Jan Fährmann, Clemens Arzt

Polizeilicher Umgang mit personenbezogenen Daten in der Corona-Pandemie

Datenschutz in der Krise

Seit Beginn[1] der Corona-Pandemie werden verschiedenste Grundrechte dem Gesundheitsschutz untergeordnet, die Versammlungsfreiheit, die Religionsfreiheit und die allgemeine Handlungsfreiheit seien hier beispielhaft genannt. Daneben werden in großem Umfang personenbezogene Daten erhoben und verarbeitet. Diskutiert wurde dies in der Literatur jenseits der Corona-Warn-App und vergleichbarer Fragen[2] bisher vergleichsweise wenig und nur selten von der Rechtsprechung überprüft.[3]

1 Einleitung

Die Polizei ist als allgemeine Gefahrenabwehrbehörde ein entscheidender Akteur während der Corona-Pandemie, insbesondere, da sie zahlreiche Maßnahmen durchsetzen muss, weil es anderen Behörden hierzu an Ressourcen fehlt.[4] Insofern stellt sich die Frage, welche Rolle die Datenverarbeitung, von deren Erhebung bis hin zu Speicherung und Übermittlung seitens der Polizei während der Pandemie einnimmt.

Dem Beitrag liegt die These zugrunde, dass sich polizeiliche Interessen und Tätigkeiten während der Pandemie nicht essentiell verändert haben, da die Polizei keine Infektionsschutzbehörde ist und keine Expertise in diesem Bereich hat.[5] Handlungsleitend ist daher vielfach nicht der Infektionsschutz, obwohl in einer Pandemie dem Gesundheitsschutz beim behördlichen Handeln ein besonderes Gewicht zukommt[6], sondern andere polizeiliche Interessen. Der Beitrag analysiert einzelne Fallkonstellationen, in denen die Polizei im Kontext der Pandemie Daten verarbeitet und untersucht, ob dies mit datenschutzrechtlichen Vorgaben vereinbar ist. Zusätzlich werden an zwei Beispielen datenschutzrechtliche Risiken beschrieben, die durch Datenverarbeitungen aufgrund der Pandemie entstehen.

Dr. Jan Fährmann

ist Jurist und Kriminologe. Nach einer Tätigkeit in der Strafverteidigung arbeitet er aktuell im Forschungsinstitut für öffentliche und private Sicherheit an der HWR Berlin, an der er auch als Dozent tätig ist. Seine Forschungsschwerpunkte liegen im Polizei-, Strafvollzugs-, Datenschutz- und Betäubungsmittelrecht.
E-Mail: Jan.Faehrmann@hwr-berlin.de

Prof. Dr. Clemens Arzt

lehrt seit 1999 öffentliches Recht mit dem Schwerpunkt Polizei- und Versammlungsrecht am Fachbereich Polizei und Sicherheitsmanagement der HWR Berlin. Er ist dort zugleich Direktor des Forschungsinstituts für öffentliche und private Sicherheit. Zahlreiche Veröffentlichungen zum deutschen und ausländischen Recht.
E-Mail: clemens.arzt@hwr-berlin.de

2 Ausgangslage

Was zuvor nicht selten als undenkbarer Grundrechtseingriff gegolten hätte, insbesondere ohne normenklare und normenbestimmte (gesetzliche) Grundlage, wurde und wird im Rahmen der Corona-Pandemie oft nicht nur als zulässig, sondern sogar

1 Der Beitrag wurde am 27.10.2020 fertig gestellt.

2 Zur sog. Corona-Warn-App vgl. die Beiträge von Dix und von Jahnel/Gerhardus/Wienert, in diesem Heft; Dochow, GuP 2020, 129; mit Blick auf die polizeiliche Tätigkeit s.a. Arzt, DPolBl 5/2020, 4 ff.; Arnd/Brockmann, Kriminalistik 2020, 283.

3 Siehe aber VerfGH Saarland, Beschl. v. 28.8.2020 – Lv 15/20 (in diesem Heft); VGH Mannheim Beschl. v. 25.6.2020 – 1 S 1739/20; VG Gera Beschl. v. 25.6.2020 – 3 E 851/20; OVG Münster Beschl. v. 23.6.2020 – 13 B 695/20.NE; VG Gelsenkirchen Beschl. v. 30.4.2020 – 20 L 536/20 [alle juris].

