

Freiheit gegen Daten – Pandemiebekämpfung per App

Die App Luca zur Kontaktnachverfolgung ist in aller Munde. Sie ist aber nur ein prominentes Beispiel von vielen. Was ist von solchen Anwendungen generell und Luca insbesondere zu halten? Luca ist umstritten. Aber was bedeutet das? Aktuell äußert sich zumindest der Chaos Computer Club kritisch.¹ Andere finden das Angebot insgesamt in Ordnung. Soll man Luca nun nutzen, obwohl die App noch in der Kritik steht? Muss man sie aufgrund der Anordnungen der Corona-Verordnungen der Länder sogar unter Umständen nutzen, weil das Pandemierecht den Datenschutz verdrängt? Wieviel Abstriche von der Perfektion kann man machen und was sind generell datenschutzrechtliche Fallstricke bei Kontaktverfolgungs-Apps und welche Alternativen gibt es zu Luca?

„Liebe Klasse 10. Herr Lehrer X ist positiv auf Corona getestet. Alle die bei ihm Unterricht hatten, warten bitte auf Post vom Gesundheitsamt. Viele Grüße. Die Schulleitung. Solche Mails zur Kontaktmeldung sind an der Tagesordnung. Sie sind datenschutzrechtlich problematisch, denn man kann wesentlich datenschonender und effizienter auf Erstkontakte mit Covid-Infizierten hinweisen.

Zum Beispiel mit Hilfe von „Luca“. Das ist eine App zur Kontaktnachverfolgung in der COVID-19-Pandemie. Per Smartphone kann man in Einkaufsläden, Geschäften, Gaststätten etc. einen QR-Code des besuchten Ortes scannen und speichern. Stellt sich heraus, dass man mit einer mit Covid-19 infizierten Person zeitgleich vor Ort war, meldet das die App. Damit die Kontaktverfolgung Sinn macht, können Gesundheitsämter direkt auf die Daten zugreifen und so den Kontakt verfolgen.

Welche Vorteile hat die App?

Die Vorteile der App liegen auf der Hand. Der Anbieter verspricht „schnelle und lückenlose Kontakt-rückverfolgung“ bei einfacher Nutzung durch das Scannen des QR-Codes. Hohe Akzeptanz soll Anreize zur Nutzung der App geben, die überregional und flächendeckend funktioniert, so dass Kontakte umfassender nachvollzogen werden können.

Wie lautet die Kritik an der App?

Die App ist trotz der Vorteile, die sie bietet, aufgrund verschiedener Aspekte in die Kritik geraten.

Unsicher

Ein Vorwurf lautet **mangelnde Sicherheit**. Jan Böhmermann hat ein Foto mit dem QR-Code des Osnabrücker Zoos getwittert und dazu aufgerufen, diesen vom Foto zu scannen und sich mit Fake-Profilen dort anzumelden. Das funktionierte. Am Ende waren über hundert Nutzer – viele unter falschem Namen – im Zoo „eingelogg“t. Das Problem ist nicht nur, dass der Login auch mit abfoto-

¹ <https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse>

grafiertem QR-Code möglich ist. Eine Schwäche der App liegt auch darin, dass nur die Einrichtung als Ganze erfasst wird, aber nicht – wie bei der „Corona-Warn-App“ – nach Kontakten in der Nähe differenziert wird. Wenn das Gelände groß ist, macht die Kontaktverfolgung wenig Sinn, weil eine tatsächliche Nachverfolgung unmöglich ist. Im Gegenteil: Die Regel wird dann Verwirrung über häufigen blinden Alarm sein.

Hinzu kommt eine IT-Panne der App, über die derzeit unter dem Begriff LucaTrack² berichtet wird. Neben einer Nutzung über das Smartphone bietet Luca eine Schlüsselanhänger-Funktion an, bei der sich Nutzer analog am jeweiligen Standort mit einem eigenen QR-Code einloggen können. Das Problem: Bloß über ein Foto des Schlüsselanhängers bzw. dieses QR-Codes lässt sich mit wenigen Schritten die Besuchs-Historie des Nutzers auslesen. Betroffen sind wohl rund 100.000 Schlüsselanhänger. Ein Sicherheitsupdate, mit dem sichergestellt wird, dass der QR-Code des Schlüsselanhängers nur für den Check-In, nicht aber auch den Zugriff auf die Daten taugt, muss her.³

Zentrale Datenhaltung

Ein weiterer Kritikpunkt ist – ebenfalls in Abgrenzung zur **dezentral** funktionierenden „Corona-Warn-App“ die Speicherung sensibler Daten auf einem zentralen Server.⁴ Die Gefahr unbefugter Kenntnisnahme ist groß, weil Gesundheitsämter, die auf die Datenbank zuzugreifen, für den Zugriff auf die gesamte Datenbank mit sensiblen Gesundheitsdaten stets denselben Schlüssel benutzen.

