

Protokoll der mündlichen Anhörung in den Rechtssachen C-623/17, C-511/18, C-512/18 und C-520/18 vor dem EuGH vom 9. und 10. September 2019

**mit Privacy International, La Quadrature du Net, French Data
Network, dem Orden der französisch- und deutschsprachigen
Anwaltskammern und anderen**

Bastien Le Querrec

übersetzt von Chloé Berthélémy und Jens Kubieziel*

17. September 2019

Am 9. und 10. September 2019 fand die Anhörung vor dem EuGH in den Fällen Privacy International, La Quadrature du Net, French Data Network, dem Orden der französisch- und deutschsprachigen Anwaltskammern und anderen.¹ Dies sind vier verbundene Fälle, weil sie auf dem gleichen Thema basieren: die Rechtmäßigkeit von Systemen zur Speicherung von Verbindungsdaten für nachrichtendienstliche Zwecke. Das Gericht stellte den Parteien vor der Verhandlung mehrere Fragen. Im Laufe des Sommers wurden schriftliche Stellungnahmen vorgelegt, und diese Anhörung wurde durch Schriftsätze, mündliche Anfragen des Gerichtshofs und anschließende Antworten wiederholt.

*Fehler in der Übersetzung gehen zu Lasten von Jens Kubieziel und können an [<jens@kubieziel.de>](mailto:jens@kubieziel.de) gemeldet werden. Ein Großteil des Dokuments wurde mit Hilfe von [DeepL](#) oder [Google Translate](#) übersetzt.

¹Der führende Fall liegt in der Verantwortung von Privacy International, daher sollte das Urteil nach ihm benannt werden.

1 Präsentation des Streitfalls

In allen vier Fällen wurden dem Gerichtshof Vorabfragen vorgelegt, in denen er aufgefordert wurde, die Konformität nationaler Maßnahmen zur allgemeinen Speicherung von Verbindungsdaten mit dem EU-Recht zu bewerten.

Verbindungsdaten sind die Daten, die eine Nachricht beinhalten. Wir können eine Parallele mit ein Brief in einem Umschlag ziehen: Die Verbindungsdaten sind das, was auf dem Umschlag steht und der Inhalt der Kommunikation ist das, was sich innerhalb des Umschlags befindet. Konkret, sind Verbindungsdaten der Empfänger und Absender einer Nachricht, die IP-Adresse eines Endgeräts, die Liste der Stationen, mit denen ein Telefon verbunden ist usw. Es sind in der Theorie nicht die Inhalte eines Gesprächs. Die klagenden Verbände haben jedoch gezeigt, dass diese Unterscheidung in der Praxis oft schwierig zu treffen ist. Die Mitgliedstaaten bewahren diese Verbindungsdaten aus Gründen der Kriminalitätsbekämpfung oder der nationalen Sicherheit auf. In Frankreich ist diese Aufbewahrungsfrist ein Jahr (Art. R10-13 EuRH). In den Urteilen Digital Rights Ireland (EuGH, 8. April 2014, aff. C-293/12 und C-594/12) und Tele2 Sverige AB (EuGH, 21. Dezember 2016, Rechtssache C-203/15 und C-698/15) kam der Gerichtshof zu dem Schluss, dass der Grundsatz der allgemeinen Speicherung von Verbindungsdaten im Widerspruch zur EU-Charta standen.

In Frankreich haben La Quadrature du Net und andere Verbände nach der Entscheidung von Digital Rights Ireland die Aufhebung von Artikel R10-13 EuRH beantragt. Erst am 26. Juli 2018 stellte der Conseil d'État durch zwei Urteile (Rechtssachen 394922 und 393099) fünf Fragen zur Einhaltung des EU-Rechts des französischen Rechts zur Datenspeicherung der Verbindung.

