Christian-Albrechts-Universität zu Kiel
Institut für Öffentliches Wirtschaftsrecht
Lehrstuhl für Öffentliches Recht

Univ.-Prof. Dr. Florian Becker, LL.M.

An den
Vorsitzenden des Innen- und Rechtsausschusses
Herrn Jan Kürschner, MdL
Schleswig-Holsteinischer Landtag
Düsternbrooker Weg 70
24105 Kiel
innenausschuss@landtag.ltsh.de

Telefon: 0431 880-5378
Telefax: 0431 880-5374
Durchwahl: 0431 880-1504
E-Mail: f.becker@law.uni-kiel.de
Homepage: www.becker.jura.uni-kiel.de

Kiel, 15.02.2023

Schleswig-Holsteinischer Landtag
Umdruck 20/877

Gesetzentwurf der Fraktionen von CDU und Bündnis 90/Die Grünen: Entwurf eines Gesetzes zur Wiedereinführung der Verkehrsdatenerhebung in § 185a LVwG (Drucksache 20/376)

Sehr geehrter Herr Vorsitzender Kürschner,
sehr geehrte Damen und Herren Abgeordnete,

mit Schreiben vom 22. Dezember 2022 haben Sie mir freundlicherweise die Gelegenheit eingeräumt, zu dem o.a. Gesetzentwurf Stellung zu nehmen. Vielen Dank für diese Möglichkeit, von der ich gerne Gebrauch mache. Bei der Abfassung dieser Stellungnahme hat mich mein Mitarbeiter, Herr Christian Margaard, sehr umfassend unterstützt.

Übersicht

I. Hintergrund des Gesetzesvorhabens

In dezidierter Abgrenzung zur höchstgerichtlich mehrfach beanstandeten Vorratsdatenspeicherung,

> in Bezug auf deutsche Regelungen EuGH NJW 2022, 3135; BVerfGE 125, 260; für Österreich und Irland EuGH NJW 2014, 2169; s. auch EuGH NJW 2021, 531 (Großbritannien, Frankreich und Belgien); EuGH NJW 2017, 717 (Schweden, Großbritannien),

ersucht das Gesetzesvorhaben, die legitimen Zwecke der gezielten Erhebung von Daten bei gleichzeitiger Reduktion der Eingriffsintensität zum Zwecke der Gefahrenabwehr zu erreichen.

Dem Vorhaben kommt es vor allem auf retrograde Verkehrsdaten an; dies sind Daten, die nicht in Echtzeit oder künftig anfallen, sondern aus zurückliegenden Zeiträumen stammen. Sie sollen in gewichtigen Gefahrenlagen – Vermisstenfälle, Terror- und Amoklagen – abgefragt werden können, wenngleich der Tatbestand darauf nicht beschränkt ist (dazu sogleich).

Im Unterschied zur Vorratsdatenspeicherung knüpft das Gesetzesvorhaben dafür aber nicht an verpflichtend zu speichernde Daten im Sinne von §§ 175 ff. TKG an, sondern an Verkehrsdaten i.S.v. § 9 TTDSG. Telekommunikationsanbieter dürfen diese Verkehrsdaten überhaupt nur verarbeiten, soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist.

Die entsprechende Standardmaßnahme in § 185a Abs. 2 Nr. 2 LVwG a.F. hatte das LVwGPO-RÄndG v. 26. Februar 2021 (GVOBl. 222) mit der gänzlichen Entfernung der Erhebung von Verkehrsdaten gestrichen, wenngleich das gesetzgeberische Ziel sich auf die Entfernung der Ermächtigung zur Vorratsdatenspeicherung – nach elf Jahren der Nichtigkeit dieser Kompetenz infolge des Urteils des Bundesverfassungsgerichts (BVerfGE 125, 260) – beschränkt hatte (Entwurf, S. 3).

II. Inhalt

Von besonderer verfassungsrechtlicher Relevanz sind die Einfügung einer Kompetenz zur Erhebung von Verkehrsdaten i.S.v. §§ 9, 12 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDG) (Abs. 2 Nr. 2 LVwG-E) einschließlich gespeicherter (retrograder) Standortdaten inklusive der Normierung der Funkzellenabfrage (Artikel 1 Nummer 2 c)) sowie die Ergänzung von besonderen Bezugspersonen der Datenerhebung gemäß § 185a Abs. 3 Nr. 2 LVwG-E. Die

übrigen Änderungen erschöpfen sich in sprachlichen Klarstellungen (Artikel 1 Nummer 2 Buchstabe a), d), e), f), g), h)) und redaktionellen Anpassungen (Artikel 1 Nummer 1, Nummer 2 b), i), j), k, Nummer 3 a), b)).

