Das „Fashion ID“-Urteil des EuGH vom 29.07.2019
Alle Klarheiten beseitigt?
[23.08.2019]

Von: **Dr. Axel-Michael Wagner**

Einleitung

Der datenschutzrechtliche Begriff der „gemeinsam Verantwortlichen“ für Datenverarbeitungsaktivitäten hat den EuGH nun in relativ kurzer Zeit schon zum dritten Mal beschäftigt. Nach der Facebook-Fanpages-Entscheidung und der Zeugen-Jehovas-Entscheidung wurde nun eine weitere Fallkonstellation im Rahmen der Fashion-ID-Entscheidung bewertet.

Den HTML-Quellcode des allseits bekannten „Like Buttons“ („Gefällt mir“) kann jeder Webseiten-Betreiber auf der Facebook-Seite generieren und als „Codeschnipsel“ in den HMTL-Code seiner eigenen Webseite einkopieren. Der EuGH hatte zu bewerten, inwieweit der Webseiten-Betreiber und Facebook gemeinsam Verantwortliche für die personenbezogenen Daten sind, die beim Aufruf der Seite – und damit des „Codeschnipsels“ – durch einen Besucher an Facebook übermittelt werden. Ist der Webseiten-Betreiber für die an Facebook übermittelten Daten datenschutzrechtlich mitverantwortlich, könnten ihn datenschutzrechtliche Pflichten – wie zur Einholung einer Einwilligung oder zur Pflichtinformation des Betroffenen – treffen.

Der konkrete Fall ist juristisch ein weiterer Baustein im Ringen um ein einigermaßen konsistentes datenschutzrechtliches Gerüst zur Bewertung der sich ständig weiterentwickelnden Internet-Technologien, das – im Wesentlichen durch den EuGH – in den nächsten Jahren ausformuliert werden muss. Bekanntlich wurde das Datenschutzrecht seit jeher hochabstrakt und „technologieneutral“ formuliert, was Fluch und Segen zugleich ist. Während sich Politiker nach Erlass der DSGVO rühmten, nun ein durchschlagendes Mittel gegen die „Datensammelwut von Google, Facebook, Amazon & Co.“ gefunden zu haben, was ihnen auch die eine oder andere Wählerstimme eingebracht haben mag, sucht man überzeugende Hinweise für genau diese durchschlagende Wirkung im Text der DSGVO eher vergeblich. Stattdessen hat die Einführung der DSGVO gerade kleinere und mittlere Unternehmen viel Blut, Schweiß und Tränen gekostet, während nach wie vor unklar ist, welchen Umtrieben der großen Internet-Konzerne nun tatsächlich Einhalt geboten wurde. Auch die Fashion-ID-Entscheidung erging nicht gegen Facebook oder die für Facebook zuständige irische Datenschutzaufsichtsbehörde, sondern gegen Fashion ID, einen „Cross-Channel Fashion-Retailer" der Peek & Cloppenburg KG Düsseldorf, der eine Facebook-Technologie verwendete.

Die drei genannten Entscheidungen des EuGH zur Stellung als „gemeinsam Verantwortliche" sind jeweils noch zum alten Recht, sprich zur Datenschutzrichtlinie 1995, ergangen. Es wird aber allgemein angenommen, dass die hier entwickelten Grundsätze auch unter der DSGVO zur Anwendung kommen, dessen Artikel 26 die Stellung als gemeinsame Verantwortliche in der unnachahmlichen Art des DSGVO-Texts schlicht so definiert:

> „Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche."

Schon nach den ersten beiden Entscheidungen des EuGH waren viele Datenschutzrechtler der Ansicht, dass die Stellung als gemeinsame Verantwortliche für Datenverarbeitungshandlungen häufiger vorliegen würde, als man dies bislang angenommen hatte. Unter der Datenschutzrichtlinie 1995 hatte diese Stellung ein „Mauerblümchendasein" geführt, weil die Richtlinie keine weitergehenden Konsequenzen anordnete als dass beide Verantwortliche für dieselben Datenverarbeitungsaktivitäten verantwortlich waren. Art. 26 der DSGVO sieht nun aber als (weitere) Rechtsfolge vor, dass die gemeinsam Verantwortlichen eine Vereinbarung abzuschließen haben, deren Inhalte sie den Betroffenen auch mitteilen müssen. Damit führt die Stellung als gemeinsam Verantwortliche nicht nur zu einer gemeinsamen Haftung, sondern löst auch unmittelbar die Pflicht aus, sich bereits im Vorfeld der Aufnahme der Datenverarbeitungstätigkeit mit dem anderen Verantwortlichen auf die Modalitäten der „Gemeinschaft" zu einigen.

Was tut ein Codeschnipsel?

Bekanntlich wird im Internet zwischen dem Endgerät eines Webseiten-Besuchers und den Servern des Webseiten-Betreibers immer wieder „irgendetwas“ hin- und hergeschickt, und die Juristen tun sich oft schwer damit, dies zu erfassen und rechtlich einzuordnen. Der Facebook-Like-Button ist ein Beispiel für eine Internet-Technik, bei der

- bereits bei Aufruf einer Internet-Seite (durch Eingabe in der Adresszeile des Browsers oder durch Klick auf einen Link) der entsprechende HTML-Code der Seite den Browser des Benutzers dazu veranlasst, den Server eines Dritten „anzufunken“, und
- der Benutzer nicht darüber informiert wird, was geschieht (und er auch keine Möglichkeit hat, dies zu verhindern).

Man kann dies aber auch weiter formulieren: Der Aufruf einer Internet-Seite startet letztlich ein Programm auf dem eigenen Rechner. Und so wie bei jedem Start eines Programms, das man nicht selbst geschrieben oder selbst analysiert („re-engineered“) hat, kann das Programm Aktionen auslösen, die man anhand der „Beschreibung“ oder einer sonstigen Erwartungshaltung nicht vermutet hätte. Da heutzutage beinahe jedes IT-System beinahe ständig mit dem Internet – sprich: mit weiteren Rechnern – verbunden ist, kann eine unerwartete Aktion eines gestarteten Programms selbstverständlich auch die Übermittlung von Daten an Dritte sein. Dasselbe Problem stellt sich beispielsweise auch mit der Übermittlung von Telemetriedaten („Nachhause-Telefonieren“) durch diverse Microsoft-Produkte, worauf wir am Ende noch zurückkommen werden. Was die „black box“ – das Programm – tatsächlich tut, kann nur eine Analyse des jeweiligen Programmcodes oder des entstehenden Netzwerkverkehrs zeigen, und auch dort sind die Möglichkeiten begrenzt: Programme können zu komplex sein, Netzwerkverkehr kann verschlüsselt werden, größere Datenmengen können „tröpfchenweise“ abfließen, ohne dass dies bei einer Analyse erkennbar wäre etc.

Im Bereich von Browser-basierten Technologien wie HTML und diversen Skript-Sprachen, deren Quellcode meist offen zutage liegt, ist dies naturgemäß einfacher zu analysieren als bei umfangreichen Programmpaketen, die (mit Administratorzugriff) installiert werden müssen. Weder einer Webseite noch einer Programm-Installationsdatei „sieht man an“ was sie auslösen wird. Es steht daher zu vermuten, dass das Hase-und-Igel-Spiel zwischen der Entwicklung neuer Techniken und der mühsamen rechtlichen Aufarbeitung immer weiter gehen wird. Die diese technischen Gegebenheiten zusammenfassende Aussage des EuGH, es sei *„nach der Vorlageentscheidung eine Eigenart des Internets, dass der Browser des Internetbesuchers Inhalte aus verschiedenen Quellen darstellen kann“*, wirkt demgegenüber etwas unbeholfen.

