# Heiligt der Zweck die Mittel?

jean-monnet-saar.eu/

## Generalanwalt Campos Sánchez-Bordona fordert weiterhin enge Grenzen für die Vorratsdatenspeicherung

18.04.2020

Ein Beitrag von Laura Katharina Woll und Asra Ak.*

## A. Einleitung

Mit vier derzeit beim EuGH anhängigen Vorabentscheidungsersuchen geht der Streit um die Vorratsdatenspeicherung in die nächste Runde. Mit Spannung wird erwartet, ob der EuGH seiner Haltung von 2016 treu bleibt und weiterhin die weitreichende allgemeine Vorratsdatenspeicherung verbietet. Damals hatte er mit klaren Worten jede unterschiedslose Vorratsdatenspeicherung für unionsrechtswidrig erklärt.[1]

Gegenstand der vier Verfahren sind Vorlagefragen von Gerichten aus dem Vereinigten Königreich (C-623/17), Frankreich (C-511/18 und C-512/18) und Belgien (C-520/18). In den Verfahren hatten sich u.a. die Nichtregierungsorganisationen *Privacy International* und *La Quadrature du Net* gegen die jeweiligen nationalen Vorschriften gewandt, welche den Betreibern elektronischer Kommunikationsdienste aufgaben, Massen-Telekommunikationsdaten zu sammeln und den Nachrichtendiensten zur Verfügung zu stellen.[2] In ihren Vorlagebeschlüssen werfen die Gerichte die Frage auf, ob die E-Privacy-Richtlinie 2002/58/EG zum Schutz personenbezogener Daten in der elektronischen Kommunikation[3] und die EU-Grundrechtecharta (GRCH) auf die Pflicht privater Telekommunikationsanbieter, Internet- und Telekommunikationsdaten ihrer Nutzer aus Gründen der öffentlichen Sicherheit weiterzugeben, anwendbar sind und ob diese Datenübermittlung unionsrechtskonform ist.[4]

Aus den anhängigen Vorabentscheidungsersuchen geht hervor, dass die vorlegenden Gerichte insbesondere im Hinblick auf Art. 4 Abs. 2 S. 3 EUV Zweifel daran haben, ob die Ausführungen des EuGH aus dem Jahr 2016 als generelles Verbot einer anlasslosen Vorratsdatenspeicherung zu verstehen sind, welches nicht einmal zur Bekämpfung erheblicher Gefahren für die öffentliche Sicherheit oder durch die Verwendung besonders restriktiver Zugriffsregelungen überwunden werden kann.[5] Generalanwalt *Manuel Campos Sánchez-Bordona* sprach sich indes am 15. Januar 2020 dafür aus, die vom EuGH 2016 in den verbundenen Rechtssachen *Tele2 Sverige und Watson* (Rs. C-203/15 und C-698/15) aufgestellten strengen Vorgaben an die Rechtmäßigkeit der Vorratsdatenspeicherung beizubehalten und nur enge Ausnahmen zuzulassen.

Angesichts der momentanen Situation in der Corona-Krise rückt zusätzlich ein weiteres datenschutzrechtliches Problem, das sogenannte „Handy-Tracking“, in den Vordergrund.[6] Hierbei soll Zugriff auf sämtliche Standortdaten ermöglicht werden, um die Kontakte von Corona-Infizierten zu identifizieren und so die Ausbreitung der Epidemie einzudämmen. Schon allein diese neuere Entwicklung macht die anstehende Entscheidung des EuGH noch interessanter, da der Aspekt der Gesundheit der Bevölkerung nun zu dem der nationalen Sicherheit hinzugetreten ist und der Problematik eine neue Dimension verliehen hat, weshalb in diesem Kontext möglicherweise sogar die seit langem hochumstrittene Vorratsdatenspeicherung neu zu beurteilen ist.