4 Vgl. dazu Bosch/Fährmann/Aden, CILIP 2020 (im Erscheinen).

5 Ebd.

6 Kugelmann in: https://verfassungsblog.de/gesundheitsnot-kennt-datenschutzgebot/.

als unausweichlich eingestuft.[7] Dieses Muster übernahmen zunächst auch die Verwaltungsgerichte, bevor nach etlichen Wochen endlich eine differenziertere rechtstaatliche Betrachtung Einzug hielt.[8] Die Auswirkungen auf den Grundrechtsgebrauch sind gravierend[9] und lassen Ungutes für andere Krisenlagen in der Zukunft erahnen. Rechtsgrundlage allfälliger und zum Teil weitreichender Beschränkungen ist dabei selten (unmittelbar) eine gesetzliche Regelung[10], sondern sind Allgemeinverfügungen und Rechtsverordnungen in großer Zahl, oft mit wöchentlich wechselndem Inhalt. Die Gerichte haben dies zum Teil problematisiert, nicht selten aber auch akzeptiert.[11] Das BVerfG wurde im Rahmen des einstweiligen Rechtsschutzes in Dutzenden von Fällen angerufen[12], recht häufig mit Blick auf Beschränkungen der Versammlungsfreiheit; mit Blick auf das Recht auf informationelle Selbstbestimmung erging indes (soweit erkennbar) keine oder kaum substanzielle Entscheidung.[13]

3 Pandemie und Datenschutz

Während in der Öffentlichkeit und in der wissenschaftlichen Fachliteratur der staatliche Umgang mit Grundrechten wie der Versammlungsfreiheit breit diskutiert wurde[14], sind das Grundrecht auf informationelle Selbstbestimmung und das europäische und deutsche Datenschutzrecht bisher – mit Ausnahme der Corona-Warn-App und vergleichbarer Instrumente – selten in den Fokus geraten, obwohl zahlreiche Eingriffe erfolgten. Gerade in Zeiten hoher Infiziertenzahlen scheint der Datenschutz in Abwägung mit gesundheitlichen Fragen von vielen nicht als sonderlich bedeutend empfunden worden zusein.[15]

Dabei sind datenschutzrechtliche Erwägungen gerade auch in einer Pandemie essenziell, da die Risiken für die Verarbeitung personenbezogener Daten mit Blick auf die Kontaktnachverfolgung[16] und andere Instrumente hoch sind. Zur Bekämpfung der Ausbreitung eines Virus kann eine Erhebung und Auswertung zahlreicher Daten beitragen – etwa Bewegungs- oder Gesundheitsdaten[17] –, beispielsweise um die Ausbreitung zu unterbrechen, um Schutzmaßnahmen zu ergreifen oder mehr Informationen über die Wirkung des Virus zu erhalten. Dies ist auch während der Corona-Pandemie der Fall[18], in der gerade am Anfang kaum Kenntnisse über Wirkung und Ausbreitung des Virus vorlagen. Daher bestand ein großes staatliches Interesse an zahlreichen Daten, um dem staatlichen Schutzauftrag entsprechen zu können – in der Krise überwiegend in der Ausprägung des Infektionsschutzes.[19] Andererseits war Ende Oktober 2020 zu erkennen, dass die Behörden immer weniger in der Lage sind, die zunehmende Menge an (Kontakt-)Daten überhaupt noch sinnvoll zu verarbeiten. Gleichwohl ist zu berücksichtigen, dass der Schutz der durch das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und zahlreiche andere Grundrechte geschützten personenbezogenen Daten selbst während einer Pandemie nicht automatisch hinter dem staatlichen Schutzauftrag zurückstehen kann. Vielmehr ist stets ein verhältnismäßiger Ausgleich zwischen den Freiheitsrechten der Betroffenen und den Schutzbemühungen des Staates zu schaffen, wobei selbstredend zu berücksichtigen ist, dass die Risiken durch eine Ausbreitung der Pandemie schwer wiegen.[20]

4 Polizei und Datenverarbeitung in der Pandemie

Deutlich wahrnehmbar in der öffentlichen Diskussion ist, – losgelöst von der Pandemie – dass stetig steigende Datenmengen in der Gesellschaft dazu führen, auf polizeilicher Seite zur Gefahrenabwehr und Strafverfolgung ein großes und weiter wachsendes Interesse am Zugriff auf personenbezogene Daten zu erzeugen[21], was zu einer kontinuierlichen Ausweitung polizeilicher Datenverarbeitungsbefugnisse führt. Unterstellt wird offenbar, dass die Sicherheitsbehörden umso besser funktionieren, je umfassender der Alltag überwacht wird und je mehr Zugriff die Polizei auf große Datenmengen hat.[22] Auch Informationen über Personen, die möglicherweise das Ziel von polizeilichen Maßnahmen sind, werden oft angefordert, um einen Schutz der Beamt*innen in der konkreten Einsatzsituation sicherzustellen. Im Folgenden wird daher die polizeiliche Datenverarbeitung im Kontext der Corona-Pandemie an Hand verschiedener Beispiele analysiert.

