KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Laura Schachtner

Der strafprozessuale Zugriff auf Handy-Daten und Gästelisten in Zeiten der Pandemie

Prüfer: Prof. Dr. Mark Zöller
Universität: Ludwig-Maximilians-Universität München
Abgabedatum: 30.9.2020

Inhaltsverzeichnis

I. Die Corona-Pandemie

Seit Jahresbeginn wird die Welt von einer Krise beherrscht: der Corona-Pandemie. Seit seiner Entdeckung hat das Sars-CoV-2-Virus sich sehr schnell ausgebreitet, da es durch „Tröpfcheninfektion" leicht übertragen werden kann. Das Virus hat durch hohe Infektionszahlen in manchen Ländern zu einer Überlastung des Gesundheitssystems geführt.[1] Um die Ausbreitung des Virus in Deutschland zu verhindern, sind daher Schutzmaßnahmen ergriffen worden. Zum Beispiel ist eine Corona-Warn-App entwickelt worden, die den Nutzer bei Kontakt mit einer infizierten Person benachrichtigt.[2] Zudem sind Restaurants verpflichtet, Gästelisten zu führen, um bei einer Infektion alle Kontaktpersonen informieren zu können. Bei diesen Prozessen werden sehr viele Daten von den Bürgern aufgezeichnet. Diese sind in einigen Bundesländern von der Polizei genutzt worden, um die Aufklärung von Straftaten voranzutreiben.[3] Dies hat die Frage aufgeworfen, ob solche Datenerhebungen zulässig sind. Daher soll diese Arbeit die Rechtslage in Bezug auf den strafprozessualen Zugriff auf zur Eindämmung der Pandemie erhobene Handy-Daten und Gästelisten zu Strafverfolgungszwecken aufzeigen.

II. Strafprozessualer Zugriff auf zur Eindämmung der Pandemie erhobene Handy-Daten und Gästelisten zu Strafverfolgungszwecken

Um die strafprozessuale Rechtslage einordnen zu können, müssen zunächst ein paar grundlegende Fragen geklärt werden. Begonnen wird hierbei mit der Rechtsgrundlage für die Erhebung der Daten.

1. Die Erhebung der Daten aufgrund der Pandemie

Jedes staatliche Handeln beruht auf einer Ermächtigungsgrundlage.[4] So muss auch das Erheben von Handy-Daten und Gästelisten auf einer Rechtsgrundlage beruhen. Die Handy-Daten, die zur Zeit einer Pandemie erhoben werden, beinhalten den Aufenthaltsort, den Kontakt mit anderen Menschen und die Möglichkeit sich infiziert zu haben.[5] Je nach angegebenen Daten lassen sich aus den Gästelisten der Aufenthaltsort, der Name, die Adresse, die Telefonnummer und die E-Mail-Adresse ableiten.[6] Hierbei handelt es sich um personenbezogene Daten, da sie sich auf eine identifizierte beziehungsweise identifizierbare Person beziehen.[7] Zwar ist es möglich, die Daten, wie bei der Warn-App, durch temporäre Identifikationsnummern zu anonymisieren, die Person muss aber dennoch identifizierbar sein, um sie über eine mögliche Infektion zu informieren.[8]

Als Rechtsgrundlage für den Zugriff auf personenbezogene Daten fungiert die Datenschutz-Grundverordnung (DSGVO), die als Öffnungsklausel die Nutzung der Daten gestattet. Laut Art. 6 Abs. 1 S. 1 lit. a und Art. 9 Abs. 2 S. 2 lit. a DSGVO i. V. m. Art. 4 Nr. 11 DSGVO ist die Datenerhebung grundsätzlich nach einer

1 *Busch*, Corona-Krise: Welche Folgen hat die Pandemie für unser Gesundheitssystem? vom 11.5.2020, abrufbar unter: https://www.bpb.de/politik/innenpolitik/coronavirus/309530/gesundheitsversorgung (zuletzt abgerufen am 28.9.2020), Frage 2; *Dochow*, GuP 2020, 129 (130); WHO Europa, Pandemie der Coronavirus-Krankheit (COVID-19), abrufbar unter: https://www.euro.who.int/de/health-topics/health-emergencies/coronavirus-covid-19/novel-coronavirus-2019-ncov (zuletzt abgerufen am 28.9.2020).
2 *Dochow*, GuP 2020, 129 (131); *Kuhlmann*, GSZ 2020, 115 (116); *Müller*, MMR 2020, 355 (355).
3 *Aden/Arzt/Fährmann*, Corona-Gästelisten – maßlose polizeiliche Datennutzung, vom 14.8.2020, abrufbar unter: https://verfassungsblog.de/corona-gaestelisten-masslose-polizeiliche-datennutzung/ (zuletzt abgerufen am 28.9.2020), Einleitung.
4 *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, 2002, S. 32.
5 *Dochow*, GuP 2020, 129 (131); *Kuhlmann*, GSZ 2020, 115 (115).
6 *Aden/Arzt/Fährmann*, Einleitung.
7 Art. 4 Nr. 1 DSGVO.
8 *Kuhlmann*, GSZ 2020, 115 (117).

freiwilligen Einwilligung des Betroffenen möglich.[9] Es gibt aber durchaus Ausnahmeregelungen, die den Zugriff auf die Daten ohne Einwilligung erlauben, wenn das Allgemeininteresse überwiegt. Bei einer Pandemie besteht dieses Interesse im Schutz der Bürger vor Gesundheitsgefahren.[10] Die Art. 6 Abs. 1 S. 1 lit. e, d, f DSGVO erlauben die Datenverarbeitung nicht sensibler Daten bei Wahrnehmung von Aufgaben im öffentlichen Interesse und zum Schutz lebenswichtiger oder berechtigter Interessen. Der Schutz der Gesundheit der Bevölkerung vor einer Pandemie stellt gerade ein solches Interesse dar. Für Art. 6 Abs. 1 S. 1 lit. d DSGVO wird dies explizit in Erwägungsgrund 46 S. 3 festgesetzt, da dieser als Grund der Datenerhebung die Überwachung der Ausbreitung von Epidemien benennt.[11] Die Verarbeitung sensitiver Daten wird durch Art. 9 Abs. 2 lit. i DSGVO ermöglicht. Dieser billigt die Verarbeitung von Gesundheitsdaten, wenn dies im Bereich der öffentlichen Gesundheit notwendig ist, um vor grenzüberschreitenden Gesundheitsgefahren zu schützen.[12] All diese Normen sind jedoch lediglich „Öffnungsklauseln". Man benötigt für die Datenerhebung noch eine gesetzliche Rechtsgrundlage im deutschen Recht. Im Bundesdatenschutzgesetz (BDSG) ist mit § 3 eine Generalklausel geschaffen worden, die die Datenverarbeitung erlaubt, wenn der Verantwortliche sie für seine Tätigkeit benötigt.[13] § 22 Abs. 1 Nr. 1 lit. c BDSG stellt die Rechtsgrundlage dar, um im Bereich der öffentlichen Gesundheit auch sensible Daten zu verarbeiten. Des Weiteren gestattet § 13 Abs. 1 Infektionsschutzgesetz (IfSG), die Daten zur Überwachung von Epidemien zu verarbeiten.[14] Zum Zwecke der Bekämpfung der Pandemie sind zudem Verordnungen durch die Bundesländer geschaffen worden, die die Erhebung von Daten zur Eindämmung der Pandemie gestatten.[15] Diese Normen verkörpern somit die Ermächtigungsgrundlagen zur Erhebung personenbezogener Daten zur Bekämpfung und Eindämmung der Pandemie.

