Sonderthema: Die digitale Welt
Wie Big Data unseren Alltag verändert

VORSCHAU I
Die Elektromobilität soll im nächsten Jahr wichtige Impulse erhalten **SEITE 14**

VORSCHAU II
Die Flüchtlingskrise wird auch 2016 im Fokus stehen **SEITE 15**

DasParlament

Berlin, 04. Januar 2016 | www.das-parlament.de | 66. Jahrgang | Nr. 1-2 | Preis 1 € | A 5544

KOPF DER WOCHE

Bald Chef für Bundesamt

Arne Schönbohm Bundeskanzler war sein Berufsziel als Kind laut einem Fragebogen. Jetzt wird Sicherheitsexperte Arne Schönbohm erst einmal Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI). Zum 1. Februar folgt er auf Wunsch von Bundesinnenminister Thomas de Maizière (CDU) Michael Hange, der altersbedingt ausscheidet. Arne Schönbohm ist seit 2012 Präsident des nichtstaatlichen Cybersicherheitsrats Deutschland und Sohn des früheren brandenburgischen Innenministers Jörg Schönbohm (CDU). Der 46-jährige Diplom-Betriebswirt hatte nach seinem Studium lange bei DaimlerChryslerAerospace und dem Luftfahrtkonzern EADS gearbeitet. Für viele kam die Berufung, die das Bundeskabinett noch bestätigen muss, überraschend, weil Arne Schönbohm zuvor selbst immer wieder Kritik an den Bemühungen des Staats um IT-Sicherheit geübt hatte. *kru*

© picture-alliance/dpa

ZAHL DER WOCHE

395

Millionen Gigabyte (GB) betrug das Datenvolumen, das 2014 über Mobilfunknetze übertragen wurde. Laut einer aktuellen Unterrichtung durch die Bundesregierung war dies ein deutlicher Anstieg gegenüber 2013 (267 Millionen GB).

ZITAT DER WOCHE

»Wie beim Wettlauf zwischen Hase und Igel«

Frank Rieger, Sprecher des Chaos Computer Clubs, beim Hackerkongress vergangene Woche in Hamburg zur Frage der Sicherheit von Computern in der digitalen Welt

IN DIESER WOCHE

THEMA

MIT DER BEILAGE

Das Parlament
Frankfurter Societäts-Druckerei GmbH
60268 Frankfurt am Main

Das neue Glasperlenspiel

BIG DATA Datenschutz muss in Zeiten der Massendatenauswertung neu gedacht werden

Das „Glasperlenspiel" ist ein literaturnobelpreisgekröntes Werk von Hermann Hesse. Dieser Begriff ist in seinem Roman die Bezeichnung für den beliebten Zeitvertreib der Mitglieder eines elitären Bildungsordens – Kastalien. Die Glasperlenspieler kombinieren unterschiedliche Wissenschaften, Sprachen und Künste miteinander, decken zwischen ihnen Verbindungen und Gemeinsamkeiten auf und übersetzen diese in Formeln. Das Glasperlenspiel von heute heißt Big Data und das Silicon Valley ist in mancherlei Hinsicht zu einer Art Kastalien geworden.

Die Logik von Big Data hat einiges mit dem „Glasperlenspiel" gemeinsam: Datenanalytiker werten große, miteinander nicht notwendigerweise in einem unmittelbaren Zusammenhang stehende Datenmengen aus, identifizieren Korrelationen und leiten daraus Aussagen und Vorhersagen über die Beschaffenheit unserer Welt ab. Ob Wissenschaftler im Labor oder Marketing-Experten bei Google und Co., die Möglichkeiten, die Massendatenauswertung bieten, sind vielfältig. Daten werden zum wiederverwertbaren Rohstoff, aus dem neue Innovationen, Dienstleistungen und Geschäftsmodelle entwickelt werden. Big Data wird zum bedeutenden Wettbewerbsfaktor. Auch Bürger profitieren von Big-Data-Lösungen, sei es durch besseren Kundenservice oder durch medizinischen Fortschritt. Big Data birgt allerdings nicht nur Chancen für Innovation und Wirtschaftswachstum, sondern auch neue Herausforderungen für die Privatheit des Individuums sowie für die Hoheit über seine Daten. Datenschutz muss neu gedacht werden.

Die riesigen Datenmengen von Big Data gleichen heute einem modernen Glasperlenspiel. © picture-alliance/Science Photo Library/Ulrich Baumgarten/Collage: Stephan Roters

Schutz der Autonomie Datenschutz „schützt" nicht die Daten an sich, sondern dient der Ermöglichung des Verfassungsgutes der informationellen Selbstbestimmung. Sie ist Voraussetzung für individuelle Autonomie in der freiheitlichen Gesellschaft. Der Einzelne soll darüber entscheiden können, wer was über ihn weiß, denn die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten durch Dritte – etwa die finanziellen Verhältnisse, die Krankengeschichte – bedrohen Privatsphäre und Selbstbestimmung. Dem tragen die grundlegenden Prinzipien des rechtlich verankerten Datenschutzes Rechnung. Unternehmen und Co. dürfen Daten nur für einen klar bestimmten Zweck im dafür erforderlichen Umfang speichern.

Datenschutz »schützt« nicht die Daten an sich, sondern die informelle Selbstbestimmung.

Dieses klassische Konzept des Datenschutzes steht in einem Spannungsverhältnis zu der Eigenlogik von Big Data. Dort geht es gerade um die Auswertung von möglichst vielen primären und daraus abgeleiteten sekundären Daten für zukunftsoffene, gerade nicht zweckgebundene Verwendungsmöglichkeiten. Big Data setzt dabei auf ein anderes Erkenntnisprinzip als die klassische Wissenschaft. Letztere forscht nach kausalen Zusammenhängen. Das Big-Data-Prinzip ist hingegen die Suche nach Korrelationen und ihrer Auswertung. Die Erkenntnis, dass etwas mit einer großen Wahrscheinlichkeit in einem korrelationalen Zusammenhang steht, ist für die Datenanalytiker ausreichend. Und in der Tat – je größer das zu verarbeitenden Datenvolumen ist, desto präziser werden algorithmen-basierte Auswertungen. Die mühsame und zeitintensive Suche nach dem Warum oder dem Wie bestimmter Zusammenhänge scheint überflüssig zu werden.

Dieses Prinzip hat auch außerhalb der Wissenschaft Fuß gefasst. Werbe-, Finanz- und Versicherungsindustrie, Sicherheitsbehörden und Gesundheitseinrichtungen – ohne Zuhilfenahme von Bewertungsalgorithmen ist die Funktionsfähigkeit vieler Institutionen mittlerweile nicht mehr denkbar. Die den Algorithmen zugrunde liegenden Rechenvorschriften zeigen Datenübereinstimmungen, kategorisieren Nutzerdaten und weisen Informationen eine bestimmte Priorität zu. Die Funktionsweise der Bewertungsalgorithmen bleibt dabei aber meist im Dunkeln.

Dabei haben die auf ihrer Grundlage getroffenen Vorhersagen und Einordnungen erhebliche Konsequenzen: Personen werden aufgrund der Auswertung etwa als kreditwürdig oder nicht-kreditwürdig beurteilt. Facebook hat beispielsweise ein Patent für Bonitätsprüfungen mit dem sogenannten „Social Kreditscoring"-Verfahren angemeldet. Demnach soll durch die Auswertung von Nutzerprofilen auf die Bonität von Personen geschlossen werden. Auf welche Weise eine solche Kategorisierung genau erfolgt, gehört aus Wettbewerbs- beziehungsweise Sicherheitsgründen fast immer zu den bestgehüteten Betriebsgeheimnissen. Umso kritischer wird es, wenn es sich um eine Falschbewertung handeln sollte. Denn auch das gehört zur Wahrheit: Das korrelationale Prinzip ist nur bedingt dazu geeignet, individuelle Entscheidungen, Handlungen und Einstellungen mit absoluten Exaktheit wiederzugeben. Eine perfekte Vorhersage wird es wohl nie geben.

Dem Datenschutz als Voraussetzung für die Datenhoheit und damit für die Möglichkeit der informationellen Selbstbestimmung kommt im Big-Data-Zeitalter daher eine zunehmend wichtigere Rolle zu. Ein Ausstieg aus der Big-Data-Entwicklung ist daher genauso wenig denkbar wie die Aufgabe beziehungsweise Lockerung des Grundrechts auf informationelle Selbstbestimmung. Das Gebot der Stunde muss daher lauten, durch Technik, Gesetzgebung, öffentliche Aufklärung aber auch durch die Entwicklung von datenschutzfreundlichen Geschäftsmodellen die Datenhoheit des Bürgers zu festigen.

Neue Ansätze Um das zu gewährleisten, sind viele Ansätze denkbar: Auf der technischen Seite kann nach Möglichkeiten gesucht werden, die Verwendung von sekundären Daten durch Anonymisierungsmodelle abzusichern und eine Re-Identifizierung des Nutzers zu verhindern. Außerdem muss mehr auf die nutzerfreundliche Anwendungsoberfläche geachtet werden. Für den Nutzer muss es auf einfache und verständliche Weise nachvollziehbar sein, was nach seiner Einwilligung mit den Daten passiert und welche Institutionen zu welchen Zwecken darauf Zugriff bekommen.

Der digitale Doppelgänger muss für Nutzer kontrollierbar und gestaltbar sein.

Zugleich muss auch die Wahlfreiheit gewährleistet werden, auf die Nutzung von bestimmten Diensten verzichten zu können, ohne dafür beruflich oder finanziell diskriminiert zu werden. Das Risiko besteht bereits: Nicht nur in den USA, sondern auch in Deutschland gehen manche Firmenchefs dazu über, ihre Angestellten mit Fitnessarmbändern auszustatten, um den Gesundheitszustand und Stressresistenz ihrer Mitarbeiter im Auge zu behalten. Was passiert mit denen, die da nicht mitmachen wollen?

Kontrolle Seinen digitalen Doppelgänger mitzugestalten und kontrollieren zu können, muss genauso selbstverständlich werden wie die Übersicht und der Zugriff auf eigene Kontodaten. Und es gibt dazu erste Ansätze: So wollen beispielsweise Life-Management-Plattformen wie Meeco oder Only Once den Nutzern ermöglichen, die eigenen Daten zentral vorzuhalten und die Datenweitergabe genau zu kontrollieren. Nur wer als vertrauenswürdig eingestuft wurde, erhält den Zugriff auf die Daten, die der jeweilige Nutzer gezielt freigibt. Die Wirtschaft darf den Datenschutz nicht länger als ein wachstumshemmendes Ungetüm empfinden, sondern muss ihn als Geschäftsmodell und als Wettbewerbsvorteil entdecken.

Dem Protagonisten in Hermann Hesses Roman wird irgendwann klar, dass Kastalier, die sich auf das Glasperlenspiel allein konzentrieren, sich von der lebenspraktischen, gesellschaftlichen und politischen Wirklichkeit abwenden. Und wo der Bezug zu dem Menschen fehlt, macht auch eine noch so intellektuell anspruchsvolle Beschäftigung keinen Sinn. Genauso wenig dürfen auch die Big-Data-Entwickler bei der Ausgestaltung der noch so vielversprechenden und innovativen Services den Menschen mit seiner Freiheit und Würde aus den Augen verlieren. Denn wenn eine technische Innovation auf Kosten der menschlichen Freiheit und Selbstbestimmung geht, verfehlt sie das, worauf es in unserer Gesellschaft eigentlich ankommt. *Nikolai Horn*

Der Autor ist Philosoph und Wissenschaftlicher Referent der Stiftung Datenschutz der Bundesrepublik Deutschland.

Unscheinbares Lager für den Rohstoff Daten: 75 Millionen Euro ließ sich der Internetgigant Google dieses Datenzentrum im irischen Dublin kosten. © picture alliance / empics

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

EDITORIAL

Öffentlich anonym

VON JÖRG BIALLAS

Der Datenkrake hat die Welt im Würgegriff. Dieses Bild zeichnen Skeptiker von „Big Data" gern. Sie verweisen auf die Gefahren, die entstehen können, wenn Unmengen Daten aus ganz unterschiedlichen Quellen zusammengefügt werden. Oft geschieht das ohne Wissen derer, die beim Surfen im Internet freiwillig oder unfreiwillig Spuren hinterlassen haben. Diese Informationen sind wertvoll, nicht nur für Sammler mit guten Absichten. Aber eben auch nicht nur für Böses, wie gern unterstellt wird.

Entscheidend ist, ob die Datenerhebung für den Einzelnen tranparent und nachvollziehbar erfolgt. Wer Persönliches preisgibt, muss sich darauf verlassen können, dass diese Daten anonym bleiben, wenn es so vereinbart ist. Bei Online-Diensten ist das längst nicht immer und längst nicht überall der Fall. Deshalb war es hohe Zeit, dass sich die Europäische Union auf eine Datenschutzreform geeinigt hat. Ab 2018 sollen damit Verbraucher gegenüber Internet-Konzernen wie Google oder Facebook mehr Rechte haben. Auch wenn Kritiker beklagen, diese Reform gehe nicht weit genug: Sie ist ein Schritt in die richtige Richtung. Jetzt kommt es darauf an, dass die Verbraucher die neuen Schutzfunktionen auch einsetzen.

Leider ist damit kaum zu rechnen. Gerade Nutzer von Online-Diensten gehen unfassbar sorglos mit persönlichen Daten um. Frei nach dem Motto „Ich habe nichts zu verbergen" wird munter Intimes gechattet und gepostet. Das machen doch alle so, wen soll das schon interessieren? Ein Trugschluss. Es gibt keine Information im Netz, die nicht für irgendjemanden außerhalb des Kreises der Adressaten von Wert ist.

Trotzdem bleibt abzuwarten, wie sich beispielsweise Eltern verhalten, wenn sie ihren Sprösslingen demnächst das Kommunizieren bei Whatsapp oder Twitter erlauben müssen. Und was machen Schulen, die bisher selbstverständlich erwartet haben, dass sich die Zöglinge über Internet-Dienste mit Nachrichten aus dem Schulalltag versorgen?

Internet und Big Data sind eine Herausforderung, aber auch eine Chance, den Risiken der Zukunft Herr zu werden. Dieser Prozess muss aufmerksam, kritisch und mit der Bereitschaft, falschen Entwicklungen rechtzeitig entgegen zu wirken, begleitet werden. In Gesellschaft, Wissenschaft und Politik gleichermaßen.

GASTKOMMENTARE

ANONYMITÄT IM NETZ EINSCHRÄNKEN?

Mit offenem Visier

PRO

© WAZ

Wilfried Goebels, Funke-Mediengruppe

Anonymität im Internet schützt, aber sie enthemmt auch. Wer in der scheinbaren Anonymität von Facebook und Twitter gegen Flüchtlinge hetzt oder sogar zur Gewalt aufruft, muss dafür juristisch geradestehen. Im Rechtsstaat sollten Blogger mit „offenem Visier" und ihrer wahren Identität auftreten – es gibt keinen Anspruch auf Anonymität im Netz.

Die Hemmschwelle bei vielen Internetnutzern ist gefallen. Dabei reicht die Bandbreite der Hassbotschaften von unanständig bis strafbar. Zeugen rassistischer Hetze im Netz sollten deshalb nicht zögern, Behörden auf dubiose Seiten, Chats und Foren hinzuweisen.

Dass Extremisten Ängste im Netz schüren können, daran sind die großen Internetanbieter nicht schuldlos. Weil sich die sozialen Netzwerke bei der Selbstkontrolle bis heute zurückhalten, will Brüssel den Druck auf ausländische Netzanbieter zum Löschen von Hasstiraden zwar erhöhen. An der Anonymität im Netz wird aber vorerst weiter nicht gerüttelt. Dabei würde das Recht auf freie Meinungsäußerung in einer Demokratie sicher nicht tangiert, wenn Menschen sich mit Realnamen im Netz zu Wort melden und nicht hinter einer Anonymität verstecken. Für viele Nerds ist die Anonymität im Internet eine „heilige Kuh", die nicht geschlachtet werden darf. Wer aber nicht nur in Online-Angeboten von Verlagen die Zunahme rüder Beschimpfungen und Beleidigungen verfolgt, muss im Sinne einer besseren Kommentarkultur die Identifizierbarkeit der Autoren befürworten.

Auch in der digitalen Welt sollte der Leitspruch gelten, dass im Netz nur akzeptabel ist, was auch im realen Leben akzeptiert wird. Anonymität ist in der deutschen Verfassung kein Grundrecht. Deshalb kann es auch keinen Anspruch darauf geben.

Preis der Freiheit

CONTRA

© Iddp ddirect

Daniel Bouhs, freier Journalist

Machen wir uns nichts vor: Natürlich ist Freiheit auch stets ein Einfallstor für Missbrauch. Anonym ins Digitale schreiben – super ist das für alle, die anonym hetzen wollen, die kein Gesicht zeigen, aber Andersdenkende mit Hass überziehen oder ihnen gar Gewalt androhen wollen. Allein: Diese Freiheit stärkt auch die Demokratie. Sie sichert den demokratischen Zugang zum Diskurs und zum Widerstand – im Guten wie im Schlechten.

Man stelle sich vor: Bei den ursprünglichen Montagsdemonstrationen hätte jeder ein Namensschild tragen müssen. Hätten sich abertausende DDR-Bürger getraut, auf die Straßen zu gehen und sich gegen das totalitäre System aufzulehnen? Wohl kaum! Die Anonymität hat den Einzelnen geschützt. Er konnte im Kollektiv der Demonstranten aufgehen und es damit stärken.

Demonstrationen leben seit jeher davon, dass jeder Präsenz zeigen und seine Meinung äußern kann, ohne seine Identität vor sich her zu tragen. Im Digitalen schützt Anonymität auch vor analogen Attacken – wer traut sich schon, Rechtsextremisten unter Klarnamen die Meinung zu sagen?

Diesen Schutz gibt es nicht ohne den Preis, dass sich in der Anonymität auch der Hass seinen Weg bahnt. Gegen diese Seuche helfen gleich zwei Rezepte: die Gegenmeinung, die dann auch jeder aus der Anonymität heraus äußern kann. Und Spielregeln gegen Extremisten samt Vollzug.

Wer wie Facebook populäre Diskussionsflächen anbietet, muss Menschenverachtung konsequent Grenzen aufzeigen und Einträge löschen, die darüber hinausgehen. Das ist stets eine Gratwanderung und damit der deutlich kompliziertere Weg. Allerdings schützt nur er auch die Freiheit.

Mehr zum Thema der Woche auf den Seiten 1 bis 13.
Kontakt: gastautor.das-parlament@bundestag.de

»Zügig an die Arbeit!«

PETER SCHAAR Der langjährige Bundesdatenschutzbeauftragte über den europäischen Datenschutz und seine Erwartungen an den Bundestag

© picture-alliance/dpa

Herr Schaar, Sie sind seit zwei Jahren nicht mehr Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Ist der Datenschutz in dieser Zeit weiter in die Defensive geraten?

Das kann man schon sagen, denn die Rahmenbedingungen sind schwieriger geworden. Zum einen hatten wir 2015 zwei schwere Terroranschläge in Europa – da wird dann reflexartig gefordert, die Sicherheitsbehörden mit zusätzlichen Datenzugriffen auszustatten. Da ist die Vorratsdatenspeicherung ein Thema, eine noch umfassendere Speicherung von Flugpassagierdaten, die lückenlose Erfassung aller Ein- und Ausreisenden, um nur einige Punkte zu nennen. Darüber hinaus werden zusätzliche Überwachungsbefugnisse auch für die Geheimdienste gefordert und ihnen auch teilweise gegeben. Zum anderen ist es für den Datenschutz auch mit der zunehmenden Effektivität der Informationstechnologie nicht einfacher geworden: Alle zwei Jahre verdoppeln sich nach dem Moore'schen Gesetz die Verarbeitungskapazität und -geschwindigkeit. Auch insofern sind die Herausforderungen größer geworden.

Was halten Sie denn von Forderungen etwa nach einem Zugriff auch des Verfassungsschutzes bei der Vorratsdatenspeicherung oder nach Beobachtungsdrohnen des Verfassungsschutzes?

Das sind alles Schnellschüsse. Ohne eine gründliche Analyse des tatsächlichen Ereignisses wird hier sehr schnell versucht, Handlungsfähigkeit zu demonstrieren, indem man sich mit solchen Forderungen überbietet. Viele dieser Vorschläge bringen wenig zusätzliche Sicherheit, aber sehr viel mehr Überwachung – nicht nur der Terroristen, sondern von uns allen.

Als Erfolg für den Datenschutz gilt das Urteil des Europäischen Gerichtshofs zum Safe-Harbor-Abkommen, der die Regelungen zum Datenaustausch zwischen den USA und der EU gekippt hat. Welche Konsequenzen muss das haben?

Der Europäische Gerichtshof versteht sich zunehmend als Wahrer der Grundrechte der EU – auch schon in seinen Urteilen zur Vorratsdatenspeicherung und zur Frage der Verantwortlichkeit von Suchmaschinen und zum Recht auf Vergessenwerden. Das ist uneingeschränkt positiv zu beurteilen. Inhaltlich geht es darum, dass die Grundrechtecharta in allen EU-Staaten durchgesetzt werden muss. Das Grundrecht auf Datenschutz gilt auch uneingeschränkt für die Übermittlung von Daten in Drittstaaten. Das Safe-Harbor-Abkommen gewährleistet aber keinen ausreichenden Schutz für die in die USA übermittelten Daten – das ist die zentrale Aussage des Gerichtshofs. Um hier voranzukommen, brauchen wir sehr viel bessere Garantien der USA für personenbezogene Daten aus Europa.

In der Europäischen Union steht die Datenschutz-Grundverordnung vor der Verabschiedung. Ist sie gut für den Datenschutz?

Es gibt drei wichtige positive Punkte. Der erste ist, dass die Harmonisierung beim Datenschutz vorangebracht wird. Es soll ja ein einheitliches Datenschutzgesetz in Europa geben statt 28 unterschiedliche. Die Kriterien für die Verarbeitung personenbezogener Daten sollen in der gesamten Union dieselben sein. Zweitens soll es gleiche Befugnisse für die unabhängigen Datenschutzbehörden geben. Bisher haben wir da riesige Unterschiede. EU-weit sollen alle Datenschutzbehörden wirksame Sanktionen verhängen können. Punkt drei ist das Marktortprinzip: Auch Unternehmen aus Drittstaaten, die in der EU Geschäfte machen, müssen sich an das europäische Datenschutzrecht halten.

Schatten sehen Sie nicht?

Doch, es gibt auch Schatten. Zum einen muss unser sehr differenziertes Datenschutzrecht in Deutschland stark überarbeitet werden. Dabei wird es sicher in Einzelfällen auch zu Absenkungen des Datenschutzniveaus kommen. Noch gravierender ist, dass das Projekt die Prinzipien und Mechanismen, die wir seit 20 Jahren haben, fortschreibt und neuen Herausforderungen wie Big Data nicht ausreichend durch innovative Ansätze Rechnung trägt.

Was wären solche Ansätze?

Eine viel stärkere Fokussierung auf die Anonymisierung von Daten etwa. Oder eine viel deutlichere Hervorhebung des Einsatzes datenschutzfreundlicher Techniken, die den Einzelnen ermächtigen, die Kontrolle über seine Daten wiederzugewinnen. Nötig sind auch klare Vorgaben, damit die Produkte nicht so ausgeliefert werden, dass sie maximal Daten absaugen. Das muss auch nach der Reform weiter diskutiert werden.

Die Grundverordnung wird ja unmittelbar geltendes Recht. Bleiben nationalen Gesetzgebern dann noch Spielräume?

In bestimmten Bereichen wird der deutsche Gesetzgeber weiterhin etwas für den Datenschutz tun können. Diese Spielräume sollten auch genutzt werden. Das gilt für den Beschäftigtendatenschutz, für die Sozial- und Gesundheitsdaten und für die Stellung betrieblicher Datenschutzbeauftragten. In diesen Bereichen können die nationalen Parlamente weiterhin ein höheres Datenschutzniveau festlegen als in der Verordnung. Das hängt aber vom politischen Willen in den Mitgliedstaaten ab. Insofern erwarte ich vom Deutschen Bundestag, dass er sich hier zügig an die Arbeit macht, damit nicht plötzlich eine Schutzlücke auftritt, wenn die Grundverordnung 2018 in Kraft tritt. Dann treten viele nationale Regelungen außer Kraft, wenn der deutsche Gesetzgeber nicht seine Möglichkeiten nutzt, für mehr Schutz zu sorgen. Da ist also höchste Eile angesagt, denn ab Frühjahr 2017 sind wir schon im Wahlkampfmodus Richtung Bundestagswahl.

Als Edward Snowden 2013 das Ausmaß der Ausspähaktivitäten der NSA enthüllte, war der Aufschrei groß, aber viel passiert ist danach im Grunde nicht.

In den USA ist noch das meiste passiert. Dort gab es eine Gesetzesänderung, die das US-interne Datensammeln begrenzt. Aber in Bezug auf die Auslandsüberwachung hat sich kaum etwas verbessert. Das Problem ist auch, dass deutsche Nachrichtendienste viele der Praktiken der US-Dienste auch selbst durchführen. Da ist es schwierig, von den Amerikanern Verbesserungen zu erwarten, wenn man selbst zu solchen Einschränkungen nicht bereit ist. Hier sehe ich den Deutschen Bundestag und die Bundesregierung gefordert, sehr viel schärfere Grenzen zu ziehen für die geheimdienstliche Überwachung.

Als es im vergangenen Herbst Meldungen gab, der Bundesnachrichtendienst habe sogar den französischen Außenminister, Unicef und einen deutschen Diplomaten ausgespäht, schien die Öffentlichkeit das fast mit einem Schulterzucken zu quittieren. Gewöhnen wir uns an die Bespitzelung?

Das ist eine ganz große Gefahr, dass wir die Bespitzelung und Überwachung, die dauerhafte oder allgegenwärtige Registrierung als unvermeidlichen Alltag akzeptieren. Dabei ist das kein unabwendbares Schicksal. Überwachung kann man begrenzen, aber dazu muss der Wille da sein und genau daran mangelt es in der Politik, jedenfalls bei denjenigen, die im Augenblick die Mehrheitsentscheidungen bestimmen.

Sehen Sie hier auch Lücken bei den staatlichen Kontrollmöglichkeiten, etwa bei den zuständigen Parlamentsgremien?

Sowohl bei den Parlamentsgremien, also bei der G10-Kommission und dem Parlamentarischen Kontrollgremium, als auch bei den Datenschutzbehörden sehe ich nur sehr begrenzte Kontrollmöglichkeiten, die noch nicht einmal optimal aufeinander abgestimmt sind. Hier wäre sehr viel bessere Kooperation, aber auch ein Kapazitätsaufbau erforderlich. Da gibt es zumindest ansatzweise parteiübergreifende Forderungen, insbesondere nach einer Stärkung der parlamentarischen Kontrolle. Ich hoffe, dass sie nicht auch wieder verhallen und ad acta gelegt werden.

Das Gespräch führte Helmut Stoltenberg.

Peter Schaar (61) war von 2003 bis 2013 Bundesbeauftragter für den Datenschutz.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

PARLAMENTARISCHES PROFIL

Der Digitalexperte: Jens Koeppen

Jens Koeppen hat keine Angst. „Wir werden an den wachsenden Datenmengen nicht ersticken", sagt der CDU-Abgeordnete. Vielmehr werden sich Daten zur Grundlage für immer mehr Geschäftsmodelle entwickeln, ist er sich sicher und verweist auf den amerikanischen Internetriesen Google, „der uns Europäern vormacht, wie man mit den Daten beherrschen und Geld verdienen kann". Und in der Tat – ob es darum geht, freie Plätze in Restaurants zu finden, medizinische Behandlungsmethoden durch Auswertung von Daten zu verbessern oder Autos autonom fahren zu lassen: Das alles fußt auf der Auswertung und Nutzung teils enormer Datenmengen. Für Koeppen steht daher fest: „Wer Wohlstand und Arbeitsplätze in Deutschland schaffen und sichern will, darf Big Data nicht als Gefahr einstufen und versuchen dagegen zu arbeiten." Politische Rahmenbedingungen ja, aber keine Verhinderungsgesetzgebung, lautet sein Credo. Es gelte „sinnvoll und smart" zu regulieren. „Ob nun alle digitalen Angebote sinnvoll sind oder benötigt werden, ist nicht das, was wir zu beantworten haben", findet der Unions-Politiker.

Koeppen weiß allerdings auch, dass ein Mehr an Daten auch ein Mehr an Datenmissbrauch möglich macht. Datensparsamkeit, so sagt er, liege aber oftmals im Entscheidungsbereich jedes Einzelnen. Außerdem gebe es jetzt die neue Europäische Datenschutzgrundverordnung, die den Grundstein dafür lege, „dass die Persönlichkeitsrechte europaweit auf hohem Niveau geschützt werden".

Und dennoch: Die NSA, aber auch der BND scheren sich augenscheinlich nicht um Privatsphäre oder Datenschutz – immer mit Verweis auf die Terrorgefahr. Muss das so hingenommen werden? Nein, sagt Koeppen und verweist auf die Untersuchungsausschüsse des Bundestags, die Verfehlungen aufarbeiten und mögliche Konsequenzen definieren sollen. Man dürfe aber den Verweis auf die Terrorgefahr nicht herunterspielen. „Ohne funktionierende und gut ausgerüstete Geheimdienste sind wir und unsere freiheitliche Gesellschaft massiv bedroht", sagt der 53-Jährige, der seit Beginn der Legislaturperiode Mitglied im Wirtschaftsausschuss ist. Im Februar 2014 fiel ihm dann die Ehre zu, den Vorsitz im neu geschaffenen Ausschuss Digitale Agenda zu übernehmen. Dass die entscheidenden Fragen zu dem Thema aber noch immer in anderen Ausschüssen federführend behandelt werden – derzeit etwa das Thema Störerhaftung bei WLAN-Netzen im Wirtschaftsausschuss – stört ihn nicht. „Wir haben den Hut bei der Koordinierung der Digitalen Agenda der Bundesregierung auf", macht der aus Schwedt an der Oder stammende Christdemokrat deutlich, dessen politischer Weg 1989 im Neuen Forum begann.

© DBT/Achim Melde

»Wer Wohlstand und Arbeitsplätze in Deutschland schaffen und sichern will, darf Big Data nicht als Gefahr einstufen.«

„Ich habe 28 Jahre im nicht freien Teil Deutschlands gelebt und wollte, dass sich endlich etwas ändert", sagt er rückblickend. Im Neuen Forum habe sich zum ersten Mal die Gelegenheit geboten, für Freiheit und Demokratie zu kämpfen. „Da die CDU aber 1990 die einzige Partei war, die die geschichtliche Chance zur Wiedervereinigung gesehen und die Einheit letztlich gestaltet hat, war meine Mitgliedschaft nur folgerichtig", erklärt er den Wechsel.

Seit 2005 ist er nun Mitglied des Bundestags. Und das, obwohl er nach eigener Aussage nie an einer Parteikarriere gearbeitet und das Bundestagsmandat lange nicht zu seiner Lebensplanung gehört hat. „Ich war 20 Jahre lang Unternehmer in meiner Heimat, der Uckermark, und habe mich ehrenamtlich in der Kommunalpolitik engagiert", sagt Koeppen.

Schließlich war es der damalige CDU-Landesvorsitzende Jörg Schönbohm, der ihn gefragt hat, ob er sich vorstellen kann, seine Heimat im Bundestag zu vertreten. Nach dem Motto: Nicht nur meckern, sondern machen. „Das fand ich so spannend, dass ich dafür meine Unternehmertätigkeit schweren Herzens aufgegeben habe, was ich aber im Nachhinein nie bereut habe", sagt Koeppen.

Götz Hausding

DasParlament

Herausgeber **Deutscher Bundestag**
Platz der Republik 1, 11011 Berlin

Mit der ständigen Beilage
Aus Politik und Zeitgeschichte
ISSN 0479-611 x
(verantwortlich: Bundeszentrale für politische Bildung)

Anschrift der Redaktion
(außer Beilage)
Platz der Republik 1, 11011 Berlin
Telefon (0 30) 2 27-3 05 15
Telefax (0 30) 2 27-3 65 24
Internet:
http://www.das-parlament.de
E-Mail:
redaktion.das-parlament@bundestag.de

Chefredakteur
Jörg Biallas (jbi)

Verantwortliche Redakteure
Claudia Heine (che)
Alexander Heinrich (ahe), stellv. CvD
Michael Klein (mik)
Claus Peter Kosfeld (pk)
Hans Krump (kru), CvD
Hans-Jürgen Leersch (hle)
Johanna Metz (joh)
Sören Christian Reimer (scr)
Helmut Stoltenberg (sto)
Alexander Weinlein (aw)

Fotos
Stephan Roters

Redaktionsschluss
30. Dezember 2015

Druck und Layout
Frankfurter Societäts-Druckerei GmbH
Kurhessenstraße 4–6
64546 Mörfelden-Walldorf

Anzeigen-/Vertriebsleitung
Frankfurter Societäts-Medien GmbH
Klaus Hofmann (verantw.)
Frankenallee 71–81
60327 Frankfurt am Main

Leserservice/Abonnement
Frankfurter Societäts-Medien GmbH
Vertriebsabteilung Das Parlament
Frankenallee 71–81
60327 Frankfurt am Main
Telefon (0 69) 75 01-42 53
Telefax (0 69) 75 01-45 02
E-Mail: parlament@fs-medien.de

Anzeigenverkauf
Frankfurter Societäts-Medien GmbH
Katrin Kortmann
Frankenallee 71–81
60327 Frankfurt am Main
Telefon (0 69) 75 01-43 75
Telefax (0 69) 75 01-45 02
E-Mail: katrin.kortmann@fs-medien.de

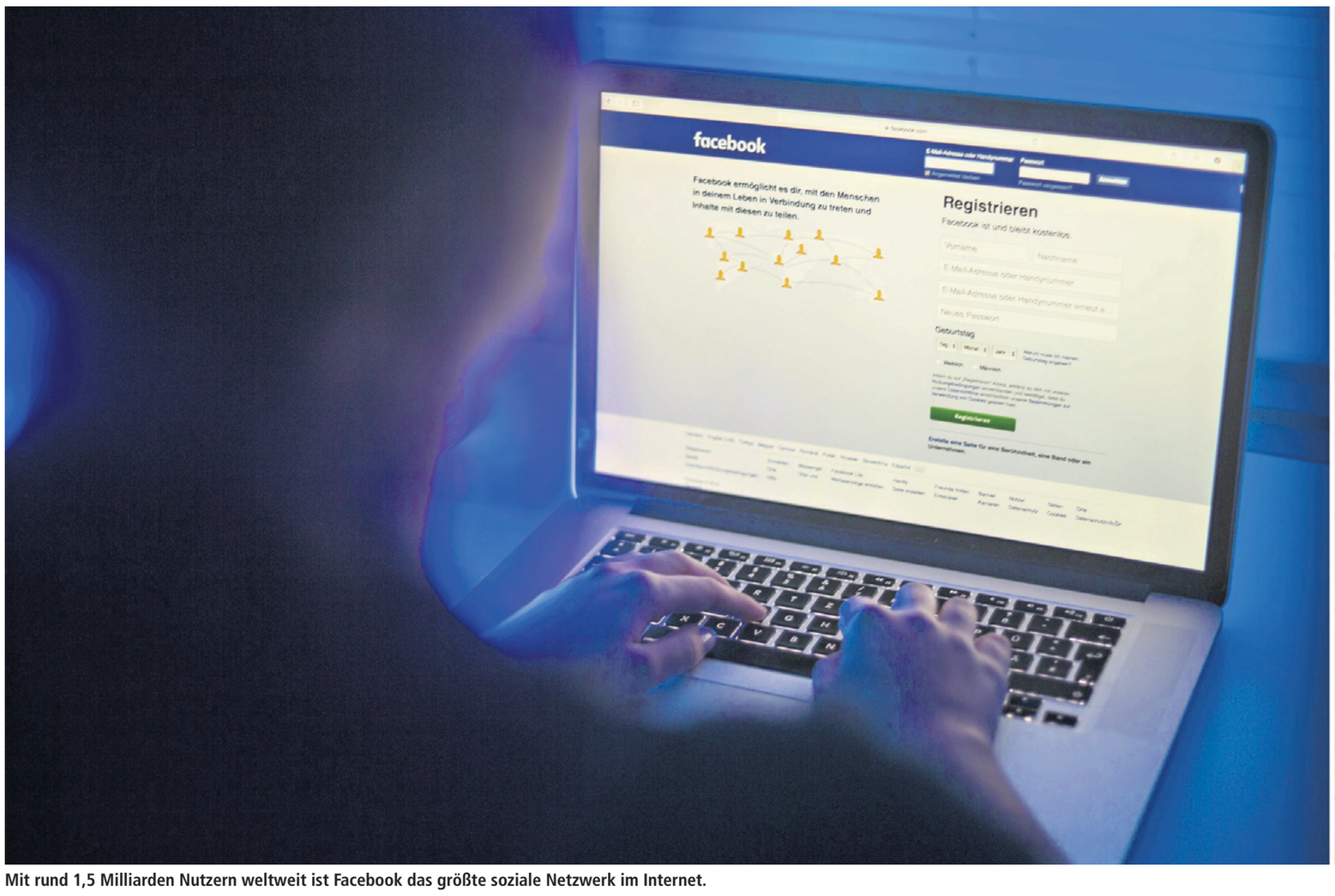
Anzeigenverwaltung, Disposition
Frankfurter Societäts-Medien GmbH
Anzeigenabteilung
Frankenallee 71–81
60327 Frankfurt am Main
Telefon (0 69) 75 01-42 74
Telefax (0 69) 75 01-45 02
E-Mail: anzeigenservice@fs-medien.de

Abonnement
Jahresabonnement 25,80 €; für Schüler, Studenten und Auszubildende (Nachweis erforderlich) 13,80 €
(im Ausland zuzüglich Versandkosten)
Alle Preise inkl. 7% MwSt.
Kündigung jeweils drei Wochen vor Ablauf des Berechnungszeitraums.
Ein kostenloses Probeabonnement für vier Ausgaben kann bei unserer Vertriebsabteilung angefordert werden.

