

Meinhard Starostik • Rechtsanwalt

RECHTSANWALTSKANZLEI
Wittestr. 30E • D- 13509 Berlin
+49 30 8800030 • Fax: +49 30 88000310
Email: kanzlei@starostik.de
USt-ID-Nr.: DE165877648

KANZLEI VEREIDIGTER BUCHPRÜFER
Schwarzenberger Str. 7 • D-08280 Aue
+49 3771 564700 • Fax: +49 3771 5647025

Berliner Bank AG
Konto: 21 45 65 400 • BLZ: 100 708 48
IBAN: DE79 1007 0848 0214 5654 00
BIC: DEUTDEB110



Kanzlei
Starostik
Berlin

RA Starostik • Wittestr. 30 E • D-13509 Berlin

An den
Gerichtshof
der Europäischen Union
durch: ECURIA

Berlin, den 14. Juli 2015

Mein Zeichen: 45/08-3

In dem Vorabentscheidungsverfahren C-582/14

vorlegendes Gericht: Bundesgerichtshof Deutschland –VI ZR 135/13 –

zeige ich die Vertretung des Klägers im Ausgangsverfahren an (Vollmacht anbei)
und beantrage

- 1. die Durchführung einer mündlichen Verhandlung und**
- 2. mir 30 Minuten Zeit für den mündlichen Vortrag einzuräumen.**

Begründung:

I. Zunächst soll in der mündlichen Verhandlung die grundlegende Bedeutung der Rechtssache aufgezeigt werden:

Der Gerichtshof entscheidet darüber, ob Internetnutzer ein Recht darauf haben, sich aus öffentlichen Internetseiten ebenso anonym, spurenlos und unbefangen informieren zu können wie es aus den traditionellen Medien wie Zeitung, Radio oder Büchern der Fall ist. Gibt es auch im Informationszeitalter ein Recht auf anonymen Zugang zu öffentlichen Informationen und auf anonyme Meinungsäußerung in der Öffentlichkeit? Oder soll jeder unserer Klicks im Netz aufgezeichnet und auf uns zurückgeführt werden können (Zitat Edward Snowden: "I do not want to live in a world where everything I do and say is recorded.")? Die große Vielzahl und Spezialisierung von Telemedien ermöglicht sogar noch weit tiefgründigere Einblicke in unsere Persönlichkeit, unser Privatleben, unsere Interessen und Vorlieben als die traditionellen, anonym nutzbaren Medien. Information und Beratung von Menschen in Not, Recherche und Whistleblowing, politischer Aktivismus, Religion und Gesundheit – in all diesen Bereichen braucht

unsere Gesellschaft Anonymität und ist ein wirklich freier, unbefangener Gebrauch von Grundrechten nur im Schutz der Anonymität möglich.

II. Zur ersten Vorlagefrage (Personenbezug von IP-Adressen bei der Bundesrepublik Deutschland) soll in der mündlichen Verhandlung auf folgende Gesichtspunkte näher eingegangen werden:

Eine Unterscheidung zwischen dynamisch und statisch zugewiesenen IP-Adressen ist den Anbietern von Telemedien technisch unmöglich. Sie kann deswegen auch rechtlich keine Rolle spielen.

Die Bundesregierung behauptet in Ziff. 21 ihrer Stellungnahme, die meisten Juristen seien der Auffassung, die Frage der Bestimmbarkeit des Betroffenen einer Datenverarbeitung sei ausschließlich anhand des beim aktuellen Datenverarbeiter vorhandenen und legal zugänglichen Wissens zu bestimmen. Rechtlich unzulässige Identifikationsmöglichkeiten seien nicht zu berücksichtigen. Tatsächlich wird zu erläutern sein, dass nur wenige Juristen das Zusatzwissen Dritter außer Acht lassen wollen und dass etwa der Deutsche Juristentag das Gegenteil beschlossen hat. In dem Anhang zur Folgenabschätzung zu ihrem Vorschlag einer Datenschutz-Grundverordnung schreibt die EU-Kommission, eine aktuelle Studie zur Auswertung der diesbezüglichen Rechtsprechung habe festgestellt, dass die überwältigende Mehrzahl der Gerichtsurteile zu dieser Frage IP-Adressen als personenbezogene Daten einordneten.