Es muss zwischen Erhaltung und Zugang unterschieden werden. Alle europäischen Rechtsvorschriften erfordern eine allgemeine Speicherung von Verbindungsdaten: Die Betreiber sind verpflichtet, einer Verpflichtung nachzukommen, um die Zugangsdaten aller ihrer Benutzer für einen variablen Zeitraum zu speichern. Das Ausmaß dieser generalisierten Speicherung variiert je nach Staat: Es kann sich um Folgendes handeln alle Verbindungsdaten (z. B. in Frankreich), oder nur bestimmte Arten von Verbindungsdaten (z. B. in Schweden bei der anstehenden Reform). Die gespeicherten Daten sind in einem zweiten Schritt zugänglich. Dieser Zugang ist theoretisch immer begrenzt beispielsweise durch die Verpflichtung, die Gründe für den Antrag auf Zugang oder Überprüfung durch eine Kontrollbehörde anzugeben.

Die Parteien wurden vom EuGH aufgefordert, den Geltungsbereich der Richtlinie 2002/58 (ePrivacy) und die Anwendbarkeit des EU-Rechts auf die Wirkung von Chilling Effects zu überprüfen gemäß der Charta unter der Annahme eines allgemeinen, aber zielgerichteten Zugangsregimes, der Erfassung einer automatisierten Analyse der Verbindungsdaten mit dem Recht auf Privatsphäre oder einer Art der Aufbewahrung von Verbindungsdaten, die am wenigsten gegen die Rechte und Freiheiten der Charta verstoßen.

2 Schriftsätze (erster Tag)

2.1 Argumente der beschwerdeführenden Verbände

Die beschwerdeführenden Verbände sind der Ansicht, dass die Gesetze der Mitgliedstaaten, die eine allgemeine Speicherung von Verbindungsdaten vorschreiben, nicht mit der Charta übereinstimmen. Das Argument basiert auf demjenigen, das 2016 im Fall Tele2 entwickelt wurde: Die generalisierte Speicherung ist eine unverhältnismäßige Beeinträchtigung der Chartarechte.

In der mündlichen Verhandlung stellten die beschwerdeführenden Verbände fest, dass nach britischem, französischem oder belgischem Recht die Verbindungsdaten, in einigen Fällen aber auch der eigentliche Inhalt der Kommunikation, unter die Aufbewahrungspflicht für die Betreiber fallen. Nach Ansicht der Beschwerdeführer sind die Garantien zum Zeitpunkt des Zugangs zu diesen Daten unzureichend oder gar nicht vorhanden.

Die Plädoyers der französischen Verbände² kritisierten auch die recht weit gefassten und unklaren Ziele der [französischen, britischen und belgischen] Gesetze, die die Einrichtung von Geheimdiensttechnik erlauben, zu denen auch der Zugang zu Verbindungsdaten gehört. Die Beschwerdeführer wollten nachweisen, dass es in Frankreich eine Massenüberwachung gibt: Durch diese ungenauen Zwecke wird der Zugang zu den Verbindungsdaten nicht eingeschränkt. In Verbindung mit der allgemeinen Speicherung trägt dieser uneingeschränkte Zugang dazu bei, dass das System nicht angemessen ist. Die Praxis des Informationsaustauschs zwischen den Staaten würde auch eine Massenüberwachung darstellen: Die Überwachung von Nachrichtenmissionen

²Die Verbände La Quadrature du Net, der Verband der Internetdiensteanbieter und Ig-wan.net, die denselben Anwalt haben, beantworteten die verschiedenen Fragen, die der Gerichtshof vor dem Publikum gestellt hatte, für seine verschiedenen Kunden.

wird im Bereich der Außenüberwachung immer lockerer; die Agenturen können jedoch durch die Zusammenarbeit zwischen den Staaten Informationen über ihre eigenen Bürger erhalten, die von einem ausländischen Staat zurückgeholt wurden, also unter einem lockeren Außenüberwachungssystem. Auf der Grundlage dieser Massenüberwachung haben die Beschwerdeführer dann die schädlichen Auswirkungen einer solchen Speicherung von Verbindungsdaten beschrieben. Abgesehen von der mangelnden Verhältnismäßigkeit einer solchen Verpflichtung wiesen die Verbände auf den derzeitigen Missbrauch solcher Maßnahmen hin: Sie erinnerten daran, dass in Frankreich die Zwecke des Nachrichtenwesens bei den „gelben Westen“ von ihrem Hauptziel und bei den sozialen Konflikten ganz allgemein von ihrem Hauptziel abgewichen wurden. Die Beschwerdeführer verwiesen auf die abschreckende Wirkung der Massenüberwachung und verwiesen auf mehrere soziologische Studien im Zusammenhang mit der Überwachung.

