

Recht auf Datenschutz des Einzelnen überwiegt nicht Recht auf Leben Dritter

Tracking von Verkehrsdaten von Corona-Infizierten zur Seuchenabwehr aus Art. 6 lit d) DSGVO -

Keine Gesetzesänderung erforderlich

31.03.2020

RA Dr. Peter Schmitz, JUCONOMY Rechtsanwälte (Düsseldorf)

In der aktuellen Diskussion wird übersehen, dass es mit Art. 6 Abs. 1 lit d) DS-GVO bereits einen verordnungsrechtlichen und gesetzlichen klar definierten Eingriffstatbestand zum Tracking Infizierter gibt, der verhältnismäßig angewendet werden kann (siehe auch Erwägungsgrund 46). Für den speziellen Fall der Seuchenabwehr nach Art. 6 Abs. 1 lit d) DS-GVO bei Gefahr für Leben und Gesundheit besteht nach Art. 94, 95 DS-GVO und der Rechtsprechung des EuGH keine Sperre durch die nach der ePrivacy-Richtlinie und dem TKG fehlende ausdrückliche Verarbeitungserlaubnis, denn diese Fälle sind dort nicht geregelt. Hierbei regelt die DS-GVO ausdrücklich auch die Verarbeitung von TK-Daten soweit die EPR keine Sonderregelungen trifft, siehe Erwägungsgrund 49 sowie Art. 94, 95 sowie den Seuchenschutz (siehe Erwägungsgrund 49), so dass auch dem Gesetzesvorbehalt des Art. 10 GG sowie Art. 52 der Charta der Grundrechte genügt wird. Das Recht auf Datenschutz und dem Fernmeldegeheimnis ist nicht grenzenlos gewährt, sondern ist auf Basis von Art. 6 Abs. 1 lit) d DS-GVO mit den anderen Rechtsgütern abzuwägen. Das Rechtsgut des Datenschutzes eines Einzelnen überwiegt hierbei nicht das Recht auf Leben und Gesundheit der anderen. Tracking von potenziell Infizierten ist damit auch ohne die Einwilligung der Betroffenen und ohne Anonymisierung durch die Seuchenschutzbehörden zur konkreten Abwehr einer großen Seuchengefahr zulässig. Die Vorgaben zu Sicherheit und Verfahren werden – jedenfalls in dieser besonderen Situation und wegen Gefahr in Verzug – durch die Vorgaben der DS-GVO und des TKG eingehalten.

Erwägungsgrund 46 2. Satz DS-GVO:

*„Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein **lebenswichtiges Interesse** der betroffenen Person oder **einer anderen natürlichen Person zu schützen**. Personenbezogene Daten sollten grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. Einige Arten der Verarbeitung können sowohl wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen; so kann beispielsweise die Verarbeitung für **humanitäre Zwecke einschließlich der Überwachung***

*von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen **erforderlich** sein.“*

1. Die **Beispiele der Seuchenbekämpfung in Südkorea und Malaysia** zeigen, dass es auch ohne generelle Ausgangssperren möglich ist, die weitere nationale Ausbreitung von Corona einzudämmen. Diese **Eindämmung** erscheint nach diesen Beispielen aber nur möglich, wenn **statt der generellen Ausgangs- oder Kontaktsperre im Gegenzug sehr umfassend auf eine Infektion getestet wird und im Falle eines positiven Befundes die zuständigen Seuchenschutzbehörden die Befugnis haben, die Verkehrs- und Bewegungsdaten der Infizierten rückwirkend für die letzten 14 Tage auszuwerten** (siehe z.B. <https://www.faz.net/aktuell/wirtschaft/kampf-gegen-corona-ein-weg-zurueck-zur-normalitaet-16697986.html>, 27.03.2020). Hierdurch sollen weitere potenziell Infizierte erkannt werden, um diese ebenfalls zu testen und in Quarantäne zu setzen, um die Infektionsketten zu durchbrechen. Diese Annahme wird folgend juristisch zugrunde gelegt, da eine gewisse Evidenz dafürspricht. Ob dies tatsächlich der Fall ist, sollte wissenschaftlich weiter untersucht und vertieft werden. Im Wege der Abwehr massiver Gefahren für die Leben und Gesundheit der gesamten Bevölkerung bedarf diese Evidenz aber keiner abschließenden Gewissheit, sondern nur plausibler Wahrscheinlichkeit (siehe unten Ziffer 4).