Die Erhebung von Verkehrsdaten knüpft an die Voraussetzungen von § 185a Abs. 1 LVwG an. Schutzgüter sind der Bestand oder die Sicherheit des Bundes oder eines Landes oder eine Gefahr für Leib, Leben oder Freiheit einer Person, § 185a Abs. 1 LVwG.

Als Regelbeispiele nennen § 185a Abs. 1 S. 2 Nr. 1, 2 LVwG insoweit konkret bevorstehende Straftaten der Staatsgefährdung gemäß §§ 89a, 89b StGB und der Bildung krimineller und terroristischer Vereinigungen nach §§ 129a, 129b StGB. Demnach sieht § 185a Abs. 2 Nr. 2 LVwG-E als gefahrenabwehrrechtliche Norm flexiblere Eingriffsvoraussetzungen vor als die streng unter dem Vorbehalt des Katalogs in § 100a Abs. 2 StPO stehende strafprozessuale Gegennorm § 100g Nr. 1 StPO.

Es wäre allerdings verfehlt, im Sinne eines Erst-recht-Schlusses die gefahrenabwehrrechtliche Norm zwangsläufig an den Anwendungsvoraussetzungen des Strafverfahrensrechts zu messen, nur um einen strafprozessual unzulässigen Vorgriff auf die Erhebung von Daten der privaten Lebensgestaltung zu vermeiden.

> So aber *Eschelbach*, in: Satzger (Hg.), SSW-StPO, 3. Aufl. 2018, § 100a Rn. 3; s. auch in Bezug auf den gesetzlichen Richter *Roggan*, Zur Doppelfunktionalität von heimlichen Ermittlungsmaßnahmen am Beispiel der Online-Durchsuchungen, GSZ 2018, 52 (56).

Die präventivpolizeiliche Tätigkeit setzt im Vergleich zum Strafverfahrensrecht funktionsgemäß eine gesteigerte Flexibilität zur Abwehr auch von im Vorhinein unbekannten Gefahrenlagen voraus. Anstatt diese Flexibilität durch strafverfahrensrechtliche Regelungsanalogien zu erstarren, gilt es in der Praxis, die Anwendbarkeit von präventivpolizeilicher und strafprozessualer Ermittlungstätigkeit nach dem Schwerpunkt der Maßnahme zu differenzieren. In einer strukturellen Gemengelage, in der Straftaten bereits eingetreten sind, und weitere Taten verhindert werden sollen, genießt die Polizei eine weitreichende Wahlfreiheit, nach welchem Regime sie ihre Eingriffsmaßnahmen ausrichtet. Das gilt gerade in Bezug auf die hier besonders relevanten Vorfeldstraftaten des kriminalpräventiven Strafrechts (§ 89a, § 89b, § 129a, 129b StGB), bei denen der Anfangsverdacht regelmäßig eng an der Schnittstelle zur Gefahrenabwehr liegt. Hier besteht eine gesetzliche Erwartung, dass die Polizeibehörden beide staatliche Aufgaben mit unterschiedlicher Zielsetzung ausüben.

> Vgl. BGH NStZ 2017, 651 (654); *Bäcker*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, D Rn. 340, 344.

Somit sind § 185a Abs. 2 Nr. 2 LVwG-E und § 100g StPO unter den jeweiligen Voraussetzungen nebeneinander anwendbar.

Mit dem Gefahrenbegriff der Dringlichkeit, den § 185a Abs. 1 LVwG wählt, werden dem Bundesverfassungsgericht zufolge sowohl erhöhte Anforderungen an die Bedeutung des betroffenen Rechtsguts hervorgehoben als auch auf eine besondere Wahrscheinlichkeit zum Eintritt des schädigenden Ereignisses abgestellt.

> BVerfGE 141, 220 (271); BVerfGE 130, 1 (32); ebenso VerfGH Rheinland-Pfalz MMR 2007, 578 (579 f.); abl. nur Schenke, Polizei- und Ordnungsrecht, 11. Auflage 2021, Rn. 78.

Insoweit geht die vorliegende Entwurfsbegründung (Entwurf, S. 6) **unzutreffend** von einem Alternativverhältnis dieser beiden Qualifikationen des Gefahrenbegriffs aus.

