NETZPOLITIK.ORG

Ingo Dachwitz

Datenschutz-Folgenabschätzungen: Vertrauen ist gut, Kontrolle ist besser

Neue Technologien wie Corona-Tracing-Apps rufen Misstrauen hervor. Ein bislang unterschätztes Instrument der Datenschutzgrundverordnung könnte mehr Transparenz und damit Vertrauen schaffen.

Seit Wochen diskutiert Deutschland über Corona-Apps[1]. Die Anwendungen sollen das Nachverfolgen von Infektionsketten erleichtern und dabei helfen, die Kontaktpersonen von Covid19-Erkrankten zu informieren. Doch die Verunsicherung ist groß: Wie weit lässt man den Staat mit den Programmen auf das eigene Smartphone? Wer garantiert für die Sicherheit der sensiblen Informationen über Gesundheitszustand und soziale Netzwerke? Was, wenn Regierungen der Versuchung nicht widerstehen können und doch mehr Informationen über BürgerInnen sammeln wollen als angekündigt?

„Wer in dieser Zeit eine Corona-App auf den Markt bringt, muss Transparenz schaffen", fordert deshalb Benjamin Bergemann vom Verein Digitale Gesellschaft. Der Politikwissenschaftler gehört zu einer Reihe von AktivistInnen, die in der Krise auf das Potenzial eines neuen und zugleich alten Datenschutzinstruments hinweisen. Es könnte helfen, die Vertrauensfrage zu beantworten: die Datenschutz-Folgenabschätzung (DSFA).

Was sperrig klingt, ist im Grunde einfach erklärt: Wer in der EU Datenverarbeitungen plant, die mit einem potenziell hohen Risiko für Grundrechte und Freiheiten einhergehen, ist nach der Datenschutzgrundverordnung (DSGVO) verpflichtet[2], vorab eine umfassende Selbstkontrolle durchführen. In Rahmen dieser Folgenabschätzung müssen Unternehmen, Vereine und staatliche Stellen systematisch auflisten, welche Verarbeitungsprozesse sie für die persönlichen Daten zu welchem Zweck planen. Außerdem müssen sie Risiken für die Betroffenen analysieren und Maßnahmen beschreiben, mit denen sie diese Risiken minimieren.

Transparenz ermöglicht Kontrolle, Kontrolle schafft Vertrauen

Die Folgenabschätzung ist Teil des sogenannten Risiko-basierten Ansatzes der DSGVO. Sie soll dem sperrigen Gesetz eine gewisse Flexibilität ermöglichen: DatenverarbeiterInnen müssen sich vorab selbst intensiv Gedanken machen und eigenständig Schutzmaßnahmen entwickeln. Wenn sie zu dem Schluss kommen, dass das Risiko trotzdem hoch bleibt, müssen sie die Aufsichtsbehörden konsultieren[3].

Eine Veröffentlichung der DSFA allerdings sieht die Datenschutzgrundverordnung nicht vor. Benjamin Bergemann hat deshalb beim Robert Koch-Institut eine Anfrage nach dem Informationsfreiheitsgesetz (IFG)[4] gestellt, um die Folgenabschätzung der Datenspende-App aus den Aktenordnern der Infektionsbehörde zu befreien. „Es gibt ein hohes öffentliches Interesse daran, nachzuvollziehen, dass die App datenschutzfreundlich entwickelt wurde. Die vom Robert Koch-Institut veröffentlichten Datenschutzinformationen erfüllen diesen Anspruch nicht", so Bergemann. Auch der Chaos Computer Club kritisierte die mangelhafte Transparenz[5] der Anwendung.

Einen anderen Weg ist das Forum der InformatikerInnen für Frieden und gesellschaftliche Verantwortung gegangen. Da die Corona-Tracing-Apps in Deutschland selbst noch nicht fertiggestellt sind, haben die DatenschützerInnen des Vereins einfach selbst eine Folgenabschätzung erstellt[6] – ein Debattenbeitrag über die gesellschaftlichen Risiken dieser Technologien, der den MacherInnen der App gleichzeitig als konkrete Anregung dienen soll.

