Rechtssache Breyer ./. Bundesrepublik (Az. C-582/14)

Plädoyer des Klägervertreters RA Meinhard Starostik am 25.02.2016

I. Zunächst soll 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. Die Datenschutzrichtlinie ist anwendbar.
Zunächst: Die Entscheidungserheblichkeit der Vorlagefragen für den Ausgangsrechtsstreit beurteilt das vorlegende Gericht grundsätzlich selbst. Es ist nicht offensichtlich, dass die Datenschutzrichtlinie auf den Ausgangsrechtsstreit keine Anwendung fände. Im Gegenteil: Im Streit steht keine Datenverarbeitung "betreffend die öffentliche Sicherheit", "die Sicherheit des Staates" oder "die Tätigkeiten des Staates im strafrechtlichen Bereich".
Das nationale Recht regelt das Angebot von Telemedien (im Europarecht: "Dienste der Informationsgesellschaft") privatrechtlich und für alle Anbieter gleich. Wenn die Bundesrepublik ihre Webserver schützen will, verfolgt sie Eigeninteressen wie jeder private Anbieter auch und nicht etwa Interessen der Allgemeinheit.
Der Richtlinienentwurf zur Cybersicherheit belegt, dass die Netz- und Informationssicherheit in den Anwendungsbereich des Gemeinschaftsrechts fällt.
Im Ausgangsrechtsstreit hat das Landgericht festgestellt, dass sich die Klage "nicht gegen ein hoheitliches Handeln" richtet. Die Bundesrepublik nehme mit ihren Telemedien zwar eine öffentliche Aufgabe wahr. Die Datenschutzregelungen seien aber nicht speziell auf sie als Trägerin öffentlicher Gewalt zugeschnitten, sondern gelten für jeden Anbieter von Telemedien gleichermaßen.

Ähnlich wie der Gerichtshof in der Rechtssache Irland vs. Europäisches Parlament (Rs. C-301/06) geurteilt hat, geht es bei der Vorratsspeicherung von IP-Adressen um die Tätigkeit der Anbieter von Telemedien und nicht um den Zugang zu den Daten oder deren Nutzung durch die Polizei- und Justizbehörden der Mitgliedstaaten. Die Vorratsspeicherung von IP-Adressen selbst bringt keine hoheitlichen Maßnahmen der Gefahrenabwehr oder Strafverfolgung mit sich. Es geht ausschließlich um Daten, die eng mit der Bereitstellung öffentlicher Telemedien verbunden sind.
Die Vorratsspeicherung von IP-Adressen erfolgt auch organisatorisch nicht bei einer Gefahrenabwehr- oder Justizbehörde, sondern bei der Stelle, die das Telemedium anbietet.
Das nationale Recht enthält Sonderbestimmungen für Strafverfolgung und Gefahrenabwehr, aber im Ausgangsrechtsstreit geht es um die IP-Adressen des Klägers, die ohne jeden Bezug zur Tätigkeit von Polizei- und Justizbehörden gespeichert werden, wann immer er öffentliche Telemedien der Bundesrepublik nutzt.

III. Zur ersten Vorlagefrage (Personenbezug von IP-Adressen bei der Bundesrepublik Deutschland):

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 wollen nur wenige Juristen das Zusatzwissen Dritter außer Acht lassen und hat etwa der Deutsche Juristentag 2012 das Gegenteil beschlossen: "Als 'personenbezogen' sind Daten anzusehen, bei denen im Sinne eines abstrakten Gefährdungspotentials, selbst auf Grund theoretisch möglicher Verknüpfungen, ein … Personenbezug hergestellt werden kann. Ob und inwieweit solche Verknüpfungen unter praktischen Gesichtspunkten vorgenommen werden, sollte unberücksichtigt bleiben." 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. Es ist gerade Sinn und Zweck des Datenschutzrechts, 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. Hinzu kommt das Grundproblem des Datenschutzrechts – dass Datenschutzverstöße in der Praxis selten entdeckt und wenn entdeckt, dann kaum je sanktioniert werden. Schon alleine das Risiko einer rechtswidrigen Wissensnutzung und -generierung kann Menschen in ihrer Freiheit wesentlich hemmen, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