Die Verbände verlangen die Benachrichtigung von Personen, die von der Überwachung betroffen waren. Der Fall des Journalisten Camille Polloni wurde zitiert: Nach einem langen, mühsamen und oft unverständlichen Verfahren von außen konnte der Journalist von einer illegalen Überwachungsmaßnahme gegen sie durch den militärischen Geheimdienst erfahren (ohne zu wissen, woraus die Überwachung bestand oder was sie illegal war) und wurde vom Conseil d'État versichert, dass der Antrag auf Löschung der illegal gesammelten Informationen tatsächlich gestellt worden sei. Dieses Beispiel veranlasst die Beschwerdeführer zu der Annahme, dass das derzeitige Verfahren vor dem Staatsrat nicht ausreicht, um Befürchtungen auszuräumen, weil es nicht transparent ist. Nur eine systematische Benachrichtigung würde dieses Problem lösen: Andernfalls können die zu überwachenden Personen nicht wissen, dass sie überwacht wurden, und können ihre Rechte im Falle von Missbrauch nicht schützen.

Die Verbände erinnerten daran, dass das EU-Recht anwendbar ist. Mit einer Gegenargumentation wollten sie zeigen, dass die Datenschutzrichtlinie, wenn sie nicht anwendbar wären, bedeutungslos gemacht würden. Die nationale Sicherheit ist für die Beschwerdeführer keine Quelle der Inkompetenz im EU-Recht. Es geht nicht nur immer noch um die Umsetzung des Unionsrechts im Sinne der Rechtsprechung von Pfleger (EuGH, 30. 4. 2014, Rechtssache C-390/12), sondern die betreffenden nationalen Gesetze gehen weit über die nationale Sicherheit allein hinaus.

Schließlich kritisierten die beschwerdeführenden Verbände den Wortlaut der vom Conseil d'État gestellten Fragen sehr kritisch. Diese würden so geändert,

dass der Gerichtshof aufgefordert wird, seine Rechtsprechung zu überprüfen, was nicht die Rolle des Staatsrates wäre.

Während der Antworten bestand La Quadrature du Net auf einer ihrer Meinungen nach zufriedenstellenden Lösung des Streits. Sie forderte den Gerichtshof nicht nur auf, seine Tele2-Rechtsprechung aufrechtzuerhalten, sondern auch zu präzisieren, dass nur ein System der spontanen Speicherung von Verbindungsdaten, wie es in den Vereinigten Staaten praktiziert wird, eine solche Effizienz ohne die Verpflichtung zur allgemeinen Speicherung von Verbindungsdaten ermöglichen würde (siehe unten).

2.2 Argumente der Mitgliedstaaten, der Europäischen Kommission und des Europäischen Datenschutzbeauftragten (EDSB)

Alle Mitgliedstaaten haben eine allgemeine Speicherung der Verbindungsdaten gefordert. Demnach können die Datenschutzrichtlinie für den elektronischen Geschäftsverkehr und die EU-Charta nicht auf den Rechtsstreit Anwendung finden, da es sich um eine Angelegenheit der nationalen Sicherheit und der ausschließlichen Zuständigkeit der Mitgliedstaaten handeln würde. Sie fordern, dass die Rechtsprechung von Tele2 nicht im Bereich der Nachrichtendienste umgesetzt wird.

Die Mitgliedstaaten erklärten auch einstimmig, dass die Rechtsprechung von Tele2 nicht angewendet werden kann und dass sie sie nicht anwenden wollen, wenn diese beibehalten oder sogar auf nachrichtendienstliche Tätigkeiten ausgedehnt wird. Die Schriftsätze der Mitgliedstaaten wurden alle von vielen Beispielen für Strafsachen begleitet, die die Notwendigkeit eines allgemeinen Systems zur Speicherung von Verbindungsdaten veranschaulichen sollten. Der Eindruck war jedoch, dass die Mitgliedstaaten mit Emotionen spielen wollten, ebenso wie Child Focus, eine Vereinigung, die sich für allgemeine Speicherpflichten einsetzte und in ihren Beispielen aufgrund der Art und Weise, wie die verschiedenen Fakten erzählt wurden, und der immer schmutzigeren Details Unbehagen in der Öffentlichkeit hervorrief.³⁴ Doch diese Beispiele vermischten sehr oft Kriminalität und nationale Sicherheit, was der Gerichtshof in seinen Fragen vom zweiten Tag feststellte.