2. Der Eingriff in das Recht auf informationelle Selbstbestimmung durch Zugriff der Strafverfolgungsbehörden

Wie im Zusammenhang mit den Rechtsgrundlagen festgestellt, handelt es sich bei den aufgezeichneten Informationen um personenbezogene Daten. Um diese in Zeiten moderner Technologien vor staatlichen Eingriffen zu schützen, hat das *BVerfG* im Volkszählungsurteil das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG herausgearbeitet. Es gewährleistet das Recht, selbst zu bestimmen, wie, wann, von wem und in welchem Umfang persönliche Daten erhoben und verwendet werden.[16] Dies umfasst den Schutz vor unbegrenzter Erhebung, Speicherung, Weitergabe und Verwendung persönlicher Daten und erteilt dem Betroffenen die Befugnis, über die Verwendung selbst zu bestimmen.[17] Dieser Schutz ist wichtig, damit der Staat sich mit den zugänglichen Informationen kein komplettes Bild der Betroffenen erschaffen und der Bürger die Verwendung seiner Daten nachvollziehen kann.[18] Aber auch dieses Grundrecht ist nicht schrankenlos gewährleistet. Da der Mensch in die Gemeinschaft eingebunden ist, betreffen viele seiner Daten die Allgemeinheit.[19] Daher kann das Recht auf informationelle Selbstbestimmung wegen überwiegender Interessen der Allgemeinheit nach

9 *Kuhlmann*, GSZ 2020, 115 (118).
10 *Kuhlmann*, GSZ 2020, 115 (119).
11 *Kuhlmann*, GSZ 2020, 115 (119, 120, 121).
12 *Kuhlmann*, GSZ 2020, 115 (121).
13 *Dochow*, GuP 2020, 129 (139); *Kuhlmann*, GSZ 2020, 115 (119 f.).
14 *Kuhlmann*, GSZ 2020, 115 (120).
15 *Aden/Arzt/Fährmann*, Einleitung.
16 *Zöller*, S. 25, 26, 27.
17 *Zöller*, S. 28.
18 *Zöller*, S. 29.
19 *Zöller*, S. 40 f.

dem Gebot des Gesetzesvorbehalts durch ein Gesetz eingeschränkt werden.[20] Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt grundsätzlich dann vor, wenn Informationen zwangsweise vom Staat erhoben werden.[21] Bei den Gästelisten liegt Zwang vor, da die Bürger ihre Angaben hinterlassen müssen.[22] Dieser Eingriff zur Bekämpfung der Pandemie lässt sich durch eine Abwägung mit der Gefahr für die Gesundheit der Bevölkerung rechtfertigen.[23] Die Sammlung von Handy-Daten hingegen erfolgt durch eine freiwillige Einwilligung,[24] welche den Verzicht auf den Schutz des Grundrechtes darstellt.[25] Daher ist die Datenerhebung zur Eindämmung der Pandemie rechtmäßig. Wenn nun die Strafverfolgungsbehörden auf diese rechtmäßig erhobenen Daten zugreifen, stellt dies einen weiteren Eingriff in das Recht auf informationelle Selbstbestimmung dar, da es sich bei jeder Weitergabe an eine Behörde um einen neuen Eingriff handelt.[26] Daher wird für diesen Zugriff eine eigene gesetzliche Grundlage, etwa in der StPO, benötigt.

3. Allgemeine verfassungsrechtliche Grundlagen

Um die Rechtmäßigkeit eines Eingriffs durch und auf Grund strafprozessualer Vorschriften beurteilen zu können, müssen die allgemeinen verfassungsrechtlichen Grundlagen beachtet werden. Die Ermächtigungsgrundlagen müssen mit den verfassungsrechtlichen Vorschriften vereinbar sein, um einen Eingriff zu rechtfertigen.[27]

a) Allgemeine Voraussetzungen der gesetzlichen Grundlagen

Wie bereits erwähnt, muss jeder Eingriff in ein Grundrecht auf einer Rechtsgrundlage beruhen. Diese Rechtsgrundlage muss die verfassungsrechtlichen Gebote der Bestimmtheit und der Normenklarheit erfüllen.[28] Sie muss so formuliert sein, dass der Bürger die Rechtslage klar erkennen kann.[29] Die Eingriffsermächtigungen müssen daher den Anlass, den Zweck und die Grenzen der Datenverarbeitungsbefugnis ausweisen.[30] Die Verpflichtung, den Zweck der Datenverarbeitung gesetzlich festzulegen, wird Zweckbindungsgebot genannt. Dieses soll vor übermäßiger Verwendung personenbezogener Daten schützen, da die Daten nur zu einem bestimmten Zweck erhoben und verwendet werden dürfen. So schützt dieses Gebot vor einer zweckentfremdenden Nutzung.[31] Jede Zweckänderung benötigt daher eine eigene Eingriffsgrundlage.[32] Eine solche Ermächtigungsgrundlage muss auch verhältnismäßig sein. Dementsprechend müssen die vorgegebenen Datenerhebungs- und Datenverarbeitungsmaßnahmen ein legitimes Ziel verfolgen und zu dessen Erreichung geeignet, erforderlich und angemessen sein.[33]

b) Zweckentfremdung

Auch die Datenerhebung von Handy-Daten und Gästelisten muss nach dem Zweckbindungsgedanken an einen

20 *Engelhardt*, Verwendung präventivpolizeilich erhobener Daten im Strafprozess, 2011, S. 96.
21 *Zöller*, S. 34.
22 *Aden/Arzt/Fährmann*, Einleitung.
23 *Aden/Arzt/Fährmann*, Staatlicher Schutzauftrag.
24 *Kuhlmann*, GSZ 2020, 115 (118).
25 *Bodenbenner*, Präventive und repressive Datenverarbeitung unter besonderer Berücksichtigung des Zweckbindungsgedankens, 2017, S. 35.
26 *Zöller*, StV 2019, 419 (420).
27 *Bodenbenner*, S. 35; *Engelhardt*, S. 96.
28 *Engelhardt*, S. 103.
29 *Bertram*, Die Verwendung präventiv-polizeilicher Erkenntnisse im Strafverfahren, 2009, S. 131.
30 *Bodenbenner*, S. 69.
31 *Engelhardt*, S. 78, 86 f.; *Zöller*, StV 2019, 419 (420).
32 *Bodenbenner*, S. 126.
33 *Bertram*, S. 134, 136; *Zöller*, S. 46.

bestimmten Zweck gebunden sein. Da diese Daten zur Nachvollziehung der Infektionsketten aufgezeichnet werden, werden sie zum Schutz der Gesundheit der Bevölkerung erhoben. Die Strafverfolgungsbehörden greifen aber zum Zweck einer effektiven Strafverfolgung auf diese Daten zu.[34] Die Daten würden demnach zweckentfremdet werden. Fraglich ist daher, ob der Zweckbindungsgedanke durch eine zweckändernde Datenverarbeitung durchbrochen werden darf. Eine zweckändernde Datenverarbeitung muss generell möglich sein, da das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist und wegen überwiegender Allgemeininteressen eingeschränkt werden kann.[35] Die Übermittlung der Daten an die Strafverfolgungsorgane stellt einen eigenständigen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Zudem vertieft sie den Grundrechtseingriff der Erhebung, da die Daten nochmals verwendet werden. Daher müssen besonders hohe Ansprüche an die Zweckänderungsermächtigung gestellt werden.[36] Zur verfassungsrechtlichen Rechtfertigung des neuen Eingriffs wird eine neue Rechtsgrundlage benötigt. Diese muss als Zweckänderungsermächtigung den Zweck der Übermittlung, deren Voraussetzungen und den Umfang der neuen Nutzung klar beinhalten und stellt somit die Übernahmeklausel für die Annahme der Daten dar. Überdies muss es eine Öffnungsklausel geben, die die Übermittlung der Daten erlaubt.[37] Die Vorschrift muss zudem die allgemeinen verfassungsrechtlichen Anforderungen, wie die Gebote der Bestimmtheit, der Normenklarheit und der Verhältnismäßigkeit, erfüllen.[38] Im Laufe der Zeit hat das *BVerfG* im Bereich der Verhältnismäßigkeit im Hinblick auf die Strafverfolgung eine neue Rechtsfigur für die Abwägung entwickelt: Den qualifizierten hypothetischen Ersatzeingriff. Dieser soll dafür Sorge tragen, dass der Erhebungszweck mit dem geänderten Verwendungszweck vereinbar ist und die Erhebungsbegrenzungen eines Rechtsgebiets nicht umgangen werden.[39] Der qualifizierte hypothetische Ersatzeingriff erlaubt die zweckändernde Datennutzung daher nur, wenn die Behörde die Daten für den geänderten Zweck auf dieselbe Weise hätte erheben dürfen.[40] Dabei muss auf die Eingriffstiefen, Anordnungsbefugnisse und die spezifischen Voraussetzungen der Maßnahme geachtet werden.[41]

c) Die allgemeinen Abwägungskriterien der Verhältnismäßigkeitsprüfung im Falle der Handy-Daten und der Gästelisten

Die strafprozessualen Ermächtigungsgrundlagen müssen diese allgemeinen Anforderungen erfüllen, damit ihre Anwendung rechtmäßig ist. Die Rechtmäßigkeit entscheidet sich vor allem im Rahmen der Verhältnismäßigkeitsprüfung. Beim Zugriff auf Handy-Daten und Gästelisten müssen hierbei einige Aspekte besonders berücksichtigt werden, die im Folgenden kurz erläutert werden.