Außerdem muss die Erhebung der Daten zur Aufklärung des Sachverhalts unerlässlich sein, § 185a Abs. 1 LVwG.

Als Adressaten kommen über Verantwortliche i.S.v. §§ 218, 219 LVwG hinaus nunmehr ausdrücklich Personen in Betracht, bezüglich derer Tatsachen die Annahme rechtfertigen, dass sie vermisst oder suizidgefährdet sind oder sich in einer hilflosen Lage befinden, und die Bestimmung ihres Aufenthalts auf andere Weise aussichtslos oder wesentlich erschwert wäre, § 185a Abs. 3 Nr. 2 LVwG-E.

Gegenstand der im Ermessen der Polizei stehenden Rechtsfolge einer Erhebung von Verkehrsdaten nach § 185a Abs. 2 Nr. 2 LVwG-E sind nach § 3 Nr. 70 TKG alle Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind. § 9 TTDSG führt die Daten näher auf:

- Nummer und Anschlusskennung, personenbezogene Berechtigungskennungen wie etwa PIN-Nummern, ggf. bei Kundenkarten deren Nummern sowie bei mobilen Anschlüssen die Standortdaten
- Angaben über Beginn und Ende von Kommunikationsverbindungen und, soweit rechnungsrelevant, übermittelte Datenmengen
- Art des in Anspruch genommenen Telekommunikationsdienstes

- bei festgeschalteten Verbindungen deren Endpunkte, Beginn und Ende sowie, soweit rechnungsrelevant, übermittelte Datenmengen.

Hinzu zählt § 185a Abs. 2 Nr. 2 LVwG-E retrograde Standortdaten, die in den Verkehrsdaten gespeichert sind.

Die Standardmaßnahme der Erhebung von Verkehrsdaten grenzt sich also gerade von individualbezüglichen ab. Ihr liegt charakteristisch zugrunde, dass Dritte unvermeidbar getroffen werden, § 185a Abs. 4 S. 2 LVwG-E.

III. Verfassungsrechtlicher Rahmen

Die Speicherung, Abfrage und Verwendung von Daten, die durch Nutzung von Telekommunikation und Telemedien anfallen, berühren entweder das Telekommunikationsgeheimnis (Art. 10 GG) oder aber das Grundrecht auf informationelle Selbstbestimmung. Während einfache Bestandsdaten, Daten zur Zugangssicherung oder statische IP-Adressen durch das letztgenannte Grundrecht geschützt sind, fallen Informationen über die Zuordnung dynamischer IP-Adressen wegen ihrer Nähe zu konkreten Kommunikationsvorgängen in den Schutzbereich des Telekommunikationsgeheimnisses,

siehe i.E. die jeweiligen Zuordnungen in BVerfGE 130, 151 (179 ff.).

Im Ergebnis ist diese Abgrenzung aber für die Intensität des Grundrechtsschutzes nicht von zentraler Bedeutung, da die Anforderungen, die das Bundesverfassungsgericht mit Blick auf das letztgenannte Grundrecht ermittelt hat, weitgehend auf die speziellere Garantie des Art. 10 GG zu übertragen sind,

BVerfGE 100, 313 (359 f.); 125, 260 (310).

In beiden Fällen sind Grundrechtseingriffe gerechtfertigt, wenn sie in verhältnismäßiger Art und Weise das staatliche Anliegen und die Sensibilität eines bestimmten Datums in einen Ausgleich bringen. Dabei ist es nicht nur erforderlich, mit der Schwere des Grundrechtseingriffs die tatbestandliche Eingriffsschwelle zu verschärfen, sondern auch prozedurale Absicherungen des Eingriffs zu gewährleisten, die es dem Grundrechtsträger ermöglichen, sich gegen den Eingriff zur Wehr zu setzen. Der heimliche Eingriff wiegt schwerer als der offene, der indirekte Zugriff wiegt schwerer als der direkte. Auch die Persönlichkeitsrelevanz der in Anspruch genommenen Daten wirkt auf die gebotene Strenge der Eingriffsermächtigung zurück.

Weitergehend hat der EuGH die Erhebung von Verkehrsdaten unabhängig von der Dauer und der Menge der Erhebung auf die Bekämpfung schwerer Kriminalität oder zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit beschränkt.

EuGH NJW 2021, 2103 (2106).

