Verbraucher Abweichungen erkennen und dagegen vorgehen kann.
- Ein weiteres PbD-Prinzip besagt, dass Daten nur anonymisiert, pseudonymisiert oder aggregiert und sowie verschlüsselt und authentisiert übermittelt werden dürfen. Kryptographischen Verfahren wie die Anonyme Attestierung stellen sicher, dass die Daten, die der Verbraucher anonym an die Scoring-Stelle übermittelt, nicht manipuliert sind. Der Verbraucher bekommt den unterschriebenen Score und leitet diesen an die Versicherung weiter. Dank mathematisch beweisbarer Sicherheitseigenschaften des Verfahrens können Datensicherheit und Sicherheit vor Datenfälschung gewährleistet und

sichergestellt werden, dass jede Stelle ausschließlich die für ihren Verarbeitungszweck erforderlichen Daten erhält

Vertraulichkeit (also „Privacy“) ist allerdings nicht der einzige Aspekt der Datensicherheit – und vielleicht nicht einmal der wichtigste. Mindestens ebenso wichtig sind Verfügbarkeit und Authentizität. Wenn ein Verbraucher, sagen wir, seine Urlaubsfotos in der Cloud speichert, dann mag es ihm wichtig sein, dass seine Verwandten und Freunde sich die Bilder ansehen können, aber andere nicht. Das ist Vertraulichkeit. Aber ebenso will der Verbraucher, dass die Bilder nicht irgendwann einfach gelöscht werden, ohne seine Zustimmung und ohne ihn rechtzeitig vorher zu informieren, um die Bilder ggf. anderswo abzuspeichern. Das ist Verfügbarkeit. Und er möchte auch nicht, dass Dritte ohne seine Zustimmung seiner Sammlung von Urlaubsbildern irgendwelche anderen Bilder hinzufügen. Das ist Authentizität.

Während der Begriff des „Privacy by Design“ längst ein feststehender Begriff im Bereich des Verbraucherschutzes ist, werden „Authenticity by Design“ und „Availability by Design“ bisher sträflich vernachlässigt. (Wir laden die geneigte Leserin bzw. den geneigten Leser dazu ein, jeweils einmal nach „Privacy by Design“, „Authenticity by Design“ und „Availability by Design“ zu googeln und die jeweiligen Anzahlen an Resultaten zu vergleichen.)

- Authenticity by Design (Auth-bD) und Availability by Design (Avail-bD) sollten ebenso entwickelt werden, wie PbD bereits entwickelt ist. Es handelt sich weder um störende Kostenfaktoren, noch um Innovationsbremsen.
- Wie bereits erwähnt muss technischer Datenschutz – der alle wichtigen Aspekte umfasst, nicht nur die Vertraulichkeit von Daten, verstärkt in der Informatikausbildung vermittelt und mit einem umfassenden Verständnis von technischen und sozialen Systemen verbunden werden.

8. Datenhandel

Wenn Personendaten die vom Verbraucher kontrollierbare lokale Geräteumgebung verlassen, verliert der Verbraucher die Souveränität über die Daten. Unternehmen, die zu einem erklärten Zweck für den Verbraucher erkennbar Daten erheben, teilen diese regelmäßig mit Subunternehmen und Partnern. Eine pauschale Zustimmung zu der in den Tiefen einer Datenschutzerklärung genannten möglichen Weitergabe von oder Handel mit diesen Daten kann keine Lösung sein.

- Die für den Urheberrechtsschutz entwickelten Techniken des Digital Rights Managements (DRM) sind für den Datenschutz weiter zu entwickeln. Dazu verschließt ein Verbraucher seine Daten vor der Übermittlung in eine kryptographische Kapsel, die sich nur unter bestimmten Bedingungen öffnet, z. B. mit dem privaten Schlüssel eines bekannten Empfängers. Versucht eine dritte Stelle auf die Daten zuzugreifen, fordert die Kapsel authentifizierbare Informationen über die Stelle und den beabsichtigen Verarbeitungszweck und sendet die Anfrage an den Verbraucher, der sie bestätigen muss. PbD heißt hier, die Systemarchitektur schließt eine Datennutzung aus, von der der Verbraucher keine Kenntnis und der er nicht zugestimmt hat.

9. Verbraucherschutzfragen für das Internet Of Things

Die Sicherheitslage ist im IoT Bereich aus einer Reihe von Gründen deutlich schlechter als in der klassischen Computerindustrie. Viele Geräte adressieren einen Markt mit sehr geringen Stückpreisen oftmals im einstelligen Eurobereich. Ein organisiertes Netzsicherheitsmanagement, welches die PC-Industrie über viele Jahre mit erheblichem Aufwand aufbaute, ist im Massenanlagenbau meist nicht zu finden. Oftmals bestehen nicht einmal ausreichende Update-Möglichkeiten. Verschärft wird dies durch eine im niedrigpreisigen Gerätemarkt geringere Kundenbindung der Hersteller, so dass die Verbraucher nicht befriedigend über nötige Sicherheitsupdates informiert werden.

Weiterhin haben viele eingebettete Systeme eine weit längere Einsatzzeit als persönliche Computersysteme. Diese kann beispielsweise bei smarten Heizungssteuerungen viele Jahre betragen. Schließlich ist auch bei vielen Verbrauchern oft nicht einmal das Wissen vorhanden, dass das wegen seiner Funktion angeschaffte Gerät einen wartungsintensiven Internet-Teilnehmer darstellt.

Von unsicheren IoT Geräten gehen Gefahren nicht nur für die digitale Welt aus. So können Störungen in industriellen Anlagen Katastrophen auslösen und auch innerhalb der Hausvernetzungen liegen etwa bei der Heizungssteuerung nicht zu unterschätzende Gefahrenpotentiale vor.
Ronen et al, (2016) demonstrierten, wie Angreifer bestimmte IoT-Geräte dazu bringen können, eine Infektion durch ein Schadprogramm weiterzugeben. Innerhalb weniger Minuten können sich Zehntausende von ungeschützten IoT-Geräten in einer Stadt zu einem einzigen, von den Angreifern kontrollierten Botnetz zusammenschließen.

9.1 Haftung für Schäden

Die seit Sommer 2016 vermehrt auftretenden Angriffe mit Millionen übernommener IoT Geräte zeigen eine neue Dimension des Problems. Für den Verbraucher entsteht unter anderem auch das Problem, dass mit übernommenen Geräten angerichtete Schäden die IP-Adresse des Besitzers als Angriffsherkunft hinterlassen. Dies kann sowohl juristische Folgen, als auch Folgen für die technischen Systeme haben. Abwehrmaßnahmen der angegriffenen Systeme können zu Störungen der unwissend für Angriffe missbrauchten IoT Systemen führen.

- Aus Sicht des Verbraucherschutzes ist eine Klärung der Haftung für von IoT Geräten verursachte Schäden und eine stärkere Inverantwortungnahme der Hersteller herbeizuführen.
- Umgekehrt muss von Verbrauchern verlangt werden, dass Sie für Geräte, die die Sicherheit der Allgemeinheit gefärden, die Verantwortung übernehmen und zumindest die Sicherheitsupdates der Hersteller auch einspielen, so es welche gibt.

9.2 Sicherheitsupdates und Nachhaltigkeit:

Die Erfahrung der letzten Jahre lehrt, dass alle Kommunikationsgeräte zu einer Gefahr für ihre Nutzer und für die Allgemeinheit werden können, wenn nicht regelmäßig entdeckte Sicherheitslücken durch Sicherheitsupdates geschlossen werden. Ein wichtiger Grundsatz ist deshalb, dass während der gesamten Lebenszeit eines Gerätes Sicherheitsupdates geschrieben und installiert werden müssen. Eingebettete und IoT Geräte sind da keine Ausnahme.