4.1 Datenübermittlung der Gesundheitsämter an die Polizei

In mehreren Bundesländern gab es Fälle, in denen Gesundheitsämter ohne konkreten Anlass Listen mit Kontaktdaten von Corona-Infizierten an Dienststellen der Polizei weitergegeben haben – teilweise aufgrund der Aufforderung durch die zuständigen Ministerien. Dies soll (im Sinne „personenbezogener Hinweise“) dazu dienen, dass Polizeibeamt*innen im Fall eines Einsatzes Vorkehrungen gegen eine Ansteckungsgefahr treffen können. Mehrere Datenschutzbeauftragte protestierten[23] und waren offenbar vorher in die Entscheidung nicht eingebunden worden.

7 Geminn/Johannes/Miedzianowski, ZD-Aktuell 2020, 07073.

8 Vgl. etwa Stache, Vorläufiger Rechtsschutz in der (Corona-)Krise in: https://www.juwiss.de/69-2020/; Madjidian, Wenn Gerichte sich weigern – Eilrechtsschutz bei Versammlungsverboten in den ersten Pandemiewochen in: https://www.juwiss.de/60-2020/ [alle Internetquellen zuletzt am 10.09.2020 abgerufen]; kritisch auch Lichdi, SächsVBl. 2020, 273 (279).

9 Stoklas, ZD-Aktuell 2020, 07093.

10 Vgl. nur Lichdi, SächsVBl. 2020, 273 ff. m.w.N.

11 Anders zuletzt VerfGH Saarland, Beschl. v. 28.8.2020 – Lv 15/20 (in diesem Heft) und hieran anschließend der Gesetzentwurf zur Kontaktnachverfolgung im saarländischen Landtag, Drs. 16/1428.

12 Allein in juris waren am 10.9.2020 deutlich über 50 Entscheidungen auffindbar.

13 In BVerfG Beschl. v. 7.7.2020 – 1 BvR 1187/20 wurde eine Verletzung gerügt, hierüber aber nicht entschieden.

14 Vgl nur Gusy in: https://verfassungsblog.de/die-corona-der-coronaleugner-und-das-versammlungsrecht/;
Fährmann/Aden/Arzt in: https://verfassungsblog.de/versammlungsfreiheit-auch-in-krisenzeiten/, Aden/Arzt/Fährmann, Gefährdung der Versammlungsfreiheit in Krisenzeiten – Lehren aus der COVID-19-Pandemie, Die Polizei 12/2020 (im Erscheinen).

15 Stoklas, ZD-Aktuell 2020, 07093; Geminn/Johannes/Miedzianowski, ZD-Aktuell 2020, 07073.

16 Siehe oben Fn. 11.

17 Vgl. schon Bretthauer in: https://verfassungsblog.de/datenschutz-versus-katastrophenschutz/; Dix, in diesem Heft.

18 Köllmann, NZA 2020, 831, 83; Schmoberg/Stroscher, ZD-Aktuell, 07074.

19 Vgl. Fährmann in: https://verfassungsblog.de/pandemie-und-strafvollzug/; Fährmann/Arzt/Aden in: https://verfassungsblog.de/corona-gaestelisten-masslose-polizeiliche-datennutzung/.

20 BVerfG, Beschl. v. 13.5.2020 – 1 BvR 1021/20 und Beschl. v. 12.5.2020 – 1 BvR 1027/20.

21 Vgl. Fährmann, MMR 2020, 228, 228.

22 Schaar, HMD 2014, 840, 843.

23 Vgl. etwa https://lfd.niedersachsen.de/startseite/allgemein/presseinformationen/erlass-zur-datenubermittlung-durch-gesundheitsamter-187289.html;

Die pauschale und vorsorgliche, anlassunabhängige Übermittlung personenbezogener Daten über möglicherweise infizierte Personen an Polizeidienststellen ist rechtswidrig. Bei den personenbezogenen Daten zu möglichen oder festgestellten Infektionen handelt es sich um Gesundheitsdaten, die als sensitive[24] bzw. „besondere Kategorien personenbezogener Daten" nur unter den Voraussetzungen von Art. 9 Abs. 2 DSGVO verarbeitet werden dürfen. Gerade medizinische Daten sind sehr sensibel, da diese Daten höchstpersönlich sind und aus deren Bekanntgabe den Betroffenen erhebliche Nachteile erwachsen können. Zwar ist das Interesse an einem Infektionsschutz der Beamt*innen für diese von Bedeutung, zumal darüber auch die Funktionsfähigkeit staatlicher Organe gewährleistet werden kann. Eine Rechtsgrundlage für eine anlassunabhängige Übermittlung dieser Daten existiert indes nicht. Weder liegen die Voraussetzungen des Art. 9 Abs. 2 DSGVO vor, noch bestehen sonstige gesetzliche Regelungen im Infektionsschutz- oder Gesundheitsrecht, die eine solche Übermittlung – auch mit Blick auf die Anforderungen der Verarbeitung besonderer Kategorien personenbezogener Daten[25] – gestatten könnten. Mit Blick auf den genannten Charakter dieser Daten ist auch eine Übermittlung nach den allgemeinen Regelungen über die Übermittlung personenbezogener Daten zwischen Ordnungsbehörden und der Polizei (z.B. § 44 ASOG Berlin) unzulässig, weil es hierfür einer besonderen Rechtsgrundlage im Sinne des Art. 9 Abs. 2 DSGVO bedürfte und zumindest bei einer pauschalen Übermittlung nicht erkennbar ist, weshalb diese Daten zur Aufgabenerfüllung der Polizei im Rahmen des Polizeirechts erforderlich sein sollten; es mangelt an einer konkreten Gefahr im Einzelfall.[26] Bei einer anlassbezogenen Übermittlung im Einzelfall mag dies anders zu beurteilen sein, wobei auch hier für die absendende Behörde als Sonderordnungsbehörde die Rechtsgrundlage allein im IfSG liegen könnte.[27]