Trotzdem sei eine Verkehrsdatenspeicherung sogar auf Vorrat zulässig, soweit die Rechtsvorschriften

- „auf der Grundlage objektiver und nicht diskriminierender Kriterien anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums für einen auf das absolut Notwendige begrenzten, aber verlängerbaren Zeitraum eine gezielte Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen;

- für einen auf das absolut Notwendige begrenzten Zeitraum eine allgemeine und unterschiedslose Vorratsspeicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, vorsehen;

- eine allgemeine und unterschiedslose Vorratsspeicherung der die Identität der Nutzer elektronischer Kommunikationsmittel betreffenden Daten vorsehen;

- vorsehen, dass den Betreibern elektronischer Kommunikationsdienste mittels einer Entscheidung der zuständigen Behörde, die einer wirksamen gerichtlichen Kontrolle unterliegt, aufgegeben werden kann, während eines festgelegten Zeitraums die ihnen zur Verfügung stehenden Verkehrs- und Standortdaten umgehend zu sichern (quick freeze)."

EuGH GSZ 2022, 280 (286).

Dies alles führt dazu, dass die Rechtfertigung von Eingriffen in das Grundrecht auf informationelle Selbstbestimmung und in das Telekommunikationsgeheimnis eine Beurteilung der Eingriffsschwere voraussetzt, von der ausgehend dann die materiellen und prozeduralen Anforderungen an die Rechtfertigung des Eingriffs entwickelt werden müssen. Die Prüfung des unionalen Grundrechtsschutzes (Art. 7, 8 und 11 sowie 52 Abs. 1 EUGRCh) verläuft im Wesentlichen parallel dazu.

BVerfGE 152, 152 (175).

IV. Beurteilung

1. Eingriffsgegenstand

Die Erhebung von Verkehrs- und Standortdaten nach § 185a Abs. 2 Nr. 2 LVwG-E greift final und unmittelbar in das Telekommunikationsgeheimnis ein. Sie befreit die Telekommunikationsunternehmen von der im Übrigen geltenden Geheimhaltungspflicht und ermöglicht die polizeiliche Verwendung im Rahmen der Gefahrenabwehr.

Unerheblich für den Bestand der Eingriffsqualität ist, dass die Herausgabe der Daten an die Polizei durch einen privaten Dienstanbieter erfolgt.

BVerfGE 125, 260 (312).

Die Intensität der Erhebung von Verkehrs- und Standortdaten haben der Europäische Gerichtshof und das Bundesverfassungsgericht wie folgt zusammengefasst:

Die Verkehrs- und Standortdaten können Informationen über eine Vielzahl von Aspekten des Privatlebens der Betroffenen enthalten, einschließlich sensibler Informationen wie sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie den Gesundheitszustand. Aus der Gesamtheit dieser Daten können sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren. Diese Daten ermöglichen insbesondere die Erstellung eines Profils der Betroffenen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikation selbst. Einen Vertraulichkeitsschutz gibt es insoweit nicht. Bezogen auf Gruppen und Verbände erlauben die Daten überdies unter Umständen die Aufdeckung von internen Einflussstrukturen und Entscheidungsabläufen.

Von Gewicht ist hierbei auch, dass unabhängig von einer wie auch immer geregelten Ausgestaltung der Datenverwendung das Risiko von Bürgern erheblich steigt, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst Anlass dazu gegeben zu haben. Es reicht etwa aus, zu einem ungünstigen Zeitpunkt in einer bestimmten Funkzelle gewesen oder von einer bestimmten Person kontaktiert worden zu sein, um in weitem Umfang Ermittlungen ausgesetzt zu werden und

unter Erklärungsdruck zu geraten. Auch die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, verschärfen deren belastende Wirkung.

Besonderes Gewicht bekommt die Speicherung der Telekommunikationsdaten weiterhin dadurch, dass sie selbst und die vorgesehene Verwendung der gespeicherten Daten von den Betroffenen unmittelbar nicht bemerkt werden, zugleich aber Verbindungen erfassen, die unter Vertraulichkeitserwartungen aufgenommen werden. Hierdurch ist jedenfalls die anlasslose Speicherung von Verkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.

EuGH, EuZW 2022, 958 (962); BVerfGE 125, 260 (319-320).

