

»DAS FLIEGENPAPIERPROBLEM«

Datenschutz in Theorie und Praxis: Prof. Dr. Indra Spiecker im Gespräch

Das Smartphone ist unser ständiger Begleiter. Dadurch ist unser Leben auf Schritt und Tritt verfolgbar. Nehmen Sie das für sich persönlich in Kauf?

Es gibt ein paar Mittel, den Gefährdungen entgegenzuwirken. Das eine ist, das Ding gelegentlich auszuschalten: Wenn ich mich nicht mit einer Funkzelle verbinde, bin ich auch nicht zu orten. Das Zweite ist, dass ich zwei Handys habe. Das eine nutze ich für Dinge, von denen ich eigentlich abrate, sie zu tun. Das andere ist das Handy, mit dem ich unterwegs bin. Das sind Strategien, die man als Diversifikation oder Dezentralisierung bezeichnet: Man sollte nicht alle Dienste über einen Anbieter abfragen, nicht alle zusammenlaufen lassen in einer Cloud et cetera. Überdies gibt es Anbieter, die ihr Geld nicht vorwiegend mit Software und Datenhandel verdienen, sondern mit guter Hardware.

Wir wollen hier keine Markennamen nennen.

Muss man auch nicht. Man kann heute wählen zwischen zwei großen Anbietern von Betriebssystemen. Damit entscheide ich mich auch für eine datenschutzsichere oder weniger sichere Umgebung. Dasselbe gilt auch für Apps und ähnliche Angebote – manchmal ist es sicherer, über den Browser als über eine App zuzugreifen.

Wie kann ich wissen, ob die Angaben des Anbieters tatsächlich stimmen?

Zunächst sind das natürlich Aussagen der Hersteller, das ist im IT-Bereich nicht anders als zum Beispiel bei der Autoindustrie. Staatliche Prüfinstanzen oder Genehmigungserfordernisse, die wir zum Beispiel im Automobilbereich haben, den TÜV vor allem, gibt es im Datenschutzbereich leider nicht. Auch so etwas wie die Stiftung Warentest oder andere etablierte zivilgesellschaftliche Institutionen fehlen weitgehend. Der Bund hat zwar die Stiftung Datenschutz gegründet, hat deren Aufgaben und Wachsen aber bedauerlicherweise nicht weiterbetrieben, im Gegenteil. Immerhin gibt es auf gesellschaftlicher Ebene

zum Beispiel den Chaos Computerclub oder bürgerrechtliche Vereinigungen, die Anwendungen, Dienstleistungen et cetera gelegentlich prüfen. Und auf der staatlichen Seite gibt es die Datenschutzaufsichtsbehörden, die das auch tun. Darüber existiert eine gewisse Kontrolle und seit der DSGVO erst recht.

Greifen denn die Kontrollen?

Wir beobachten diesen Mechanismus öfter: Wenn eine rechtliche Anforderung nicht nur formuliert, sondern tatsächlich durchgesetzt und sanktioniert wird, steigt die Rechtsbefolgungsrate der Unternehmen. Denn es wird teuer für sie, wenn sie ein rechtswidriges Produkt oder eine rechtswidrige Dienstleistung anbieten. Und auch Reputationseffekte spielen eine Rolle: Als Facebook bestätigen musste, dass Daten an das britische Unternehmen Cambridge Analytica verkauft und zur Wahlbeeinflussung genutzt wurden, hat das Kenner der Materie nicht überrascht, weil der Datenhandel Facebooks Geschäftsmodell war und ist. Aber die Öffentlichkeit war entsetzt. Darunter leidet Facebook bis heute; es hat sicherlich andere soziale Medien gestärkt.

Das lag wohl daran, dass hier Wahlen beeinflusst wurden. Ansonsten scheint es längst Konsens zu sein, dass man vieles mit seinen Daten bezahlt.