2. Die **Weitergabe von Verkehrsdaten sowie Bestandsdaten durch die Mobilfunknetzbetreiber an die zuständige Seuchenschutzbehörde und die Auswertung dieser Daten durch die Seuchenschutzbehörde zum Zwecke der Eindämmung der Corona-Pandemie ist nach Art. 6 Abs. 1 lit d) DS-GVO i.V.m. Art. ePrivacy-Richtlinie 2002/58/EG (EPR) rechtmäßig. Einer Änderung der nationalen Gesetze, der DS-GVO oder der EPR oder der Seuchenschutzgesetze bedarf es nicht.**
 - a. Weder das (nationale) TKG, noch die nach Art. 95 DS-GVO weiterhin anwendbare EPR sehen ausdrücklich die Berechtigung vor, die Verkehrsdaten der Telekommunikation für die o.g. Zwecke zu verarbeiten. Diese Vorschriften basieren noch auf der damals geltenden allgemeinen Datenschutzrichtlinie 95/46/EG (DSR). Der EuGH hat mit Ur. v. 19.10.2017 (C-582/14) entschieden, dass es Art. 7 lit f) der DSR erfordert, dass eine Abwägung der Verarbeitung immer möglich sein muss, auch wenn die umsetzenden nationalen Gesetze dies nicht ausdrücklich vorsehen. Deshalb hat der EuGH entschieden, dass die Verarbeitung von IP-Adressen bei der Webseiten-Nutzung zu Zwecke der Sicherheit rechtmäßig ist, wenn die Sicherheit dies gebietet und das Interesse an einer Verarbeitung die Interessen des Nutzers, dass eine solche Verarbeitung unterbleibt, überwiegt. Der BGH (Ur. v. 16.05.2017 – VI ZR 135/17) hat im Falle der IP-Adressen bestätigt, dass dies bei der Verarbeitung von IP-Adressen zur

Aufklärung und Verhinderung konkreter Sicherheitsangriffe auf die Webseite der Fall ist. Hervorzuheben ist, dass es hierbei um die Speicherung und Auswertung aller IP-Adressen ging, während die Angriffe nur von bestimmten IP-Adressen ausgingen (siehe in der Literatur z.B. Spindler/Schmitz, TMG. 2. A, § 15, Rn. 134 ff.).