Keine zentrale Schnittstelle

Weil die Luca-App zudem nicht per sog. „**Gateway-Lösung**“ allen Gesundheitsämtern eine zentrale Schnittstelle anbietet, um damit auf die Daten unterschiedlicher Kontaktnachverfolgungs-Apps zuzugreifen, sondern auf Exklusivität setzt, verhindert sie die Bündelung von Informationen.

Nutzung mit Klarnamen?

Auch die Frage der pseudonymen Nutzung ist komplex. Laut Eigenerklärung auf der Homepage des Anbieters soll die Nutzung von Luca sogar anonym möglich sein. Das dürfte aber datenschutzrechtlich fragwürdig sein, auch wenn es Mechanismen zum Identitätsschutz der Nutzer gibt. Es spricht viel dafür, dass man wenn überhaupt von einer Pseudonymisierung sprechen kann. Jedenfalls solange der Quellcode nicht öffentlich ist, lässt sich die Frage, nach einer Pseudonymisierung oder gar Anonymisierung noch nicht sicher prüfen. Nach den Nutzungsbedingungen von Luca muss der Nutzer allerdings richtige Angaben machen. Gleichzeitig betont der Anbieter, dass er selbst nicht in der Lage ist, die Richtigkeit der Angaben zu überprüfen. Im Unterschied zur „Corona-Warn-App“, die auf Klarnamen verzichtet, drohen somit sowohl bei unzureichender Datensicherheit als auch bei einer Klarnamenpflicht mit Blick auf unberechtigte Zugriffe Risiken für Nutzer.

² <http://lucatrack.de/LucaTrack%20Pressebeschreibung.pdf>

³ <http://lucatrack.de/LucaTrack%20Pressebeschreibung.pdf>

⁴ https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/datenschutz/dsk_stellungnahmen/DSK-Stellungnahme_20210326_final.pdf

Quellcode zunächst nicht offen gelegt

Der Quellcode von Luca ist zwischenzeitlich offengelegt.⁵ Datenschützer legen darauf besonderen Wert. Unternehmen wollen demgegenüber ihre geldwerten Geschäftsgeheimnisse wahren. Beide Positionen beißen sich. Sie sind jeweils verständlich und berechtigt. Im Ergebnis kann man den Anbieter nicht auf Transparenz verpflichten. Faktisch dürfte es die Akzeptanz der Anwendung steigern, dass ihre technische Funktionsweise offen gelegt ist.

Wo liegen die datenschutzrechtlichen Fallstricke von Kontakterfassungs-Apps?

Das datenschutzrechtliche Pflichtprogramm für Kontakterfassungs-Apps ist neben ihrer Eignung zur Pandemiebekämpfung im konkreten Anwendungsfall insbesondere die Freiwilligkeit ihrer Nutzung. Der Tausch Freiheit gegen Gesundheitsdaten verlangt zudem eine eindeutige Bestimmung der Verwendungszwecke der erhobenen Daten. Denn die Sorge vor Missbrauch der Daten und vor Verhaltenssteuerung sitzt in Deutschland traditionell tief. Die Zwecke sollten möglichst gesetzlich festgelegt werden. Die Entscheidung für eine zentrale Lösung bei der Datenhaltung will gut überlegt sein.

Treuhänder für zentrale Datenhaltung

Dass der Anbieter einer App ein geeigneter Datentreuhänder ist, darf man bezweifeln. Eine zentrale Schlüsselverwaltung für den Zugang zur Datenbank der Luca-App ist dennoch essentiell. Unverzichtbar sind zudem Transparenz und hinreichende Information über die Zwecke der Datenverarbeitungen und deren gesetzlichen Rahmen. Eine starke Verschlüsselung ist ebenso wichtig wie Schutzmaßnahmen zur Gewährleistung der Datensicherheit.