Ja und nein: Natürlich wissen wir alle, dass unsere Daten genutzt werden. Doch die wenigsten können realistisch einschätzen, welche Aussagen damit getroffen werden können. Es geht so weit, dass sich Preise aufgrund der Daten anders berechnen oder meinen Kindern der Zugang zu einem Dienst verweigert wird. Wenn meine Zahlungsbereitschaft oder mein Interesse an einem Produkt bekannt ist, dann werden mir andere, nämlich personalisierte Preise angeboten. Da stellt sich schon die Frage: Wollen wir das als Gesellschaft? Ist das mit einer freien, sozialen und fairen Marktwirtschaft vereinbar?

Und diese Gefahr geht von Facebook, Google und WhatsApp aus?

Sie nennen drei große Akteure, es gibt natürlich noch andere, man denke nur an TikTok aus China. Die Daten werden übrigens auch intern zum Ausbau der eigenen Wettbewerbsposition genutzt. Von Google weiß man, dass Daten aus Suchmaschinenanfragen oder Routenplanern etwa zur Entwicklung selbstfahrender Autos eingesetzt werden. Viele Trainingsdaten für den Einsatz künstlicher Intelligenz braucht Google daher nicht mühsam einzukaufen, sondern kann sie sich selbst beschaffen – und anderen vorenthalten. Forschung und Weiterentwicklung werden also nachhaltig davon geprägt, wer auf welche Daten Zugriff hat. Hinzu kommt eine wachsende Zahl zentral aufgestellter Dienste über Plattformstrukturen. Daten aus Handynutzung, E-Mail-Kontakten und Browser-Nutzung setzen einen Datenfluss in Gang, der wie eine Spinne im Netz Daten abgreift und weitergibt.

Haben wir eine Möglichkeit, uns davor zu schützen? Wir hängen ja alle schon im Spinnennetz drin.

Was immer hilft, ist die Macht in der Masse. Wenn viele ihr Verhalten ändern, verändern sich Märkte, weil sich die Angebote der Nachfrage anpassen. Jeder Nutzer bewirkt etwas, der im Laden fragt: Ist dieses Produkt datenschutzgerecht? Der beim Fernseherkauf nicht nur sagt: »Toll, internetfähig!«, sondern auch fragt: »Wer erfährt, was meine Familie über den Fernseher aus dem Netz hochlädt?«

Wenn ich mich umsehe, habe ich nicht das Gefühl, dass die Menschen wirklich viel Wert darauf legen.

Viele Leute denken: Wenn das alle nutzen, wird das schon nicht so schlimm sein. Das ist das bekannte Fliegenpapierproblem: Die Fliege, die herumwirrt, wird von einer anderen gewarnt: Setz dich nicht dahin! Aber die sagt nur: Da sitzen doch so viele, da ist es also sicher, denn so viele können nicht irren. Können sie eben schon. Schwarmintelligenz ist nicht immer das Beste.

Beispiel WhatsApp: Als Mutter kommt man kaum darum herum, weil viele Elterngruppen über WhatsApp kommunizieren.

Das ist besonders schade, eben weil es datenschutz- und IT-sichere Alternativen gibt. Mein persönlicher Umgang damit ist: Ich sage zu, die Kosten für die sichere Messenger-App zu übernehmen. Zumindest in kleineren, neueren Gruppen, zum Beispiel wenn der Klassenchat, die Sport- oder Firmgruppe erst eingerichtet wird, funktioniert das.

Nutzen Sie auch einen anderen Browser als andere?

Ich verwende Firefox und immer im Private-Browsing-Modus. Als Suchmaschine benutze ich Startpage. Das greift auf Google zu, funktioniert aber ohne Personalisierung und Tracking.

Wie erfahren Sie von datenschutzrechtlich sicheren Angeboten?

Ich nehme meine Umwelt natürlich auch durch diese Brille wahr – Newsletter et cetera halten mich auf dem Laufenden. Und eine meiner studentischen Hilfskräfte recherchiert ständig neue Angebote. Das Ergebnis teile ich dann unter anderem zu Beginn meiner Datenrechtsvorlesung mit.

Haben Sie weitere Tipps für unsere Leser?