- b. Die **EPR und das deutsche TKG bilden im Ergebnis keine Sperre für die Verarbeitung der Verkehrsdaten**, wenn diese nach **Art. 6 Abs. 1 lit d.) DS-GVO** erforderlich ist, um „lebenswichtige Interessen einer anderen natürlichen Person zu schützen“.
- i. Zunächst besagt schon die **Übergangsregelung des Art. 95 DS-GVO**, dass die TK-Anbieter keinen weiteren Pflichten als jenen, die speziell mit dem gleichen Ziel in der EPR geregelt sind, unterliegen. Deshalb ist der Verarbeitungstatbestand des Art. 6 Abs. 1 lit d) DS-GVO nach Art. 95 DS-GVO durch Art. 6 EPR **nicht gesperrt**, denn für die Seuchenbekämpfung und Gefahrenabwehr für Leben und Gesundheit enthält die **EPR** anders als Art. 6 DS-GVO gerade **keine speziellen Regelungen, Art. 6 Abs. 1 lit d) DS-GVO ist deshalb in diesem speziellen Fall ohne Einschränkungen auch auf die Mobilfunkdaten anwendbar**.
- ii. Aus der **Rechtsprechung des EUGH** und Art. 94 Abs. 2 DS-GVO folgt zudem, dass selbst unabhängig von einer klaren gesetzlichen Regelung der übergeordnete Abwägungsgrundsatz aus der ehemaligen DSR auch für die „Nachfolgeregelung“ in **Art. 6 Abs. 1 lit d) DS-GVO** gilt. Hiernach ist eine Verarbeitung von personenbezogenen Daten erlaubt, wenn dies erforderlich ist, um „lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen“. Diese Erlaubnis sind auch in die EPR und das TKG ordnungskonform hineinzulesen, wie es der EUGH bei dem deutschen TMG und der DSR angenommen hat. Erwägungsgrund 46 der DS-GVO bestärkt dies ausdrücklich.
- c. Die **Verarbeitung ist für den Schutz von Leben und Gesundheit** von noch nicht infizierten Personen nach der unter 1) genannten Annahme nach **Art. 6 Abs. 1 lit d) DS-GVO erforderlich im engeren Sinne und angemessen im weiteren Sinne**. Denn ohne diese Verarbeitung lassen sich die Kontaktpersonen, die dem Infizierten möglicherweise selbst bei dem Willen zur eigenen Benennung namentlich nicht bekannt sind, gerade im öffentlichen Bereich nicht ausreichend ermitteln. Diese Ermittlung ist aber erforderlich, um

die Infektionskette zu unterbrechen und weitere Personen somit vor einer potenziell lebensbedrohlichen Ansteckung mit Coronaviren zu bewahren.

- d. Die **Abwägung** unter dem allgemeinen Grundsatz der Verhältnismäßigkeit geht **zugunsten der Verarbeitung der Mobilfunkstandortdaten des Infizierten** aus. Denn die Gefahrenabwehr zugunsten des Lebens anderer sowie das gesellschaftliche Interesse der Seucheneindämmung überwiegen das Interesse des Einzelnen, dass seine Verkehrswege und Kontakte der letzten 14 Tage nicht der Seuchenschutzbehörde bekannt werden. Die Eindämmung einer Epidemie ist von Erwägungsgrund 46 der DS-GVO ausdrücklich als rechtmäßiger Verarbeitungszweck anerkannt. Zwar wiegt das Interesse des Einzelnen an der Vertraulichkeit seiner Aufenthaltsorte und Kontaktpersonen sehr hoch und das für den Zeitraum der Inkubation erstellte Bewegungsprofil greift schwerwiegend in das Recht auf informationelle Selbstbestimmung bzw. das Recht auf Datenschutz ein. Das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG) oder Art. 7 der Charta der Grundrechte der EU sind jedoch nicht grenzenlos gewährt, sondern es sind auch die Rechte der anderen Bürger auf Gesundheit und Leben abzuwägen. Dies entspricht auch der anerkannten Rechtsprechung des BVerfG, wie sie grundlegend im Volkszählungsurteil (BVerfGE 65 ff.) begründet wurde. Das Recht auf Leben und Gesundheit der Personen, die noch nicht infiziert sind und mit dem Tracking vor einer Infektion bewahrt werden können, wiegt aber höher. Denn das Recht auf Datenschutz des Einzelnen steht nicht über dem Recht auf Leben und Gesundheit der anderen. Der Einzelne muss grundsätzlich Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen, soweit es jedenfalls nicht den letzten „unantastbaren Bereich privater Lebensgestaltung“ betrifft, wie höchstprivate Tagebucheintragungen. Einschränkungsmöglichkeiten hat das BVerfG z.B. insbesondere dann angenommen, wenn – wie vorliegend – „der einzelne als in der Gemeinschaft lebender Bürger in Kommunikation mit anderen tritt, durch sein Verhalten auf andere einwirkt und dadurch die persönliche Sphäre seiner Mitmenschen oder die Belange der Gemeinschaft berührt“ (BVerfGE 80, 367, 373). Es ist anerkannt, dass die Mobilfunkdaten zwar dem Fernmeldegeheimnis unterliegen, aber verhältnismäßigen Eingriffsmöglichkeiten unterliegen.
- e. Nach der deutschen Gesetzgebung ist es allerdings erforderlich, dass Eingriffe in Art. 10 GG (**Fernmeldegeheimnis**) dem sog. **Gesetzesvorbehalt** und **Zitiergebot** unterliegen und „nur aufgrund eines Gesetzes angeordnet werden“, siehe auch Art. 52 der Charta der Grundrechte. Art. 6 Abs. 1 lit d) DS-GVO i.V.m. Art. 94, 95 DS-GVO ist ein solches „Gesetz“, denn die DS-GVO regelt hiernach ausdrücklich auch die Verarbeitung von Daten der Telekommunikation