aa) Entgegenstehendes Interesse: effiziente Strafverfolgung

Um den Eingriff in das Recht auf informationelle Selbstbestimmung rechtfertigen zu können, müssen die entgegenstehenden Interessen in der Verhältnismäßigkeitsprüfung gegeneinander abgewogen werden.[42] Ziel der strafprozessualen Vorschriften ist eine funktionierende und effektive Strafverfolgung.[43] Durch das Strafprozessrecht

34 *Aden/Arzt/Fährmann*, Einleitung; *Kuhlmann*, GSZ 2020, 115 (119); *Zöller*, S. 55 f., 59 f.
35 *Bodenbenner*, S. 125 f.
36 *Bodenbenner*, S. 130 f., 170; *Zöller*, StV 2019, 419 (421).
37 *Engelhardt*, S. 219 f.; *Zöller*, StV 2019, 419 (421).
38 *Engelhardt*, S. 103; *Zöller*, StV 2019, 419 (421).
39 *Bodenbenner*, S. 137, 140.
40 *Bodenbenner*, S. 138, 143.
41 *Bodenbenner*, S. 144.
42 *Bodenbenner*, S. 130, 134, 135.
43 *Bodenbenner*, S. 134; *Zöller*, S. 55 f., 59 f.

werden aufgrund eines Anfangsverdachts Straftatbestände untersucht, die Wahrheit ermittelt und Sanktionen verhängt.[44] So sorgt das Strafprozessrecht für ein geordnetes Zusammenleben der Gesellschaft und für Rechtsfrieden.[45] Um diesen Pflichten nachkommen zu können, müssen die Strafverfolgungsbehörden Zugriff auf personenbezogene Daten erhalten, da diese einen Anfangsverdacht begründen, bei den Ermittlungen helfen und als Beweismittel dienen können.[46] Werden in diesem Bestreben jedoch Freiheitsrechte von Bürgern beeinträchtigt, muss gegebenenfalls die Strafverfolgung hinter diesen zurückstehen.[47] Dabei wird das Strafverfolgungsinteresse in der Abwägung nach der Schwere der Tat, der Aufklärungswahrscheinlichkeit und dem Verdachtsgrad bemessen.[48]

bb) Allgemeine Abwägungskriterien beim Zugriff auf Handy-Daten

Um die Rechtmäßigkeit des Zugriffs auf Handy-Daten überprüfen zu können, muss die Bedeutung der Daten bei der Abwägung beachtet werden. Nur so kann festgestellt werden, wie hoch die Anforderungen an die Ermächtigungsgrundlage und den Zugriff sind. Hierbei sind drei Punkte besonders zu beachten: die Anonymisierung und Bedeutsamkeit der Daten sowie die Streubreite des Eingriffs. Handy-Daten, die zur Bekämpfung einer Pandemie gesammelt werden, sind Kontaktdaten. Diese Daten zeigen an, mit wem man Kontakt hatte, und verdeutlichen das Vorliegen einer (möglichen) Infektion. Dabei können die Daten bei dem Nutzer selbst oder auf einem Server eines Providers gespeichert sein. Bei der Corona-Warn-App wird festgestellt, wer sich nahe und lange genug für eine Infektion neben einer weiteren Person aufgehalten hat. Diese Daten werden als temporäre Identifikationsnummern für 14 Tage auf dem Gerät des Nutzers gespeichert. Zudem wird diese Nummer im Falle einer Infektion an einen Server gesendet, von dem die anderen Nutzer diese herunterladen können.[49] Daher müssen bei dieser Art der Datensammlung bezüglich des strafprozessualen Zugriffs auf Handy-Daten einige Punkte beachtet werden. Der erste Punkt betrifft die Anonymisierung. Anonym sind Daten, die keiner natürlichen Person mehr zuzuordnen sind. Daher sind anonyme Daten keine personenbezogenen Daten mehr und erhalten nicht den Schutz des Rechts auf informationelle Selbstbestimmung.[50] Laut der DSGVO sind Daten einer Person zuzuordnen, wenn sie sich anhand einer Kennung oder besonderer Merkmale zuordnen lassen. Die temporären Identifikationsnummern stellen zwar keine direkten Angaben zu einer Person dar, sie schließen aber eine Zuordnung zu einer bestimmten Person nicht aus. Diese kann vor allem während der Kommunikation zwischen Nutzer und Server stattfinden, da bei diesem Vorgang viele Daten benötigt werden, die eine Identifizierung erleichtern. Daher stellen diese Daten nur Pseudonyme dar, die als personenbezogene Daten gewertet werden.[51] Des Weiteren ist die Streubreite der Maßnahme in diesem Zusammenhang zu beachten, d. h., wie viele Menschen von der Datenerhebung betroffen sind.[52] Wenn die Strafverfolgungsbehörden auf die Handy-Daten zugreifen, ist es ihnen möglich, sämtliche Kontaktpersonen ausfindig zu machen. Somit sind alle Personen, die sich über einen bestimmten Zeitraum nahe des Verdächtigen aufgehalten haben, betroffen. Demnach liegt eine große Streubreite vor, wodurch der Grundrechtseingriff intensiver ist.[53] Als letzter Punkt muss die Bedeutung der erhobenen Daten berücksichtigt werden. Die gesammelten Daten handeln von dem (möglichen) Vorhandensein einer Infektion. Der Infektionsstatus einer Person stellt ein Gesundheitsdatum dar, da er Aufschluss über deren körperliche Gesundheit gibt. Das gilt auch für die Daten, die

44 *Bertram*, S. 149; *Zöller*, S. 59 f.
45 *Zöller*, S. 59 f.
46 *Zöller*, StV 2019, 419 (419 f.).
47 *Zöller*, S. 60.
48 *Bertram*, S. 250, 251, 252.
49 *Dochow*, GuP 2020, 129 (131).
50 *Kuhlmann*, GSZ 2020, 115 (117).
51 *Kuhlmann*, GSZ 2020, 115 (117 f.).
52 *Bertram*, S. 108.
53 *Bertram*, S. 108 f.

nur eine mögliche zukünftige Infektion betreffen.[54] Gesundheitsdaten stellen nach Art. 9 Abs. 1 DSGVO besondere personenbezogene Daten dar, die daher besonders zu schützen sind.[55]

cc) Allgemeine Abwägungskriterien beim Zugriff auf Gästelisten

Auch im Fall des Zugriffs auf eine Gästeliste greifen zwei Kriterien, die bei einer Verhältnismäßigkeitsprüfung in Bezug auf die Ermächtigungsgrundlage besonders zu beachten sind: die Streubreite der Maßnahme und die Bedeutsamkeit der Daten. Bei dieser Maßnahme werden auch die Kontaktdaten der Bürger erfasst, die mit der zu ermittelnden Straftat nicht in Berührung gekommen sind. Dies kann deren Recht innerhalb einer Abwägung schwerer wiegen lassen, da sie keinen Anlass zu der Maßnahme gegeben haben.[56] Daher muss die Streubreite bei der Verhältnismäßigkeitsprüfung des Zugriffs auf Gästelisten berücksichtigt werden. Ein weiterer Punkt, der beachtet werden muss, ist die Bedeutsamkeit der Daten. Die Gästeliste kann Name, Adresse, Telefonnummer oder E-Mail-Adresse enthalten. Außerdem zeigen diese Daten, welche Person sich wann an welchem Ort aufgehalten hat und eventuell sogar mit wem.[57] Ergänzt durch andersartig erlangte Daten, kann viel über einen Bürger preisgegeben werden.[58] Daher muss dies bei der Abwägung berücksichtigt werden.