Im konkreten Fall des Like-Buttons wird vom Betreiber der Seite (d. h. vom Ersteller des „Programms“) – wie auch bei Google Maps, Google Fonts etc. – ein „Codeschnipsel“ des jeweiligen Drittanbieters in die Seite integriert. Beim Aufruf der Seite wird den Servern von Facebook, durch den „Codeschnipsel“ ausgelöst bzw. gesteuert, mitgeteilt, auf welcher Seite sich der Benutzer gerade befindet (sowie möglicherweise einige Informationen über das von ihm verwendete System übermittelt). Daneben wird, wenn sich ein Facebook-Cookie auf dem Rechner des Benutzers befindet, dieser ausgelesen und an Facebook gesendet. Ist der Benutzer bei Facebook angemeldet, enthält das Cookie die Facebook-Sitzungs-ID, sodass Facebook den Aufruf der Seite einem Facebook-Kunden und dessen Profil zuordnen kann. Ist der Benutzer nicht bei Facebook angemeldet, so setzt bzw. liest der Codeschnipsel – so die im Internet verfügbaren Informationen – ein eigenes Zwei-Jahres-Cookie, welches Facebook den Aufbau eines zunächst pseudonymen „Surf-Profils“ erlaubt. Dass dabei auch die IP-Adresse des Benutzers übertragen wird, ist ohnehin selbstverständlich, denn ohne deren Übermittlung wäre technisch keine Kommunikation zwischen dem Rechner des Benutzers und dem Social-Media-Anbieter möglich.

All dies merkt der Benutzer natürlich nicht, wie auch der EuGH – anscheinend etwas ungläubig – ausführt:

> „Offenbar erfolgt diese Übermittlung, ohne dass sich der Besucher dessen bewusst ist und unabhängig davon, ob er Mitglied des sozialen Netzwerks Facebook ist oder den „Gefällt mir“-Button von Facebook anklickt.“

Auf das Auslesen des Cookies kommen wir später noch zurück; der EuGH hat diesen Teil des Sachverhalts nicht bewertet, sondern die Ermittlung des technischen Sachverhalts insoweit dem Oberlandesgericht Düsseldorf überantwortet (s. u.). Zunächst geht es demnach nur um das Erheben und Übermitteln von IP-Adresse, aktuell besuchter Webseite und ggf. Informationen über das verwendete System im Zuge des Aufrufs der Webseite bzw. des „Codeschnipsels“.

Ahnungsloser Lockvogel?

Ähnlich wie auch schon in der dem Fanpage-Urteil des EuGH zugrundeliegenden Konstellation handelt es sich um ein Zusammenwirken zweier Parteien: Ein Webseiten- oder Fanpage-Betreiber „lockt mit seinen Inhalten Benutzer an“ und ermöglicht so dem Social-Media-Anbieter die Erhebung und Analyse von personenbezogenen Daten. Was dem Social-Media-Anbieter genau ermöglicht wird, wissen die wenigsten Webseiten-Betreiber, und das ist im Rahmen ihrer originären Tätigkeit (z. B. Online-Shop) auch gar nicht notwendig bzw. für die Zweckerreichung (Erhöhung der Aufmerksamkeit „auf Facebook“ und damit der Reichweite) irrelevant. Der Betreiber bzw. dessen Web-Agentur wird daher im Regelfall auch weder eine Beschreibung des „Codeschnipsels“, wenn es eine solche überhaupt gibt, zur Kenntnis nehmen (außer die technische Anleitung über die Einbindung), noch analysieren, welchen Aufruf der aufgenommene „Codeschnipsel“ des Social-Media-Anbieters tätigt bzw. welche Parameter er übergibt. Er könnte ohnehin auch nichts verändern, wie der EuGH ausführt:

> „Welche Informationen der Browser übermittelt und was der Drittanbieter mit diesen Informationen macht, insbesondere, ob er diese speichert und auswertet, kann der den Drittinhalt auf seiner Website einbindende Betreiber nicht beeinflussen.“

Aus Haftungssicht müsste man sagen: Er hätte aber natürlich auch auf die Einbindung verzichten können.

Im konkreten Fall geht der EuGH dennoch von einem Wissen der konkreten Webseiten-Betreiberin aus, denn diese hat den „Codeschnipsel“ von Facebook

> „in ihre Website offenbar in dem Wissen eingebunden, dass dieser als Werkzeug zum Erheben und zur Übermittlung von personenbezogenen Daten der Besucher dieser Seite dient, unabhängig davon, ob es sich dabei um Mitglieder des sozialen Netzwerks Facebook handelt oder nicht“.

Woher genau dieses (umfassende) Wissen stammt, ist unklar. Im Ausgangsverfahren vor dem LG Düsseldorf erklärte der Webseiten-Betreiber, keine Kenntnis darüber zu haben, inwieweit Facebook einen Abgleich der IP-Adressen der Facebook-Nutzer mit den durch den „Codeschnipsel“ übermittelten IP-Adressen der Besucher der Website vornehmen kann. Gleichermaßen, so der Webseiten-Betreiber weiter, habe er keine Kenntnis von der vom klagenden Verbraucherschutzverband behaupteten Möglichkeit, dass Facebook – durch das Setzen eines dauerhaften Cookies – die Zuordnung auch nachträglich herstellen kann, sobald der Besucher der Webseite einen Facebook-Account zu einem späteren Zeitpunkt erstellt.

Allerdings hatte der Webseiten-Betreiber in seiner Datenschutzerklärung Hinweise zur Nutzung des „Like-Buttons" („Social Plugins") aufgenommen und die Besucher der Webseite darauf hingewiesen,

> „dass es, um die Speicherung Ihrer Daten und eine Verknüpfung mit den in dem sozialen Netzwerk gespeicherten Informationen zu verhindern, ratsam sei, sich zuvor aus dem entsprechenden sozialen Netzwerk auszuloggen. Auch sei es möglich, die Funktion der Plugins der sozialen Netzwerke mit sog. Add-Ons für den Browser zu blockieren."

Zudem war in der Datenschutzerklärung ein Link auf die Datenschutzerklärung Facebooks enthalten, die eine Information über die dort stattfindenden Datenerhebungs- und Verarbeitungsvorgänge enthielt. Schließlich berief sich der Webseiten-Betreiber selbst darauf,

> „ein sich im Internet bewegender Nutzer rechne regelmäßig damit, dass die Einbindung von Drittinhalten die Weitergabe von technischen Informationen an den Drittanbieter impliziere, dieses Bewusstsein habe er schon vor Aufruf einer Seite."

Es steht zu vermuten, dass der EuGH dem Webseiten-Betreiber „vorwirft" – parallel zu dessen gerade zitierter Aussage –, dass wer eine erhöhte Reichweite seines Internetauftritts anstrebt und sich dazu eines „Codeschnipsels" eines Social-Media-Anbieters bedient, sich wohl automatisch darüber bewusst ist, dass beim Aufruf der Webseite (stets?) personenbezogene Daten an den Social-Media-Anbieter übermittelt werden. Die Hinweise des Webseiten-Betreibers zur Nutzung des „Social Plugins" in seiner eigenen Datenschutzerklärung legen nahe, dass dieser zumindest eine vage Vorstellung von der Funktionsweise des „Codeschnipsels" gehabt haben musste, auch wenn die angeratene Maßnahme, sich vorab auszuloggen, aus der Perspektive der Datenerhebung und -übermittlung letztlich nutzlos war.