Zudem ist auch eine Weitergabe personenbezogener Daten in Listen nicht mit dem datenschutzrechtlichen Grundsatz der Erforderlichkeit in Einklang zu bringen. Die Polizei erhält so Zugriff auf Gesundheitsdaten sehr vieler Menschen, mit denen sie vermutlich nicht in Kontakt treten wird. Außerdem sind die Listen in vielen Einsatzsituationen nicht praktikabel, da die Polizist*innen oft nicht wissen, wer ihr Gegenüber ist, sodass Schutzmaßnahmen erst nachträglich ergriffen werden können.[28] Dies gilt insbesondere, weil die Polizei oft sehr schnell handeln muss. Ein effektiveres und milderes Mittel wäre daher, die Polizei mit entsprechenden Schutzmaßnahmen gegen eine Infizierung auszustatten – jedenfalls dann, wenn hohe Infiziertenzahlen vorliegen.

Im Ergebnis liegt bei einer pauschalen Übermittlung von Listen möglicherweise infizierter Personen eine verfassungsrechtlich unzulässige Vorratsdatenspeicherung bei der Polizei vor,[29] die allenfalls in Ausnahmefällen zum Infektionsschutz der Beamt*innen beitragen könnte und daher unverhältnismäßig ist. Zwar muss konzediert werden, dass die Behörden aufgrund der Überforderung durch die Corona-Pandemie zum Teil unter großem Druck standen und ein Handeln unter Unsicherheit insbesondere in den ersten Wochen der Pandemie an der Tagesordnung war. Gleichwohl wird deutlich, dass sowohl Polizei- als auch Innenbehörden den Schutz sensibler Daten in einer solchen Situation den polizeilichen Interessen pauschal in sehr vielen Fällen unterordnen, ohne sich dabei um rechtsstaatliche Grundsätze zu kümmern. Hier ist dringend der Gesetzgeber gefragt, der sich indes zumindest bis Ende Oktober 2020 jeder parlamentarischen Absicherung einschneidender Maßnahmen verweigert hat.[30]

4.2 Ausweispflicht

Ein weiteres Beispiel für eine sehr schnelle und rechtsstaatswidrige Ausweitung der polizeilichen Befugnisse, die nicht zur Verringerung von Infektionen beitrug, war die Ausweispflicht in Berlin und Sachsen-Anhalt zu Beginn des Lockdowns. Nach beiden Corona-Verordnungen musste ein amtlicher Ausweis stets mitgeführt und auf Verlangen vorgelegt werden, um die Durchsetzung des Kontaktverbotes durch die Polizei zu gewährleisten.[31] Neben der Innenverwaltung ordnete zumindest die Gewerkschaft der Polizei (GdP) in Berlin diese Ausweispflicht als essenziell für die polizeiliche Arbeit ein und bezeichnete deren Abschaffung als „Aprilscherz".[32]

Eine Pflicht, stets ein Ausweisdokument mitzuführen und sich auszuweisen, gibt es indes Deutschland grundsätzlich nicht. Dies wird nach ganz herrschender Ansicht daraus hergeleitet, dass weder im PAuswG noch im PassG eine entsprechende Pflicht enthalten ist und sich auch niemand ohne konkreten Anlass ausweisen muss.[33] Eine Identitätsfeststellung findet also ihre Grundlagen nicht im Ausweisrecht, sondern im Polizeigesetz, der StPO oder anderen Gesetzen. Auch das AufenthG beinhaltet keine Pflicht, sich gegenüber der Polizei jederzeit durch Vorlage eines Ausweisdokuments zu legitimieren. Eine Mitführens- und Vorlagepflicht kann daher nur spezialgesetzlich vorgeschrieben werden. Auch erscheint es maximal sinnvoll zu sein, Menschen auf die Einhaltung eines Kontaktverbotes hinzuweisen und nur bei offenkundigen Verstößen einzuschreiten, was auch eine Identitätsfeststellung beinhalten kann. Die schnelle Abschaffung der Maßnahme in beiden Bundesländern offenbarte ihre rechtliche Halt- und Sinnlosigkeit.