(siehe Erwägungsgrund 49 sowie Art. 94 und 95 DS-GVO sowie Erwägungsgrund 46 zur Eindämmung einer Epidemie) und die DS-GVO ist direkt anwendbares Recht in Deutschland.

3. Die **Angemessenheit der Maßnahmen** auf Basis der „gesetzlichen“ Grundlage von Art. 6 Abs. 1 lit d) DS-GVO i.V.m. §§ 97 ff. TKG in verordnungskonformer Auslegung bestätigt sich auch im **Vergleich zu anderen erlaubten Zwecken**.
 - a. Wenn eine Auswertung der Standortdaten von – auch unbeteiligten - Mobilfunkkunden erlaubt und angemessen ist, um z.B. eine schwere räuberische Erpressung oder Mord aufzuklären, dann ist dies auch angemessen, um das Leben und die Gesundheit von Bürgern vor einer ganz konkreten und lebensgefährlichen Bedrohung durch Corona zu schützen. Im Übrigen bestätigt auch die Wertung von § 100e Abs. 6 Nr. 2 StPO, dass eine Verwendung von (bereits erhobenen) Verkehrsdaten „zur Abwehr einer im Einzelfall bestehenden Lebensgefahr oder einer dringenden Gefahr für Leib oder Freiheit einer Person“ möglich ist.
 - b. Wenn der EuGH und BGH es erlauben, dass IP-Daten von Webseiten zur konkreten Abwehr von Sicherheitsverletzungen verarbeitet werden, obwohl dies im TMG nicht vorgesehen aber in der DSR angelegt war, dann sind auch Mobilfunkstandortdaten zu verarbeiten, wenn es der Schutz von Menschenleben erfordert um eine große und konkrete Gefahr durch die Corona-Seuche abzuwehren und in Art. 6 Abs. 1 lit d) DS-GVO vorgesehen ist.
 - c. Der EuGH (C-203/15) hat zur „Vorratsdatenspeicherung“ entschieden, dass ein besonderer Anlass und Rechtfertigung für eine solche Speicherung und Übermittlung an die Behörden, die schwer in das Grundrecht auf Datenschutz eingreift, gegeben sein muss (siehe Rn. 102). Vorliegend liegt diese besondere Rechtfertigung und der besondere Anlass in der Bedrohung des Lebens durch Corona, bei welcher jeder potenziell gefährdet ist oder durch eine Infizierung auch Gefährder sein kann. Diese Datenverarbeitung bleibt – anders als die bisherige Vorratspeicherung - auf diesen besonderen Anlass und Zweck beschränkt. Zudem werden nur die ohnehin vorhandenen Daten beauskunftet, es werden keine zusätzlichen „Vorratsdaten“ erhoben.
 - d. Hierdurch entsteht auch **kein übermäßiger „Überwachungsstaat“**, weil der **Zweck der Seuchenabwehr** auf die sehr spezielle und konkrete Gefahrenlage

für Leib und Leben begrenzt ist und allein hieraus seine Rechtfertigung erfährt. Es geht auch nicht um Repression und Überwachung als Zweck, sondern um **Gefahrenabwehr** für Leib und Leben, siehe Erwägungsgrund 46 der DS-GVO.