## B. Die E-Privacy-Richtlinie

Mit der sogenannten E-Privacy-Richtlinie 2002/58/EG wurden Bestimmungen über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Rahmen elektronischer Kommunikation erlassen. Die Vorschriften gewährleisten Schutz gegenüber nichtstaatlichen Dienstanbietern. Geschützt wird die freie Entfaltung der Persönlichkeit durch einen privaten, von der Öffentlichkeit verborgenen Austausch von Informationen.[7] Die Vertraulichkeit von individueller Kommunikation soll erhalten bleiben, wenn diese wegen der räumlichen Distanz zwischen den Kommunikationsteilnehmern und den damit einhergehenden Zugriffsmöglichkeiten Dritter auf den Kommunikationsvorgang besonders verletzlich ist.[8] Die RL schützt folglich nicht nur den eigentlichen Inhalt des Kommunikationsvorgangs, sondern auch dessen nähere Umstände, insbesondere wer mit wem und wie oft kommuniziert.[9]

Grund hierfür ist, dass auch Informationen über Beteiligte, Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen eine erhebliche Aussagekraft entfalten können, weil sie Rückschlüsse auf die Art und Intensität der Beziehungen zulassen und damit auch auf den Inhalt bezogene Schlussfolgerungen ermöglichen.[10] Das Problem dabei ist nicht neu, die Telekommunikationsüberwachung (TKÜ) gehört zu den ältesten technikgestützten heimlichen Überwachungsmethoden der Sicherheitsbehörden.[11] Relativ neu ist die zunehmende Aufmerksamkeit, die das Thema wohl nicht nur wegen seiner Bedeutung im nationalen und internationalen vernetzten Kommunikationsmarkt bekommt. Regelmäßig ist die TKÜ nun Bestandteil heftiger politischer Kontroversen anlässlich zunehmender Maßnahmen der Terrorbekämpfung.[12] Grund hierfür ist die besondere Eingriffsintensität dieser Überwachungsmethode, die unter Mitwirkung des Dienstanbieters heimlich durchgeführt wird und mit einer erheblichen Streubreite das soziale Umfeld der Zielperson einbezieht, weshalb sie sich auch auf völlig unverdächtige Kommunikationsteilnehmer erstreckt.[13]

## C. Bisherige Rechtsprechung des EuGH

Der EuGH hat sich in der Vergangenheit sehr klar zur Speicherung von und zum Zugang zu personenbezogenen Daten geäußert. Hier ist zum einen das Urteil vom 8. April 2014 in den verbundenen Rechtssachen *Digital Rights Ireland u.a.* (C-293/12) und *Seitlinger u.a*. (C-594/12), zum anderen das Urteil vom 21. Dezember 2016 in den verbundenen Rechtssachen *Tele2 Sverige* (C-203/15) und *Watson u.a.* (C-698/15) zu nennen.

Im Urteil von 2014 wurde die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der E-Privacy-Richtlinie 2002/58/EG für ungültig erklärt, weil sie einen unverhältnismäßigen Eingriff in die in der Grundrechtecharta verankerten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten zuließ.[14]

Nach dem EuGH ist die Bekämpfung von Terrorismus und von organisierter Kriminalität für die nationale Sicherheit zwar von größter Bedeutung. Auch sah der Gerichtshof ein, dass die Gewährleistung der nationalen Sicherheit von der Nutzung moderner Ermittlungstechniken abhängen kann. Dennoch war eine Vorratsdatenspeicherung in der durch die Neuregelung vorgesehenen Dimension für die Kriminalitätsbekämpfung wegen der mit ihr verbundenen erheblichen Grundrechtsbeeinträchtigungen nicht zu rechtfertigen.[15]

Im Urteil von 2016 ist Art. 15 Abs. 1 der E-Privacy-Richtlinie ausgelegt worden. Nach dieser Vorschrift können die Mitgliedstaaten u.a. aus Gründen der nationalen Sicherheit Rechtsvorschriften erlassen, mit denen bestimmte Rechte und Pflichten aus der Richtlinie beschränkt werden.[16] Diese Bestimmung ist im Lichte der GRCH auszulegen, da – wie der Gerichtshof zunächst feststellte – die nationalen Vorschriften wegen Art. 3 und 5 Abs. 1 der E-Privacy-Richtlinie in den Geltungsbereich des Unionsrechts fielen,[17] d.h. der Anwendungsbereich der Charta gem. Art. 51 Abs. 1 GRCH eröffnet war.