4.3 „Corona-Gästelisten" und Verfolgung von Straftaten oder Ordnungswidrigkeiten

Für die polizeiliche Datenverarbeitung besteht seit Inkrafttreten der DSGVO und der JI-RL (EU) 2016/680 ein zum Teil recht unübersichtliches Normengeflecht aus Polizei- und Datenschutzrecht, wobei die Länder und der Bund hier sehr unterschiedliche Regelungswege gegangen sind.[34] Im Falle der Verfolgung von Straftaten oder Ordnungswidrigkeiten greifen daneben die StPO und das OWiG. Das IfSG enthält zwar eine ganze Reihe von Re-

https://www.datenschutz-bayern.de/corona/weitergabe.html; https://www.stuttgarter-nachrichten.de/inhalt.kritik-des-datenschutzbeauftragten-polizei-will-corona-listen.87c18ec0-9095-4a7b-8f34-d82eae7346d9.html; https://taz.de/Datenschutz-und-Pandemie/!5680851/.

24 Vertiefend Dix, in diesem Heft.

25 Hierzu Schwabenbauer in: Handbuch des Polizeirechts, 6. Aufl., G 1042.

26 Vgl. nur Schmidbauer in: ders./Steiner, PAG, 5. Aufl., Art. 60 Rn. 3.

27 Schwabenbauer in: Handbuch des Polizeirechts, 6. Aufl., G 1043.

28 https://www.datenschutz-bayern.de/corona/weitergabe.html.

29 https://www.datenschutz-bayern.de/corona/weitergabe.html; https://lfd.niedersachsen.de/startseite/allgemein/presseinformationen/erlass-zur-datenubermittlung-durch-gesundheitsamter-187289.html.

30 Ausnahme auf Druck des LVerfGH ist hier das Saarland, s.o. Fn. 36.

31 Ausführlich dazu Fährmann/Arzt/Aden in: https://verfassungsblog.de/ausweispflicht-per-corona-verordnung/.

32 https://www.gdp.de/gdp/gdpber.nsf/id/DE_Angepasste-Verordnung-und-Bussgeldkatalog-Senat-liefert-verspaeteten-Aprilscherz?open&ccm=000.

33 BGH NJW 1972, 2004 (2005).

34 Vgl. etwa Arzt, SächsVBl. 2019, 345.

gelungen zur Verarbeitung personenbezogener Daten, nicht aber eigenständige Datenverarbeitungsregelungen für die Polizei, mit Ausnahme der Erhebung von Daten bei der Grenzkontrolle in § 36 Abs. 8 IfSG. Kommt es zu Verstößen gegen das IfSG oder hierauf beruhenden Rechtsverordnungen, kann die Polizei auf Grundlage der StPO, gegebenenfalls im Rahmen des § 46 OWiG, den Sachverhalt ermitteln. All dies impliziert die Erhebung personenbezogener Daten und deren (weitere) Verarbeitung, ohne dass hier bei Verstößen gegen das IfSG oder darauf beruhenden Rechtsvorschriften besondere Regelungen oder Anforderungen gelten. Beschränkungen können sich indes aus dem rechtstaatlichen Verhältnismäßigkeitsgrundsatz ergeben.

Bei zahlreichen Veranstaltungen, beim Besuch von Restaurants, kulturellen oder sportlichen Einrichtungen, Veranstaltungen, Kirchen, aber auch beim Besuch von Bordellen, müssen im Rahmen der jeweiligen „Corona-Verordnungen" der Länder Kontaktdaten der Gäste gegenüber dem/der Betreiber*in angeben werden.[35] Zum Teil wird dies auch bei dem Art. 8 GG unterfallenden Versammlungen behördlich oktroyiert.[36] Erfasst werden in der Regel neben dem Namen auch die Anschrift und Rufnummer, Mailadresse und Begleitpersonen. Teilweise geschieht dies mittlerweile elektronisch, zumeist aber noch immer in Papierform. Diese Datenerhebung und Speicherung stellt einen Grundrechtseingriff mit erheblichem Gewicht dar.[37] Datenschutzrechtlich Verpflichtete erheben diese Daten von allen Gästen teilweise individuell, andere mittels offen ausliegender oder an mehrere Gäste ausgehändigter Kontaktlisten, die von allen anderen Gästen eingesehen und zum Beispiel auch fotografiert werden können.

