4. Die Rolle der Plattformanbieter Apple (iOS) und Google (Android) ist kritisch zu diskutieren und über den gesamten Verarbeitungsprozess hinweg zu begleiten. Eine Bluetooth-basierte Corona-Tracing-App ist aus technischen Gründen auf die Kooperation der Plattformanbieter angewiesen, da der Zugriff auf das Bluetooth-Modul der Geräte auf Betriebssystemebene ermöglicht werden muss. Diese Machtposition haben die Plattformanbieter in den vergangenen Wochen genutzt, um gegen zahlreiche Regierungen eine dezentrale und somit datenschutzfreundlichere Architektur zu erzwingen. Damit ist das Datenschutzrisiko, das von den Plattformbetreibern selbst ausgeht, in der öffentlichen Diskussion weitestgehend aus dem Blick geraten. Als Betriebssystemhersteller ist es prinzipiell möglich (und auch realistisch, wie die DSFA zeigt), d… Kontaktinformationen gelang… über Infektionsfälle und Expo… Eine kritische Begleitung der… erfordert daher eine umfassende Sensibilisierung für dieses Problem und die rechtliche Verpflichtung der Unternehmen, sich datenschutzkonform zu verhalten.

Diskussion in gesellschaftlicher Breite

Insbesondere die quelloffene Entwicklung von Server und Apps nebst allen ihren Komponenten – beispielsweise als freie Software – ist eine wesentliche Voraussetzung dafür, dass nicht nur für Datenschutzaufsichtsbehörden die nötige Transparenz bezüglich der Umsetzung der Datenschutz-Grundsätze vorliegt, sondern auch für die Betroffenen und die Öffentlichkeit insgesamt. Diese Datenschutz-Folgenabschätzung zeigt aber auch, dass eine Fokussierung allein auf die Quelloffenheit der Technik die durchaus größeren gesellschaftlichen Implikationen des gesamten Verfahrens verschleiern kann. Nur Datenschutz-Folgenabschätzungen können Derartiges offenlegen und sollten in diesem, aber auch in anderen ähnlich folgenreichen Datenverarbeitungsprojekten veröffentlicht werden, damit sie nicht nur von den Datenschutz-Aufsichtsbehörden, sondern auch in gesellschaftlicher Breite und sozialwissenschaftlicher Tiefe diskutiert werden können.

Anmerkungen

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

…corona-cwa
…-app/cwa-documentation/blob/
…ument.de.md
…n.de/interviews/steinmueller/index.html
4 https://www.fiff.de/presse/dsfa-corona
5 https://de.wikipedia.org/wiki/Funktionale_Differenzierung
6 https://dejure.org/gesetze/DSGVO/35.html
7 https://www.datenschutzzentrum.de/sdm/
8 https://www.fiff.de/presse/dsfa-corona
9 https://de.wikipedia.org/wiki/Funktionale_Differenzierung

Quelle: https://netzpolitik.org/2020/contact-tracing-apps-kritik-an-datenschutzfolgenabschaetzung-fuer-die-corona-warn-app/

Ingo Dachwitz interviewt Kirsten Bock

„Risiken und Maßnahmen nicht ausreichend dargelegt“

Vieles ist gut gelaufen bei der Entwicklung der Corona-Warn-App, doch aus Sicht des Datenschutzes gibt es noch Luft nach oben, findet Kirsten Bock. Im Interview kritisiert sie die Datenschutz-Folgenabschätzung (DSFA) der Anwendung und fordert eine gesetzliche Grundlage, um möglichen Missbrauch zu verhindern.

Noch nicht ausgereift

netzpolitik.org: *Mit dem Start der Corona-Warn-App Mitte Juni wurde auch die Datenschutz-Folgenabschätzung veröffentlicht. Telekom, SAP und Robert-Koch-Institut sind damit einer Forderung der Zivilgesellschaft[1] gefolgt. Was ist Ihr erster Eindruck von dem mehr als hundertseitigen Dokument?*

Kirsten Bock: Erstmal freuen wir uns, dass die DSFA der Corona-Warn-App[2] veröffentlicht wurde. Das ist eine wichtige Entscheidung. Was man aber vorweg schon sagen kann, ist, dass sich das Team offensichtlich zum ersten Mal mit einer Datenschutz-Folgenabschätzung befasst hat und – um es mal positiv zu formulieren – versucht hat, sich dem Ziel zu nähern. Aus meiner Sicht ist das jedoch noch keine ausgereifte DSFA.

netzpolitik.org: *Wo liegt das Problem?*

Kirsten Bock: Dem Anspruch nach ist dies eine verpflichtende DSFA nach Artikel 35 der Datenschutzgrundverordnung. Damit gehen bestimmte methodische Vorgaben einher. Der Artikel schreibt zum Beispiel vor, dass die Prüfung vor dem Start einer Technologie durchzuführen ist und enthält insofern auch eine Vorgabe, wie man Privacy by Design materiell umsetzt. Das ist in diesem Fall ganz offensichtlich nicht passiert.