4. Mögliche Rechtfertigungen: Verhältnismäßigkeitsprüfung

Nachdem die allgemeine Verfassungs- und Rechtslage und die Problematiken in den Fällen Handy-Daten und Gästelisten aufgezeigt wurden, werden nun die einzelnen Ermächtigungsgrundlagen zum strafprozessualen Zugriff auf die Daten dargelegt und ihre Rechtmäßigkeit in den Fällen der Zugriffe auf die Handy-Daten und Gästelisten überprüft.

a) Die Ermittlungsgeneralklauseln, §§ 161, 163 StPO

Begonnen wird zunächst mit den Ermittlungsgeneralklauseln der StPO, die die Befugnisse der Staatsanwaltschaft und der Polizei bei der Ermittlung von Straftaten und deren Grenzen festlegen. [59] Nach den §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO können die Staatsanwaltschaft, sowie die Polizei, Ermittlungen jeder Art vornehmen und Auskunft von den Behörden verlangen, um einen Sachverhalt aufzuklären.[60] Diese Vorschriften sollen für Grundrechtseingriffe dienen, die nicht so intensiv sind, dass sie speziell geregelt werden müssen.[61] Das Recht zu ermitteln beinhaltet auch das Erheben von Daten, soweit dies nicht speziell geregelt ist.[62] Diese Normen stellen somit sowohl Ermittlungs- als auch Datenerhebungsgeneralklauseln dar.[63] Die Strafverfolgungsbehörden können daher die personenbezogenen Daten im Laufe einer Ermittlungsanfrage gegenüber Behörden und privaten Stellen erheben.[64] Einzige Voraussetzung hierfür ist der Anfangsverdacht. Dieser liegt vor, wenn es nach der Auswertung der konkreten Tatsachen mit Bezug auf die kriminologische Erfahrung danach aussieht, dass eine Straftat

54 *Dochow*, GuP 2020, 129 (132).
55 *Dochow*, GuP 2020, 129 (133).
56 *Bertram*, S. 108 f.
57 *Aden/Arzt/Fährmann*, Einleitungsgedanke.
58 *Zöller*, S. 29.
59 *Zöller*, in: HK-StPO, 6. Aufl. (2019), § 161 Rn. 1, 2, § 163 Rn. 1.
60 *Griesbaum*, in: KK-StPO, 8. Aufl. (2019), § 163 Rn. 9; *Zöller*, in: HK-StPO, § 161 Rn. 1, 19, § 163 Rn. 10.
61 *Zöller*, S. 69.
62 *Bertram*, S. 175.
63 *Bodenbenner*, S. 42.
64 *Sackreuther*, in: BeckOK-StPO, 37. Ed. (Stand: 1.7.2020), § 161 Rn. 10, 11.

begangen wurde.[65] Zum Zweck der Strafverfolgung ermöglichen die Generalklauseln daher eine kaum begrenzte Datenerhebung und -übermittlung. Da dies jedoch einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, muss für die Rechtmäßigkeit des Zugriffs das Verhältnismäßigkeitsgebot erfüllt werden.[66] Dabei sind der Gesetzesvorbehalt, das Bestimmtheitsgebot und das Übermaßverbot besonders zu beachten.[67] Wie bereits bei den allgemeinen Ausführungen erwähnt, müssen außerdem die speziellen Voraussetzungen für die zweckändernde Datennutzung erfüllt sein, falls die Datenerhebung durch eine zweckändernde Übermittlung der Daten erfolgt. Hieraus folgt, dass die Ermittlungsgeneralklauseln grundsätzlich für den Zugriff auf Handy-Daten und Gästelisten als Ermächtigungsgrundlagen anwendbar wären, da sie Datenübermittlungen an die Strafverfolgungsbehörden ermöglichen. Dennoch muss die Verfassungsmäßigkeit noch in den Einzelfällen überprüft werden, um über die Rechtmäßigkeit der Datenverarbeitung zu entscheiden.

aa) Handy-Daten

Wie gerade ausgeführt, muss eine Verhältnismäßigkeitsprüfung stattfinden. Da die Datenerhebungsgeneralklauseln allgemeingültig bestimmt sind, darf das Recht, in das eingegriffen wird, nicht zu stark wiegen. Dies führt besonders dann zu Problemen, wenn Ermittlungsmethoden, die die Grundrechte stark beeinträchtigen können, beim Fehlen spezieller Regelungen auf Grund der Generalklauseln eingesetzt werden.[68] Dies ist nicht möglich, da die Generalklauseln nur angewendet werden dürfen, wenn der Eingriff das Recht nur so leicht beeinträchtigt, dass keine speziellere Regelung nötig ist.[69] Durch den Zugriff auf die Handy-Daten wird nicht nur in ein technisches System eingegriffen,[70] sondern auch, wie erwähnt, in Gesundheitsdaten. Des Weiteren werden die Daten aller Kontaktpersonen eingesehen. So sind die Daten vieler unbeteiligter Personen betroffen. Gesundheitsdaten sind nach dem Datenschutzrecht besonders geschützt, da dieses den Zugriff auf diese Daten stark einschränkt.[71] Auch die betroffenen Rechte der unbeteiligten Dritten lassen den Eingriff schwerer rechtfertigen.[72] Zudem wird das Mobiltelefon als technisches System zusätzlich durch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geschützt.[73] All diese Faktoren sorgen dafür, dass hohe Ansprüche an die Eingriffsermächtigung zu stellen sind. Daher kann eine Generalklausel den Zugriff auf die Handy-Daten nicht erlauben, da sie für den Eingriff in solche sensiblen Daten von unbeteiligten Personen zu unbestimmt ist.[74] So kann der Zugriff auf die Handy-Daten nicht durch die Ermittlungsgeneralklauseln gerechtfertigt werden.

bb) Gästelisten

Fraglich ist daher, ob zumindest der Zugriff auf die Gästelisten auf Grundlage der Ermittlungsgeneralklauseln möglich ist. Die Ermittlungsgeneralklauseln besitzen seit 2007 eine Ergänzung in § 161 Abs. 3 S. 1 StPO, die die zweckändernde Nutzung von Daten, die durch andere Vorschriften als die der StPO erhoben worden sind, begrenzt.[75] Diese Vorschrift könnte also die Anwendung der Generalklauseln für die zweckändernde Verwendung der Gästelistendaten zu Strafverfolgungszwecken sperren. § 161 Abs. 3 S. 1 StPO beinhaltet eine Normierung des

65 *Bodenbenner*, S. 48, 170.
66 *Bodenbenner*, S. 48 f.; *Zöller*, StV 2019, 419 (421, 423).
67 *Bodenbenner*, S. 49; *Zöller*, in: HK-StPO, § 161 Rn. 19.
68 *Bodenbenner*, S. 49.
69 *Bertram*, S. 176.
70 *Singelnstein*, NStZ 2012, 593 (598).
71 *Dochow*, GuP 2020, 129 (133).
72 *Bertram*, S. 108 f.
73 *Singelnstein*, NStZ 2012, 593 (598).
74 *Bodenbenner*, S. 49.
75 *Bertram*, S. 229; *Zöller*, in: HK-StPO, § 161 Rn. 1.

hypothetischen Ersatzeingriffs in bestimmten Fällen.[76] Dieser beschränkt die Verwendung von durch andere Gesetze erlangte personenbezogene Daten zu Beweiszwecken ohne Einwilligung der betroffenen Person. Die Regelung gilt aber allein für Zugriffsmaßnahmen, die nach der StPO nur bei Verdacht bestimmter Straftaten angewendet werden dürfen. Diese Daten dürfen nur zu Strafverfolgungszwecken genutzt werden, wenn die Maßnahme zur Aufklärung der bestimmten Straftat nach den strafprozessualen Regelungen auch hätte angeordnet werden können. Somit öffnet diese Vorschrift die Tür für die Verwendung von Daten im Strafverfahren, die durch außerstrafprozessuale hoheitliche Maßnahmen erhoben wurden.[77] Durch den hypothetischen Ersatzeingriff soll trotz der Zweckänderung dem Zweckbindungsgrundsatz Genüge getan werden.[78] Entscheidend ist, ob nach einer hypothetischen Betrachtung die Daten auf Grund einer entsprechenden Vorschrift der StPO rechtmäßig hätten erhoben werden können.[79] Diese Eingriffsfigur fordert eine entsprechende Maßnahme in einem Gesetz und die reelle Möglichkeit, diese Maßnahme nach der StPO zur Aufklärung einer Katalogtat anzuordnen.[80] Das sich gegenseitig Entsprechen der Maßnahmen bedeutet, dass die personenbezogenen Daten auch nach der StPO mit vergleichbar schwerwiegenden Mitteln hätten erhoben werden dürfen.[81] Es ist nicht erforderlich, dass alle Voraussetzungen der Erhebungsmaßnahmen denen der StPO entsprechen.[82] Für die Möglichkeit der Anordnung reicht der Verdacht bezüglich einer Katalogtat aus.[83] Dabei macht es keinen Unterschied, ob die Daten nach dem anderen Gesetz rechtmäßig oder rechtswidrig erhoben worden sind.[84] Ist § 161 Abs. 3 S. 1 StPO erfüllt, können die erhobenen Daten auch im Strafverfahren als Beweismittel verwendet werden.[85] Diese Rechtsfigur trägt dafür Sorge, dass die strafprozessualen Anordnungsvoraussetzungen nicht umgangen werden.[86] Diese Vorschrift gilt allerdings nur als Beschränkung der Nutzung der Daten als Beweismittel in der Hauptverhandlung gemäß §§ 243 ff. StPO. Sobald die Daten als Spurenansatz oder zu weiteren Ermittlungen benutzt werden, können sie wieder uneingeschränkt nach den Ermittlungsgeneralklauseln verwendet werden.[87] Daher ist die Nutzung der Gästelisten als Ermittlungsansatz ausschließlich nach §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO zu beurteilen. Fraglich bleibt noch, ob § 161 Abs. 3 StPO die Benutzung der Gästelisten als Beweismittel beschränkt. Das Benutzungsverbot gilt jedoch nur für solche Vorschriften, die eine Maßnahme an einen Straftatenkatalog oder bestimmte schwerwiegende Straftaten knüpfen. Sollte dies nicht zutreffen, richtet sich die Datenverwendung wieder nach den allgemeinen Vorschriften der §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO.[88] Diese müssen bei dem Zugriff auf die Gästelisten allein angewendet werden, da es dafür keine vergleichbare Norm der StPO gibt.[89] Die Rechtmäßigkeit des Zugriffs muss daher allein anhand der Verfassungskonformität der §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO und der Verhältnismäßigkeit dieser Ermächtigungsgrundlage im Einzelfall eingeschätzt werden. Daher ist nun zu überprüfen, ob die Generalklauseln die zweckändernde Datennutzung im vorliegenden Fall erlauben. Die §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO bilden nicht nur die Datenerhebungsgeneralklauseln, sondern auch die Zweckänderungsgeneralklauseln. Sie beinhalten daher auch eine Verwendungsermächtigung, durch die bereits