Namentlich gekennzeichnete Artikel stellen nicht unbedingt die Meinung der Redaktion dar. Für unverlangte Einsendungen wird keine Haftung übernommen. Nachdruck nur mit Genehmigung der Redaktion.
Für Unterrichtszwecke können Kopien in Klassenstärke angefertigt werden.

„Das Parlament" ist Mitglied der Informationsgesellschaft zur Feststellung der Verbreitung von Werbeträgern e. V. (IVW)

Für die Herstellung der Wochenzeitung „Das Parlament" wird ausschließlich Recycling-Papier verwendet.



Mit rund 1,5 Milliarden Nutzern weltweit ist Facebook das größte soziale Netzwerk im Internet.

© picture-alliance/Jakob Gruber/picturedesk.com/Fabian Stratenschulte

Der gläserne Neuländer

SOZIALE MEDIEN Anbieter wie Facebook und WhatsApp sammeln die Daten ihrer Nutzer im großen Stil

Dieser Post gehört bereits zu den Klassikern: „Aufgrund der neuen Allgemeinen Geschäftsbedingungen in Facebook widerspreche ich hiermit der kommerziellen Nutzung meiner persönlichen Daten gemäß Bundesdatenschutzgesetz. Das Copyright meiner Profilbilder liegt ausschließlich bei mir. Die kommerzielle Nutzung bedarf ausdrücklich meiner schriftlichen Zustimmung.“ Mit schöner Regelmäßigkeit veröffentlichen Facebook-Nutzer diese Zeilen auf den eigenen Profilseiten – unabhängig davon, ob der Internet-Konzern nun wirklich gerade seine Nutzungsbedingungen geändert hat oder auch nicht. Vor allem aber outen sie sich damit als weitgehend ahnungslose Nutzer jener digitaler Welten, die Bundeskanzlerin Angela Merkel (CDU) im Sommer 2013 während einer Pressekonferenz von US-Präsident Barack Obama als „Neuland“ bezeichnete und sich damit eine Menge Spott und Hohn einhandelte.

Bei näherer Betrachtung erweist sich der Spott für die deutsche Kanzlerin jedoch als unangebracht. Denn auch wenn das Internet seinen weltweiten Siegeszug bereits vor 25 Jahren antrat, so präsentieren sich die Bürger von „Neuland“ mitunter als erschreckend unaufgeklärt über ihre Rechte beziehungsweise deren Abtretung an Internet-Giganten wie Facebook, Google und Co. Bestes Beispiel ist eben jene Widerspruchserklärung bei Facebook, die man zwar als eine Art symbolischen Protest werten mag, die jedoch keinerlei rechtliche Relevanz hat.

Marktführer Von der eigentlich naheliegenden Reaktion eines Kunden, der das Geschäftsgebaren einer Firma nicht akzeptiert, sich nämlich schlicht und ergreifend aus dem sozialen Netzwerk abzumelden, machen nur die wenigsten Facebook-Nutzer Gebrauch. Im Gegenteil: Obwohl das von den vier Havard-Studenten Dustin Moskovitz, Chris Hughes, Eduardo Saverin und Mark Zuckerberg 2004 veröffentlichte Netzwerk immer wieder wegen seiner Datenschutzpraktiken in der Kritik steht, steigen die Nutzerzahlen beständig an. Verfügte Facebook laut eigenen Angaben im ersten Quartal des Jahres 2009 über weltweit rund 197 Millionen Nutzer, so stieg deren Zahl bis zum dritten Quartal 2015 auf 1,54 Milliarden an. In Deutschland waren es Ende 2014 rund 22 Millionen Nutzer. Weltweit liegt Facebook auf Platz zwei der meistbesuchten Internetseiten.

Doch warum stellen so viele Menschen trotz ständiger Warnungen von Daten- und verbraucherschützern ihre Daten so freimütig einer Privatfirma zur Verfügung? Ist es ein prinzipiell verändertes Verhältnis zur Privatsphäre, wie gerne behauptet wird, oder geschieht dies doch eher aus Unwissenheit? Während die Vorratsdatenspeicherung in Deutschland noch immer als politisches Reizwort gilt und die Abhör- und Ausspäh-Aktionen der Geheimdienste viele Bürger noch immer erzürnt, servieren ebenso viele ihre Privatleben in den sogenannten Sozialen Medien auf einem Silbertablett zum freien Zugriff.

Nutzungsbedingungen Das Problem, wenn man es denn als ein solches begreifen will, beginnt bereits bei der erstmaligen Anmeldung bei Facebook. Wer sich dort registriert, akzeptiert zugleich die Nutzungsbedingungen. Annähernd fünf Seiten eng bedrucktes Papier, wenn man sie denn ausdrucken würde. Hinzu bestätigt der Nutzer, dass er die Datenrichtlinie und die Richtlinie über den Einsatzes von Cookies gelesen hat. Zusammen nochmal gut zehn Seiten Papier.

Die Kernaussage der Richtlinien ist denkbar einfach: Gesammelt und gespeichert werden alle Arten von Daten – etwa Bilder, Videos oder Textbeiträge – die Nutzer entweder aktiv im Netzwerk posten, oder die Facebook anderweitig automatisiert erheben kann. Zum Beispiel darüber, mit welchen anderen Nutzern sie kommunizieren, welche Inhalte abgerufen werden, aber auch welche anderen Internetseiten die Nutzer ansteuern. Vor allem dürfen diese Daten von Facebook kommerziell genutzt werden – und zwar weltweit. Auch wenn Facebook als besonders gierige Datenkrake gilt, verfügen auch andere Anbieter über ähnliche Nutzungsbedingungen.

Es ist ein simples Tauschgeschäft, das die extrem erfolgreiche Geschäftsidee von Netzwerken wie Facebook, Twitter und Google+ oder Messenger-Diensten wie WhatsApp und Snapchat bildet. Der angebotene Dienst ist vermeintlich „kostenfrei“, der Kunde zahlt mit seinen persönlichen Daten, aus denen sich für die Werbewirtschaft individuelle Kundenprofile erstellen lassen.

Unnütze Daten gibt es nicht, denn Daten sind pures Gold in der Welt der Werbung.

Herausfiltern aus dem Surfverhalten der Nutzer im Internet und aus selbst veröffentlichten Daten lässt sich so gut wie alles: Alter, Geschlecht, Wohnort, Beruf, politische oder sexuelle Präferenzen, gesundheitliche Gebrechen, bevorzugte Kleidungs- oder Schuhmarken, Urlaubsziele und Hobbys, kulinarische, literarische oder sportliche Vorlieben. Unnütze Daten gibt es nicht, denn Daten sind pures Gold in der Welt der Werbung. Und viele Menschen werfen mit diesem Gold höchst freigiebig um sich. So konnte Facebook seinen Umsatz mit Werbung von 1,9 Milliarden Dollar im Jahr 2010 auf mehr als elf Milliarden Dollar im Jahr 2014 steigern.

Welchen Nutzen die Werbewirtschaft aus den gesammelten Daten ziehen kann, zeigen die Facebook-Nutzungsbedingungen, die zum 30. Januar 2015 in Kraft traten. Sie ermöglichen es beispielsweise, den durch die GPS-Funktion eines Smartphones übertragenen Standort eines Nutzers mit Werbeanzeigen zu koppeln. Hat Facebook aus dem Surfverhalten eines Nutzers ermittelt, dass dieser sich für ein bestimmtes Produkt interessiert, so können ihm entsprechende Angebote von Geschäften in seiner Nähe angezeigt werden. Ob man solche Werbepraktiken als störende Manipulation des eigenen Konsumverhaltens interpretiert oder als praktischen Einkaufstipp, ist letztlich Geschmackssache.

Umstrittenes Cookie Immerhin regt sich in Europa zunehmend Widerstand gegen den Umgang mit persönlichen Daten durch Facebook. Erst Anfang November 2015 untersagte ein Gericht in Belgien dem Konzern, das Surfverhalten von Internetnutzern aufzuzeichnen, die nicht Mitglied des sozialen Netzwerkes sind. Facebook habe 48 Stunden Zeit, diese Praxis zu beenden. Ansonsten drohe eine Strafe von 250.000 Euro täglich. Geklagt hatte Belgiens oberster Datenschützer. Bei der gerichtlichen Auseinandersetzung ging es um das sogenannte Identitäts-Cookie „datr“. Diese kleine Datei wird von Facebook im Web-Browser eines Internet-Nutzers gespeichert, wenn dieser eine Facebook-Seite ansteuert ohne selbst Mitglied des Netzwerkes zu sein. Dies ist bei Facebook-Seiten von Firmen oder Institutionen oftmals möglich. Facebook kündigte zwar an, die Auflage des belgischen Gerichts zunächst einzuhalten, will das Urteil jedoch anfechten. Der Internet-Konzern argumentiert, das umstrittene Cookie helfe, falsche Profile herauszufiltern und verhindere Cyber-Attacken.

Safe-Harbor-Urteil Bereits Anfang Oktober hatte der Europäische Gerichtshof das sogenannte Safe-Harbor-Abkommen gekippt. Dies hatte es amerikanischen Internet-Konzernen ermöglicht, die Daten ihrer europäischen Nutzer in die USA zu übermitteln. Der österreichische Datenschutzaktivist Maximilian Schrems hatte gegen dieses Abkommen der EU mit den Vereinigten Staaten geklagt, weil er nicht akzeptieren wollte, dass Facebook seine Daten auf Servern in den USA speichert. Seine Begründung: Seine Daten seien dort nicht ausreichend vor dem Zugriff der amerikanischen Geheimdienste gesichert.

Die Deutschen sind sich der Datensammelleidenschaft von Facebook und Co. durchaus bewusst. In einer aktuellen Emnid-Umfrage geben 84 Prozent der Befragten an, die sozialen Netzwerke und Kommunikationsdienste im Internet würden zu viele Daten der Verbraucher erheben. Umgekehrt kann aber auch ein naiv-leichtfertiger Umgang mit den eigenen Daten beobachtet werden, vor allem bei Kindern und Jugendlichen.

Stephan Finke weiß davon ein Lied zu singen. Der 45-jährige Social-Media-Manager aus dem rheinland-pfälzischen Frankenthal hält regelmäßig Vorträge an Schulen seiner Heimatstadt, in denen er den Schülern aber auch Lehrern und Eltern die Möglichkeiten und Gefahren der sozialen Medien näher bringen will. „Wer liest denn heute noch die Allgemeinen Geschäftsbedingungen?“, fragt er spöttisch. Finke ist immer wieder überrascht, wie leichtfertig Eltern ihre Sprösslinge in die digitale Welt entlassen. Diese würden ihrem Nachwuchs zwar beibringen, wie er sicher eine Straße zu überqueren hat, beim Umgang mit Computern oder Smartphones beließen sie es all zu oft bei einem wenig hilfreichen „Pass halt auf“. Der Grund dafür ist jedoch denkbar simpel: Viele Eltern verfügen schlicht und ergreifend selbst nicht über die nötigen Kenntnisse, um ihre Kinder anzuleiten.

Sexting Kinder und Jugendliche sind sich oftmals nicht bewusst, wie schnell sich die von ihnen gesendeten Bilder in den sozialen Medien unwiderruflich verbreiten können. Im schlimmsten Fall mit katastrophalen Folgen – etwa beim sogenannten „Sexting“, dem Versenden von erotischen und pornografischen Inhalten. „Stellen Sie sich folgenden Fall vor: Ein junges Mädchen schickt ihrem Freund über WhatsApp ein Nacktfoto von sich, womöglich sogar in einer eindeutig pornografischen Pose. Zwei Wochen später macht sie aber mit ihrem Freund Schluss. Der will sich rächen und verbreitet das Foto unter den Klassenkameraden“, erzählt Finke. Dies führe schnell zu einem massiven Mobbing gegenüber dem Mädchen. „In extremen Fällen endete das bereits im Selbstmord“, warnt Finke.

84 Prozent der Deutschen kritisieren, es würden zu viele Daten im Internet gesammelt.

Immer wieder erreichen Finke die Hilferufe von Eltern, deren minderjährige Kinder ein unvorteilhaftes Foto in einem der sozialen Netzwerke veröffentlicht haben. Doch wenn das Foto erst einmal von einem anderen Nutzer „geliked“ oder auf dessen Profilseite geteilt wurde, besteht kaum Aussicht darauf, es wieder aus dem Netz zu bekommen.

Solche Fotos können den Betreffenden ein Leben lang begleiten. Schon längst durchforsten die Personalabteilungen von Firmen die Netzwerke nach den Profilseiten von Bewerbern. Kein Wunder: Welcher Firmenchef möchte schon, dass sein Außendienstmitarbeiter bei Facebook betrunken unter dem Tisch liegend oder in anderen unvorteilhaften Momenten „bewundert“ werden kann? In seinen Vorträgen versucht Finke den Jugendlichen deshalb einen verantwortungsvollen Umgang mit den neuen Medien zu vermitteln. Und lässt dabei auch solch drastischen Beispiele nicht aus, um ihnen die Konsequenzen ihres Handelns zu verdeutlichen.

Sinkende Altersgrenze Dies ist um so notwendiger, da die Altersgrenze in den vergangenen Jahren ständig gesunken ist. Hielt Stephan Finke seine Vorträge in den vergangenen Jahren vor Schülern der siebten Klasse und getrennt davon für deren Eltern und Lehrer, so wird er dies auf Bitten eines Schulleiters zukünftig bereits in der fünften Jahrgangsstufe tun. Viele Schüler besäßen inzwischen bereits ab dem neunten oder zehnten Lebensjahr ein internetfähiges Smartphone. Und damit auch Zugang zu den sozialen Netzwerken und Kommunikationsplattformen, wenn die Eltern dies nicht unterbinden. Gerade bei den jüngeren Jugendlichen stünden Dienste wie Whats-App oder Snapchat inzwischen höher im Kurs als etwa Facebook, erläutert Finke.

Die Nutzung von Facebook ist zwar laut eigener Geschäftsbedingungen erst ab 13 Jahren und die von WhatsApp sogar erst ab 16 Jahren erlaubt. Allerdings kann jeder Nutzer sein Alter selbst angeben bei der Anmeldung. Überprüft werden die gemachten Angaben bislang nicht. Benötigt wird lediglich eine gültige E-Mail-Adresse oder Telefonnummer. Die Anbieter selbst sichern sich rechtlich mit entsprechenden Klauseln gegen Falschangaben ihrer Nutzer ab. Dies könnte sich allerdings ändern, wenn die neue EU-Datenschutzverordnung 2018 in Kraft tritt. *Alexander Weinlein*

> STICHWORT

Soziale Medien

> **Soziale Netzwerke** Internet-Dienste, die es ihren Nutzern ermöglichen, sich auf eigenen Profilseiten zu präsentieren, mit anderen Nutzern Daten aller Art (Bilder, Videos, Texte) auszutauschen. Zu den bekanntesten gehören Facebook, Twitter oder Xing.

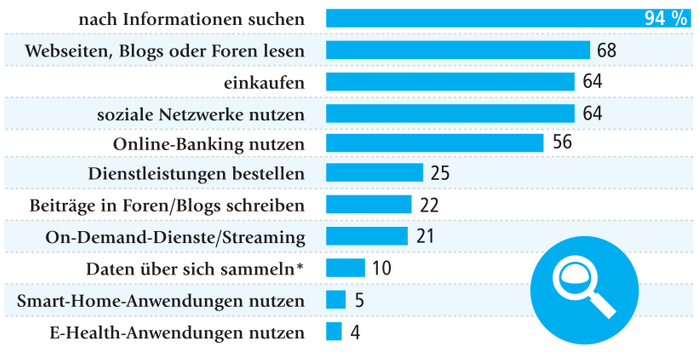
> **Instant Messaging** Sofortiger Versand von Texten, Bildern oder Videos zwischen zwei oder mehreren Nutzern beispielsweise über internetfähige Mobiltelefone. Zu den bekanntesten Anbietern gehören WhatsApp oder Snapchat.

© picture-alliance/dpa

Im Netz unterwegs

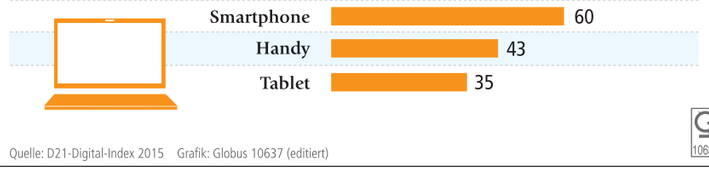
Repräsentative Befragung von 30.015 Internetnutzern ab 14 Jahren von April bis Juli 2015

1. Anteil der Internetnutzer, die mindestens einmal in der Woche im Internet ...
(Anteil in Prozent, Mehrfachnennung)



*z.B. Schritte/Kalorien zählen

2. Mit welchem Gerät gehen Sie ins Internet?
(Anteil in Prozent, Mehrfachnennung)



ROT

Quelle: D21-Digital-Index 2015 Grafik: Globus 10637 (editiert)

10637

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Europa macht ernst beim Datenschutz

VERORDNUNG Die EU stellt strengere Regeln für den Umgang mit Daten auf und stärkt die Rechte der Verbraucher. Viele deutsche Gesetze werden obsolet

Ein „Recht auf Vergessen" für Internetnutzer und harte Sanktionen für Konzerne: Die neuen Regeln sollen ab Anfang 2018 in ganz Europa gelten. © picture-alliance/dpa

Nach beinahe vier Jahren Verhandlungen haben sich Vertreter des Europäischen Parlaments und der EU-Mitgliedstaaten Mitte Dezember auf neue europäische Regeln für den Datenschutz geeinigt. Die Datenschutzgrundverordnung, die im ersten Halbjahr 2018 in Kraft treten soll, ersetzt europäische Vorschriften aus dem Jahr 1995, einer Zeit, als es weder soziale Medien noch Online-Shopping gab. Jan Philipp Albrecht (Grüne), der Verhandlungsführer des Europäischen Parlaments, bezeichnete die neuen Regeln „als Riesenschritt für starke Verbraucherrechte und mehr Wettbewerb im digitalen Zeitalter".

Die Verhandlungen hatten sich so lange hingezogen, weil es sich um eine extrem komplexe Materie handelt. Es galt, einen Ausgleich zwischen den Interessen von Verbrauchern und Unternehmen zu finden. Zudem hatten sich Lobbyisten massiv in den Gesetzgebungsprozess eingeschaltet, weil es beim Geschäft mit dem Daten für die Wirtschaft um Milliardenbeträge geht. Parlamentarier haben 3.999 Änderungsanträge eingebracht – ein Rekord. Herausgezögert haben sich die Beratungen aber vor allem, weil sich die Mitgliedsstaaten nicht auf eine Position einigen konnten. Im Rat argumentierte die Bundesregierung lange, dass europäische Regeln zum Datenschutz das bisher hohe Niveau in Deutschland senken würden.

Die Enthüllungen über massive Spionage des US-Geheimdiensts NSA im Jahr 2013 haben dem Thema Privatsphäre dann zu neuer Bedeutung verholfen. Der Kompromiss ist vor diesem Hintergrund sehr verbraucherfreundlich ausgefallen. Aus der Wirtschaft kam daher herbe Kritik an den neuen Regeln. „Dies stellt einen gewaltigen Rückschritt für Europas digitale Ökonomie dar", sagt etwa Sébastien Houzé, Generalsekretär der europäischen Vereinigung der Direktmarketingunternehmen. Der Schattenberichterstatter der Europäischen Christdemokraten (EVP), Axel Voss (CDU), kritisiert ebenfalls: „Das neue Gesetz wird den digitalen Herausforderungen nicht gerecht." Allerdings hatte er erst sehr spät in den Verhandlungen darauf hingewiesen, dass die massenhafte Analyse von Daten („Big Data") durch das neue Gesetz erheblich erschwert wird. In Brüssel hat diese Kritik zu einem Zeitpunkt, an dem die großen Linien längst festgelegt waren, für Irritationen gesorgt.

Vorteile für Unternehmen Die neuen europäischen Regeln werden die bisherigen 28 nationalen Vorschriften ablösen. In Deutschland wird das Bundesdatenschutzgesetz genauso obsolet wie unzählige Paragrafen zum Datenschutz, die sich in der Landesgesetzgebung befinden, etwa den Schulgesetzen der Länder oder aber auch im Arzneimittelgesetz und dem Telekommunikationsgesetz.

Für Unternehmen haben einheitliche europäische Regeln den Vorteil, dass sie sich nicht mehr in die unterschiedlichen nationalen Besonderheiten einarbeiten müssen. Nach Schätzungen der EU-Kommission sparen sie deshalb künftig im Jahr 2,3 Milliarden Euro. Einheitliche Regeln bedeuten aber auch, dass sich die Firmen nicht mehr den Standort mit den schwächsten Datenschutzregeln heraussuchen können, wie es Facebook gemacht hatte. Das US-amerikanische Unternehmen siedelte seine Europa-Zentrale bewusst in Irland an.

Gleichzeitig können Verbraucher sich im Heimatland beschweren, sollten sie Verstöße gegen den Datenschutz feststellen. Bisher mussten sie sich an die zuständige Behörde im Ausland wenden, was abschreckend wirkte.

Die Harmonisierung ist allerdings nicht so weit vorangeschritten, wie ursprünglich geplant. Juristen weisen darauf hin, dass etwa bei der Verarbeitung von personenbezogenen Daten von Arbeitnehmern und für Behörden Ausnahmen gelten. Experten gehen davon aus, dass Deutschland von diesen Ausnahmen Gebrauch machen wird.

Mit den neuen Regeln erhalten die Nutzer die Entscheidungshoheit über ihre Daten. Klar sei nun, „dass die Daten dem Individuum gehören und nicht dem Unternehmen", betont Viviane Reding, Christdemokratin aus Luxemburg, im Europäischen Parlament. Sie hatte als Justizkommissarin die Datenschutzgrundverordnung auf den Weg gebracht. „Was mit den persönlichen Daten geschieht, bedarf der Einwilligung des Individuums", ergänzte Reding.

Internetunternehmen wie Google, Facebook und Amazon müssen künftig eine Zustimmung bei den Nutzern einholen, wenn sie deren Daten nutzen wollen. Sie können die Daten dann auch nur zu dem Zweck einsetzen, den sie angegeben haben. Bisher durften Unternehmen in Deutschland Daten auch für andere Zwecke nutzen, etwa um einen Kunden für seine Treue zu belohnen, wenn er viel eingekauft hatte. Kunden erhalten außerdem das Recht, dass ihre Daten im Internet gelöscht werden („Recht auf Vergessen") und dass ihnen Daten übergeben werden, wenn sie etwa von Facebook in ein anderes soziales Netzwerk wechseln wollen. Die Idee dahinter ist: Kunden sollen nicht an einen Anbieter gebunden werden, weil der an ihren Daten festhält. So soll der Wettbewerb gestärkt werden.

Ökonomen gehen allerdings nicht davon aus, dass die Datenübertragbarkeit grundsätzlich den Wettbewerb stärken wird. „Wenn auch kleine Anbieter Datenübertragbarkeit sicherstellen müssen, verlassen sie möglicherweise den Markt oder wagen gar keinen Markteintritt, weil die Kosten zu hoch sind", warnt Barbara Engels vom Institut der Deutschen Wirtschaft (DIW). Sie kritisiert die neue Regulierung in dieser Hinsicht als „zu vage", weil sie die Eigenheiten des jeweiligen Markts nicht berücksichtigt.

In der Praxis muss sich ohnehin noch zeigen, was die Datenübertragbarkeit bedeutet. Muss etwa der Eigentümer eines Leasingwagens dem Kunden die Daten auf einem USB-Stick aushändigen? Für Juristen ist dies noch nicht abschließend geklärt.

Unternehmen jedenfalls drohen künftig hohe Strafen, wenn sie sich nicht an Regeln halten. Bußgelder können bis zu vier Prozent des weltweiten Jahresumsatzes erreichen oder maximal 20 Millionen Euro. Die Mitgliedstaaten wollten die Bußgelder bei zwei Prozent des weltweiten Jahresumsatzes deckeln, doch die Europaabgeordneten drangen auf höhere Strafen. Mit ihrer Forderung nach maximal fünf Prozents des Umsatzes konnten sie sich jedoch nicht durchsetzen. In Deutschland gab es bisher Bußgelder von maximal 300.000 Euro, die jedoch nur selten verhängt wurden.

Die Verordnung sieht auch vor, dass Bürger einen Verbraucherverband damit beauftragen können, bei einem Verstoß gegen das Datenschutzrecht in ihrem Namen zu klagen. Verbraucherverbände sehen dies als „großen Fortschritt". Sie konnten bisher in Deutschland nur Verbandsklage einreichen, wenn Unternehmen ihre Allgemeinen Geschäftsbedingungen nicht deutlich offenlegten. Nun können sie auch vor Gericht ziehen, etwa wenn Daten unzulässig zu Werbezwecken genutzt werden.

Die neuen europäischen Regeln haben sich durchaus vom deutschen Datenschutz inspirieren lassen. Künftig müssen europäische Unternehmen, die in großem Stil sensible Daten verarbeiten oder das Verhalten von Verbrauchern überwachen, einen Datenschutzbeauftragten benennen. Bisher gab es dieses Amt verpflichtend nur in Deutschland, Italien und Schweden.

Neues Gremium Ein Novum ist der Europäische Datenschutzausschuss, in dem die Aufsichtsbehörden aller Mitgliedstaaten vertreten sein werden. Kommt es zum Verstoß eines Unternehmens, den die Datenschutzbehörden der Mitgliedstaaten unterschiedlich interpretieren, hat der Ausschuss das letzte Wort und fasst rechtskräftige Beschlüsse. In Deutschland ist allerdings noch nicht geklärt, welche Landesbehörde im Ausschuss vertreten sein wird: die Landesbehörde, in dem das betroffene Unternehmen ansässig ist oder eine Behörde, die Erfahrung mit ähnlich gelagerten Fällen hat? Der Föderalismus könnte sich hier für Deutschland als Nachteil erweisen, denn Datenschutz ist hierzulande Ländersache. Theoretisch stimmen sich die Länder beim Datenschutz im sogenannten Düsseldorfer Kreis ab, doch in der Praxis haben sie bisher unterschiedlich agiert.

Experten gehen davon aus, dass es dauern wird, bis sich zwischen den Behörden der Bundesländer eine einheitliche Rechtspraxis entwickeln wird. Und möglicherweise wird Deutschland bei den Diskussionen in dem Brüsseler Gremium nicht so entschlossen auftreten können wie etwa ein Zentralstaat wie Frankreich, das im Vorgängergremium des Europäischen Datenschutzausschusses sehr aktiv war und viele Vorschläge eingebracht hat.

Und auch in anderer Hinsicht wird wohl erst in einigen Jahren Klarheit herrschen: Weil einiges in der neuen Verordnung nicht eindeutig festgelegt ist, gehen Juristen davon aus, dass die Gerichte in den kommenden Jahren oft angerufen werden. „In vielen Fragen werden wir erst durch Richterrecht Klarheit bekommen", prognostiziert die Anwältin Sibylle Gierschmann von der Kanzlei Taylor Wessing.

Das EU-Parlament und die Mitgliedstaaten müssen dem Kompromiss Anfang des Jahres noch offiziell zustimmen, doch das gilt als Formsache. *Silke Wettach*

Die Autorin ist Korrespondentin der Wirtschaftswoche in Brüssel.

Neue Hürden für Facebook & Co.

SAFE-HARBOR-URTEIL Bisher konnten US-amerikanische Firmen Daten von EU-Bürgern problemlos in die USA übertragen. Das soll sich schnell ändern

Es war ein Schock für Politiker und Internetunternehmen gleichermaßen, als der Europäische Gerichtshof Anfang Oktober mit dem inzwischen schon legendären Schrems-Urteil das Safe-Harbor-Abkommen zwischen der EU und den Vereinigten Staaten kippte. Die Luxemburger Richter knüpften mit ihrem Urteil nicht nur die Übertragung persönlicher Daten von Europa nach Amerika an strenge Bedingungen, sondern errichteten zugleich neue Hürden für die ohnehin schwierigen Verhandlungen über das geplante transatlantische Freihandelsabkommen TTIP .

Seit dem Jahr 2000 konnten amerikanische Unternehmen die Daten von Europäern problemlos in die USA übertragen, dort speichern und verarbeiten. Vorausgesetzt sie erklärten sich dazu bereit, bestimmte Datenschutzstandards einzuhalten. Basis dafür war eine Entscheidung der Europäischen Kommission, mit der die Vereinigten Staaten zum „sicheren Hafen" für die Daten der Europäer erklärt wurden. Dass das nicht der Fall ist, war zwar spätestens seit den Enthüllungen des ehemaligen amerikanischen Geheimdienstmitarbeiters Edward Snowden über die umfassende Spionage der Amerikaner wohl allen klar. Die Kommission sah aber dennoch keinen Grund, das Safe-Harbor-Abkommen aufzuheben. Sie nahm lediglich Verhandlungen mit den Amerikanern über ein Nachfolgeabkommen auf.

Dem Europäischen Gerichtshof ging das nicht weit genug. Er erklärte nach einer Beschwerde des österreichischen Aktivisten Max Schrems, angesichts des weitgehenden Zugriffs der amerikanischen Geheimdienste auf europäische Daten sei das Abkommen mit sofortiger Wirkung ungültig. 4.400 amerikanische Unternehmen standen plötzlich vor der Frage, wie sie mit den Daten der EU-Bürger umgehen sollten. Eigentlich hätten sie vom Tag des Urteils an keine Daten mehr in die USA mehr übertragen dürfen und diese stattdessen in der EU speichern müssen. Eine Riesenherausforderung für Facebook, Amazon oder Apple, erst recht aber für die vielen kleineren Dienstleister, die bisher von der Regelung profitiert haben. Zumal das Urteil, anders als von einigen Anwälten suggeriert, nicht leicht zu umgehen sein sollte. So haben mehrere Datenschutzbehörden Zweifel daran angemeldet, ob Unternehmen auf anderer rechtlicher Grundlage Daten übertragen können, wenn sich die Rechtslage in Amerika nicht ändert.

Zwar verschafften die EU-Datenschutzbehörden den Unternehmen etwas Luft, indem sie der EU-Kommission und ihren amerikanischen Verhandlungspartnern bis Ende Januar Zeit gaben, ein neues Abkommen auszuhandeln. Die Gespräche gestalten sich aber offenbar alles andere als einfach, auch wenn beide Seiten Optimismus verbreiten. Grund dafür ist nicht zuletzt, dass die Luxemburger Richter faktisch verlangt haben, dass die Daten in den USA künftig genauso gut geschützt sein müssen wie in Europa.

US-Internetriesen wie Facebook sollen Daten von Europäern nicht mehr so ohne weiteres nach Amerika übertragen können. © picture-alliance/prisma

Die EU-Justizkommissarin Věra Jourová hat inzwischen sehr genau skizziert, wie sie das sicherstellen will. So sollen die Amerikaner garantieren, dass ihr Zugriff auf die Daten den Prinzipien von Notwendigkeit und Verhältnismäßigkeit entspricht und dass es eine entsprechende richterliche Aufsicht gibt. Zudem müsse sichergestellt sein, dass Beschwerden von EU-Bürgern bearbeitet und beigelegt würden, wenn US-Unternehmen die Datenschutzgrundsätze nicht beachteten.

Das allein reicht nach Ansicht von Jourová jedoch nicht aus. Sie will den Internetunternehmen keine Blankoschecks für die Übertragung europäischer persönlicher Daten mehr ausstellen. Das Abkommen soll engmaschig überwacht und jederzeit von der Europäischen Kommission ausgesetzt werden können. Die Kommission fordert deshalb einen alljährlichen Bericht über die Anzahl der von den Geheimdiensten abgefragten europäischen Daten. Zugleich müssten die Unternehmen ihrerseits über die Zahl der Anfragen berichten, damit die Kommission die Angaben der US-Behörden überprüfen kann.

Ob die amerikanische Regierung bereit ist, soweit zu gehen, ist unklar. Zwar hat sie den Zugriff der Geheimdienste nach den Snowden-Enthüllungen beschränkt. Das gilt aber vor allem für amerikanische Bürger. Die Amerikaner zumindest werben schon dafür, die Frist für den Abschluss der Verhandlungen auszuweiten. Eine Einigung im Februar oder März wäre doch schon beachtlich, sagte die oberste amerikanische Datenschützerin Julie Brill im Dezember in Brüssel. Fraglich ist, ob die EU-Datenschutzbehörden, deren Rolle der Gerichtshof mit seinem Urteil zudem gestärkt hat, solange warten.

Damit aber könnte das Safe-Harbor-Urteil auch noch zum Problem für TTIP werden. Die Amerikaner dringen auch hier auf einen möglichst ungehinderten Transfer für persönliche Daten, wenn sie im Zusammenhang mit der Ausführung der Geschäfte des Dienstleistungsanbieters steht. Genau den darf die Kommission aber auf Basis des Urteils eigentlich nicht mehr gewähren. *Hendrik Kafsack*

Der Autor ist Korrespondent der FAZ in Brüssel.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Sicherheit vor Überwachung und Datenschutz sind die Argumente, mit denen junge Start-Ups um Kunden kämpfen. © picture-alliance/moodboard/Collage: Stephan Roters

Die Nicht-Sammler

NEUE GESCHÄFTSFELDER IT-Unternehmen werben mit Datensparsamkeit

Kostenlose E-Mail-Provider stehen seit der NSA-Affäre, aber auch angesichts einer dramatischen Zunahme von Hacker-Angriffen massiv unter Druck: Sie scheinen keine sichere Nachrichtenübertragung und -speicherung garantieren zu können. Das ist die Chance für kleinere Anbieter. Sie stoßen in die Lücke, die ihnen die großen Internet-Dickschiffe im Datenmeer bieten, indem sie den elektronischen Postverkehr für ihre Kunden anonymisieren. Und sie sind ein Beleg dafür, dass sich kleinere Provider trotz übermächtiger Konkurrenz gut behaupten können – nicht so sehr wegen der Datensicherheit, sondern weil sie ihren Kunden in zwei Punkten entgegen kommen: Sie sind werbefrei und vor allem mit keinem der großen, globalen Player auf dem Markt der digitalen Dienstleistungen verbunden.

Deutsche E-Mail-Anbieter wie zum Beispiel Posteo expandieren deshalb kräftig. 2009 wurde das Unternehmen gegründet und wuchs langsam und nur mit Eigenkapital. In wenigen Jahren stieg die Zahl der verwalteten E-Mail-Accounts auf 10.000. Heute sind es bereits 100.000 elektronische Postfächer, die von dem Start-Up-Unternehmen, das auf dem Gelände der ehemaligen Berliner Schultheiss-Brauerei angesiedelt ist, verwaltet werden. Dazwischen lagen 2013 die NSA-Veröffentlichungen von Edward Snowden. „Danach stieg die Zahl unserer Nutzer rasant“, erklärt Sabrina Löhr, die zusammen mit ihrem Mann Patrick das Unternehmen gegründet hat. Ihre Überzeugung: „Sicherheit in der digitalen Kommunikation ist für alle wichtig, nicht nur für Nerds.“ Deshalb verwaltet Posteo die E-Mail-Accounts ihrer Kunden auch anonym. Im Gegensatz zu Facebook und Co. will das Berliner Start-Up so wenig Daten wie möglich von ihren Kunden speichern und verspricht einen hohen Datenschutzstandard unter anderem durch das Speichern der Nutzerdaten und E-Mails auf Servern im Inland. Selbst die Bezahlung bei dem kostenpflichtigen Angebot erfolgt anonym: Heute liegt der Umsatz bei rund 1,2 Millionen Euro im Jahr.

Verschlüsselungen Ähnlich geht „aikQ“ vor. Dahinter steht das Berliner Unternehmen 8bit, das für Computeradministration, Grafikdesign und Beratung verantwortlich ist. Es bietet seinen Kunden an, alle Mails mit SSL- oder TLS-Verschlüsselung zu versenden. Das sei sicherer als so manches Online-Banking. Auch hier kann man sich problemlos unter einem Pseudonym anmelden. Niemand prüft die Daten oder interessiert sich für Kontakte. Vergleichbare Angebote bieten auch die Unternehmen mailbox.org, secure-mail.biz oder das Schweizer Unternehmen MyKolab.com. Beim Hoster JP-Berlin muss man zwar seinen Namen und seine Adresse angeben, ist aber technisch ähnlich geschützt. Darüber hinaus wirbt der Provider damit, noch mehr als nur Mail-Adressen sicher schützen zu können. Beispielsweise kann man eine eigene Domain beanspruchen. Außerdem ist es möglich, Mailing-Listen einzurichten oder direkt sichere Webseiten hosten zu lassen.