Ich mache mich derzeit angesichts der Flut von Videokonferenzformaten sehr für kleine sichere Anbieter wie BigBlue-Button oder WebEx von der Telekom stark. Die Telekom gibt sich ja datenschutzfreundlich, und vor allem kann ich vor deutschen Gerichten klagen und in Deutschland vollstrecken, wenn Zusagen nicht eingehalten werden. Bei anderen Formaten mit Sitz im Ausland, ohne Vermögen in Deutschland, mit Servern in Asien oder Übersee ist das nicht so, und dann sind wir wieder beim Punkt der effektiven Rechtsverfolgung. Wünschen würde man sich vor allem, dass auch hier deutschland- und europaweit investiert und in Zeiten von Corona Kapazitäten hochgefahren werden. Die Goethe-Universität hat das

Grundproblem an sich schon vor Langem erkannt und übliche Voice-over-IP- und Videokonferenzsysteme wie Skype wegen der rechtlichen Probleme (auch im Urheberrecht) untersagt und auf Vidyo vom Deutschen Forschungsnetzwerk umgestellt – trotzdem nutzen wir jetzt andere Tools, weil hier nicht schnell genug hochgefahren wurde. Da darf man sich nicht wundern, wenn die Marktmacht der internationalen Player wächst und damit auch die europäischen Rechtsvorstellungen herunterfallen.

Ist es nicht längst schon zu spät? Gerade die Jüngeren haben offenbar wenig Probleme damit, dass ihre Daten irgendwo landen.

Der Schlüssel ist die Bildungspolitik: Wir brauchen einen frühen integrativen Medienunterricht, sobald Kinder anfangen, diese Medien zu nutzen. Ich darf die Kinder nicht in der ersten Klasse Grundschule an den Computer setzen und ihnen beibringen: »Google das mal!« In der Corona-Krise sind wir mit Macht im digitalen Zeitalter angekommen, aber was wird an den Schulen eingesetzt? Zum Großteil Produkte amerikanischer Marktführer! Warum nutzen wir Video-Tools, von denen wir wissen, dass die Server im Ausland stehen und die Inhalte dort abgegriffen werden? Die Generation der Zehn- bis Zwanzigjährigen lassen wir damit aufwachsen, dass es scheinbar keine Alternativen gibt. Auf keinen Fall geht es an, dass Lehrer Aufgaben über Facebook verbreiten oder eine WhatsApp-Gruppe gründen. Das ist glücklicherweise inzwischen auch gerichtlich entschieden.

Was halten Sie von der Corona-Tracking-App?

Ich halte das – unter den gegebenen Bedingungen – für ein sehr gutes weiteres Tool zur Begleitung der Pandemie. Man hat auf die erheblichen datenschutz- und IT-sicherheitsrechtlichen Bedenken reagiert und agiert sehr transparent; die Menschen erleben, dass nicht an ihnen vorbei entschieden wird, dass sie tatsächlich eine Wahl haben und dass Datennutzung eng beschränkt ist mit

einer präzisen technischen Löschung. Das ist alles sehr erfreulich. Ungeklärt ist aber weiterhin, wie wir sicherstellen, dass die Nutzung freiwillig ist und nicht etwa sozialer Druck aufgebaut wird, indem Arbeitgeber oder Restaurants oder Veranstalter verlangen, die App einzusetzen oder indem Gerichte womöglich eine Mitschuld konstruieren, wenn jemand die App nicht genutzt hat. Darüber darf nicht einmal nachgedacht werden, weil dies die Freiwilligkeit unterläuft.

Haben Sie selbst sich die App heruntergeladen?

Auf mein »Zweithandy« schon, aber ich bin sehr skeptisch, ob die Politik begreift, wie wichtig es ist, die App auch wirklich beschränkt zu halten. Schon werden Begehrlichkeiten der Strafverfolgungsbehörden und anderer Interessenten laut. Wenn diesen nachgegeben wird, ist der enorme Vertrauensgewinn, den man gerade aufgebaut hat, sofort wieder weg. Und schlimmer noch: Dann verlieren die Bürgerinnen und Bürger die Fähigkeit, auf eine Selbstbeschränkung des Staates zu vertrauen.

Das Interview führte Anke Sauter.

● You can read an English translation of this article online at: www.aktuelles.uni-frankfurt.de/forschung-frankfurt-englisch