Die Datenschutz-Folgenabschätzung ist – so wie ich das lese – nachträglich erstellt worden. Das ist eigentlich nicht Sinn und Zweck der Sache. Die Verantwortlichen sehen ein „lebendes Dokument“ und wollen die Folgenabschätzung fortführen. Das ist positiv, aber ein Minimum des Notwendigen für neue, eigenständige Komponenten. Eine DSFA ist eigentlich mit einem klaren Ergebnis abzuschließen und wird danach Gegenstand des Datenschutz-Managementsystems der Verantwortlichen.

netzpolitik.org: *Nun war der Zeitraum für die Entwicklung der Tracing-App aber auch ein sehr kurzer.*

Kirsten Bock: Das stimmt natürlich. Aber es war von Anfang an klar, dass man eine hohe Zahl von Nutzern dafür gewinnen will.

Deshalb wäre es umso wichtiger, dass man nicht einfach drauflos entwickelt. Wenn man so ein Projekt macht, muss man sofort auch ein DSFA-Team an seiner Seite haben, das kontinuierlich das reflektiert, was entwickelt wird.

Nicht nur die App, sondern das gesamte System betrachten

netzpolitik.org: *Sie haben mit dem FIfF schon im April eine Muster-Datenschutz-Folgenabschätzung für eine mögliche Corona-Tracing-App vorgelegt. Als Debattenbeitrag und Anregung, die in der offiziellen DSFA nun auch als eine Grundlage erwähnt wird. Wo sind Unterschiede?*

Kirsten Bock: Was ich erwartet hätte, ist eine Auseinandersetzung nicht nur mit der Corona-App als solcher, sondern mit dem gesamten Verfahren. Dazu gehört etwa auch die Serverinfrastruktur. Die wird in dieser DSFA zwar angesprochen, aber es fehlen genauere Information: Was passiert da eigentlich genau? Was wird geloggt? Wird das gelöscht? Wie lange werden Daten aufbewahrt? Wir finden hierzu unterschiedliche Angaben zum einen im Glossar der DSFA und zum anderen im Haupttext. Es gibt ja unterschiedliche Serverfunktionen für die unterschiedlichen Funktionalitäten der App. Es wäre deshalb zwingend erforderlich, zu beschreiben, was da eigentlich passiert.

netzpolitik.org: *Sie meinen die Übermittlungsserver, über die die Tagesschlüssel der positiv getesteten Personen verteilt werden?*

Kirsten Bock: Genau. Wir haben es hier dann ja letztlich mit Krankheitsinformationen zu tun. Auch wenn die IDs für sich genommen wenig Aussagegehalt haben, hängen sie ja doch immer an der Person beziehungsweise an dem Handy, das sie hochlädt. Wenn ich diesem Server nicht vertraue im Hinblick auf die Verkehrsdaten, kann ich mir diese ganze Diskussion um Pseudonymisierung der Daten eigentlich sparen. Wenn hier Verkehrsdaten nicht von Inhaltsdaten getrennt werden und zusammen im Back-End verbleiben, habe ich ein Problem in der ganzen Architektur.

netzpolitik.org: *Weil die Betreiber der Server über die Metadaten potenziell re-identifizieren könnten, wer die Tagesschlüssel hochlädt, also wer an Covid-19 erkrankt ist?*

Kirsten Bock: Genau.

netzpolitik.org: *Und das wird in dem Dokument nicht dargelegt?*

Kirsten Bock: Die Risiken und Maßnahmen werden meines Erachtens nicht ausreichend dargelegt.

netzpolitik.org: *Benennt die Folgenabschätzung denn zumindest dieses Risiko, dass es vonseiten des Betreibers zumindest potenziell zur Re-Identifikation kommen könnte?*

Kirsten Bock: Nein, und das ist ein weiteres grundsätzliches Problem: Es fehlt in dem Papier eine datenschutzspezifische Risikomodellierung. Das liegt wahrscheinlich daran, dass es einfach keine hinreichende Orientierung an operativem Datenschutz gibt. Aus Datenschutzsicht ist ja nicht jemand Externes Hauptangreifer auf die Rechte und Freiheiten, sondern der Verantwortliche selbst. Deshalb hätte dargelegt werden müssen, wie die Grundsätze aus Artikel 5 DSGVO [Anm. der Red.: Zweckbindung, Datenminimierung, Nachvollziehbarkeit etc.] umgesetzt werden und diese hätten als Risikokriterien herangezogen werden müssen.