Ob auch dann, wenn dieses Wissen nicht bestanden hätte – es wäre interessant gewesen zu erfahren, ob und welche „Prüfpflichten" (Code-Untersuchungen) der EuGH hier voraussetzen würde –, ein „Wissenmüssen" ausgereicht hätte, ist unklar. Immerhin könnte in ähnlichen Fallkonstellationen die Erhebung und Übermittlung personenbezogener Daten durch die eingesetzten Programme „verschleiert" stattfinden (sog. „obfuscation"), sodass der Umfang dieser Aktivitäten kaum zu durchschauen ist.

Jedenfalls im Wissen um dessen Funktion gerät der Betreiber also durch die Einbindung eines „Codeschnipsels" in eine Mithaftung für die Datenverarbeitungstätigkeit des Social-Media-Anbieters. In erster Näherung werden demnach die Mittel der Datenverarbeitung – bezogen auf die an den Social-Media-Anbieter übermittelten Daten – von beiden „arbeitsteilig" festgelegt: Vom Social-Media-Anbieter über das Design des Codeschnipsels und der dahinterliegenden, die Daten verarbeitenden Server-Plattform, vom Betreiber über die Integration des Codeschnipsels in den Code seiner Webseite. Der EuGH nähert sich dieser Thematik freilich etwas anders, wie unten noch zu zeigen sein wird.

Wer ist zivilrechtlich für ein datenschutzwidriges Webdesign verantwortlich?

Im Zusammenhang mit der Frage des Wissens um die Funktion des „Codeschnipsels" ist noch anzufügen, dass eine Webseite häufig nicht von ihrem späteren Betreiber selbst verfasst wird. Üblicherweise entwickelt eine Web-Agentur den Internet-Auftritt und implementiert in diesem Zuge „Codeschnipsel" von Drittanbietern. In diesem Zusammenhang stellt sich die Frage, ob der Vertrag zwischen dem Webseiten-Betreiber und seiner Web-Agentur eine – ggf. nicht ausdrücklich geschriebene – Verpflichtung zur (rechtlichen) Prüfung der „Compliance" des Arbeitsergebnisses und entsprechender Aufklärung und Beratung des Webseiten-Betreibers enthält. Bezüglich der vergleichbaren Konstellation bei Urheberrechtsverletzungen durch Aufnahme von Inhalten Dritter auf einer Webseite hat die Rechtsprechung vereinzelt bereits eine Prüfungs- und Beratungspflicht des gewerblich tätigen Webdesigners bezüglich möglicherweise bestehender Urheberrechte Dritter bejaht und dies sogar dann, wenn dem Webdesigner das Material von seinem Auftraggeber, also dem Website-Betreiber selbst, zur Verfügung gestellt wurde. Auch im Rahmen von Softwareentwicklungsverträgen sollen ungeschriebene Aufklärungspflichten des Unternehmers über eventuell bestehende gesetzliche Erfordernisse, denen die Software genügen muss, bestehen. Eine allgemeine Rechtsberatungspflicht soll dagegen nicht bestehen. Auch hängt der Umfang der Beratungspflichten wesentlich von den Fachkenntnissen des Auftraggebers im Einzelfall ab.

Übertragen auf den Fall des EuGH hieße das, dass die zuständige Web-Agentur eventuell auf die Notwendigkeit des Abschlusses einer Vereinbarung mit Facebook – als „gemeinsam Verantwortlichen" – hätte hinweisen müssen. Allerdings könnte eine solche Verpflichtung zur datenschutzrechtlichen „Rechtsberatung" des Auftraggebers gegen das Rechtsdienstleistungsgesetz verstoßen. § 5 Abs. 1 RDG gibt vor:

„Erlaubt sind Rechtsdienstleistungen im Zusammenhang mit einer anderen Tätigkeit, wenn sie als Nebenleistung zum Berufs- oder Tätigkeitsbild gehören. Ob eine Nebenleistung vorliegt, ist nach ihrem Inhalt, Umfang und sachlichen Zusammenhang mit der Haupttätigkeit unter Berücksichtigung der Rechtskenntnisse zu beurteilen, die für die Haupttätigkeit erforderlich sind.“

Die Tätigkeit einer Web-Agentur wird in den gängigen Kommentaren zu dieser Vorschrift nicht aufgegriffen. Es ist also unklar, in welcher Detailtiefe eine Web-Agentur hätte aufklären können und müssen – insbesondere, ob sie das Urteil des EuGH hätte „vorhersehen“ müssen (und für den nun eingetretenen Schaden – zumindest Kosten – haften würde) und ob sie in zukünftigen Fällen auch nur geringfügige Abweichungen zum „Facebook-Like-Button“-Fall rechtlich analysieren müsste. Muss also der Webseiten-Betreiber die rechtliche Zulässigkeit der technischen Details einer Webseite, die er nicht selbst erstellt hat, mit eigenen Kapazitäten (Datenschutzbeauftragter) oder durch Rechtsanwälte prüfen (lassen), um derartigen „Fallen“ zu entgehen? Und wie würde er sich entscheiden (sollen), wenn das Standard-Argument doch lautet, „dass das alle so machen“? Was würde er tun, wenn Facebook – was zu vermuten ist – sich weigern würde, eine solche Vereinbarung abzuschließen, weil Facebook eine andere Ansicht zur datenschutzrechtlichen Einordnung vertritt?

Vermutlich ist dies ein Fall für „Legal Tech“, namentlich die maschinelle Auswertung von Webseiten-Code und die Erstellung eines (rechtlichen) Gutachtens aus entsprechenden Versatzstücken. Dadurch wird aber auch noch nicht klarer, wie eine „vernünftige“ Lösung des Problems aussehen kann.

Phasenscheibchen

Das wirklich Neue am Facebook-Like-Button-Urteil des EuGH ist (in Weiterentwicklung der sog. Zeugen-Jehovas-Entscheidung des EuGH), dass die gemeinsame Verantwortlichkeit des Webseiten-Betreibers und des Social-Media-Betreibers – die datenschutzrechtliche „Mithaftung“ –in zeitliche Phasen aufgeteilt wird. Sie erstreckt sich also nicht auf sämtliche Datenverarbeitungshandlungen bezüglich der an Facebook übermittelten Daten (insbesondere diejenigen, die ausschließlich bei Facebook stattfinden), sondern nur auf die Phase der Erhebung und Übermittlung der Daten an den Social-Media-Betreiber. In Zukunft ist also – wie granular im Einzelnen, ist offen – jede Verarbeitungshandlung auf eine Mittel- und/oder Zwecküberschneidung mit möglichen anderen Verantwortlichen zu prüfen. Ergibt sich eine Überschneidung für einzelne Verarbeitungshandlungen, liegt für diese Verarbeitungshandlungen eine gemeinsame Verantwortlichkeit vor und eine entsprechende Vereinbarung muss für diese Phase abgeschlossen werden. Der EuGH liest diese Aufteilung in Phasen – natürlich – wie selbstverständlich aus der EU-Datenschutzrichtlinie heraus.