[76] *Bodenbenner*, S. 170.
[77] *Bodenbenner*, S. 177.
[78] *Bodenbenner*, S. 177.
[79] *Bodenbenner*, S. 178.
[80] *Engelhardt*, S. 172.
[81] *Griesbaum*, in: KK-StPO, § 161 Rn. 35a.
[82] *Engelhardt*, S. 185.
[83] *Engelhardt*, S. 200.
[84] *Bodenbenner*, S. 311.
[85] *Engelhardt*, S. 172 f.
[86] *Bertram*, S. 229 f.
[87] *Bodenbenner*, S. 79, 182.
[88] *Zöller*, in: HK-StPO, § 161 Rn. 31.
[89] *Aden/Arzt/Fährmann*, Verstoß gegen den Grundsatz der Zweckbindung.

durch andere Stellen erhobene Daten für ein Strafverfahren übermittelt werden können. Diese dürfen dann aufgrund der Ermächtigung von den Strafverfolgungsbehörden genutzt werden, solange sie rechtmäßig erhoben worden sind.[90] Fraglich ist, ob die Generalklauseln die Anforderungen an eine Zweckänderungsvorschrift erfüllen. Eine Zweckänderungsvorschrift durchbricht den Zweckbindungsgrundsatz und muss daher den neuen Zweck und die zweckentfremdende Datennutzung genau bestimmen.[91] Da die Daten ohne große Einschränkungen durch die §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO generell zweckentfremdet werden dürfen, verstößt diese Auslegung der Norm gegen den Bestimmtheitsgrundsatz und das Verhältnismäßigkeitsprinzip. Eine zweckändernde Verwendung benötigt eine klar bestimmte gesetzliche Erlaubnisnorm.[92] Zudem verstößt dies gegen das Übermaßverbot, da keine Verwendungsvoraussetzungen außer eines Anfangsverdachts vorliegen.[93] Eigentlich müssten an die zweckändernde Verwendung stärkere Anforderungen gestellt werden, da diese den durch die Datenerhebung entstandenen Eingriff vertieft und gleichzeitig einen neuen begründet.[94] Somit muss die Norm an die Intensität des Eingriffs angepasst sein. Dies ist bei den Generalklauseln nicht der Fall. Sie erlauben sogar mehr Datenverwendungen als eigentlich gestattet, da auch Daten verarbeitet werden können, die nach der StPO gar nicht hätten erhoben werden dürfen.[95] Dadurch wird kein genauer Rahmen für die Datenverarbeitung festgelegt. Zudem gibt es außer Absatz 3 keine festgesetzten Grenzen für die Verwendung der Daten. Daher sind die Vorschriften zu unbestimmt und verstoßen gegen das Übermaßverbot.[96] Des Weiteren ist diese Universalerlaubnis bei der Verwendung als Ermittlungsansatz kritisch zu bewerten, da mit dieser meist weitere Grundrechtseingriffe verbunden sind. Die Vorschrift hätte daher besonders ausführlich geregelt werden müssen, um verhältnismäßig zu sein.[97] Somit wird die allgemeine Verfassungsmäßigkeit dieser Generalklauseln im Bezug zur zweckändernden Datennutzung bezweifelt. Um mit den Vorschriften der Verfassung vereinbar zu sein, müssten die Normen konkreter sein und die Verwendung einschränken. Dies hätte durch den hypothetischen Ersatzeingriff geregelt werden können, indem dieser allgemein für die zweckändernde Datenverwendung angewandt wird. So würden klare Grenzen für die Verwendung der Daten gesetzt werden.[98] Ferner kann die Verhältnismäßigkeit direkt im Einzelfall des Zugriffs auf die Gästelisten bezweifelt werden. Bei Gästelisten liegt eine große Streubreite der Maßnahme vor. Daher muss das Interesse, das dem Recht auf informationelle Selbstbestimmung entgegensteht, besonders beachtenswert sein.[99] Zudem kann es in einzelnen Bundesländern vorkommen, dass detaillierte Informationen gespeichert werden.[100] Aus diesem Grund ist das Recht des Bürgers in der Abwägung besonders zu berücksichtigen. Das entgegenstehende Interesse der Strafverfolgung ist allerdings nicht an bestimmte Straftaten gebunden, da die Ermittlungsgeneralklauseln keine Einschränkungen enthalten.[101] Deshalb kann der Zugriff aufgrund jedweder Straftat erfolgen. Gerade jedoch in Fällen kleiner Kriminalität lässt sich ein so intensiver Eingriff in das Grundrecht nicht rechtfertigen.[102] Daher ist der Einsatz der Generalklauseln in manchen Fällen auch im konkreten Einzelfall unverhältnismäßig. Aus diesen Gründen können diese Vorschriften den Zugriff der Strafverfolgungsbehörden auf die Gästelisten nicht rechtfertigen. Wie bereits ausgeführt, benötigt eine Zweckänderungsermächtigung zudem eine Empfangs- und eine Übermittlungsermächtigung. Eine Vorschrift muss die Übermittlung und eine andere den Empfang der Daten erlauben.

90 *Bodenbenner*, S. 169 f.; *Zöller*, StV 2019, 419 (421).
91 *Engelhardt*, S. 219 f.; *Zöller*, StV 2019, 419 (421, 423).
92 *Bodenbenner*, S. 170, 173; *Zöller*, StV 2019, 419 (422).
93 *Bodenbenner*, S. 173.
94 *Bodenbenner*, S. 130 f., 170.
95 *Bodenbenner*, S. 172.
96 *Bodenbenner*, S. 170, 173.
97 *Zöller*, StV 2019, 419 (422).
98 *Bodenbenner*, S. 172 f.; *Zöller*, StV 2019, 419 (423).
99 *Bertram*, S. 108 f.; *Bodenbenner*, S. 173.
100 *Aden/Arzt/Fährmann*, Einleitung.
101 *Bodenbenner*, S. 173.
102 *Hauschild*, in: MüKo-StPO, 2014, § 94 Rn. 24; *Singelnstein*, NStZ 2012, 593 (603).

Nur wenn beides gegeben ist, darf ein solcher Datenaustausch stattfinden. §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO stellen nur die Empfangsermächtigung dar.[103] Die Übermittlungsermächtigungen sind, im Falle der Gästelisten, die Verordnungen der Bundesländer, die das Anfertigen von Gästelisten in der Pandemie regeln. Diese erlauben aber bisher nur die Weitergabe an die Gesundheitsbehörden. Manche Verordnungen verbieten die zweckentfremdende Verarbeitung, andere erlauben explizit nur die Verwendung zur Infektionsnachverfolgung und wieder andere beinhalten keine offensichtlichen Regelungen zu diesem Thema. Außerdem gibt es im Infektionsschutzgesetz keine Regelung zur Verwendung der Daten zu Strafverfolgungszwecken.[104] Daher gibt es keine Übermittlungsermächtigung, die den Zugriff auf die Daten gestatten kann. Aus diesen Gründen lässt sich die zweckändernde Verwendung der Daten durch Zugriff der Strafverfolgungsbehörden auf die Gästelisten nicht durch die Ermittlungsgeneralklauseln der StPO rechtfertigen.

cc) Zusammenfassung

Die Ermittlungsgeneralklauseln sind daher nicht geeignet, den strafprozessualen Zugriff auf Handy-Daten und Gästelisten zu Zeiten der Pandemie zu ermöglichen.

