»Wie fühlst du dich?«, fragen die Internetkonzerne. Aber was machen sie mit unseren Antworten?

»Ich bin mir sicher, dass jemand mithört, wenn ich telefoniere«

Interview: Martina Kix
Fotos: Arvida Byström

Facebook, »Safe Harbor« und der Überwachungsstaat: Der Grünen-Politiker Jan Philipp Albrecht kämpft im EU-Parlament für den Schutz unserer Daten und Bürgerrechte. Er sagt: Jetzt werden die Regeln festgelegt, nach denen wir in der digitalen Zukunft leben werden.

Am Eingang des Europäischen Parlaments in Brüssel hängen die Fahnen der 28 Mitgliedsstaaten der Europäischen Union schlaff im Nieselregen. Unzählige Menschen gehen an diesem grauen Oktobertag in Mänteln, Kostümen und Anzügen durch die Sicherheitsschleuse am Eingang: Anwälte, Aktivisten, Beamte, Lobbyisten und Abgeordnete. In den verspiegelten Bürotürmen werden Gesetze ausgearbeitet, die in ganz Europa gelten werden. Auch Jan Philipp Albrecht, Europaabgeordneter der Grünen für Hamburg und Schleswig-Holstein, arbeitet in der belgischen Hauptstadt. Statt Anzug trägt er ein grün-blaues Ringelshirt. In der Hand hält er eine Flasche der Hackerbrause Club-Mate. Ein Statement: Politik kann man auch machen, wenn man ein Nerd aus der linken Aktivistenszene ist. 2009 wurde Albrecht mit 26 Jahren als damals jüngster deutscher Abgeordneter ins Parlament gewählt. Heute ist er innen- und justizpolitischer Sprecher der Grünen-Europafraktion. Seine Mission: eine neue Datenschutzverordnung, die die Rechte der Bürger wirklich schützt. Es sind aufregende Monate für ihn, er verhandelt mit dem EU-Ministerrat und der EU-Kommission über Details und debattiert mit Industrievertretern. Die neue Verordnung wird Auswirkungen darauf haben, wie Internetkonzerne in Zukunft mit unseren Daten umgehen.

—

Jan Philipp, ich habe mich gerade bei Facebook eingeloggt und im Status markiert, dass ich im »European Parliament« bin. Ich habe sofort 25 Likes von Freunden aus Hamburg, New York und Teheran bekommen. Was genau passiert da eigentlich?

Dein Status-Update wird wohl zunächst an das knapp 30 000 Quadratmeter große Facebook-Datenzentrum im schwedischen Luleå gesendet. Bisher kannst du davon ausgehen, dass deine Daten mindestens einmal auf einem Server gespiegelt werden, der in einem anderen Land liegt – irgendwo in Indien, den USA oder Asien. Und dort gilt der europäische Datenschutz nicht. Das ist ein Problem. Denn die Internetkonzerne machen mit unseren Daten häufig, was sie wollen. Vielleicht liegt auf einem Server im Silicon Valley ein Partyfoto, das du vor drei Jahren gelöscht hast. Vielleicht gibt Facebook deine Daten an die NSA weiter. Das ist ziemlich intransparent.

Facebook speichert die Daten nicht nur, sondern analysiert sie genau. ›

› Ja, du meldest dich ja nicht nur an, sondern markierst die Urlaubsfotos deiner Freunde mit »gefällt mir«, postest Songs und Nachrichten und pflegst Kontakte. Mit jeder Aktion wird das Bild, das Facebook von dir hat, konkreter und erlaubt Rückschlüsse auf dein Leben. Die Informationen werden an Werbepartner verkauft. Im digitalen Zeitalter sind persönliche Daten zu einer neuen Währung geworden. Wenn du Babyfotos likest, wird dir Babybreiwerbung angezeigt. Das ist natürlich eine ziemlich intensive Analyse deines Lebens.

Der Österreicher Max Schrems forderte vor einiger Zeit bei Facebook seinen Datensatz an und bekam ein Dokument mit 1222 Seiten zugesandt. Darunter waren auch Freundschaftsanfragen, die er abgelehnt hatte, sowie Fotos, Chats und Statusmeldungen, die längst gelöscht waren.