In der Praxis ist die Einhaltung dieses Grundsatzes ein Problem. Erstens haben die Hersteller, wenn sie ihre Geräte einmal verkauft haben, oft kein ökonomisches Interesse an einer weiteren Pflege und dem Erstellen vom Sicherheitsupdates. Zweitens ist, vor allem bei kleinen Herstellern, nicht klar, wie lange dieser Hersteller am Markt sein wird, bzw. wie lange es eine verantwortliche Firma gibt, die Sicherheitsupdates erstellen kann. Um dieses Problem zu lösen, schlagen wir das Folgende vor.

- Hersteller sind während der gesamten Lebenszeit eines IoT Gerätes dazu verpflichtet, Sicherheitsupdates zu schreiben und an die Nutzer zu verbreiten.
- Wollen die Hersteller sich, nach Ablauf einer angegebenen Lebenszeit, dieser Verpflichtung entziehen, müssen sie spätestens zu diesem Zeitpunkt ihre Quelltexte als Open-Source veröffentlichen. Damit soll sichergestellt werden, dass zumindest Dritte das Schreiben und ggf. Verbreiten von Sicherheitsupdates übernehmen können.
- Soweit die Quelltexte der Hersteller anfänglich nicht Open-Source sind, müssen sie bei einem Treuhänder hinterlegt werden. Kommt ein Hersteller den genannten Verpflichtungen nicht nach oder existiert der Hersteller nicht mehr, sorgt der Treuhänder für die Veröffentlichung der Quelltexte als Open-Source.

10. Geschlossene Systeme und Systemsicherheit

Die Frage, ob geschlossene oder offene Systeme hinsichtlich der Systemsicherheit vorzuziehen sind, ist zentral innerhalb der Informatik. Während geschlossene Systeme im günstigen Falle durch eine ausreichende Qualitätskontrolle einige Angriffe verhindern können, ist, falls die Qualitätskontrolle versagt, der Schaden vom Nutzer selbst nur schwer abwehrbar.

Neben der im Folgenden ausführlicher beleuchteten Trusted Computing Infrastruktur verbaut Intel in zahlreichen seiner Prozessoren eine eigene Sicherheitsarchitektur. Diese ist ein geschlossenes Konzept, welches höchst problematische Eigenschaften aufweist. Daher ist eine grundsätzliche Deaktivierung der Intel Active Management Technology (AMT) zu empfehlen.

10.1 Fallbeispiel: Trusted Computing und Windows 10

Mit Windows 10 nimmt Microsoft einen starken Paradigmenwechsel in der Sicherheitsarchitektur von persönlichen Computern vor. Hierzu soll ein Trusted-Computing-Modul (TPM) in die persönlichen Computer und Mobilgeräte eingebaut werden. Dieses enthält einen Schlüssel, auf den der Besitzer des Computers keinen Zugriff hat.

Durch den zwangsweise aktivierten TPM-Chip und durch von Microsoft implementierte Verfahren innerhalb von Windows 10 (insbesondere Secure Boot) wird den Nutzern weitgehend die Kontrolle über ihre eigene Hardware und Software entzogen.

- Bewertung des BSI zu Trusted Computing Module: „Aus Sicht des BSI geht der Einsatz von Windows 8 in Kombination mit einem TPM 2.0 mit einem Verlust an Kontrolle über das verwendete Betriebssystem und die eingesetzte Hardware einher. Daraus ergeben sich für die Anwender, speziell auch für die Bundesverwaltung und kritische Infrastrukturen, neue Risiken.“ (BSI, Bonn, 21. August 2013)

Besonders brisant ist, dass die geheimen Schlüssel während des Herstellungsprozesses außerhalb des Chips erzeugt und danach in den Chip übertragen werden. Hier ist es trivial, eine Kopie aller Schlüssel herzustellen. Es ist nicht auszuschließen, dass entsprechende Rechtsvorschriften bestehen und über diese nicht berichtet werden darf. Zur Abhilfe beitragen könnte eine internationale Kontrolle und Zertifizierung und eine Offenlegung der sicherheitsrelevanten Codeteile.

- Behinderung alternativer Betriebssysteme: In den Hardwareanforderungen für Windows 10 wird Secure Boot verpflichtend vorausgesetzt. Alternative

> Betriebssysteme können in der Praxis bisher nur mit technisch und rechtlich problematischen Notkonstruktionen starten.

Microsoft hat ohne nachvollziehbare Begründung konkurrierende Bootloader deaktiviert. Ein Szenario, in welchem Microsoft (möglicherweise durch US-Regierungsdruck) die Berechtigung für die von Microsoft unterschriebenen Bootloader für Linux-Distributionen zurückzieht, ist insbesondere für sicherheitskritische Systeme oder eingebettete Systeme höchst problematisch.

Aus Verbraucherschutzsicht problematisch ist, da es die freie Auswahl von konkurierensen Betriebssystemen behindert, auch, dass Microsoft die übliche Praxis verlassen hat und den Sicherheitschip automatisch einschaltet und sich dieser bei vielen Systemen selbst nicht mehr ausschalten lässt. Wünschenswert wären hingegen ein Opt-In, um die Verbraucherautonomie beim Eintritt in ein geschlossenes System sicherzustellen, und analog ein Opt-Out für die Verbraucherautonomie beim Austritt aus einem geschlossenen System.

10.2 Versagen einer geschlossenen Architektur

Durch einen groben Fehler ermöglichte Microsoft 2016 das Umgehen der gesamten Sicherheitsinfrastruktur. Die Tatsache, dass ein solcher die Sicherheitsarchitektur aushebender Fehler nun in der Praxis auftrat und auch nur schwer zu beheben ist, sollte zu einer Neubewertung von geschlossenen Systemen führen.

Microsoft Security Bulletin MS16-100 - Important Security Update for Secure Boot (3179577)

Published: August 9, 2016

> "Vulnerability Information Secure Boot Security Feature Bypass Vulnerability – CVE-2016-3320
>
> A security feature bypass vulnerability exists when Windows Secure Boot improperly loads a boot manager that is affected by the vulnerability. An attacker who successfully exploited this vulnerability could disable code integrity checks, allowing test-signed executables and drivers to be loaded onto a target device. Furthermore, the attacker could bypass Secure Boot Integrity Validation for BitLocker and Device Encryption security features.
>
> To exploit the vulnerability, an attacker who has gained administrative privileges or who has physical access to a target device could install an affected boot manager.The security update addresses the vulnerability by blacklisting affected boot managers. "

10.3 Alternative Vertrauensanker

Es ist zwingend notwendig, Alternativen zum Vertrauensanker von Microsoft zur Verfügung zu stellen. Aus technischen Gründen ist dies sogar deswegen notwendig, weil Microsoft mit einer Schlüssellänge von 2048 bit arbeitet, welche vom BSI nicht für langfristige Sicherheit empfohlen wird. Auch die Weiterverwendung von kryptographisch gebrochenen Verfahren (z. B. SHA-1) wird von der kryptographischen Forschung abgelehnt.

- Für den staatlichen Bereich könnte beispielsweise die Bundesnetzagentur eine führende Position einnehmen. Hier sind im Zusammenhang mit dem Signaturgesetz schon erhebliche Vorarbeiten vorgenommen worden.
- Für nichtstaatliche Bereiche erscheint eine gemeinnützige Stiftung außerhalb der USA die bessere Lösung. Als Beispiele könnten hier die Reformen bei ICANN und das verteilte Erzeugen von DNSSEC-Rootzonenschlüssel dienen.