b) Auskunftsrecht von Polizei und Staatsanwaltschaft

Des Weiteren ist fraglich, ob der Zugriff auf die Handy-Daten und Gästelisten nicht auf Grund des Auskunftsrechts der Staatsanwaltschaft und der Polizei erlangt werden kann. Dieses Auskunftsrecht findet sich in den §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO wieder. Die Strafverfolgungsbehörden können hierdurch Ermittlungsanfragen an öffentliche und private Stellen, wie Privatpersonen oder Wirtschaftsunternehmen, stellen. Da durch das Anfragen gegenüber Privatpersonen deren Daten in den öffentlichen Bereich gelangen, liegt für diese ab der Anfrage Grundrechtsbindung vor.[105] Das Auskunftsrecht stellt gegenüber Privatpersonen zudem keine Verpflichtung zur Herausgabe der Daten dar. Von ihnen kann nur verlangt werden, sich vor der Staatsanwaltschaft oder einem Richter als Zeuge zu äußern.[106] Die Handy-Daten liegen beim Besitzer bzw. auf einem Server des Providers vor.[107] Bei den Gästelisten sind sie im Besitz des Geschäftsinhabers.[108] Diese Daten sind somit nicht in den Händen staatlicher Behörden, sondern in denen privater oder nicht öffentlicher Stellen. Daher können die Strafverfolgungsbehörden durch das Auskunftsrecht keinen Zugriff auf die Handy-Daten und Corona-Gästelisten verlangen. Sie können durch dieses Recht nur dann Zugriff auf die Daten erlangen, wenn diese freiwillig herausgegeben werden.[109]

c) Die Beschlagnahme, § 94 StPO

Der Zugriff auf die Handy-Daten und Gästelisten könnte aber durch die formlose Sicherstellung und die Beschlagnahme gemäß § 94 StPO zulässig sein.[110] Diese Vorschrift stellt gegenüber den Generalklauseln und dem Auskunftsrecht eine speziellere Eingriffsbefugnis für den Zugriff auf Daten durch die Strafverfolgungsbehörden dar.[111]

[103] *Zöller*, StV 2019, 419 (421).
[104] *Aden/Arzt/Fährmann*, Verstoß gegen den Grundsatz der Zweckbindung.
[105] *Bodenbenner*, S. 47; *Zöller*, in: HK-StPO, § 161 Rn. 7.
[106] *Singelnstein*, NStZ 2012, 593 (603).
[107] *Dochow*, GuP 2020, 129 (131).
[108] *Aden/Arzt/Fährmann*, Einleitung.
[109] *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (325).
[110] *Gercke*, in: HK-StPO, 6. Aufl. (2019), § 94 Rn. 37.
[111] *Singelnstein*, NStZ 2012, 593 (603).

Sie gestattet die Sicherstellung von Gegenständen, damit sie als Beweis für die Strafverfolgung zur Verfahrenssicherung genutzt werden können.[112] Ein Beweismittel kann jeder körperliche Gegenstand sein, der mittelbar oder unmittelbar einen Beweis für eine Tat oder deren nähere Umstände erbringen kann.[113] Dies bezieht sich nicht nur auf den Beweis in der Hauptverhandlung, sondern auch auf Gegenstände, die als Erkenntnisquellen dienen.[114] Daten können nur über den Datenträger beschlagnahmt werden, da sie für sich allein keine beschlagnahmefähigen körperlichen Gegenstände sind.[115] Erforderlich für die Sicherstellung ist ein bereits eingeleitetes Strafverfahren mit Untersuchung.[116] Dafür muss ein Anfangsverdacht gemäß § 152 Abs. 2 StPO vorliegen.[117] Durch das Legalitätsprinzip sind die Strafverfolgungsbehörden dann verpflichtet, Beweismittel sicherzustellen, sobald ihnen eine potentielle Beweisbedeutung zugewiesen werden kann.[118] Sicherstellung stellt dabei den Oberbegriff für zwei Arten der Herstellung staatlicher Gewalt über den Gegenstand dar. Es gibt die formlose Sicherstellung nach § 94 Abs. 1 StPO und die förmliche Beschlagnahme nach § 94 Abs. 2 StPO.[119] Eine formlose Sicherstellung ist die freiwillige Herausgabe des Gegenstandes durch den Gewahrsamsinhaber. Dabei ist zu beachten, dass die Freiwilligkeit nur vorliegen kann, wenn dem Betroffenen bewusst ist, dass ihn keine Pflicht zur Herausgabe trifft.[120] Eine förmliche Beschlagnahme wird dann benötigt, wenn der Gegenstand nicht freiwillig herausgegeben wird und somit die Sicherstellung erzwungen werden muss.[121] Dann müssen die Formvorschriften des § 98 StPO gewahrt werden.[122] Durch die Wegnahme des Gegenstands wird in grundrechtlich geschützte Positionen eingegriffen.[123] Bei der Weitergabe von Datenträgern werden Daten übermittelt. Wenn Datenträger beschlagnahmt werden, ist daher das Recht auf informationelle Selbstbestimmung betroffen.[124] § 94 StPO stellt hierfür die wegen des Gesetzesvorbehalts notwendige gesetzliche Eingriffsermächtigung dar.[125] Der Paragraph weist jedoch nur geringe Voraussetzungen für einen Eingriff auf, obwohl auch sensible Daten betroffen sein können. Daher müssen im Einzelfall die allgemeinen strafprozessualen und verfassungsrechtlichen Grenzen, wie die Verhältnismäßigkeit, zur Einschränkung der Eingriffsmaßnahme herangezogen werden.[126] So untersteht auch die Beschlagnahme dem Verhältnismäßigkeitsgebot. Dabei muss die Beschlagnahme in einem angemessenen Verhältnis zur Schwere der Tat und zur Stärke des Tatverdachts stehen. Außerdem muss der Gegenstand für die Ermittlungen notwendig sein, da nur so das Übermaßverbot beachtet wird.[127] Ein Eingriff in sensible Daten kann nicht verhältnismäßig sein, sofern nur eine leichte Straftat oder eine geringe Beweisbedeutung vorliegt.[128] Zudem wiegen die betroffenen Rechte der Verletzten bzw. der Unbeteiligten mehr als die des Beschuldigten und es ist zu prüfen, ob nicht ein milderes Mittel, wie die formlose Sicherstellung, für den Zugriff angewendet werden kann.[129] Es muss demnach stets eine umfassende Abwägung der Interessen erfolgen. Dabei stehen sich die funktionstüchtige Strafrechtspflege und in diesem Fall das Recht auf informationelle Selbstbestimmung mit Berücksichtigung der Intensität ihrer Beeinträchtigung gegenüber.[130] Bei der formlosen Sicherstellung ist dies unbeachtlich, da bei einer freiwilligen Einwilligung keine

112 *Gercke*, in: HK-StPO, § 94 Rn. 1, 2.
113 *Gercke*, in: HK-StPO, § 94 Rn. 6, 8.
114 *Gercke*, in: HK-StPO, § 94 Rn. 7.
115 *Gercke*, in: HK-StPO, § 94 Rn. 18.
116 *Gercke*, in: HK-StPO, § 94 Rn. 29.
117 *Gercke*, in: HK-StPO, § 94 Rn. 31.
118 *Gercke*, in: HK-StPO, § 94 Rn. 35.
119 *Gercke*, in: HK-StPO, § 94 Rn. 37, 42.
120 *Gercke*, in: HK-StPO, § 94 Rn. 39, 40.
121 *Gercke*, in: HK-StPO, § 94 Rn. 42.
122 *Kipker/Voskamp*, ZD 2013, 119 (120).
123 *Hauschild*, in: MüKo-StPO, § 94 Rn. 2.
124 *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (332).
125 *Hauschild*, in: MüKo-StPO, § 94 Rn. 2.
126 *Singelnstein*, NStZ 2012, 593 (597).
127 *Burhoff*, Handbuch für das strafrechtliche Ermittlungsverfahren, 8. Aufl. (2019), Rn. 986, 987; *Hauschild*, in: MüKo-StPO, § 94 Rn. 23.
128 *Singelnstein*, NStZ 2012, 593 (597).
129 *Burhoff*, Rn. 988, 990; *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (331).
130 *Gercke*, in: HK-StPO, § 94 Rn. 52.