Ja. Und Facebook ist nicht der einzige Datensammler auf der Welt. 2014 wurde bekannt, dass die Taschenlampen-App Brightest Flashlight Free jederzeit Standortdaten an den App-Betreiber versandte. Der Aufenthaltsort der knapp fünfzig Millionen Nutzer wurde dann weiterverkauft, ohne dass die Nutzer jemals eingewilligt hatten. Erst nach Protesten mussten die App-Entwickler alle personenbezogenen Daten löschen.

Viele nehmen das hin, aber Max Schrems reichte am Europäischen Gerichtshof Klage gegen Facebook ein – und gewann den Prozess. Damit hat er die »Safe Harbor«-Erklärung gekippt, die es Unternehmen wie Facebook einfach machte, personenbezogene Daten aus den Ländern der Europäischen Union in die USA zu übermitteln und dort zu speichern. Für seine Klage wird Schrems nun als Held gefeiert, aber Facebook ist immer noch online. Was wird das Urteil verändern?

Unmittelbar wird es dazu führen, dass Facebook und Co unsere Daten über andere Wege in die USA schaffen. Langfristig wird es hoffentlich dazu führen, dass Mark Zuckerberg und seine Kollegen aus dem Silicon Valley mehr Datenzentren in europäischen Ländern bauen werden. Nur so können sie die EU-Richtlinie aus dem Jahr 1995 befolgen, die regelt, wie personenbezogene Daten als Grundrecht geschützt werden.

Reichen die bestehenden Regeln denn aus?

Wir arbeiten seit vier Jahren an der Neuordnung des europäischen Datenschutzrechts. Im Moment sind die zuständigen Behörden in den einzelnen Mitgliedsländern nicht gut ausgestattet, die Bußgelder bei Verstößen sind gering und Firmen müssen sich mit 28 verschiedenen Datenschutzrechten beschäftigen. Unsere Reform verfolgt drei Ziele: Stärkung der Verbraucherrechte. Härtere Sanktionen bei Gesetzesbrüchen. Und das Regelwerk soll in ganz Europa verbindlich sein. So wird es Unternehmen erleichtert, sich ans Gesetz zu halten. Die Chancen, dass die Verhandlungen noch in diesem Jahr abgeschlossen werden, stehen gut.

Aber natürlich hat jeder Facebook-Nutzer den Allgemeinen Geschäftsbedingungen zugestimmt. Das heißt doch, dass wir mit der Speicherung der Daten einverstanden sind, oder?

Die größte Lüge im Internet ist doch immer noch: »Ich habe die Datenschutzerklärung gelesen und akzeptiere sie!«

Kein Mensch würde einen Mietvertrag unterschreiben, ohne ihn genau gelesen und sich informiert zu haben. Warum klicken wir im Internet so leichtgläubig auf den O.k.-Knopf?

Wenn wir wirklich alle Datenschutzerklärungen durchlesen würden, würde uns das die Hälfte unserer Lebenszeit kosten. Außerdem sind die Formulierungen so vage gewählt, dass ihre Interpretation selbst dann, wenn es zu einem Gerichtsprozess käme, Auslegungssache wäre. Deshalb fordern wir in der neuen Datenschutzverordnung, dass dir nicht nur der Text angezeigt wird, sondern standardisierte Symbole – wie Verkehrszeichen. Die sagen: Deine Daten werden weitergegeben, etwa in ein anderes Land, verkauft oder zu einem anderen Zweck genutzt, den ich nicht auf den ersten Blick erkennen kann. Bei vielen Apps ist bisher nicht nachvollziehbar, was passiert.

Grundsätzlich sinkt das Vertrauen in soziale Medien. Laut der aktuellen Shell-Jugendstudie vermuten 84 Prozent der Menschen zwischen 12 und 25 Jahren, dass große Konzerne wie Facebook oder Google Geld mit den Daten der Nutzer verdienen. 53 Prozent sagen, dass sie Facebook »nicht ganz vertrauen«. Überrascht dich das?