Gemeinsame Festlegung der Zwecke und Mittel der Verarbeitung

Die entscheidende Frage an dieser Stelle ist, wo die Grenzen der gemeinsamen Verantwortlichkeit innerhalb einer Phase liegen. Es ist unter der DSGVO nach wie vor offen, ob lediglich eine Überschneidung von Zweck „oder“ Mittel ausreicht – so hatte es einst die Art.-29-Arbeitsgruppe unter der EU-Datenschutzrichtlinie formuliert – oder ob eine Überschneidung in beiden Dimensionen gleichermaßen vorliegen muss. Ebenso ist offen, ob jedes Maß an Teilüberschneidung reicht. Hierzu führt der EuGH einerseits aus, dass eine gemeinsame Verantwortlichkeit für Verarbeitungsvorgänge voraussetzt, dass *„über deren Zwecke und Mittel“* gemeinsam entschieden wird. Andererseits führt der EuGH aus, dass eine datenschutzrechtliche Haftung einer verantwortlichen Person für vor- und nachgelagerte Verarbeitungsvorgänge ausscheidet *„für die sie weder die Zwecke noch die Mittel festlegt“*. Ersteres führt zu „und“, letzteres zu „oder“. Im weiteren Verlauf der Entscheidung wird allerdings das (sich auch aus dem Text der DSGVO ergebende) „und“ als Basis für die Subsumtion verwendet. Auch in der Fanpage-Entscheidung des EuGH wurde ein *„Beitrag zur Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten“* gefordert. Die entgegenstehenden Äußerungen der Art.-29-Datenschutzgruppe könnten damit obsolet sein.

PSP MÜNCHEN

Mittelüberschneidung

Was nun zunächst die Mittel angeht, so ergibt sich natürlich bei technischer Betrachtung, dass der Webseiten-Betreiber, der den „Codeschnipsel“ einbindet, mithilfe seines Servers die an den Social-Media-Betreiber gesendeten Daten weder „erhebt“ noch „weitergibt“. Die Daten werden, wenn man dies so interpretieren möchte, allenfalls vom Facebook-„Codeschnipsel“ (als verlängerter Arm von Facebook) erhoben und weitergegeben, eigentlich aber eher vom Browser des Benutzers, der diesbezüglich durch den „Codeschnipsel“ gesteuert wird. Die maßgeblichen Daten gelangen zu keinem Zeitpunkt an den Server des Webseiten-Betreibers; der Browser des Benutzers nimmt vielmehr direkt Kontakt zum Social-Media-Betreiber auf.

Dass es aber für die rechtliche Einstufung als gemeinsam Verantwortliche nicht notwendig ist, dass jeder Beteiligte auch technisch Zugang zu den generierten Daten haben muss, stellt der EuGH in diesem Zusammenhang (nochmals) ausdrücklich klar. Dementsprechend ist der rechtliche Anknüpfungspunkt der gemeinsamen Verantwortlichkeit im Rahmen der Festlegung gemeinsamer Mittel – wie auch in der Fanpage-Entscheidung – eher in einer (Mit-)Verursachung als in einem „gemeinschaftlichen Erheben“ der Daten zu sehen. Dadurch, dass der Webseiten-Betreiber den „Codeschnipsel“ von Facebook eingebunden hat, hat er einen kausalen „Tatbeitrag“ gesetzt. Dementsprechend formuliert der EuGH dann auch deutlich:

> „Mit der Einbindung eines solchen Social Plugins in ihre Website hat Fashion ID im Übrigen entscheidend das Erheben und die Übermittlung von personenbezogenen Daten der Besucher dieser Seite zugunsten des Anbieters dieses Plugins, im vorliegenden Fall Facebook Ireland, beeinflusst, die ohne Einbindung dieses Plugins nicht erfolgen würden.“

Im Grunde geht es also nicht um die (Teil-)Überschneidung von EDV-Mitteln – also den Einsatz derselben Hard- oder Software –, sondern um einen „Kausalbeitrag“ zur Datenverarbeitung durch den Webseiten-Betreiber, oder in den Worten der klassischen Kausalitätsformel: Das Handeln des Webseiten-Betreibers kann nicht hinweggedacht werden, ohne dass dadurch nicht auch die Datenverarbeitung durch den Social-Media-Betreiber entfiele. Der EuGH folgert offensichtlich alleine aus dieser Kausalität, dass die Mittel der Datenverarbeitung gemeinsam festgelegt wurden, d. h. wenn jemandem auch nur eine „Möglichkeit zur Mitbeeinflussung“ der Verarbeitung eingeräumt wird, selbst wenn er sich ansonsten (nämlich bei der eigentlichen Verarbeitung) „im Hintergrund hält“, kommt es bereits zu einer gemeinsamen Verantwortung.

Man könnte dem EuGH nun natürlich entgegenhalten, dass wenn der Gesetzgeber mit „gemeinsame Festlegung der Mittel“ (nur) ein „Verursachen der Datenverarbeitung eines Verantwortlichen durch einen anderen“ gemeint hätte, er das dann wohl auch so geschrieben hätte – in Art. 82 DSGVO kommt der Begriff der Verursachung im Zusammenhang mit der Haftung mehrmals vor, d. h. dem Gesetzgeber ist dieser Begriff als solcher wohlbekannt. Aus der Formulierung des „gemeinsamen Festlegens“ in der DSGVO wäre dann eigentlich zu folgern, dass es irgendeine Form von Absprache zwischen den (dann) gemeinsam Verantwortlichen gegeben haben muss, ansonsten hätte das Wort „gemeinsam“ keinen Sinn. Und eine Absprache zwischen dem Social-Media-Betreiber und dem Webseiten-Betreiber liegt alleine in der faktischen Verwendung eines „Codeschnipsels“ nicht, es sei denn, man geht von einer urheberrechtlichen Nutzungsrechtseinräumung (Lizenz) am „Codeschnipsel“ aus und damit von einer (stillschweigenden) Lizenzvereinbarung. Der EuGH hingegen konstruiert diese Absprache auf einer anderen Ebene, wie noch zu zeigen sein wird.

Zu resümieren bleibt hier indes nur, dass Mittel gemeinsam festgelegt werden, wenn beide Verantwortlichen „kausal“ für die Datenerhebung waren. Hierauf beschränkt wäre auch der Arbeitgeber kausal für die Datenerhebung durch die Finanzbehörden, wenn er die Daten eines neuen Arbeitnehmers weitergibt. Aber es ist ja daneben auch noch die Zwecküberschneidung notwendig.

Zwecküberschneidung

Was den Zweck anbelangt, so fällt auf, dass der EuGH den „Zweck" teilweise sehr spezifisch datenschutzrechtlich versteht, teilweise aber auch als „außerrechtlichen" Zweck formuliert. An einer Stelle heißt es, der hier maßgebliche Zweck sei das *„Erheben bestimmter personenbezogener Daten der Besucher ihrer Website und deren Weitergabe durch Übermittlung*". Es wäre dann irrelevant, zu welchem (weiteren) Zweck erhoben bzw. übermittelt wird. Später führt der EuGH dann aber aus:

> „Was die Zwecke dieser Vorgänge der Verarbeitung personenbezogener Daten betrifft, scheint es, dass die Einbindung des „Gefällt mir"-Buttons von Facebook durch Fashion ID in ihre Website ihr ermöglicht, die Werbung für ihre Produkte zu optimieren, indem diese im sozialen Netzwerk Facebook sichtbarer gemacht werden, wenn ein Besucher ihrer Website den Button anklickt."