Auch die großen Internetdienstleister versuchen inzwischen, mit mehr Datenschutz und sicherer Verschlüsselungstechnik zu punkten. Das gilt auch für United Internet mit den Internet-Dienstleistern Web.de und GMX. Zusammen kommen sie auf rund 30 Millionen Nutzer in Deutschland und bieten seit kurzem ebenfalls Ende-zu-Ende-Verschlüsselungsverfahren an. Zusammen mit der Deutschen Telekom haben sie die Initiative „E-Mail made in Germany“ gegründet. Sie wirbt mit einer hundertprozentigen SSL-Verschlüsselung durch deutsche SSL-Zertifikate. Darüber hinaus bieten sie ebenfalls eine Perfect Forward Secrecy an, was einen zusätzlichen Schutzmechanismus gegen das nachträgliche Entschlüsseln von Daten bieten soll. Ferner wurde ein neues Verfahren zur Zertifikatsvalidierung und Identitätsprüfung unter den Providern eingerichtet, das bei jeder Datenübertragung Zertifikat und Identität des Providers überprüft, um zu verhindern, dass sich Dritte in die Kommunikation einschalten.

Alleinstellung Was also bleibt als Alleinstellungsmerkmal für die kleineren Provider im Markt? „Vor allem die Tatsache, dass es sich bei ihnen um genau das handelt – kleinere Anbieter“, meint Maurice Shad, beim Branchenverband Bitkom zuständig für Netzpolitik, Datenschutz und IT-Sicherheit. „Kunden der kleineren Anbieter wollen ganz bewusst nichts mit den großen Massenanbietern zu tun haben, auch wenn diese mittlerweile einen vergleichbaren Sicherheitsstandard garantieren können.“

Die Größe der der »kleinen Anbieter« ist eines ihrer Alleinstellungsmerkmale.

Das sieht auch Sabrina Löhr ähnlich: „Wir sehen deshalb unseren Dienst gut für die Zukunft aufgestellt, da wir nicht monothematisch unterwegs sind, sondern viele Kunden auch durch ein konsequentes Nachhaltigkeitskonzept und die Werbefreiheit gewinnen.“ Vor allem aber betont die Posteo-Mitbegründerin die eigenen Anstrengungen und die ihrer Mitbewerber, die die großen Anbieter unter Zugzwang setzen. „Seit 2013 hat sich immer wieder gezeigt, dass durch kleine Anbieter wie uns Druck im Markt aufgebaut wurde.“ Beispielsweise würden nun auch die großen deutschen Provider damit beginnen, die Sicherheitstechnologie Dane einzusetzen. „Wir haben diese Technologie im Mai 2014 eingeführt und daran mitgewirkt, dass sie jetzt über eine BSI-Richtlinie weitere Verbreitung in Deutschland erhalten wird“, sagt Löhr.

Verschlüsselungstechnologien werden immer wichtiger. Das gilt besonders, wenn die Daten in einer Cloud abgelegt werden. Und auch hier bieten sich Geschäftsmöglichkeiten. Boxcryptor aus Augsburg und Cloudfogger aus Göppingen verfolgen das Ziel, durch Verschlüsselung Cloud-Dienste im In- und Ausland wie Dropbox, Google Drive, Microsoft Onedrive, Strato Hidrive oder der Telekom Cloud sicherer zu machen. Für den deutschen Cloud-Markt sieht Bitkom Potenzial. Zunehmend zeigten sich Unternehmen offen für Cloud-Lösungen, aber viele Unternehmen sorgten sich vor unberechtigtem Zugriff auf ihre Daten (siehe auch Seite 7). Laut Bitkoms „Cloud-Monitor 2015“ sei Kunden daher wichtig, dass die Anbieter ihren Sitz der Rechenzentren und ihres Hauptsitzes idealerweise in Deutschland, aber zumindest in einem Land der der EU haben.

Überwachung Doch weder bei den Servern am Boden noch in der Daten-Wolke ist heute letzte Sicherheit garantiert – und sei es nur vor dem Zugriff von staatlichen Behörden und Nachrichtendiensten. Während für AOL, Gmail, Outlook und Yahoo ganz klar US-Recht und hier besonders der „Patriot Act“ gilt, weisen Kritiker darauf hin, dass selbst bei Firmen, die ihren Sitz in Deutschland haben, manchmal nicht klar ist, welche Sicherheitsstandards sie am Ende wirklich einhalten müssen. Ihre Forderung: Anbieter sollten sich auditieren lassen und Standards wie beispielsweise die internationale IT-Sicherheitsnorm ISO 27001 erfüllen. Eine weitere Krux liegt darin, dass auch deutsche Anbieter nicht immer vor dem US-Geheimdienst NSA sicher sind. Denn wenn sie in den USA Niederlassungen führen, unterliegen diese dem US-Recht. Die NSA kann dann auch die Herausgabe von Daten fordern, wenn sie in Deutschland liegen – eine Zwickmühle für deutsche Anbieter, im einen Fall verstoßen sie gegen deutsches, im anderen Fall gegen amerikanisches Recht.

Und auch deutsche Sicherheitsbehörden sind nicht sonderlich zimperlich: In einem jährlichen Transparenzbericht schildert etwa Posteo die Versuche deutscher Sicherheitsbehörden, an Kundendaten heranzukommen. Immer wieder sei es dabei zu formal nicht korrekten Anfragen gekommen, teilweise wurden diese unverschlüsselt über nicht-dienstliche E-Mail-Adressen gestellt. 2014 hat der Anbieter daher in 15 Fällen Beschwerde beim Landesdatenschutzbeauftragten eingelegt. Posteo war nach eigenen Angaben der erster deutsche Provider, der einen solchen Bericht veröffentlichte. Auch die Telekom und 1&1 haben inzwischen nachgezogen. Die meisten Ersuchen an Posteo blieben im Übrigen erfolglos: Namen, Zahlungsdaten und IP-Adressen der Inhaber konnte Posteo nicht herausgeben, denn die wurden ja nicht gespeichert. Und was auf keinem Server liegt oder in einer Datenwolke kreist, kann auch niemandem in die Hände fallen. *Christoph Birnbaum*

Der Autor ist freier Journalist in Bonn.

Privater Surfen im World Wide Web

SICHERHEIT Mit ein paar Tricks und Kniffen lässt sich etwas mehr Souveränität über die eigenen Daten erlangen

Sich um den Schutz der eigenen Daten im Netz zu kümmern erfordert einige Mühe und die Bereitschaft, sich mit Dingen auseinanderzusetzen, die auf den ersten Blick extrem spröde und zugleich relativ kompliziert wirken. Aber es lohnt sich: Mit Muße und einem klickfreudigen Finger kann der Nutzer es schaffen, mehr Souveränität über die Daten im Netz zu erlangen.

Das beginnt schon mit dem Betriebssystem. Auf dem heimischen Rechner gilt insbesondere das neue Windows 10, das auch auf Tablets und Smartphones angeboten wird, als Datenkrake. Wer das Betriebssystem in seinen Standardeinstellungen belässt, der teilt recht viele Informationen mit dem Softwareriesen. Über die Datenschutzeinstellungen lässt sich beispielsweise einschränken, wie viele Daten zum Nutzungsverhalten als „Feedback“ an den Konzern übermittelt werden. Auch der Zugriff von installierten Apps auf Kontakte, Kalender und Positionsdaten kann hier gegebenenfalls eingeschränkt werden.

Von den Einstellungen am jeweiligen Gerät ist es dann ein kurzer Schritt zum eigentlichen Nutzerkonto. Hier lassen sich zum Beispiel Einstellungen zu personalisierter Werbung und geräteübergreifender Synchronisation bearbeiten. Das gilt nicht nur für Microsoft, sondern zum Beispiel auch für Nutzer von Google-Diensten auf dem Computer oder Smartphone.

Apps und Daten Apropos Smartphones: Auch die beliebten Apps wollen gern Zugriff auf persönliche Daten, mal aus naheliegenden Gründen, wenn die Navigations-App etwa auf den Standort zugreifen will, mal, um viele Daten für das Marketing zu erhalten. In den jeweiligen App-Stores werden die erforderlichen Zugriffsrechte in der Regel grob angezeigt. Wer Details will, muss ein bisschen suchen. Inwieweit diese Zugriffsrechte im Nachgang eingeschränkt werden können, ist systemabhängig. Bei Apple und Microsoft lässt sich dies in Teilen besser gestalten als im Google-Mobilsystem Android. Wer seiner Privatsphäre den Vorrang geben will, muss im Zweifel auf eine App verzichten – oder weniger datenhungrige Alternativen nehmen.

Auch beim ganz normalen Surfen im Netz hinterlässt der Nutzer immer Spuren. Gespeichert werden diese in sogenannten „Cookies“, die von Webseiten auf dem jeweiligen Rechner angelegt werden. Das ist dann nützlich, wenn zum Beispiel Zugangsdaten abgespeichert werden, um nicht jedes Mal erneut Benutzername und Passwort eingeben zu müssen. Problematisch wird es dann, wenn Drittanbieter Webseiten übergreifend („Tracking“) Informationen sammeln und anderen zur Verfügung stellen. So lassen sich genaue Profile erstellen und Nutzer identifizieren, um dann beispielsweise passgenaue Werbung anzuzeigen. Diese Datensammlungen vom Rechner zu bekommen, ist mitunter aufwändig. Browser-Erweiterungen wie „Ghostery“, „BetterPrivacy“ und „No-Script“ bieten zumindest die Möglichkeit, Verfolgung nachzuvollziehen und gegebenenfalls zu unterbinden. Wer ganz offiziell aus einem Teil des Tracking-Werbungs-Business aussteigen möchte, kann über diverse Webseiten der Anbieter seinen Ausstieg erklären (z.B. www.youronlinechoices.com).

© dpa

Datenschutz ist manchmal mühsam, aber lohnt sich.

Soziale Medien Datenschutz spielt auch im Umgang mit Sozialen Medien eine große Rolle. Das beginnt beim Posten und Co.: Kein soziales Netzwerk zwingt Nutzer dazu, ganze Lebensläufe und Werdegänge einzustellen. Niemand nötigt die Nutzer dazu, illustre Party- und Urlaubsfotos mit der Chefin, dem Opa oder dem Ex-Freund zu teilen. Faktisch lässt sich bei den persönlichen Daten „schummeln“, auch wenn etwa Facebook eigentlich eine Klarnamenpflicht hat. Zudem lässt sich inzwischen sehr detailliert steuern, was andere Nutzer des Netzwerkes sehen können. Klar ist aber auch: Facebook will Daten und zeigt das auch recht offen. Personalisierte Werbung lässt sich zwar im Zweifel abstellen, wer aber ein Problem damit hat, dass Nutzungs- und Kommunikationsdaten von dem Riesenunternehmen gespeichert werde, muss dem Netzwerk den Rücken kehren. Ein Blick in die Einstellungen zur Privatsphäre lohnt sich auf jeden Fall. *scr*

Weitere Tipps gibt es zum Beispiel auf www.klicksafe.de, einem Angebot der EU vor allem für Jugendliche. oder auf www.verbraucher-sicher-online.de der Technischen Universität Berlin.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

GLOSSAR

Apps

App ist im Smartphone- und Tablet-Bereich der gängige Begriff für Anwendungsprogramme. Durch die zunehmende Verbreitung geräteübergreifender Software (zum Beispiel Windows 10) tritt er inzwischen auch im PC-Bereich auf. Apps können in der Regel in den jeweiligen App-Stores der Betriebssystemhersteller gekauft oder kostenlos heruntergeladen werden.

Big Data

Big Data ist eines der großen Trendwörter der vergangenen Jahre, das in vielen Kontexten gebraucht wird. In der Grundbedeutung meint Big Data eine große Datenmenge, auch Massendaten genannt, deren Verarbeitung mit klassischen, manuellen Methoden nicht zweckmäßig oder unmöglich ist. In der Regel kommen komplexere Algorithmen zum Einsatz. Im medial-gesellschaftlichen Gebrauch wird der Begriff aber auch zur Bezeichnung zahlreicher Aspekte unter anderem der Internet- und Werbe-Wirtschaft sowie staatlicher Überwachung (NSA und Co.) genutzt.

Cloud Computing

„Cloud Computing“ ist ein jüngeres Organisationsprinzip für IT-Infrastrukturen. Dabei werden IT-Kapazitäten geräteunabhängig zur Verfügung gestellt. Zum Beispiel Speicherplatz: Wer seine Daten bei einem Cloud-Anbieter speichert, kann von überall mit praktisch jedem Gerät darauf zugreifen. Auch Software, Rechenpower und Anwendungen können so aus der Ferne bereitgestellt werden.

Cookies

Ein „Cookie“ (dt. Keks, Plätzchen) ist eine von einer Webseite erzeugte Textdatei mit Informationen. Diese Informationen können bei einem erneuten Besuch abgerufen werden, um zum Beispiel die individuellen Einstellung des Nutzers wiederherzustellen.

Ende-zu-Ende-Verschlüsselung

Eine Ende-zu-Ende-Verschlüsselung bedeutet, dass die übertragenen Daten (zum Beispiel eine E-Mail) beim Sender verschlüsselt und erst beim Empfänger wieder entschlüsselt werden. Eventuelle Zwischenstationen können die übermittelten Daten nicht auslesen. Eine gängige Methode zur Verschlüsselung von E-Mails ist dabei PGP (Pretty Good Privacy). Einige deutsche Webmail-Anbieter bieten inzwischen eine solche Ende-zu-Ende-Verschlüsselung an. Auch über E-Mail-Programme lassen sich mit ein wenig technischem Sachverstand entsprechende Vorkehrungen einrichten.

Profiling/Profilbildung

Profilbildung aufgrund von Datenauswertung findet in ganz unterschiedlichen Kontexten statt. Verfügbare Daten, ob nun personenbezogenen Daten oder Nutzungsdaten, werden dabei kombiniert, um ein Profil des Daten erzeugenden Nutzers zu erstellen und dieses gegebenenfalls mit anderen Profilen abzugleichen. Die Profile können zu verschiedenen Zwecken eingesetzt werden. Online-Shops können ihre Produktempfehlungen steuern oder Online-Dating-Portale die vermeintlich beste Verpartnerungsoption anbieten. Problematisch ist Profilbildung vor allem, wenn der Nutzer keine Möglichkeit hat, darauf Einfluss zu nehmen oder sie zu verhindern.

Tracking

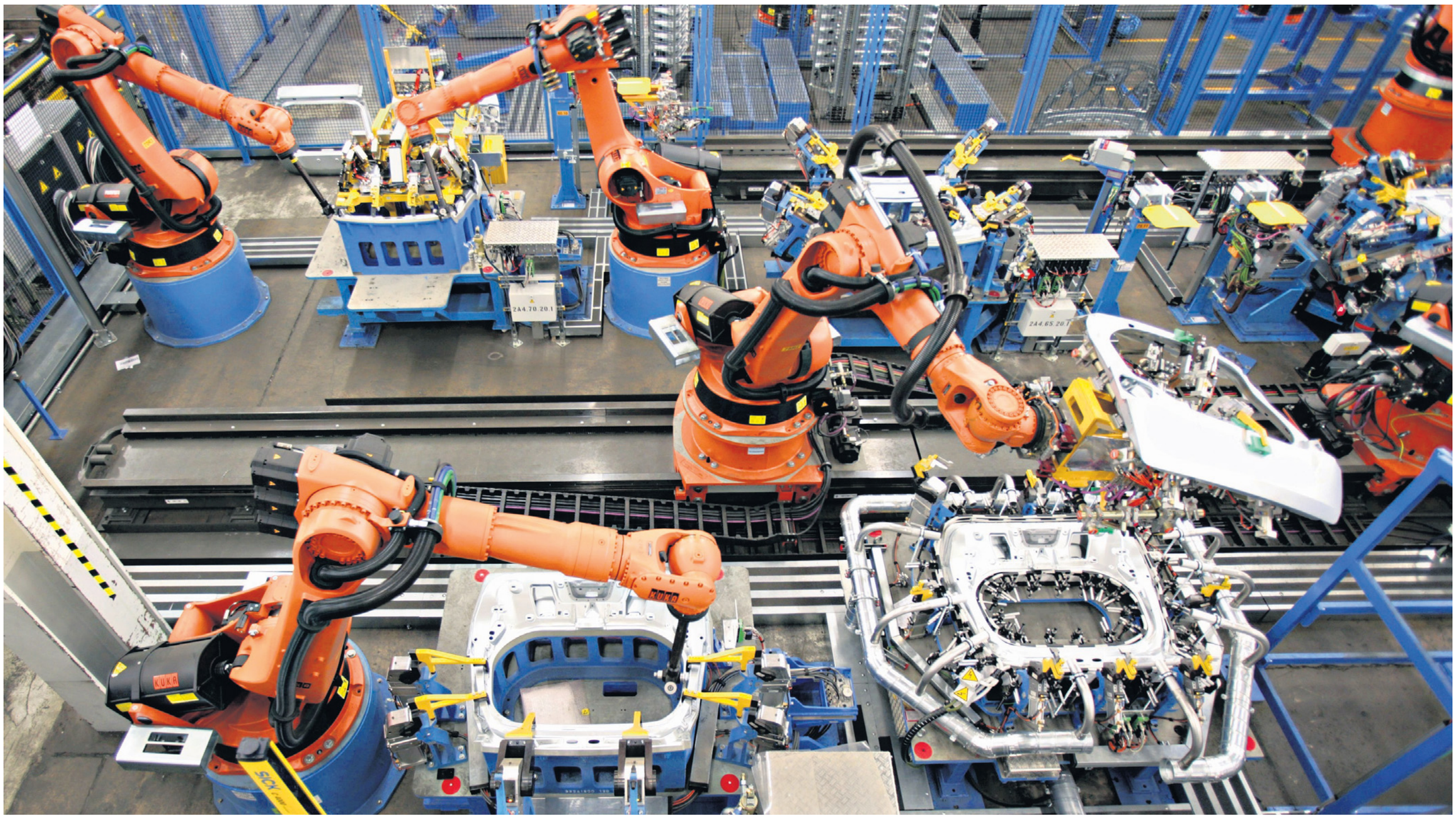
Ein häufig auf Cookies basierendes Verfahren mit dem das Verhalten von Nutzern ausgespäht wird. Die entsprechenden Cookies sind häufig nur schwer vom eigenen Rechner zu entfernen. Die gespeicherten Informationen können von Dritten zum Beispiel zur passgenauen Schaltung von Werbung genutzt werden.

Viren, Trojaner und Co.

Viren, Trojaner und Co. sind schädliche Computerprogramme, die zu unterschiedlichen Zwecken eingesetzt werden. Sie können sich teils unbemerkt verbreiten. Manche Schadprogramme zielen auf die gezielte Zerstörung von Programmen oder Daten. Sogenannte Trojaner dienen unter anderem dazu, Daten auf der Festplatte oder Passwörter im Internet auszuspähen oder den Computer aus der Ferne zu übernehmen. Abhilfe schaffen Anti-Virusprogramme und ein bewusstes Surfverhalten.

Web 2.0

Dieser Trendbegriff bezeichnet grob eine Veränderung in der Art und Weise, wie das Internet genutzt und wahrgenommen wird. Im Gegensatz zum gedachten Web 1.0 tritt der Nutzer im Web 2.0 nicht nur als Konsument auf, sondern produziert eigene Inhalte und kann diese zum Beispiel auf leicht bedienbaren Blogs mit anderen Inhalten verknüpfen. Auch die Vernetzung durch Soziale Netzwerke wie Facebook ist ein Phänomen des Web 2.0. *scr*



Schöne neue Arbeitswelt: Menschen werden bei vielen Tätigkeiten nicht mehr gebraucht. © picture-alliance/Ulrich Baumgarten

Kollege Roboter immer bereit

INDUSTRIE 4.0 Deutsche Maschinenbauer sehen weltweit enormes Wachstumspotenzial. Angst vor Arbeitsplatzabbau

Schöne neue Roboterwelt: In der Fabrik der Zukunft sollen nicht mehr Menschen die Maschinen bedienen, sondern die Maschinen sollen gleich selbst das Kommando übernehmen. Nicht mehr der Mitarbeiter vor Ort drückt auf den Knopf, sondern Maschinen entscheiden künftig selbst, wann sie was fertigen, wie sie mit einem Werkstück umgehen und was sie zur Fertigung eines neuen Produkts brauchen. „Industrie 4.0." heißt das, wovon Maschinenbauer, IT-Spezialisten und Software-Entwickler geradezu ins Schwärmen geraten. Und eigentlich sind es auch gar keine richtigen Maschinen mehr, sondern Robotermaschinen. Sie stehen mit Kollegen in anderen Werkhallen auf der gesamten Welt in direktem Kontakt – via Datencloud und Internet. Der Mensch schaut allenfalls nur noch zu – und kontrolliert mit dem Tablet-PC von irgendwoher die Produktion. Ein riesiger Markt der Zukunft, prognostizieren viele Maschinenbauer besonders aus Deutschland, denn als Maschinenausrüster der Welt sieht die Branche in der Industrie 4.0. ein enormes Wachstumspotential.

Produktion kann künftig mit ein und derselben Maschine effizienter werden.

Vierte Revolution Nach Dampfmaschine, Fließband und Elektronik steht die Wirtschaft so vor ihrer nunmehr vierten Revolution: die digitale Vernetzung von Produkt, Maschine und Werkzeug. Im Zentrum der Idee steht dabei das Konzept der „Smart Factory" – der intelligenten, vernetzten Fabrik, in der Maschinen und Werkstücke permanent Informationen austauschen und selbständige Entscheidungen treffen können. Das können sie vor allem deshalb, weil industrielle 4.0-Roboter eingebaute Kleinstcomputer und Sensoren haben, die zu einem Netzwerk zusammengeschaltet werden können. Aus Internetclouds können sie sich dabei alle notwendigen Daten ziehen, um so sich selbst konfigurierenden Produktionsressourcen mit den zugehörigen Planungs- und Steuerungssystemen zu verbinden. So wachsen physische und virtuelle Produktionselemente zusammen, wenn sich „smarte Maschinen" etwa Software-Updates oder passende Datensätze für ein bestimmtes Material, das sie zum ersten Mal bearbeiten, von einem Datenmarktplatz herunterladen.

Der Vorteil: Produktionen können mit ein und derselben Maschine künftig flexibler, kundenorientierter und vor allem effizienter werden, weil sie zum Beispiel vollautomatisch zwischen verschiedenen Aufgaben wechseln oder Monteure bei ihrer Arbeit unterstützen können. Im Siemens-Elektronikwerk in Amberg etwa tragen schon heute Chips, Stecker und jedes Bauteil einen Strichcode, die von Robotermaschinen gelesen werden, so dass sie daraus anschließend verschiedene Steuerungseinheiten zusammen bauen – für die unterschiedlichsten Anwendungen wie Bordsysteme von Kreuzfahrtschiffen oder aber Skilifte, je nachdem, was gerade gebraucht wird und wie die Auftragslage aussieht.

In den Fertigungshallen solcher „smarten" Fabriken stehen deshalb „social machines", die selbständig und untereinander weltweit mit Zuliefer- und Kundensystemen in Kontakt stehen. Kapazitätsengpässe oder freie Ressourcen können damit sofort erkannt und die Roboter eigenständig und situationsbedingt auf Abweichungen und Anforderungen reagieren. Auch die Kosten lassen sich so senken, die Produktivität steigern und der Trend zur Verlagerung der Produktion in Niedriglohnländer abbremsen. Kollege Roboter kennt keinen Tarifvertrag und kann sich auch nachts mit einem Industrieroboter in China kurzschließen, um ihm ein neues Ersatzteil etwa im schwäbischen Ditzingen zu bestellen

© picture-alliance/dpa

Fast schon menschliche Roboter

Eine faszinierende Perspektive. Doch kann ein „smarter" Roboter wirklich das ersetzen, was im menschlichen Gehirn in Millisekunden abläuft und sich aufgrund von Wissen, jahrelanger Erfahrung oder aber auch auf Grund reiner Intuition am Ende zu einem Gedanken und einer Entscheidung formt? Im Reich der Maschinen ist ein solcher Denkvorgang vor allem das Ergebnis einer unfassbar großen Rechenaufgabe. Das vorerst größte Problem der „smart factories" und der „Industrie 4.0." sind deshalb auch die unglaublichen Datenmengen, die die Maschinen verarbeiten müssen, damit sie überhaupt entscheiden können, was zu tun ist.

Wachsende Datenströme Deshalb sagen Industrie-4.0-Experten auch voraus, dass das Kommunikationsvolumen zwischen den Maschinen in den nächsten Jahren deutlich größer werde als die Datenströme von Mensch zu Mensch zum Beispiel in der Sprachtelefonie, im E-Mail-Verkehr oder bei Austausch von Texten und Bildern. Heute schon können eine Milliarde Datenmengen in weniger als zehn Sekunden ausgewertet werden, damit Maschinen eine folgerichtige Produktionsentscheidung treffen können. Bislang nutzten diese riesigen Rechnersysteme von „Big Data" fast ausschließlich Banken und Versicherungen unter anderem für die Risiko-Analyse großer Datenmengen und an den elektronischen Börsen. Da entscheiden bereits heute Computer in Millisekunden über Kauf oder Verkauf von Milliardenwerten.

Jetzt entdeckt die Industrie die neuen Möglichkeiten im globalen Produktionszeitalter. Neben neuen Rechnerleistungen gilt es dabei aber auch noch eine andere Hürde zu nehmen, denn eine Voraussetzung für 4.0-Roboter ist, dass alle so viele Produktionsroboter wie möglich auf der gesamten Welt untereinander dieselbe „Sprache" sprechen. Eine Roboter-lingua franca sozusagen. Gelingt es nicht, sich weltweit auf eine oder zumindest wenige Standards zu einigen, könnte die komplette Vision der intelligenten Produktion am Ende in einem globalen Kauderwelsch untergehen.

Die schiere Menge an Daten und ihre globale Bewältigung sind das eine Problem, das andere ist die Datensicherheit im weltumspannenden 4.0-Datenaustausch. Der intensive Datenaustausch macht 4.0-Unternehmen und Fabriken zum attraktiven Ziel für Hacker. Datendiebstahl oder Sabotage der Produktion – beides ist möglich. Hier gibt es noch viel zu tun, wenn man bedenkt, dass etwa in den USA gänzlich andere Datenschutzbestimmungen gelten als in der EU. Wie hier unterschiedliche Rechtsräume miteinander verschmelzen sollen ist deshalb für die Industrie 4.0 eine weitere riesige Baustelle.

Und dann ist da noch der Mensch. Wenn Roboter immer stärker die Arbeit von Menschen übernehmen, wird das große Auswirkungen auf den Arbeitsmarkt haben. Noch lassen sich diese Folgen kaum abschätzen. Die Gewerkschaft Verdi warnt jedoch bereits heute vor Jobverlusten, wenn die Rechner dem Menschen künftig auch das Denken abnehmen. „Ganze Berufsfelder sind von der Digitalisierung bedroht", prophezeit Ver.di-Vorsitzender Frank Bsirske. Betroffen sein könnten selbst hochqualifizierte Facharbeiter. In jedem Fall dürfte sich der Trend fortsetzen, dass weniger ungelernten Arbeiter gebraucht werden.

Bei allen Problemen und aller Skepsis: Deutsche Unternehmen setzen riesige Hoffnungen in die Industrie 4.0. Denn eins ist klar: Es gibt keine bessere Wiege für den Sprung in ein neues industrielles Zeitalter. Deutsche Unternehmen erwirtschaften ein Drittel der industriellen Wertschöpfung der gesamten EU, in Deutschland sitzen die Weltmarktführer im Mittelstand, hier brummt der Maschinenbau. Bis 2020 will die deutsche Industrie deshalb 40 Milliarden Euro pro Jahr in solche Anwendungen investieren. Das entspricht knapp der Hälfte der geplanten neuen Ausrüstungsinvestitionen, das heißt, dass zwei Drittel der Unternehmen bereits aktiv an der Digitalisierung und Vernetzung ihrer Wertschöpfungskette arbeiten. Branchenexperten rechnen damit, dass Unternehmen damit ihre Umsätze um bis zu 2,5 Prozent jährlich steigern können. Auf die Gesamtheit aller Industrieunternehmen in Deutschland bezogen entspricht das einem jährlichen Umsatzpotenzial von über 30 Milliarden Euro. *Christoph Birnbaum*

Der Autor ist freier Journalist in Bonn.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Wie von Geisterhand gesteuert

VERKEHR Selbstfahrende Autos sollen zukünftig Staus vermeiden helfen

Aus den großen Containerterminals der Welthäfen, aber auch aus vielen Hochregallagern kennen wir sie bereits: selbstfahrende Transporter, die wie von Geisterhand gesteuert ihre geschulterten Metallkisten an den vorherbestimmten Standort bringen. Nun soll es schon bald Zuwachs im öffentlichen Straßenraum geben: Besonders in den USA sind die ersten autonomen Autos unterwegs:

Im Frühjahr vergangenen Jahres stellte Google sein erstes selbstfahrendes Fahrzeug vor. Und auch in Deutschland ist Bundesverkehrsminister Alexander Dobrindt (CSU) nicht untätig geblieben: Jetzt sollen auch deutsche Autobauer eine Möglichkeit bekommen, ihre Autos der Zukunft auf die Straße zu bringen. Eine erste Teststrecke für selbstfahrende Autos in Bayern auf der Autobahn A9 nimmt jetzt nach und nach ihren Betrieb auf.

Teststrecke in Bayern Auf ihr werden Fahrzeuge mit so genannten Assistenzsystemen genauso getestet werden, wie später auch vollautomatische Autos. Schon heute können etwa Fahrzeuge mit einem Spurassistenten automatisch mittig auf der richtigen Fahrbahnseite gehalten werden oder aber vollautomatisch im innerstädtischen Verkehr in eine Parklücke einparken. Jetzt sollen sie auch gänzlich eigenständig im normalen Verkehr mithalten können. Dazu wird die neue Teststrecke technisch so ausgerüstet, dass es dort zusätzliche Angebote der Kommunikation zwischen Straße und Fahrzeug wie auch von Fahrzeug zu Fahrzeug geben wird. So könnten die Autos beispielsweise frühzeitig informiert werden, wenn sich vor ihnen ein Unfall ereignet hat. Selbstfahrende Auto werden in Zukunft auch keinen großen Sicherheitsabstand brauchen. So können Staus vermieden werden.

Der Verkehrsminister ist dabei überzeugt, dass schon bald die Wertschöpfung eines Autos sich immer weniger über die Motorleistung und immer stärker über den Anteil an Digitalisierung definieren wird. Mithilfe von Ausnahmegenehmigungen testen Daimler und BMW ihre autonomen Fahrzeuge auch jetzt schon vereinzelt auf deutschen Autobahnen. Dabei beschleunigen, bremsen und lenken die Fahrzeuge tatsächlich eigenständig, auch die Spur wechseln sie ohne Hilfe – allerdings sitzt trotzdem immer ein Fahrer hinterm Steuer, um notfalls einzugreifen.

Unter Druck gerät die deutsche Automobilindustrie vor allem durch amerikanische Firmen wie Google, die im Herbst letzten Jahres ihr erstes selbstfahrendes Auto vorgestellt haben. Mittlerweile hat Google angekündigt, für weitergehende Tests seines ersten selbstfahrenden Autos eine Flotte aus 150 Wagen aufzubauen. Zuletzt machte auch Mercedes mit einem selbstfahrenden Lkw von sich reden.

Neben technischen Fragen sind aber auch noch viele Haftungs- und Genehmigungsprobleme ungelöst. Deutschland ist etwa an das Wiener Übereinkommen für den Straßenverkehr gebunden, das Autofahren ohne Fahrer bislang nicht zulässt. Gestattet sind jedoch unter besonderen Auflagen Tests zum autonomen Fahren. *cb*

Auf der Teststrecke: Ein Auto ohne Fahrer © picture-alliance/dpa

Der Feind im PC

WIRTSCHAFT Die Gefahren durch den Datenklau werden unterschätzt. Der Schaden beträgt in Deutschland zwölf Milliarden Euro

Firmengeheimnisse ausgespäht? Kriminaltechniker untersuchen die Tastatur eines Computers in einem Unternehmen. © picture-alliance/Science Photo Library

Bei der Wirtschaft hatte Arthur Scherbius einfach kein Glück. Telegramme und Telefonate, so argumentierte der geniale Erfinder in den 1920er Jahren, könnten doch einfach abgefangen und abgehört werden und hohe Schäden verursachen: Der deutschen Industrie bot der Elektrotechniker seine Chiffriermaschinen an, die „Enigma"-Modelle kosteten zwischen 1.000 und 8.000 Mark – zu viel, meinten die Manager damals. Erst als die Generäle der Reichswehr erfuhren, dass ihre miesen Verschlüsselungstechniken im Ersten Weltkrieg keine Herausforderung für die Gegenseite gewesen waren, schwenkten sie um und orderten Scherbius' Maschinen. Manchmal wiederholt sich Geschichte. Auch heute scheut mancher Unternehmer, in die Sicherheit seiner Firmeninformationen zu investieren.

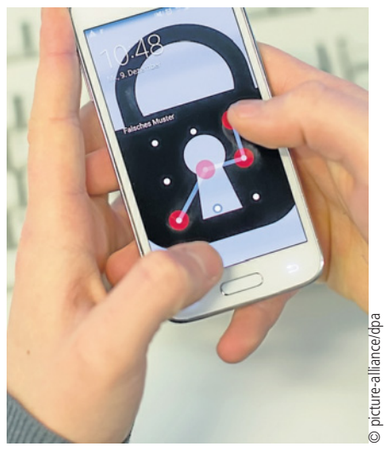
Raffinierte Attacken Cyberkriminalität nimmt zu, die Attacken werden raffinierter. Der Schaden ist immens. Nach einer Studie des Münchener Sicherheitsunternehmens Corporate Trust hatte jedes zweite deutsche Unternehmen in den vergangenen beiden Jahren einen Spionageangriff oder Verdachtsfall zu beklagen. Konkret waren 26,9 Prozent von einem konkreten Vorfall betroffen. Dies stellt einen Anstieg um 5,5 Prozent im Vergleich zu den Ergebnissen aus der Studie 2012 dar. Der jährliche finanzielle Schaden durch Industriespionage: 11,8 Milliarden Euro.

Im Fokus des Datenklaus steht der Mittelstand. „Die Geheimnisse des deutschen Mittelstands sind besonders begehrt. Die hochspezialisierten ‚Hidden Champions' verfügen über Know-how, das Cyberspione aus dem Ausland besonders interessiert", sagte Gerhard Schindler, Chef des Bundesnachrichtendienstes (BND), jüngst in Berlin. Eine weitere Studie bringt es auf den Punkt: Nach Angaben der Wirtschaftsberatungsgesellschaft KPMG herrscht ein gravierendes Missverhältnis bei der deutschen Wirtschaft in der Einschätzung von allgemeiner und eigener Betroffenheit – neun von zehn Unternehmen sähen allgemein ein hohes Risiko für deutsche Unternehmen, Opfer von Cyberverbrechen zu werden. Dagegen schätzt weniger als die Hälfte die eigene Gefährdungslage als hoch ein. „Viele Unternehmen verdrängen noch immer entsprechende Risiken", bilanziert KPMG.

Und die meisten Fälle werden nicht gemeldet. Einen ganz klassischen Versuch des Datenklaus berichtet etwa ein baden-württembergischer Mittelständler, ein echter „Hidden Champion", der seinen Namen in diesem Zusammenhang nicht in der Zeitung lesen will: Da gab es einen angeblichen Käufer, der zur „Firmenbesichtigung" vorbeischaute, umringt von zwei spärlich gekleideten Damen; das Ablenkungsmanöver, zwinkert der Geschäftsführer, habe indes nicht funktioniert, das Trio habe man schnell hinaus komplimentiert.

In der virtuellen Welt indes wird das für Spione zu bestellende Feld immer größer. Das Internet wächst beständig, sensible Firmendaten wandern zunehmend ins Netz, immer mehr infrastrukturelles Wissen wird in den sogenannten Datenwolken (Cloud) archiviert. Mittelständler steigen verstärkt in Onlinegeschäfte ein. Das größte Risiko besteht dabei im Verlust von Kundendaten und dem folgenden Imageschaden. Hacker suchen übrigens nicht die möglichst größte Beute, sondern achten darauf, dass sie ihre Tat möglichst einfach ausführen können.

Firmen müssen also umdenken. Ein Notfallplan, so die einhellige Expertenmeinung, sei oberste Pflicht, um die Folgen eines IT-Sicherheitsvorfalls minimieren zu können. Dieser listet zum Beispiel die wichtigsten Geschäftsprozesse des Unternehmens auf und beschreibt, was im Schadensfall zu tun und wer zu informieren ist. „Alle Unternehmen müssen sich darauf einstellen, dass Cyber-Angriffe durchgeführt werden und auch erfolgreich sind", sagte Michael Hange, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI). „Neben der Prävention müssen auch die Säulen der Detektion und Reaktion gestärkt werden, denn dadurch können Folgeschäden erheblich gemindert werden."