Unsere Generation hat bereits einige Daten-GAUs erlebt. Edward Snowdens Enthüllungen über die Datenspionage der Geheimdienste. Die gehackten Playstation-Server des Sony-Konzerns. Die Kriminellen, die Kreditkartendaten klauen. Das alles führt dazu, dass sich die Sensibilität für den Umgang mit Daten grundlegend verändert. Noch vor wenigen Jahren hatte die Post-Privacy-Theorie, die die Abschaffung von Datenschutz und Privatsphäre forderte, deutlich mehr Anhänger. Heute überlegen die allermeisten es sich gut, ob man ein Nacktfoto bei Tinder verschickt oder mit seiner Kollegin per Mail über den Chef lästert. Denn bei allen Daten, die man verschickt, muss man sich fragen, ob sie nicht irgendwann bei der Oma, dem Chef oder der Polizei landen.

Man nennt uns Digital Natives – wir müssten doch wissen, wie sensibel unsere Daten sind.

Durchaus. Unsere Eltern haben früher an Autos geschraubt, heute finden wir es cool, Apps für Smartphones zu entwickeln, und müssen nicht einmal befürchten, den Nerd-Stempel aufgedrückt zu bekommen. Viele junge Menschen arbeiten derzeit an Programmen, die Daten sicherer machen. Das ist wunderbar.

Die kommerzielle Nutzung unserer Daten ist eine Sache. Die Überwachung, die Big-Data-Anwendungen ermöglichen, eine andere. Wie ist das bei dir? Gehst du davon aus, dass Geheimdienste deine E-Mails lesen und dein Telefon abhören?

Ja, aber als Politiker ist meine Arbeit öffentlich, und wenn ich dabei schon überwacht werde, kann das auch gleich live gestreamt werden. Im Ernst: Im Europaparlament stehen in allen Büros Computer mit Microsoft-Betriebssystemen und Telefone des amerikanischen Anbieters Cisco. Der Quellcode von deren Hard- und Software ist geheim, sodass darin Hintertüren für Geheimdienste versteckt sein könnten, durch die sie Zugriff auf unsere Daten gewinnen. Außerdem beweisen die Snowden-Dokumente, dass der britische Geheimdienst gemeinsam mit der NSA die belgischen Kommunikationsdienstleister abhört, um Informationen über die EU-Institutionen und die NATO zu bekommen. Ich mache mir nicht vor, dass sie mein Telefon auslassen.

Und was machst du, wenn du nicht abgehört werden willst?

Meine Handynummer habe ich seit Jahren. Damals habe ich noch als Aktivist gegen Castor-Transporte demonstriert. Ich bin mir sehr sicher, dass jemand mithört, wenn ich telefoniere. Privat benutze ich auch mal andere Telefone und vor allem Verschlüsselungsdienste wie Textsecure oder Signal. Inzwischen wird ja leider jeder überwacht.

Du spielst damit auf das Gesetz zur Vorratsdatenspeicherung an, das gerade in Deutschland verabschiedet wurde. Telekommunikationsunternehmen müssen nun zehn Wochen lang speichern, mit wem wir telefoniert haben.

Das ist ein Eingriff in unsere Grundrechte. Das Gesetz konzentriert sich ja gar nicht darauf, Verdächtige zu überwachen. Es werden enorme Datenmengen von Menschen gesammelt, die vollkommen unbescholten sind. Jede SMS, die wir verschicken, wird gespeichert, jeder Anruf bei Oma. Deshalb gab es auch so massiv viele Proteste gegen das Gesetz.

Was ist mit den deutschen Kämpfern des Islamischen Staats? Ich bin ganz froh, dass deren Whatsapp-Gruppen überwacht werden.

Es geht um die Verhältnismäßigkeit solcher Maßnahmen. Stell dir vor, auf einem Platz in deiner Stadt passieren regelmäßig Straftaten. Dann wäre es doch auch nur wirksam und angemessen, den entsprechenden Platz zu überwachen und nicht gleich das ganze Land.

Braucht dann jeder ein abhörsicheres Krypto-Handy wie Angela Merkel?

Nein, eigentlich nicht. Bei Diensten wie dem Messaging-Service Threema und auch bei iMessage kann niemand so schnell deine Urlaubsfotos abgreifen. Die Nachrichten werden den Herstellern zufolge vom Sender zum Empfänger verschlüsselt. Der einzige Haken: Auch diese Dienste legen ihren Quellcode nicht offen. Wirklich sicher sind nur Open-Source-Anbieter, die keine eigenen Interessen verfolgen und ihre Technik offenlegen.