³Der Anwalt des Vereins beschrieb unter anderem die Geschichte eines „kleinen Mädchens im Alter von 10 bis 12 Jahren“ und eines sexuellen Raubtiers „seiner ultimativen Fantasie nahe“.

⁴Child Focus schien auch der belgischen Regierung nahe zu stehen: Der Wortlaut der Klagebeantwortung dieser Vereinigung wurde unter den Mitgliedern der belgischen Regierung verbreitet, und die Antwort wurde mit den belgischen Agenten vorbereitet.

Viele Mitgliedstaaten haben vor allem Maßnahmen ergriffen, um ihre nationalen Rechtsvorschriften gegen folgende Probleme zu verteidigen: generalisierte Speicherung von Verbindungsdaten. Garantien, die auf der Zugangsstufe gewährt werden, waren Gegenstand vieler Entwicklungen. Auf diese Weise konnten wir regelmäßig feststellen, dass ein Richter oder eine unabhängige Verwaltungsbehörde für die Überwachung der Anträge zuständig war. Zugriff auf die Verbindungsdaten und Überprüfung, ob die Bedingungen – streng nach den zahlreichen Vorgaben der Mitgliedstaaten – waren gut erfüllt. Es sei darauf hingewiesen, dass im französischen Fall La Quadrature du Net und die französische Regierung sind radikal dagegen. Frankreich behauptet, dass die Kontrolle a priori und a posteriori wirksam ist, während La Quadrature vor dem Staatsrat die Unwirksamkeit der von der Nationalen Geheimdienstkontrollkommission (CNCTR) genutzten Techniken demonstrierte.

Die Rechtsprechung des EGMR, insbesondere Big Brother Watch gegen das Vereinigte Königreich (EGMR, 13. September 2018, Big Brother Watch et. al, 58170/13, 62322/14 und 24960/15) wurde von den Mitgliedstaaten zur Unterstützung der Annahme von Maßnahmen durch den Straßburger Gerichtshof genannt. Die Mitgliedstaaten haben den Gerichtshof aufgefordert, diesem Urteil nachzukommen.

Einige Mitgliedstaaten wie Schweden sind der Ansicht, dass es nicht notwendig ist, eine allgemeine und undifferenzierte Speicherung von Verbindungsdaten vorzunehmen, sondern nur eine allgemeine Speicherung bei bestimmten Arten von Verbindungsdaten. Die Europäische Kommission und der Europäische Datenschutzbeauftragte (EDSB) teilen diese Position.⁵ Laut ihnen, sollte es eine vollständige Liste der Arten von Verbindungsdaten geben, die Gegenstand der allgemeinen Speicherung sind. Dies würde unter anderem Webadressen ausschließen, ein Thema der Diskussion zwischen Frankreich und La Quadrature du Net. Frankreich oder das Vereinigte Königreich haben insbesondere die Speicherung nur bestimmter Verbindungsdaten abgelehnt und für eine generalisierte und undifferenzierte Speicherung plädiert.

Alle Mitgliedstaaten waren der Auffassung, dass die einzige Alternative zur allgemeinen Speicherung die gezielte Speicherung wäre, um die Glaubwürdigkeit einer solchen Hypothese unverzüglich zu untergraben.

⁵Die Kommission hat sich auch dem Standpunkt der Mitgliedstaaten zur Nichtanwendbarkeit von Tel2 angeschlossen, was möglicherweise erklärt, warum sie kein Vertragsverletzungsverfahren eingeleitet hat.

