Bundesrepublik Deutschland

Bundesministerium für Wirtschaft
und Energie
Referat E A 5 – 81202/001#564, 81202/002#473, 480, 481
StA Klebs / RD Kanitz

Bundesministerium der Justiz
und für Verbraucherschutz
Referat IV C 2 - ###
OStA Hellmann

Berlin, den 6. September 2019

# Plädoyer

in den Rechtssachen

**C-623/17 (Privacy International)**

**C-511/18 und C-512/18 (La Quadrature du Net u.a.)**

**C-520/18 (Ordre des barreaux francophones et germanophone u.a.)**

Mündliche Verhandlung vor dem
Gerichtshof der Europäischen Union in Luxemburg
(Große Kammer)
am Montag, dem 9. September 2019,
um 9 Uhr

**Herr Präsident,**

**Frau Vizepräsidentin,**

**meine Damen und Herren Richter**

**(Berichterstatter: v. Danwitz),**

**Herr Generalanwalt (Campos Sánchez-Bordona )**

## I. Einleitung

1 Der Gerichtshof verhandelt heute vier Rechtssachen gemeinsam. Die Bundesregierung begrüßt dies. Denn so besteht Gelegenheit, *nicht nur* auf die Parallelen hinzuweisen, *sondern vor allem* auch auf die Unterschiede.

## II. Zur Rechtssache C-623/17 (Nachrichtendienste und nationale Sicherheit)

2 Ich komme **zunächst** zu den Befugnissen der Nachrichtendienste, also zur Rechtssache C-623/17.

3 Es macht – und damit antworte ich zugleich auf die **erste Frage** des Gerichtshofs – einen Unterschied, ob Daten unmittelbar *vom Staat* gespeichert werden oder ob die *privaten Betreiber* von Kommunikationsnetzwerken dazu *verpflichtet* werden, *Daten auf Vorrat zu speichern*. Im ersten Fall greift die Bereichsausnahme des Art. 1 Abs. 3 der Richtlinie 2002/58 für staatliche Aktivitäten, nur im letzten Fall ist der Anwendungsbereich der Richtlinie eröffnet.

4 Die Relevanz dieser Unterscheidung ergibt sich aus dem Urteil *Tele2 Sverige und Watson* [C-203/15 und C-698/15;Rn. 69, 70 und 74]. Im dortigen Ausgangssachverhalt wurden private Netzbetreiber verpflichtet, bestimmte Daten auf Vorrat zu *speichern*. Deswegen sah der Gerichtshof den Anwendungsbereich der Richtlinie 2002/58 eröffnet [Rn. 75].

5 Im vorliegenden Fall geht es aber darum, dass der Staat, konkret die Nachrichtendienste, die Daten *selbst* speichern.

6 Allerdings *leiten* die Betreiber die Daten vorliegend zum Zwecke der Speicherung und Verarbeitung an die britischen Nachrichtendienste *weiter*. Hieraus will die Kommission auf die Eröffnung des Anwendungsbereichs des Unionsrechts schließen.

7 Dies überzeugt die Bundesregierung nicht.

8 **Erstens** zäumt die Kommission das Pferd quasi von hinten auf: Sie argumentiert, dass immer dann, wenn die Vertraulichkeit der Kommunikation verletzt werde, der Anwendungsbereich der Richtlinie 2000/58 eröffnet sei [vgl. Rn. 33 aE der StN KOM]. Folgte man diesem Argument, liefe Art. 1 Abs. 3 der Richtlinie weitestgehend leer. Denn auch wenn der Staat selbst Daten erhebt und speichert, wird ja in das Recht auf Vertraulichkeit dieser Daten eingegriffen.