Ist Datenschutz Aufgabe des Staates oder müssen wir uns selbst darum kümmern?

Nach den Snowden-Enthüllungen haben einige Politiker gesagt: »Wer Angst vor der Überwachung seiner Daten hat, soll das Internet nicht mehr nutzen.« Das ist vollkommen inakzeptabel. Kein Politiker würde doch behaupten, dass man halt nicht auf die Straße gehen darf, wenn man sich vor einem Unfall fürchtet. Das Leben findet heute zum Großteil im Internet statt. Die Politik muss deshalb auch Regeln für den Onlineverkehr festlegen und Gesetze verabschieden, die sicherstellen, dass Daten nicht einfach gesammelt, analysiert und weitergegeben werden. Es darf nicht sein, dass jeder App-Anbieter oder jedes Netzwerk mir meine Daten wie Geldscheine aus der Tasche zieht. Ich muss individuell entscheiden, wem ich meine Daten gebe und wer sie zu welchem Zweck nutzen darf. Wir haben ein Recht auf Selbstbestimmung.

Die US-Konzerne Yahoo und Google arbeiten offenbar daran, dass wir in Zukunft E-Mails mit einem Klick verschlüsseln können. Wenn wir diese Funktion nutzen, löst dann am Ende der Markt das Datenschutzproblem?

Bei Konzernen muss man skeptisch bleiben und sich immer fragen, warum sie so eine Vision in die Welt setzen. Dagegen zeigen Initiativen wie die Kampagne »Free Your Data«, die sich derzeit noch durch Crowdfunding finanziert, wie wir auch durch neue innovative Angebote die Hoheit über unsere Daten zurückerhalten können. Das finde ich toll.

In dem Dokumentarfilm »Democracy – Im Rausch der Daten«, der deine Arbeit zeigt, kommt in einer Szene ein Anwalt auf dich zu und sagt, dass er für einen amerikanischen Konzern arbeitet. Wie viel Druck üben Lobbyisten auf dich aus?

Es werden keine Briefumschläge mit Euro-Scheinen unter der Bürotür durchgeschoben, aber Lobbyismus spielt hier in Brüssel eine große Rolle. Man erfährt leider nicht einmal, für wen die Anwälte arbeiten, weil sie sich bei ihrer Lobbytätigkeit auf das Mandatsgeheimnis berufen. Nachdem die damalige EU-Justizkommissarin Viviane Reding den Entwurf zum neuen EU-Datenschutzrecht vorgestellt hatte, haben Hunderte Interessenvertreter, vor allem aus der Wirtschaft, an meine Tür geklopft. Man muss verdammt aufpassen, dass man dabei keine einseitige Wahrnehmung entwickelt.

Wie würde eine ideale Welt aussehen, in der alle unsere Daten sicher sind?

Datensparsamkeit ist eine gute Grundeinstellung. Wir sollten in unserer Kommunikation darauf achten, weniger personenbezogene Daten freizugeben, und zweimal überlegen, ob private Informationen aus unserem eigenen Leben oder dem anderer tatsächlich mit allen geteilt werden müssen. Manchmal ist es absolut ausreichend, Dienste anonym zu nutzen. Und nicht alle Fotos müssen in der Cloud liegen, einige sollte man vielleicht auf einer externen Festplatte speichern oder ganz oldschool ausdrucken. ●

Foto: Stefan Thomas Kröger / laif

JAN PHILIPP ALBRECHT, 32,

ist innen- und justizpolitischer Sprecher der Grünen-Fraktion im Europäischen Parlament. Sein wichtigstes Thema: Bürgerrechte im digitalen Zeitalter. Aktuell arbeitet er an einer Datenschutzreform für die gesamte Europäische Union. 2014 erschien sein Buch »Finger weg von unseren Daten!«. Ein Filmteam hat Albrecht und seine Mitarbeiter zwei Jahre lang für die tolle Dokumentation »Democracy – Im Rausch der Daten« begleitet. Der Film läuft ab dem 12. November im Kino.