Entgegen den Auffassungen der Mitgliedstaaten sprach sich der EuGH für eine enge Auslegung der Richtlinie aus. Dies begründete er damit, dass sie mit Art. 15 Abs. 1 den Erlass von die Vertraulichkeit der Kommunikation einschränkenden Rechtsvorschriften nur ausnahmsweise ermöglicht.[18] Diese Ausnahme, so der Gerichtshof, sei indes nach ständiger Rechtsprechung eng auszulegen.[19] Die in Rede stehenden nationalen Vorschriften erlaubten aber im Rahmen der Kriminalitätsbekämpfung die Speicherung und Verarbeitung sämtlicher personenbezogenen Daten, ohne Differenzierung von Personenkreisen. Dass die nationalen Vorschriften die Ausnahme des Art. 15 Abs. 1 zum Normalfall machten, sei mit dem Sinn und Zweck dieser Bestimmung nicht vereinbar. In Weiterentwicklung seiner Rechtsprechung aus dem Jahr 2014 betonte der Gerichtshof deshalb insbesondere den unverhältnismäßig schweren Eingriff in Art. 7, 8 GRCH und erteilte der flächendeckenden Speicherung sämtlicher Verkehrs- und Standortdaten von Telekommunikationsnutzern eine klare Absage.[20]

In diese Rechtsprechung reihen sich nun auch die Schlussanträge von GA *Campos Sánchez-Bordona* ein, die im Folgenden näher analysiert werden sollen.

## D. Die Schlussanträge von GA Campos Sánchez-Bordona vom 15.01.2020

### I. Anwendbarkeit der E-Privacy-Richtlinie auf geheimdienstliche Maßnahmen

Zunächst geht der Generalanwalt der Frage nach, ob die E-Privacy-Richtlinie auf bestimmte geheimdienstliche Maßnahmen anwendbar ist, die in die elektronische Kommunikation eingreifen. Die Besonderheit bei dieser Art von staatlicher Telekommunikationsüberwachung ist, dass es sich letztlich um eine Frage der nationalen Sicherheit handelt. Hierfür sieht die E-Privacy-Richtlinie mit Art. 15, wie bereits erwähnt, eine Sonderregelung vor.

Der Generalanwalt wendet hier jedoch ein, dass die Pflicht zur *Sammlung* der Daten bei der allgemeinen Vorratsdatenspeicherung, wie die nationalen Vorschriften sie vorsehen, nicht den Behörden direkt obliegt, sondern privaten Anbietern. Sobald aber Privatpersonen in die Pflicht gezogen werden, statuiert die E-Privacy-Richtlinie eine Pflicht der privaten Betreiber elektronischer Kommunikationsdienste zum Schutz der personenbezogenen Daten ihrer Nutzer.[21] Die E-Privacy-Richtlinie ist daher, so GA *Campos Sánchez-Bordona,* auf die in Rede stehenden Fälle anwendbar. Sie greife lediglich dann nicht ein, wenn die Behörden, gänzlich ohne Privatpersonen in die Pflicht zu nehmen, selbst und auf eigene Rechnung tätig werden.[22]

Sofern die Betreiber elektronischer Kommunikation wie hier gesetzlich verpflichtet sind, die Daten zu speichern und den Behörden Zugang zu gewähren, findet die Richtlinie Anwendung, wobei sie den Mitgliedstaaten nach Art. 15 Abs. 1 sodann folgende Einschränkungen gestattet: „Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.“

Wie sich zeigen wird, wurden diese Anforderungen seitens der nationalen Gesetzgeber in den hiesigen Fällen nicht beachtet, wobei nur einige Punkte der Unvereinbarkeit mit der E-Privacy-Richtlinie näher beleuchtet werden sollen.

## II. Unvereinbarkeit der nationalen Sicherheitsgesetze mit der E-Privacy-Richtlinie

1. Verbundene Rechtssachen C-511/18 und C-512/18

In den verbundenen Rechtssachen *C-511/18 und C-512/18* steht die Richtlinie nach Ansicht des Generalanwalts den einschlägigen französischen Vorschriften im Ergebnis entgegen. Diese erlegen nämlich den Betreibern und Anbietern elektronischer Kommunikationsdienste eine Pflicht zur allgemeinen und unterschiedslosen Speicherung von Verkehrs- und Standortdaten aller Teilnehmer auf. Unter Bezugnahme auf das Urteil *Tele2 Sverige und Watson* nimmt der Generalanwalt einen nach Art. 15 Abs. 1 der Richtlinie 2002/58 nicht zu rechtfertigenden Eingriff an.[23]

Die nach der Ausnahmevorschrift des Art. 15 Abs. 1 erlassenen Rechtsvorschriften sind, wie eingangs erwähnt, restriktiv und im Lichte der Grundrechtecharta auszulegen.[24] Hier maßgeblich betroffen sind Art. 7, 8 und 11 GRCH, [25] d.h. insbesondere der Schutz des Privatlebens, der Schutz personenbezogener Daten sowie der Schutz der Meinungsfreiheit.

