CORONA-App:
Was heißt hier „anonym“? – Eine Begriffsklärung und ein Plädoyer.

Von Karin Schuler

Alle Welt, so scheint es, beschäftigt sich derzeit mit den Möglichkeiten und der Gestaltung so genannter Corona-Apps. Dabei wird fast inflationär der Begriff der Anonymisierung verwandt und so der Eindruck erweckt, das Nachverfolgen mit diesen Apps sei harmlos. Sogar Informatiker äußern sich in diesem Sinne, die eigentlich besser wissen sollten, was bei der Zielsetzung der App logisch möglich ist – und was nicht. Einwände werden regelmäßig vom Tisch gewischt.

Wer wissen und entscheiden will, was eine Corona-App leisten soll und kann, muss sich daher auch damit auseinandersetzen, was sich tatsächlich hinter den hier diskutierten Begriffen verbirgt und was die Konsequenzen sind. Erst deren präzise Verwendung ist die Grundlage für die richtigen Fragen und für die Bestimmung wirksamer Schutzmaßnahmen.

Anonymisierung bezeichnet einen Vorgang, bei dem der Bezug zwischen einem Datum oder Datensatz und einem Individuum so vollständig getilgt wird, dass nach fachlichem Ermessen anschließend keine personenbezogene Zuordnung mehr möglich ist. Der Vorgang soll unumkehrbar sein.

Daten, die fachgerecht anonymisiert wurden, zählen (Achtung!) nicht mehr als personenbezogene Daten. Die Verpflichtungen, die Datenschutzgesetze (Datenschutzgrundverordnung, BDSG) vorsehen, gelten für diese Daten nicht. Weder müssen anonymisierte Daten nach ihrer Anonymisierung besonders geschützt werden, noch muss ihre Verarbeitung beschränkt werden. Weil ein Bezug zu Personen nicht mehr besteht, können durch die Verarbeitung per definitionem keine Persönlichkeitsrechte verletzt werden.

Wer in Zusammenhang mit anonymisierten Daten von einer **De-Anonymisierung** spricht, benennt einen Widerspruch in sich. Wären die Daten erfolgreich anonymisiert worden, dürfte eine spätere Rückführung auf Personen gar nicht möglich sein. Und so wird dieser Begriff auch genutzt: er signalisiert, dass etwas schiefgelaufen ist und die Anonymisierung letztlich nicht erfolgreich war. Der Begriff wird fachlich verwendet, um ein Risiko zu beschreiben: dass nämlich ein Anonymisierungsverfahren so fehlerhaft ist, dass ein Angriff (also der Versuch, unberechtigt den Personenbezug wiederherzustellen) erfolgreich sein kann. De-Anonymisierung geschieht meist unerwartet und ist jedenfalls immer unerwünscht. Sie stellt einen groben Fehler im (Anonymisierungs-) System dar.

Ob ein geplantes Verfahren sich überhaupt dafür eignet, Daten zu anonymisieren, lässt sich durch eine einfache Frage prüfen. Gibt es in dem Verfahren irgendeinen Zeitpunkt x, zu dem ein Bezug zwischen Datum und Person erforderlich ist, um den Zweck des Verfahrens zu erreichen? Wohlgemerkt unabhängig davon, wer (Mensch) oder was (Maschine) zu diesem, möglicherweise sehr kurzen Zeitpunkt, diesen Bezug benötigt.

Damit sind wir beim Zweck von Corona-Apps. Der wird allgemein so beschrieben, dass zumindest im Falle einer erkannten Infektion nachträglich potenziell gefährdete Personen informiert werden sollen. Unabhängig davon, wie gut zuvor auch Nahkontakte durch technische Maßnahmen verschleiert worden sind: im Benachrichtigungsfall muss die Tatsache des Nahkontakts mit dem Infizierten auf eine oder mehrere Personen bezogen werden, damit diese überhaupt benachrichtigt

werden können. Dass die Rückführung über mehrere Stufen (wechselnde IDs u.ä.) geschieht, ändert nichts daran, dass am Ende die richtige Person (die Kontakt gehabt hat) benachrichtigt werden muss.

Alleine diese Erkenntnis verbietet, eine echte Anonymisierung einzusetzen, da dann (Definition!) die Verbindung zwischen Infiziertem und Kontaktperson gar nicht mehr erkennbar sein dürfte – was aber dem Zweck der App widerspräche.

Was in allen beschriebenen Konzepten hingegen stattdessen (für diesen Zweck sinnvollerweise) eingesetzt wird, sind Methoden der **Pseudonymisierung**. Darunter versteht man Verschleierungsmethoden, die den Bezug zwischen Datum und Person so unterbrechen, dass eine Zuordnung nur noch unter sehr gut zu kontrollierenden Bedingungen zugelassen werden kann. Durch geschickten Einsatz technischer Möglichkeiten trennt man Datum und Personenbezug voneinander und kann so bestimmen und gestalten, wer wann unter welchen Bedingungen und zu welcher Zeit eine Zusammenführung zwischen pseudonymem Datum und Person herbeiführen kann und darf.

Bei einer solchen Aufdeckung des Pseudonyms handelt es sich um eine gewollte, gestaltete und durchaus sinnvolle Schutzmaßnahme zur Wahrung der Persönlichkeitsrechte von Betroffenen, die bewusst gestalteter Teil eines Verfahrens ist. Pseudonymisierte Daten gelten eben wegen der Möglichkeit zur Aufdeckung des Betroffenen aber weiterhin als personenbezogene Daten und dürfen gemäß geltender Datenschutzgesetze nur zu einem zulässigen Zweck verarbeitet werden und sind hierbei vor unberechtigtem Zugriff zu schützen.

Die sichere Gestaltung ihrer Verarbeitung beinhaltet die Festlegung, wer in welchen Fällen und unter welchen Bedingungen Pseudonyme auflösen darf. Es ist wichtig zu erkennen, dass es sich hierbei eben weder um anonyme Daten noch um eine De-Anonymisierung (unerwünschtes Risiko, s.o.) handelt, sondern um gestalteten Gebrauch pseudonymer Daten – also Daten, die immer noch einen Personenbezug haben und von Rechts wegen zu schützen sind.

Der saubere Gebrauch dieser Begriffe ist essentiell, wenn man die mit einer bestimmten Verarbeitung einhergehenden Risiken systematisch bestimmen und durch Schutzmaßnahmen begrenzen will. Die Verwendung unzutreffender Begriffe führt nicht nur dazu, dass fachfremden Personen eine Sicherheit vorgegaukelt wird, die de facto nicht vorhanden ist („ist ja alles anonym – kann gar nichts passieren“) sondern sie führt auf der fachlichen Ebene auch dazu, dass die juristische Einordnung fehlerhaft wird und wichtige Fragen in Zusammenhang mit Bedrohungsszenarien gar nicht erst gestellt werden.

Ich wünsche mir daher, gerade von Informatikerinnen und Informatikern, eine Rückkehr zur korrekten Begriffsverwendung!

Bonn, 16.4.2020

Dipl.-Inform. Karin Schuler
Datenschutz & IT-Sicherheit und
Netzwerk Datenschutzexpertise
buero@schuler-ds.de
0228/24 20 733