Sowohl die grammatikalische als auch die teleologische Auslegung ergeben entgegen den Ausführungen der Bundesregierung, dass alle vernünftigerweise zur Identifikation einsetzbaren Mittel zu berücksichtigen sind. In der mündlichen Verhandlung wird zu erläutern sein, dass es gerade Sinn und Zweck des Datenschutzrechts ist, nicht erst Persönlichkeitsrechtsverletzungen zu verbieten, sondern ihnen schon vorzubeugen, indem das Entstehen vermeidbarer Datensammlungen von vornherein verhindert wird. Dieser vorgelagerte Schutz des Persönlichkeitsrechts ist weitaus wirksamer. Nur, wenn schon die Ansammlung von Daten unterbleibt, ist ihre missbräuchliche oder versehentliche Verwendung von vornherein ausgeschlossen. Die Erfahrung zeigt, dass das Risiko von Datenverlust, Datenklau, Datenverkauf oder Datenmissbrauch real ist, sich immer wieder verwirklicht und deswegen – entgegen der Meinung der Bundesregierung (Ziff. 47) – "vernünftigerweise" berücksichtigt werden muss. Schon alleine das Risiko einer rechtswidrigen Wissensnutzung und -generierung kann Menschen in ihrer Freiheit wesentlich hemmen, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

Die Konsequenzen einer etwaigen Verneinung des Personenbezugs von IP-Adressen werden darzustellen sein, nämlich dass zeitlich unbegrenzt sensible Informationen über den Inhalt unserer privaten und geschäftlichen Internetnutzung angesammelt und weitergegeben werden dürften. Der Einzelne wäre schutzlos gestellt, würde man eine unbeschränkte Sammlung und Speicherung von Informationen über ihn mit dem Argument zulassen, seine Identität könne von der momentan speichernden Stelle mit legalen Mitteln nicht bestimmt werden. Die relativierende Auffassung würde ein Eldorado für Kreditauskunfteien, Detekteien, Werbeunternehmen usw. eröffnen. Die Meinung der Bundesregierung, dies reiße keine Schutzlücke auf (Ziff. 35), findet keine Grundlage in der Datenschutzrichtlinie und gewährleistet keinen wirksamen Schutz, wie auszuführen sein wird.

Die Bundesregierung will außer Acht lassen, dass der Bund befugt ist, zur Strafverfolgung oder Gefahrenabwehr IP-Adressen zu identifizieren (Ziff. 46). Dem wird entgegen zu halten sein, dass die Bundesregierung die Nutzung ihrer Internetportale gerade zu dem erklärten Zweck personenbezogen speichert, um im Bedarfsfall zur Strafverfolgung oder Abwehr von Angriffen eine Identifizierung vornehmen zu können. Eben dies ist ihren zuständigen Stellen gesetzlich gestattet (§ 113 Telekommunikationsgesetz) und findet jährlich in einer fünfstelligen Zahl von Fällen statt. Es handelt sich daher um ein "vernünftigerweise" in Betracht zu ziehendes Mittel.

III. Zur zweiten Vorlagefrage (Vereinbarkeit mit der Datenschutzrichtlinie) soll in der mündlichen Verhandlung auf folgende Gesichtspunkte näher eingegangen werden:

Es soll erläutert werden, dass die zur Prüfung vorgelegte Vorschrift die Anonymität ausschließlich der Nutzung öffentlich zugänglicher Telemedien (Internetportale) schützt. Das Protokollierungsverbot gilt nicht für Kanäle (Ports), Zugänge oder Server, die nicht zur öffentlichen Nutzung freigegeben sind, insbesondere nicht für das unerlaubte Eindringen über nicht-öffentliche Zugänge.

Zur europäischen Rechtslage soll darauf eingegangen werden, dass Art. 7 Buchst. f) der Datenschutzrichtlinie 95/46/EG eine unbestimmte Generalklausel darstellt, die der Konkretisierung bedarf, um sie handhabbar zu machen. Anders als im Fall ASNEF (Az. C-468/10 und C-469/10) schließt die hier vorgelegte Vorschrift des Telemediengesetzes nicht "kategorisch und verallgemeinernd die Verarbeitung bestimmter Kategorien personenbezogener Daten aus". Soweit der Gerichtshof in der Rechtssache ASNEF die Berücksichtigung "besonderer Umstände des Einzelfalls" gefordert hat, gibt es doch abstrakt umschreibbare Fallgruppen, in denen unter keinen denkbaren Umständen ein überwiegendes Interesse des Datenverarbeiters im Sinne des Art. 7 Buchst. f) vorliegen kann. Es ist dem nationalen Gesetzgeber nach Art. 5 der Datenschutzrichtlinie nicht nur gestattet, sondern sogar geboten, abschließende Spezialregelungen für solche Fallgruppen zu erlassen, um die Generalklausel des Art. 7 Buchst. f) handhabbar zu machen, die praktische Wirksamkeit des Grundrechts auf Datenschutz und Rechtssicherheit zu gewährleisten.