Danach muss die gezielte Konservierung nach Kriterien erfolgen, die notwendigerweise diskriminierend sind oder sogar die Unschuldsvermutung untergraben (was bei einer generalisierten Konservierung und einem gezielten Zugang nicht der Fall wäre). Diese Annahme basiert auf der vom Vereinigten Königreich bekräftigten Annahme, dass die Speicherung oder der Zugriff auf Verbindungsdaten keine Intelligenz schafft, sondern nur eine Voraussetzung für Intelligenz ist. Dabei lehnten die Mitgliedstaaten implizit die Hypothese einer gezielten Speicherung nach Kriterien ab, die sich aus der vorherigen Überwachung durch andere (individuelle) Nachrichtentechniken ableiten lassen. Man hätte sich vorstellen können, dass die Verbindungsdaten einer Person oder Gruppe von Personen, die zuvor als potenzielle Bedrohung identifiziert wurden, erhalten bleiben und dass nach der Erhaltung eine detaillierte Analyse der Verbindungsdaten durchgeführt wird, um die Befürchtungen zu bestätigen oder zu widerlegen. Die Mitgliedstaaten lehnten diese Hypothese ebenfalls ab und erklärten, dass eines der Ziele der Maßnahmen zur Speicherung und zum Zugriff auf Verbindungsdaten darin besteht, unbekannte Bedrohungen (schwache Signale) zu erkennen, nicht nachweisbar durch ausschließlich menschliche Analyse).

3 Fragen des Gerichtshofs (Tag zwei)

Der zweite Tag war den Fragen des Gerichtshofs gewidmet, zunächst dem Berichterstatter, dann dem Generalanwalt, gefolgt von den anderen Richtern bei der Bildung des Gerichts. Der Richterberichterstatter ist derselbe wie bei Tele2.

Der Eindruck, der sich aus den Fragen des Gerichtshofs ergibt, ist, dass er sehr vorsichtig ist, nicht in die Sicherheitsvision der Mitgliedstaaten zu fallen. In zahlreichen Erklärungen der Richter wurden die Widersprüche der Mitgliedstaaten hervorgehoben. Der Präsident und der Generalanwalt schienen verärgert über die wiederholten Appelle der Regierungen des Vortages. Richter und Berichterstatter erinnerten daran, dass das Big Brother Watch Urteil, das von den Staaten sehr regelmäßig angewandt wird. Mitglieder, um zu argumentieren, dass eine generalisierte Aufbewahrungsmaßnahme für Verbindungsdaten wäre nicht gegen die EMRK verstoßen, ist nicht endgültig, und der Generalanwalt hat die Mitgliedstaaten über die Relevanz ihrer Beispiele, die sich sehr selten mit der Problematik der nationale Sicherheit. Der Gerichtshof hat mehrmals die vom Ausschuss geäußerten Bedenken bekräftigt. von Venedig über eine generalisierte Speicherung von Verbindungsdaten.

Die Kommission und Frankreich wurden regelmäßig durch Fragen des Berichterstatters und des Generalanwalts in Schwierigkeiten gebracht. Sie schienen nicht von der Argumentation der Mitgliedstaaten über die Verhältnismäßigkeit einer allgemeinen Erhaltungsregelung mit gezieltem Zugang überzeugt zu sein. So fragte der Berichterstatter die Kommission beispielsweise, ob es nicht zu einer Umkehrung zwischen der Regel und der Ausnahme in Bezug auf den Datenschutz kommen würde, wenn eine solche Regelung akzeptiert würde. Frankreich konnte nicht erklären, wie man eine Analyse der Verbindungsdaten durch algorithmisches Monitoring (die „Black Boxes“) durchführen könnte, ohne auch eine Analyse des Inhalts der Kommunikation selbst zu haben.⁶

Der Berichterstatter des Richters wies auch das Argument der Mitgliedstaaten zurück, sich der allgemeinen Erhaltung und Erhaltung zu widersetzen. Letzteres ist nicht die einzige Alternative zur allgemeinen Erhaltung. Die Frankreich konnte dem Generalanwalt nicht mitteilen, welche Arten von Verbindungsdaten es gibt. wäre es unerlässlich, in die von der Kommission vorgeschlagene vollständige Liste aufzunehmen, um zu vermeiden, dass undifferenziertere Erhaltung, wobei anerkannt wird, dass eine solche Liste durch folgende Maßnahmen möglich ist z. B. Webseitenadressen ausschließen.