Datenschutz ist auch im Detail wichtig

Speicherdauer und Löschkonzepte müssen ebenso stimmen, wie die Dokumentation der Datenverarbeitung. Vertrauen schafft auch eine zeitliche Befristung von Maßnahmen. In diese Richtung gehen Anregungen und Kritik der Konferenz der deutschen Datenschutzbeauftragten, die sich intensiv mit Luca befasst haben.⁶ Eine sog. Datenschutz-Folgenabschätzung zur Abschätzung der Risiken der Anwendung ist unabhängig von ihrer rechtlichen Erforderlichkeit⁷ für die Akzeptanz der Anwendung essentiell. Dass der Quellcode offen gelegt wurde, ist ein wichtiger Schritt in Richtung Transparenz.⁸

Was sind Alternativen?

Luca ist die hippste Lösung und von Smudo beworben. Wenn die genannten Kritikpunkte und zudem stört, dass das Erlös-bzw. Finanzierungsmodell der App aktuell nicht bekannt ist, kann auf Alternativen warten.

5 <https://www.gmx.net/magazine/digital/macher-luca-app-stellen-programmcode-komplett-35722056>

6 https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/datenschutz/dsk_stellungnahmen/DSK-Stellungnahme_20210326_final.pdf

7 Dazu <https://www.heise.de/hintergrund/Auslegungssache-Der-Datenschutz-Podcast-des-c-t-Magazins-5069656.html>.

8 <https://www.gmx.net/magazine/digital/macher-luca-app-stellen-programmcode-komplett-35722056>

Die datenschutzfreundlichste Lösung

Eine datenschutzfreundliche Alternative zur Luca-App ist das Konzept von CrowdNotifier.⁹ Die Anwendung setzt zwar wie die Luca-App auf das Einchecken per QR-Code an einem bestimmten Ort, ist aber auch auf Zusammenkünfte anwendbar und setzt datenschutzrechtliche Vorgaben durch eine entsprechende technische Ausgestaltung um. Daten der Nutzer werden dezentral gespeichert. Dabei werden im Sinne der Datensparsamkeit keine Daten von Nutzern verarbeitet, sondern beim Check-In wird nur eine verschlüsselte ID für Nutzer erstellt. Eine Angabe persönlicher Daten ist nicht erforderlich. Der technische Kniff: Die App arbeitet letztlich mit zwei verschiedenen QR-Codes, die für sich keine Informationen enthalten und erst bei einem Zusammenfügen im Infektionsfall eine Warnung von Besuchern, die sich an einem bestimmten Ort aufgehalten haben, ermöglichen. Das System nutzt die App NotifyMe¹⁰.

Die standardisierten Lösungen

Um zu verhindern, dass sich der Konkurrenzkampf zwischen verschiedenen Anbietern zum Nachteil der Pandemiebekämpfung auswirkt, wirbt die Initiative „Wir für Digitalisierung“ für eine Standardisierung der Systeme, um sicherzustellen, dass Gesundheitsämter über eine einheitliche Schnittstelle auf Kontaktdaten zugreifen können.¹¹ Ein gemeinsames Gesundheitsamt-Portal verschiedener Anbieter von Kontaktnachverfolgungs-Apps soll so im Sinne einer Plattform den Zugang zu einer Vielzahl von Kontaktdaten ermöglichen. Einen Anschluss an ein derartiges Netzwerk hat die Luca-App bislang verweigert und setzt demgegenüber auf Exklusivität. Der Initiative gehören etwa Recover, bomocha, iStaysafe und viele andere Kontakterfassungs-Dienste an.

Das Maß der Dinge (Corona-Warn-App)

Mit Blick auf den Datenschutz bleibt das Maß der Dinge die dezentrale Corona-Warn-App des RKI. Um den Mehrwert der App zu steigern, wurde die App um ein Presence Tracing erweitert werden, bei dem Nutzer der App mittels QR-Code in Restaurants, Einkaufsläden etc. einchecken können und die Kontaktnachverfolgung somit auch auf diesem Wege erfolgen kann. Allerdings werden auch beim Check-In keine persönlichen Daten verarbeitet. Eine Warnung der Nutzer im Infektionsfall erfolgt nur innerhalb der App, eine Übertragung der Check-In-Daten an das Gesundheitsamt findet nicht statt.¹² Ein Vorteil: Die neue Funktion der Corona-Warn-App kann auch die QR-Codes der Luca-App erkennen und ist somit breit einsetzbar. In weiteren Updates sollen in Zukunft auch Ergebnisse von Schnelltests über die App verwaltet werden können, so dass die Corona-Warn-App längerfristig als digitaler Impfpass dienen soll.¹³

9 <https://github.com/CrowdNotifier/documents/blob/main/CrowdNotifier%20-%20White%20Paper.pdf>