11. Datenschutzfreundliche Kryptographie

Die Kryptographieforschung hat Lösungen für feingranulare Sicherheitspolitiken mit mathematisch beweisbaren Sicherheitseigenschaften entwickelt. Beispielsweise können Vertrauensbeziehungen durch mehrere mögliche Stellen dezentralisiert werden oder eine Zusammenarbeit von mehreren Instanzen erforderlich gemacht werden. Mit Hilfe geeigneter kryptographischer Protokolle kann man sich unter anderem Eigenschaften von Daten anonym attestieren lassen. Das kann konkret zum Beispiel Pflichtberatungsbescheinigungen von Sexarbeitern betreffen ebenso wie die Kundschaft von Versicherungen etc.

Als einfaches, konkretes Beispiel nehmen wir an, Jens will gegenüber seiner Autoversicherung beweisen, dass er an nicht mehr als 600 Minuten im Jahr schneller als 130 km/h gefahren ist. Jens kann natürlich seiner Versicherung den vollständigen Datensatz seines eingebauten Navigationsgerätes geben. Allerdings verrät er der Versicherung dann viel mehr über sich, als er für den Versicherungszweck eigentlich verraten muss. Zum Beispiel erfährt die Versicherung, ob Jens regelmäßig mit dem Auto zur Arbeit pendelt. Die datenschutzfreundliche Alternative für Jens ist, den vollen Datensatz anonym bei einem Treuhänder abzugeben. Der Treuhänder – das kann sogar die Versicherung selbst sein – weiß nicht, *wessen* Daten er unterschreibt, aber er unterschreibt, dass die Daten eine *bestimmte Bedingung* erfüllen. Jens gibt die Unterschrift an die Versicherung weiter. Die Versicherung erfährt nichts über die Daten von Jens, außer dass er die vertraglich festgelegte Bedingung eingehalten hat. Mit geeigneten kryptographischen Verfahren kann man sicherstellen, dass Jens der Versicherung nicht etwa die Unterschrift unter den Datensatz einer anderen Person unterjubeln kann, sondern nur die Unterschrift unter seinen eigenen Datensatz.

1982 entwickelte David Chaum die Idee der **Blinden Unterschrift**. Angenommen, Partei A hat ein Dokument D, dass sie von Partei B unterzeichnen lassen will, dessen Inhalt B aber nicht bekannt ist. Eine Blinde Unterschrift erlaubt es Partei A, Dokument D zu verschlüsseln, das verschlüsselte Dokument Partei B zum Unterschreiben vorzulegen und, gegeben die gültige Unterschrift von Partei B unter die verschlüsselte Fassung von D, daraus eine gültige Unterschrift für das unverschlüsselte Dokument D vorzulegen. Gegeben das Dokument D und die gültige Unterschrift, kann niemand, nicht einmal Partei B selbst, feststellen, wann und für wen sie dieses Dokument unterzeichnet hat. Anschaulich könnte man sich die Verschlüsselung von D so vorstellen, dass man D mit einem Stück Kohlepapier in einen Briefumschlag steckt und von B verlangt, die Unterschrift auf dem Briefumschlag zu leisten. Wenn A später den Briefumschlag öffnet, ist die Unterschrift von B, dank des Kohlepapiers, auf D durchgeschrieben.

Blinde Unterschriften können unter anderem dazu genutzt werden, digitales Geld zu erzeugen, dass ohne „Datenspuren“ gehandelt werden kann, ähnlich wie Geldmünzen. Immer, wenn eine Bank B für einen Kunden A eine, sagen wir, „Ein-Euro-Münze“ unterschreibt, bucht B einen Euro vom As Konto ab. A, und andere Kunden, geben ihre „Münzen“ bei Händlern aus. Den verschiedenen, von B selbst unterschriebenen „Münzen“ kann B nicht mehr ansehen, welche „Münze2 ursprünglich für welchen Kunden generiert wurde. („Protokolle ohne Wissensübertragung“) wurden 1985 von Goldwasser, Micali und Rackoff erfunden. Gemeinsam mit Babai und Moran gewannen sie 1993 für diese Arbeit den damals neu gestifteten Gödel-Preis. Die Kernidee bei einem Zero-Knowlege-Protokoll ist, dass man beweisen kann, dass man ein über ein bestimmtes Wissen verfügt, ohne dieses Wissen selbst preiszugeben. Quisquater, Guillou und Berson haben dafür, unter dem Titel "How to Explain Zero-Knowledge Protocols to Your Children" sehr anschaulich erklärt, was den Begriff des Protokolls ohne Wissensübermittlung ausmacht.

Grundsätzlich kann man mit Hilfe Blinder Unterschriften **Attestate** ausstellen. Dabei tritt allerdings das Problem auf, dass der Unterzeichner (der Treuhänder im Beispiel mit Jens und der Autoversicherung) möglicherweise zwar nicht alle Daten, die ihm Jens vorlegt, einsehen soll, aber sich davon überzeugen muss, dass bestimmte Werte im Datensatz bestimmte Eigenschaften haben. Letztlich muss Jens den Treuhänder mit Hilfe eines Zero-Knowledge-Protokolls von diesen Eigenschaften überzeugen. (Tatsächlich läuft das Protokoll natürlich zwischen den Computern von Jens und dem Treuhänder ab – die beteiligten natürlichen Personen brauchen selbst keine besondere Expertise.) Anders ausgedrückt, Blinde Unterschriften haben das offensichtliche Problem, dass der Unterzeichner B nicht weiß, und nicht wissen darf, was er unterzeichnet. Der Einsatz zum Erzeugen von „Münzen“ funktioniert unter anderen nur, wenn die Bank mit einem Schlüssel nur „Münzen“ eines bestimmten Wertes unterschreibt, also, z.B., für 50-Cent- 1-Euro- und 2-Euro-Münzen jeweils verschiedene Signaturschlüssel benutzt. Für die Anwendung der Anonymen Attestierung muss B sich sicher sein, dass in dem Dokument D bestimmte Sachverhalte, die B bestätigt, tatsächlich verzeichnet sind, ohne dass B das Dokument D wirklich lesen kann. Deshalb basieren Verfahren zur **Anonymen Attestierung** auf der Kombination von Zero-Knowledge-Protokollen (um den Unterzeichner B davon zu überzeugen, dass D das enthält, was B attestiert) mit Verfahren für anonyme Unterschriften (damit B nicht mehr über den Inhalt von D erfährt, als er unbedingt muss).

Das erste Verfahren zur anonymen Attestierung wurde 2004 von Brickell, Camenisch und Chen als „Direct Anonymous Attestation“ entwickelt und sollte für den Bereich des Trusted Computing eingesetzt werden. Noch im selben Jahr wurde auf bestimmte

Schwächen dieses Ansatzes hingewiesen. Die Arbeit von Smyth, Ryan und Chen (2015) gibt den aktuellen Stand der Forschung wieder.

Grundsätzlich kann man mit Protokollen zur Anonymen Attestierung zwei sich widerstrebende Sicherheitseigenschaften miteinander verbinden:

- Sicherheit gegen Datenfälschung (also die Sicherheit der Versicherung gegen mögliche Betrugsversuche von Jens) und
- Datenschutz (Sicherheit von Jens gegenüber dem Informationshunger seiner Versicherung).

12. Die Notwendigkeit der Datensparsamkeit

Beginnend mit dem Volkszählungsurteil des Bundesverfassungsgerichts (1983) hat sich in Deutschland ein weltweit beachtetes Datenschutzrecht in Gesetzgebung und Rechtsprechung entwickelt. Datensparsamkeit ist die verfassungsrechtlich und höchstrichterlich geforderte einzuhaltende Norm.