solche Prüfung stattfindet, da der Eingriff erlaubt wird.[131] Liegt jedoch bei der Beschlagnahme ein Verstoß gegen das Verhältnismäßigkeitsgebot vor, dann führt dies zu einem Beschlagnahmeverbot.[132] Daher ist bei der Verhältnismäßigkeit eines Zugriffs nach § 94 StPO auf die Handy-Daten und die Gästelisten in Zeiten der Pandemie die Unterscheidung dieser zwei Arten der Sicherstellung besonders wichtig. Bei der formlosen Weitergabe des Datenträgers kommt es nur darauf an, dass dies durch eine freiwillige Einwilligung geschieht. Dies setzt voraus, dass die Einwilligung mit den Zielen der Ermächtigung übereinstimmt, zur Erreichung dieser Ziele geeignet ist, der Gewahrsamsinhaber dispositionsbefugt ist und dass Freiwilligkeit vorliegt.[133] Der Inhaber ist dabei dispositionsbefugt, die Daten des Kunden herauszugeben, da dieser bei Beweisbedeutung des Datenträgers dies dulden muss.[134] Die formlose Sicherstellung stellt also lediglich einen Realakt dar, der keine Anordnungsbefugnis benötigt.[135] Bei einer förmlichen Beschlagnahme sind die Vorschriften des § 98 StPO zu beachten, welcher eine formelle Anordnung durch einen Richter beinhaltet. Diese muss die zu beschlagnahmenden Gegenstände bestimmt genug bezeichnen, den Beschlagnahmezweck aufzeigen und aktenkundig gemacht werden.[136] Dabei muss sie inhaltlich so konkretisiert sein, dass der Eingriff messbar und kontrollierbar bleibt und kein Zweifel bezüglich des Umfangs der Maßnahme aufkommen kann.[137] Zudem sind die Person des Beschuldigten, der Sachverhalt, der Strafbarkeitsvorwurf, der Tatverdacht und die Stellung des Gegenstands als Beweismittel in die Anordnung aufzunehmen.[138] Dieser Richtervorbehalt des § 98 Abs. 1 StPO dient der Kontrolle des staatsanwaltschaftlichen Grundrechtseingriffs.[139] Wegen des Grundrechtseingriffs fordert das Verfassungsrecht daher eine Verhältnismäßigkeitsprüfung im Rahmen der Anordnung.[140] Aufgrund dieser Unterschiede im Sicherstellungsverfahren ist die Verfassungsmäßigkeit, gerade wenn es um die Daten Dritter geht, in den Fällen der formlosen Sicherstellung und der förmlichen Beschlagnahme unterschiedlich zu bewerten. Dies wird im Folgenden anhand der Anwendbarkeit der §§ 94 ff. StPO in den Fällen des Zugriffs auf Handy-Daten und Gästelisten erläutert.

aa) Handy-Daten

Wie bereits erörtert, sind beim Zugriff auf die Handy-Daten zu Zeiten der Pandemie sensible Gesundheitsdaten betroffen. Daher muss der Eingriff besonders gerechtfertigt sein. Wenn die Daten direkt beim Besitzer des Mobiltelefons erhoben werden, wäre eine formlose Sicherstellung denkbar. Zwar wird auch hier der Zweck der Datenverarbeitung verändert, aber der Inhaber wird darüber informiert. Er weiß somit, was mit seinen Daten geschieht und kann durch eine Einwilligung den Eingriff in sein Grundrecht erlauben.[141] Bei einer förmlichen Beschlagnahme kann sich der Betroffene gegen die Datenerhebung nicht wehren. Ihm wird aber durch die Anordnung mitgeteilt, aus welchen Gründen seine Daten erhoben und wie sie genutzt werden. Außerdem wird vor dem Zugriff die Lage von einem Richter überprüft. Da dieser auch die Frage der Verhältnismäßigkeit mitberücksichtigen muss, wird für die Verhältnismäßigkeit von Maßnahme und Eingriff Sorge getragen.[142] Sollte im konkreten Einzelfall das Interesse des Betroffenen überwiegen, kann der Richter den Zugriff verbieten. Zudem wird der Betroffene

131 *Gercke*, in: HK-StPO, § 94 Rn. 39; *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (339).
132 *Park*, Durchsuchung und Beschlagnahme, 4. Aufl. (2018), § 3 Rn. 638.
133 *Gercke*, in: HK-StPO, § 94 Rn. 39; *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (339, 341).
134 *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (343).
135 *Hauschild*, in: MüKo-StPO, § 94 Rn. 43.
136 *Gercke*, in: HK-StPO, § 98 Rn. 1, 4; *Kipker/Voskamp*, ZD 2013, 119 (120).
137 *Gercke*, in: HK-StPO, § 98 Rn. 15.
138 *Park*, § 3 Rn. 481, 483, 484, 488.
139 *Park*, § 3 Rn. 476.
140 *Burhoff*, Rn. 835.
141 *Kipker/Voskamp*, ZD 2013, 119 (120); *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (339).
142 *Burhoff*, Rn. 835; *Gercke*, in: HK-StPO, § 94 Rn. 42, § 98 Rn. 4.

rechtlich angehört.[143] Daher ist der Zugriff auf die Handy-Daten durch die förmliche Beschlagnahme beim Betroffenen verfassungsgemäß. Fraglich ist allerdings, ob auch der Zugriff auf Daten beim Serverprovider verhältnismäßig ist, da der Betroffene nicht in das Geschehen der zweckändernden Datenverarbeitung eingebunden ist. Bei der formlosen Sicherstellung würde die Einwilligung des Providers ausreichen, um die zweckändernde Datenverarbeitung zu erlauben.[144] Somit wären in einem solchen Fall keine weiteren Anforderungen als die Einwilligung und ein Anfangsverdacht nötig, um einen strafprozessualen Zugriff auf sensible Daten eines Dritten zu erlauben.[145] Diese Situation gleicht daher dem Zugriff durch die Ermittlungsgeneralklauseln, vor allem, da die Beweismittel auch als Ermittlungsansatz genutzt werden können. Die drei Vorschriften haben nur den Anfangsverdacht als Einschränkung bzw. als Voraussetzung und erlauben fast jeglichen Eingriff. Sie geben weder einen bestimmten Rahmen noch Grenzen für die Datenverarbeitung vor. Wenn schon bei den Ermittlungsgeneralklauseln die Verfassungskonformität eines solchen Eingriffs bestritten wird, dann ist dies auch hier der Fall. Daran ändert auch die Voraussetzung der Einwilligung nichts, da diese nicht von der Person kommt, deren Daten betroffen sind. Aus diesen Gründen verstößt eine formlose Sicherstellung in diesem Fall gegen Bestimmtheitsgebot und Übermaßverbot. Der Zugriff könnte aber durch die förmliche Beschlagnahme zulässig sein. Dabei liegt eine richterliche Anordnung vor.[146] Die förmliche Beschlagnahme benennt die genauen Umstände des Zugriffs und der Verwendung in einem bestimmten Verfahren und benötigt eine Verhältnismäßigkeitsprüfung eines Richters.[147] Somit ist diese bestimmter als die formlose Sicherstellung und die Ermittlungsgeneralklauseln, da die Datenverwendung durch die Zustimmungsbedürftigkeit eingegrenzt wird. So können das geforderte Übermaßverbot, Bestimmtheitsgebot und der Zweckbindungsgrundsatz bei der Zweckänderung eingehalten werden.[148] Somit ist die zweckändernde Datenverwendung verfassungsgemäß, nicht zuletzt da dem Betroffenen nach der Beschlagnahme gemäß § 33 Abs. 3 StPO rechtliches Gehör gewährt werden muss.[149] So wird nochmals sichergestellt, dass der Bürger über die Verwendung seiner Daten Kenntnis hat und dass der Zugriff rechtmäßig ist. Daher kann eine förmliche Beschlagnahme den Zugriff auf die Handy-Daten beim Provider erlauben. Dennoch gibt es noch ein weiteres Kriterium der zweckändernden Datenverwendung, das vom *BVerfG* gefordert wird: die Öffnungsklausel. Wie bereits festgestellt, fehlt eine solche im Infektionsschutzgesetz, welches das Erheben von Gesundheitsdaten während einer Pandemie erlaubt. Nur wenn eine solche Klausel hinzugefügt wird, kann die Datenübermittlung gestattet werden.[150]

bb) Gästelisten

Die Gästelisten, die zur Überwachung der Infektionsketten erstellt werden müssen, befinden sich ausschließlich bei den Betreibern der Geschäfte.[151] Daher kann keine Anfrage zur Herausgabe an den in seinen Grundrechten betroffenen Dritten gestellt werden. Demnach folgen dieselben Überlegungen wie beim Zugriff auf die Handy-Daten beim Provider. Ohne die Anordnung durch einen Richter und die Anhörung des Dritten kann die formlose zweckändernde Sicherstellung der Daten nicht gerechtfertigt werden. Sie ist auch in diesem Kontext zu unbestimmt und verstößt gegen das Übermaßverbot. Wie vorher ausgeführt, kann daher nur die förmliche Beschlagnahme die verfassungsrechtlichen Anforderungen erfüllen, da die Anordnung bestimmt genug ist, Grenzen setzt