4. Für die **Frage der Verhältnismäßigkeit** ist die Frage zu stellen, **wie weit es der Gewissheit** bedarf, dass die Maßnahmen geeignet sind. Da es um einen **Eingriff zur Gefahrenabwehr** und nicht um die repressive Überwachung von Bürgern geht und der potenzielle Schaden mit vielen Toten sehr hoch ist, reicht hierfür die durch die Beispiele von Südkorea und Malaysia belegte **Wahrscheinlichkeit**. Zudem ist es plausibel und entspricht gängiger Praxis bei der Seuchenbekämpfung, Infizierte und deren Kontaktpersonen zu ermitteln. Es wäre nicht plausibel und könnte ein **pflichtwidriges Unterlassen** darstellen, warum der Staat, der zum Schutz seiner Bürger verpflichtet ist, hierfür nicht die verfügbaren und gesetzmäßig vorhandenen Maßnahmen ergreifen darf und muss.
5. Die **Frage der Verhältnismäßigkeit** stellt sich auch für die **Mobilfunkanbieter**, welche die Standortdaten und ggf. die Bestandsdaten an die Seuchenschutzbehörden übermitteln müssen. Hierfür gibt es allerdings bereits technische Wege nach §§ 112, 113 TKG nebst einer angemessenen Erstattung des Aufwands nach § 23 JVEG.
6. Das Erfordernis, **Garantien für wirksamen Schutz** der Daten vor Missbrauchsrisiken vorzusehen, ist i.E. erfüllt. Die TK-Unternehmen unterliegen bereits den Regeln zur Sicherheit nach § 109a TKG sowie ergänzend (z.B. Bestandsdaten) nach Art. 32 DS-GVO. Auf Seiten der empfangenden Behörden bestehen die Vorgaben aus Art. 32 DS-GVO.
7. Das Auslesen bzw. Anfordern der Verkehrsdaten müsste allerdings im Normalfall einer **richterlichen Kontrolle** oder der Kontrolle einer unabhängigen Behörde unterliegen. Der EuGH hat aber geurteilt, dass in **hinreichend begründeten Eilfällen** hierauf verzichtet werden kann (C-203/15, Rn. 120). Ein solcher Eilfall liegt unter zwei Gesichtspunkten vor: Zum einen müssten erst die Kapazitäten bei Gericht für die Prüfung dieser Anträge aufgebaut werden, was so schnell nicht möglich ist. Zum anderen besteht Eilbedürftigkeit durch die konkrete Lebensgefahr durch Corona. Ein Vergleich mit der Wertung der – hier nicht einschlägigen - StPO zeigt, dass auch das deutsche Recht einen Datenzugang ohne richterliche Anordnung bei Gefahr im Verzug kennt (§ 100e Abs. 1 S. 2 StPO).
8. Eine weitere Ergänzung der gesetzlichen Vorschriften wäre zu begrüßen gewesen und kann noch erfolgen. Die aufgezeigten **Handlungsoptionen bestehen** wegen der

Größe und der Nähe der Gefahr und wegen der besonderen Eilbedürftigkeit und Gefahr im Verzug für Leib und Leben aber bereits jetzt, solange diese besonderen Voraussetzungen bestehen und auf diesen besonderen Zweck begrenzt.

RA Dr. Peter Schmitz, JUCONOMY Rechtsanwälte

31.03.2020



RA Dr. Peter Schmitz ist durch vielfache Veröffentlichungen (insbesondere auch in Spindler/Schmitz, TMG, 2. A.) sowie Lehr- und Vortragstätigkeit im Bereich des Datenschutzes als fachkundig ausgewiesen. Er hat im Jahre 2000 zum Datenschutz promoviert und ist seit rund 20 Jahren im Bereich Datenschutz, Telekommunikation und Telemedien als Rechtsanwalt und Autor tätig.