Für das saarländische Recht hat der LVerfGH festgestellt, dass dieses „zugleich eine Unterschreitung des Schutzes [darstellt], den der Staat Betroffenen gegenüber Dritten gewähren muss, wenn er eine Kontaktdatenerhebung bewirkt. Zu dieser Pflicht zum ‚Datenschutz' zählen auch normative Vorkehrungen, die infektionsschutzrechtlich möglicherweise gebotene Offenbarung personenbezogener Informationen vor den Augen Dritter geheim zu halten. Auch das trägt zum Gewicht des mittelbaren Eingriffs bei."[38] Ein solcher Grundrechtseingriff bedarf der gesetzlichen Grundlage, die bisher, auch in der DSGVO, nicht gegeben ist.[39] Diese Feststellung des Saarländischen Verfassungsgerichtshofes strahlt auch auf die anderen Bundesländer aus, da die entsprechenden Verordnungen durchgängig nicht auf einer insoweit verfassungsgemäßen Rechtsgrundlage fußen und daher einen solchen Grundrechtseingriff nicht rechtfertigen können.

Die Rechtmäßigkeit der Erstellung insbesondere solcher offenen Listen soll hier indes nicht weiter thematisiert werden, sondern allein deren spätere „Nutzung" durch die Polizei, die sich in aller Regel offenbar nicht auf die Verfolgung von Straftaten nach dem IfSG richtet. Kontaktlisten werden von der Polizei nicht selten nach §§ 94, 98 StPO sichergestellt oder beschlagnahmt.[40] Die Erhebung und Speicherung dieser Gästedaten stellt indes gleichsam eine neue Form der Vorratsdatenspeicherung dar, da personenbezogene Daten unter Androhung von Bußgeldern im Falle der Nichterfassung von Privaten für die staatliche Nutzung unabhängig vom Anfangsverdacht einer Straftat oder einer konkreten Gefahr erhoben und gespeichert werden müssen, allein zum Zwecke der staatlichen Nutzung und ohne eigenen Anlass.[41] BVerfG[42] und EuGH[43] haben wiederholt betont, dass die Verarbeitung von auf Vorrat gesammelten Datenmengen einen beträchtlichen Grundrechtseingriff darstellt, da sich die Menschen diesen Datenerhebungen kaum entziehen können, so auch während der Pandemie. Auch kann deren Erfassung dazu führen, dass Betroffene Orte mit einer solchen Erhebung der Kontaktdaten nicht mehr aufsuchen oder deren Besuch in Frage stellen; Einschüchterungseffekte können so hervorgerufen werden.[44] Eine gesetzliche Regelung unterliegt daher hinsichtlich ihrer Begründung und ihrer Ausgestaltung, auch in Bezug auf die vorgesehenen Verwendungszwecke der erhobenen Daten, besonders strengen Anforderungen.[45]

Daher ist eine vorsorgliche Datenspeicherung ohne hinreichende Rechtsgrundlage gerade in einer seit Monaten durch Gesetz deklarierten Pandemie nationaler Tragweite (§ 5 Abs. 1 IfSG) schlichtweg unzulässig, weil die entsprechenden Rechtsgrundlagen für solche Datenverarbeitungen längst hätten geschaffen werden können.[46] Diese sollten dann auch Regelungen zum Verbot der Zweckänderung enthalten. So sollte neben einer klaren rechtlichen Begrenzung des Zwecks und der ausschließlichen Nutzung durch die Gesundheitsämter – soweit kompetenzrechtlich möglich – analog § 4 Abs. 3 S. 5 Bundesfernstraßenmautgesetz ein ausdrückliches Verbot der Übermittlung, Zweckänderung, Verwendung und Beschlagnahme zu polizeirechtlichen oder strafprozessualen Zwecken jenseits der Abwehr oder Verfolgung von Verstößen gegen das IfSG selbst gesetzlich verankert werden.[47] Die beabsichtigte Nachverfolgung möglicher Infektionsketten wird ohne ein klares Zweckänderungsverbot konterkariert. Wenn Menschen damit rechnen müssen, dass diese Daten zu polizeilichen Ermittlungszwecken jedweder Art verwendet werden können, dürften nicht wenige davon abgehalten werden, korrekte Daten anzugeben, nicht nur dann, wenn sie selbst Strafverfolgung befürchten. Diese Verhaltensweise bestätigt sich in unser aller Erfahrungswelt alltäglich. Gerade Daten, die dazu dienen, einen nie dagewesenen Ausnahmezustand in den Griff zu bekommen, sollten daher nicht für Zwecke der Strafverfolgung jenseits des IfSG verwendet werden dürfen. Dies gilt umso mehr, weil solche Anwesenheitsdaten nach der Pandemie auch mit einer gesetzlichen Regelung nicht mehr erhoben werden dürften. Offenbar ist das Interesse der Polizei gleichwohl hoch, dieses kurze Zeitfenster für polizeiliche Ermittlungen zu nutzen, was rechtsstaatlich bedenklich ist.

Bliebe es entgegen dieser Auffassung bei einem Verzicht auf ein gesetzliches Zweckänderungsverbot für die polizeiliche Verwendung von Gästelisten in einer anderen Angelegenheit als der Kontaktnachverfolgung – die im Übrigen nicht polizeiliche, sondern gesundheitsbehördliche Aufgabe ist – so bedarf eine solche Zweckänderung einer hinreichend bestimmten und verhältnismäßigen Ermächtigungsgrundlage.