Die französische Regelung zur Vorratsdatenspeicherung ist sehr weitgehend und u.a. auch auf Einzelpersonen anwendbar, bei denen keinerlei Anhaltspunkte dafür vorliegen, dass ihr jeweiliges Verhalten in einem auch nur entfernten Zusammenhang mit schweren Straftaten stehen könnte.[26] Letztlich ist es diese allgemeine und unterschiedslose Sammlung und Speicherung der personenbezogenen Daten, die nach ständiger Rechtsprechung des EuGH einen ungerechtfertigten Eingriff in Art. 7, 8 und 11 GRCH darstellt.[27] Für den Generalanwalt ändert sich hieran auch nichts durch das Anliegen der Terrorismusbekämpfung. Vielmehr führt er an, dass der Gerichtshof schon 2016 im Urteil *Tele2 Sverige und Watson* darauf hingewiesen habe, dass auch dieses Ziel ihn nicht zu einer Änderung seiner strengen Rechtsprechung bewegen könne.[28]

Generalanwalt *Campos Sánchez-Bordona* erkennt durchaus an, dass eine – von ihm grundsätzlich als zulässig angesehene[29] –nur teilweise und sehr differenzierte Speicherung personenbezogener Daten den nationalen Nachrichtendiensten die Möglichkeit des Zugangs zu Informationen nehmen würde, die für die Erkennung von Gefahren für die öffentliche Sicherheit nützlich sein können.[30] Dem hält er aber entgegen, dass auch Terrorismusbekämpfung nicht allein aus dem Blickwinkel der Wirksamkeit und Nützlichkeit betrachtet werden sollte: „Es zeigt die Schwierigkeit, aber auch die wahre Größe der Terrorismusbekämpfung, wenn ihre Mittel und Methoden den Erfordernissen des Rechtsstaats entsprechen, der in erster Linie bedeutet, dass Macht und Stärke den Grenzen des Gesetzes und insbesondere einer Rechtsordnung, deren Grund und Zweck die Verteidigung der Grundrechte ist, unterliegen.“[31] In anderen Worten, der Zweck heiligt gerade nicht die Mittel.

Eine weitere Unvereinbarkeit der französischen Regelung mit der E-Privacy-Richtlinie sieht der Generalanwalt in der mangelnden Pflicht, die Betroffenen über die Verarbeitung ihrer personenbezogenen Daten durch die zuständigen Behörden zu unterrichten, sobald die behördlichen Maßnahmen von dieser Unterrichtung nicht mehr beeinträchtigt werden können.[32] Eine Unterrichtung sowie ein möglicher Rechtsbehelf sind aber in einem Rechtsstaat unabdingbar, in dem für heimliche Maßnahmen der „Grundrechtsschutz durch Verfahren“ ermöglicht werden muss.

Aus Art. 15 Abs. 2 der Richtlinie 2002/58/EG ergibt sich eine Anwendbarkeit des Kapitel III der Richtlinie 95/46/EG über Rechtsbehelfe, Haftung und Sanktionen im Hinblick auf innerstaatliche Vorschriften, die nach der RL 2002/58/EG erlassen wurden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte. Der Generalanwalt führt hier aus, dass die vom vorlegenden Gericht angeführten nationalen Rechtsschutzgarantien davon abhängig zu sein scheinen, dass derjenige, der den Verdacht hat, dass Informationen über seine Person gesammelt werden, selbst die Initiative ergreift. Das Recht auf Zugang zu einem Gericht muss jedoch für alle effektiv

wirksam sein, was bedeutet, dass jeder die Möglichkeit haben muss, die Verarbeitung personenbezogener Daten gerichtlich überprüfen zu lassen, sodass folglich eine gesetzliche Unterrichtungspflicht bestehen muss.[33]

Sobald also die behördlichen Ermittlungen, für die Zugang zu den gespeicherten Daten gewährt wird, nicht mehr beeinträchtigt werden können, ist die betroffene Person über den Zugang zu informieren,[34] woran es im einschlägigen Fall mangelt.