Auch aus rein technischer Sicht zeigt die Tatsache, dass gespeicherte Daten in der real existierenden IT-Welt (2016) nicht gesichert werden können, die Notwendigkeit eines verfassungsrechtlichen Schutzes.

- Grundannahme: **Jeder Technische Schutz für Daten versagt eines Tages**.

12.1 Generelle Hackbarkeit

Bedeutend für eine gesellschaftliche Einschätzung ist auch die Tatsache, dass neben den Diensten fremder Staaten auch Privatpersonen und Firmen in der Praxis recht einfach (in der Regel rechtswidrigen) Zugriff auf die heutigen Computersysteme erlangen können. Es haben sich hier Online-Marktplätze für ausnutzbare Sicherheitslücken (Zero-Days) gebildet, an denen sich in rechtlich problematischer Weise auch deutsche Dienste beteiligen. Die Preise sind schwankend, allerdings meist für höhere Einkommen und kleinere Firmen durchaus finanzierbar.

Heute müssen sich Datenschutzexperten daher auch in hoch konfliktäre Diskussionen einbringen. Das hier leider vorherrschende politische Diskussionsklima schreckt dabei verständlicherweise viele Wissenschaftler ab. Dennoch gebietet es die gesellschaftliche Verantwortung, darauf hinzuweisen, wenn technische Entwicklungen, wie eine allumfassende Überwachung oder die praktische Angreifbarkeit von Computersystemen, juristische Datenschutzsicherungen praktisch unwirksam werden lassen.

In der Computer-Sicherheitsforschung herrscht die Meinung vor, dass Daten auf vernetzten Computersystemen generell als hackbar anzusehen sind.

- **Wenn man nicht bereit ist, das Risiko einer möglichen Veröffentlichung von vertraulichen Daten einzugehen, darf man die Daten gar nicht erst speichern.**

12.2 Bilderkennung durch neuronale Netze

Auf der All Things Digital D9 Konferenz 2011 erklärte der vormalige Google-CEO Erik Schmidt eine bemerkenswerte Einsicht zu den Risiken der Gesichtserkennung:

> „We built that technology and we withheld it. As far as I know, it's the only technology Google has built and, after looking at it, we decided to stop."
>
> „I'm very concerned personally about the union of mobile tracking and face recognition." (Huffington Post 01.08.2011)

Da in sozialen Netzwerken häufig auch Fotos von Nichtmitgliedern veröffentlicht und mit Namen versehen werden, betrifft die Gefährdung auch Menschen, die selbst nicht Mitglieder in diesen sozialen Netzen sind.

Weniger Bedenken zeigten 2016 die russischen Entwickler der App FindFace. Durch die Verknüpfung mit dem Facebook ähnlichen sozialen Netzwerk vk.com und einem den Google-Verfahren qualitativ nicht nachstehenden Gesichtserkennungsalgorithmus wurde eine sehr hohe Erkennungsrate erreicht. Die allgemeine Zugänglichkeit der App führte zu unangenehmen sozialen Auswirkungen.

Global Voices, Posted 22 April 2016:

Facial -Recognition Service Becomes a Weapon Against Russian Porn Actresses

"On April 9, three days after the media reported on Tsvetkov's art project, users of the Russian imageboard "Dvach" (2chan) launched a campaign to deanonymize actresses who appear in pornography. After identifying these women with FindFace, Dvach users shared archived copies of their Vkontakte pages, and spammed the women's families and friends with messages informing them about the discovery. The effort also targeted women registered on the website "Intimcity," which markets prostitution services."

- Wir halten es weder für wünschenswert noch für realistisch, den Einsatz von Software zur Gesichtserkennung grundsätzlich zu verbieten. Grundsätzlich sollte der Anbieter eines Dienstes verpflichtet werden, auf die Gesichtserkennung hinzuweisen, falls er sie einsetzt. Vor allem glauben wir aber, **dass die technischen Möglichkeiten zur Gesichtserkennung in großem Umfang, und die damit verbundenen Risiken für die Verbraucher, viele unserer anderen Handlungsempfehlungen noch dringlicher machen, also sie ohne diese Möglichkeiten sowieso schon wären.**

12.3 Daten von besonders gefährdeten Personengruppen

Wer Daten speichert, oder eine Verpflichtung zum Speichern bestimmter Daten einführt, muss die Vorteile, die sich aus einer Speicherung ergeben, mit den Nachteilen, die sich aus einer Veröffentlichung der Daten ergeben würden, abwägen – selbst wenn eine Veröffentlichung der Daten nicht vorgesehen ist. Es genügt keinesfalls, die Daten nur rechtlich zu sichern (also, ihre Veröffentlichung zu verbieten bzw. unter Strafe zu stellen). Es genügt nicht einmal, die Daten, zusätzlich zu dem juristischen Schutz auch technisch zu schützen, mit Maßnahmen, die dem Stand der Technik entsprechen. Denn nicht einmal die Kombination von rechtlichen und technischen Sicherungsmaßnahmen gibt eine Garantie dafür, dass die Daten auf Dauer geheim bleiben. Erwachsen aus einer möglichen Veröffentlichung besonders schwere Nachteile für die Betroffenen, oder sogar eine Gefahr für Leib und Leben, müssen die Vorteile einer Speicherung diesen Nachteilen und Gefahren gegenübergestellt werden.

Kritisch muss man, in dem Zusammenhang, ein aktuelles Gesetz betrachten. Dieses Gesetz sieht eine Pflichtregistrierung von Sexarbeiterinnen und Sexarbeitern vor. Dieses Vorgehen wurde vom Bundesrat, Frauenrechtlerinnen, Sozialorganisationen, Datenschützern und Verfassungsrechtlern heftig kritisiert. Von den Berufsvertreterinnen wurde in diesem Zusammenhang neben der Sorge vor staatlicher Diskriminierung und gesellschaftlicher Ächtung durch religiösen oder politischen Fanatismus auch auf eine erhöhte Gefahr für Leib und Leben hingewiesen.

Während die beiden ersten Punkte Teil einer verbittert geführten Diskussion sind, auf die hier nicht näher eingegangen werden soll, ist es unstrittig, dass angesichts der erhöhten Gefährdung der zugesicherte juristische Datenschutz in keiner Weise als ausreichend angesehen werden kann. Vom Gesetzgeber in keiner Weise ausreichend gewürdigt, ist die Mehrfachgefährdung von homosexuellen und transsexuellen Sexarbeitern (*siehe auch:* Biselli, Anna, *CDU/CSU sind stolz: „Im Prostitutionsgewerbe wird es keine Anonymität mehr geben.“*, netzpolitik.org, 17.05.2015).

12.4 Handlungsempfehlungen

- Datenregister, welche zu erheblichen Gefährdungen von ganzen Menschengruppen führen könnten, wie die historisch belasteten „Rosa Listen“ und Sexarbeiterregister, sollten aus moralischen Gründen nicht eingerichtet werden.
- Rechtswidrige Speicherungen innerhalb von Landespolizeien sind abzustellen.
- Bescheinigungen über Pflichtberatungen sind durch kryptographische Methoden zu anonymisieren.
- Ausweispflicht für Sexarbeiter ist abzulehnen. **Ein Foto im Ausweis stellt wegen den Fortschritten bei neuronalen Netzen selbst bei einer vorgesehenen Pseudonymverwendung eine unakzeptable Gefährdung dar.**
- Die im Gesetz vorgesehene Weitergabe den persönlichen Intimbereich betreffende Daten für statistische Zwecke ist abzulehnen. **Mindestforderung ist ein Schutz der Daten durch Techniken der Differential Privacy.**

13. Vertrauliche Daten in statistischen Datenbanken

13.1 K-Anonymität

Das Sammeln sensibler Daten in Datenbanken und die statistische Auswertung dieser Daten wird schon seit langem betrieben, aber erst seit Anfang des 21. Jahrhunderts wurde nach Methoden gesucht, die Beeinträchtigung der Vertraulichkeit zu spezifizieren und zu minimieren. Einer der ersten Ansätze dazu stammt von Latanya Sweeney, die K-Anonymität. Die Daten einer Person sind nicht von den Daten von mindestens K-1 anderer Personen unterscheidbar. Leider kann es sein, dass eine Gruppe von mindestens K Personen ein sensibles Merkmal teilt. Wenn man z. B. abspeichert, welche Personen in einer Datenbank HIV-positiv sind, und eine Zielperson ist Teil einer Gruppe von K HIV-Positiven, dann ist klar, dass die Zielperson selbst HIV-positiv ist.