Nach der Theorie der Bundesregierung eines „relativen Personenbezugs“ soll das Datenschutzrecht zwar nicht für die Speicherung, wohl aber für die Übermittlung „relativ“ personenbezogener Daten an eine Stelle mit Zusatzwissen gelten. Diese in freier Rechtsschöpfung vorgenommene Unterscheidung findet keinerlei Stütze in der Datenschutzrichtlinie. Die dortigen Regelungen sowohl der Datenspeicherung wie auch der Datenübermittlung beziehen sich gleichermaßen auf personenbezogene Daten. Es ist in sich widersprüchlich, dass ein und dasselbe Datum für ein und dieselbe Stelle einmal (bei der Speicherung) nicht personenbezogen, ein andermal (bei der Übermittlung) aber personenbezogen sein soll.

Der "relative Personenbezug" würde auch keinen wirksamen Schutz gewährleisten: Konsequenz einer Verneinung des Personenbezugs gespeicherter IP-Adressen wäre, dass zeitlich unbegrenzt sensibelste Informationen über den Inhalt unserer privaten und geschäftlichen Internetnutzung angesammelt 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. Dass ein Datum bei der aktuell speichernden Stelle 'relativ anonym' sein mag, beruhigt im Zeitalter des Internet niemanden mehr. Schon die – erfahrungsgemäß nicht unbegründete – Befürchtung von Nachteilen infolge einer Identifizierung beeinträchtigt die freie Entfaltung der Persönlichkeit. Die Menschen sehen ein reales Risiko von Datenmissbrauch und richten ihr Verhalten darauf ein. Die Rechtsordnung muss dem Rechnung tragen.

Die Bundesregierung will außer Acht lassen, dass der Bund befugt ist, zur Strafverfolgung oder Gefahrenabwehr IP-Adressen zu identifizieren (Ziff. 46). Dem ist entgegen zu halten, 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 (so auch Rn. 2 des Vorlagebeschlusses). 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):

Zunächst ist zu betonen: Das nationale Recht (§ 15 TMG) schützt die Anonymität ausschließlich der Nutzung öffentlich zugänglicher Telemedien (Internetportale). 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.

Art. 7 Buchst. f) der Datenschutzrichtlinie 95/46/EG stellt eine unbestimmte Generalklausel dar, die der Konkretisierung bedarf, um sie handhabbar zu machen. Anders als in der Rechtssache 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.

Eine personenbezogene, systematische Aufzeichnung der Nutzung öffentlicher Telemedien ist weder geeignet noch in einer demokratischen Gesellschaft notwendig und verhältnismäßig, um "die generelle Funktionsfähigkeit des Telemediums zu gewährleisten". Die generelle Funktionsfähigkeit öffentlicher Telemedien ist ohne personenbezogene Nutzungsprotokollierung zu gewährleisten. Dies belegen beispielsweise die Internetportale von Bundesjustizministerium, Bundesfinanzministerium und Bundesdatenschutzbeauftragter, die keine IP-Adressen speichern. Im Ausgangsrechtsstreit ist ein ausführliches technisches Gerichtsgutachten zu der Frage eingeholt worden, das zu dem eindeutigen Ergebnis gelangt: "Eine Speicherung von IP-Adressen ist weder zur Angriffserkennung noch zur Angriffsabwehr zwingend erforderlich. Vielmehr existiert eine Reihe von bekannten und in der Praxis angewendeter Verfahren, die ohne eine Speicherung von IP-Adressen Angriffe erfolgreich erkennen und abwehren können."

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 Angriffen oder 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 Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich ist". Nach deutschem Recht darf eine Verurteilung nicht über den Antrag hinaus erfolgen.

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.

Abschließend ist nochmals hervorzuheben, warum ein so 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.

In Anlehnung an Edward Snowden meint der Kläger: Niemand hat das Recht, alles, was wir im Netz sagen, und alles, was wir tun, aufzuzeichnen. Als Generation Internet haben wir das Recht, uns im Netz ebenso unbeobachtet und unbefangen informieren zu können, wie es unsere Eltern aus Zeitung, Radio oder Büchern konnten. Europa muss der NSA-Methode einer Totalerfassung des digitalen Lebens eine klare Absage erteilen und den Grundrechten auf Informations- und Meinungsfreiheit im Internet zur Geltung verhelfen.