2. Rechtssache C-520/18

Im Rahmen des zweiten Vorabentscheidungsersuchens, der Rechtssache *C-520/18,* steht die E-Privacy-Richtlinie im Ergebnis einer belgischen Regelung entgegen, die zwar nicht nur das Ziel der Ermittlung, Feststellung und Verfolgung von schweren Straftaten hat, sondern u.a. auch konkret der Sicherstellung der nationalen und öffentlichen Sicherheit bzw. der Landesverteidigung dienen soll (was grundsätzlich Art. 15 Abs. 1 der E-Privacy-Richtlinie unterfiele). Doch obgleich der Zugang zu den personenbezogenen Daten hier genau festgelegten Garantien unterliegt, wird auch in diesem Fall den Betreibern eine Pflicht zur allgemein-unterschiedslosen Speicherung auferlegt, die ununterbrochen besteht, und somit nach Ansicht des Generalanwalts unionsrechtswidrig ist.[35] Auch hier sind Art. 7, 8 und 11 der GRCH verletzt.[36]

In seinen Ausführungen weist der Generalanwalt explizit darauf hin, dass eine vorübergehende Speicherung von bestimmten Verkehrs- bzw. Standortdaten möglich und mit der EuGH-Rechtsprechung vereinbar sein kann, sofern die Daten kein detailliertes Abbild vom Leben der betroffenen Person liefern und strengen Sicherheitsanforderungen unterworfen werden.[37] Daraus könnte sich letztlich ein europarechtskonformer Mittelweg für die einzelnen Mitgliedstaaten ergeben.

3. Rechtssache C-623/17

In der Rechtssache *C-623/17* stellte sich die Frage, ob die staatliche Anweisung an einen Betreiber elektronischer Kommunikation, den Sicherheits- und Nachrichtendiensten des Vereinigten Königreichs Massen-Telekommunikationsdaten zur Verfügung zu stellen, mit der Richtlinie vereinbar ist.[38] Die Richtlinie steht nach Ansicht des Generalanwalts trotz Art. 4 Abs. 2 S. 3 EUV und Art. 1 Abs. 3 RL 2002/58/EG, wonach die nationale Sicherheit grundsätzlich in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt[39], einer solchen Regelung entgegen.

Das vorlegende Gericht tendiert zu einer Verneinung der Anwendbarkeit der E-Privacy-Richtlinie, indem es u.a. auf Art. 4 Abs. 2 EUV hinweist. Diesem Argumentationsversuch erteilt der Generalanwalt jedoch eine Absage: Die Speicherung der Daten und ihre Übermittlung ließen sich als Verarbeitung personenbezogener Daten durch den Betreiber elektronischer Kommunikationsdienste charakterisieren, weshalb sie in den Geltungsbereich der Richtlinie fielen.[40] Gründe der nationalen Sicherheit könnten dieser Feststellung nicht vorgehen, denn dann fiele die streitige Pflicht schon gar nicht in den *Anwendungsbereich* des Unionsrechts.[41]

Art. 4 Abs. 2 EUV kann gleichwohl nicht als Ausnahme von der E-Privacy-Richtlinie herangezogen werden, vielmehr kann eine Beschränkung gewisser Rechte und Pflichten nur nach Maßgabe des Art. 15 der RL 2002/58/EG erfolgen – welcher wiederum im Lichte der GRCH auszulegen ist. Hier verweist der Generalanwalt nun auf seine Ausführungen in den verbundenen Rechtssachen *C-511/18 und C-512/18* und weist abschließend erneut darauf hin, dass die E-Privacy-Richtlinie zwar nicht anwendbar ist, wenn die staatlichen Behörden eine Datenerfassung im Namen der nationalen Sicherheit unmittelbar und mit eigenen Mitteln vornehmen; dass sie allerdings sehr wohl anwendbar ist, wenn hierfür Unterstützung durch Privatpersonen erfolgt, denen Verpflichtungen zur Herausgabe der Daten staatlich auferlegt werden.[42]