Neuere Ansätze, den Schwächen der K-Anonymität zu begegnen, sind die L-Diversität und die T-Nähe (t-closeness). Die Entwicklung ist im Fluss.

13.2 Differentielle Vertraulichkeit

2006 entwickelte Cyntia Dwork die Differentielle Vertraulichkeit. Siehe auch Dwork, Roth (2015). Die Differentielle Vertraulichkeit ist eine mathematisch äußerst wirkungsvolle Methode, den (maximal möglichen) Verlust an Vertraulichkeit zu messen, der durch die Auswertung anonymisierter persönlicher Daten entstehen kann. Auch wenn dieser Ansatz erst zehn Jahre alt ist, ist er bereits gut erforscht und verstanden. **Wer vertrauliche Daten in statistischen Datenbanken verarbeitet, ist gut beraten, die Vertraulichkeit dieser Daten mit diesem Ansatz zu kontrollieren.**

Man beachte, dass der Einsatz der differentiellen Vertraulichkeit an sich keinen Datenschutz garantiert! Mit der differentiellen Vertraulichkeit kann man einen Verlust an Vertraulichkeit messen bzw. festlegen. Es gibt die **ε**-differentielle und die (**ε**, **δ**)-differentielle Vertraulichkeit. **Vertraulichkeit bedeutet, dass ε und δ nicht zu groß sind.** Bei den Lösungsvorschlägen geben wir sinnvolle Schranken für ε und δ an.

13.3 Lösungsvorschlag: Einsatz von Methoden der Differentiellen Vertraulichkeit

Dem aktuellen Stand der Forschung entsprechend schlagen wir vor, dass sensible statistische Daten stets mit **Methoden der differentiellen Vertraulichkeit** verarbeitet werden sollen. Diese verbinden einen hohen wissenschaftlichen Nutzen in statistischen Anwendungsszenarien mit zahlreichen Benutzern und gleichzeitig ein quantifizierbar-kleines Maß an Verlust der Vertraulichkeit für die einzelnen Verbraucher, von denen die Daten stammen. Dies entspricht der Idee der **Privacy by Design.**

Sind X und Y zwei Datenbanken, aus identischen Rohdaten, bis auf einen zusätzlichen Eintrag in Y, dann gilt bei der ε-differentiellen Vertraulichkeit: Die Wahrscheinlichkeit, dass ein Auswertungsalgorithmus A mit Zugriff auf X ein bestimmtes Ergebnis liefert, ist um nicht mehr als den Faktor $\mathbf{e^{\varepsilon}}$ („e hoch epsilon“) kleiner oder größer sein als die Wahrscheinlichkeit, dass A mit Zugriff auf Y dieses Ergebnis liefert:

$$\mathbf{Pr[A(X) = 1] * e^{-\varepsilon} <= Pr[A(Y) = 1] <= e^{\varepsilon} * Pr[A(X) = 1]}$$

Man beachte, dass in der linken (unteren) Schranke der Faktor („e hoch **minus** epsilon“) steht, in der rechten (oberen) Schranke dagegen („e hoch epsilon“).

Vereinfacht gesagt ist **ε** das Maß für den Verlust an Vertraulichkeit, den ein Nutzer durch den Eintrag in die Datenbank höchstens erleidet.

Für viele Anwendungen ist die **ε**-differentielle Vertraulichkeit leider zu restriktiv – mit einer gewissen (geringen!) Wahrscheinlichkeit kann der Verlust an Vertraulichkeit das durch **ε** angegebene Maß übersteigen. Der Wert **δ bezeichnet** diese Wahrscheinlichkeit. Anders ausgedrückt, die **ε**-differentielle Vertraulichkeit ist der Spezialfall der (**ε**, **δ**)-differentiellen Vertraulichkeit, bei der die Wahrscheinlichkeit **δ=0** ist. Die **ε**-differentielle Vertraulichkeit kann man entsprechend auch als (**ε**, **0**)-differentielle Vertraulichkeit bezeichnen.

Bleibt die Frage, wie groß **ε** und ggf. **δ** maximal sein dürfen. Naturgemäß gibt es keine Schranke, bis zu der **ε** unbedenklich und ab der **ε** schlecht ist. Doch im wissenschaftlichen Alltag ist es üblich geworden, eine Wahrscheinlichkeit von **5%** als Grenze für die „Signifikanz“ anzusehen.

Parametervorschlag

Für die **ε**-differentielle Vertraulichkeit schlagen wir als absolute Obergrenze den Wert

$$\mathbf{\varepsilon <= 0{,}0488}$$

vor. Dann ist $\mathbf{e^{\varepsilon} <= 1.05}$.

Kann dieser Wert mit der Wahrscheinlichkeit **δ > 0** verletzt werden, sollte **ε** zur Kompensation entsprechend verringert werden. Für die (**ε**, **δ**)-differentielle Vertraulichkeit schlagen wir deshalb die folgende Obergrenze vor:

$$\mathbf{\varepsilon + \delta * 2 <= 0{,}0488}.$$

Ist zum Beispiel **δ=1%**, dann muss **ε <= 0.0288** gelten.

14. Grundlagenforschung für den Verbraucherschutz

Eine der Schlüsseltechnologien, um Verbrauchern in der digitalen und immer mehr vernetzten Medienwelt ein Höchstmaß an digitaler Souveränität zu ermöglichen, ist die Kryptographie:

- Bereits heute werden kryptographische Protokolle wie TLS (Transport Layer Security) routinemäßig genutzt, um im Internet eine vertrauliche und authentische Kommunikation zwischen einem Klienten (also dem Verbraucher, bzw. dem Computer des Verbrauchers) und einem Server zu etablieren. Ohne TLS könnte man zum Beispiel im Internet nicht sicher einkaufen und bezahlen. Leider wird TLS regelmäßig von gravierenden Sicherheitslücken geplagt. Eine Übersicht bieten Meyer, Schwenk (2013), auch wenn die Arbeit nicht mehr aktuell ist.
- Die Methode der differentiellen Vertraulichkeit bietet, wie an anderer Stelle geschildert, die Möglichkeit, gute Daten für die statistische Auswertung zu sammeln, wie sie unter anderem für medizinische Forschung gebraucht werden, ohne die digitale Souveränität der Patienten zu verletzten. Die differentielle Vertraulichkeit wird aber in der Praxis bei weitem nicht überall genutzt, wo sie nützlich wäre.
- Bisher noch kaum genutzt wird der ebenfalls an anderer Stelle erwähnte Ansatz, Eigenschaften von Daten anonym attestieren zu lassen. Auch wenn der grundlegende Ansatz seit langem bekannt ist, muss für bestimmte Anforderungen bzw. ein bestimmtes Datenproblem jeweils ein geeignetes Protokoll entwickelt werden. Protokolle für die anonyme Attestierung sind, quasi, „maßgeschneidert“ für bestimmte Anwendungen.