2. Eingriffsschwere

Im Hinblick auf die Eingriffsintensität einzelner Datensätze nach ihrer Erhebung unterscheidet sich die nun vorgeschlagene Erhebung von Verkehrsdaten nicht wesentlich von der einer Vorratsdatenspeicherung. Denn Rückschlüsse auf die private Lebensgestaltung sind aus Datensätzen ungeachtet der schlichten Herkunft der Daten aus einem angeordneten Vorrat oder aus der Aufbereitung zu Abrechnungszwecken zu ziehen.

Allerdings limitiert der Gesetzesentwurf den Bestand potenziell zu erhebender Daten erheblich und stellt ihre Vorhaltung unter einen unternehmerischen Vorbehalt der Abrechnung: Eigentlich verpflichten §§ 9, 12 TTDSG die Telekommunikationsanbieter gar nicht zur Speicherung oder Vorhaltung von Daten, sondern gerade zur Datenlöschung. Die Provider dürfen Verkehrsdaten überhaupt nur zum Zwecke des Aufbaus und der Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen verarbeiten. Verkehrsdaten ohne diese Zweckbestimmung sind nach § 9 Abs. 1 S. 2 TTDSG unverzüglich zu löschen. Für die gespeicherten Verkehrsdaten gelten keine Mindestspeicherfristen; je nach Vertragsgestaltung kann die Vorhaltung sieben Tage bis einige Monate dauern (Entwurf, S. 3 f.); für die Speicherung von Daten zur Störungsbeseitigung und zum Aufdecken von Missbrauchsfällen durch Netzbetreiber gilt eine zulässige Höchstfrist von sieben Tagen.

BGH, ZUM-RD 2011, 151.

Die Provider sind gemäß § 10 Abs. 2 S. 1 TTDSG verpflichtet, nach Beendigung der Verbindung die für die Zwecke der Abrechnung relevanten Verkehrsdaten unverzüglich zu ermitteln und nicht benötigte Daten nach § 10 Abs. 2 S. 3 TTDSG unverzüglich zu löschen.

Indem § 185a Abs. 2 Nr. 2 LVwG-E an die Bestimmungen des TTDSG anknüpft, reduziert er also die für die Erhebung von Verkehrsdaten erforderliche Speicherung auf das für die Funktionsfähigkeit der Telekommunikation und ihre Abrechnung durch die Provider nötige Minimum.

Dadurch begrenzt der Gesetzesentwurf den umfassenden Effekt dieser Standardmaßnahme auf die betroffene Bevölkerung gerade im Vergleich zur Vorratsdatenspeicherung erheblich. Zugleich muss davon ausgegangen werden, dass einige Netzbetreiber eine Speicherung der Daten schon deswegen nicht vornehmen, weil es für ihre technische und kaufmännische Abwicklung unerheblich ist (wenn sie mit einem Flatrate-Modell mit Pauschalpreis operieren). So ist die Abrufbarkeit dieser Daten weitgehend vom Zufall abhängig.

> *Henrichs/Weingast,* in: Karlsruher Kommentar zur Strafprozessordnung, 9. Aufl. 2023, § 100g Rn. 4.

3. Bestimmtheit

In Gestalt der Adjektive „suizidgefährdet“ und „vermisst“ enthält der Entwurf in § 185a Abs. 3 Nr. 2 LVwG-E zu konkretisierende Rechtsbegriffe. Sie sollen Personen charakterisieren, die den Anlass für die Datenerhebung bilden können ohne unbedingt verantwortlich i.S.v. §§ 218, 219 LVwG zu sein.

Zwar gelingt der Entwurfsbegründung eine anschauliche Darstellung der besonderen Bedeutung der Verkehrsdaten in Vermisstenfällen (Entwurf, S. 4). Wann aber eine gesuchte Person als hinreichend vermisst im gefahrenabwehrrechtlichen Sinne gelten kann, bleibt gerade unter Berücksichtigung der Intensität der dargestellten Grundrechtseingriffe eine auslegungsbedürftige Frage. Unbestimmte Rechtsbegriffe begründen freilich ein legitimes Instrument gesetzgeberischen Handelns und sind als solches mit der Unbestimmtheit im verfassungsrechtlich nach Art. 20 Abs. 3 GG erheblichen Sinne nicht gleichzusetzen.

Doch gerade in den regelmäßig äußerst grundrechtssensiblen Anwendungsfällen des § 185a Abs. 2 Nr. 2 LVwG-E bedarf es der vollständigen gerichtlichen Überprüfbarkeit und Konkretisierung dieses Merkmals, um eine ausufernde Anwendung zu vermeiden.