In dem gut hundert Seiten starken Dokument kamen die ExpertInnen schon sehr früh in der Debatte zu dem Schluss, dass es aus Sicht des Datenschutzes erhebliche Unterschiede mit sich bringt, ob ein dezentrales oder ein (teil-)zentralisiertes Modell[7] umgesetzt wird. Doch auch beim dezentralen Modell stellt die Folgenabschätzung erhebliche Risiken fest, für die der Verein jeweils konkrete Schutzmaßnahmen vorschlägt.

Licht in die Black Box bringen

Moderne Informations- und Kommunikationstechnologien sind für die wenigsten Menschen gänzlich durchschaubar. Eigentlich würde man erwarten, dass die allgegenwärtigen Datenschutzerklärungen hier einen Beitrag leisten würden. Ihre Veröffentlichung ist nach der DSGVO zwar verpflichtend, doch weil sie meist nicht zur Aufklärung, sondern zur rechtlichen Absicherung verfasst werden, erfüllen sie diesen Anspruch nur selten.

Gerade bei komplexen datenbasierten Systemen, die heute oft die Label Big Data oder Künstliche Intelligenz tragen, könnte die DSFA deshalb eine Möglichkeit sein, gesellschaftliche Auswirkungen überhaupt erst diskutierbar zu machen. „Viele solcher

Systeme operieren als ‚Black Boxes' – undurchsichtige Software-Werkzeuge, die sich aussagekräftiger Überprüfung und Verantwortlichkeit entziehen", schrieben Kate Crawford und Meridith Whitthaker 2018 in einem Bericht über automatisierte Entscheidungssysteme[8]. Die Forscherinnen des US-amerikanischen Think Tanks AI NOW brachten deshalb *Algorithmic Impact Assesments* ins Spiel. Folgenabschätzungen, die dem Privacy Impact Assessment der DSGVO nicht unähnlich sind.

Tatsächlich steht die DSFA in der Tradition der parlamentarischen Technik-Folgenabschätzung, bei der es nicht nur um einzelne Datenverarbeitungen, sondern um die Diskussion gesellschaftlicher Konsequenzen geht. Vor dem Hintergrund der Debatte um die kommerzielle Nutzung von Atomenergie habe sich dieses Instrument seit den 70er Jahren etabliert, um „die Chancen und Risiken der Technik für die Gesellschaft sowie deren Akzeptanz […] unter einem ganzheitlichen und damit interdisziplinären Winkel" zu erforschen, erklärt das Forschungsprojekt *Forum Privatheit* in einem White Paper[9].

Bereits seit Ende 70er Jahre sei dieses Element auch schon in einigen deutschen Datenschutzgesetzen angelegt gewesen, wurde jedoch nie wirklich entfaltet. Erst mit der Datenschutzgrundverordnung wird der alten Idee neues Leben eingehaucht.

Als führe man den TÜV in der eigenen Garage durch

Ein Gespräch mit Stefan Brink zeigt: Überall angekommen ist das noch nicht. Doch die Zahl der DatenverarbeiterInnen, die selbstständig eine DSFA durchführen, nehme kontinuierlich zu, berichtet der Landesdatenschutzbeauftragte von Baden-Württemberg. Wann das notwendig ist, definiert die DSGVO nicht genau, Orietierung geben Handreichungen der Aufsichtsbehörden[10]. Im Vergleich zu den Vorabkontrollen, die das alte Bundesdatenschutzgesetz vorgesehen hatte, habe sich die Zahl der Folgenabschätzungen jedenfalls mehr als verdoppelt, so Brink.

Bislang behalten DatenverarbeiterInnen die Dokumente jedoch lieber für sich. Eine Praxis, die auch Lea Pfau vom Transparenzportal *Frag den Staat* kritisiert. Es sei nur schwer vorstellbar, dass Verantwortliche in der Selbstprüfung jemals zu dem Ergebnis kämen, dass sie die Aufsichtsbehörde konsultieren müssen, weil sie das Risiko nicht in den Griff bekommen: „Das wäre ungefähr so, als würde man den TÜV für sein Auto in der eigenen Garage selbst durchführen."

Eine Veröffentlichung der Abschätzung erfülle jedoch nicht nur eine Kontrollfunktion. Die Transparenzmaßnahme könne zudem die Qualität des Datenschutzes verbessern, weil es einen Feedback-Kanal gebe. Das gelte besonders im Fall der Corona-Apps: „Das öffentliche Interesse geht hier einher mit einem erheblichen Maß an vorhandener Expertise", so Pfau.