Der Zweck ist hiernach nicht mehr nur die Erhebung durch den Webseiten-Betreiber, sondern der übergeordnete Zweck, zu dem der „Codeschnipsel" des Social-Media-Betreibers eingefügt wurde, also der Zweck des „Kausalbeitrags" zur späteren Erhebung durch den Social-Media-Betreiber. In anderen Worten geht es hier, wenn man den Kausalbeitrag tatsächlich als „Mittel" der Datenverarbeitung ansieht, um den „Zweck des Mittels", also warum der „Codeschnipsel" (als Mittel) aufgenommen wurde. Der EuGH fügt an:

> „Um in den Genuss dieses wirtschaftlichen Vorteils kommen zu können, der in einer solchen verbesserten Werbung für ihre Produkte besteht, scheint Fashion ID mit der Einbindung eines solchen Buttons in ihre Website zumindest stillschweigend in das Erheben personenbezogener Daten der Besucher ihrer Website und deren Weitergabe durch Übermittlung eingewilligt zu haben. Dabei werden diese Verarbeitungsvorgänge im wirtschaftlichen Interesse sowohl von Fashion ID als auch von Facebook Ireland durchgeführt, für die die Tatsache, über diese Daten für ihre eigenen wirtschaftlichen Zwecke verfügen zu können, die Gegenleistung für den Fashion ID gebotenen Vorteil darstellt."

Innerhalb der Diskussion um den Zweck ist demnach von einer „Einwilligung" des Webseiten-Betreibers in die Erhebung der Daten des Betroffenen durch den Social-Media-Anbieter die Rede, was zu der vorher getroffenen Aussage des EuGH passt, der Webseiten-Betreiber habe wohl um die Erhebung und Übermittlung personenbezogener Daten durch den „Codeschnipsel" gewusst (s. o.). Damit wird im Rahmen der Diskussion des gemeinsam festgelegten Zwecks offenbar eine Art Absprache unterstellt. Diese liegt aber nicht in der Einräumung von Lizenzrechten am „Codeschnipsel" selbst, sondern in einem darüber hinausgehenden Austauschgeschäft von Leistung und Gegenleistung, das der EuGH anhand der wirtschaftlichen Ziele definiert: Der Social-Media-Anbieter erhält Daten, der Webseiten-Betreiber erhält eine erweiterte Außenwirkung. Es ist zwar offen, ob die Verwendung des „Codeschnipsels“ zivilrechtlich ein (stillschweigendes) gegenseitiges Vertragsverhältnis zwischen dem Webseiten-Betreiber und dem Social-Media-Betreiber begründen würde, aber dem EuGH genügt offensichtlich ein „gegenseitiges Interesse“, also eine Art (außerrechtliches) Interessen-Austauschgeschäft.

In diesem Austauschgeschäft ist aber das Interesse des Webseiten-Betreibers auf sehr viel mehr gerichtet als nur auf die „gemeinsame Phase“, sprich die Erhebung und Übermittlung durch bzw. an den Social-Media-Betreiber, nämlich just auf *„verbesserte Werbung für die Produkte“* durch die sich anschließende Geschäftstätigkeit des Social-Media-Betreibers. Dieser – sowohl die dahinterstehende Vorstellung – „macht irgendetwas für den Webseiten-Betreiber Gutes mit den Daten“ und daran hat der Webseiten-Betreiber ein Interesse und dieses Interesse ist Teil eines Interessen-Austauschgeschäfts. Während sich demnach die gemeinsame Verantwortlichkeit nur auf eine Phase der „gemeinsamen Festlegung der Zwecke und Mittel“ bezieht, greift das zur Begründung der gemeinsamen Festlegung der Zwecke herangezogene Interesse weit über diese Phase hinaus. Man könnte sich also schon darüber Gedanken machen, warum die „gemeinsame Phase“ schon so früh enden soll, wie der EuGH das – aus der Perspektive des Webseiten-Betreibers „freundlicherweise“ – herbeidefiniert. Denn der Webseiten-Betreiber ist im Rahmen des Interessen-Austauschgeschäfts nicht nur an der Erhebung und Übermittlung der Daten interessiert, sondern gerade an der weiteren Verarbeitung („Ausschlachten“) der Daten durch Facebook, was immer das im Detail heißt, das dann (hoffentlich) irgendwie zu einer erhöhten Wahrnehmbarkeit des Webseiten-Betreibers führt. Welche Mechanismen auf Facebook-Seite dem Webseiten-Betreiber tatsächlich wie helfen, scheint für den EuGH indes keine Rolle zu spielen. Wenn aber hier der gemeinsame Zweck noch nicht endet, enden dann hier die gemeinsamen Mittel, sprich bricht der Kausalstrang, den der Webseiten-Betreiber mit gesetzt hat, ab? Man weiß es nicht.

Wie lautet die Formel?

Es lässt sich also resümieren: Wer als Webseite-Betreiber weiß, dass ein anderer Daten eines Betroffenen erheben und an sich übermitteln wird, und die Ursache für diese Erhebung durch den anderen selbst setzt (hier durch Einbindung des „Codeschnipsels“), wird insoweit (d. h. hierauf beschränkt) zum gemeinsam Verantwortlichen mit dem anderen, vorausgesetzt der Webseiten-Betreiber hat an der weiteren Verarbeitungstätigkeit des anderen Interesse und der andere hat Interesse an den Daten. Dies ist also die auf die konkrete Fallkonstellation des EuGH heruntergebrochene Ausformulierung der dürren DSGVO-Worte *„Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche“*.

Man kann dies als „vernünftige Konkretisierung“ der Gesetzesformulierung ansehen oder nicht – um eine rechtsdogmatisch-methodologisch „richtige“ Gesetzesauslegung geht es hier ohnehin nicht –, zwingend (und vorhersehbar) ist diese Interpretation aber nicht. Dies wird sich umso mehr zeigen, wenn man versucht, diese Formel auf andere Fallgestaltungen anzuwenden (s. u.). In der zusammenfassenden, stärker auf den Fall bezogenen Formel des EuGH selbst findet sich das Interessen-Austauschgeschäft schon nicht mehr; hiernach liegt eine gemeinsame Verantwortlichkeit (bereits) dann vor, wenn

> „der Betreiber einer Website wie Fashion ID, der in diese Website ein Social Plugin einbindet, das den Browser des Besuchers dieser Website veranlasst, Inhalte des Anbieters dieses Plugins anzufordern und hierzu personenbezogene Daten des Besuchers an diesen Anbieter zu übermitteln“.

An die vielen holzschnittartigen Formulierungen des EuGH, der nur selten „feingetunte“ Begriffsgerüste erarbeitet, schließt sich am Ende die bereits in der Fanpage-Entscheidung enthaltene Formulierung an, die man schon fast als „verräterisch“ bezeichnen müsste. In dem Fall nämlich, dass der Betroffene keinen Facebook-Account hat,

> „erscheint die Verantwortlichkeit des Betreibers einer Website, wie im vorliegenden Fall Fashion ID, hinsichtlich der Verarbeitung der personenbezogenen Daten dieser Personen noch höher, da das bloße Aufrufen einer solchen Website, die den „Gefällt mir“-Button von Facebook enthält, offenbar automatisch die Verarbeitung ihrer personenbezogenen Daten durch Facebook Ireland auslöst“.

Nun wird aus der Stellung als Verantwortlichem im datenschutzrechtlichen Sinne, die („digital") entweder gegeben sein kann oder auch nicht, eine Verantwortlichkeit im graduellen Sinne, die mehr oder weniger gegeben sein kann. Hätte das nicht der EuGH geschrieben, müsste man wohl ausrufen, dass der Betreffende das Datenschutzrecht nicht einmal ansatzweise verstanden hat. So wird man in diesem Satz eine noch tiefere Wahrheit suchen müssen als in den vorangehenden.