35 Vgl. zur Übersicht Härting in: https://www.cr-online.de/blog/2020/05/10/vorratsdatenspeicherung-in-der-gastronomie-kein-essen-ohne-kontaktdaten/.

36 Vgl. VG Köln, Beschl. v. 7.5.2020 – 7 L 809/20 [juris]; VG Gelsenkirchen 30.4.2020 – 20 L 536/20.

37 VerfGH Saarland, Beschl. v. 28.8.2020 – Lv 15/20, S. 25.

38 Ebd. S. 25 f.

39 Ebd. S. 27 ff.

40 Vgl. Fährmann/Arzt/Aden in: https://verfassungsblog.de/corona-gaestelisten-masslose-polizeiliche-datennutzung/ m.w.N.

41 Ausführlich VerfGH Saarland, Beschl. v. 28.8.2020 – Lv 15/20, S. 22 ff, s.a. Urt. vom 6.10.2020 - C-511/18, C-512/18 und C-520/18.

42 BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08; VerfGH Saarland, Beschl. v. 28.8.2020 – Lv 15/20, S. 22 ff.

43 EuGH (Große Kammer), Urt. v. 21.12.2016 – C-203/15, C-698/15.

44 VerfGH Saarland, Beschl. v. 28.8.2020 – Lv 15/20, S. 24.

45 BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08 –, Rn. 206.

46 VerfGH Saarland, Beschl. v. 28.8.2020 – Lv 15/20, S. 32.

47 S.a. § 6 GE Bündnis 90/Die Grünen, BT-Drs. 19/20037.

Eine hinreichend präzise gesetzliche Vorschrift zur Zweckänderung im Sinne der hypothetischen Datenneuerhebung[48] fehlt. Der Übergang dieser Daten in das Strafverfahren ist nicht geregelt und wird daher auf die Ermittlungsgeneralklausel gestützt.[49]

Sollen mittels dieser Daten Straftaten jenseits des IfSG nachgewiesen werden, so kollidiert das Recht auf informationelle Selbstbestimmung mit dem staatlichen Strafverfolgungsinteresse.[50] Zu beachten ist dabei das hohe Eingriffsgewicht einer solchen Zweckänderung bei Massendaten wie die eines einfachen Besuchs von Restaurants usw. Daher ist hierfür eine bereichsspezifische Ermächtigungsgrundlage erforderlich. Die strafprozessuale Regelung zur Sicherstellung und Beschlagnahme in § 94 StPO enthält weder Vorgaben zur Zweckänderung im Rahmen der Beschlagnahme personenbezogener Daten noch wird klargestellt, unter welchen Umständen und mit welchen Verfahrensvorkehrungen die Daten beschlagnahmt werden dürfen. Der Richtervorbehalt in § 98 StPO greift nur, wenn Wirt*innen oder Veranstalter*innen die Daten nicht freiwillig herausgeben.

Vor dem Hintergrund der Sensitivität dieser Daten zum Beispiel beim Besuch eines Gottesdienstes oder auch einer politischen Veranstaltung (Art. 9 DSGVO) und der schieren Datenmengen ist eine Speicherung allein auf Grundlage einer Rechtsverordnung nicht mehr haltbar.[51] Insbesondere bedarf es klarer Regeln, wann Daten von Privatpersonen sichergestellt oder beschlagnahmt werden dürfen, damit §§ 94, 98 StPO nicht zu einer Vorratsdatenspeicherung „durch die Hintertür" führen, auch vor dem Hintergrund der Rechtsprechung zu den Grenzen der Vorratsdatenspeicherung.[52]

4.4 Corona-Warn-App und Immunitätsausweis

Im Anschluss an die Ausführungen oben (4.3) und den Beitrag von Dix in diesem Heft soll hier nur kurz auf die Corona-Warn-App eingegangen werden, für die aus gutem Grund der Erlass eines deren Nutzung regelnden Gesetzes auf der politischen Ebene verlangt wird.[53] Auch dieses muss das Verbot der Zweckänderung vorsehen.[54] Solange ein solches Gesetz nicht existiert, gelten die bereits dargestellten Voraussetzungen für einen möglichen polizeilichen Zugriff[55] auf personenbezogene Daten, bspw. auf Smartphones oder iPhones, soweit ein Eingriff in die Telekommunikationsfreiheit aus Art. 10 GG überhaupt verneint werden kann. Die Zulässigkeit einer pauschalen Übermittlung von Gesundheitsdaten im Kontext der Corona-Pandemie an die Polizei wurde oben (4.1) bereits verneint, dies gilt entsprechend auch für Daten einer Corona-Warn-App. Eine Rechtsgrundlage für die polizeiliche Einsicht in eine solche App etwa gegenüber Personen, von denen die Polizei annimmt, diese könnten infiziert sein, ist nicht erkennbar.