© picture-alliance/dpa

Handy als Einfallstor ins Firmennetz

Eine Voraussetzung für mehr Sicherheit ist verschlüsselter Datenverkehr oder die Ablage von Daten nur in geschützten Bereichen. Der Umgang mit sensiblen Informationen muss erlernt sein. Hierfür bieten sich Schulungen oder andere Weiterbildungsmaßnahmen an. Eine weitere Idee: der Verzicht auf die Umleitung von E-Mails und Daten über amerikanische Leitungen. Wenn die Daten der Europäer in europäischen Leitungen und auf europäischen Servern bleiben, könnte das Geheimdiensten und Wirtschaftsspionen aus Übersee oder Osteuropa den Zugriff erschweren.

Das beginnt im Kleinen: Handys zum Beispiel sind solch ein Einfallstor gegen Konzernsicherheit. Leicht lassen sie sich zu Wanzen umbauen. Der Benutzer erfährt dies nicht; eine Software, oft als Mailanhang versteckt angekommen, installiert sich von allein. Der Bericht des BSI für das Jahr 2015 sieht hier die Schwachstellen: Computer und Smartphones seien einem „Risiko auf sehr hohem Niveau" ausgesetzt. Besonders großen Handlungsbedarf sehen das BSI und das Bundesinnenministerium bei Sicherheitslücken von Software. Schlecht schneiden in dem BSI-Report für kritische Schwachstellen zum Beispiel die Programme Adobe Flash und Microsoft Internet Explorer sowie die Betriebssysteme OS X von Apple und Windows von Microsoft ab. Bei ihnen wurden bis September 2015 jeweils mehr als 100 kritische Schwachstellen registriert. „Das ist nicht gut", sagte Bundesinnenminister Thomas de Maizière (CDU) bei der Vorstellung des Berichts. „Es ist das Recht eines Kunden und Nutzers eines Softwareproduktes, vom Hersteller erwarten zu können, dass regelmäßig ein Sicherheitsupdate zur Verfügung gestellt wird."

> **»Unternehmen müssen sich auf Cyber-Angriffe einstellen.«**
> *Michael Hange, Bundesamt für Sicherheit in der Informationstechnik*

Senioren surfen sicher Was für Firmen gilt, trifft natürlich auch private Verbraucher. Nach Angaben der Software-Firma Symantec für 2015 haben im vergangenen Jahr zwölf Millionen deutsche Internetnutzer Erfahrungen mit Internetkriminalität gemacht. Überraschend sind die Ergebnisse hinsichtlich des Alters der von Cyberkriminalität betroffenen Nutzer. Bei der Generation 55Plus waren dies nur zwölf Prozent, während der Anteil bei jüngeren Nutzern bei 21 Prozent liegt. Eine mögliche Erklärung dafür sieht Symantec darin, dass die ältere Generation in Deutschland mehr auf Sicherheit achte und die Jüngeren ein riskanteres Sicherheitsverhalten im Vergleich zu anderen Altersgruppen zeigten und häufiger online seien. Insgesamt gaben nur 56 Prozent aller Befragten in der Symantec-Studie an, ein sicheres Passwort zu benutzen.

In jeder Krise steckt natürlich auch eine Chance. Wer ausspioniert wird, ist begehrt – und könnte daraus Kapital schlagen. Der Markt für Sicherheitstechnologien wird sich rasant entwickeln; eine Chance für etliche deutsche Betriebe. „Unser technisches Know-how und unser digitales Werteverständnis könnten uns als Standort attraktiver machen und international stärken", haben Wolfgang Ischinger, Leiter der iMünchener Sicherheitskonferenz, und Telekom-Chef Timotheus Höttges schon vor zwei Jahren in einem Gastbeitrag für das „Handelsblatt" geschrieben. „Die hiesige IT-Wirtschaft mit ihren sicheren Liefer- und Produktionsketten sowie ihren hohen Sicherheitsstandards bei der Datenlagerung könnte sich mit eigenen High-End-Sicherheitsprodukten im Wettbewerb mit US-amerikanischen und chinesischen Hard- und Softwareprodukten erfolgreich positionieren." *Jan Rübel*

Der Autor ist freier Journalist in Berlin.

Alle Daten sind gleich — oder doch nicht?

INTERNET Konzerne könnten sich Überholspuren einrichten und damit die Netzneutralität hintergehen

Internet ohne Überholspuren: Solche „Netzneutralität" geriet keineswegs zu einem Reizwort in der Auseinandersetzung zwischen Regierung und Opposition. Doch wird die einschlägige EU-Richtlinie dieser Vorgabe auch gerecht? Darüber gehen die Meinungen im Bundestag gründlich auseinander. Der Schlagabtausch hält noch an. Denn die jeweilige Ausgestaltung obliegt nationalen Regulierungsbehörden – in Deutschland der Bundesnetzagentur.

Wichtiger Zugang Bei dieser Umsetzung seien „die Entwicklungen im Bereich der Netzneutralität sorgfältig zu beobachten, zu evaluieren und gegebenenfalls Konsequenzen zu ziehen", heißt es in einem Antrag der Koalitionsfraktionen (Drucksache 18/6643 vom 11. November 2015) zu „Industrie 4.0 und Smart-Services". Hervorgehoben wird darin, wie wichtig ein „leistungsfähiger Breitbandzugang" nicht zuletzt für die „Attraktivität von Unternehmensstandorten" sei. Und dass er „zur Gründung neuer und zum Ausbau bestehender Unternehmen" beitrage. Fazit: „Bei alledem kommt der Netzneutralität entscheidende Bedeutung für den Erhalt des offenen und freien Internets und für die Sicherung von Teilhabe, Meinungsvielfalt, Innovation und fairem Wettbewerb zu."

Die Bundesregierung begrüßt die EU-Richtlinie, die auch dem Koalitionsvertrag entspreche – dort ist die gesetzliche Verankerung der Netzneutralität festgeschrieben. Die EU sichere „erstmals Netzneutralität im offenen Internet", heißt es in einer Erklärung des Bundeswirtschaftsministeriums. Alle Datenpakete müssten gleich behandelt werden: „Die Internetnutzer sollen erstmals ein Recht auf diskriminierungsfreie Datenübertragung erhalten."

Bisher würden Anwendungen und Dienste mit gesonderten Anforderungen parallel zum offenen Internet angeboten – zum Beispiel bei „Triple-Play"-Angebotem: Internet, Telefon und Rundfunk über ein und dieselbe Leitung. „Dies soll auch weiterhin möglich sein", so das Ministerium. Dienste mit besonderen Merkmalen sollen parallel zum offenen Internet angeboten werden dürfen, solange sie dies nicht gefährden würden: „Deshalb sollen für Spezialdienste, die von einem Anbieter parallel zum offenen Internet erbracht werden, klare Maßgaben gelten."

Dann die Spezialdienste im Internet: Darunter fallen laut Günther Oettinger, dem EU-Kommissar für Digitales, nur Gesundheits-, Notruf- und Mobilitätsdienste.

Die Grünen-Fraktion kommt zu einer völlig konträren Beurteilung der EU-Vorgabe: „Die Bundesregierung verramscht die Netzneutralität über den Umweg Europa." Statt, wie von der Bundesregierung behauptet, würden nun „Überholspuren im Netz", „Diensteklassen" und „special services" eingeführt, „die es großen und marktmächtigen Telekommunikationsanbietern ermöglichen doppelt abzukassieren". Für die Grünen bedeutet dies „ein wahres Lobbygeschenk".

Bereits im Juli 2015 hatte die Fraktion einen Antrag (Drucksache 18/5382) vorgelegt mit der Überschrift „Netzneutralität als Voraussetzung für eine gerechte und innovative digitale Gesellschaft effektiv gesetzlich sichern." Mitte November nahmen die Grünen im Parlament diesen Antrag zur Messlatte bei ihrer Bewertung der Netzpolitik der Koalition: „Aller Argumente zum Trotz bleibt die Bundesregierung stur und leistet dem Zwei-Klassen-Internet in Berlin und Brüssel Vorschub."

Letzte Chance Allerdings sieht die Fraktion immer noch „eine letzte Chance": „In den nächsten Monaten können die nationalen Regulierungsbehörden, die die Einhaltung der Netzneutralität sowie die Einhaltung der Regeln für Verkehrsmanagementmaßnahmen überwachen und die Verfügbarkeit eines nicht diskriminierenden Internetzugangs sicherstellen, Qualitätskriterien formulieren."

Auch die Linksfraktion macht noch Spielraum aus: Die EU-Verordnung erlaube „tatsächlich Telekommunikationsunternehmen, bestimmte Angebote vom Prinzip der Netzneutralität auszunehmen und sie als priorisierte Dienste zu behandeln." Speziell geht sie auf „zweiseitige Märkte" ein – bei denen insbesondere die Anbieter von Inhalten zusätzlich zum Anschluss an das Netz auch noch für die Nutzung der Zugangsnetze bezahlen müssten. Und sie verweist auf „Zero-Rating"-Angebote – Nutzung von spezifischen Diensten wird vom monatlichen Datentransfervolumen ausgeklammert. Indes: „Aus Sicht der Linken enthält die EU-Verordnung trotz der Unbestimmtheit und Auslassung bei einer strengen Auslegung der betroffenen Bestimmungen und strengen Auflagen die Möglichkeit, genau diese zweiseitigen Märkte und Zero-Rating-Angebote auszuschließen." *Franz Ludwig Averdunk*

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Spion in der Dose

ENERGIEWENDE Digitale Stromzähler sollen ab 2017 beim Strom sparen helfen und die Netze spürbar entlasten. Doch Daten- und Verbraucherschützer warnen

Nach dem Willen der Bundesregierung sollen „Smart Meter" von 2017 an nach und nach in allen Haushalten eingebaut werden. © picture-alliance/Collage: Stephan Roters

Von der Energiewende ist in den meisten deutschen Privathäusern bislang nicht viel zu spüren. Der Strom kommt wie gewohnt zuverlässig aus der Steckdose, auch wenn am Horizont inzwischen das eine oder andere Windrad zu sehen ist. Und in den Hausfluren und Kellern drehen sich wie seit Jahrzehnten die rotierenden Scheiben der analogen Ferraris-Zähler. Doch das wird sich höchstwahrscheinlich bald ändern: Anfang November hat das Bundeskabinett einen vom Bundeswirtschaftsministerium vorgelegten Gesetzentwurf zur „Digitalisierung der Energiewende" beschlossen, der in vielen Häusern ab 2017 den verpflichtenden Einbau digitaler Stromzähler („Smart Meter") vorsieht. Die Haushalte sollen dadurch Energie sparen. Ziel ist es aber auch, den Strommarkt der Zukunft so flexibel wie nötig zu gestalten. Verbraucherschützer zweifeln den Nutzen jedoch an.

Bereits 2009 hatte die EU-Kommission in einer Richtlinie von den Mitgliedstaaten verlangt, die Einführung digitaler Zähler zu prüfen. Das über den Tag schwankende Stromangebot solle möglichst effizient genutzt werden, Verbraucher könnten zudem Strom sparen, so die Argumente. Daraufhin untersuchte die Wirtschaftsprüfergesellschaft Ernst & Young 2013 im Auftrag der Bundesregierung die Vorteile einer flächendeckenden Smart-Meter Einführung. Ihre Studie kam zu dem Ergebnis, dass Smart Meter ein volkswirtschaftlich lohnendes Projekt seien.

Der nun von der Bundesregierung vorgelegte Gesetzentwurf soll schon im Januar in erster Lesung vom Bundestag beraten werden. Im Mai soll das Gesetz verabschiedet sein. Es sieht eine stufenweise Einführung der Smart Meter bis 2023 vor. Zur Mindestausstattung gehört ein einfacher, digitaler Stromzähler, der nicht mit der Außenwelt kommunizieren kann. Diese Geräte sollen von den lokalen Stromnetzbetreibern in allen Haushalten installiert werden. Sie können später aufgerüstet werden, doch zunächst wird sich für die meisten Verbraucher nichts ändern: Die erfassten Daten bleiben im Haus, Einbau und Nutzung sind für sie nicht mit zusätzlichen Kosten verbunden.

Kontakt mit der Außenwelt Einige Haushalte sollen jedoch echte Smart Meter, ein sogenanntes „intelligentes Messsystem", bekommen. Verpflichtend soll das für Nutzer sein, die mehr als 6.000 Kilowattstunden Strom pro Jahr verbrauchen, was etwa auf fünf Prozent aller Haushalte zutrifft. Ebenfalls betroffen sind die Betreiber einer Kraft-Wärme-Kopplungs- oder Erneuerbare-Energien-Anlage mit mehr als sieben Kilowatt Leistung.

Die Messsysteme sind teuer: Bis zu hundert Euro pro Jahr soll der Netzbetreiber den Stromkunden dafür in Rechnung stellen dürfen. Bisher kostete die Verbraucher der Betrieb der Strommessstelle in der Regel 20 Euro pro Jahr. Dazu kommt: Auch bei anderen Verbrauchern, die unter die 6.000-Kilowattstunde-Grenze fallen, können die Smart Meter eingebaut werden, wenn dies der Messstellenbetreiber – meist der lokale Versorger – möchte. Dann darf er nur nicht so viel Geld dafür verlangen.

Für die Kritiker werfen aber nicht nur die hohen Kosten eine Reihe von Fragen auf. Sie warnen auch vor einer Verletzung der digitalen Selbstbestimmung", schließlich können intelligente Messsysteme grundsätzlich mit der Außenwelt, insbesondere mit dem Netzbetreiber, kommunizieren. Holger Schneidewindt, Experte bei der Verbraucherzentrale in Nordrhein-Westfalen warnt: Verbraucher dürften nicht vom Staat dazu gezwungen werden, Daten über ihr Verhalten offen zu legen, Fakt aber ist: Auch wenn die Auslesung vieler Daten bislang nicht vorgesehen ist – theoretisch lässt sich mit den kommunikationsfähigen Varianten das Verhalten der Verbraucher zu Hause genau überwachen. Ist jemand in der Wohnung, welche Geräte laufen wann und wie lange? Gelingt der Zugriff auf solche Daten, wäre das ein Albtraum nicht nur für Datenschützer. Die Geräte könnten zudem ein mögliches Ziel für digitale Sabotage sein.

Gestritten daher über die Frage, ob es eine sogenannte Opt-Out-Möglichkeit geben soll, also ein Widerspruchsrecht für die Verbraucher. Ein möglicher Kompromiss könnte am Ende eine Opt-Out-Light-Lösung sein: Wer widerspricht, bekommt das Gerät zwar trotzdem eingebaut, aber alle Kommunikationsfunktionen werden ausgeschaltet.

Doch was nützt der ganze Aufwand eigentlich? Bundesenergieminister Sigmar Gabriel (SPD) ist überzeugt: „Erst mithilfe der Digitalisierung lassen sich Stromerzeugung, Gebäude und Verkehr intelligent miteinander verknüpfen und effizienter machen." So könnten zum Beispiel für Haushalte mit Smart Metern in Zukunft Tarife angeboten werden, die mit den Preisen an der Strombörse steigen und fallen. Dann, so die Hoffnung, würden die Verbraucher möglicherweise ihr Verhalten anpassen und Strom nur dann verbrauchen, wenn er gerade ausreichend verfügbar und deshalb günstiger ist. Netze und Kraftwerkspark würde durch diese Steuerung von Angebot und Nachfrage entlastet, sie könnten dann wiederum kleiner dimensioniert werden. Sollte sich zum Beispiel die Elektromobilität flächendeckend durchsetzen, könnte es für die Fahrer interessant sein, ihr Gefährt dann nur zu laden, wenn die Preise gerade besonders niedrig sind.

Der Digitalverband Bitkom hält die Einführung der smarten Zähler für dringend notwendig, um die Energiewende voranzubringen. Felix Dembski, Bereichsleiter Intelligente Netze und Energie bei Bitkom, sagt: „Das Energiesystem erfährt durch die Erneuerbaren Energien erheblichen Stress. Der soll in Preissignale umgewandelt werden. Dann besteht ein Anreiz, Geräte und Maschinen darauf zu trainieren, sich stärker nach Wind und Sonne zu richten." Wenn Deutschland 2050 tatsächlich 95 Prozent seiner Energie aus Erneuerbaren erzeugen wolle, müssten sich Verbrauch und Erzeugung aufeinander zubewegen. Auch einige Stromversorger geben sich optimistisch. Hatte etwa der Stadtwerkeverband VKU die Smart-Meter-Pflicht anfangs noch deutlich kritisiert, spricht er inzwischen von einem „Potenzial für neue Geschäftsfelder".

Für die Verbraucherschutzverbände ist die geplante Einführung der Smart Meter hingegen eine Form der „Zwangsdigitalisierung". Zudem halten Fachleute, wie Holger Schneidewindt, die Einsparmöglichkeiten für normale Verbraucher für „sehr gering". Er ist überzeugt: „ Kaum jemand wird sein privates Verhalten aufgrund eines Smart Meters ändern." Die Waschmaschine, die angeblich nachts angestellt werden könne, sei ein beliebtes Positivbeispiel. „Tatsächlich zeigt es aber eher das sehr begrenzte Potenzial", sagt Schneidewindt. „Wegen ein paar Cent möglicher Einsparungen wird fast niemand einen Waschgang verschieben." Damit sei auch der Nutzen für das Stromsystem insgesamt begrenzt.

Auch der Bundesverband Neue Energiewirtschaft (BNE), der sich in der Regel für Innovationen stark macht, rät zur Vorsicht: Bei der Einführung der digitalen Messsysteme „sollte man dort ansetzen, wo ein wirkliches Potenzial besteht und wo Kunden von entsprechenden Angeboten und Dienstleistungen auch profitieren können", sagt BNE-Geschäftsführer Robert Busch.

Gegen einen Zwang Die Opposition im Bundestag ist ebenfalls skeptisch.Die energiepolitische Sprecherin von Bündnis 90/ Die Grünen, Julia Verlinden, betont zwar, dass Smart Meter ein wichtiger Baustein der Energiewende seien. „Für uns Grüne ist aber auch klar, dass es keine Zwangsbeglückung für private Haushalte geben darf." Vielmehr müsse es eine einfache und praktikable Ausstiegsregelung geben.

Unabhängige Experten, wie Ulrich Greveler, Professor an der Hochschule Rhein-Waal und Informatikexperte, halten die Digitalisierung der Energie-Infrastruktur für „letztlich unausweichlich". Aber den Nutzen von Smart Metern findet auch Greveler fragwürdig. Das Einsparpotenzial sei nachweislich begrenzt und gehe nicht entscheidend über den Effekt einer einmaligen Energieberatung hinaus, meint er. Problematisch sei zudem, dass die Technik, die nun eingebaut werden solle, „in 15 bis 20 Jahren vermutlich längst veraltet ist".

In Sachen Datenschutz hält Greveler den Gesetzentwurf der Bundesregierung allerdings für vorbildlich. „Die vorgeschriebene Verschlüsselung und das Prinzip, Daten nur dann zu übermitteln, wenn sie auch wirklich benötigt werden, sind aus heutiger Sicht eine gute Lösung", urteilt er.

Besorgte Verbraucher Wie viele Haushalte genau von der Neuregelung betroffen sein werden, ist noch unklar. Tatsache ist, dass gut ein Viertel des Stromverbrauchs in Deutschland heute auf private Haushalte entfällt. Und dort sind die Vorbehalte gegen die Smart Meter groß, wie eine Studie des Verbraucherzentrale Bundesverbandes (vzbv) ergab. 70 Prozent der Befragten lehnten deren verpflichtenden Einbau ab. Die größten Sorge der Verbraucher neben den hohen Kosten: die Sicherheit ihrer Daten. *Jakob Schlandt*

Der Autor arbeitet als freier Journalist mit dem Schwerpunktthema Energie in Berlin.

Thunfische im Datenmeer

WISSENSCHAFT Big Data revolutioniert die Umweltforschung – durch die Analyse von Satellitendaten können Forscher dem Puls unseres Planeten heute in Echtzeit nachspüren

Wo trocknet der Aralsee am schnellsten aus? Wie gierig wächst die Zockermetropole Las Vegas in die Wüste? Wie schnell fallen die Bäume des Amazonas-Regenwaldes im brasilianischen Bundesstaat Rondônia? Mit Hilfe von Satellitendaten lassen sich all diese Fragen im Prinzip gut beantworten – wenn man Zugang zu den entsprechenden Informationen hat. Ein Projekt des Suchmaschinenriesen Google, die „Earth Engine", soll diese nun für jedermann bereitstellen. Es ist nur ein Beispiel dafür, wie Big Data die Umweltforschung in den kommenden Jahren revolutionieren wird: Kraftvolle IT ermöglicht Analysen von Daten aus verschiedenen Quellen. Forscher, Behörden und Zivilgesellschaft können dem Pulsschlag unseres Planeten in Echtzeit nachspüren.

„Seit Jahrzehnten haben Satelliten Erdbeobachtungsdaten gesammelt", sagt Google-Manager Dave Thau in einem Promo-Video der Firma. „Aber es war schwierig, Zugang dazu zu bekommen. Außerdem gibt so es viele Daten, dass sie nur schwer zu analysieren wären, selbst wenn man Zugang zu Ihnen hätte." Um das Problem zu lösen, bietet Google nun seine Dienste an. Das Unternehmen hat Petabytes an Satellitendaten zur Atmosphärenzusammensetzung, zur Waldbedeckung oder zur Lichtverschmutzung gesammelt. Die Informationen können von Interessierten auf den Rechnern im gigantischen Netzwerk der Firma analysiert werden.

Zu den bereits nutzbaren Datensätzen gehören: die Entwicklung der Weltbevölkerung, Verbreitung der Malaria, Oberflächenbedeckung, Temperaturen, Winde, Bilder der Nasa-Satelliten „Landsat", „Aqua" und Terra sowie vom „Sentinel 1" der europäischen Weltraumbehörde Esa.

Esa und EU wollen mit einer gemeinsamen Initiative, dem Copernicus-Programm, diese und andere Anwendungen ermöglichen. Die Daten sind kostenlos nutzbar – und sie werden aus Sicht von Vincent-Henri Peuch, bei Copernicus für die Überwachung der Atmosphäre verantwortlich, die Art und Weise revolutionieren, wie sich Regierungen, Unternehmen und Privatpersonen auf Veränderungen der Umwelt einrichten können.

Auf Googles „Earth Engine" greift auch ein Vorzeigeprojekt des World Resources Institute in den USA zurück: „Global Forrest Watch" liefert gebündelte Informationen zur Abholzung von Wäldern, quasi in Echtzeit. Neben Satellitendaten zu Waldbedeckung oder Rauchentwicklung werden Augenzeugenberichte genutzt. So sollen auch Unternehmen Informationen darüber erhalten, ob ihre Lieferketten auf problematisches Holz aus Raubbau setzen. Die Daten werden frei zur Verfügung gestellt, auch für den kommerziellen Einsatz.

Bei Microsoft sowie dem Uno-Umweltprogramm wiederum blickt man in die Zukunft: mit einer Simulation allen Lebens auf der Erde. Das „Madingley Model" nimmt die Idee der bereits existierenden Klimamodelle auf und erweitert sie auf Ökosysteme. Das soll unter anderem dabei helfen, Antworten auf die Frage zu finden, wie der Klimawandel die Nahrungsketten unseres Planeten verändern wird. Schon mehr als drei Jahre lang haben die Forscher von Microsofts Computational Science Lab in Cambridge an der Entwicklung gearbeitet. Modelliert haben sie bereits das tierische Leben an Land und im Ozean. Was passiert, wenn es keine Bienen mehr gibt? Oder keine Pandabären, Thunfische oder Tiger? So lauten nur einige der Fragen, die sich mit Hilfe der Rechnungen beantworten lassen sollen.

Der Klimawandel und die Folgen für die Nahrungsketten: Was passiert, wenn es auf der Erde keine Thunfische oder Bienen mehr gibt? © picture-alliance/Franco Banfi/WaterFrame

Klassische Klimasimulationen, etwa am Center for Climate Simulation der Nasa in Maryland oder dem Deutschen Klimarechenzentrum (DKRZ) in Hamburg – basieren interessanterweise ist nicht per se auf Big Data: „Wir produzieren riesige Datenmengen, die aber vergleichsweise langweilig sind", sagt der Informatiker Thomas Ludwig, der das DKRZ leitet. Die Ergebnisse der Klimamodellierungen seien ziemlich homogen. „Spannend wird es, wenn man Daten aus anderen Quellen damit zusammenführt."

Genau das versucht ein Team um Anders Levermann vom Potsdam-Institut für Klimafolgenforschung (PIK) mit der Plattform Zeean.net. „Die Wissenschaft ist schon sehr weit gekommen im Verständnis der großskaligen Klimawandelfolgen", erklärt Levermann. „Was wir bisher nicht vorhersagen können, sind aber Veränderungen in den Wetterextremen."

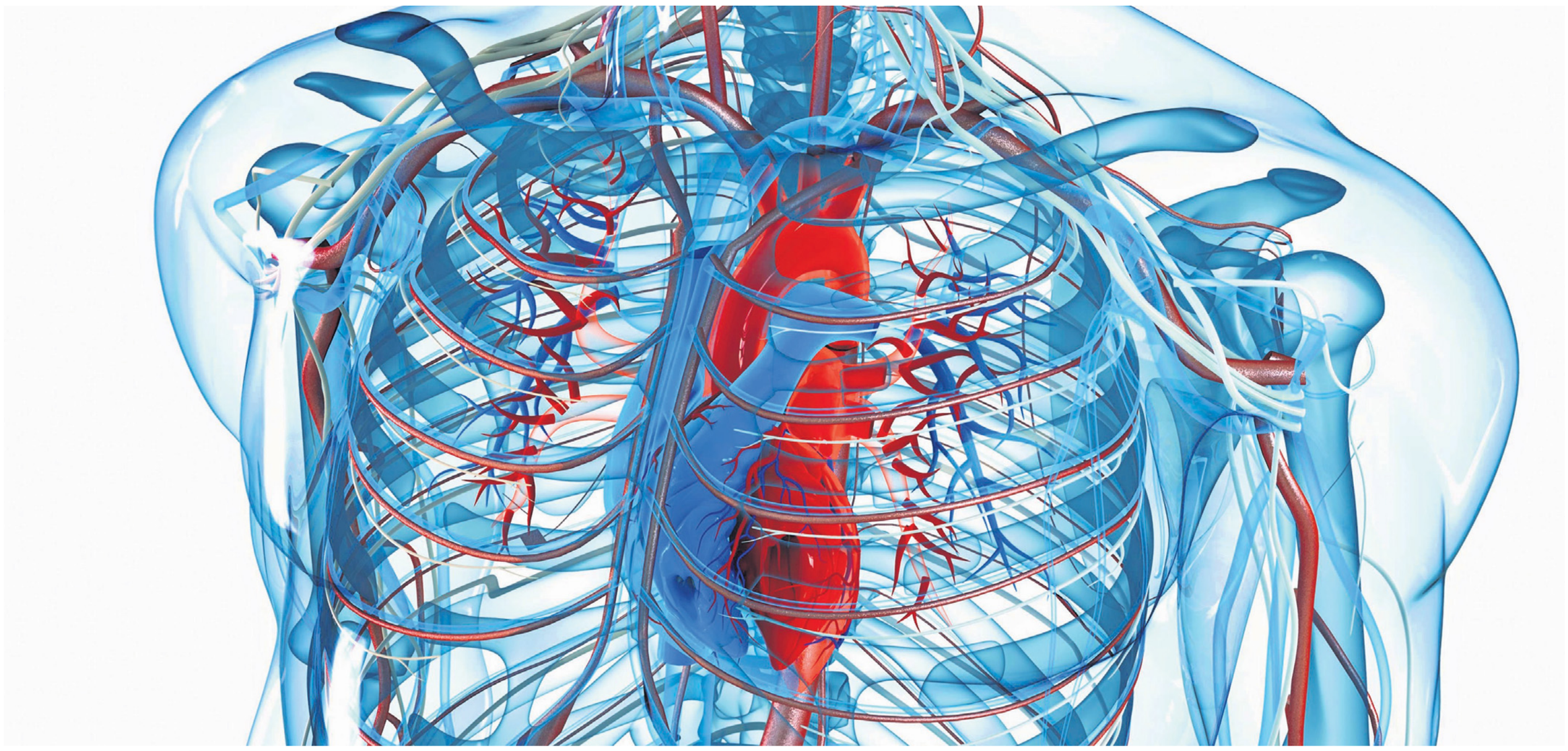
Zeean soll helfen, die wirtschaftlichen Folgen von Extremereignissen zu analysieren. Dabei geht es um ganz konkrete Fragen: Der Taifun Haiyan zum Beispiel verwüstete im November 2013 die Philippinen. Dort werden 60 Prozent des weltweiten Kokosöls produziert. Das wiederum ist eines von nur zwei pflanzlichen Fetten in unseren Lebensmitteln – und damit extrem begehrt. Was also passiert nach solch einem Sturm mit der deutschen Lebensmittelwirtschaft? „Mit Zeean versuchen wir, die Wirtschaftsvernetzung der Welt zu erfassen", sagt Levermann.

Sein Ziel ist es, eine Art Wikipedia für Daten aufzubauen. Dafür brauchen seine Kollegen und er aber die Hilfe der Bevölkerung. Verwendet werden nur öffentlich zugängliche Informationen, andere Nutzer können deren Qualität bewerten. Mit den Daten wird dann das Modell gefüttert, von dem es im kommenden Jahr eine stark verfeinerte Version geben soll.

„Die Arbeit ist kompliziert und wir brauchen alle Hilfe, die wir kriegen können", sagt Levermann. *Christoph Seidler*

Der Autor ist Wissenschaftsredakteur bei „Spiegel Online".

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**



Mit schnellen Rechnern und großen Speichern können heute Gesundheitsdaten umfassend analysiert werden. Das bringt neue Chancen für das Verständnis von Krankheiten. Skeptiker befürchten jedoch den „gläsernen Patienten“. © picture-alliance/Ikon Images

Tiefgekühlt und gut gesichert

FORSCHUNG Wissenschaftler suchen nach den Ursachen für Volkskrankheiten und werten dabei riesige Datensätze aus

Der Schatz ist ganz gut versteckt in dem unscheinbaren Bürogebäude der Charité in Berlin Mitte. Lilian Krist schließt die Türe zu einem kleinen Raum auf, in dem große Kühltruhen stehen. Als sie den schweren Deckel öffnet, steigt Dampf hoch. Die Leiterin des Studienzentrums hebt eine mit Eisflocken bedeckte, flache Platte an, darunter stapeln sich bei minus 80 Grad Celsius kleine schwarze Kästchen, sogenannte Racks. Darin befinden sich Bioproben, frisch entnommen von Probanden, die sich in Berlin an der bisher größten und aufwendigsten Reihenuntersuchung zum Thema Volkskrankheiten in Deutschland beteiligen, der Nationalen Kohorte (NAKO).

Die Bioprobenröhrchen enthalten Blut, Urin, Speichel und Nasensekret der Probanden. Das Biomaterial, sagt Krist, ist tiefgekühlt mindestens 30 Jahre haltbar und damit für die Gesundheitsforschung von unschätzbarem Wert. In einem Raum nebenan werden Urin und Blut mit Hilfe eines Pipettierroboters, der einem größeren Kaffeeautomaten nicht unähnlich ist, auf Röhrchen gezogen. Die Racks gehen dann per Trockeneislieferung in ein zentrales Lager des Helmholtz-Zentrums am Stadtrand von München. Aus Sicherheitsgründen werden dort nur rund zwei Drittel der pseudonymisierten Proben langfristig gelagert, der Rest verteilt sich auf 15 dezentrale Lager, die bundesweit eingerichtet wurden. In einigen Jahren werden rund 28 Millionen Bioproben zur Verfügung stehen.

Herz in 3-D Sicherheit und Datenschutz spielen bei dem über drei Jahrzehnte angelegten Projekt, das seit gut einem Jahr läuft, eine maßgebliche Rolle und sind in langen „Workflows“ niedergelegt. Immerhin werden in 18 Studienzentren Datensätze von 200.000 Menschen im Alter zwischen 20 und 69 Jahren erstellt, wobei die Forscher nicht nur an medizinischen Informationen interessiert sind, sondern auch an Faktoren wie Umwelt, Soziales, Arbeit, Lebensstil und Genetik. Die Fragebögen für die Probanden sind lang, das Untersuchungsprogramm dauert mehrere Stunden. Nach der Anmeldung durchlaufen die Probanden verschiedene Stationen, wo ein Riechtest ansteht und die Handgreifkraft sowie Gewicht und Körperfett gemessen werden. Auch eine Augenuntersuchung und ein Lungenfunktionstest gehören dazu, sogar eine 3-D-Aufnahme des Herzens entsteht hier.

Charité-Projektkoordinator Thomas Keil schwärmt von den technischen Möglichkeiten des Digitalzeitalters und hofft, dass die Gesundheitsforschung von der Politik nicht ausgebremst wird. Es sei höchste Zeit, mehr über Wechselwirkungen bei der Entstehung von Volkskrankheiten wie Diabetes, Krebs oder Demenz zu lernen. „Eigentlich“, sagt er, „hätten wir eine solche Studie schon vor 30 Jahren gebraucht, dann wüssten wir heute mehr zum Beispiel über die Früherkennung von demenziellen Erkrankungen.“ Damals war die Technik aber noch nicht so weit.

Sorgen davor, dass die größte Sammlung an personenbezogenen Gesundheitsdaten in Deutschland in falsche Hände gelangen könnte, hat er nicht und verweist auf die strikte Trennung von „Personidentifizierenden Daten“ und „Pseudonymisierten Studiendaten“. Welchem Probanden welcher Datensatz zuzuordnen ist, weiß nur die unabhängige und speziell gesicherte Treuhandstelle in Greifswald.

> **»Die neuen Technologien vereinfachen die Arbeit der Forscher erheblich.«**
> *Prof. Wolfgang Ahrens, Epidemiologe*

Ähnliche Großstudien laufen laut Keil derzeit in Großbritannien, Frankreich und den Niederlanden, sodass der Forschung damit in einigen Jahren theoretisch ein Datensatz von 800.000 Probanden zur Verfügung steht. Solche riesigen Datenmengen erfordern leistungsstarke Rechner, viel Speicherkapazität und auch Fachleute wie Epidemiologen und Medizinstatistiker, die das Datenmaterial auswerten können. Wie Keil sagt, gibt es in Deutschland noch zu wenige Spezialisten, die diese schwierige Aufgabe beherrschen, bei der NAKO sei jedoch ausreichend Expertise vertreten.

Neue Fragestellungen Dieser interdisziplinäre Ansatz auf der Basis eines IT-gestützten Datenmanagements wird auch als Systemmedizin bezeichnet. Hintergrund ist ein neues Krankheitsverständnis: Es wird nicht mehr davon ausgegangen, dass eine Krankheit nur auf einer Ursache oder einem Mechanismus beruhen muss. So können bestimmte Krebsarten unterschiedliche molekulare Ursachen haben, und ein Gendefekt kann verschiedene Krankheiten hervorrufen, die scheinbar nichts miteinander zu tun haben. Die moderne Medizin orientiert sich an der molekularen Signatur einer Krankheit. Mit sogenannten Omics-Technologien können Biomoleküle einer Zelle erfasst werden, vom Erbgut (Genomics) über Proteine (Proteomics) bis hin zum Stoffwechsel (Metabolomics). An der molekularen Medizin beteiligen sich Mathematiker, Bioinformatiker, aber auch Juristen und Ethiker, denn die Methoden führen zu neuen rechtlichen und ethischen Fragestellungen. Unlängst warfen Wissenschaftler in einem Beitrag die Frage auf, wofür und in welchem Umfang systemmedizinisch fundierte Risiko-Scores klinisch genutzt werden dürfen. Und weiter: „Wer entscheidet über die Mitteilungsbedürftigkeit, und welche Befunde sollen gegebenenfalls mitgeteilt werden? Wie sollen im Rahmen einer Big-Data-Medizin Zusatz- und Nebenbefunde mitgeteilt werden?“

Science Data Der Wissenschaftler Wolfgang Ahrens vom Leibniz Institut für Präventionsforschung und Epidemiologie in Bremen kennt die kritischen Stimmen im Umgang mit Gesundheitsdaten, fordert indes eine faire Interessenabwägung zwischen Datenschutz und Verbraucherschutz im Gesundheitswesen und verweist auf Studien zur Arzneimittelsicherheit, für die „große Datensätze von Millionen Versicherten“ benötigt würden. Dabei sei ein Datenaustausch zwischen Forschern und Krankenkassen sinnvoll, weil Selbstauskünfte von Versicherten oft ungenau ausfielen.

Zudem müsse unterschieden werden zwischen Big Data und Science Data, meint Ahrens, der auch im Vorstand der NAKO sitzt. Bei Big Data sei zunächst unklar, zu welchem Zweck sie erhoben würden, wohin sie gelangten und von wem sie genutzt würden. „Was wir machen, ist Science Data. Unsere Datensammlungen haben einen konkreten Forschungszweck und werden mit Einverständnis der Studienteilnehmer gesammelt.“ Mit der modernen Computertechnologie könnten Daten heute viel besser analysiert und komplexe statistische Modelle gerechnet werden. Das vereinfache die Forschungsarbeit erheblich.