4. Verhältnismäßigkeit

Um verhältnismäßig zu sein, müsste die Intensivierung der Gefahrenabwehr, die aus der Erhebung von Verkehrsdaten folgt, in einem angemessenen Verhältnis zur Wirkung der Streuweite der zu erhebenden Daten auf die private Lebensgestaltung und die Vertraulichkeit der Telekommunikation stehen.

Das eklatante Anwachsen der elektronischen Telekommunikation stellt die Gefahrenabwehr gerade bei der Prävention von schweren Straftaten wie jenen der Staatsgefährdung, des Terrorismus und von qualifizierten Delikten gegen Leib, Leben und Freiheit der Person vor gewichtige Herausforderungen. Insbesondere rückwirkend erhobene Verkehrsdaten können als legitimes Mittel dazu beitragen, schwere Straftaten und Schäden für elementare Rechtsgüter zu verhindern.

Der Tatbestand der Erhebung von Verkehrsdaten lässt die Erhebung von Daten nur unter höchsten Anforderungen an den Gefahrenbegriff und das betroffene Schutzgut zu. Zu beachten ist insoweit, dass die Schwere der im Raum stehenden Verletzung der Güter Leib, Leben und Freiheit der Person nach § 185a Abs. 1 S. 1 LVwG nach systematischer Auslegung mit § 185a Abs. 1 S. 2 LVwG von vergleichbarem Gewicht etwa mit den dort genannten Straftaten sein muss. Deshalb unterliegt die Anwendung der Erhebung von Verkehrsdaten strengsten Voraussetzungen zur Abwehr der sowohl nach Wahrscheinlicheitsgrad als auch Intensität des Schadenseintritts qualitativ herausgehobenen Gefahr.

Die Intensität der Erhebung im Einzelfall wird durch den nach §§ 9, 12 TTDG limitierten Bestand potenziell zu erhebender Daten begrenzt. Die Provider halten die Verkehrsdaten nicht für die Behörde vor, sondern werden die Daten in vielen Fällen vernichtet haben, bevor die Behörde eine Erhebung von Daten anordnen kann.

Die Annahme eines ständigen Gefühls des Beobachtetseins wird demnach weniger begründet sein als im Falle der Vorratsdatenspeicherung. Ein möglicher Missbrauch dieser Kompetenz kann ohnehin nicht das primäre Kriterium sein, um die Verfassungskonformität einer Regelung zu bewerten, die gerade die legale Erhebung von Daten sichern soll.

Zwar ermöglicht auch die vorgeschlagene Regelung eine weitreichende Beeinträchtigung der informationellen Selbstbestimmung. Auch mit den so erhobenen Verkehrsdaten lassen sich Bewegungsprofile erstellen und Aufschlüsse über privateste Informationen über persönliche Einstellungen, private Kontakte, Gewohnheiten des täglichen Lebens und Aufenthaltsorte ziehen. Die Zugriffsmöglichkeit ist jedoch derart voraussetzungsreich, dass der Anwendungsbereich

hinreichend reduziert ist. Die konkrete Anordnung im Einzelfall muss auch stets anlassbezogen sein, sodass eine ziellose Vorhaltung ausgeschlossen scheint.

Die besonders intensive Funkzellenabfrage steht überdies unter der Subsidiaritätsklausel, dass die Aufgabenerfüllung nach § 185a Abs. 1 LVwG sonst nicht möglich oder wesentlich erschwert wäre.

V. Ergebnis

Insgesamt adressiert die gegenständliche Erhebung von Verkehrsdaten in auf das Notwendigste begrenzter Weise das besondere Gefahrenpotenzial der Telekommunikation in der modernen Gesellschaft und schafft eine auf die Zwecke der Abwehr von Gefahren für die ranghöchsten Güter der objektiven Rechtsordnung verhältnismäßig zugeschnittene Befugnis.

Durchgreifenden Bedenken begegnet die Umsetzung dieses Gesetzesvorhabens aus verfassungsrechtlicher Sicht nicht. Es steht aber zu empfehlen, den Gefahrenbegriff der dringenden Gefahr in der Entwurfsbegründung (Entwurf, S. 6) nach der Rechtsprechung des Bundesverfassungsgerichts auszurichten, um der hohen Grundrechtsrelevanz der Erhebung von Verkehrsdaten Rechnung zu tragen.

Für Rückfragen stehe ich jederzeit zur Verfügung.

Mit freundlichen Grüßen

Professor Dr. Florian Becker