„Wer nach außen demonstrieren will, dass man Datenschutz kapiert hat, hat mit Veröffentlichung der Folgenabschätzung ein ideales Werbemittel, um die eigene Seriosität zu demonstrieren", findet auch Stefan Brink, der in Baden-Württemberg nicht nur Beauftragter für Datenschutz, sondern auch für Informationsfreiheit ist. „Anstatt sich wegzuducken, kann man sich demonstrativ offen zeigen. Nach dem Motto: Prüft uns, macht Verbesserungsvorschläge." Brink bestätigt derweil, dass es so gut wie nie vorkomme, dass Unternehmen seine Behörde in Folge der internen Folgenabschätzung konsultieren würden.

Security by Obscurity ist eine schlechte Ausrede

Zumindest die Datenschutz-Folgenabschätzung von Behörden seien in der Regel IFG-pflichtig, bestätigt Stefan Brink. Dass das in der Praxis durchaus anders aussehen kann, zeigt ein Fall aus der Redaktion von netzpolitik.org: Als Kollegin Anna Biselli beim Bundesamt für Migration und Flüchtlinge per IFG die Datenschutz-Folgenabschätzungen von IT-Assistenzsystemen[11] anfragte, mit der etwa die Herkunft von AsylbewerberInnen plausibilisiert werden soll, wurde sie zunächst fast ein ganzes Jahr hingehalten. Am Ende wurde die Anfrage abgelehnt, da die Bekanntgabe des Inhalts der Folgenabschätzung die öffentliche Sicherheit gefährden könne. Dritte könnten mit ihr „mögliche Sicherheitslücken der Datenverarbeitung" aufspüren und ausnutzen.

Dieses Argument bekomme er öfter zu hören, sagt Datenschutz-Aktivist Benjamin Bergemann. Doch davon solle man sich nicht blenden lassen: „Wer auf *Security by Obscurity* setzt, hat ohnehin ein Problem." IT-Sicherheitsarchitekturen sollten nicht davon abhängen, dass sie undurchschaubar seien. Allerdings könne man über die Detailtiefe der Informationen einer veröffentlichten DSFA diskutieren, da hier nicht der einzelne Verarbeitungsvorgang, sondern der Grundrechtsschutz insgesamt im Vordergrund stehe.

Diese Sichtweise unterstützt auch die Rechtsanwältin Nina Diercks. Sie berät regelmäßig Unternehmen in Datenschutzfragen und auch bei der Erstellung von DSFA. Da die Folgen-

Ingo Dachwitz

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 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[14]) erreichbar und als *@roofjoke* auf Twitter unterwegs.

abschätzung ohnehin in vielen Fällen vorgenommen werden müsse, sei der Weg zur Veröffentlichung nicht mehr weit. Notfalls könnten Verantwortliche die Folgenabschätzung um sicherheitsrelevante Aspekte bereinigen und eine leicht abgespeckte Variante veröffentlichen, so Diercks.

Österreich macht es vor

Dass das Robert Koch-Institut die Folgenabschätzung der Datenspende-App nicht proaktiv veröffentliche, sei wenig vertrauensbildend, findet Diercks. Auch Bergemann sieht die Behörden bei Corona-Apps in einer Bringschuld. „Das sind Hochrisiko-Technologien, die flächendeckend eingesetzt werden sollen. Da muss der Staat gegenüber den Bürgern nachweisen, dass sie grundrechtskonform funktionieren."

Folgenabschätzungen seien kein Allheilmittel, doch sie würden Technologien und ihre Folgen überhaupt erst diskutierbar machen – „eine Voraussetzung dafür, dass wir sie gesellschaftlich kontrollieren können." Inzwischen fordert auch der Europäische Datenschutzausschuss[12], also das Gremium aller nationalen Datenschutzaufsichtsbehörden der EU, die Veröffentlichung der Folgenabschätzungen für Tracing-Apps.

Wie das konkret aussehen kann, demonstriert in Österreich das Rote Kreuz. Schon früh hatte die Organisation zusammen mit der Beratungsfirma Accenture in der Alpenrepublik die „Stopp Corona"-App an den Start gebracht. Mitte April wurde die gut 100 Seiten starke Folgenabschätzung veröffentlicht. Mehrere NGOs konnten zudem den (inzwischen ebenfalls veröffentlichten) Source Code einsehen und haben die Anwendung auf dieser Basis geprüft[13].