In der NAKO haben die Probanden das Recht, einzelne Ergebnisse, die sich aus dem Monitoring ergeben, nicht zu bekommen. Immerhin könnten bestimmte Befunde einen Lebensplan ändern. Das Recht auf Nichtwissen wird respektiert. Die pseudonymisierten Unterlagen können künftig von industrieunabhängigen Wissenschaftlern für relevante Forschungsfragen beantragt werden. Die Industrie bleibt bei der Langzeitstudie außen vor. Die Herausgabe von Daten an die Pharmaindustrie sei ausgeschlossen, zumal die NAKO als Verein kein Gewinnziel verfolge, versichert Keil, räumt aber ein, dass die Wirtschaft ein starkes Interesse an aufbereiteten Gesundheitsdaten habe, um daraus neue Wirkstoffe und Medikamente zu entwickeln.

Gesundheitsdaten repräsentieren einen milliardenschweren Markt und lösen leicht Begehrlichkeiten aus. Pharmakonzerne erhoffen sich Gewinne, Versicherungen neue Geschäftsfelder. Andererseits werden Industriemittel für den wissenschaftlichen Fortschritt benötigt. Es geht aber auch um Kostensenkungen für Krankenkassen, die mit chronisch steigenden Gesundheitsausgaben zu kämpfen haben (siehe Beitrag unten). Schon lange fordern Experten mehr Effizienz im deutschen Gesundheitssystem. Mit der digitalen Vernetzung sollen die technischen Voraussetzungen dafür geschaffen werden, allerdings bietet das Projekt E-Health nun schon seit mehr als zehn Jahren Anlass für Streit im Zusammenhang mit der elektronischen Gesundheitskarte (eGK). 70 Millionen gesetzlich Versicherte, rund 2.000 Krankenhäuser, 21.000 Apotheken und mehr als 200.000 Ärzte sollen miteinander vernetzt auf die digitale Datenautobahn geschickt werden. Die Regierung spricht von einem national bedeutsamen IT-Projekt, die Gegner vom Einstieg in die gläserne Patientenmanufaktur. Das sogenannte E-Health-Gesetz bekam unlängst im Bundestag Grünes Licht, womit die Weichen in eine Richtung gestellt sind, die nach Ansicht vieler Gesundheits- und IT-Experten unvermeidlich ist. Digital verfügbare Gesundheitsdaten ermöglichen Ärzten den schnellen Zugriff auf präzise Daten der Versicherten. So lassen sich Risiken vermeiden und Therapien miteinander abstimmen - ein selten bestrittener Vorteil gegenüber vergilbten Karteikarten und verloren gegangenen Impfpässen. Die elektronische Patientenakte, der digitale Medikationsplan und das E-Rezept sind auf dem Weg in eine neue gesundheitspolitische Ära schon absehbar. *Claus Peter Kosfeld*

Auf Schritt und Tritt von der App begleitet

GESUNDHEITSDATEN Krankenkassen nutzen den digitalen Fitnesstrend und bieten den Versicherten Boni an

Wenn Christian joggen geht, ist seine Running App immer dabei. Sie erfasst Strecke, Geschwindigkeit, Zeit und Kalorienverbrauch. Damit liegt der junge Mann voll im Trend. Laut einer Studie des Universitätsklinikums Freiburg haben mehr als die Hälfte der Verbraucher Gesundheits-Apps auf ihren Smartphones installiert. Jeder Fünfte nutzt diese häufig. Nach einer Befragung der Universität Bielefeld unter Studenten kontrollieren mehr als 70 Prozent der App-Nutzer ihr tägliches Bewegungspensum oder ihr Schlafverhalten nachts.

Befeuert wird der Trend durch eine riesige Auswahl an Apps und sogenannten Wearables wie Fitnessarmbändern, Sensorkleidung, Datenbrillen und Smartwatches. Laut der Freiburger Studie gibt es mindestens 380.000 Gesundheits-Apps. Allein in den Kategorien „Gesundheit & Fitness“ und „Medizin“ der großen Stores für die Betriebssysteme, Android und iOS (Apple), stehen mehr als 100.000 Apps bereit. Monatlich kommen rund 1.000 hinzu.

Der Bundesverband der Digitalen Wirtschaft beziffert den Umsatz mit E-Health-Produkten allein in Deutschland auf rund 6,5 Milliarden Euro. Der globale Umsatz mit digitalen Gesundheitsprodukten und -dienstleistungen soll Schätzungen zufolge 2020 bei mehr als 200 Milliarden US-Dollar liegen. Großunternehmen wie Google, Apple, IBM, SAP oder Sanofi sind in das Geschäft mit Gesundheitsdaten schon eingestiegen, andere werden folgen.

Was mit den massenhaft aufgezeichneten Daten passiert, ist für die meisten Verbraucher zweitrangig. „Steht ein junger Erwachsener vor der Wahl, eine Gesundheits-App zu installieren, sind die Bedenken hinsichtlich des Datenschutzes nicht ausschlaggebend. Entscheidender ist, wie groß der Gesundheitsgewinn eingeschätzt wird und wie andere die App bewerten“, erläutert der Gesundheitswissenschaftler Christoph Dockweiler die Bielefelder Umfrage. Dass Gesundheitsdaten von Nutzern nicht unbedingt als „sensibel“ eingestuft werden, zeigt eine Studie zur „digitalen Sicherheitslage in Deutschland“. Demnach halten Menschen Onlinebanking und Onlineshopping für weitaus riskanter als vernetzte Gesundheits- und Vitaldienste. Tatsächlich könnte sich laut einer YouGov-Studie sogar fast jeder dritte Deutsche (32 Prozent) vorstellen, seine Gesundheitsdaten an eine Krankenversicherung weiterzugeben, wenn er davon Vorteile hat. Unter den 14- bis 34-Jährigen hätten sogar zwei von drei kein Problem damit, wie eine Umfrage der Schwenninger Krankenkasse ergab.

Die gesetzlichen Krankenkassen haben das Potenzial bereits erkannt und erwägen, ihre Bonusprogramme für gesundheitsbewusstes Verhalten zu ergänzen. So plant die AOK Nordost für 2016 ein Bonusprogramm, „das digital und mobil mit einer neu entwickelten App genutzt werden kann“, wie eine Sprecherin sagt. Wearables bezuschusst die Kasse bereits seit 2015 mit 50 Euro. Auch die DAK passt ihre Programme an. „Voraussetzung für den Zuschuss ist, dass die Geräte mit einer entsprechenden App ausgestattet sind und der Kunde die Dokumentation seiner Gesundheitswerte belegen kann“, sagt ein DAK-Sprecher. Eine elektronische Übermittlung von Trainingsdaten sei aus datenschutzrechtlichen Gründen nicht geplant. „Möglich wäre als Beleg ein Screenshot oder Ausdrucken der Aufzeichnungen.“ Die Versicherungsgruppe Generali will mit dem „Vitality“-Programm ab 2016 gesundheitsbewusstes Verhalten mit einer Fitness-App dokumentieren und belohnen. Als Anreize seien Vergünstigungen beim Sportartikelkauf denkbar. „Eine Senkung der Krankenversicherungsbeiträge für „Vitality“-Teilnehmer ist im ersten Schritt nicht angedacht“, sagt Sprecher Björn Collman.

Verbraucherschützer mahnen, möglichst nicht so viele Daten preiszugeben. „Für Fitness-Training oder Therapien können die digitalen Geräte nützlich sein“, meint Kai Vogel vom Verbraucherzentrale Bundesverband. Dessen ungeachtet sind die Gesundheits-Apps von wachsender Bedeutung. Die Motivation der Nutzer ist dabei höchst unterschiedlich. Einige wollen schlicht ihre Fitness verbessern und fühlen sich von elektronischen Mahnern und durch das Teilen ihrer Daten mit Gleichgesinnten stärker angespornt. Andere nutzen die digitalen Helfer, um Therapien, zum Beispiel bei Diabetes, Herzkreislauferkrankungen oder Raucherentwöhnung zu optimieren.

© picture-alliance/dpa

Smartwatches zeichnen Körperdaten auf.

Christian möchte seine App beim Joggen jedenfalls nicht mehr missen. „Die macht das Training angenehmer. Ich habe meinen elektronischen Coach, der mich anleitet“, sagt der Freizeitalpinist. Dass seine Daten auf irgendeinem Cloud-Server in den USA gespeichert sind und auch von einem Sportartikelhersteller für Produktwerbung via Mail oder SMS genutzt werden können, stört ihn nicht. „Die klicke ich ungelesen weg.“ *Katrin Neubauer*

Die Autorin ist freie Journalistin.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Duell der Unerkannten

CYBERWAR Die Schadsoftware Stuxnet legte Irans Atomprogramm lahm und sorgte damit für den digitalen Erstschlag

In der Wüste von Idaho steht eines der größten Forschungszentren für Energiegewinnung der Welt. Mehr als 50 Atomreaktoren wurden auf dem Gelände gebaut, zwei sind noch in Betrieb. Im März 2007 richtet sich die Aufmerksamkeit der Forscher auf einen simplen Dieselgenerator. Der ruckelt ein paar Mal, erst steigt weißer Rauch auf, dann schwarzer, dann fliegt die Maschine auseinander. In wenigen Minuten zerstören die Forscher den Generator – aus der Ferne. Das Experiment ist als „Aurora Generator Test“ in die Geschichte der IT-gestützten Kriegsführung (Cyberwar) eingegangen.

Welche Ausmaße so ein IT-Schaden annehmen kann, wurde 2010 bekannt. Damals sorgte ein Sabotageprogramm für Wirbel, das in verschiedenen Industriesteueranlagen gefunden wurde. Was anfangs nach Industriespionage aussah, entpuppte sich als der bis dato schwerwiegendste Fall IT-gestützter Kriegsführung. Stuxnet hatte die iranische Atomanreicherung unterwandert und manipuliert. Das Programm zerstörte die Zentrifugen in der Urananreicherungsanlage in Natanz. Das Atomprogramm des Landes wurde für Jahre zurückgeworfen. Stuxnet gilt als erste belegte Aktivität digitaler Kriegsführung mit konkreter Schadwirkung in der physischen Welt, eine Art digitaler Erstschlag.

Sichere Distanz Als Urheber werden die USA und Israel vermutet. Bis heute bleibt Stuxnet der einzige halbwegs gesicherte Vorfall der digital geführten Kriegführung, der zu einem expliziten Schaden geführt hat. Zumindest ist es der einzige Vorfall, der auf eine, wenn man so will, digitale Angriffswaffe zurückzuführen ist. Doch auch die im Jugoslawienkrieg eingesetzten Mittel wie Überwachung und Manipulation der Telefonnetze, elektronische Angriffe auf Banken und verschiedene Abhöraktionen werden dem Arsenal der elektronischen Kriegsführung zugeschrieben. Und wenn es um Schäden geht, dürften Drohnen-Angriffe einen der vorderen Plätze belegen. Auch diese Waffen werden heute rein digital und aus großer Entfernung eingesetzt.

Der größte Vorteil des Krieges auf dem digitalen Schlachtfeld dürfte sein, dass die eigenen Kräfte kaum gefährdet sind. Während konventionelle Waffen immer auch das Leben der eigenen Soldaten bedrohen, kann ein digitaler Krieg aus sicherer Distanz geführt werden. Auch die gegnerische Seite profitiert unter Umständen. Der Einsatz von Stuxnet hat nach derzeitigen Kenntnissen kein einziges Menschenleben direkt gefordert.

Geringe Kosten Jedoch steigt mit der zunehmenden Zahl an Vorfällen, die der digitalen Kriegsführung zugerechnet werden, die Gefahr eines Gegenschlages mit konventionellen Waffen. Auch das Risiko, dass ein digitaler kriegerischer oder auch terroristischer Angriff urbane Infrastrukturen in Schutt und Asche legt, wird größer.

Geringe Kosten gelten als der zweite große Vorteil eines Angriffs mit einer digitalen Waffe. So gilt Stuxnet, der einen drei- bis vierstelligen Millionenbetrag gekostet hat, durchaus als Schnäppchen – zumindest aus militärischer Sicht, erklärt Ralph Langner, der die Schadsoftware als einer der ersten analysiert hat: „Stuxnet hat vom Ergebnis her genau das Gleiche erreicht wie ein Luftschlag. Und das zu einem Spottpreis, bei dem auch jeder Militär sagen muss: wunderbar, das machen wir natürlich künftig immer so.“

> **»Stuxnet hat vom Ergebnis her genau das Gleiche erreicht wie ein Luftschlag.«**
> *IT-Experte Ralph Langner*

Besonders verlockend für Militärs ist auch der dritte große Vorteil eines digitalen Angriffs: Die Möglichkeiten der perfekten Verschleierung. Wer clever und gut ist, fliegt nicht auf. Demzufolge sind auch Schuldzuweisungen mit Vorsicht zu genießen. So werden China und Russland immer wieder pauschal mindestens der digitalen Spionage verdächtigt. Die USA bezichtigten China zuletzt des Angriffs auf eine US-Krankenversicherung. Konkrete Beweise wurden nicht veröffentlicht.

Gute Tarnung Meist lässt sich weder feststellen, woher ein Angriff kommt, noch, wer dahinter steckt. Der IT-Sicherheitsberater Christoph Fischer betont: „Seit es Geheimdienste gibt, tarnen die sich. Und sich auf Computern zu tarnen, ist noch viel einfacher als im richtigen Leben.“

So nutzen mutmaßlich viele Geheimdienste aus, dass gerade Russland, aber auch China massiv in den digitalen militärischen Sektor investieren. „Ich würde sagen, dass sich einige eine chinesische Tarnkappe überziehen“, meint Sicherheitsexperte Fischer.

Warum aber wurde Stuxnet bekannt? Experten gehen davon aus, dass die Schadsoftware nach erfolgreichem Einsatz noch eine weitere Funktion hatte. Die Urheber wollten entdeckt werden, sie wollten zeigen, was sie können und dass sie gewillt sind, ihre Fähigkeiten einzusetzen.

ür Staaten wie Deutschland gilt es vor allem, digitale Bedrohungen abzuwehren. Doch künftig soll auch die Bundeswehr die Fähigkeiten der digitalen Kriegsführung ausbauen – ungeachtet der Tatsache, dass die Truppe schon seit Jahren international anerkannte und begehrte Ausrüstung vorweisen kann, wie die Flottendienstboote „Alster“, „Oker“ und „Oste“, die maßgeblich zur elektronischen Informationsgewinnung über Ex-Jugoslawien beitrugen. Verteidigungsministerin Ursula von der Leyen (CDU) will die vorhandenen Fähigkeiten zentral bündeln und erweitern. Verschiedene Medien schreiben, damit wolle die Ministerin die Armee für die „Cyber-Kriegsführung“ umbauen. Doch worum geht es – Angriff oder Abwehr? Für letzteres gäbe es eine effektivere „Waffe“: Eine Pflicht, Sicherheitslücken in Hard- und Software zu schließen und in angemessener Zeit zu veröffentlichen. Außerdem sollten Unternehmen für Fehler haften. Solche Pflichten würden gleich in mehrfacher Hinsicht für mehr Sicherheit sorgen. Denn wenn Lücken schnellstmöglich nach Bekanntwerden geschlossen würden, würde das einen florierenden Handel austrocknen: Besonders effektive Lücken werden für hohe Summen weitergegeben. Die Lücken, die Stuxnet ausgenutzt hat, sollen mehrere Millionen US-Dollar wert gewesen sein. Ohne eine solche Pflicht bleibt alles, wie es ist: Der Handel blüht, Militärs und Nicht-Militärs rüsten gegenseitig weiter auf und es wird immer wieder zu schweren Zwischenfällen kommen, wie dem Hacker-Angriff auf den Bundestag.

Wirksamer Schritt Ein Vorwurf aus IT-Kreisen lautet: Mit dem 2015 verabschiedeten IT-Sicherheitsgesetz hätten sowohl die Haftung für als auch die Veröffentlichung von Sicherheitslücken festgeschrieben werden können. Doch diese Abwehrmaßnahme im digitalen Krieg will sich offenbar niemand leisten. „Das IT-Sicherheitsgesetz ist ein Witz, ein vollständiger Fehlanreiz“, kritisiert die Informatikerin Constanze Kurz, Sprecherin des Chaos Computer Clubs. Mit weniger bestehenden Sicherheitslücken hätten es auch Angreifer in der digitalen Welt schwer – egal ob IT-Kriminelle oder bewaffnete Kräfte. Trojaner, Viren, Würmer und andere digitale Angriffswerkzeuge würden vielfach ins Leere laufen. Es wäre nicht der einzige, aber ein ziemlich wirksamer Schritt im „Cyber-Kampf“.

Jan Rähm

Der Autor ist freier Journalist.

Spezialisten versuchen heutzutage, Cyber-Angriffe auf Regierungsstellen, Unternehmen oder kritische Infrastrukturen zu verhindern © picture-alliance/empics

Wenn Computer potenzielle Täter ausfindig machen

KRIMINALITÄT Die Polizei setzt in der Verbrechensbekämpfung auch auf Datenanalysen. Nicht immer mit Erfolg

Am Tatort sein, bevor der Täter verschwinden kann, ja vielleicht sogar, bevor er überhaupt Zeit hatte, seine Tat zu begehen – Computerprogramme versprechen der Polizei, ihr diesen Traum zu erfüllen. Mit Datensammlungen und Statistik soll es ihr möglich werden, Verbrechen vorherzusehen. Predictive Policing heißt das Konzept, voraussagende Polizeiarbeit. Weltweit arbeiten Firmen an diesem Versprechen und hoffen auf einen riesigen Markt.

IBM hat dafür „Blue Crush“ programmiert, eine Weiterentwicklung der firmeneigenen Software SPSS, die in der Wissenschaft seit vielen Jahren zur statistischen Analyse eingesetzt wird. Die Polizei in der amerikanischen Großstadt Memphis setzt „Blue Crush“ ein, um Kriminalität zu bekämpfen, die Tennessee Highway Patrol will mit ihr Unfallschwerpunkte erkennen. „Predpol“ basiert auf Algorithmen aus der Erdbebenforschung. Polizisten in Los Angeles, in Atlanta und auch die Metropolitan Police in London nutzen das Programm.

„Precobs“ ist ein deutscher Anbieter, dessen gleichnamige Software in mehreren Bundesländern getestet wird, um Einbrecher zu fangen. Bei der Stadtpolizei in Zürich ist sie bereits im Dauereinsatz. Palantir Technologies wertet für seine Vorhersagesoftware frei zugängliche Daten in sozialen Netzwerken aus und bietet die Ergebnisse unter anderem dem US-Geheimdienst CIA an. Accenture ist eigentlich eine Management-Beratungsfirma, aber auch sie hat ein Computersystem entwickelt, um Kriminelle zu erkennen. Die Guardia Civil in Spanien hat es eingesetzt und auch die Londoner Polizei. Accenture will damit nicht Orte von Kriminalität untersuchen, sondern gar einzelne Menschen aus Datensätzen filtern, die mit hoher Wahrscheinlichkeit Gewaltverbrechen begehen werden.

Prognosesoftware soll dabei helfen, Einbrüche vorherzusagen. © picture alliance/blickwinkel

Daten für die Polizei zu analysieren ist eine wachsende Industrie. Die Programme machen letztlich alle dasselbe: Sie sollen auf Basis vorhandener Daten errechnen, wo wann und mit welcher Wahrscheinlichkeit ähnliche Verbrechen geschehen werden. Früher taten Beamte das gleiche mit Hilfe von Erfahrung und einer Karte ihrer Stadt. Sie steckten bunte Stecknadeln hinein, um Orte zu erkennen, an denen bestimmte Taten häufiger begangen wurden. Computer sind genauer. Vor allem aber können sie viel mehr Daten in die Analyse einbeziehen. Neben den polizeieigenen Daten über Kriminalität können das auch die Altersstruktur sein, die Einkommensverteilung, der Mietspiegel oder Standorte von Geldautomaten. Doch ist das nur der Anfang. Verkehrsmessungen und selbst der Wetterbericht spielen in mancher Kalkulation eine Rolle. Und Facebook, Twitter, YouTube oder Instagram bieten noch viel mehr Quellen für Informationen.

Klare Muster Trotz der Daten und komplexen Rechenmodelle kann Predictive Policing das gemachte Versprechen bislang nicht erfüllen. Denn längst nicht alle Taten eignen sich dafür. Mord etwa lässt sich kaum vorhersagen, zu selten kommt er vor, um eine gute Datenbasis zu haben, zu irrational und persönlich sind oft die Motive. Spontane Taten sind auf diese Art kaum zu erfassen. Die Software ist immer dann gut, wenn sich im Verhalten zumeist professioneller Täter klare Muster finden. Wer hingegen nachts mit einem riesigen Flachbildfernseher durch die Straßen schleicht, ist entweder ein Idiot, oder ein Beziehungstäter, der das Gerät seiner Ex-Freundin wegnehmen will. Beides kann kein Computer vorherberechnen.

Die Firmen, die Vorhersageprogramme anbieten, werben trotzdem damit, die Verbrechensraten um bis zu 30 Prozent senken zu können. Zum Teil wirken die Erfolge auch beeindruckend. Die Züricher Polizei ist beispielsweise überzeugt, dass sie dank „Precobs“ die Zahl der Einbrüche auf den niedrigsten Stand seit Jahren senken konnte. Doch haben die Hersteller auf wichtige Fragen keine Antwort: Zum Beispiel auf die, ob die Täter durch die gezielten Streifen nicht einfach woandershin verdrängt werden. Oder ob sie auf andere Taten ausweichen und ob sie nun Handtaschen rauben, statt Wohnungen leerzuräumen.

In Deutschland werden nur zehn bis 15 Prozent aller Wohnungseinbrüche aufgeklärt – das Interesse der Polizei ist daher hoch, diese Systeme zu nutzen. Precobs, Predpol, IBM, sie alle werden auch hierzulande erprobt, zum Teil in großen und langdauernden Studien. Kritiker sehen das mit Sorge. Denn da ist auch noch der Datenschutz. In Deutschland ist es der Polizei verboten, bestimmte Datenbanken zu einer neuen zusammenzuführen. Deswegen verwendet Precobs nur wenige und anonymisierte Daten für die Analyse. Gezielt potenzielle Menschen zu identifizieren, ist damit nicht möglich und soll es auch auf keinen Fall sein.

In anderen Ländern hat man weniger Skrupel, in Großbritannien und den USA werden gezielte Gefährderanalysen eingesetzt und die so Stigmatisierten von der Polizei beobachtet und gewarnt. In Chicago heißt das Konzept „Heat List“. Wen die Computer auf diese Liste setzen, weil er in einer schlechten Gegend lebt und Freunde hat, die gewalttätig waren oder sind, bekommt Besuch von der Polizei. Ob es immer die richtigen trifft? Das ist schwer zu sagen. Wenn der Mensch auf der Liste keine Tat begeht, ist nicht klar, ob er es entweder nie vorhatte, oder ob es dank der Software verhindert werden konnte.

Kai Biermann

Der Autor gehört zum Investigativ-Team bei „Zeit Online“.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Sammeln und sortieren

GEHEIMDIENSTE Die Stasi hätte gerne Facebook genutzt

Geheimdienste sammeln Informationen. Das haben sie früher schon getan. Jedoch haben sich die Methoden verändert. Bei der DDR-Staatssicherheit war quasi alles noch Handarbeit, heute laufen Suchprozesse vollautomatisch ab. Aus der analogen Zettelwirtschaft der Stasi ist ein digitales High-End-Produkt geworden mit unbegrenzten Filtermöglichkeiten nach Stichworten und Personen. Ein früherer Stasi-Offizier merkte einmal zu den von Whistleblower Edward Snowden aufgedeckten Schnüffelmethoden des US-Geheimdienstes NSA an: „Hätten wir solche Möglichkeiten gehabt, wäre unser Traum in Erfüllung gegangen.“

Datenmissbrauch Der Vergleich zwischen Stasi (rund 90.000 hauptamtliche Mitarbeiter) und NSA (rund 40.000 Mitarbeiter), sagt der Chef der Stasiunterlagenbehörde, Roland Jahn, in einem Video-Blog für die Bundeszentrale für politische Bildung, liege zwar auf der Hand. Er hinke aber deswegen, weil der eine Dienst einer Diktatur diente, der andere letztlich für die Freiheitsrechte einer Demokratie stehe. In der DDR habe die Stasi im Interesse der Einheitspartei gelauscht, in der Demokratie sei das Abhören rechtsstaatlich geregelt. Datenmengen allein seien wenig aussagekräftig, entscheidend sei die Frage, wo Daten missbraucht und Menschen in ihrem Selbstbestimmungsrecht übergangen würden, meint Jahn.

Die Aktivisten der Organisation OpenDataCity (ODC) haben, unabhängig von der politischen Einordnung, gleichwohl die Datenmengen von Stasi und NSA visualisiert (http://bit.ly/1GmV3Ij), um den Unterschied zwischen damals und heute zu verdeutlichen. Die Datenaufbereitungsspezialisten von ODC nahmen dabei als Basis eine Zahl, die von einem ehemaligen NSA-Technikdirektor stammt und vom National Public Radio (NPR) in den USA veröffentlicht wurde. Demnach kann das neue Datenzentrum der NSA in Utah fünf Zettabyte (21 Nullen) an Speicherkapazität verarbeiten. Die Aktivisten rechnen sodann vor: „Unter der Annahme, dass ein Aktenschrank 0,4 Quadratmeter Platz benötigt und 60 Aktenordner (30.000 Seiten Papier), also etwa 120 Megabite Daten fassen kann, würde das Utah-Rechenzentrum ausgedruckt etwa 17 Millionen Quadratkilometer Platz verbrauchen. Damit kann die NSA fast eine Milliarde Mal mehr Daten erfassen als die Stasi!“

Inzwischen werden auch andere Vergleiche gezogen, weil sich die Ausgangslage ideell drastisch verändert hat. So verweisen Netzaktivisten auf das größte soziale Netzwerk Facebook, dem rund 1,5 Milliarden Menschen ihre persönlichen Daten überlassen. Zum Vergleich: Die Stasi hatte vor allem die eigene Bevölkerung fest im Blick, das waren rund 16 Millionen Einwohner.

Der Facebook-Konzern betreibt nach einem Bericht der „Frankfurter Rundschau“ über seine elektronische Gesichtserkennung die international größte Datenbank mit biometrischen Merkmalen. Auf den Serverfarmen der Firma liegen demnach mehr als 75 Milliarden Fotos, davon mindestens 450 Millionen, die mit Personennamen (getaggt) sind. Und das alles ganz freiwillig.

Jahn stellte dazu in einem Gespräch fest: „Wenn ich in Schulen über die Stasi erzähle, kommt die Diskussion sofort auf Facebook und die Bundestrojaner. Das finde ich klasse.“ Seiner Ansicht nach hätte die Staatssicherheit ein Instrument wie Facebook „brutal genutzt“. Die Stasi mit ihrer opulenten Zettelsammlung, den Tonbändern, Wanzen und Videos, die einst den zweifelhaften Ruf des „besten Geheimdienstes der Welt“ genoss, wirkt heute technisch natürlich total antiquiert. In einem Punkt hat die Stasi aber bis heute zumindest skurrile Maßstäbe gesetzt: mit ihrem ominösen Geruchsprobenarchiv.

Claus Peter Kosfeld

Die große Hoffnung

TRANSPARENZ Mehr Demokratie, mehr Innovation – das sind die großen Versprechen von Open Data. In Deutschland werden staatliche Daten nur Schritt für Schritt weitergegeben, weil eine zentrale Gesetzesgrundlage fehlt

Hamburg gilt mit seinem Transparenzgesetz als bundesweiter Vorreiter in Sachen Open Data. © Stephan Roters

Das Versprechen von Open Data ist groß: Wenn der Staat Daten und Informationen für alle Beteiligten leichter verfügbar macht, wird politisches Handeln nicht nur demokratischer, sondern auch effizienter. Unternehmen können die Daten für neue Geschäftsmodelle verwenden, womit der Staat mit seinen Daten erheblich zur Entwicklung der Digitalwirtschaft beitragen kann. Es geht dabei nicht mehr um eine exklusive Vermarktung der Daten, sondern um eine Verwertung frei verfügbarer Daten durch verschiedene Analysen, die von einem möglichst großen, verlinkbaren Datenbestand profitieren.

Dass mit Open Data verschiedene Ziele erreicht werden können, zeigte eine Analyse der Weltbank bereits 2003 anhand eines Index für Transparenz und für Informationszugang: Regierungshandeln wird besser, wenn diese beiden Faktoren positiv sind. Und ein besseres Regierungshandeln geht wiederum mit einem höheren Wirtschaftswachstum einher. Das Gutachten „Open for Business“, das 2014 im Rahmen des G20-Treffens veröffentlicht wurde, kommt zu dem Schluss, dass Open Data das Wirtschaftswachstum in den G-10-Staaten um 1,1 Prozent über einen Zeitraum von fünf Jahren steigern könnte.

Am erfolgreichsten sind derzeit Unternehmen, die Analyse-Dienstleistungen für verschiedene Industriebranchen anbieten. Sie kombinieren frei verfügbare Daten mit selbst erstellten Informationen. Die häufigsten Geschäftsmodelle sind Bezahlmodelle mit einer Dienstleistung, wie sie etwa die Climate Corporation anbietet. Das US-Unternehmen nutzt staatliche Wetter- und Satellitendaten, mit denen das Wachstum von Ackerpflanzen modelliert werden kann. Historische Daten wie Wetter, Boden und Pflanzenertrag werden mit aktuellen Wettermodellen kombiniert, um Prognosen für Pflanzen auf einzelnen Feldern erstellen zu können. Das Unternehmen wurde vor einiger Zeit von Monsanto für über eine Milliarde Dollar übernommen.

„Open Data“ in Deutschland kommt bislang nicht so richtig voran. In ihrer im Dezember präsentierten Umfrage unter 134 Ländern stellte die britische „Open Knowledge Foundation“ fest, dass Deutschland im Kreis der Industrieländer im „Global Open Data Index“ deutlich vom Vorjahresplatz 9 auf Platz 26 zurückfiel. In keiner der 13 Kategorien konnte sich Deutschland verbessern, hingegen wurde es in den Bereichen Gesetzgebung und Unternehmensregister schlechter eingestuft.

Der „Open Data Index“ ist recht streng: Positiv wird bewertet, wenn Daten online und kostenfrei verfügbar sind und überdies regelmäßig aktualisiert werden. Punkten können die Länder außerdem mit offenen Lizenzen, Maschinenlesbarkeit und großen zusammenhängenden Datenmengen. Wegen letzterem schnitt Deutschland in diesem Jahr bei den Daten zu Wahlergebnissen schlechter ab, weil etwa Daten auf der Ebene von Wahlstationen nicht verfügbar sind, sondern nur an Orten mit über 100.000 Personen.

Ohne gesetzliche Grundlage sehen Behörden keinen Handlungsbedarf.

Während Spitzenreiter Großbritannien für sein Open-Data-Portal bereits 25.000 Datensätze frei gegeben hat, sind es in Deutschland nur rund 15.000. Darunter sind knapp 3.000 Datensätze, die nur eingeschränkt verwendet werden dürfen. Es fehlen wichtige Daten wie beispielsweise zu staatlichen Ausschreibungen und Vergaben sowie Wirtschaftsdaten wie etwa das Handelsregister und Geodaten. Die Anzahl der verwendeten Lizenzen bezeichnet die Open Knowledge Foundation als „unüberschaubar“, immerhin ein Viertel sei nicht offen.

Ziele im Koalitionsvertrag Die Bundesregierung will Open Data Schritt für Schritt umsetzen. Bisher hat sie das Thema mit dem weiten Blick auf „Open Government“ im Bundesinnenministerium verankert. Dort werden aber derzeit die relevanten 1,5 Personalstellen abgebaut. Auf eine parlamentarische Nachfrage der grünen Bundestagsfraktion teilte das Ministerium mit, dass ein Beitritt zum weltweiten Bündnis „Open Government Partnership“ lediglich „geplant“ sei, obgleich dieser im Koalitionsvertrag bereits beschlossene Sache war. In diesem Zusammenschluss von mehr als 60 Staaten sollen mit Hilfe von Open Data verschiedene Ziele erreicht werden, wie etwa eine größere politische Offenheit durch Transparenz und eine bessere Zusammenarbeit mit der Zivilgesellschaft.

Im Koalitionsvertrag wurde eine gesetzliche Grundlage angekündigt, um Verwaltungsbehörden die Veröffentlichung von Daten zu erleichtern. Zwar gibt es inzwischen einige Gesetze mit Open-Data-Bezug, doch ein zentrales Dateninfrastrukturgesetz wurde noch nicht geschaffen. Jörn von Lucke, Professor an der Zeppelin-Universität in Friedrichshafen und Leiter des Open Government Institute, betont: „Wenn wir uns an den Aufbau einer Dateninfrastruktur machen, brauchen wir auch Gesetze, auf deren Grundlage Geld und Personal bereitgestellt werden können.“ Sonst sähen die Behörden keine Notwendigkeit zu handeln, sagt von Lucke.

Einblick in die Skepsis der Verwaltung gibt Göttrik Wewer, E-Government-Lobbyist bei der Deutschen Post und ehemaliger Staatssekretär im Bundesinnenministerium. Zur US-Initiative „Open Government Partnership“ schrieb er, dass Deutschland seinen Beitritt „sorgfältig“ abwägen sollte, da damit eine „neue staatliche Daueraufgabe mit einem erheblichen Koordinierungsaufwand“ entstünde. Die Regierung würde „zur Getriebenen von Aktivisten, ohne dass wesentliche Fortschritte für Good Governance“ zu erwarten seien. Strategisch diene die Initiative der USA dazu, „autoritäre Regime durch eine offizielle Partnerschaft und durch die Aktivierung der Zivilgesellschaft ‚von oben‘ und ‚von unten‘ gleichsam in die Zange zu nehmen“.

Innovative Sicht Hamburg gilt mit seinem Transparenzgesetz als bundesweiter Vorreiter. Das bisherige Open-Data-Portal der Stadt ist inzwischen im Transparenzportal aufgegangen. Die Stadt will den Umgang mit Open Data in der öffentlichen Verwaltung fördern. So wird derzeit geprüft, welche weiteren Daten veröffentlicht werden können. Live-Daten gibt es auch bereits, wie etwa Parkplatzbelegungsdaten und die jeweils größten 50 Baustellen. Auch wurde die technische Infrastruktur so gestaltet, dass Verwaltungsmitarbeiter praktisch per Klick entscheiden können, ob und wie sie Daten der Behörde veröffentlichen. Die zur Veröffentlichung verpflichteten Unternehmen haben aber bisher nur „verhältnismäßig wenige Unterlagen“ veröffentlicht, berichtet der Hamburger Informationsfreiheitsbeauftragte Johannes Caspar.

Hamburg hat mit seinem Transparenzgesetz bundesweit eine Vorreiterrolle.

Für von Lucke ist klar, dass es eine innovative Sicht auf Open Data braucht: „Wir müssen aus staatlicher Sicht eine Geschäftsfeldentwicklung vornehmen.“ Vorbildlich sei Großbritannien, das 2012 ein „Open Data Institute“ (ODI) mit 10 Millionen Pfund Wirtschaftsförderung eingerichtet hat, da es Open Data als wichtigen Motor der Digitalwirtschaft begreift. Mit seinem Inkubator fördert das Institut datengetriebene Startups. In Wien wurde in diesem Jahr mit dem „ODI Node Vienna“ ein Ableger gegründet, der über die Vernetzung mit weiteren „Nodes“ und Initiativen das „Open-Data-Ökosystem“ weiter aufbauen soll.

Alexander Dobrindt (CSU), Bundesminister für Verkehr und digitale Infrastruktur, stellt jetzt im Rahmen eines „Modernitätsfonds“ 100 Millionen. Euro Fördergelder für „digitale Innovationen“ bereit. Erst im November organisierte er mit dem „BMVI Data-Run“ den ersten staatlichen Hackday zu Mobilitätsdaten, dessen Gewinner aus dem Fonds eine Förderung erhielt. Dies wertet von Lucke als einen ersten Schritt in die richtige Richtung. Letztlich müsse der Staat aber die Frage beantworten: „Wie stellen wir sicher, dass datengetriebene Innovation auch in Deutschland eine Chance hat? Wir dürfen uns von dieser Entwicklung nicht abkoppeln.“

Christiane Schulzki-Haddouti

Die Autorin arbeitet seit 1996 als IT- und Medienjournalistin.

Gescheitert an inneren Widersprüchen

PIRATENPARTEI Den Anspruch, mit Hilfe des Internets und direkter Demokratie eine andere Politik zu machen, konnte die neue Partei nicht umsetzen

Was ist der Unterschied zwischen der Vorratsdatendatenspeicherung und der Piratenpartei? Während der ewige Zombie der Netzpolitik wieder fröhliche Auferstehung feiert, kommt einer ihrer schärfsten Gegner nicht mehr aus dem Keller der Umfragen heraus. Ob Netzneutralität, Datenschutzverordnung, Urheberrecht, Massenüberwachung: Wenn es Julia Reda nicht mit Ach und Krach ins Europaparlament geschafft hätte, gäbe es derzeit keine einzige wahrnehmbare Stimme aus der Piratenpartei in netzpolitischen Debatten. In Deutschland genauso wenig wie in Europa.

Kein Wunder, dass Medien und Politikexperten die Partei inzwischen abgeschrieben haben. Der Namensgeber, der schwedische Pirate-Bay-Gründer Peter Sunde, bedauerte im April 2015, dass die Internet-Themen in Form einer politischen Partei vertreten würden. „Geh in andere Parteien und bring ihnen die naheliegenden Themen bei“, forderte er die Mitglieder auf. Sogar die früheren Parteivorsitzenden Bernd Schlömer und Sebastian Nerz leisteten dem inzwischen Folge und traten im vergangenen Oktober in die FDP ein.