Eine Vorschrift des vom vorlegenden Gerichts genannten Inhalts ist schon deswegen mit Art. 7 Buchst. f) der Datenschutzrichtlinie 95/46/EG vereinbar, weil es kein berechtigtes Interesse der Anbieter öffentlicher Internetportale an einer personenbezogenen Aufzeichnung der Nutzung ihres Angebots gibt oder weil jedenfalls das Interesse und die Grundrechte der betroffenen Nutzer auf anonymen und unbefangenen Informationszugang schwerer wiegen. Entgegen der Stellungnahmen der EU-Kommission (Ziff. 27) und der Österreichischen Regierung (Ziff. 13) fehlt es nicht an einer spezifischen Rechtsgrundlage, sondern schon am berechtigten Interesse des Anbieters öffentlicher Telemedien an einer personenbezogenen Nutzungsprotokollierung.

Es wird zu zeigen sein, dass eine personenbezogene Aufzeichnung der Nutzung öffentlicher Telemedien weder geeignet noch in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist, um "die generelle Funktionsfähigkeit des Telemediums zu gewährleisten". Die generelle Funktionsfähigkeit öffentlicher Telemedien ist ohne personenbezogene Nutzungsprotokollierung zu gewährleisten. Entscheidend für die generelle Funktionsfähigkeit und Sicherheit öffentlicher Telemedien ist die fachgerechte Einrichtung und Instandhaltung der erforderlichen Systeme. Es ist unverhältnismäßig, wegen der allgemeinen Möglichkeit von Sicherheitsverletzungen das Nutzungsverhalten auch aller rechtmäßig handelnder Nutzer personenbezogen aufzuzeichnen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit Störungen stehen könnte.

Soweit das vorlegende Gericht die Abwehr sogenannter Überlastungsangriffe ("Denial-of-Service"-Attacken) anspricht (Ziff. 36 f.), ist die Vorlage unzulässig, weil offensichtlich nicht entscheidungserheblich. Wie das vorlegende Gericht selbst anführt (Ziff. 3), beantragt der Kläger im Ausgangsrechtsstreit ein Verbot der personenbezogenen Protokollierung ausdrücklich nur, "soweit die Speicherung nicht im Störfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist". Nach deutschem Recht darf eine Verurteilung nicht über den Antrag hinaus erfolgen, § 308 Absatz 1 Satz 1 Zivilprozessordnung.

Soweit die Portugiesische Regierung das Strafverfolgungsinteresse anführt (Ziff. 17), ist dieses nicht Gegenstand von Artikel 7 Buchst. f) der Datenschutzrichtlinie 95/46/EG und damit nicht Gegenstand der

Vorlage. Strafverfolgung ist nicht Aufgabe der Anbieter öffentlicher Telemedien. Das Telemediengesetz enthält Sonderregelungen für Strafverfolgungszwecke.

Es soll in der mündlichen Verhandlung abschließend erläutert werden, warum ein überragendes Interesse an einer anonymen Nutzung auch elektronischer Medien besteht, welches etwaige Speicherinteressen der Anbieter überwiegt. Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung betont, dass die Internetnutzung nicht inhaltlich festgehalten und damit rekonstruierbar bleiben darf. Wer mit Nachteilen wegen des Inhalts seiner Internetnutzung rechnen muss, wird möglicherweise nicht mehr unbefangen von seiner Informations- und Meinungsäußerungsfreiheit im Internet Gebrauch machen. Eine Speicherung des Internet-Nutzungsverhaltens erlaubt die Rekonstruktion des Inhalts der gelesenen oder geschriebenen Informationen und hat damit eine noch weiter reichende Qualität als eine Speicherung von Verkehrs- oder Metadaten. Der Gerichtshof sollte sein wegweisendes Urteil zur Unverhältnismäßigkeit einer unterschiedslosen Vorratsspeicherung von Verkehrsdaten aufgreifen und die unterschiedslose Erfassung sogar des Inhalts unserer Internetnutzung als erst recht unverhältnismäßiges Mittel verwerfen.

IV. In Anbetracht der oben genannten komplexen Hintergründe und der hohen Bedeutung der Rechtssache ist ein mündlicher Vortrag von 30 Minuten angemessen und erforderlich, um eine ausreichende Darlegung bzw. Widerlegung der maßgeblichen Punkte zu ermöglichen.



Starostik
-Rechtsanwalt-