Diese Liste von Anwendungen der Kryptographie ließe sich beliebig verlängern. Im Sinn der digitalen Souveränität gibt es viele Herausforderungen für die Forschung in der Kryptographie:

- Im Bereich der Grundlagenforschung ist zum Beispiel die Entwicklung kryptographischer Protokolle dringlich, die auch dann noch sicher sind, wenn es funktionsfähige Quantencomputer gibt (Post-Quantum Kryptographie; keines der in TLS verwendeten Verfahren zum Schlüsselaustausch ist Post-Quantum-sicher). Eine Einführung bietet die Arbeit von Bernstein (2009)

- Bei der angewandten Forschung betrifft dies unter anderem Verbesserungen beim Einsatz der differentiellen Vertraulichkeit.
- Ebenfalls dringlich ist ein stärkerer Fokus der Kryptographischen Forschung auf Robustheit, d.h., auf die Entwicklung von Kryptosystemen, die bei typischen Implementationsfehlern, oder wenn kryptographische Grundoperationen sich als nicht ganz so sicher herausstellen, wie ursprünglich angenommen, nicht unmittelbar alle wünschenswerten Sicherheitseigenschaften verlieren. (Die meisten der unten angegebenen Referenzen beziehen sich auf verschiedene Formen der Robustheit.)
- Tatsächlich beruhen viele bekannte Angriffe auf wichtige Sicherheitsprotokolle nicht auf einer Schwäche des Protokolls selbst, sondern auf einer fehlerhaften Implementation des jeweiligen Protokolls. Zum Beispiel gilt dies für den berühmten „Heartbleed“-Fehler in OpenSSL. OpenSSL selbst ist die am weitesten verbreitete TLS-Bibliothek. Für Hunderttausende von Web-Servern wurde es durch Heartbleed nötig, die Schlüssel zu wechseln. Der Kern von Heartbleed und vielen ähnlichen Fehlern besteht in der fehlerhaften Verarbeitung ungültiger Eingaben für die kryptographischen Funktionen, siehe Bratus et al. (2014) und Sassaman et al. (2012).

15. Systemrelevante Open-Source Softwareprojekte

Die genannten Open-Source Projekte stellen systemrelevante Sicherheitssoftware für den Erhalt der digitalen Souveränität dar. Eine nachhaltige Sicherung dieser Projekte ist wichtig für die digitale Souveränität und damit auch Aufgabe staatlicher Stellen. Aufgrund der vielen ehrenamtlichen Projektteilnehmer sind die entstehenden Kosten gering. Die Offenen Lizenzen garantieren die Nachhaltigkeit

- **TrueCrypt/VeraCrypt: Speicherverschlüsselungt**

Firmengeheimnisse und andere vertrauliche Daten sollten immer verschlüsselt gespeichert werden – vor allem, auf mobilen Geräten, die leicht gestohlen werden können. Das vielfach dafür genutzte Truecrypt wird offiziell nicht mehr weiterentwickelt, aber die offene Lizenz erlaubte eine Weiterentwicklung unter dem Namen Veracrypt.

- **Open SSH: Kommunikations-Sicherheit**

Open SSH dient unter anderem der abhör- und fälschungssicheren Übermittlung von Steuerinformationen an eingebettete Systeme oder Internetserver.

- **Open SSL: Datentransport-Sicherheit**

TLS (Transport Layer Security) ist das im Internet am meisten genutzte Sicherheitsprotokoll. Leider gibt es immer wieder Sicherheitslücken im TLS-Protokoll, oder in einzelnen TLS-Bibliotheken. Open SSL ist die meistgenutzte und deshalb wichtigste TLS-Bibliothek.

- **GNU Privacy Guard: Anwendungs-Sicherheit**

Der GNU Privacy Guard wurde zum Versenden von verschlüsselten und unterschriebenen E-Mails nach dem Open PGP Standard entwickelt. GnuPG ist auch wichtig, um die Herkunft und Echtheit von Sicherheitsupdates zu überprüfen.

- **Das TOR Projekt: Anonym Surfen**

Mit Hilfe des TOR-Browsers kann man im Netz surfen, ohne seine Identität zu verraten. Das TOR Projekt wird momentan vorwiegend vom US Verteidigungsministerium finanziert.

16. Zusammenfassung und Handlungsempfehlungen

In diesem Kapitel fassen wir unsere wesentlichen Erkenntnisse und Handlungsempfehlungen zusammen. Ausführlicher werden die Erkenntnisse und auch die Handlungsempfehlungen in den jeweiligen Kapiteln behandelt.

16.1 Kurzfristige Handlungsempfehlungen

Wir beginnen mit einigen Empfehlungen, die aus unsere Sicht kurzfristig umsetzbar sind.

- Alternative Vertrauensanker
    - Es ist zwingend notwendig, zeitnah Alternativen zum Vertrauensanker von Microsoft zur Verfügung zu stellen.
    - Für den staatlichen Bereich könnte beispielsweise die Bundesnetzagentur eine führende Position einnehmen. Hier sind im Zusammenhang mit dem Signaturgesetz schon erhebliche Vorarbeiten vorgenommen worden.
    - Für nichtstaatliche Bereiche erscheint eine gemeinnützige Stiftung außerhalb der USA die bessere Lösung. Als Beispiele könnten hier die Reformen bei ICANN und das verteilte Erzeugen von DNSSEC-Rootzonenschlüssel dienen.
- Schutz gefährdeter Personengruppen
    - Beim Schutz von besonders gefährdeten Personengruppen ist zu beachten, dass insbesondere die technischen Möglichkeiten zur Gesichtserkennung in großem Umfang, und die damit verbundenen Risiken, viele unserer Handlungsempfehlungen noch dringlicher machen, also sie ohne diese Möglichkeiten sowieso schon wären. (Siehe Abschnitt 12.4.)
- Vorratsdatenspeicherung
    - Abschaffung der Vorratsdatenspeicherung.
- Wahl der Darstellung
    - Wir sehen keinen aktuellen gesetzgeberischen Handlungsbedarf beim Recht auf Wahl der Darstellung. Technologien, die das Recht auf Wahl der Darstellung einschränken, und Technologien, die das Recht auf Wahl der Darstellung wiederherstellen, stellen ein für Verbraucher wie für Inhaltsanbieter akzeptables Gleichgewicht her.

- Wichtig ist jedoch, dass Verbraucherschützer sich möglichen Initiativen, dieses Gleichgewicht zu Gunsten der Inhaltsanbieter zu verschieben und verbraucherfreundliche Technologien einzuschränken oder zu verbieten, entgegenstellen, siehe Abschnitt 5.

16.2 Mittelfristige Empfehlungen

In vielen Bereichen, die die Autoren dieser Studie beschrieben haben, sehen die Autoren dieser Studie nicht in der Lage, kurzfristig (etwa innerhalb der nächsten ein bis zwei Jahre) umsetzbare Handlungsempfehlungen zu geben.