9 **Zweitens** würde der Anwendungsbereich der Richtlinie so überdehnt. Die bloße *technische Unterstützung* durch die Betreiber darf aus Sicht der Bundesregierung nicht dazu führen, den staatlichen Charakter der Datenerhebung und -verarbeitung aufzuheben. Das gilt insbesondere für das ungefilterte Weiterleiten des Verkehrs (*forwarding in real-time)*, das Sie in Ihrer **dritten Frage** ansprechen. Wegen des untergeordneten Beitrags bleibt die Weiterleitung eine „Aktivität des Staates" im Sinne von Art. 1 Abs. 3 der Richtlinie 2002/58.

10 Dies gilt *umso mehr*, wenn es um die Aufgaben der Nachrichtendienste der Mitgliedstaaten geht. Denn die Nachrichtendienste schützen die nationale Sicherheit. Sie bilden das Frühwarnsystem eines jeden Staates zum rechtzeitigen Erkennen existenzbedrohender Entwicklungen und sind typischerweise weit im Vorfeld gravierender Bedrohungen tätig. Sie sind somit ein besonders sensibler Bestandteil der Abwehrfähigkeit eines Staates.

Es geht hier um den Kernbereich nationaler Sicherheit, der nach Art. 4 Abs. 2 EU-Vertrag weiterhin in die alleinige Verantwortung der Mitgliedstaaten fällt. Eine Erstreckung von Sekundärrecht in diesem Bereich würde ultra-vires Fragen aufwerfen und könnte von MS als Angriff auf den Kernbereich ihrer Eigenstaatlichkeit gewertet werden.

11 Im Ergebnis fällt die in der Rechtssache C-623/17 streitige britische Regelung folglich nicht in den Anwendungsbereich der Richtlinie 2002/58.

12 Damit komme ich zum **zweiten Teil**, zur Tätigkeit der Strafverfolgungsbehörden und der Polizei zum Schutz der öffentlichen Sicherheit.

## III. Zu den Rechtssachen C-511/18, C-512/18 und C-520/18 (öffentlichen Sicherheit und Strafverfolgung)

13 Lassen Sie mich einen tatsächlichen Fall aus der strafrechtlichen Praxis schildern. Es ist ein Fall wie aus einem Spionageroman des Schriftstellers John le Carré.

14 Am 23. Juli 2017 wurden mitten in Berlin zwei vietnamesische Staatsangehörige vom vietnamesischen Geheimdienst entführt. Sie wurden auf offener Straße nahe des Brandenburger Tores in einen Lieferwagen gezerrt und dann nach Vietnam gebracht. Es handelte sich um einen ehemaligen Partei-und Wirtschaftsfunktionär, der dann später in Vietnam zu lebenslänglicher Haft verurteilt wurde.

15 Sie können sich vorstellen, dass der Fall in Deutschland viel Aufsehen erregt hat. Die Aufklärung gelang nur durch den Rückgriff auf gespeicherte Telekommunikationsdaten und glich einem Puzzlespiel.

16 Die Ermittlungsbehörden gingen davon aus, dass die Opfer vor der Tat von den Tätern eine Zeit lang beobachtet wurden. Über die Kreditkartendaten und die Hoteladresse konnten Orte ermittelt werden, an denen sie sich die Entführungsopfer in den Tagen vor der Tat aufgehalten haben. Für diese Orte wurde mit richterlicher Genehmigung eine Funkzellenabfrage vorgenommen. Dabei fiel auf, dass dort immer wieder dieselben Mobilfunknummern eingebucht und aktiv waren. Das waren die Telefone der Täter, die ihre Opfer in den Tagen vor der Tat ausspähten.

17 Nachdem die ersten Mobilfunknummern der Verdächtigen bekannt waren, konnte eine weitere richterliche Verfügung erwirkt werden, um ihre Verbindungsdaten auszuwerten. Durch die Auswertung konnten sich die Ermittler ein Bild von dem Kommunikationsverhalten der Täter machen. Ja, sie konnten sogar erkennen, welcher der Beteiligten die Operation leitete und wo er sich dabei aufgehalten hatte. Auf diese Weise konnte einer der Tatbeteiligten in Deutschland verhaftet und verurteilt werden.