## E. Ausblick auf das Urteil des EuGH

Im Ergebnis empfiehlt Generalanwalt *Campos Sánchez-Bordona* dem EuGH, seine 2016 mit dem Urteil *Tele2 Sverige und Watson* begründete Rechtsprechung zu bestätigen. Denn eine allgemeine und unterschiedslose Speicherung sämtlicher Verkehrs- und Standortdaten von Telekommunikationsteilnehmern sei auch unter dem Gesichtspunkt der Aufrechterhaltung der nationalen Sicherheit bzw. Terrorismusbekämpfung unionsrechtswidrig.[43]

Der EuGH könnte den Mitgliedstaaten indes teilweise entgegenkommen, indem er den Empfehlungen des Generalanwalts folgt, eine begrenzte und differenzierte Speicherung von und einen begrenzten Zugang zu personenbezogenen Daten zu erlauben.[44] Auch ist zu bedenken, dass nach Ansicht des Generalanwalts selbst eine weitreichende und allgemeine Datenerfassung bei einer unmittelbar bevorstehenden Bedrohung oder einer durch außergewöhnliche Gefahr gekennzeichneten Ausnahmesituation zu rechtfertigen wäre, da sie dann nicht anlasslos erfolgt.[45] Ob eine Pandemie, wie wir sie derzeit im Rahmen der Corona-Krise erleben, als eine solche gelten könnte, ist indes fraglich, da bei der allgemeinen Vorratsdatenspeicherung die Verbrechensbekämpfung im Fokus steht.

Aus der Systematik der E-Privacy-Richtlinie und den umfassenden Erwägungen des Generalanwalts ergibt sich dennoch, dass die allgemeine Vorratsdatenspeicherung lediglich als sehr enge Ausnahme möglich sein kann. Seine eher strenge Rechtsprechung dürfte der EuGH, wenn er, wie in den meisten Fällen, den Schlussanträgen im Ergebnis folgt, erneut bestätigen. Dies würde auch zur Unionsrechtswidrigkeit deutscher Regelungen führen, welche ebenfalls die Erhebung weitreichender Daten ohne spezifischen Anlass und geographisch-personelle Begrenzung sowie eine Speicherung dieser personenbezogenen Daten von vier bis zehn Wochen vorsehen.[46]

Mit Spannung bleibt daher abzuwarten, ob der Gerichtshof sich den Ausführungen von Generalanwalt *Campos Sánchez-Bordona* anschließt und damit seiner Rechtsprechungslinie treu bleibt – oder sich doch zu deren Aufweichung überreden lässt, wie sie nicht zuletzt auch die Europäische Kommission gefordert hatte.[47]

---

* Laura Katharina Woll ist wissenschaftliche Mitarbeiterin und Doktorandin, Asra Ak war wissenschaftliche Hilfskraft am Lehrstuhl von Univ.-Prof. Dr. Thomas Giegerich.

[1] EuGH, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige und Watson, Rn. 134.

[2] *Gröning/Wildt*, EuGH-Generalanwalt fordert enge Grenzen für Vorratsdatenspeicherung, Anwaltsblatt, https://anwaltsblatt.anwaltverein.de/de/news/eugh-generalanwalt-fordert-enge-grenzen-fuer-vorratsdatenspeicherung (16.04.2020).

[3] ABl. L 201 v. 31.7.2002, S. 46.

[4] *Gröning/Wildt*, EuGH-Generalanwalt fordert enge Grenzen für Vorratsdatenspeicherung, Anwaltsblatt, https://anwaltsblatt.anwaltverein.de/de/news/eugh-generalanwalt-fordert-enge-grenzen-fuer-vorratsdatenspeicherung (16.04.2020).

[5] BVerwG, Pressemitteilung Nr. 66/2019 vom 25.09.2019, https://www.bverwg.de/pm/2019/66 (16.04.2020).

[6] *Schieb*, Handytracking gegen Corona: Wirklich ein Unding? https://blog.wdr.de/digitalistan/handytracking-gegen-corona-wirklich-ein-unding/ (16.04.2020). Siehe hierzu ausführlich den Artikel von Annika Blaschke auf unserem Blog: Flatten the curve! Doch mit welchen Mitteln? – Handy-Ortung während der Corona-Krise.

[7] RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 201 v. 31.7.2002, S. 37.

[8] *Kühling/Seidel/Sividis*, Datenschutzrecht, 3. Auflage 2015, S. 79 f.

[9] *Tinnefeld/Buchner/Petri/Hof*, Einführung in das Datenschutzrecht, 7. Auflage 2020, S. 294.