Nichtwissen ist keine Option

netzpolitik.org: *Das klingt ein bisschen grundsätzlich. Wir hatten ja eine intensive öffentliche Debatte, an deren Ende die datenschutzfreundlichere Variante umgesetzt wurde. Braucht es da überhaupt noch so eine ausführliche Folgenabschätzung?*

Kirsten Bock: Natürlich ist es ein Erfolg, dass am Ende diese dezentrale Variante ausgewählt wurde. Aber die ausführliche Folgenabschätzung braucht es schon allein deshalb, weil sie gesetzlich vorgeschrieben ist und der Prozess des *Datenschutz durch Technikgestaltung* auch formal begleitet werden soll. Wir wissen wie gesagt nicht genau, was auf dem Server passiert und das kann sich ja auch jederzeit ändern. Wir vertrauen darauf, dass die Serverbetreiber das tun, was sie uns versprechen. Das kann nur nachvollzogen werden, wenn das tatsächlich kontrolliert erfolgt.

Deshalb ist es auch unbedingt notwendig, dass die DSFA öffentlich ist. Wer auf Open Source setzt, sollte immer auch die Datenschutz-Folgenabschätzung veröffentlichen. Damit Ankündigung und Realität miteinander abgeglichen werden können und die Risiken klar auf dem Tisch liegen. Die DSFA bietet begleitende Einordnung und Kontrolle. Das führt uns aber direkt zum nächsten Problem.

netzpolitik.org: *Welches wäre das?*

Kirsten Bock: Die Verantwortlichen ziehen sich in einem sehr relevanten Bereich auf Nichtwissen zurück, das geht für eine Datenschutz-Folgenabschätzung überhaupt nicht. Ich spreche die Prozesse an, die auf Betriebssystemebene bei Google und Apple laufen. Also dieser ganze ENF-Bereich, da heißt es in der Folgenabschätzung: Naja, das läuft ja bei denen und da können wir nur den Informationen vertrauen, die sie uns liefern, aber prüfen können wir das nicht. Das positive ist: Diese Lücke wird deutlich gemacht. Denn das könnte ja auch einfach unter den Tisch fallen. Das Problem ist nur, dass man als Verantwortliche an diesem Punkt nicht stehen bleiben und sagen kann: Ja, tut uns leid, das können wir nicht prüfen.

netzpolitik.org: *Die Verantwortlichen machen hier Sicherheitsbedenken geltend. Wenn bekannt wäre, wie genau das Verfahren bei Apple und Google funktioniert, wäre es angreifbar. Lassen Sie das Argument gelten?*

Kirsten Bock: Nein. Wenn man in Bereiche gerät, in denen Fachleute zu dem Schluss kommen, dass eine öffentliche Darstellung problematisch ist, weil sie neue Risiken birgt, dann muss man eine vertrauenswürdige dritte Person hinzuziehen und das Ganze testen lassen. Da sind wir im Bereich Zertifizierung. Da müssten dann zumindest die Kriterien offengelegt werden, nach denen geprüft wurde. Und dann kann man so eine Prüfung, die nicht öffentlich erfolgt, auch in eine DSFA einbeziehen. Aber man kann sich nicht zurückziehen und sagen: Da vertrauen wir mal den Playern und dabei belassen wir es.

Vertrauen ist gut, ein Gesetz wäre besser

netzpolitik.org: *Wenig überraschend kommen Telekom, SAP und das Robert-Koch-Institut in ihrer Folgenabschätzung insgesamt zu dem Schluss, dass die Risiken beherrschbar sind und dass genug Maßnahmen ergriffen wurden, um sie zu einzudämmen. Bedeutet Ihre Kritik an dem Dokument im Umkehrschluss, dass sie an diesem Ergebnis zweifeln?*

Kirsten Bock: Das große Problem ist, dass die Zusagen, die derzeit gemacht werden, nirgends festgeschrieben sind. Die App ist sehr weit verbreitet und ihre Funktionalität kann mit wenigen Handgriffen verändert werden. Das Robert-Koch-Institut behält sich das ja auch vor. Wir können also nicht sicherstellen, dass der Zustand erhalten bleibt, in dem die App ihre Arbeit rechtskonform erledigt. Man kann die Sicherheit hier outsourcen und sagen: die Zivilgesellschaft wird das schon überprüfen – wir machen so viel wie möglich öffentlich und da gucken dann immer Leute drüber. Das ist der jetzt gewählte Weg und das ist bis zu einem bestimmten Punkt auch gut und vertrauensbildend. Aber natürlich kann die Verantwortliche nicht ihre gesamte Verantwortlichkeit externalisieren. Sondern sie muss eben selbst die DFSA in einem Datenschutz-Managementsystem fortschreiben, das wäre eine Maßnahme.

netzpolitik.org: *In der Muster-Folgenabschätzung haben Sie mit dem FIfF eine andere Maßnahme in den Vordergrund gestellt.*