Liegt nun eine Stellung als „gemeinsam Verantwortliche" vor, stellt sich natürlich die Frage, was dies – abseits der mit Ausnahme der Notwendigkeit einer Vereinbarung wenig aussagekräftigen Regelungen in Art. 26 DSGVO – „wirklich" bedeutet. Zwei der insoweit einschlägigen Folgefragen hatte der EuGH zu beantworten.

Doppelt gemoppelt hält besser

Wenn eine Stellung als gemeinsam Verantwortliche vorliegt und eine konkrete Datenverarbeitungshandlung auf das berechtigte Interesse des Verantwortlichen gestützt werden soll, ist natürlich offen, ob das „jeweilige" berechtigte Interesse für die „jeweilige" Verarbeitung ausreicht oder ob die Verarbeitung nur zulässig ist, wenn sowohl der eine als auch der andere Verantwortliche ein berechtigtes Interesse hat. Diese Frage ist deshalb wichtig, weil zum Zeitpunkt der Datenerhebung – dem Aufruf der Webseite – meist weder eine Einwilligung abgefragt wird noch ein Vertrag zwischen dem Besucher und dem Webseiten-Betreiber zustande kommt (wenn man nicht von einem vertragsähnlichen Webseiten-Benutzungs-Verhältnis ausgeht), sodass in der Praxis häufig die Interessenabwägung die einzig gangbare datenschutzrechtliche Legitimationsgrundlage darstellt.

An dieser Stelle erinnert der EuGH zunächst daran, dass nach der ePrivacy-Richtlinie von 2002, die immer noch nicht in eine ePrivacy-Verordnung überführt wurde, das Setzen und Abfragen eines Cookies der Einwilligung des Betroffenen bedürfen. Die Cookie-Richtlinie der EU von 2009 erwähnt der EuGH in diesem Zusammenhang nicht. Technisch – aber diese Prüfung überlässt der EuGH dem Oberlandesgericht Düsseldorf – führt die Aufnahme des Like-Button-„Codeschnipsels" zu einer Übermittlung etwaiger Cookie-Daten, die auf dem Rechner des Besuchers gespeichert sind, an Facebook. Hat der Besucher keinen Facebook-Account und ist noch kein Cookie vorhanden, setzt der „Codeschnipsel" – so die Informationen im Internet über die Funktionsweise des „Codeschnipsels" – ein neues Cookie. Damit scheint eine „Vorschaltseite", auf der der Besucher eine Einwilligung erteilen muss, bevor Cookie-bezogene Daten an Facebook übermittelt oder Cookies gesetzt werden, unumgänglich zu sein. Die Frage allerdings, ob sich das deutsche Recht, das für Cookies „für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien" auch eine Widerspruchsmöglichkeit ausreichen lässt, mit der europarechtlichen Einwilligungsnotwendigkeit vereinbaren lässt, ist beim EuGH noch im sog. „Planet49"-Verfahren anhängig. Die Zeichen stehen diesbezüglich auf „nicht vereinbar", d. h. reine Widerspruchs-Cookie-Banner könnte es bald nicht mehr geben.

Doch nun zur eigentlichen Frage, da es ja nicht nur um Cookie-Inhalte geht: Der EuGH verlangt eine datenschutzrechtliche Legitimationsgrundlage für jeden der gemeinsam Verantwortlichen. Soll die Verarbeitung mit einem berechtigten Interesse gerechtfertigt werden, muss dies bei beiden Beteiligten gleichermaßen vorliegen. Dies dürfte für sämtliche Datenverarbeitungshandlungen innerhalb der „gemeinsamen Phase" gelten. Mit anderen Worten: Wenn zwei Verantwortliche gemeinsam Verantwortliche sind und eine Datenverarbeitungsaktivität in einer „gemeinsamen Phase" (s. o.) liegt, ist es

> „erforderlich, dass jeder dieser Verantwortlichen mit diesen Verarbeitungsvorgängen ein berechtigtes Interesse im Sinne von Art. 7 Buchst. f der Richtlinie 95/46 wahrnimmt, damit diese Vorgänge für jeden Einzelnen von ihnen gerechtfertigt sind."

Dies bedeutet zunächst einmal, dass dieselbe Datenverarbeitungsaktivität beiden Verantwortlichen datenschutzrechtlich voll „zugerechnet" wird. Die Aktivität des einen gilt als Aktivität des anderen und umgekehrt. Das ist insoweit bemerkenswert, als hier letztlich über die – angebliche – gemeinsame Mittel- und Zweckfestlegung der einen Stelle Aktivitäten zugerechnet werden, an welcher technisch ausschließlich die andere Stelle beteiligt ist. Der Webseiten-Betreiber bindet zwar den „Codeschnipsel" ein, steuert aber die damit erhobenen und übermittelten Daten nicht und hat diese auch zu keinem Zeitpunkt unter einer faktischen (Mit-)Kontrolle. Er muss sich damit

- eine Datenverarbeitungsaktivität zurechnen lassen, die er „eigentlich" nicht im Einzelnen kennt, und
- sicherstellen, dass er selbst ein berechtigtes Interesse an dieser Datenverarbeitungsaktivität hat, die er nicht im Einzelnen kennt, und
- sicherstellen, dass der andere gemeinsam Verantwortliche ein berechtigtes Interesse an einer Datenverarbeitungstätigkeit hat, die er nicht im Einzelnen kennt.

Diese Aufgabe dürfte nur dann lösbar sein, wenn die Datenverarbeitungsaktivität, die dem Webseiten-Betreiber zugerechnet wird, für ihn völlig transparent ist. Damit wären wir wieder beim Thema „Beschreibung" oder „Analyse" der Funktionsweise des „Codeschnipsels". Ersteres bedingt Vertrauen in die Beschreibung des Social-Media-Anbieters, letzteres löst nicht unerhebliche Analysekosten aus.

Es ist offen, ob der EuGH wusste, was er damit sagte, als er die „doppelte Interessenabwägung" forderte.

...und die Einwilligung holt er auch noch ein

Das Oberlandesgericht Düsseldorf blieb aber nicht bei der Frage der Interessenabwägung stehen. Gesetzt den Fall, dass eine Interessenabwägung nicht möglich ist (Cookies) oder für die gemeinsam Verantwortlichen negativ ausgeht (sonstige Daten), bedarf es einer Einwilligung des Betroffenen. Wer von den beiden gemeinsam Verantwortlichen muss diese nun einholen? Man wäre versucht zu sagen beide, wenn schon eine doppelte Interessenabwägung gefordert wird. Aber so weit geht der EuGH doch nicht. Er fordert, dass der Webseiten-Betreiber die Einwilligung einholt, und zwar schlicht deswegen, weil er den „ersten Kontakt“ mit dem Betroffenen hat. Die Einwilligung muss nämlich

> „vor dem Erheben der Daten der betroffenen Person und deren Weitergabe durch Übermittlung erklärt werden. Daher obliegt es dem Betreiber der Website und nicht dem Anbieter des Social Plugins, diese Einwilligung einzuholen, da der Verarbeitungsprozess der personenbezogenen Daten dadurch ausgelöst wird, dass ein Besucher diese Website aufruft. Wie der Generalanwalt in Nr. 132 seiner Schlussanträge ausgeführt hat, entspräche es nämlich nicht einer wirksamen und rechtzeitigen Wahrung der Rechte der betroffenen Person, wenn die Einwilligung lediglich gegenüber dem gemeinsam für die Verarbeitung Verantwortlichen erklärt würde, der erst zu einem späteren Zeitpunkt beteiligt ist, also gegenüber dem Anbieter dieses Plugins.“