Sie empfehlen jedoch, jetzt bereits zu damit beginnen, Handlungsoptionen zu entwickeln, die mittelfristig (innerhalb der nächsten höchstens fünf Jahre) konkret umsetzbar sein sollten:

- Plausible Ansätze, das Recht auf Vergessenwerden (bzw. das Recht auf Löschen) durchzusetzen, sollen unterstützt werden. Ggf. können Anbieter von sozialen Netzwerken und anderen Online-Diensten verpflichtet werden, ihren Kunden entsprechende Optionen anzubieten, wie in Abschnitt 4.3 beschrieben.
- Das Scoring von Verbrauchern verspricht, wirtschaftlich extrem wichtig zu werden und auch massive Auswirkungen auf die Digitale Souveränität der Verbraucher zu haben.
- Eine wichtige Rolle bei verbraucherfreundlichen Regelungen von Scoring und Datenhandel werden Audits der Algorithmen durch unabhängige Sachverständige spielen – was zunächst einmal eine Implementation der Algorithmen voraussetzt, die Audits überhaupt ermöglicht (eine Art „Audit-Schnittstelle“).
- Eine gesellschaftliche Diskussion und weitere Forschung zum Thema Scoring sind von großer Bedeutung. Erst wenn beides stattgefunden hat, wird es möglich werden, konkrete Lösungsansätze zu erarbeiten.
- Die Sicherheit im Internet of Things muss dringend – und möglichst in Form einer internationalen Verständigung – weiterentwickelt werden. Dazu gehören die Verpflichtung zum Schreiben von Sicherheitsupdates durch die Hersteller sowie die Offenlegung der Quelltexte als Open-Source Dokumente nach Ablauf der Lebenszeit, bzw. wenn der Hersteller seiner Verpflichtung, Sicherheitsupdates zu Entwicklern, nicht nachkommt.

- Das Triumvirat aus
  - Privacy by Design,
  - Authenticity by Design und
  - Availability by Design

als wesentliche Eigenschaften von Informations- und Kommunikationssystemen muss weiterentwickelt und im Rahmen einschlägiger Vorschriften verankert werden. Bisher wurden Authenticity by Design und Availability by Design stark vernachlässigt.

16.3 Schaffen notwendiger Voraussetzungen

Die aktuelle Entwicklung des Digitalen Verbraucherschutzes ist durchaus besorgniserregend. Seit dem Urteil des Bundesverfassungsgerichts zur Volkszählung von 1983 wurde in Deutschland ein Datenschutzrecht entwickelt und in seinen Kernideen inzwischen von der Europäischen Union übernommen, um das der Rest der Welt Europa beneidet. Diese Errungenschaft muss gegen kurzfristige Partikularinteressen verteidigt werden. Digitaler Verbraucherschutz ist nicht nur im Interesse der Verbraucher. Er kann auch, als mögliches europäisches Alleinstellungsmerkmal in der Digitalen Welt, für europäische Anbieter zu einem echten wirtschaftlichen Vorteil führen, auf einem bisher vor allem von amerikanischen Großunternehmen dominierten Markt.

Zu den wesentlichen Herausforderungen eines Verbraucherschutzes, der die Digitale Souveränität der Verbraucher sicherstellt, gehören insbesondere die folgenden:

- Der Grundsatz der Datensparsamkeit ist mit Nachdruck zu verteidigen bzw. wieder in Erinnerung zu rufen, gegenüber staatlichen Datenverarbeitern genauso wie gegenüber den Anbietern von informationsverarbeitenden Dienstleistungen.
- Verstärkt muss der Einsatz von datenschutzfreundlichen kryptographischen Methoden zur Verarbeitung persönlicher Informationen in statistischen Datenbanken und zur anonymen Attestierung eingefordert und ggf. auch vorgeschrieben werden.
- Es wird zunehmend wichtiger, die Grundlagenforschung in einschlägigen Gebieten und die Weiterentwicklung geeigneter Open-Source Software zu unterstützen.

Gesamtverzeichnis Literatur und Quellen

- Abed, Forler, List, Lucks, Wenzel: RIV for Robust Authenticated Encryption. FSE 2016: 23-42
- Abed, Berti, Lucks: Insecurity of RCB: Leakage-Resilient Authenticated Encryption. IACR Cryptology ePrint Archive 2016: 1121 (2016)
- Admiral: Website von Firstcarquote.
- Aggarwal, Charu C.; Yu, Philip S. (2008). "A General Survey of Privacy-Preserving Data Mining Models and Algorithms". Privacy-Preserving Data Mining – Models and Algorithms. Springer. pp. 11–52
- Andreeva, Bogdanov, Luykx, Mennink, Mouha, Yasuda, How to Securely Release Unverified Plaintext in Authenticated Encryption. ASIACRYPT (1) 2014: 105-125
- BamS, Digitale Souveränität zurückgewinnen. Interview mit Alexander Dobrindt, 22.12.2013
- Barr, Alistair, Google Mistakenly Tags Black People as ‘Gorillas,’ Showing Limits of Algorithms, The Wall Street Journal, 01.07.2015
- Barwell, Page, Stam: Rogue Decryption Failures: Reconciling AE Robustness Notions. IMA Int. Conf. 2015: 94-111
- Bernstein: *Introduction to post-quantum cryptography*. *2009*
- Biselli, Anna, CDU/CSU sind stolz: „Im Prostitutionsgewerbe wird es keine Anonymität mehr geben.“, netzpolitik.org, 17.05.2015
- Bitkom 2015. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., *Digitale Souveränität. Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa*, 2015
- BMI 2013. TNS Infratest für den IT-Planungsrat beim Bundesministerium des Innern, Zukunftspfade Digitales Deutschland 2020, Oktober 2013
- BMWi 2015, Monitoring-Report Wirtschaft DIGITAL 2015, TNS Infratest für Bundesministerium für Wirtschaft und Energie, Oktober 2015
- BMWi 2015a, *Leitplanken Digitaler Souveränität*, zum 9. IT-Gipfel 19.11.2015

- Bosker, Bianca, *Facial Recognition: The One Technology Google Is Holding Back*, The Huffington Post, 01.06.2011
- Bratus, Darley, Locasto, Patterson, Shapiro, Shubina: Beyond Planted Bugs in "Trusting Trust": The Input-Processing Frontier. IEEE Security & Privacy 12(1): 83-87 (2014)
- Brickell, Camenisch, Chen (2004). *"Direct Anonymous Attestation"* (PDF). ACM Conference on Computer and Communications Security: 132–145.
- Brickell, Chen; Li (2009). *"Simplified security notions of Direct Anonymous Attestation and a concrete scheme from pairings"*.Jornal of lomputing, Philadelphia: *Society for Industrial and Applied Mathematics*, 18 (1): 186–208
- Chaum, David (1983). *"Blind signatures for untraceable payments"* (PDF). Advances in Cryptology Proceedings of Crypto. 82 (3): 199–203.-- 2nd International System Administration and Networking Conference, Amsterdam, 2004.
- Dwork, C., Differential privacy. In Proceedings of the International Colloquium on Automata, Languages and Programming (ICALP), 2006.
- Dwork, C. ; Roth, A., *The Algorithmic Foundations of Differential Privacy* (PDF). Foundations and Trends in Theoretical Computer Science. Now Publishers, 2015.1
- Facebook Platform Policy, o.D.
- Generali, Pressemitteilung: Versicherung neu denken: Generali Vitality geht an den Start, 23.06.2016
- Goldwasser, S.; Micali, S.; Rackoff, C. (1989), *"The knowledge complexity of interactive proof systems"* (PDF), SIAM Journ
- Greis, Friedhelm, Kaum ein Monat ohne gehackte Autos, Golem, 07.09.2015
- Heath, Alex, Facebook will fight the lawsuit that claims its 'ethnic affinities' ad targeting tool is illegal, Business Insider Deutschland, 7.11.2016
- Hern, Alex, Facebook's 'ethnic affinity' advertising sparks concerns of racial profiling, The Guardian, 22.03.2016
- Hoang, Reyhanitabar, Rogaway: Online Authenticated-Encryption and its Nonce-Reuse Misuse-Resistance. CRYPTO (1) 2015: 493-517