Kirsten Bock: Richtig, es wäre angezeigt gewesen, dass man die Funktionalität des Systems in einem Gesetz festschreibt. Da müsste dann der Gesetzgeber die Hosen runterlassen und festlegen, zu welchen Zwecken Daten verarbeitet werden. Wenn das Gesetz festschreibt, dass die App in jeder Hinsicht immer freiwillig sein muss, dann kann das eine positive Wirkung haben. Natürlich könnte es aber auch so ausgehen, dass der Gesetzgeber sagt: Wenn du im Krankenhaus arbeitest, dann verlange ich von dir die Installation der App und dann musst du das Ding auch immer bei dir tragen.

netzpolitik.org: *Das heißt, nicht in jedem Fall wäre ein Gesetz die weniger eingriffsintensive Variante.*

Kirsten Bock: Das kommt darauf an. Im Moment ist es ja so, dass die App auf einer Einwilligungslösung basiert. Da kann man sich sehr drüber streiten, ob überhaupt in jedem Fall die Voraussetzungen der freiwilligen Einwilligung gegeben sind. Aber die Einwilligung hat erstmal den Vorteil, dass ich als ein Individuum sagen kann: Das Ding will ich nicht, dem traue ich nicht und ich nutze das nicht. Nur: In einer demokratischen Gesellschaft sollten die wesentlichen Dinge wie der Zweck, Datenkategorien und Rechtsfolgen durch ein Gesetz geregelt werden. In diesem Fall schon allein deshalb, weil so viele Personen betroffen sind.

netzpolitik.org: *Die AutorInnen der offiziellen Datenschutz-Folgen-Abschätzung kommen zu dem Ergebnis, dass es kein Spezialgesetz braucht.*

Kirsten Bock: Das wird sich zeigen. Wir sind zu dem Schluss gekommen, dass es eine gesetzliche Grundlage braucht, weil wir in den allermeisten Fällen die datenschutzrechtliche Voraussetzung für die freiwillige Einwilligung nicht sehen. Viele Menschen installieren die App nicht freiwillig, sondern aus dem Gefühl heraus, sie müssten einen solidarischen Beitrag an die Gesellschaft leisten – was ja auch positiv ist, aber eben nicht freiwillig im datenschutzrechtlichen Sinne.

Das gilt erst Recht, wenn Unternehmen diese App jetzt verpflichtend machen. Wir haben ja bereits von Fällen gehört. Wenn Arbeitgeber plötzlich die Installation verlangen oder Menschen ohne App nicht mehr im lokalen Supermarkt einkaufen können, werden sie sich beschweren. Das wird dann auch nochmal juristisch interessant werden, wenn es Prüfungen und Klagen gibt. Da werden auch die Datenschutzbehörden tätig werden müssen, um Prüfungen vorzunehmen und um die Rechtsfragen zu klären, die sich um die App ranken.

netzpolitik.org: *Vielen Dank für das Gespräch!*

Quelle: https://netzpolitik.org/2020/interview-zu-corona-warn-app-risiken-und-massnahmen-nicht-ausreichend-dargelegt/

Anmerkungen

1 *https://netzpolitik.org/2020/datenschutz-folgenabschaetzung-dsgvo-vertrauen-ist-gut-kontrolle-ist-besser/*
2 *https://www.coronawarn.app/assets/documents/cwa-datenschutz-folgenabschaetzung.pdf*
3 *https://pgp.mit.edu/pks/lookup?op=get&search=0x05550760A5E4E814*

Kirsten Bock und Ingo Dachwitz

Kirsten Bock arbeitet hauptberuflich im Datenschutz. Sie ist Mitglied beim *Forum der InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)* und eine der AutorInnen von dessen *Muster-Datenschutz-Folgenabschätzung (DSFA)* für Tracing-Apps.

Ingo Dachwitz ist Medien- und Kommunikationswissenschaftler, Redakteur bei *netzpolitik.org* und Mitglied beim Verein *Digitale Gesellschaft*. Er schreibt und spricht über Datenpolitik, Überwachungskapitalismus und den digitalen Strukturwandel der Öffentlichkeit. Ingo Dachwitz gibt Workshops für junge und ältere Menschen in digitaler Selbstverteidigung und lehrt manchmal an Universitäten zur politischen Ökonomie digitaler Medien. Gelegentlich moderiert er auch Veranstaltungen und Diskussionen, etwa auf der *re:publica* oder beim *Netzpolitischen Abend* in Berlin. Ingo ist Mitglied der sozialethischen Kammer der EKD und berät kirchliche Organisationen bei der digitalen Transformation. Kontakt: Ingo ist per Mail an *ingo | ett | netzpolitik.org* (PGP-Key[3]) erreichbar und als *@roofjoke* auf Twitter unterwegs.