10 <https://notify-me.ch/>

11 <https://www.wirfuerdigitalisierung.de/>

12 https://www.chip.de/news/Corona-Warn-App-2.0-Neue-Version-kommt-mit-Check-in-Funktion_183370693.html

13 <https://www.spiegel.de/netzwelt/apps/corona-warn-app-erhaelt-wichtige-neue-funktion-a-663dde81-b57e-4c6a-85e1-2367d1894e1f>

Pandemierecht verlangt personalisierte Kontakterfassung

Aufgrund der technischen und datenschutzrechtlichen Schwachstellen der Luca-App rät etwa der CCC derzeit nicht nur von der Nutzung ab, sondern fordert gar ein Moratorium der gesamten App.¹⁴ Manche Länder empfehlen demgegenüber in ihren Corona-Landesverordnungen ausdrücklich die Nutzung der Luca-App, so etwa Mecklenburg-Vorpommern (vgl. §§ 13a und b Corona-LVO M-V). Das dürfte aus vergabe- und wettbewerbsrechtlichen Gründen schon zu weit gehen. Die Verordnungen anderer Länder wiederum, so zum Beispiel Baden-Württemberg (vgl. § 6 Abs. 4 CoronaVO BaWü), ordnen die Notwendigkeit einer personalisierten Kontaktnachverfolgung an und erklären damit z.B. die Corona-Warn-App faktisch für nicht einsetzbar. Da auch in der analogen Welt zur Kontaktnachverfolgung letztlich eine Klarnamenpflicht besteht, ist im digitalen Raum ein Recht auf Anonymität schwer begründbar. Zumal die DS-GVO die analoge und die digitale Kontakterfassung unter der Voraussetzung der Speicherung der Daten in einem Dateisystem gleichbehandelt.

Sollte man die Luca-App benutzen?

Insgesamt werden viele Probleme aufgeworfen aber keine Lösung angeboten und auch die entscheidende Frage nicht beantwortet. Sie lautet auf den Punkt gebracht: Ist es nicht besser, datenschutzrechtliche Detailfragen zugunsten der Pandemiebekämpfung zurückzustellen? Luca erfüllt die datenschutzrechtlichen Anforderungen etwa im Vergleich zur „Corona-Warn-App“ weniger gut. Sicherheitslücken müssen schnell behoben werden. Sie ist aber auch keine Datenschleuder. Ihre Stärke liegt vielleicht darin nicht perfekt, aber dafür einsatzfähig zu sein. Sie steht für einen Ansatz Probleme mit dem Mut zum kalkulierbaren Restrisiko anzugehen, während die „Corona-Warn-App“ bei aller Perfektion und Vorsicht faktisch wirkungslos zum Millionengrab von Steuergeldern verkommt.

Die konsequente Fortentwicklung der Kontakterfassung auch bei der „Corona-Warn-App“ ist ein wichtiger und überfälliger Schritt. Bis die perfekten Möglichkeiten der Digitalisierung hier ausgeschöpft sind, sollte jeder der das möchte, Alternativen nutzen. Dafür kommt grundsätzlich jede Anwendung in Betracht, die unter dem Strich verantwortbar ist und für die sich eine Mehrheit finden muss. Misst man die Datenschutzrisiken von Luca an den Risiken, die alle Welt im Ergebnis in vielen anderen Fällen bedenkenlos eingeht, indem zahllose Daten einschließlich Gesundheitsdaten in die Trichter von Sozialen Netzwerken und Suchmaschinen eingespeist werden, dann steht die Aufregung über Luca dazu in keinem angemessenen Verhältnis. Wer sich der hier beschriebenen Risiken bewusst ist, ist so wie es aussieht kein Hasardeur, wenn er auf dieser Basis Daten gegen Freiheit tauscht, bevor die Pandemie vorbei ist.

¹⁴ <https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse>



DataAgenda

ist das Informationsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet Videos, News, Whitepaper und Seminartipps rund um den Datenschutz.

Datakontext

ist einer der führenden Fachinformationsdienstleister in den Bereichen Datenschutz und IT-Sicherheit und bietet Kompetenz aus einer Hand: Fachbücher, Fachzeitschriften und Seminare, Zertifizierung und Beratung.



Autoren

Prof. Dr. Rolf Schwartmann

Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Leiter der Kölner Forschungsstelle für Medienrecht (TH Köln) und Mitglied der Datenethikkommission.



Dr. Tobias Jacquemain, LL.M.

Mitglied der Geschäftsführung der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