Musste es in den vier Jahren seit dem 18. September 2011 so weit kommen? Damals waren die Piraten mit einem fulminanten Erfolg (8,9 Prozent) ins Berliner Abgeordnetenhaus gezogen und mischten gut ein Jahr lang den deutschen Politikbetrieb auf. Innerhalb von zwölf Monaten verdreifachte sich fast die Zahl der registrierten Mitglieder bundesweit auf rund 34.000. Derzeit liegt sie wieder bei etwa 17.000, wobei nur jeder dritte stimmberechtigt ist, weil er seine Mitgliedsbeiträge überweist. Für eine angebliche Mitmachpartei ist das sehr wenig. Dazu hatte nun offenbar auch der Fraktionschef der Piraten im Berliner Abgeordnetenhaus keine Lust mehr und trat im Dezember 2015 aus der Partei aus.

Plötzlich Protestpartei Der Niedergang war von Anfang an im Aufstieg angelegt. Aus der Nischenpartei mit dem Kernthema Netzpolitik war über Nacht eine Protest- und Nichtwählerpartei geworden. Dass diese Klientel nicht bei der Stange gehalten werden konnte, lag im Konzept der Partei selbst begründet. Sie warb mit dem Charme des Dilettantischen, Direkten und Undisziplinierten. Doch genau das war es, was viele Bürger wieder hatte auf Distanz gehen lassen. Politologen schätzten die internetaffine Kernwählerschaft der Piraten nie höher als 2,0 bis 2,5 Prozent ein.

Bei dem Versuch, sich inhaltlich breiter aufzustellen, zerfleischten sich die verschiedenen Flügel gegenseitig. Es ist klar, dass Piraten gegen Vorratsdatenspeicherung, Netzsperren, Leistungsschutzrecht, Überwachung und für Netzneutralität sind. Aber wenn es beispielsweise um Wirtschaftspolitik ging, fanden auf Massenparteitagen mit 2.000 Mitgliedern wie 2012 in Bochum selbst allgemein gehaltene Positionen keine Mehrheit. Die Piraten scheiterten an ihrem Anspruch, mit Hilfe des Internets und direkter Demokratie eine andere, gar bessere Politik zu machen.

Im Gegenteil: Das Netz mit seinen Twitter-Stürmen und öffentlichen Pöbeleien verhinderte sogar, dass sich konstruktive Diskussionskultur etablieren konnte. Der Versuch, über das Internet eine „ständige Mitgliederversammlung“ einzurichten, ist bundesweit nie umgesetzt wurden. Auch in dem Fall des Abstimmungstools Liquid Feedback scheiterte die Partei an ihren inneren Widersprüche. Den Technikbefürwortern wie Christopher Lauer, die moderne Werkzeuge für eine demokratische Beteiligung nutzen wollten, standen extreme Datenschutzverfechter wie der Kieler Landtagsabgeordnete Patrick Breyer gegenüber. Das Misstrauen gegen jede Art von elektronischer Überwachung und Datenspeicherung übertrug sich auf die eigene Partei. Auffallend bei den Piraten war zudem die Tatsache, dass sie viele politikferne Menschen angezogen hat. Die Aussage: „Ich wollte nie was mit Politik zu tun haben, bis ich die Piraten kennenlernte“, war häufig von Mitgliedern zu hören. Politikroutiniers, die schon in anderen Parteien Erfahrung gesammelt hatten, wurde eher mit Skepsis begegnet.

Bruno Kramm, Chef der Berliner Piraten, im Mai 2015 bei einer Protestaktion vor dem Kanzleramt © picture-alliance/NurPhoto

Gerade auf Bundesparteitagen war bei vielen Teilnehmern häufig der Wille zu spüren, sich politischem Denken und Handeln komplett zu verweigern. Versammlungsleiter beklagten eine fehlende politische Bildung und aggressive Grundhaltung. Die Piraten erschienen somit von außen wie ein Fußballverein, bei dem jedes Mitglied nicht nur über die Mannschaftsaufstellung entscheidet, sondern sich auch noch selbst ins Spiel einwechseln kann, um dann möglichst viele Eigentore zu schießen. Selbst der im August 2014 angekündigte erste bundesweite „Basisentscheid“ per Post konnte wegen der Klage eines Mitglieds nie gestartet werden.

Nach Ansicht des Politologen Oskar Niedermayer sind die Piraten inzwischen aus den Köpfen der Leute verschwunden. „Zwar sind die inhaltlichen Streitereien nach der Niederlage des so genannten progressiven Flügels auf dem Parteitag 2014 deutlich zurückgegangen. Nur: Das interessiert kaum mehr jemanden“, sagt Niedermayer. Die finanzielle Situation werde immer prekärer, so dass die Partei kaum mehr in der Lage sei, einen flächendeckenden Wahlkampf zu finanzieren. „Die Piraten haben immer noch kein strategisches Zentrum, das in der Lage wäre, inhaltliche Steilvorlagen wie den Beschluss zur Vorratsdatenspeicherung aufzugreifen und die Partei wieder ins Gespräch zu bringen“, sagt Niedermayer.

Friedhelm Greis

Der Autor ist netzpolitischer Redakteur bei dem Internetportal golem.de.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Der Google-Staat

ALGORITHMEN Wie der US-Internetkonzern zunehmend Politik auf leisen Sohlen macht

Eingang zur neuen Welt: Googolplex, die Zentrale von Google im kalifornischen Mountain View mitten im Silicon Valley © picture-alliance/landov

Es ist das größte Betriebsgeheimnis überhaupt: Googles Suchalgorithmus PageRank. Er entscheidet, welche Treffer uns die Suchmaschine anzeigt, welche Informationen uns zur Verfügung stehen und letztlich, was unser Ruf im Netz ist. Wenn Google seinen Suchalgorithmus modifiziert, hat das massive Auswirkungen auf den Traffic von Webseiten. Der Zustrom ganzer Nachrichtenseiten kann versiegen, andere werden förmlich überschwemmt. Ein paar Zahlencodes als Machtinstrument. „Ein Algorithmus ist eine formale Handlungsvorschrift zur Lösung von Instanzen eines Problems in endlich vielen Schritten“ – so lautet die Definition des Informatik-Professors Hanjo Täubig von der TU München. Das Prinzip funktioniert nach dem Muster Eingabe – Algorithmus – Ausgabe. Zum Beispiel bei einem Ikea-Schrank: Die Eingabe sind die Einzelteile, der Algorithmus die Bauanleitung, die Ausgabe das fertige Möbelstück. Soweit die Theorie.

Der Algorithmus, den die Google-Gründer Larry Page und Sergey Brin einst auf dem Campus der Stanford University in Kalifornien austüftelten, ist in der Praxis deutlich komplexer. Das Problem ist, dass PageRank keiner öffentlichen Überprüfbarkeit unterzogen werden kann. Algorithmen sind eine Black Box. Im Juni fiel dem schwarzen Programmierer Jack Alciné ein Fotoalbum von ihm und seiner Freundin auf, das die Google-App „Photos“ automatisch mit Gorillas überschrieben hatte. Die Software setzte einen Menschen mit einem Tier gleich. Algorithmen sind keine wertneutralen Konstrukte, wie das die Entwickler oft betonen – sie können offen diskriminieren. Google betont, dass es mit seiner Suchmaschine jedem das Wissen der Welt zugänglich macht. Allein, der weltgrößte Suchmaschinenanbieter geht bei seinem Angebot nicht wie ein Bibliothekar vor, der Quellen feinsäuberlich nach Signaturen ordnet, sondern eher wie ein Kaufhausbetreiber, der sein Warensortiment wie in einem Schaufenster arrangiert. Google ordnet seine Trefferliste nicht nach Kriterien der Relevanz, sondern ökonomischer Verwertbarkeit an. Denn Werbung ist das Kerngeschäft von Google. 2014 verdiente der Konzern damit 16,5 Milliarden US-Dollar.

»Recht auf Vergessen« Die Geschäftsinteressen kollidieren zuweilen mit Persönlichkeitsrechten. 2010 stellte der Spanier Mario Costeja González fest, dass bei der Eingabe seines Namens in die Suchmaschine zwei Artikel im Archiv der spanischen Tageszeitung „La Vanguardia“ auftauchten, in denen die Versteigerung seines Grundstücks im Jahr 1998 wegen bestehender Verbindlichkeiten bei der Sozialversicherung und einer anstehenden Pfändung angekündigt wurde. Die Schulden waren längst bezahlt, doch das unschöne Wort der Pfändung war weiter im Netz zu lesen – und hätte Zweifel an seiner Kreditwürdigkeit nähren können. Seiner Aufforderung gegenüber Google und der Tageszeitung zur Löschung respektive Änderung der jeweiligen Seiten mit seinem Namen kamen beide Unternehmen nicht nach. González erhob daraufhin Beschwerde bei der spanischen Datenschutzaufsichtsbehörde AEPD. Diese forderte Google auf, den Zugang zu dem Artikel zu trennen. Gegen diese Aufforderung erhob der Suchmaschinenriese Klage. Der Europäische Gerichtshof entschied im Mai 2014 in einer wegweisenden Entscheidung, dass Suchmaschinenbetreiber wie Google auf Antrag Informationen aus ihren Suchergebnissen streichen müssen, wenn die Informationen die Persönlichkeitsrechte betroffener Personen verletzen. EU-Bürger haben ein „Recht auf Vergessenwerden“ im Internet. Seit dem Richterspruch sind bei Google 350.000 Löscheinträge eingegangen. Allein, Google löscht Suchergebnisse nur auf europäischen Seiten wie google.de oder google.fr, während sie auf google.com weiter auftauchen. Der Suchmaschinenbetreiber verweigert sich hartnäckig der Aufforderung der französischen Datenschutzbehörde CNIL, das in Europa vorgeschriebene „Recht auf Vergessen“ weltweit umzusetzen. Was für Europa gelte, sei global kein Gesetz.

Hier zeigt sich einmal mehr das Bild eines Giganten, der ungehindert über das kleinteilige Recht der Nationen hinwegschreitet, als wären es Gartenzäune. Nationales Recht stößt bei der Regulierung des Internetkonzerns an seine Grenzen. Dabei ist Google Search nur Teil eines riesigen Konglomerats, das seit August 2015 unter dem Namen „Alphabet“ firmiert. Google entwickelt smarte Kontaktlinsen und selbstfahrende Autos, konstruiert Drohnen, forscht in seinen geheimen X-Laboren der Bekämpfung von Krankheiten, vermisst mit seinem Kartendienst „Maps“ die hintersten Winkel der Erde, verlegt Glasfaserkabel und versorgt im Rahmen des „Project Loon“ den Inselstaat Sri Lanka mit schnellem Internet. Google ist längst zu einem transnationalen Akteur avanciert, der sich anschickt, die öffentliche Daseinsvorsorge zu übernehmen. Ist Google auf dem Weg zum Superstaat?

Der Staatsrechtler Georg Jellinek hat im 19. Jahrhundert den Staat als „die mit ursprünglicher Herrschaftsmacht ausgerüstete Körperschaft eines sesshaften Volkes (Gebietskörperschaft)“ umschrieben, bestehend aus Staatsgebiet, Staatsvolk und Staatsgewalt. Nun lässt sich die berühmte Drei-Elemente-Lehre schwerlich auf Google übertragen. Es ist kaum vorstellbar, dass Google Schlagbäume errichtet und Verwaltungsakte vollzieht. Interessanter ist das Element der Staatsgewalt und der ihr inhärente Machtgedanke. Google kartiert Weltmeere und Kontinente – ein Privileg, das früher Königen und Fürsten vorbehalten war – und übt damit Macht aus. Ob Google auf seinen Karten das Meer zwischen dem Iran und der arabischen Halbinsel als „Persischer Golf“ oder „Arabischer Golf“ bezeichnet, ist de facto eine politische Entscheidung – oder zumindest eine Entscheidung mit erheblicher politischer Wirkung. Als Google 2012 den Namen „Persischer Golf“ aus seinem Kartendienst strich, gab es heftige Proteste aus Teheran. „Wenn Google nicht umgehend seinen Fehler berichtigt, werden wir offiziell Klage einreichen“, sagte damals ein Sprecher des Außenministeriums. Der Internetkonzern zeichnet damit die politische Wirklichkeit, die auf Dauer zu Gewohnheitsrecht erstarken kann. Es ist eine Art Abstimmung durch Aufrufe und Klicks.

Googles Dienste haben weltweit eine Milliarde Nutzer. Der Konzern kennt die Gewohnheiten seiner Nutzer, er kennt die Präferenzen und Interessen und kann aus Suchanfragen Muster ableiten – zum Beispiel den Verlauf von Grippewellen (Flu Trends). Google weiß mehr als jede Auskunftei oder Statistikbehörde. Eric Schmidt sagte, jeden zweiten Tag erzeugen die Menschen so viele Informationen, wie bis vor 2003 in der gesamten Zivilisation vorhanden waren. In dem Wissen um die Präferenzen könnte Google eine Herrschaft etablieren.

Einfluss auf Wahlen Eine Studie des US-Verhaltensforschers Robert Epstein belegt, dass die Ergebnislisten von Suchmaschinen das Wahlverhalten beeinflussen können. Google könnte damit Wahlen manipulieren. „Das Programm entscheidet schon heute über den Ausgang von Wahlen in aller Welt“, sagte Epstein auf der IT-Messe CeBIT. Googles Algorithmen seien eine „Gefahr für die Demokratie“. Das Neue an der Politik, die einige schon als „Biopolitik“ bezeichnen, ist, dass Macht unsichtbar wird. Man muss nicht mehr stapelweise Wahlzettel in die Urne werfen, um Wahlen zu manipulieren, es genügen einige Modifikationen des Algorithmus.

Die Macht im Google-Imperium kommt subtil daher. Lange bemäntelte der Konzern seine wahren Intentionen mit dem Slogan „Don’t be evil“, doch in Wirklichkeit geht es darum, alle Lebensbereiche auf Marktförmigkeit umzucodieren. Dass der Konzern politische Ambitionen hegt, zeigt die Gründung eines „Government Innovation Lab“ in den USA. In den Countys Kern, San Joaquin und Alameda in Kalifornien bildet Google neuerdings Regierungsbeamte aus. Das Überraschende an dem Projekt ist nicht die Technik, sondern die Tatsache, dass Google nach „Lösungen“ für das politische System sucht. Arbeitslosigkeit und Armut sind im Denken Googles kein gesellschaftliches Problem, sondern genuin betriebswirtschaftliche Fehler, die sich mit ein paar technischen Handgriffen „lösen“ lassen. Solutionism nennt das der Internetphilosoph Evgeny Morozov. Staaten sind für Google etwas Gestriges, ein überkommenes Gehäuse, das mit der richtigen Software programmiert werden muss.

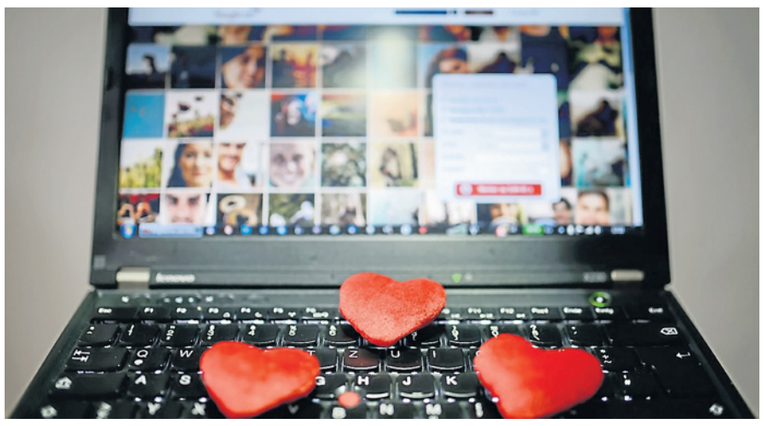
2014 kündigte Larry Page ein Projekt namens „Google 2.0“ an, das mit der Entwicklung einer Modellstadt beauftragt werden soll. Parallel dazu wurde eine Abteilung mit der Bezeichnung „Google Y“ – analog zum Geheimlabor Google X – gegründet. Man hat sich nichts weniger zum Ziel gesetzt, als das Leben aller Menschen zu verbessern. Dazu wolle man ganze Städte und Infrastrukturen von Grund auf neu planen. Im Juni gründete Google die Tochter Sidewalk Labs, die mit dem Aufbau eines großen WLAN-Netzes in New York City begonnen hat.

Der Konzern arbeitet an einer Verknüpfung von search und social. Ob man nach links oder rechts geht, ist schon heute keine Frage der Intuition mehr, sondern der Technik. Google lotst uns mit seiner Navigationssoftware an Geschäften vorbei, die mit unseren Präferenzen korrespondieren und am meisten für Werbung bezahlen. Der Internetkonzern steuert damit nicht nur das Suchverhalten im Netz, sondern auch im realen Raum. Larry Page will autonome Zonen kreieren, in denen man mit sozialen Regeln experimentieren kann. Eine Google City wäre eine Investorenstadt und ein Labor der Subjektivität, in dem der Einzelne so berechenbar wie der Stromverbrauch wird. Das Leben im Google-Universum mag bequem sein. Es hat jedoch einen Preis: Wir zahlen mit unseren Daten und unserer Privatsphäre. *Adrian Lobe*

Der Autor ist freier Journalist in Stuttgart.

Das perfekte Profil fürs Zusammensein

PARTNERSUCHE Das Internet hat die Suche nach dem richtigen Lebensgefährten enorm verändert. Es gibt viele neue Möglichkeiten – und neue Probleme



Online-Partnerbörsen sind groß im Kommen. © picture-alliance/dpa

Die Partnersuche im Internet boomt. Nach einer Studie von Fittkau und Maaß geben mehr als die Hälfte der 5.254 Befragten an, dass sie sich vorstellen können, online den Partner für Ihr Leben zu finden. Der Grund dafür liegt auf der Hand: Die unbegrenzte Reichweite des Internets schafft eine größtmögliche Auswahl; ein Faktum, das wir gerne auch in anderen Lebenslagen nutzen: beim Kauf eines Fahrzeugs, bei der Suche nach einer Mietwohnung oder Immobilie – oder auf der Schnäppchen-Jagd.

Fragebögen Die Internet-Partnerbörsen haben in den vergangenen 20 Jahren eine regelrechte Revolution durchlaufen. Zu Beginn boten sie wenig mehr als ein nach Volltext oder bestimmten Parametern durchsuchbares Datenkonvolut. Nutzer registrierten sich und gaben bestimmte Basisdaten wie Wohnort, Größe, Augenfarbe, Schulabschluss oder Hobbies an – andere Nutzer wiederum konnten gezielt nach solchen und anderen Kriterien suchen. Das Problem hierbei: Ein Partner ist kein Gebrauchtwagen. Selbst, wenn die äußerlichen Parameter stimmen mögen, muss sich beim ersten Date nicht unbedingt Sympathie einstellen. Denn zu komplex und unvorhersehbar ist das Spiel aus Wunsch und Wirklichkeit – es kann der schönste Mensch nicht attraktiv wirken, wenn sich unterschiedliche Lebensauffassungen oder Konzepte für eine dauerhafte Partnerschaft zeigen. Und vielleicht verlieben wir uns auch gar nicht in das Äußere eines Menschen, sondern in seinen Humor und seine Warmherzigkeit.

Aus diesem Grund arbeiten moderne Partnerbörsen wie Parship, Elitepartner oder OKCupid nach einem völlig anderen Modell. Mithilfe eines aufwändigen Fragebogens werden ganz grundlegende Werte erfasst: Wie wichtig ist einer Person Ehrlichkeit und Offenheit? Wie viel Freiraum braucht sie in einer Partnerschaft? Darf es etwas leidenschaftlicher sein oder soll es sich um eine platonische Beziehung handeln? Möchte man in der Beziehung ungehemmt dem Hedonismus frönen oder lieber die Welt verbessern? Hinter den psychologisch ausgearbeiteten Fragen steckt letztlich ein Datenmodell. Alle wichtigen charakterliche Eigenschaften eines Menschen werden in einer Matrix aus Eigenschaft und ihrer jeweiligen Ausprägung hinterlegt – und nicht immer muss Übereinstimmung das beste „Match“ bieten: Eine dominante Persönlichkeit wird sich beispielsweise tendenziell besser mit einer duldsamen verstehen anstatt mit ihresgleichen.

Im Unterschied zu den Datenfriedhöfen der Partnerbörsen aus der ersten Generation sind zeitgemäße Datingplattformen proaktiv. Jede neu angemeldete Person, jeder neue Datensatz, wird umgehend mit den gespeicherten abgeglichen. Wer eine solche Partnerbörse nutzt, erhält regelmäßig neue Partnervorschläge. Aus dem Kontaktverhalten nach der Zustellung solcher Vorschläge lassen sich Verfeinerungen der Profile generieren, der Algorithmus lernt gewissermaßen hinzu. Je mehr Daten vorliegen, desto besser zugeschnitten sind die Vorschläge.

Nun ist das seitenlange Ausfüllen von Fragebögen nicht Jedermanns Sache. Aus diesem Grund wird auch hier der Ansatz der so genannten Gamification gewählt: Machen wir ein Spiel draus! So bei OKcupid, einer der erfolgreichsten Singlebörsen, können Nutzer selbst Fragen entwerfen und dem Kanon hinzufügen. Somit ist sichergestellt, dass sich für jedes Interessensgebiet – und sei es noch so abwegig – ein potenzieller Partner findet. Nicht zuletzt gerät das Blättern durch die Fragebögen zuweilen zum unterhaltsamen Selbstzweck.

Doppelte Übereinstimmung Ähnlich, wenn auch psychologisch wesentlich weniger ausgefeilt, verhält es sich mit mobilen Apps wie Tinder oder Lovoo: Partnervorschläge erscheinen hier direkt als Foto auf dem Touchscreen des Smartphones: Per Wisch nach links oder rechts wird aussortiert – die guten ins Töpfchen, die schlechten ins Kröpfchen. Zusätzlich gilt bei vielen dieser Apps das Prinzip des „Double opt-in“: Wenn Person A Gefallen an Person B gefunden hat, muss letztere ebenfalls eine Übereinstimmung vermelden – nur dann kommt ein Kontakt zustande. Auch hier lernt der zu Grunde liegende Algorithmus wieder aus den Ja-Nein-Entscheidungen beider Parteien: Je länger man die App nutzt, desto geringer ist die Chance, eine Person vorgeschlagen zu kommen, die nicht dem eigenen Attraktivitätsschema entspricht.

Ein großes Thema bei allen zeitgemäßen Singlebörsen ist der Datenschutz. In unseren Profilen sind sensible, höchst vertrauliche Daten gespeichert, und nicht jede Partnerbörse oder App macht transparent, welche Daten erhoben werden, wie sie gespeichert und gesichert werden – und was sonst noch so mit diesen Daten geschieht. Besonders riskant sind Applikationen, bei denen Facebook als Registrations- und Freischaltungsplattform genutzt wird: Im Feuereifer der Partnersuche, in der Vorfreude auf mögliche „Matches“, werden allzu häufig schnell die Allgemeinen Geschäftsbedingungen ignoriert – mit wenigen Klicks können die Betreiber der App persönliche Vorlieben oder pikante, über die App geführte, Konversationen mit realen Personenstammdaten verknüpfen. Bei einem Hackerangriff sind die Folgen zuweilen fatal: Im Juli 2015 hackten Aktivisten die Fremdgeh-Partnerbörse Ashley Madison und machten nicht nur die Tatsache publik, dass ein großer Anteil der Profile lediglich Fakes waren – sie veröffentlichten unter anderem auch die Nutzernamen und E-Mail-Adressen aller registrierten Nutzer im Darknet. Weing später beging ein Priester, der bei Ashley Madison registriert war, Selbstmord.

Es lohnt sich also, eine Partnerbörse nicht nur nach ihren Features zu beurteilen, sondern auch danach, wie ernst sie die Datensicherheit ihrer Nutzer nimmt. Ansonsten gilt schnell die Gleichung: „Big Data“ = „Big Problems“. *Jochen Reinecke*

Der Autor ist freier Wissenschaftsjournalist in Berlin.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Spuk der Kraken

LITERATUR Romane spielen auf George Orwells Spuren die allgegenwärtige Digitalisierung gedanklich durch. Es sind auch Versuche, das geschriebene Wort gegen die visuelle Kultur des Internets zu verteidigen

Ein Wandbild in Paris erinnert an George Orwells Roman „1984“, der ein düsteres Bild totaler Überwachung zeichnet. © picture-alliance/dpa

Der Glaube an die eigene Erwähltheit und der Glaube daran, dass die Welt eine bessere werden kann: Das gehört in der Enthüllungsorganisation des fiktiven Whistleblowers Andreas Wolf zusammen. Dessen auf der digitalen Technik fußendes „Sunlight Project“ ist eine literarische Nachbildung des neuen Machtfaktors im Nachrichten- und Gerechtigkeitsgeschäft – Wikileaks und Snowden sind ein guter Erzählstoff, das hat das Kino schon bewiesen. Und es ist kein Wunder, dass ausgerechnet Jonathan Franzen, der von Kritik wie Publikum gleichermaßen geschätzte Bestsellerautor aus New York, mit dem hinter dem Eisernen Vorhang aufgewachsenen Andreas Wolf einen an Julian Assange erinnernden Charakter in die Welt der Romane einführt. Anhand der sektenartigen Gemeinschaft der Hacker und Polit-Aktivisten, an deren Spitze der suspekte Hamlet-Charakter steht, treibt Franzen seine mehrfach geäußerte digitale Skepsis auf die Spitze. „Ersetzte man Sozialismus durch Netzwerke, hatte man das Internet“, heißt es einmal in seinem gewaltigem neuen Gegenwartspanorama „Unschuld“.

Schuld und Unschuld Der Vergleich von DDR und Facebook, die Behauptung des totalitären Systems „Internet“ – die digitale Sphäre mit ihren durchaus fragwürdigen Transparenz- und Reinheitsbestrebungen wird von Franzen auf provozierende Weise kompromittiert. Der Klappentext spricht von einer „tiefschwarzen Komödie“, dabei ist „Unschuld“, dieser mehrere Jahrzehnte umfassende Roman, doch viel eher eine überaus ernste Studie über Schuld und Unschuld, Manipulation und Kontrollverlust. Es geht um Deutschland, ausgerechnet, und um die grundsätzliche Schuld, die jedes menschliche Wesen mit sich herum trägt. Die Sehnsucht nach dem ultimativ Guten, der persönlichen Exkulpation? Wird gestillt, indem man sich auf die Seite der neuen Supermoralisten gesellt. Sie brauchen lediglich einen Internetanschluss. Und im Falle des international gesuchten Andreas Wolf ein Camp in Südamerika, das vor dem Zugriff der Behörden geschützt ist.

Wer sein Erleben nicht online teilt, der hat gar keines.

In seiner Kritik folgt Franzen einem anderen amerikanischen Romancier, der die Zurschaustellung der negativen Implikationen der digitalen Revolution noch um einiges krasser betreibt. Dave Eggers, ein mit teilweise journalistischen Mitteln zu Werke gehender Diagnostiker des Zeitgeists, beschäftigte sich in seinem literarischen Werk bereits mit Krieg und Vertreibungen in Afrika (in seinem Roman „Weit gegangen“) und der Hurrikan-Katastrophe in New Orleans (in „Zeitoun“). So parteiisch wie in seiner Internet-Dystopie „The Circle“ war Eggers jedoch noch nie. Wer die digitale Schattenexistenz von Internet-Nutzern, wer die Verquickung von sozialem Miteinander, Ökonomie und Technik verdächtig findet, für den könnte das plakative Anti-Internet-Fanal „The Circle“ zur Bibel werden.

Aber was heißt Schattenexistenz: In „The Circle“, das nicht zu Unrecht als Update von Orwells „1984“ beschrieben worden ist, ist das digitale Leben das eigentliche. Wer sein Erleben nicht online „teilt“, der hat gar keines. Im fiktiven und an Google oder Facebook erinnernden „Circle“, dem hippen Vorzeige-Unternehmen des Internet-Zeitalters, herrscht ein radikaler Konformitätsdruck: Der Lifestyle der Mitarbeiter soll nach außen strahlen und die völlige Umwertung aller Werte befördern. Intimsphäre und Privatheit sind gestrige Konzepte, jetzt heißt es: „Teilen ist heilen“ und „Alles Private ist Diebstahl“.

Eggers verwebt in der verblüffend festgefügten Story um die junge Mae Holland, die neu zum „Circle“ kommt und die zunächst euphorisch begrüßte „Alle-sind-mit-allen-verbunden-Philosophie“ erst spät anzuzweifeln beginnt, die Internet-kritischen Motive zu einer Gegenwartsdiagnose, die frei ist von jeglicher Ambivalenz. Der Roman wirkt wie ein rot blinkendes Warnschild, das der durchdigitalisierenden Weltgesellschaft in den Weg gestellt werden soll. Die totale Transparenz, die der „Circle“ anstrebt, ermöglicht zum einen den totalen Konsum. Das soziale Netzwerk als Datensammler, der Hersteller und Distributoren mit Adressen, Wünschen und Kauf-Gewohnheiten versorgt, das kennt man von Facebook. Auch die Komplett-Durchleuchtung des Individuums – mitsamt seiner Körperfunktionen -, wie Eggers sie imaginiert, klingt erschreckend realistisch. Und so stellt der Roman vor allem die Frage, wie wir leben wollen. Wollen wir wirklich eine von messianischem Furor getriebene visionäre Firma unser aller Leben kapern lassen? Wollen wir die Art von Scheinfreiheit, die diese propagiert? Oder erkennen wir die Unfreiheit, die der Überwachung und Vorführung unseres Innersten folgt?

Totale Moral „The Circle“ wirkt, bei aller Wiedererkennbarkeit, in allem, was der Roman zu porträtieren sucht, wie eine maßlose Übertreibung. Sie ist so maßlos (auch in der Metaphorik), dass manch einer das Buch für eine Satire hielt. Wer Eggers‘ Romane kennt, der weiß, dass dem nicht so ist; sie gehören in den Bereich der engagierten Literatur und lassen stets den Humanisten erkennen, der Eggers ist. Wie in Franzens „Unschuld“ machen sich die Verfechter des Digitalen im „Circle“ zum Anwalt der totalen Moral. Sie herrscht dann, wenn Handlungen nicht mehr unbeobachtet vollzogen werden können. Die Überwachung von Politikern ist ein Kernziel, noch besser aber ist direkte Demokratie via Mausklick. Dass dies zum Beispiel eine Entkoppelung von Vernunft und Entscheidungsfindung zur Folge haben könnte, muss so genau gar nicht thematisiert werden. In der schonungslosen Roman-Draufsicht auf die neue Zeit reicht der Blick auf sagenhaft naive und unselbständige Figuren, um zu dem Schluss zu kommen: So kann kein Gemeinwesen der Welt sein Zusammenleben organisieren. Oder?

„The Circle“ spielt im Silicon Valley, aber es ist die große Gegenschrift zum dort gängigen Fortschritts-Enthusiasmus. Auf „Unschuld“, das in ästhetischer Hinsicht wenig überraschend wesentlich höher einzuschätzen ist (man beachte die Tiefe der Figurenzeichnung), trifft dies ebenfalls zu. Wo in der von Franzen beschriebenen „Sunlight“-Welt ein europäisch grundierter Wille zum Drama zu finden ist, der mit der ödipal gestörten Anlage des Heilsbringers Wolf zu tun hat, ist in „The Circle“ jedes Konfliktpotenzial auf maximal deutliche Weise angelegt, so dass einem die Story doch recht schnell fad erscheint. Dass ein soziales Netzwerk als „I like“-Korrektiv und exhibitionistisches „Schaut alle her“-Kollektiv keine Form von Individualismus mehr zulässt und deswegen gefährlich ist, ist als Aussage doch zu offensichtlich und erwartbar. „The Circle“ funktioniert zwar als Zusammenfassung aller kursierenden Problemstellungen über das, was digitale Umwälzungen mit uns machen oder machen könnten. Der Impuls zur gedanklichen Dialektik, die Vor- und Nachteile abwägt und das Verhalten eines aufgeklärten Bürgers angesichts der Fülle an Möglichkeiten auszuloten versucht, geht jedoch kaum von dem Roman aus.

Die totale Transparenz, die der »Circle« anstrebt, ermöglicht totalen Konsum.

Alarmismus Er unterschlägt in seinem grellen Alarmismus die nachgerade altmodische Vorstellung, dass man sich dem Terror des Teilens entziehen kann, indem man auch mal einfach nur analoge Dinge tut, wie zum Beispiel ein Buch zu lesen. Gibt es eine ähnlich unsoziale und den Netzwerken entzogene Tätigkeit? In der Romanwelt von „The Circle“ müsste man sich beim Lesen freilich filmen lassen oder mindestens den „Gefällt mir“-Button zücken.

Vielleicht müssen es unbedingt Schriftsteller sein, jene Schöpfer einer Form, die selbst dem Druck des Digitalen ausgesetzt ist, die den Spuk der Krake aufs Tapet bringen. Die Internet-Kultur ist eine visuelle Kultur. Wer ihr mit einem Pamphlet gegen die Macht der Großkonzerne und der Transparenz-Ideen zu Leibe rückt, der versucht sich auch an der Rettung des geschriebenen Worts. *Thomas Andre*

Der Autor ist Redakteur beim „Hamburger Abendblatt“.

Der Flaschenhals heißt Facebook

POST-PRIVACY Unternehmen sind nicht mächtig, weil sie viele Daten sammeln, sondern weil sie andere von ihrem exklusiven Datenreichtum ausschließen können

Wenn wir über Big Data sprechen, taucht meistens als erstes die bange Frage nach der Privatsphäre auf. Wie können wir unsere Privatheit in Zeiten von Big Data schützen? Diese Frage verstellt jedoch die wirklichen Herausforderungen, wenn es um Big Data geht. Big Data heißt erstmal nur das, was der Name verspricht: Es geht um das Auswerten großer Datenmengen. Groß ist relativ, aber der Einfachheit halber kann man sagen, dass Big Data dort anfängt, wo ein einzelner Rechner zur Bewältigung der Daten nicht mehr ausreicht. MapReduce, das algorithmische Verfahren, das Google zum Zweck der Auswertung großer Datenmengen entwickelt hat, erlaubt es, Datenmengen auf verschiedene Rechner aufzuteilen (Map), sie dort parallel zu sortieren und die Ergebnisse zusammenzuführen (Reduce).

Mithilfe von Big Data lassen sich sogar Erkenntnisse in großen Datenmengen finden, an die Forscher vorher gar nicht gedacht haben. Fällt ihnen eine Korrelation ins Auge, ist das oft ein Ansatzpunkt, um danach weiter zu forschen. Chris Andersons bekannte These vom „Ende der Theorie“ rührt genau von diesem Umstand her. Tatsächlich findet in vielen Wissensgebieten ein Umbruch statt: erst die Daten, dann die Theorie.

Die Bedrohungen für die Privatsphäre liegen auf der Hand: Mithilfe von Big Data können eine Menge Informationen aus Daten herausgelesen werden, die darin gar nicht zu vermuten sind. So konnten 2008 Studenten aus einer Clusteranalyse des Facebook-Freundeskreises herauslesen, ob jemand homosexuell ist. Startups aus dem Medizinbereich suchen nach Korrelationen, die das Risiko von Herzinfarkten sichtbar machen. Neuronale Netze prägen sich Gesichter ein und können Personen auf jedem beliebigen Foto oder auf Videoaufzeichnungen wiedererkennen.

Die Gefährdungen der Privatsphäre sind real. Und trotzdem führt die Frage nach der Privatsphäre in eine gefährlich falsche Richtung. Sie verfehlt die Macht von Big Data komplett.

Chancen und Risiken Big Data ist in erster Linie ein Paradigmenwechsel bei der Frage, wie wir die Welt deuten. Darin liegt das eigentlich revolutionäre Potenzial, dort liegen die Chancen genauso wie die Risiken. Und das Problem zeichnet sich bereits deutlich ab: Die neue Deutungsmacht liegt in den Händen von Wenigen. Sie bestimmen, was wir zum Frühstück in unseren Newsfeeds lesen (Facebook), welche Prozesse bei der Arbeit eingeführt werden (Big Data Management), wie Lieferketten funktionieren und wie Städte geplant werden. Data Scientists beraten sogar Politiker bei der Planung und Durchführung von neuen Regulierungskonzepten (Behavioral Economics/Nudging). Die „Data Scientists“ sind als neue, sehr mächtige Akteure in den demokratischen Diskurs getreten. Sie sind die neuen Priester der Wahrheit.

Diese Ungleichverteilung der neuen Deutungsmacht hat viele Ursachen und die meisten sind der Tatsache geschuldet, dass wir es hier noch mit einem recht jungen Wissensfeld zu tun haben. Und vieles lässt sich ebenso leicht beheben. Die Ausbildung wird nachziehen und mehr und mehr qualifizierte Data Scientists ausbilden. Der Zugang zur Technologie wird außerdem immer günstiger. Viele Software ist heute schon Open Source und für jeden verfügbar. Nur ein Flaschenhals wird sich auch in Zukunft weiter verengen, wenn wir nicht umdenken: der beschränkte Zugang zu Daten.