18 Hohes Gericht, dieser Fall macht folgendes deutlich:

19 Erstens: Es wäre nicht möglich gewesen, den vorliegenden Fall mit einer zielgerichteten Speicherpflicht von Telekommunikationsdaten aufzuklären. Denn vor dem Verbrechen konnte

niemand ahnen, dass eine solche Tat bevorstand. Die Aufklärung der Tat war überhaupt nur möglich, weil Verkehrsdaten der Verdächtigten gespeichert und ausgewertet werden konnten, obwohl die Verdächtigen vorher nie strafrechtlich in Erscheinung getreten waren.

20 Zweitens: Dieser Fall demonstriert, welche Möglichkeiten eine Vorratsdatenspeicherung für die Ermittlungsbehörden eröffnet. Es lassen sich nicht nur einzelne Täter identifizieren, sondern es können auch ganze Netzwerkstrukturen und Beziehungsgeflechte von Tatverdächtigen festgestellt werden. Das ist gerade in den Bereichen Organisierte Kriminalität und Terrorismus von großer Bedeutung.

21 Der Fall demonstriert damit aber auch die möglichen Risiken umfassender Datenspeicherung für die Freiheitsrechte der Bürger. Eine der Fragen des Gerichtshofs lautet: Wie bewertet sich die Eingriffsintensität („intrusiveness“) einer Maßnahme, die den Zugang zu Kommunikationsdaten ermöglicht, im Vergleich mit dem Zugang zu den Inhalten der Kommunikation?

22 Die Antwort lautet: Die Datenmenge macht den Unterschied! Wenn man sämtliche Verkehrsdaten eines Menschen über z.B. 2 Jahre speichern würde, dann erhielte man eine so große Datenmenge, dass man daraus unter Umständen viel

über diesen Menschen erfahren könnte. So viel, dass die Eingriffsintensität einem Zugang zu den Inhalten der Kommunikation schon recht ähnlich wird.

23 Beschränkt man die Menge der über einen Menschen gespeicherten Verkehrsdaten demgegenüber auf das unbedingt Notwendige und hält die Menge „klein", dann bleibt auch die Eingriffsintensität geringer. Sie lässt sich dann nicht mit dem Zugang zu den Inhalten der Kommunikation vergleichen.

24 Die entscheidende Frage lautet deshalb: Wie kann man die Menge der gespeicherten Daten auf das absolut Notwendige beschränken? Ein Mittel besteht darin, die Speicherfristen zu beschränken und je nach Eingriffstiefe zu differenzieren. In Deutschland betragen sie z.B. 10 Wochen für Verkehrsdaten. Und für die besonders sensiblen Standortdaten beträgt die Speicherfrist sogar nur vier Wochen.

25 Ein weiteres Mittel besteht darin, genau zu prüfen, welche Kommunikationsdaten für Ermittlungszwecke besonders relevant sind und die Speicherverpflichtung auf diese Datenkategorien zu beschränken. In Deutschland hat der Gesetzgeber z. B. entschieden, dass die Daten von E-Mails nicht gespeichert werden müssen.

26 Ich komme noch einmal auf den vietnamesischen Entführungsfall zurück. Die Aufklärung war nur möglich, weil die Kommunikationsdaten aus der Vergangenheit noch vorlagen.

Das war nicht selbstverständlich, denn zum fraglichen Zeitpunkt gab es in Deutschland keine gesetzliche Speicherpflicht. Die Ermittler waren darauf angewiesen, dass die Telekommunikationsunternehmen entsprechende Daten noch zu Abrechnungszwecken vorhielten. Aber das ist u.a. wegen der Flatrate-Tarife mittlerweile immer seltener oder gar nicht mehr der Fall.

27 Letztendlich war es Zufall, dass die notwendigen Daten bei den Telekommunikationsunternehmen noch vorhanden waren. Aber die Aufklärung solcher Verbrechen darf nicht dem Zufall überlassen werden.

## IV. Schluss

28 Ich danke für Ihre Aufmerksamkeit.