Bundesgesundheitsminister Spahn ist bereits früh in der Corona-Pandemie mit dem Vorschlag eines „Immunitätsausweises" in die Öffentlichkeit gegangen. Geändert werden sollten dafür die Regelungen zu Impfausweisen. Mit Blick auf die breite Kritik wurde das Vorhaben zunächst zurückgestellt. Im Ausweis bzw. Pass sollte bescheinigt werden, dass der/die Inhaber*in eine Covid19-Infektion überstanden habe und immun sei, was indes zunehmend medizinisch umstritten ist. Für Menschen mit diesem Ausweis sollten Zwänge der Corona-Regelungen nicht mehr gelten. Bei möglichen Kontrollen im öffentlichen Raum müsste die Polizei dann überprüfen, ob die kontrollierte Person unter solche Ausnahmeregelungen fällt, was nur durch eine Datenerhebung durch Identitätsfeststellung (IDF) und Vorlage des Corona-Passes möglich wäre. Da eine Rechtsgrundlage für die damit verbundene IDF als Eingriff in das Recht auf informationelle Selbstbestimmung regelmäßig fehlen wird, bedürfte es entweder eines mit Passbildes versehenen Immunitätsausweises als amtlichem Dokument oder einer gesetzlichen Regelung vergleichbar § 48 WaffG, wonach Polizeibeamt*innen der Personalausweis und die waffenrechtliche Berechtigung auf Verlangen zur Prüfung auszuhändigen sind. Wie dies beispielsweise bei einer Versammlung im Schutzbereich des Art. 8 GG im Einklang mit diesem Grundrecht implementiert werden sollte, wäre noch zu klären.

Corona-Warn-App und „Immunitätsausweis" implizieren beide die Verarbeitung sensitiver personenbezogener Daten, letzterer vermutlich noch stärker als die App, weil hier Gesundheitsdaten gleichsam amtlich bestätigt werden. Ein polizeilicher Zugriff auf solche Daten ist rechtlich nicht ohne hinreichend bestimmte gesetzliche Regelung möglich, deren nähere Ausgestaltung noch nicht im Ansatz ausdiskutiert ist. Die oben (4.1 bis 4.3) formulierten Bedenken und Rahmenbedingungen wären dabei auf jeden Fall zu berücksichtigen.

5 Fazit

Auch wenn die Polizei insbesondere durch Präsenz und Kontrollen dazu beitragen kann, die Infiziertenzahlen zu reduzieren, so ist der Erfolg mit Blick auf die Verarbeitung personenbezogener Daten in diesem Kontext fraglich und sensitive (besondere Kategorien) personenbezogener Daten waren und sind dem Risiko ausgesetzt, jenseits des Infektionsschutzes dem allgemeinen polizeilichen Interesse dienend genutzt zu werden. Gerade der polizeiliche Zugriff auf „Gästelisten" macht deutlich, dass die Datenverarbeitung zudem nicht zwingend dem Infektionsschutz dienen muss, sondern diesem sogar zuwiderlaufen kann, wenn nämlich die berechtigte Sorge vor einer polizeilichen Nutzung und Zweckänderung solcher Daten zu willentlich falschen Angaben führt. Gerade hier wurden – mit Unterstützung zum Beispiel des bayerischen Innenministers[56] – datenschutzrechtliche Maßgaben „kleingeredet" oder offensiv missachtet. Daher sind gesetzliche Regelungen erforderlich, die das Verhältnis der polizeilichen Arbeit zum Infektions- und Datenschutz auch in der Pandemie in ein ausgewogenes Verhältnis bringen, da diese offenkundig noch einige Zeit bestehen bleiben wird.

48 BVerfG 20.4.2016 – 1 BvR 966/09 und 1 BvR 1140/09, Rn. 287.
49 VerfGH Rheinland-Pfalz, Urteil v. 24.2.2014 – VGH B 26/13, Rn. 47 f.
50 Schmidt, Der Grundsatz der Verfügbarkeit, 2018, S. 1.
51 VerfGH Saarland, Beschl. v. 28.8.2020 – Lv 15/20, S. 29.
52 EuGH (Große Kammer), Urt. v. 21.12.2016 – C-203/15, C-698/15; Roßnagel, NJW 2017, 696.
53 Bspw. Johannes, ZD-Aktuell 2020, 07114; s.a. Gesetzentwurf Bündnis90/Die Grünen, BT-Drs. 19/20037.
54 Vgl. Fn. 50.
55 Vertiefend: Arzt, Corona-App, Corona-Pass und Immunitätsausweise, DPolBl 5/2020, 4 ff.
56 https://www.spiegel.de/panorama/justiz/corona-gaestelisten-joachim-herrmann-verteidigt-nutzung-von-durch-polizei-a-64d25ef3-009c-4dac-a4a2-2da6aabc8729.