[10] EuGH, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige und Watson, Rn. 98.

[11] *Nowak*, Lauschen zur Gefahrenabwehr, https://www.heise.de/tp/features/Lauschen-zur-Gefahrenabwehr-3425639.html (17.04.2020).

[12] *Grunert*, Entschlüsseln der Vergangenheit?, https://www.faz.net/aktuell/politik/vorratsdatenspeicherung-entschluesseln-der-vergangenheit-16403103.html (19.02.2020).

[13] EuGH, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger u.a., Rn. 58; Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 115.

[14] EuGH, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger, Rn. 65.

[15] EuGH, verb. Rs. C-293/12 und C-594/12, Digital Rights Ireland und Seitlinger, Rn. 51.

[16] EuGH, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige und Watson, Rn. 108.

[17] *Kipker*, Neues in Sachen Vorratsdatenspeicherung: Das jüngste Urteil des EuGH vom 21.12.2016, https://community.beck.de/2017/01/07/neues-in-sachen-vorratsdatenspeicherung-das-juengste-urteil-des-eugh-vom-21122016 (17.04.2020).

[18] EuGH, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige und Watson, Rn. 89 ff.

[19] EuGH, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige und Watson, Rn. 89.

[20] *Kipker/Schefferski/Stelter*, EuGH: Allgemeine und unterschiedslose Vorratsdatenspeicherung unzulässig, Anmerkung zum Urteil vom 21.12.2016 – C-203/15 u. C-698/15 – Tele2 Sverige, ZD 2017, S. 124 (131).

[21] https://www.otto-schmidt.de/news/wirtschaftsrecht/mittel-und-methoden-der-terrorismusbekampfung-mussen-den-erfordernissen-des-rechtsstaats-entsprechen-2020-01-15.html (16.04.2020).

[22] Schlussanträge GA Campos Sánchez-Bordona, Rs. C-623/17, Privacy International, Rn. 79.

[23] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 115, 117.

[24] EuGH, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige und Watson, Rn. 89, 91.

[25] EuGH, verb. Rs. C-203/15 und C-698/15, Tele2 Sverige und Watson, Rn. 92; Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 94.

[26] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 115.

[27] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 111-117.

[28] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 121.

[29] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 133.

[30] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 129.

[31] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 130.

[32] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 155.

[33] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 151.

[34] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 153.

[35] Schlussanträge GA Campos Sánchez-Bordona, Rs. C-520/18, Ordre des barreaux francophones et germanophone, Rn. 155.

[36] Schlussanträge GA Campos Sánchez-Bordona, Rs. C-520/18, Ordre des barreaux francophones et germanophone, Rn. 86.

[37] Schlussanträge GA Campos Sánchez-Bordona, Rs. C-520/18, Ordre des barreaux francophones et germanophone, Rn. 93.

[38] Schlussanträge GA Campos Sánchez-Bordona, Rs. C-623/17, Privacy International, Rn. 19.

[39] Schlussanträge GA Campos Sánchez-Bordona, Rs. C-623/17, Privacy International, Rn. 45.

[40] Schlussanträge GA Campos Sánchez-Bordona, Rs. C-623/17, Privacy International, Rn. 30.

[41] Schlussanträge GA Campos Sánchez-Bordona, Rs. C-623/17, Privacy International, Rn. 31.

[42] Schlussanträge GA Campos Sánchez-Bordona, Rs. C-623/17, Privacy International, Rn. 34.

[43] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 155; Schlussanträge GA Campos Sánchez-Bordona, Rs. C-520/18, Ordre des barreaux francophones et germanophone, Rn. 155; Schlussanträge GA Campos Sánchez-Bordona, Rs. C-623/17, Privacy International, Rn. 45.

[44] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 146 und 155.

[45] Schlussanträge GA Campos Sánchez-Bordona, verb. Rs. C-511/18 und C-512/18, La Quadrature du Net, Rn. 104.

[46] Betroffen wären §§ 113 a, 113 b TKG, vgl. hierzu *Gröning/Wildt*, EuGH-Generalanwalt fordert enge Grenzen für Vorratsdatenspeicherung, Anwaltsblatt, https://anwaltsblatt.anwaltverein.de/de/news/eugh-generalanwalt-fordert-enge-grenzen-fuer-vorratsdatenspeicherung (16.04.2020).

[47] *Ibid*.