Nehmen wir Facebook. Das Unternehmen hat viele Daten über viele Menschen. Wer sich für Fragen der Privatsphäre interessiert, wird sich nun mit Facebook darüber streiten, wie man den Zugriff auf diese Daten beschränken kann. Das Paradoxe: Damit stärkt der Datenschutz Facebooks Monopolanspruch auf die Daten.

Data Scientists könnten in Unternehmen bald viel gesuchte Fachleute werden, um den immer größeren Wust an Daten aufzubereiten und zu analysieren. © picture-alliance/dpa

Der blinde Fleck des Datenschutzes ist folgender: Facebook ist nicht so mächtig, weil es so viele Daten hat. Es ist mächtig, weil es die Daten exklusiv hat, sie exklusiv auswerten darf und damit exklusive Inhalte erstellen kann. Facebook kann durch den Algorithmus seines Newsfeeds die Weltsicht von 1,5 Milliarden Menschen entscheidend beeinflussen; ohne, dass diese das je merken würden. Niemand ist in der Lage mit Facebooks Newsstream zu konkurrieren. Niemand kann überprüfen, in welche Richtung Facebooks Algorithmen Meinungen manipulieren. Das ginge nur, wenn Dritte Zugriff auf Facebooks Daten hätten. Das aber wollen weder Facebook, noch Datenschützer.

Die besorgte Frage nach der Privatsphäre hilft den Datenmonopolisten. Sie ist eine prima Rechtfertigungsgrundlage, andere von ihrem Datenreichtum auszuschließen.

Wir sollten in der Debatte um Big Data aufhören, immer nur nach der Privatsphäre zu fragen und anfangen, das große Ganze zu sehen. Wie können wir die Macht der Datenmonopole beschränken, ohne dass wir deren nützliche Services verbannen oder unmöglich machen? Das geht nicht dadurch, den Zugang zu Daten weiter einzuengen. Im Gegenteil: Wir müssen den Zugang zu den Datenreichtümern öffnen. Für Wettbewerber, für Privatpersonen, für möglichst viele. *Michael Seemann*

Der Autor betreibt den Podcast wir.muessenreden.de und schreibt unter anderem für „Zeit Online“ und „Spiegel Online“.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Meilenweit entfernt

E-MOBILITÄT Auf Deutschlands Straßen sind erst 19.000 Fahrzeuge zugelassen. Es gibt nicht genügend Kaufanreize

In Deutschland sind Elektrofahrzeuge bisher eher selten. Das soll sich aber ändern. © picture-alliance/Robert B. Fishman

Die Verkehrsleistung in Deutschland steigt weiter, der Energieverbrauch nimmt zu, die Immissionsgrenzwerte in Städten werden nicht eingehalten und die verkehrsbedingten CO2-Emissionen wachsen. Doch die Elektromobilität in Deutschland ist meilenweit von den geplanten Ausbauzielen entfernt. Eine Million E-Mobile möchte die Bundesregierung bis zum Jahr 2020 auf deutschen Straßen sehen. Gerade einmal 18.948 Elektrofahrzeuge waren gemäß Kraftfahrt-Bundesamt Anfang 2015 auf deutschen Straßen unterwegs. Zwar stieg die Zahl der von Januar bis Oktober neu zugelassenen Elektroautos mit 9.438 gegenüber dem Vorjahr deutlich an, doch das entspricht nur 0,3 Prozent aller Neuzulassungen. Im internationalen Electric Vehical Index von McKinsey landet der deutsche Markt für Elektroautos auf Platz zehn, weit abgeschlagen hinter Ländern wie Norwegen, Niederlande, USA oder China.

Ein zentraler Grund ist, dass die Kaufanreize für die vergleichsweise immer noch sehr teuren Elektroautos in Deutschland im internationalen Vergleich bisher mager sind. Ab 1. Januar 2016 wird nun sogar die bisher gültige zehnjährige Befreiung von der KfZ-Steuer auf fünf Jahre verkürzt. Bundesumweltministerin Barbara Hendricks und Wirtschaftsminister Sigmar Gabriel (beide SPD) forderten jüngst Kaufprämien. Doch in der großen Koalition ist dies bisher nicht konsensfähig, vor allem weil eine Erhöhung der Mineralölsteuer zur Gegenfinanzierung tabu zu sein scheint. Und der Autoindustrie über eine Bonus-Malus-Regelung schaden möchte man anscheinend auch nicht. Fahrzeuge mit einem hohen CO2-Ausstoß würden entsprechend deutlich höher belastet, um die Kaufprämie zu finanzieren. Vor der Einführung einer verpflichtenden Quote für E-Autos hat man anscheinend auch Angst. Nicht von der Bundesregierung aufgegriffen wurde bisher die Forderung des Bundesrates zur Einführung einer Sonderabschreibung für gewerblich angeschaffte Elektroautos.

Neue Arbeitsplätze Dies, obwohl es nach den jüngst bekannt gewordenen Abgasskandalen etliche positive Signale aus der deutschen Automobilindustrie pro Elektromobilität gibt. So kündigte BMW-Chef Harald Krüger Anfang Dezember eine neue Offensive des Konzerns bei Stromautos ans. Neben dem 2013 eingeführten i3 soll auch eine Cabrio-Version des i8 kommen sowie eine weiteres Elektroauto der i-Familie. Zudem soll die übrige Modellpalette mit Hybridmotoren ausgerüstet und die Brennstoffzelle zum Serieneinsatz gebracht werden. Mehr als eine Milliarde Euro will Porsche bis 2019 in die Serienversion eines „Mission-E" mit reinem Elektroantrieb investieren, beschloss der Aufsichtsrat des Autobauers in der ersten Dezemberwoche. Mit dem E-Flitzer mit 600 PS, und einer Reichweite von 500 Kilometern möchte Porsche auf die angesagte kalifornische Konkurrenz von Tesla reagieren. 1.000 neue Arbeitsplätze sollen auf diese Weise im Stammwerk in Zuffenhausen entstehen.

In einer gemeinsamen Erklärung mit dem Bundeswirtschaftsministerium vom 1. Dezember sprach sich zudem der Verband der Automobilindustrie (VDA) dafür aus „Deutschland zum weltweiten Leitanbieter und Leitmarkt für Elektrofahrzeuge zu machen" und den „zusätzlichen Strombedarf für Elektrofahrzeuge aus dem Ausbau der erneuerbaren Energien bereitzustellen".

Die bisher nur mangelhafte Ladeinfrastruktur möchte die Bundesregierung mit einer Standardisierung voranbringen. Hierzu verabschiedete das Kabinett Ende Oktober den Entwurf über technische Mindestanforderungen an den sicheren und interoperablen Aufbau und Betrieb von öffentlich zugänglichen Ladepunkten für Elektromobile (Ladesäulenverordnung). Vorgesehen ist, dass alle öffentlich zugänglichen Ladepunkte für E-Fahrzeuge mit einheitlichen Steckdosen und Fahrzeugkupplungen ausgerüstet sein müssen und dies der Bundesnetzagentur angezeigt und nachgewiesen werden muss.

Doch derzeit hängt die Verordnung, mit der auch EU-Recht umgesetzt wird, aufgrund von Bedenken der Länder und von Interessengruppen im Bundesrat. Den einen geht die Regelung zu weit, den anderen nicht weit genug. So befürchtet der Verband kommunaler Unternehmen (VKU), dass die vorgesehene Regelung durch „ein Höchstmaß an Bürokratie" gar den Zubau von Ladestationen erschwert.

Doch gerade im kommunalen Bereich bewegt sich einiges pro Elektromobilität. So sind nach einer aktuellen VKU-Umfrage mehr als zwei Drittel der Stadtwerke im Bereich E-Mobilität aktiv. Sie errichten und betreiben Ladeinfrastruktur, beschaffen Elektrofahrzeuge für ihre Fuhrparks, setzen auf E-Carsharing und Mietangebote für E-Autos. So haben beispielsweise die Stadtwerke Osnabrück schon 29 Elektro-Pkw im Einsatz, dies entspricht über zehn Prozent ihres Fuhrparks. Betankt werden sie mit selbst erzeugtem Solarstrom. Damit soll vor allem die Nachhaltigkeit gefördert werden. Zudem sind die Unterhaltskosten gut 35 Prozent günstiger als bei konventionellen Fahrzeugen. *Hans-Christoph Neidlein*

Der Autor ist freier Journalist in Berlin.

Die Niedrigzinspolitik wird zum Problem

FINANZEN Aktionäre machen weiter dicke Gewinne

Der Aufwärtstrend der europäischen Finanzmärkte im ablaufenden Jahr war stark getrieben von der expansiven Geldpolitik. Europas Aktienleitindex Eurostoxx50 legte von Januar bis April um fast 25 Prozent zu. Hauptgrund war das große Anleihekaufprogramm der Europäischen Zentralbank (EZB). Für 60 Milliarden Euro kauft sie nun Monat für Monat Papiere, vor allem Staatsanleihen. Trotz Verlusten steht am Jahresende der Eurostoxx50 aber noch neun Prozent höher als im Januar.

Der deutsche Aktienindex Dax hat 2015 wie der Eurostoxx50 eine Berg- und Talfahrt durchgemacht. Mit rund 10.770 Punkten lag er Ende Dezember elf Prozent über dem Jahresanfangsstand. Verglichen mit dem Tiefstand 2009, mitten in der globalen Rezession, hat der Dax seinen Wert aber gut verdreifacht – getragen auch von der Geldschwemme der Notenbanken.

Bundesbank erfolglos Auch 2016 wird die Geldpolitik die Finanzmärkte in ihrem Bann halten und die Kurse möglicherweise treiben. Anfang Dezember hatte die EZB eine weitere Ausweitung ihrer Anleihekäufe beschlossen durch eine Verlängerung des umstrittenen Programms um sechs Monate. Das Volumen der Käufe bis Frühjahr 2017 steigt damit von 1,14 auf 1,5 Billionen Euro. Bundesbankpräsident Jens Weidmann war gegen das Kaufprogramm und die Ausweitung. Doch konnte er – wieder einmal – EZB-Chef Mario Draghi nicht von seinem Kurs abhalten. Mit diesem soll die Inflation Richtung zwei Prozent gehoben werden. Derzeit liegt sie nur knapp über null. Draghi will die Geldschleusen weit offen halten, um die Inflation anzuheizen.

> **Die Deutsche Bundesbank sieht Gefahren für die Finanzstabilität der Geldhäuser.**

Im Unterschied zur EZB hat die US-Notenbank Federal Reserve jüngst eine Zinswende eingeleitet. Nach sieben Jahren mit Nullzins hat sie den Leitzins um einen Viertelprozentpunkt angehoben. Der Arbeitsmarkt habe sich ausreichend erholt und die Kerninflationsrate steige in Richtung zwei Prozent, erklärte Fed-Chefin Janet Yellen. 2016 werden vielleicht zwei, drei oder vier weitere Zinsschritte folgen, erwarten Ökonomen. Zwischen Europa und Amerika kündigen sich damit gravierende Verschiebungen an. Hält die EZB die Geldpolitik locker, während die Fed strafft, sollte der Euro-Wechselkurs gegenüber dem Dollar abwerten. Einige Banken hatten schon kurzfristig damit gerechnet, dass der Euro unter einen Dollar sinken könnte. Nachdem Draghi die Anleihekäufe nicht so stark wie von vielen Börsianern erhofft ausgeweitet hat, ist der Abwärtstrend zunächst gestoppt worden. Trotzdem bleibt der Euro tendenziell unter Druck.

Deka-Bank-Chefvolkswirt Ulrich Kater sieht bis Ende 2016 die Euro-Dollar-Parität kommen. Einige andere Banken haben einen viel weitergehenden Euro-Absturz prognostiziert. Robin Brooks, Chef-Währungsstratege von Goldman Sachs, rechnete mit einem Sinkflug sogar bis auf 0,80 Dollar bis Ende 2017. Die Deutsche Bank erwartet ebenfalls eine lange Schwächephase: Sie sieht den Euro mittelfristig bei 0,85 Dollar. Ein sinkender Euro-Kurs brächte einen Schub für den Export. Andererseits bedeutet er, dass die Euro-Vermögen weniger wert sind.

Durch die Niedrigzinspolitik bleiben auch die Banken unter Druck. Es gebe zunehmende Risiken für die Finanzstabilität, wenn die Zinsen so lange so ungewöhnlich niedrig bleiben, warnt die Bundesbank. Denn die niedrigen Zinsen treiben die Anleger in riskante Anlagen. Ein kritisches Auge hat die Bundesbank auch auf die Entwicklung der deutschen Immobilienmärkte geworfen. Ihr Befund: In einigen attraktiven Großstädten erscheinen die stark gestiegenen Wohnungspreise um etwa 15 Prozent überbewertet. Eine Blase sei das aber noch nicht, sagt Bundesbank-Vize Claudia Buch. Denn die meisten Häuserkäufer nehmen keine übermäßigen Kredite auf.

In Europa sind die Bankbilanzen durch die EZB durchleuchtet worden. Viele Banken mussten ihre Kapitaldecken zur Absicherung gegen eventuelle Verluste verstärken. In Griechenland haben die vier Großbanken jüngst nochmals neue Kapitalspritzen benötigt. Damit seien nun alle ausreichend kapitalisiert, sagt die EZB. Andere Analysten bleiben skeptisch. In Südeuropa gebe es noch immer viele Probleme in den Banken durch faule Kredite, heißt es von der Ratingagentur S & P. So bleibt auch das Vorhaben der EU-Kommission zur Einrichtung einer vergemeinschafteten Einlagensicherung von 2020 an besonders in Deutschland umstritten. Sparkassen und Genossenschaftsbanken fürchten, dass ihre relativ gut gefüllten Sicherungstöpfe dazu verwendet werden, um Bankenpleiten in Krisenländern abzufedern.

Unsicher bleibt auch, ob 2016 wie geplant die Finanztransaktionssteuer kommt, die von etlichen EU-Ländern gefordert, von anderen aber – vor allem den Briten mit dem Finanzzentrum London – abgelehnt wird. Mitte Dezember verkündeten einige Staaten abermals einen „Durchbruch": EU-Kommissar Pierre Moscovici sagte, bis zur Einigung seien es nur noch „einige Zentimeter". Zehn EU-Finanzminister, allen voran der deutsche und der französische, wollen das Projekt weiter verfolgen. Das heißt aber, dass 18 EU-Länder nicht dabei wären. Offen ist noch die Höhe einer möglichen Steuer. Umstritten ist auch, welche Finanzprodukte der Steuer unterworfen werden sollen.. *Philip Plickert*

Der Autor ist Wirtschaftsredakteur der „Frankfurter Allgemeinen Zeitung".

Anlauf in zweiter Runde

ARBEIT UND SOZIALES Meilensteine und Korrekturen

Eine Million Flüchtlinge im Jahr 2015 – darauf musste auch das Bundesministerium für Arbeit und Soziales (BMAS) eine Antwort finden. Eine erste fand sich im Haushaltsplan des BMAS für 2016, der gegenüber ersten Planungen deutlich, nämlich um rund 2,6 Milliarden Euro, angehoben wurde. So steigen nicht nur die Ausgaben für die berufliche Integration der Zuwanderer, sondern auch die Kosten für die Grundsicherung für Arbeitssuchende und die Verwaltungskosten der Bundesagentur für Arbeit, vor dem Hintergrund der vielen zu versorgenden Flüchtlinge.

Inklusion Ein weiteres Großprojekt ist ein noch zu schaffendes Bundesteilhabegesetz zur Stärkung des Selbstbestimmungsrechts von Menschen mit Behinderungen. Damit soll auf Basis der bereits 2009 in Deutschland verabschiedeten UN-Behindertenrechtskonvention die gesellschaftliche Teilhabe von Behinderten auf eine völlig neue Grundlage gestellt werden. Im Sommer 2015 hatte das BMAS seinen Abschlussbericht zur Tätigkeit einer Arbeitsgruppe Bundesteilhabegesetz vorgestellt. Ziel war es ursprünglich, bis Ende 2015 einen Gesetzentwurf zu präsentieren. Der Entwurf für eine Weiterentwicklung des Behindertengleichstellungsgesetzes liegt dagegen den Bundesländern und zivilgesellschaftlichen Gruppen zur Stellungnahme vor. Zu seinen Schwerpunkten zählt unter anderem die Verbesserung der Barrierefreiheit in der Bundesverwaltung, die Einrichtung einer Schlichtungsstelle und die Stärkung der leichten Sprache.

Hartz IV Das Ministerium plant zudem Rechtsvereinfachungen im Zweiten Buch Sozialgesetzbuch (Hartz IV). Nach mehr als eineinhalb Jahren Beratung hat die Bundesregierung Anfang Dezember 2015, später als geplant, einen Referentenentwurf dazu vorgelegt, der auf Vorschläge der eigens dafür gegründeten Bund-Länder-Arbeitsgruppe zurückgreift. Hauptziel soll es sein, die Verfahren zu vereinfachen, unnötige Bescheide wegfallen zu lassen, um dadurch mehr Zeit für die Betreuung der Arbeitslosen zu schaffen. Dies sei für die Jobcenter eine wichtige Weichenstellung, betonte Ministerin Andrea Nahles (SPD) im November vor dem Bundestag. So plant die Regierung unter anderem, den Bewilligungszeitraum für Hartz-IV-Leistungen von sechs auf zwölf Monate zu verlängern. Bestimmte Leistungen sollen stärker pauschaliert werden. Dies rief bereits Kritik des Deutschen Gewerkschaftsbundes hervor, der davor warnte, dies als Hintertür für Leistungskürzungen zu nutzen. Ursprünglich sollten auch die Hartz-IV-Sanktionsmechanismen für unter 25-Jährige geändert werden. Davon ist im Entwurf nun keine Rede mehr.

Leiharbeit und Betriebsrenten Auf der Agenda 2016 stehen außerdem noch Maßnahmen gegen den Missbrauch von Werkverträgen und Leiharbeit. Die derzeit bekannten Pläne stoßen jedoch auf deutliche Kritik bei der Opposition, der Wirtschaft – und der Kanzlerin. Außerdem plant das Ministerium ein „Rückkehrrecht in Vollzeit" durch eine Änderung des Teilzeitrechts und eine Stärkung der betrieblichen Altersvorsorge. *Claudia Heine*

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

Lautstarke Kritik

KULTUR Regierung will den Kulturgutschutz novellieren

Kulturstaatsministerin Monika Grütters (CDU) wird erst einmal tief Luft holen, wenn der Bundestag das von ihr vorgelegte Kulturgutschutzgesetz in den kommenden Wochen verabschieden wird. Seit Monaten läuft eine wütende Phalanx aus Händlern, Sammlern und Künstlern Sturm gegen das Vorhaben.

Mit der Novelle sollen drei bereits gültige Gesetze zum Kulturgutschutz zusammengeführt und an bestehendes EU-Recht angepasst werden. Ziel ist es einerseits, die Einfuhr von illegal erworben Kulturgütern zu unterbinden, zum Beispiel aus Kriegsgebieten wie Syrien oder dem Irak. Anderseits soll aber auch die legale Ausfuhr an höhere Auflagen gekoppelt und im Fall von „national wertvollem Kulturgut" sogar unterbunden werden. An diesem Punkt entzündet sich die Kritik. Der Handel befürchtet finanzielle Einbußen und Sammler und Künstler den Wertverlust ihrer Werke, wenn deren Verkauf ins Ausland reglementiert oder gar verboten wird.

Alter und Wert Für den Export von Kulturgütern in Nicht-EU-Länder gelten allerdings bereits seit 23 Jahren Auflagen. Nun soll auch der Handel innerhalb des EU-Binnenmarktes abhängig von Art, Wert und Alter des Kulturgutes genehmigungspflichtig werden. Der Gesetzentwurf sieht allerdings großzügigere Alters- und Wertgrenzen als die entsprechende EU-Verordnung vor. So soll die Ausfuhr eines Gemäldes erst ab einem Alter von 70 Jahren und einem Wert von 300.000 Euro genehmigungspflichtig sein. Die Werke lebender Künstler dürften somit kaum betroffen sein. Für archäologische Gegenstände oder Bestandteile von Bau- und Kulturdenkmälern soll eine Altersgrenze von 100 Jahren unabhängig vom Wert gelten.

Untersagt werden soll die Ausfuhr, wenn es sich bei einem Kunstwerk handelt, das im Verzeichnis „national wertvolles Kulturgut" eingetragen ist. Darüber entscheidet eine Expertenkommission. In dieses Verzeichnis eingetragen werden können Kulturgüter, die sich im Eigentum oder Bestand einer öffentlich-rechtlichen Einrichtung befindet. Betroffen sein könnten also auch Leihgaben von privaten Sammlern. Auch gegen diesen Punkt richtet sich die Kritik. Allerdings sieht der Gesetzentwurf vor, dass die Eintragung nur mit Genehmigung der privaten Verleihers erfolgen kann.

Weitgehend unstrittig hingegen sind jene Regelungen des Gesetzes, mit denen die Umsetzung der Unesco-Konvention von 1970 zur Rückgabe von illegal eingeführten Kulturgütern verbessert werden soll. Denn das Kulturgüterrückgabegesetz aus dem Jahr 2007, mit dem Deutschland die Unesco-Konvention umsetzte, hat sich nicht bewährt. Dies sieht eine Rückgabe von unrechtmäßig gehandelten Kulturgütern nämlich nur dann vor, wenn diese in ihren Herkunftsländern als geschütztes Kulturgut in entsprechenden Listen eingetragen sind. Doch viele Länder führen solche Listen erst gar nicht. In der Folge kam es nach Angaben der Bundesregierung bis heute trotz mehrerer Anträge zu keiner einzigen Rückgabe von unrechtmäßig gehandelten Kulturgütern. Mit der Gesetzesnovelle soll deshalb die Einfuhr von Kulturgütern aus Nicht-EU-Staaten an die Regeln des europäischen Binnenmarktes angepasst und an eine Ausfuhrgenehmigung des Herkunftslandes gekoppelt werden.

Nachdem der Bundesrat bereits am 18. Dezember über den Gesetzentwurf beraten hat, wird der Bundestag voraussichtlich noch in diesem Monat erstmalig über ihn debattieren. *Alexander Weinlein*

Auf der Zielgeraden

UMWELT Endlager-Kommission arbeitet an Abschlussbericht

Für die Mitglieder der Endlager-Kommission geht es 2016 auf die Zielgerade ihrer Arbeit. Bis Ende Juli soll der Abschlussbericht stehen. In ihm soll das Gremium darlegen, unter welchen wissenschaftlichen und gesellschaftlichen Kriterien ein Endlager insbesondere für hoch radioaktive Abfallstoffe gefunden werden kann. Ausgestattet mit dem Bericht soll der Bundestag den Suchprozess dann auf den Weg bringen. Der Standort soll demnach 2031 feststehen, in den 2050er Jahren mit der Einlagerung begonnen werden. Allerdings zweifeln auch einige Mitglieder der Kommission daran, ob dieser Zeitplan einzuhalten ist.

Den eigenen Zeitplan müssen die Kommissionsmitglieder allerdings einhalten. Die im Standortauswahlgesetz (StandAG) ausgeführte Möglichkeit, die Arbeit einmalig um sechs Monate zu verlängern, hat die Kommission in Anspruch genommen. Eine weitere Fristverlängerung ist nicht vorgesehen. Entsprechend intensiv wird am Abschlussbericht gearbeitet. Voraussichtlich Ende März soll ein Entwurf in der Öffentlichkeit zur Diskussion gestellt werden.

© dpa

Ab den 2050er Jahren sollen die Castoren endgelagert werden.

Konsenssuche Die Arbeit an dem Bericht gestaltet sich mühselig. Denn Ziel ist es, ein breites Einvernehmen unter den Kommissionsmitgliedern zu erzielen. Das Auswahlgesetz sieht als Ideal eine konsensuale Entscheidung über den Abschlussbericht vor. Ist eine solche Einigung nicht möglich, braucht es eine Zweidrittelmehrheit der Mitglieder. Stimmberechtigt sind dabei nur die 16 Vertreter aus Wissenschaft und Gesellschaft. Die 16 Vertreter des Bundestages und der Bundesländer stimmen nicht mit ab. Auf der Grundlage des Berichts soll der Bundestag das StandAG evaluieren und auch die Kriterien und Entscheidungsgrundlagen für die Endlager-Suche gesetzlich festschreiben.

Erste Ergebnisse auf Grundlage der Kommissionsarbeit sollen aber bereits vor dem Abschlussbericht implementiert werden. So kündigte Bundesumweltministerin Barbara Hendricks (SPD) an, dass im ersten Halbjahr 2016 die bundeseigene Gesellschaft für kerntechnische Entsorgung (BGE) gegründet werden soll. Diese Gesellschaft soll sämtliche Betreiberfunktionen im Bereich Endlager übernehmen. Die aktuell bestehenden Gesellschaften (DBE und Asse-GmbH) sollen innerhalb von zwei Jahren in die BGE überführt werden. Als Aufsichts- und Genehmigungsbehörde soll das bereits aus der Taufe gehobene Bundesamt für kerntechnische Entsorgung fungieren. Das Bundesamt für Strahlenschutz, das bisher im Bereich Atommüll eine bedeutende Rolle spielte, soll entsprechend Zuständigkeiten verlieren. *scr*

Eine Familie aus dem Irak spricht im „Wartezentrum“ im bayerischen Erding mit einem Bundeswehr-Angehörigen und einem Übersetzer. © picture-alliance/dpa

Warten aufs Asylpaket II

FLÜCHTLINGE Der neue »Ankunftsnachweis« kommt. Andere Koalitionsvorhaben stecken noch fest

Der anhaltende Flüchtlingszuzug wird auch 2016 ein beherrschendes Thema sein – für die EU (siehe Beitrag unten), aber natürlich auch für den Bundestag. Das geht schon direkt nach der parlamentarischen Weihnachtspause am 11. Januar los, wenn die Abgeordneten zur ersten Sitzungswoche des neuen Jahres nach Berlin reisen: An diesem Montag geht es in einer Sachverständigen-Anhörung des Innenausschusses um den von der schwarz-roten Regierungskoalition vorgelegten Gesetzentwurf zur schnelleren Registrierung der Asylbewerber (18/7043), der bereits drei Tage danach zur abschließenden Beratung auf der Tagesordnung des Bundestagsplenums steht.

Schon beim ersten Kontakt zu einem Flüchtling sollen die Daten erhoben werden.

Er sieht neben der rascheren Registrierung der Flüchtlinge vor, dass die dabei erfassten Informationen den berechtigten Stellen elektronisch zur Verfügung gestellt werden. Ferner sollen die Asylsuchenden einen neuen, mit fälschungssicheren Elementen ausgestatteten, bundeseinheitlichen „Ankunftsnachweis“ erhalten. Er soll ab dem geplanten Inkrafttreten des Gesetzes im Februar ausgestellt werden und grundsätzlich Voraussetzung für staatliche Leistungen sowie für die Stellung eines Asylantrages sein. Damit will die Regierung „einen Anreiz schaffen, rasch die zugewiesene Aufnahmeeinrichtung aufzusuchen sowie dort zu bleiben“, wie der Parlamentarische Staatssekretär im Bundesinnenministerium, Ole Schröder (CDU), im Dezember bei der ersten Lesung des Entwurfs im Bundestag zu Protokoll gab.

Die Daten der Ankommenden sollen nicht erst bei der Stellung eines Asylantrages, sondern von den Behörden bereits beim ersten Kontakt zu einem Flüchtling erhoben und in einem zentralen „Kerndatensystem“ gespeichert werden. Um Doppelregistrierungen zu verhindern, werden alle zur Registrierung befugten Stellen mit einem „Fingerabdruck-Schnell-Abgleichsystem“ ausgerüstet. Über eine Sofortabfrage können sie damit unverzüglich feststellen, ob zu einer Person bereits Daten vorhanden sind.

Zu den schon heute zu speichernden „Grundpersonalien“ wie Namen, Geburtsdatum und -ort sollen der Vorlage zufolge für Asyl- und Schutzsuchende sowie unerlaubt Eingereiste künftig weitere Daten gespeichert werden. Dazu zählen etwa die bei der erkennungsdienstlichen Behandlung erhobenen Fingerabdruckdaten, das Herkunftsland und Informationen zu Gesundheitsuntersuchungen und Impfungen. Bei Asyl- und Schutzsuchenden sollen zudem Informationen zu Schulbildung, Berufsausbildung sowie sonstige Qualifikationen gespeichert werden, die für die schnelle Integration und Arbeitsvermittlung erforderlich sind.

Nach der Speicherung soll Schröder zufolge „unverzüglich“ ein „Sicherheitsabgleich“ erfolgen. mit dem die Sicherheitsbehörden überprüfen können, „ob zu einer Person schwerwiegende Sicherheitsbedenken bestehen“. Zur Beschleunigung der Asylverfahren ist zudem vorgesehen, den Kreis der Behörden zu erweitern, die Informationen aus dem Kerndatensystem erhalten. Dies betrifft neben den Sicherheitsbehörden beispielsweise das Bundesamt für Migration und Flüchtlinge, die Aufnahmeeinrichtungen, die Bundesagentur für Arbeit und die Meldebehörden.

Weitere Gespräche Der einheitliche Ausweis für die Flüchtlinge und der verbesserte Datenaustausch zwischen den beteiligten Behörden spielte schon Anfang November eine Rolle, als sich Bundeskanzlerin Angela Merkel (CDU) mit CSU-Chef Horst Seehofer und dem SPD- Vorsitzenden Sigmar Gabriel auf ein „Asylpaket II“ verständigten, nachdem der Bundestag wenige Wochen vorher bereits ein umfangreiches Maßnahmenbündel zur Bewältigung des Flüchtlingsandrangs beschlossen hatte. Dieses zweite Paket sah unter anderem die Einrichtung von drei bis fünf „besonderen Aufnahmeeinrichtungen“ mit verschärfter Residenzpflicht für Flüchtlinge aus sicheren Herkunftsstaaten wie vom West-Balkan vor, deren Asylverfahren dort innerhalb weniger Wochen abgeschlossen sein sollten. Vereinbart worden war ferner, den Familiennachzug für Flüchtlinge mit lediglich subsidiärem Schutz für zwei Jahre auszusetzen – ein Punkt, an dem es anschließend in der Koalition hakte, nachdem aus der Union die Aussetzung des Familiennachzugs auch für Syrer ins Gespräch gebracht wurde, während die SPD davon ausging, dass Flüchtlinge aus Syrien nicht von dieser Neuregelung betroffen seien. Weitere Streitpunkte betrafen verbesserte Gesundheitsleistungen etwa für schwangere Flüchtlinge und die geplante Eigenbeteiligung von Flüchtlingen an den Kosten für Integrationskurse. So war schon Anfang Dezember klar, dass das Gesetzespaket nicht wie geplant zum 1. Januar in Kraft treten würde. Und auch nach den Weihnachtsfeiertagen hieß es im Bundesinnenministerium dazu, die Verhandlungen zwischen den Koalitionspartnern seien „noch nicht abgeschlossen“. *Helmut Stoltenberg*

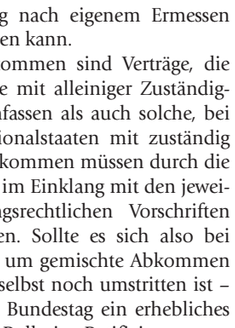
> STICHWORT

DAS NEUE »DATENAUSTAUSCH-VERBESSERUNGSGESETZ«

> **Registrierung** Nach dem Gesetz sollen Flüchtlinge in Deutschland früher als bisher von den Behörden registriert werden. Doppelregistrierungen sollen vermieden werden.

> **Datenaustausch** Die in diesem Zusammenhang erfassten Informationen sollen den berechtigten Stellen auf elektronischem Weg zur Verfügung stehen.

> **Ausweis** Der von Bundesinnenminister Thomas de Maizière (CDU, rechts) vorgestellte „Ankunftsnachweis“ soll auch Voraussetzung für den Bezug staatlicher Leistungen sein.



© picture-alliance/dpa

Flüchtlingshilfe und ein Gesetz gegen Drogen

GESUNDHEIT 2015 war ein wichtiges Reformjahr für die Gesundheitspolitik, 2016 wird das Jahr der Umsetzung. Gleich sechs große Gesetzentwürfe zur Gesundheitspolitik passierten im vergangenen Jahr den Bundestag, die meisten sind mit Jahresbeginn in Kraft getreten.

Mit dem Pflegestärkungsgesetz II hat der Bundestag 2015 die große Pflegereform weitgehend abgeschlossen, jedoch wird der neue Pflegebedürftigkeitsbegriff erst 2017 wirksam. An einem neuen Verfahren zur Bewertung von Pflegeeinrichtungen wird noch gefeilt, nachdem der bisherige Pflege-TÜV mit der Vergabe von Schulnoten von Fachleuten als unbrauchbar eingestuft worden war. Auch der Bürokratieabbau in der Pflege ist ein Dauerthema des Pflegebevollmächtigten Karl-Josef Laumann (CDU).

Abgerundet wird die Pflegereform 2016 mit dem Pflegeberufegesetz, das eine einheitliche Grundausbildung vorsieht. Das Gesetz soll dazu beitragen, ausreichend viele Pflegespezialisten heranzubilden, die in einem personell stark unterbesetzten Markt zu angemessenen Konditionen arbeiten sollen. Auch ein Pflegestärkungsgesetz III zur Einbindung kommunaler Angebote in die Pflegeversicherung ist bereits in Vorbereitung. Mit dem im vergangenen Jahr verabschiedeten Hospiz- und Palliativgesetz soll sich zudem die Betreuung sterbenskranker Menschen entscheidend verbessern.

Die Regierung will außerdem 2016 gesetzlich gegen die zunehmende Verbreitung psychoaktiver Drogen vorgehen. Diese Stoffe firmieren auch unter der Bezeichnung „legal high´s“und werden häufig als Kräutermischungen, Badesalze, Lufterfrischer oder Pflanzendünger verkauft. Auf diese Weise wird zu Unrecht der Eindruck erweckt, die Substanzen seien harmlos. Geplant ist, Herstellung, Handel, Einfuhr, Lagerung und Weitergabe solcher Stoffe zu verbieten.

Flüchtlinge Hingegen soll mit einer gesetzlichen Regelung der Zugang zu Cannabis als Medizin für Schmerzpatienten ermöglicht werden. Derzeit werden solche Therapien mit Hilfe der Droge nur in Ausnahmen genehmigt und nicht immer von den Krankenkassen bezahlt.

Ein bleibendes Thema ist die medizinische Versorgung der vielen Flüchtlinge. Der Bund hat 2015 die Voraussetzungen dafür geschaffen, dass die Länder in Abstimmung mit den Kommunen und Krankenkassen die elektronische Gesundheitskarte (eGK) auch an Asylbewerber ausgeben dürfen.

Das würde den Ausländern die Behördengänge ersparen, die bisher nötig sind, um einen Arzttermin zu bekommen. Noch ist unklar, wie viele Länder die neue Möglichkeit nutzen. Bremen und Hamburg sind hier Vorreiter, Nordrhein-Westfalen, Berlin und Brandenburg ziehen nach, die Bayern sind skeptisch.

Ein nach wie vor großes Problem ist die Betreuung psychisch kranker, zumeist von der Flucht traumatisierter Menschen. Hier hat der Bund 2015 einen vereinfachten Zugang zu Psychotherapeuten und Psychiatern beschlossen. Ungelöst ist aber die Übersetzungsfrage bei Therapiegesprächen, da es an Dolmetschern mangelt.

Einige Experten befürchten außerdem, dass Psychotherapien bei einer Änderung des Aufenthaltsstatus der Flüchtlinge abrupt beendet werden könnten, mit fatalen Folgen für die Patienten. Neuerdings berichten Psychologen auch von Drogenproblemen der Flüchtlinge als Folge der schweren Traumatisierungen. *Claus Peter Kosfeld*

Im Zeichen des Krisenbogens

AUSWÄRTIGES Konflikte von Nahost bis nach Afghanistan bleiben ebenso auf der Tagesordnung wie Spannungen in der Ukraine

Als Vertreter der Bundesregierung vor knapp zwei Jahren von einer gewachsenen „außenpolitische Verantwortung“ für Deutschland sprachen, hätte wohl keiner geglaubt, mit welcher Wucht die Probe aufs Exempel folgen würde. 2014 war das Jahr, in dem der Krieg in der Ostukraine aufflammte, Russland die Krim annektierte und die Bundesregierung diplomatisch alle Hände voll zu tun hatte, den Konflikt halbwegs einzuhegen. Es war das Jahr, in dem sich der „Islamische Staat“ (IS) daran machte, Teile des Iraks und Syrien einzunehmen und obendrein immer mehr Islamisten aus Europa in diesen Konflikt zogen. Hinzu tritt seither die wachsende Zahl der Flüchtlinge, die sich von den Krisenherden von Nahost bis Afghanistan auf den Weg nach Europa machen und deren Aufnahme die Solidarität innerhalb der EU auf die Probe stellt. Auch 2016 dürfte außenpolitisch ganz im Zeichen dieser Krisen und Konflikte stehen.