Diese Lösung ist insbesondere deshalb interessant, weil sie auch hätte völlig anders ausfallen können. Schließlich ist es „physisch“ der Social-Media-Anbieter, dessen „Codeschnipsel“ die Daten erhebt und übermittelt. Daher hätte auch der Social-Media-Anbieter die Möglichkeit, den „Codeschnipsel“ so zu designen (Privacy by Design), dass dieser eine Einwilligung einholt (d. h. die Seite „grau schaltet“ und eine Abfragebox mit Hinweistext einblendet), bevor er fortfährt und Daten erhebt und übermittelt. Stattdessen wird die Pflicht einem der gemeinsam Verantwortlichen – und zwar dem, der die Erhebung und Übermittlung gar nicht physisch durchführt – aufgebürdet. Würde es um die DSGVO und nicht um die Datenschutzrichtlinie 1995 gehen, wäre man versucht zu sagen, dass da irgendetwas bei dem Versuch, es den „großen Datenkraken“ mit einer „bissigen“ Verordnung zu zeigen, nicht geklappt hat.

...und die Pflichtinformation übernimmt er auch noch

Aus der Sicht des EuGH ist es da nur folgerichtig, dass auch die Pflichtinformationen dem Betroffenen vom Webseiten-Betreiber zur Verfügung gestellt werden müssen. Wiederum geht der EuGH davon aus, dass der „arme" Social-Media-Betreiber zum Zeitpunkt der Datenerhebung keine Pflichtinformationen anzeigen kann:

> „Es scheint somit, dass der für die Verarbeitung Verantwortliche diese Information sofort zu geben hat, d. h. zum Zeitpunkt des Erhebens der Daten."

Der Betreiber muss also, um richtig informieren zu können, entweder vom Social-Media-Anbieter mit den relevanten Informationen „beliefert" werden oder sich diese Informationen anderweitig beschaffen. Dies gilt auch für zwischenzeitliche Veränderungen, die dem Betreiber vielleicht nicht immer zeitnah transparent sind. Die Folgen unzureichender Pflichtinformationen liegen auf der Hand.

USA?

Die Vorlagefragen an den EuGH waren nicht spezifisch auf Facebook, sondern auf *„den Anbieter des Social Plugins"* gemünzt. Der EuGH unterstellte, dass dies die Facebook Ireland Ltd. war. Es ist jedoch allgemein bekannt, dass Facebook keine spezifisch europäische Serverstruktur unterhält, also gleichsam ein „europäisches Facebook" anbietet. Die Daten werden an Facebook-Server in den USA übermittelt und könnten bei behördlichen Untersuchungsanordnungen an staatliche Stellen ausgeliefert werden. Zwar ist Facebook dem „EU-US Privacy Shield" beigetreten, das (noch) eine Übermittlung in die USA legitimiert. Aber ob dies seine Legitimationskraft auch in Zukunft behalten wird, ist Gegenstand des vor dem EuGH anhängigen Schrems-Verfahrens. Entsprechend muss sich – im Anschluss an die vorherigen „Guidelines" des EuGH – für den Webseiten-Betreiber die Frage anschließen, ob eine Datenübermittlung in ein Drittland vorliegt. Ist dies der Fall, muss der Webseiten-Betreiber einerseits den Besucher nach Art.13 Abs.1 lit. f) DSGVO darüber informieren sowie andererseits die Einhaltung der Art. 44 ff. DSGVO prüfen. Auch insoweit muss sich der Webseiten-Betreiber die Informationen vom Social-Media-Anbieter beschaffen.

Was ist zu tun?

Die konkrete Entscheidung des EuGH dürfte, wenn das Oberlandesgericht Düsseldorf diese entsprechend umsetzt, dazu führen, dass nach den Fanpage-Betreibern nun auch die Like-Button-Einbindenden mit Facebook eine Vereinbarung über die Stellung als „gemeinsam Verantwortliche" abschließen müssen. Daneben müssen sie Überlegungen über die datenschutzrechtliche Legitimationsgrundlage der Facebook-Daten, ggf. die Einholung einer Einwilligung, das Setzen und Auslesen von Cookies sowie die Mitteilung von Pflichtinformationen anstellen. Ob jeder Webseiten-Betreiber nun weiß, was das bedeutet bzw. was er nun machen muss, ist zweifelhaft, zumal es nach der Fanpage-Entscheidung des EuGH längere Zeit gedauert hat, bis Facebook eine entsprechende formularmäßige Vereinbarung veröffentlichte, die nach Ansicht der Datenschutzbehörden nicht ausreichend ist. Als Alternative bleibt natürlich immer, den „Codeschnipsel" aus dem HTML-Code des Webseiten-Anbieters zu entfernen.

In diesem Zusammenhang ist auf die von Heise Online entwickelte „Shariff"-Lösung einzugehen. Diese verhindert, dass der „Codeschnipsel" bereits beim Aufruf der Seite ausgeführt wird. Dessen Ausführung beginnt vielmehr erst dann, wenn der Besucher den „Codeschnipsel" manuell durch Klick auf ein Symbol aktiviert. Dies hat zur Folge, dass auch der Like-Button erst mit einem „zweiten Klick" erreichbar wird. Dieses Vorgehen führt dazu, dass für den Webseiten-Betreiber die Möglichkeit besteht, seine Seite ohne entsprechende Datenschutzverstöße anzeigen zu lassen. Wird aber der „Codeschnipsel" freigeschaltet, muss gleichwohl eine datenschutzrechtlich zulässige Pflichtinformation erfolgen, ein „joint controller agreement" vorliegen und ggf. eine wohlinformierte Einwilligung eingeholt werden, denn die Stellung als „gemeinsam Verantwortliche" und die Erhebung und Übermittlung von Daten nach Freischaltung des „Codeschnipsels" verändern sich dadurch nicht. In einer Vielzahl von Anwendungsfällen – nämlich wenn der Seitenbesucher nicht auf das Symbol klickt – besteht dann mangels Erhebung und Übermittlung der hier diskutierten Daten kein datenschutzrechtliches Risiko. Aber wenn der Seitenbesucher auf das Symbol klickt, stellen sich prinzipiell dieselben Probleme wie vom EuGH aufgezeigt – nur zeitlich verschoben auf den Zeitpunkt des Klicks.

Nachfolgend soll nun auf zwei weitere Fallgestaltungen eingegangen werden, die von der EuGH-Entscheidung ebenfalls betroffen sein könnten, mal weniger, mal mehr offensichtlich.

PSP MÜNCHEN

Folgewirkungen 1 – Hyperlinks?