- Hoang, Krovetz, Rogaway: Robust Authenticated-Encryption AEZ and the Problem That It Solves. EUROCRYPT (1) 2015: 15-44
- Katz, Lucks, Thiruvengadam: Hash Functions from Defective Ideal Ciphers. CT-RSA 2015: 273-290
- Koalitionsvertrag 2013. Deutschlands Zukunft gestalten, Koalitionsvertrag zwischen CDU, CSU und SPD, 18. Legislaturperiode, 27.11.2013
- Krempl, Stefan, IT-Gipfel: Gabriel plädiert für Datensouveränität statt Datenschutz, Heise Online, 19.11.2015
- Krempl, Stefan, Reichtum statt Sparsamkeit: Dobrindt will Datenschutz lockern, Heise Online, 17.11.2016
- Li, Ninghui; Li, Tiancheng; Venkatasubramanian, S. (April 2007). *"t-Closeness: Privacy Beyond k-Anonymity and l-Diversity"*. IEEE 23rd International Conference on Data Engineering, 2007. ICDE 2007: 106–115.
- Maas, Heiko, Internet-Charta: Unsere digitalen Grundrechte, Zeit Online, 10.12.2015
- Machanavajjhala, Ashwin; Kifer, Daniel; Gehrke, Johannes; Venkitasubramaniam, Muthuramakrishnan (March 2007). *"L-diversity: Privacy Beyond K-anonymity"*. ACM Trans. Knowl. Discov. Data. **1** (1).
- Maheshwari, Sapna und Mike Isaac, Facebook Will Stop Some Ads From Targeting Users by Race, New York Times, 11.11.2016
- Marco Civil da Internet, Lei No. 12.965, de 23 de Abril de 2014, Diário Oficial da União, República Federativa do Brasil, 24.04.2014 (inoffizielle englische Übersetzung, o.A., 25.03.2014)
- Meyer, Schwenk: Lessons Learned From Previous SSL/TLS Attacks - A Brief Chronology Of Attacks And Weaknesses. IACR Cryptology ePrint Archive 2013: 049 (2013)
- Microsoft Security Bulletin MS16-100 – Important Security Update for Secure Boot (3179577), Published: August 9, 2016
- NDR, Nackt im Netz: Millionen Nutzer ausgespäht, Panorama 3, 01.11.2016
- Quisquater, Jean-Jacques; Guillou, Louis C.; Berson, Thomas A. (1990). *"How to Explain Zero-Knowledge Protocols to Your Children"*.

- Reinbold, Fabian, Facebook, Google und Co.: Warum Merkel an die Algorithmen will, Spiegel Online, 26.10.2016
- Rogaway, Shrimpton: A Provable-Security Treatment of the Key-Wrap Problem. EUROCRYPT 2006: 373-390
- Róna-Tas, Ákos und Stefanie Hiß, Das Kreditrating von Verbrauchern und Unternehmen und die Subprime-Krise in den USA mit Lehren für Deutschland, Schufa, Wiesbaden, September 2008
- Rothrock, Kevin, Facial Recognition Service Becomes a Weapon Against Russian Porn Actresses, Global Voices, 22.04.2016
- Ronen, E., O'Flynn, C., Shamir, A., Weingarten, A.: IoT Goes Nuclear: Creating a ZigBee Chain Reaction. IACR Cryptology ePrint Archive 2016: 1047 (2016).
- Ruddick, Graham, Admiral to price car insurance based on Facebook posts, The Guardian, 02.11.2016
- Sassaman, Patterson, Bratus, Locasto: Security Applications of Formal Language Theory. IEEE Systems Journal 7(3): 489-500 (2013)
- Schröder, Michael und Jürgen Taeger (Hrsg.), Scoring im Fokus: Ökonomische Bedeutung und rechtliche Rahmenbedingungen im internationalen Vergleich, BIS-Verlag der Carl von Ossietzky Universität Oldenburg 2014
- Schufa, Was ist Scoring?, o.D.
- Schulzki-Haddouti, Christiane, Digitaler Souveränitätsverlust. Deutschen Behörden entgleitet die Kontrolle über kritische IT-Systeme, 21.08.2015
- Smyth, Ryan, (2015). *"Formal analysis of privacy in Direct Anonymous Attestation schemes"* (PDF). Science of Computer Programming. **111** (2).
- Spiegel Online, Amazon löscht digitale Exemplare von "1984", 20.07.2009
- Sweeney, L. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570.
- Wagener, Andreas, Predictive Profiling: Mieter und ihre Integrität anhand des Social Media Verhaltens einschätzen, Nerdwärts, 22.06.2016
- Weichert, Thilo und Karin Schuler, Datenschutz contra Wirtschaft und Big Data? Eine politische Fehlentwicklung, Netzwerk Datenschutzexpertise, 31.12.2015

- Weis, R., Modern Security Architectures, NLLUG Najaarconferentie Security, De Reehorst, 2003.
- Weis, R., Ist Trusted Computing wirklich vertrauenswürdig, Tagungsband ZEI, Koenig, Ch./Neumann, A./Katzschmann, T. (Hrsg.), Vertrauenswürdige Systemumgebungen, Heidelberg 2004a.
- Weis, R., Trusted Computing: Chancen und Risiken, Datenschutz und Datensicherheit, DuD 11/04, Vieweg, 2004b.
- Weis, R., "Kryptographie nach Snowden", in: "Überwachtes Netz – Edward Snowden und der größte Überwachungsskandal der Geschichte", Hrsg: Markus Beckedahl und Andre Meister, Verlag epubli Berlin 2014a.
- Weis, R, "Vor Windows 8 wird gewarnt" in: "Jahrbuch Netzpolitik 2014',, Hrsg: Markus Beckedahl, Anna Biselli und Andre Meister, Verlag epubli Berlin 2014b.
- Weis, R., "Trusted Computing sowie ergänzende und alternative Techniken zur Gewährleistung von IT-Sicherheit", - 13. @kit-Kongress – 3. Forum „Kommunikation & Recht“, Datenschutz und Datensicherheit als Herausforderung des Rechts, 22./23. Mai 2014c – Berlin
- Weis, R., Lucks, S., Bogk, A., TCG 1.2 - fair play with the 'Fritz' chip?, SANE 2002.
- YouGov, Pressemitteilung: YouGov-Studie „Quantified Health“. Self-Tracking: Rund jeder Dritte würde gesundheitsbezogene Daten an Krankenversicherer weitergeben, 20.01.2015
- Zaks, R.: Mein erster Computer. Sybex-Verlag, 1981.

Danksagungen

Ausdrücklich bedanken möchten wir uns für die gute Zusammenarbeit und die zahlreichen Anmerkungen von Mitgliedern des Sachverständigenrates und den Mitarbeiterinnen und Mitarbeitern des Bundesministeriums für Justiz und Verbraucherschutz, insbesondere bei Lucia Reisch, Gesche Joost, Thomas Fischer, Irina Domurath, Christian Groß und Marco Stoll.

Sachverständigenrat für Verbraucherfragen

Der Sachverständigenrat für Verbraucherfragen ist ein Beratungsgremium des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV). Er wurde im November 2014 vom Bundesminister der Justiz und für Verbraucherschutz, Heiko Maas, eingerichtet. Der Sachverständigenrat für Verbraucherfragen soll auf der Basis wissenschaftlicher Erkenntnisse und unter Berücksichtigung der Erfahrungen aus der Praxis das Bundesministerium der Justiz und für Verbraucherschutz bei der Gestaltung der Verbraucherpolitik unterstützen.

Der Sachverständigenrat ist unabhängig und hat seinen Sitz in Berlin.

Vorsitzende des Sachverständigenrats ist Prof. Dr. Lucia Reisch.

SVRV Sachverständigenrat für Verbraucherfragen