Der Gerichtshof versuchte auch, die Folgen zu ermitteln, die die Kommission und der EDSB aus dem Urteil Digital Rights Ireland gezogen haben. Der Gerichtshof erinnerte daran, dass er in Digital Rights Ireland erklärt hat, dass es keinen Grund gibt, zu dem Schluss zu kommen, dass eine weitreichende Speicherung erforderlich ist, um die Ziele der Verbrechensbekämpfung zu erreichen. Anschließend fragte sie die Kommission und dann den EDSB, ob nach diesem Urteil Studien durchgeführt wurden und ob sie zu dem Schluss kommen würden, dass eine allgemeine Erhaltung erforderlich ist. Es wurde jedoch keine Studie von der Kommission oder dem EDSB durchgeführt.

Schließlich bat der Generalanwalt die beschwerdeführenden Verbände um Klärung der US-Regelung für die Speicherung von Verbindungsdaten. Im Anschluss an diese Frage konzentrierte sich die Antwort auf La Quadrature du Net insbesondere auf die Lösung eines spontanen Aufbewahrungsregimes für Verbindungsdaten nach dem amerikanischen Modell. Die spontane Speicherung von Verbindungsdaten basiert auf der Annahme, dass die Betreiber bestimmte

⁶Zu diesem Punkt hatte La Quadrature du Net bereits vor den französischen Gerichten erklärt, dass es technisch nicht möglich ist, den Inhalt der Kommunikation mit algorithmischer Überwachung der Verbindungsdaten nicht zu analysieren: Um auf Verbindungsdaten zuzugreifen, müssen „Black Boxes“ auch den Inhalt der Kommunikation analysieren, um Verbindungsdaten zu extrahieren.

Verbindungsdaten aus legitimen Gründen (einschließlich Abrechnung und Infrastrukturschutz) und spezifisch für ihre Aktivitäten aufbewahren müssen (nicht alle Betreiber haben die gleiche Aktivität und speichern daher nicht die gleichen Arten von Verbindungsdaten für diesen Zweck). Nach Ansicht von La Quadrature du Net würde ein System der spontanen Speicherung von Verbindungsdaten es nach Ansicht von La Quadrature du Net ermöglichen, keine allgemeine oder differenzierte Speicherung vorzuschreiben (siehe oben), und wäre daher mit der Rechtsprechung des EuGH Tele2 vereinbar und bietet gleichzeitig eine ähnliche Wirksamkeit wie das deutsche Modell, das dem in den Vereinigten Staaten am nächsten kommt.⁷

4 Weiterverfolgung des Streits

Die Schlussanträge des Generalanwalts werden voraussichtlich Ende Dezember 2019 oder Anfang Januar 2020 vorliegen. Das Urteil des EuGH wird einige Monate später ergehen. Der Gerichtshof scheint mit seinen Fragen auf die Feststellung hinzuwirken, dass das Unionsrecht auf die nationale Sicherheit und die Aufrechterhaltung eines allgemeinen und undifferenzierten Verbots der Speicherung von Verbindungsdaten anwendbar ist.

Andererseits kann sie eine allgemeine Speicherung nur bestimmter Arten von Verbindungsdaten akzeptieren (d. h. die Speicherung wäre nicht mehr unterschiedslos), wie von der Kommission, dem EDSB oder einigen Mitgliedstaaten wie Schweden gefordert. Es ist auch möglich, dass die Position von La Quadrature du Net, die darin besteht, jede, auch differenzierte, generalisierte Erhaltung zu verbieten, beibehalten wird, wobei die einzig mögliche Lösung eine Gesetzgebung, die auf der spontanen Speicherung von Verbindungsdaten basiert.

Update vom 18. September: FrenD Data Network wurde fälschlicherweise als Anwalt von Le Quadrature du Net bezeichnet.

VERSIONSHISTORIE

Datum	Autor	Kommentar
4. Dezember 2019	Bastien Le Querrec, Chloé Bert-hélémy, Jens Kubieziel	initiale Version des Dokuments

⁷Das deutsche Modell basiert ebenfalls auf einer allgemeinen Verpflichtung zur Aufbewahrung von Trennungsdaten, aber diese Verpflichtung ist viel geringer als in Frankreich und betrifft nicht insbesondere den Zugang zu Informationszwecken, wie von der Bundesregierung in ihrer Antwort angegeben.