Ihr Fazit: Es gibt Verbesserungsvorschläge, aber alles in allem ist die Anwendung sicher und datenschutzfreundlich. Wer dem Urteil der ExpertInnen nicht traut, kann sich nun immerhin selbst ein Bild machen. Denn Vertrauen ist gut – Kontrolle ist besser.

Quelle: https://netzpolitik.org/2020/datenschutz-folgen-abschaetzung-dsgvo-vertrauen-ist-gut-kontrolle-ist-besser/

Anmerkungen

1 *https://netzpolitik.org/2020/faq-corona-apps-die-wichtigsten-fragen-und-antworten-zur-digitalen-kontaktverfolgung-contact-tracing-covid19-pepppt-dp3t/*
2 *https://dsgvo-gesetz.de/art-35-dsgvo/*
3 *https://dsgvo-gesetz.de/art-36-dsgvo/*
4 *https://fragdenstaat.de/anfrage/datenschutz-folgenabschatzung-zur-corona-datenspende-app/*
5 *https://netzpolitik.org/2020/die-datenspende-app-braucht-mehr-transparenz/*
6 *https://www.fiff.de/presse/dsfa-corona/*
7 *https://netzpolitik.org/2020/welche-technologie-bietet-den-besseren-datenschutz/*
8 *https://ainowinstitute.org/aiareport2018.pdf*
9 *https://www.forum-privatheit.de/download/datenschutz-folgenabschaetzung-3-auflage-2017/*
10 *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236*
11 *https://fragdenstaat.de/anfrage/datenschutz-folgeabschatzungen/*
12 *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf*
13 *https://epicenter.works/sites/default/files/analyse_stopp_corona_app_v1.0.pdf*
14 *https://pgp.mit.edu/pks/lookup?op=get&search=0x05550760A5E4E814*

Tomas Rudl

Die Krise als Hebel für Überwachung und Kontrolle

Weltweit bauen demokratische Staaten Grundrechte ab, um gegen das Coronavirus vorzugehen. Manchen Regierungen scheint das aber nur ein vordergründiges An… …hmen zur Dauereinrichtung werden – und zum Schuss ins eigene…

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

Ein ausgeschaltetes Parlament, I… …n Israel: Dort setzt die Regierung des Premiers Benjamin Netanyahu höchst invasive Techniken ein, die das Land sonst im Anti-Terror-Kampf nutzt[3]. Dem Inlandsgeheimdienst ist nun unter anderem erlaubt[4], sämtliche Handys des Landes zu tracken, ohne die Daten zuvor zu anonymisieren[5]. Das soll dazu dienen, die Einhaltung der Quarantäne zu überprüfen und gegebenenfalls Infektionsketten nachzuverfolgen.

Verbreiten von „Falschnachrichten" oder für Verstöße gegen das Ausgehverbot: So weit wie das von Viktor Orbán regierte Ungarn ist bislang noch kein EU-Land gegangen, um die Coronakrise einzudämmen. Sollte das Parlament dem Gesetzentwurf nächste Woche mit der notwendigen Zweidrittelmehrheit zustimmen – wovon Beobachter des Landes ausgehen[1] –, dann hätte Ungarn bis auf Weiteres sein demokratisches und schon länger humpelndes Experiment beendet.

In aller Welt versuchen derzeit die Regierungen[2], schnell die richtige Antwort auf die Pandemie zu finden. Manche, darunter Orbáns rechte Fidesz-Partei, scheinen eher die Gunst der Stunde zu nutzen, um ihre Macht abzusichern und ihre Kritiker zum Verstummen zu bringen, als mit demokratischen Mitteln die aktuelle Gesundheitskrise in den Griff zu bekommen.

1. Staaten könnten bleibende Fakten schaffen

Solche Meldungen lassen vielerorts die Alarmglocken schrillen. „Ich befürchte, in den nächsten Wochen und Monaten wird ungefähr jede vorstellbare digitale Überwachungsmaßnahme ins Spiel gebracht werden", sagt der Überwachungsexperte Wolfie