143 *Burhoff*, Rn. 835; *Singelnstein*, NStZ 2012, 593 (598).
144 *Radtke*, in: FS Meyer-Goßner, 2001, S. 321 (339, 343).
145 *Gercke*, in: HK-StPO, § 94 Rn. 31; *Singelnstein*, NStZ 2012, 593 (597, 598).
146 *Gercke*, in: HK-StPO, § 98 Rn. 1, 4.
147 *Burhoff*, Rn. 835; *Park*, § 3, Rn. 481, 483, 484, 488.
148 *Bodenbenner*, S. 49, 69; *Zöller*, in: HK-StPO, § 161 Rn. 19.
149 *Singelnstein*, NStZ 2012, 593 (598).
150 *Aden/Arzt/Fährmann*, Verstoß gegen den Grundsatz der Zweckbindung.
151 *Aden/Arzt/Fährmann*, Einleitung, Verstoß gegen den Grundsatz der Zweckbindung.

und das Verhältnismäßigkeitsgebot eingehalten wird. Die §§ 94 Abs. 2, 98 Abs. 1 StPO kommen also auch in den Fällen der Gästelisten als Ermächtigungsgrundlage in Betracht. Bei Gästelisten liegt jedoch eine große Streubreite der Maßnahme vor und es werden zum Teil viele Daten des Bürgers aufgezeichnet. Daher muss das Interesse der Bürger in der Abwägung stärker beachtet werden.[152] So kann der Richter in der Verhältnismäßigkeitsprüfung zum Ergebnis kommen, dass die Anwendung der Vorschrift im konkreten Einzelfall unverhältnismäßig ist. Abschließend kann nochmals angefügt werden, dass auch beim Zugriff auf Gästelisten die Öffnungsklausel in den Pandemie-Verordnungen fehlt. Erst wenn eine solche in den Verordnungen vorhanden ist, kann der Zugriff gestattet werden. Nur wenn der Dritte bei seiner rechtlichen Anhörung den Zugriff erlaubt, kann dieses Problem durch den Grundrechtsverzicht umgangen werden.

cc) Zusammenfassung

Da eine Öffnungsklausel in den Gesetzen fehlt, kann nur die freiwillige Aufgabe des Grundrechtsschutzes den Zugriff auf die personenbezogenen Daten rechtfertigen. Wäre eine solche Klausel gegeben, dann könnte ein rechtmäßiger strafprozessualer Zugriff in Form der förmlichen Beschlagnahme auf die Handy-Daten und die Gästelisten erfolgen.

d) Zwischenergebnis

Nachdem nun die möglichen Eingriffsermächtigungen der StPO untersucht worden sind, lässt sich feststellen: Der zweckverändernde strafprozessuale Zugriff auf die zur Pandemiebekämpfung erhobenen Daten lässt sich nur nach den §§ 94, 98 Abs. 1 StPO rechtfertigen. Die anderen Regelungen sind zum einen für die Datenerhebungen in den konkreten Fällen zu ungenau und nicht verhältnismäßig und zum anderen fehlt es an der Öffnungsklausel in den notwendigen Gesetzen. Daher ist ein Datenzugriff nur in wenigen Fällen möglich. Dies kann unter anderem behoben werden, indem eine Öffnungsklausel in den entsprechenden Gesetzen eingefügt wird. Zukünftige, ähnliche Konfliktlagen können aber nur gelöst werden, wenn der Gesetzgeber die Regelungen für die allgemeine und zweckändernde Datenverwendung der Strafverfolgungsbehörden den Anforderungen des Verfassungsrechts anpasst.

5. Die Bedeutung des rechtswidrigen Zugriffs für die Verwertbarkeit der Daten

Wie ausgeführt, haben die Strafverfolgungsbehörden in den konkreten Fällen meist keine Zugriffserlaubnis für die Daten besessen. Daher muss nun die Frage gestellt werden, ob die Daten, die ohne gültige Ermächtigung erhoben worden sind, dennoch als Beweismittel im Strafverfahren genutzt werden dürfen. Denn nicht jeder Verstoß gegen eine Beweiserhebungsvorschrift oder ein Datenverwendungsverbot führt automatisch zu einem strafprozessualen Verwertungsverbot. Dies ist immer nach den Umständen des Einzelfalls zu bewerten, wenn eine ausdrückliche Vorschrift oder übergeordnete, gewichtige Gründe ein solches Verbot verlangen.[153] In diesen Fällen dürfen die Daten nicht für die Beweiswürdigung und die Entscheidungsfindung verwendet werden.[154] Im Falle der §§ 161 Abs. 1 S. 1, 163 Abs. 1 S. 2 StPO könnte ein Verstoß gegen ein Datenverwendungsverbot vorliegen, denn sie sind nicht dafür geeignet, die zweckändernde Datennutzung in den Fällen des Zugriffs auf die Handy-Daten

[152] *Bertram*, S. 108 f.; *Singelnstein*, NStZ 2012, 593 (597).
[153] *Eisenberg*, Beweisrecht der StPO, 10. Aufl. (2017), Rn. 335; *Hauschild*, in: MüKo-StPO, § 94 Rn. 57, 58.
[154] *Eisenberg*, Rn. 356.

und Gästelisten zu gestatten. Datenverwendungsverbote sperren die weitere Verarbeitung der Daten. Daher führen sie automatisch auch zu dem Verbot, die Daten als Beweismittel oder als Ermittlungsansatz zu nutzen.[155] Ein Datenverwendungsverbot kann aus dem Verfassungsrecht und dem einfachen Recht abgeleitet werden. Da eine Datenverwendung eine verfassungsrechtliche Legitimation benötigt, wird eine nicht legitimierte Datenverwendung wie ein ausdrückliches Verbot gewertet.[156] Da die Ermittlungsgeneralklauseln nicht geeignet sind, die zweckändernde Nutzung der Handy-Daten und Gästelisten für die Strafverfolgung zu rechtfertigen, wären die Daten nicht legitim erlangt worden. Dies verbietet ihre Verwendung und damit auch ihre Verwertung. Fraglich ist noch, wie die §§ 94, 98 StPO dies regeln. Wenn gegen die Verfassung verstoßen wird, leitet sich aus diesem Verstoß ein Verwertungsverbot für den sichergestellten Gegenstand ab.[157] Der Verhältnismäßigkeitsgrundsatz begründet dabei ein Beweisverwertungsverbot, wenn die Vorgaben des *BVerfG* nicht eingehalten werden.[158] Beim Zugriff auf die Handy-Daten und Gästelisten ist das Erfordernis der Öffnungsklausel nicht eingehalten und zum Teil gegen das Bestimmtheitsgebot und Übermaßverbot verstoßen worden. Daher liegt ein Beweisverwertungsverbot vor. Aus diesen Gründen können die rechtswidrig erlangten Daten nicht als Beweismittel oder Ermittlungsansatz eingesetzt werden.

III. Appell und Lösungsvorschläge

Abschließend lässt sich feststellen: Die vorliegenden Vorschriften würden grundsätzlich ohne nähere Überprüfung den Zugriff auf die zur Pandemiebekämpfung erhobenen Daten erlauben. Zieht man jedoch die notwendigen verfassungsrechtlichen Anforderungen heran, kann festgestellt werden, dass die strafprozessualen Vorschriften hinsichtlich der zweckändernden Datenverarbeitung diesen Ansprüchen beim Zugriff auf Handy-Daten und Gästelisten meist nicht genügen. Dies kann der Bürger als Laie aber nicht vorhersehen. Um daher Klarheit zu schaffen und Unmut in der Bevölkerung zu vermeiden, muss eine klare Stellungnahme erfolgen. Ein guter Anfang wäre dabei, Transparenz zu ermöglichen. Der Grundrechtseingriff wäre geringer, wenn der Bürger weiß, wie seine Daten verarbeitet werden können und wie er sich dagegen wehren kann. Das verpflichtende Anzeigen einer Rechtsbelehrung beim Herunterladen der Corona-Warn-App oder auf der Gästeliste würde hierzu einen großen Beitrag leisten. Letztendlich müsste aber der Gesetzgeber Öffnungsklauseln in den Vorschriften ergänzen und die strafprozessualen Normen den Anforderungen des *BVerfG* anpassen.

[155] *Bodenbenner*, S. 224.
[156] *Bodenbenner*, S. 226 f.
[157] *Gercke*, in: HK-StPO, § 94 Rn. 61.
[158] *Burhoff*, Rn. 915.