Noch im Dezember nahm der Bundestag vor allem mit der Koalitionsmehrheit zwei nicht unumstrittene Weichenstellungen vor: Zum einen mit der Entscheidung, von der Abzugsperspektive in Afghanistan vorerst abzurücken und das Mandat für die „Resolute Support Mission“ auszuweiten. Zum anderen mit dem Beschluss, als Reaktion auf Pariser Anschläge des IS mit Luftaufklärung und -betankung als Teil einer internationalen Koalition die Terrororganisation in Syrien zu bekämpfen. Im Gespräch ist weiterhin, den Bundeswehreinsatz zur Ausbildung der kurdischen Peschmerga im Kampf gegen den IS auszuweiten und außerdem deutlich mehr Bundeswehrsoldaten ins westafrikanische Mali im Rahmen der Minusma-Mission zu schicken, letzteres auch, um Frankreich für den Kampf gegen den IS zu entlasten. Beide Mandate stehen Mitte Januar auf der Tagesordnung des Bundestagsplenums.

Die Rolle Assads im Übergangsprozess in Syrien dürfte weiter umstritten bleiben.

UN-Friedensplan Militärisch ist der Konflikt in Syrien nicht zu lösen, es braucht einen politischen Rahmen. Zwar scheint mit der einstimmigen Resolution des UN-Sicherheitsrates zu einem Friedensfahrplan für Syrien kurz vor Weihnachten ein Knoten geplatzt zu sein. Doch hoch umstritten dürfte etwa zwischen Russland und den USA die Frage nach der Rolle des syrischen Präsidenten Assad beim Übergang bleiben. Ziel des UN-Plans ist es, ein breites Spektrum der Oppositionskräfte zusammenzubringen, die Gespräche mit der syrischen Regierung aufnehmen sollen. Der Friedensfahrplan sieht eine Art Einheitsregierung vor und binnen 18 Monaten „freie und faire Wahlen“.

OSZE Deutschland übernimmt in diesem Jahr den Vorsitz der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) und die Bundesregierung will dies vor allem dafür nutzen, verloren gegangenes Vertrauen unter den OSZE-Mitgliedern wiederzugewinnen. Dabei geht es sowohl um eine politische Strategie der Konfliktbeendigung in der Ostukraine als auch allgemein um gegenseitige Rüstungskontrolle und vertrauens- und sicherheitsbildende Maßnahmen in Europa. Der Friedensplan von Minsk, der ja nicht nur einen Waffenstillstand, sondern eine „Reintegration“ der „Volksrepubliken“ vorsieht, soll vorangetrieben werden – unter anderem weiterhin im Rahmen des „Normandie-Formates“, in dem sich die Außenminister der Ukraine, Russlands, Deutschlands und Frankreichs zuletzt im November trafen. Aber auch im Rahmen der OSZE, die etwa die für Februar geplanten Regionalwahlen in diesen Gebieten begleiten soll.

EU-Strategien Auf EU-Ebene warten zudem jene Aufgaben, die die Staats- und Regierungschefs bei ihrem vorweihnachtlichen Gipfel auf 2016 vertagt haben – darunter das Thema Migration und die britischen Forderungen zu einer Reform der EU. Einigkeit besteht darin, dass die Strategie zur Flüchtlingskrise viel zu langsam greift und etwa die Erstaufnahmezentren für Flüchtlinge („Hotspots“) in Italien und Griechenland noch immer nicht wie geplant funktionieren. Geklärt werden muss, wie die drei Milliarden Euro aufgebracht werden sollen, die die EU-Staats- und Regierungschefs der Türkei beim Gipfel Ende November zur Bewältigung der Flüchtlingskrise versprochen hatten. Und auch der Vorschlag der EU-Kommission, die Grenzschutzagentur Frontex mit größeren Befugnissen zum Schutz der EU-Außengrenzen auszustatten, bleibt umstritten. *ahe*

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

In eigener Sache

JUSTIZ Rechte des Bundestags und Opferentschädigung

Es ist ein Thema von grundsätzlicher Bedeutung für die Stellung des Bundestags im deutschen und europäischen Verfassungsgefüge, mit dem sich die Rechtspolitiker des Parlaments ins neue Jahr stürzen: die „Beteiligung des Deutschen Bundestages an gemischten völkerrechtlichen Abkommen der Europäischen Union“. Am 13. Januar 2016 steht dazu eine öffentliche Anhörung im Rechtsausschuss an. Dabei geht es darum, ob das deutsche Parlament beispielsweise beim geplanten Freihandelsabkommen TTIP zwischen der EU und den USA oder dem bereits fertig ausgehandelten CETA-Handelsabkommen mit Kanada ein Wörtchen mitzureden hat oder ob die Bundesregierung nach eigenem Ermessen ja oder nein sagen kann.

Gemischte Abkommen sind Verträge, die sowohl Bereiche mit alleiniger Zuständigkeit der EU umfassen als auch solche, bei denen die Nationalstaaten mit zuständig sind. Solche Abkommen müssen durch die Mitgliedstaaten im Einklang mit den jeweiligen verfassungsrechtlichen Vorschriften ratifiziert werden. Sollte es sich also bei TTIP und CETA um gemischte Abkommen handeln – was selbst noch umstritten ist – besteht für den Bundestag ein erhebliches Interesse, seine Rolle im Ratifizierungsverfahren zu klären.

Zu den Vorhaben aus dem Koalitionsvertrag von CDU, CSU und SPD, die 2016 abgehakt werden sollen, gehört die Einführung eines Angehörigen-Schmerzensgelds. Es soll Hinterbliebenen von Menschen zustehen, die durch die Schuld anderer ums Leben gekommen sind. Außerdem soll ein neuer Anlauf bei der Bekämpfung von Menschenhandel und Zwangsprostitution unternommen werden. In der vergangenen Legislaturperiode hatte die CDU/CSU/FDP-Koalition einen Gesetzentwurf verabschiedet, den der Bundesrat jedoch vor der Bundestagswahl nicht mehr behandelt hatte und der der Diskontinuität anheim fiel. Ebenfalls auf der To-Do-Liste steht ein Thema, das durch den Fall Gustl Mollath in den Blickpunkt der Öffentlichkeit geraten war. Es geht um die Neufassung von Paragraf 63 des Strafgesetzbuches, der die zwangsweise Unterbringung in einem psychiatrischen Krankenhaus regelt.

Die Opposition möchte den Rechtsschutz für Opfer von sexueller Nötigung und Vergewaltigung erweitern. Dazu soll Paragraf 177 des Strafgesetzbuches neu gefasst werden. Auch eine Ausweitung des Diskriminierungsverbots auf Fälle der Benachteiligung aufgrund des Gesundheitszustands will die Opposition auf die Tagesordnung setzen. *Peter Stützle*

AUFGEKEHRT

Der Urlaub ist politisch

Sag' mir, wie Du Urlaub machst, und ich sag' Dir, wer Du bist. Da das Private bekanntlich inzwischen politisch ist, ist es wenig verwunderlich, dass auch der Urlaub zum Politikum werden kann. Rudolf Scharping (SPD), einst Verteidigungsminister, ließ sich mal frisch verliebt beim Planschen im Pool auf Mallorca ablichten, als sich gerade seine Soldaten auf einen Einsatz in Mazedonien vorbereiteten. Das kam nicht wirklich gut an. Er blieb nicht mehr lange im Amt.
Malle ist überhaupt ein schwieriges Pflaster für Politiker. Dort sitzen vermutlich auf jedem Quadratmeter vier Boulevardjournalisten und 16 Paparazzi: Innenminister Thomas de Maizière (CDU) versuchte Ende Oktober, sich ganze 3,5 Tage auf Mallorca zu entspannen, schon stand der Boulevard am Frühstückstisch und fragte ihn, was das solle. Es sei ja schließlich Flüchtlingskrise. Husch, husch, ab zurück ins Büro!
Wehe dem Politiker, der zu relaxen wagt. Es sei denn, es handelt sich um die Bundeskanzlerin. Dann frohlockt der Boulevard, zumal wenn es noch „exklusive" Fotos zu zeigen gibt. Nach einem aufreibenden Jahr voller Probleme, Krisen, Probleme, Horst Seehofer und noch mehr Krisen würde man der Kanzlerin ja glatt ein Frühstück mit Meeresblick oder das Planschen im Pool gönnen. Doch auch im Urlaub, so zeigen es die Urlaubsanalytiker des Boulevards, schont sich die Kanzlerin nicht. Sie „erholt" sich beim Wandern in den Schweizer Alpen. Immer höher, immer weiter. Sie schreitet voran, ihr Mann hinterher, Pausen werden wohl auch nicht gemacht. So geht Urlaub auf protestantisch. Immerhin: Angela Merkel kann im Urlaub von der Macht lassen. Ihr Mann darf die Touren auswählen. *Sören Christian Reimer*

VOR 15 JAHREN...

Minister gehen wegen BSE

9.1.2001: Fischer und Funke treten zurück Es begann am 24. November 2000 auf einem Hof in Schleswig-Holstein: Erstmals war BSE bei einer in Deutschland geborenen Kuh diagnostiziert worden. Die folgenden Bilder von torkelnden Rindern beunruhigten Verbraucher, denn der Erreger, der BSE bei den Tieren und die tödliche Creutzfeldt-Jakob-Krankheit beim Menschen auslöst, ist derselbe. Der Bundestag reagierte mit Sofortmaßnahmen, darunter ein Eilgesetz: Es verbot das Verfüttern von Tiermehl, das als BSE-Überträger galt. Dennoch gerieten Landwirtschaftsminister Karl-Heinz Funke (SPD) und Gesundheitsministerin Andrea Fischer (Bündnis 90/Die Grünen) in die Kritik. Am 9. Januar 2001 traten beide zurück.
„Ich muss erkennen, dass das Vertrauen der Bürger in die Fähigkeit der Bundesregierung das Problem BSE in ihrem Sinne zu bewältigen, erschüttert ist", sagte Fischer und räumte Fehler ein, „die aber eigentlich nicht zu einem Rücktritt gereicht hätten". Im Dezember hatte sie erklärt, es gebe keinen Anlass für den von der EU ins Gespräch gebrachten Verkaufsstopp für bestimmte Wurstwaren. Einen Tag später ruderte sie zurück. Funke begründete seinen Rücktritt mit mangelndem Rückhalt für seine Agrarpolitik in der Koalition. Noch am 5. Januar hatte er ein Programm für eine Landwirtschaftsreform vorgelegt.
Die von einigen Experten befürchteten Tausenden Todesfälle blieben allerdings aus. Bis Juni 2014 starben 229 Menschen an der Creutzfeldt-Jakob-Krankheit, die meisten in Großbritannien, wo BSE lange grassierte. Deutsche Opfer gab es nicht. *Benjamin Stahl*

© (c) Berlin Picture Gate

Andrea Fischer (B90/Die Grünen) erklärte am 9.1.2001 ihren Rücktritt.

Weiterführende Links zu den Themen dieser Seite finden Sie in unserem **E-Paper**

ORTSTERMIN: SIMULATION EUROPÄISCHES PARLAMENT 2015

Die Bundestagsabgeordnete Sonja Steffen (SPD) unterstützte die Teilnehmer der Parlamentssimulation. © Jan Steinhauer

»Von Politikverdrossenheit war nichts zu spüren«

Zu einem Kompromiss zu gelangen, ist nicht immer ganz einfach. Erst recht nicht in der Politik, obwohl dort Kompromisse gang und gäbe sind. Die 200 jungen Leute, die Mitte Dezember an der in den Gebäuden des Bundestags durchgeführten „Simulation Europäisches Parlament 2015" (SIMEP) teilgenommen haben, wissen dies jetzt auch. Zwei Tage lang schlüpften sie in die Rolle von Europaabgeordneten und diskutierten über die Themen Klima- und Energiepolitik, die Entwicklungspolitik der EU und das Freihandelsabkommen zwischen EU und den USA (TTIP). Teilgenommen an der Veranstaltung der Jungen Europäischen Bewegung Berlin-Brandenburg haben auch Friederike Handwerg und Celina Hollmichel, Elftklässlerinnen aus Oranienburg bei Berlin.
Die beiden jungen Frauen waren beeindruckt, „wie umfangreich die politischen Themen doch sind und wie schwer es sein kann, andere von der Meinung der Fraktion zu überzeugen, um am Ende ein für alle weitgehend zufriedenstellendes Ergebnis zu haben". Dennoch: Aus ihrer Sicht war die Simulation „ein voller Erfolg". Schließlich trafen die Teilnehmer auch auf „echte" Politiker wie die Bundestagsabgeordnete Sonja Steffen (SPD) und den Europaabgeordneten Hans-Olaf Henkel, die ihnen bei der Erarbeitung der Positionspapiere ihrer Fraktionen zur Hand gingen.
Zu Beginn der Veranstaltung stellte sich Stefan Liebich, Obmann der Linksfraktion im Europaausschuss, den Fragen der Programmteilnehmer. Er weihte sie auch in politische Eigenarten ein, wie etwa den Formelkompromiss. Dabei, so Liebich, werde ein Problem innerhalb einer Partei oder Fraktion durch das Finden einer Formulierung, die alle mittragen, vorläufig gelöst, die aber sogleich von allen unterschiedlich interpretiert werden kann. Als Beispiel nannte er die in seiner Fraktion gefundene Formulierung: „Wir wollen einen Neustart der EU." Dahinter fänden sich alle wieder – sowohl jene, die der EU mehr Befugnisse einräumen wollen, als auch diejenigen, die für eine Stärkung der Nationalstaaten plädieren.
Stefan Liebich zeigte sich im Anschluss an die Diskussionsrunde angetan von der Idee des Programms. „Ich finde es großartig, dass gerade in diesen Tagen, in denen die EU vor dem Hintergrund der Flüchtlingspolitik und auch der Austeritätspolitik auseinanderzudriften droht, junge Leute versuchen, Europa besser zu machen", sagte er. Die interessierten Fragen an ihn hätten gezeigt, „dass bei den Teilnehmern von Politikverdrossenheit nichts zu spüren war".
Ganz im Gegenteil: Die beiden 19-Jährigen Felix Klein und Lucas Trudwin aus Wernigerode im Harz waren gar schon zum dritten Mal in Berlin dabei. Die SIMEP biete eine Plattform, um sich mit politisch interessierten Menschen gleichen Alters zu treffen und mit ihnen zu diskutieren, sagt Felix Klein und findet: „Projekte wie dieses können zu einem besseren Bewusstsein der Menschen für die europäische Idee, die europäische Gemeinschaft und zu mehr Solidarität der Europäer untereinander beitragen." *Götz Hausding*

LESERPOST

Zu den Ausgaben 50-51 und 52 vom 7. und 21. Dezember 2015, „Wählerstimmen werden mehr Wert" (50-51, S. 13) und „Goldhandel lohnt sich nicht mehr" (52, S. 6):
Es ist allseitig bekannt, dass politische Parteien – abhängig vom jeweiligen Wahlergebnis – staatliche Gelder erhalten. Dabei hat das Bundesverfassungsgericht festgelegt, dass diese staatlichen Geldzuweisungen immer nur eine Teilfinanzierung der Parteienarbeit sein dürfen. Also benötigt jede Partei für mindestens die Hälfte ihrer Einnahmen andere Quellen. Eine junge, neue Partei, die noch nicht in allen Landtagen und auch nicht im Bundestag vertreten ist, wird natürlich alles daran setzen, dadurch im politischen Wettbewerb keine Nachteile zu haben. Eine solche Partei verfügt eben noch nicht wie die Altparteien über politische Stiftungen, angespartes Vermögen, Immobilien, Verlagsanteile etc.

Claus Hörrmann,
Neustadt in Sachsen

Der Selbstbedienungsladen für die Parteien steht mal wieder offen. Egal mit welcher Begründung die Farbe der „Mäuse" ausgestattet wird, Hauptsache die Katze (Parteien) kann sie fressen. Spätestens wenn wieder Gesetzesvorhaben beraten werden und die Lobbyisten ihre Vorlagen vorlegen, werden die jetzigen Begründungen ad absurdum geführt. Stecken nicht in diesen Verfahren der ständigen Selbstbedienung der Parteien die Begründungen für extreme Parteien und für die Unzufriedenheit der Wähler?

Manfred Müter,
Bad Lippspringe

Zu „Das Parlament" im Allgemeinen:
Durch Zufall hatte ich während der Sommerferien ein älteres Exemplar von „Das Parlament" in einer Leihbücherei gesehen und mitgenommen. Seitdem bin ich Abonnent der Zeitung.
Mit jeder Ausgabe freue ich mich über die informative Berichterstattung und die schöne Kombination aus aktueller Berichterstattung, Debattendokumentation und APuZ. Dies ist die beste Zeitung, die ich kenne, und ich finde es schade, dass ich 50 Jahre gebraucht habe, um darauf zu stoßen.

Karl Jonas,
per E-Mail

Zur Ausgabe 49 vom 30. November 2015, „Kopf der Woche" (Clemens Binninger) auf Seite 1:
Nach dem Lesen dieses Artikels war ich mir nicht ganz sicher, ob es sich hier um eine Glosse handelt oder ob der Verfasser es tatsächlich ernst meint. Was prädestiniert eigentlich Clemens Binninger (CDU) mit diesem „Format" und seiner Unberechenbarkeit in einem weiteren Ausschuss tätig zu sein, wenn er schon einmal aus „ungeklärten" Gründen den Bettel hingeworfen hat? Ist es als „Lohn" für seine Parteizugehörigkeit, ist es seine Abgeordnetentätigkeit seit zirka 13 Jahren oder welche verborgenen Eigenschaften hat Herr Binninger?

Gerhard Grünwald,
Schwandorf

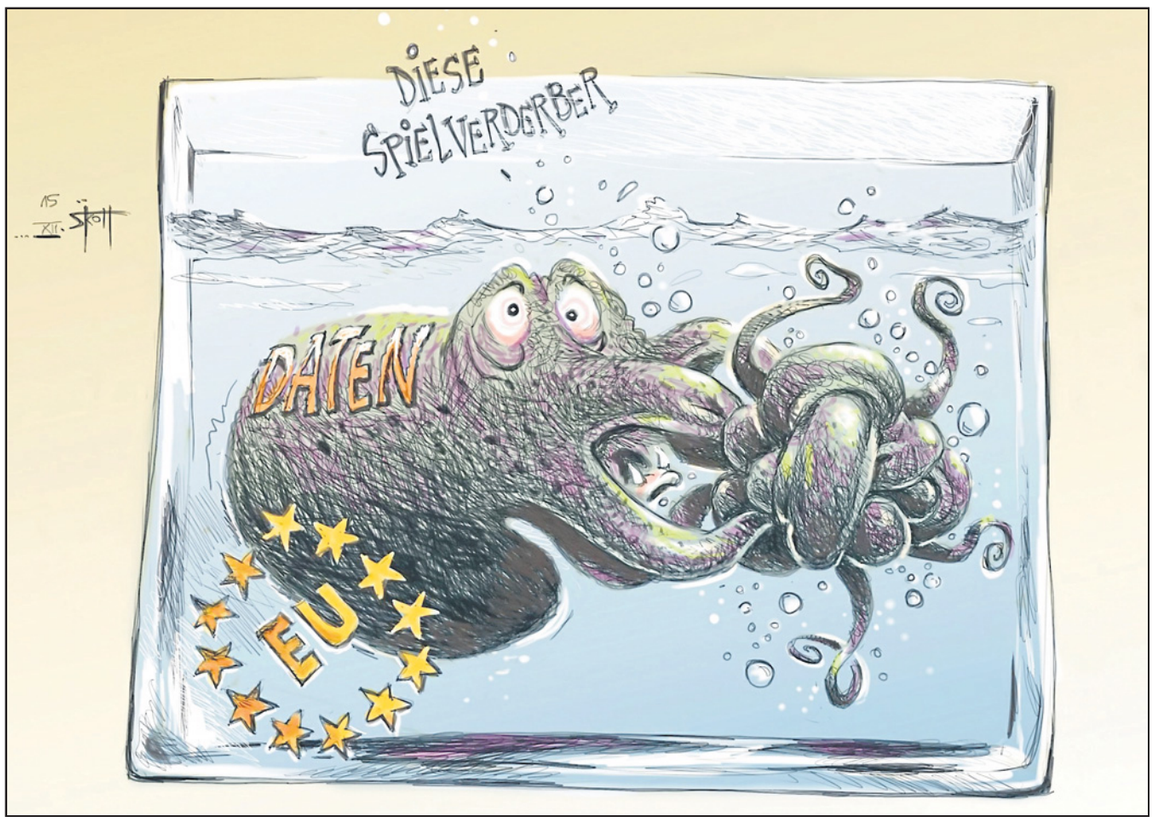
Haben Sie Anregungen, Fragen oder Kritik?
Schreiben Sie uns:

Das Parlament
Platz der Republik 1
11011 Berlin
redaktion.das-parlament@bundestag.de

Leserbriefe geben nicht die Meinung der Redaktion wieder. Die Redaktion behält sich vor, Leserbriefe zu kürzen.

Die nächste Ausgabe von „Das Parlament" erscheint am 18. Januar.

SEITENBLICKE



BUNDESTAG LIVE

Topthemen vom 11. – 15.1.2016

Lebensmittelkennzeichnung (Do)
Pestizide (Fr)

Phoenix überträgt live ab 9 Uhr

Auf www.bundestag.de:
Die aktuelle Tagesordnung sowie die Debatten im Livestream

PERSONALIA

>Wolfgang Ehmke
Bundestagsabgeordneter 1983-1985, Die Grünen
Am 5. Januar wird Wolfgang Ehmke 70 Jahre alt. Der Diplom-Agrarbiologe, promovierte Agrarwissenschaftler und zuletzt, von 1986 bis 1999, Abteilungsleiter Naturschutz im Hessischen Umweltministerium trat dem Bund für Umwelt und Naturschutz Deutschland bei. 1990 wurde er Mitglied der Partei „Die Grünen". Im Bundestag gehörte Ehmke dem Innenausschuss an.

>Klaus-Dieter Uelhoff
Bundestagsabgeordneter 1987-1998, CDU
Am 9. Januar begeht Klaus-Dieter Uelhoff seinen 80. Geburtstag. Der promovierte Jurist und Verwaltungsbeamte aus Dahn/Kreis Südwestpfalz trat 1969 der CDU bei. Er begann seine Karriere im rheinland-pfälzischen Staatsdienst, war von 1972 bis 1979 Landrat des Kreises Pirmasens und von 1979 bis 1987 Staatssekretär im Innen- bzw. im Umwelt- und Gesundheitsministerium in Mainz. Von 1979 bis 1996 gehörte er dem CDU-Kreis- und Bezirksvorstand Rheinhessen-Pfalz an. Der Direktkandidat des Wahlkreises Pirmasens arbeitete im Bundestag im Verteidigungs- sowie im Haushaltsausschuss mit. Von 1989 bis 1999 gehörte Uelhoff der Nordatlantischen Versammlung an.

>Georg Bamberg
Bundestagsabgeordneter 1981-1990, SPD
Georg Bamberg vollendet am 9. Januar sein 80. Lebensjahr. Der Bundesbahnbeamte trat 1964 der SPD bei, war von 1966 bis 1981 Mitglied des Stadtrats von Rosenheim und gehörte von 1974 bis 1981 dem Bezirkstag von Oberbayern an. Bamberg, der im Februar 1981 in den Bundestag nachrückte, war in allen drei Legislaturperioden Mitglied des Verkehrsausschusses.

>Sigrid Folz-Steinacker
Bundestagsabgeordnete 1987-1990, FDP
Am 10. Januar wird Sigrid Folz-Steinacker 75 Jahre alt. Die Kauffrau aus Brake trat 1977 der FDP bei. Sie gehörte dem FDP-Landesvorstand Niedersachsen sowie dem Bundesfachausschuss Entwicklungspolitik ihrer Partei an. Im Bundestag arbeitete Folz-Steinacker im Wirtschaftsausschuss sowie im Ausschuss für wirtschaftliche Zusammenarbeit mit.

>Manfred Schmidt
Bundestagsabgeordneter 1969-1990, SPD
Am 16. Januar vollendet Manfred Schmidt sein 80. Lebensjahr. Der Münchner Rechtsanwalt trat 1957 in die SPD ein und war zeitweise Mitglied des Münchner Parteivorstands. Schmidt engagierte sich im Bundestag vorwiegend im Rechtsausschuss. Von 1974 bis 1978 gehörte er dem Europäischen Parlament sowie von 1980 bis 1990 der Parlamentarischen Versammlung des Europarates und der Westeuropäischen Union an.

>Hannegret Hönes
Bundestagsabgeordnete 1985-1987, Bündnis 90/Die Grünen
Am 16. Januar wird Hannegret Hönes 70 Jahre alt. Die Journalistin trat 1979 der Partei Die Grünen bei und gehörte von 1981 bis 1983 dem Landesvorstand von Baden-Württemberg an. 1985 rückte Hönes in den Bundestag nach und war Mitglied des Innenausschusses. Zugleich amtierte sie als Fraktionssprecherin. Seit Jahren hat sie ein Mandat in der der Gemeindevertretung von Niedernhausen im Rheingau-Taunus-Kreis inne.

>Klaus Bühler
Bundestagsabgeordneter 1976-2002, CDU
Klaus Bühler wird am 16. Januar 75 Jahre alt. Der Realschullehrer aus Bruchsal schloss sich 1962 der CDU an. Von 1968 bis 1976 war er Mitglied des Stadtrats seiner Heimatstadt und von 1971 bis 1973 Kreistagsabgeordneter in Bruchsal bzw. von 1973 bis 1989 in Karlsruhe. Im Bundestag engagierte sich der Direktkandidat des Wahlkreises Karlsruhe-Land vorwiegend im Verkehrsausschuss. Von 1987 bis 2002/03 gehörte er der Parlamentarischen Versammlung des Europarats und der Westeuropäischen Union an. Von 1996 bis 1999 war Bühler Vizepräsident des Europarats und von 2000 bis 2002 Präsident der WEU.

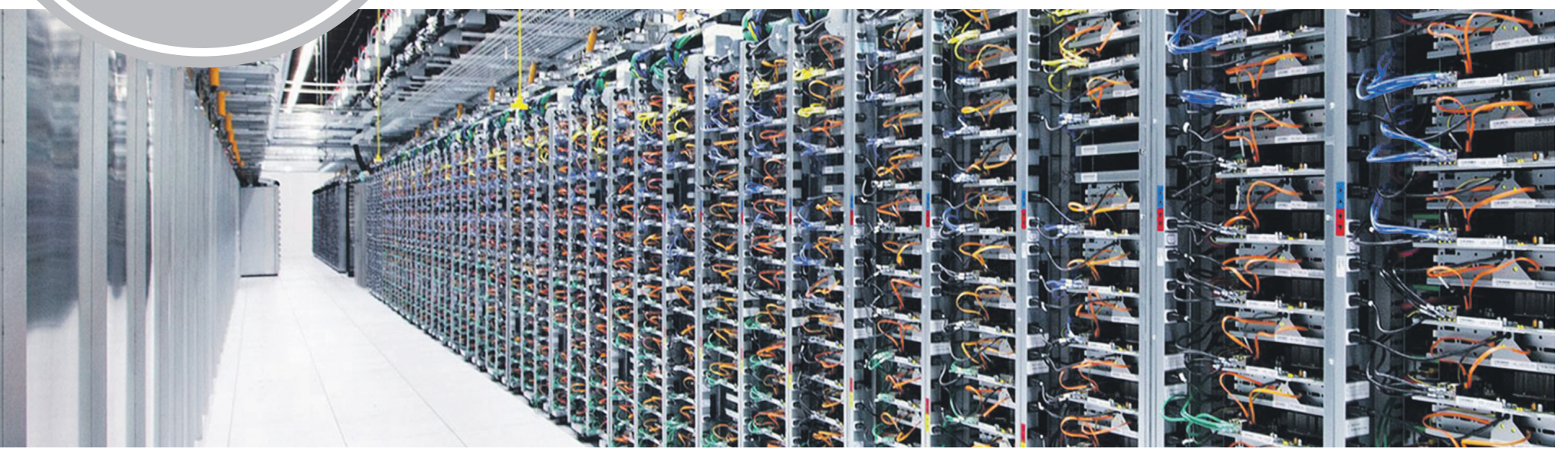
>Elfriede Eilers
Bundestagsabgeordnete 1957-1980, SPD
Elfriede Eilers vollendet am 17. Januar ihr 95. Lebensjahr. Die Sozialarbeiterin aus Bielefeld trat 1945 der SPD bei. Von 1972 bis 1990 amtierte sie als stellvertretende Bundesvorsitzende der Arbeiterwohlfahrt. Dem SPD-Parteivorstand gehörte sie von 1966 bis 1977 und dem Parteipräsidium von 1972 bis 1977 an. Von 1973 bis 1979 stand sie zudem an der Spitze der Arbeitsgemeinschaft sozialdemokratischer Frauen. Im Bundestag war Eilers, die von 1977 bis 1980 als Parlamentarische Geschäftsführerin ihrer Fraktion amtierte, vorwiegend Mitglied des Ausschusses für Jugend, Familie und Gesundheit. Sie gehört neben sechs weiteren Abgeordneten zu den letzten Mitgliedern des 3. Deutschen Bundestags von 1957 bis 1961. *bmh*

Informationen in leichter Sprache Ausgabe-Nr. 28 Beilage für: DasParlament

leicht erklärt!

Daten-Sammlungen

Daten nutzen, Daten schützen



Was sind Daten?

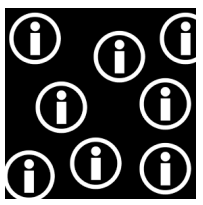
„Daten“ ist ein Wort
aus der schweren Sprache.

Damit sind alle Infos gemeint,
die man über eine Sache haben kann.

Vor allem aber auch
über einen Menschen.

Daten über einen Menschen
sind zum Beispiel:

- Sein Name.
- Seine Adresse.
- Seine Lieblings-Farbe.



„Daten-Sammlung“ bedeutet,
dass man sehr viele Infos
zusammen-sucht.

Man fragt also zum Beispiel
ganz viele Menschen
nach ihrer Lieblings-Farbe.

Diese Infos speichert man dann ab.

Zum Beispiel in einem Computer.

Heutzutage werden
sehr viele Daten gesammelt.

Das hat damit zu tun,
dass das von Computern
gemacht wird.

Zum Beispiel, wenn jemand
im Internet unterwegs ist.

Und weil es heute
so viele Computer gibt,
gibt es auch so viele Daten.

Was macht man mit Daten?

Wenn man viele Daten
über eine Sache hat,
dann kann man die Daten auswerten.

„Auswerten“ ist schwere Sprache.

Das bedeutet, dass man sich
die Daten ganz genau anguckt.

Und so neue Infos
über die Sache bekommt.

Infos, die man vorher
noch nicht hatte.

Ein Beispiel: Einkaufen im Internet

Viele Menschen
kaufen Dinge in Internet-Läden.

Diese Internet-Läden
speichern dazu Daten.

Zum Beispiel:

- Was eine Person gekauft hat.
- Wann sie es gekauft hat.
- Ob sie es zurück-gegeben hat.

Dabei entstehen sehr viele Daten.

Denn jeden Tag kaufen unheimlich
viele Menschen im Internet ein.

Ein Internet-Laden
kann die Daten nun auswerten
und eine Menge erfahren.

Zum Beispiel, welche Dinge
die Kunden besonders oft kaufen.

Dann kann der Internet-Laden
noch mehr davon anbieten.

Der Internet-Laden lernt auch
immer mehr über einzelne Kunden.

Denn er speichert alles,
was eine Person gekauft hat.

Dann weiß er immer genauer,
was die Person mag.

Und er kann das vergleichen
mit anderen Menschen,
die ähnliche Dinge gekauft haben.

Irgendwann kann der Internet-Laden
der Person dann Dinge zum Kaufen
vorschlagen.

Dinge, die ihr gefallen könnten, weil
sie auch anderen Kunden mit einem
ähnlichen Geschmack gefallen haben.

Dadurch kauft die Person
dann vielleicht etwas,
das sie ohne den Vorschlag
nicht gekauft hätte.

Was ist gut an Daten-Sammlungen?

Wenn man sich Daten
genau anschaut,
dann kann man also
bestimmte Dinge besser verstehen.

Man kann auch Vermutungen
über die Zukunft machen.

Und dann
bessere Entscheidungen treffen.

Und je mehr Daten man hat,
desto genauer sind oft die Dinge,
die man daraus lernen kann.

Bei großen Daten-Sammlungen
hat man sehr viele Daten.

Und man guckt sie sich
natürlich nicht einfach so an.

Man lässt das
einen Computer machen.

Darum kann man dadurch
besonders viel erfahren.

Die Auswertung
von Daten-Sammlungen
hilft also bei vielen Dingen.

Nicht nur bei Internet-Läden.

Man kann sie zum Beispiel
auch benutzen,
um Verbrechen zu verhindern.

Die Polizei sammelt dafür
beispielsweise Infos,
an welchen Orten
Verbrechen passiert sind.

Dann untersucht sie die Daten.

Und kann dann vorhersagen,
wo vielleicht wieder ein Verbrechen
passieren wird.

Ein anderes Beispiel sind Flugzeuge.

Früher mussten Techniker Flugzeuge
nach der Landung checken.

Sie mussten gucken,
ob das Flugzeug irgendwo kaputt war.

Das dauerte lange.

Solange konnte das Flugzeug
nicht fliegen.

Und die Flug-Gesellschaft
konnte damit kein Geld verdienen.

Eine bestimmte Firma
macht das jetzt anders.

Sie baut Motoren für Flugzeuge.

Die Flugzeuge senden
während dem Flug
die ganze Zeit Daten an die Firma.

So erfährt sie sofort,
ob etwas mit dem Flugzeug
nicht stimmt.

Noch während es fliegt.

Die Techniker von der Firma
können dann herausfinden,
was genau kaputt ist.

Und wie man es reparieren kann.

Das sagen sie dann
der Flug-Gesellschaft.

Und die kann das Flugzeug sofort
reparieren, wenn es gelandet ist.

Durch die Auswertung der Daten
geht die Reparatur also viel schneller.

Was ist schlecht an Daten-Sammlungen?

Es gibt auch Leute, die manche
Dinge an Daten-Sammlungen
nicht gut finden.

Vor allem, wenn man
Infos über Menschen sammelt.

Die eigenen Daten sind nämlich
etwas sehr Persönliches.

Und manche Dinge will man vielleicht
vor anderen Menschen
geheim-halten.

Darum sollte jeder Mensch
selbst entscheiden,
wer seine Daten haben darf.

Und welche Daten genau.

Und was damit gemacht wird.

Persönliche Nachteile

Manche Menschen haben Angst,
dass sie irgendwann
keine Geheimnisse mehr haben.

Auch dafür gibt es ein Beispiel:

Es gibt inzwischen besondere Geräte.

Man trägt sie
wie Uhren am Hand-Gelenk.

Sie messen den ganzen Tag,
wie gesund ein Mensch ist.

Zum Beispiel messen sie:
- Den Blut-Druck,
- den Herz-Schlag
- und wie viel man sich bewegt.

Es könnte nun passieren,
dass die Kranken-Kasse
diese Infos bekommt.

So erfährt sie dann zum Beispiel,
wenn ein Mensch sehr ungesund lebt.

Zum Beispiel,
weil er sich zu wenig bewegt.

Dann könnte die Kranken-Kasse
für die Person teurer werden.

Daten und die NSA

Besonders bekannt ist das Problem
mit den persönlichen Daten
zum Beispiel durch die NSA geworden.

Die NSA ist ein Geheim-Dienst.

Und zwar einer aus den USA.

Ein Geheim-Dienst ist eine Behörde.

Er sammelt Infos.

Zum Beispiel:

- Über gefährliche Gruppen
  im eigenen Land.

- Oder über andere Länder.

Dadurch soll der Geheim-Dienst
Gefahren abwehren.

Und zum Beispiel Verbrecher finden.

Im Jahr 2013 kam dann heraus:

Die NSA hat mehr Infos gesammelt,
als man bisher gedacht hatte.

Und zwar
in vielen Ländern auf der Welt.

Sie hat zum Beispiel heimlich
bei Telefon-Gesprächen mitgehört.

Und heimlich E-Mails gelesen.

Und sie hat das
auch bei Menschen gemacht,
die nichts Schlimmes getan haben.

Die NSA hat also
viele persönliche Daten
über diese Menschen bekommen.

Und das, ohne sie vorher zu fragen.

Es ist zwar die Aufgabe
von einem Geheim-Dienst,
Infos zu sammeln.

Trotzdem waren viele Menschen
erschrocken.

Weil die NSA
so viele Daten gesammelt hat.

Und weil
niemand etwas davon wusste.

Viele Menschen sprechen also
im Moment über Daten-Sammlungen.

Manche sehen die Vorteile.

Andere sehen eher die Nachteile.

Und manche machen sich Sorgen.

In Zukunft müssen wir uns darum
viele Gedanken darüber machen,
wie man große Daten-Sammlungen
richtig nutzen kann.

Weitere Informationen in leichter
Sprache gibt es unter:
www.bundestag.de/leichte_sprache

Impressum

Dieser Text wurde in leichte Sprache
übersetzt von:

Nachrichten Werk
www.nachrichtenwerk.de

Ratgeber Leichte Sprache:
http://tny.de/PEYPP

Die Bilder sind von Picto-Selector und:
Titelbild: dpa/picture-alliance

Beilage zur Wochenzeitung
„Das Parlament“ 1-2/2016

Die nächste Ausgabe erscheint am
18. Januar 2016