Eine bislang kaum gestellte Frage ist, inwieweit die vom EuGH mittlerweile entwickelten juristischen Formeln für die Stellung als gemeinsam Verantwortliche nicht auch auf eine der ältesten Internet-Technologien, den Hyperlink, Anwendung finden können bzw. müssen. Schon vor vielen Jahren wurde das Thema Prüfpflichten beim Verwenden von Links auf Drittseiten aus verschiedenen Perspektiven (Urheberrechtsverletzung, Haftung für Schadcode etc.) diskutiert, wobei die Diskussion seit einiger Zeit durch viele neue Themen überlagert wurde. Besteht also (auch) eine datenschutzrechtliche Prüfpflicht hinsichtlich der Daten, die von der verlinkten Seite erhoben werden? Eindeutig ist das nicht:

- Auch beim Link wird das Erheben und Übermitteln der Daten durch das Setzen des Links „verursacht“. Ohne Link keine Weiterleitung zur Zielseite inklusive Erheben und Übermitteln. Damit könnte – nach der Argumentation des EuGH – die Festlegung gemeinsamer Mittel vorliegen.
- Der gemeinsame Zweck bzw. das „Interessen-Austauschgeschäft“ liegt darin, dass der Link-Setzer seine Webseite durch Verweis auf weiterführende Informationen attraktiver machen möchte, während der Betreiber der Zielseite grundsätzlich an mehr „Traffic“ interessiert sein dürfte. Folglich liegt eine ähnliche Zwecküberschneidung wie im Like-Button-Fall vor.
- Der (kleine) Unterschied scheint hier zwar zunächst darin zu liegen, dass der Betreiber der Zielseite normalerweise gar nicht weiß, wer (alles) auf seine Seite verlinkt. Allerdings weiß Facebook dies im Fall des EuGH zunächst auch nicht – der Codeschnipsel kann jederzeit in „irgendeine“ HTML-Seite eingebaut werden. Und so wie Facebook von der Existenz seines Codeschnipsels auf einer fremden Seite spätestens beim ersten Aufruf erfährt, so erfährt auch der Betreiber der Zielseite eines Links über den „Referer“-Parameter beim ersten Aufruf des Links, von welcher „Quellseite“ ein Aufruf stammt. Der Unterschied besteht also lediglich darin, dass der Verlinker hier nicht auf irgendwelche „Codeschnipsel“ des Betreibers der Zielseite zurückgreifen muss, sondern das Setzen eines Links auf eine andere Webseite ist eine Standard-Technologie.
- Der Betreiber der verlinkenden Seite weiß, dass er durch das Setzen des Links dafür sorgt, dass zumindest die IP-Adresse des Benutzers (meist aber auch HTTP-User-Agent-String mit Angaben über das System des Benutzers) – also ein personenbezogenes Datum – vom Betreiber der verlinkten Seite erhoben wird. Zumindest diese Erhebung durch den Betreiber der verlinkten Seite wird durch den Klick auf den vom Betreiber der verlinkenden Seite gesetzten Hyperlink ausgelöst. Man kann also auch hier sagen, dass die Erhebung und Übermittlung im Rahmen einer Phase der Stellung als gemeinsam Verantwortliche geschieht.

- Die Erhebung erfolgt zu einem Zeitpunkt, zu dem der Betreiber der verlinkten Seite noch gar keine Pflichtinformationen über diese Datenerhebung anzeigen kann. Aber selbst wenn der Betreiber der verlinkten Seite die entsprechenden Pflichtinformationen später bereitstellen würde, käme dies wohl zu spät – so der EuGH im Like-Button-Fall. Damit würden Informationspflichten des Betreibers der verlinkenden Seite ausgelöst, was die gemeinsame Phase anbelangt. Der Betreiber der verlinkenden Seite kann sich nicht dadurch „exkulpieren", dass er ja am entsprechenden technischen Datenaustausch nicht beteiligt ist – das ist der Betreiber der Webseite im Like-Button-Fall auch nicht (s. o.).
- Daneben müsste sich der Betreiber der verlinkenden Seite darüber Gedanken machen, welche datenschutzrechtliche Legitimationsgrundlage die Erhebung und Übermittlung (auch) durch den Betreiber der verlinkten Seite rechtfertigt. Ist eine Einwilligung notwendig, müsste der Betreiber der verlinkenden Seite diese einholen. Ob der Klick auf den Link bereits eine Einwilligung des Betroffenen sein kann, ist zweifelhaft, denn die Informationen, die der Betroffene wissen muss, um eine informierte Einwilligungserklärung abgeben zu können, kennt der Betroffene zu diesem Zeitpunkt nicht. Dazu zählen neben den in der DSGVO und den Erwägungsgründen genannten Informationen z. B. nach Meinung von Datenschutzaufsichtsbehörden auch die Kenntnis der Speicherdauer.

Würde man Hyperlinks – entsprechend der Like-Button-Entscheidung – als Fälle gemeinsamer Verantwortlichkeit einstufen, so würde sich jeder Webseiten-Betreiber vor lauter Vereinbarungen über die gemeinsame Verantwortlichkeit kaum mehr retten können. Es liegt deshalb nahe, dass sich der EuGH, würde er dazu befragt, ein Differenzierungskriterium ausdenken würde, der den gewöhnlichen Link vom Like-Button-Fall unterscheidet. Man darf gespannt sein, was dieses Kriterium sein wird. So könnte der EuGH z. B. argumentieren, dass im Unterschied zum „Codeschnipsel" eines Social-Media-Anbieters, der bzw. dessen Server-Kontaktaufnahme nicht auch manuell eingegeben werden kann, der Aufruf einer Zielseite einfach über die Eingabe der Link-Adresse in der Adresszeile des Browsers geschehen kann. Dies gilt aber grundsätzlich nur für „einfache" Links (d. h. für Second-Level-Domains oder eine Ebene darunter), während es umgekehrt auch „sehr lange" Deep-Links gibt, die man manuell nicht „finden" bzw. eingeben würde. Und wenn man sie nur über eine Suchmaschine finden könnte, wäre es wieder eine Verlinkung in den angezeigten Suchergebnissen.

Folgewirkungen 2 – Telemetriedaten?

Ein Arbeitgeber, der seinen Angestellten vorgibt, Microsoft-Produkte zu benutzen, „lockt diese an“ – so könnte man sagen –, damit Microsoft ihre personenbezogenen Daten über die Benutzungshandlungen als Telemetriedaten erhebt und in die USA übermittelt. So könnte das Like-Button-Konstrukt des EuGH auf jede Form von Diagnosedaten von Betroffenen übertragen werden, wenn Betroffener, Softwarehersteller und Software-Betreiber auseinanderfallen. In den seltensten Fällen findet eine ausführliche Dokumentation der dabei erhobenen und übermittelten Daten statt, und selbst bei einer entsprechenden Dokumentation könnte sich der Arbeitgeber – etwa im Rahmen einer Datenschutzfolgenabschätzung – nie sicher sein, ob die Dokumentation richtig ist. Beispiele für Telemetriedaten sind etwa – mit der jeweiligen Rechner- bzw. User-ID sowie mit einem Zeitstempel versehene – Angaben über das Starten des Systems und von Diensten bzw. Anwendungen, über Programmabstürze, vorgenommene Updates oder Auslastungsdaten.

Dementsprechend hat das niederländische Justizministerium in verschiedenen (Rahmen-)Datenschutzfolgenabschätzungen die Risiken von Microsoft Windows 10 und Office 365 bewerten lassen. In den Niederlanden verwenden ca. 300.000 Staatsbedienstete laufend Microsoft-Produkte. Der konkrete Einsatz dieser Software ist zwar jeweils von den einzelnen Behörden zu bewerten, aber die Rahmen-Datenschutzfolgenabschätzungen kommen zu dem Schluss, dass derzeit – selbst unter Anwendung möglichst restriktiver Vorgaben innerhalb der Software – ein „niedriges“ Risiko bestehe. Denn es werden zwar verschiedene personenbezogene Daten über die Aktivität des Nutzers erhoben und übermittelt, aber diese sind „nicht sehr sensibel“. Ein Abfluss von Inhaltsdaten (von Dokumenten etc.) konnte nicht festgestellt werden. Gleichwohl wird kritisiert, dass keine ausreichende Zweckeingrenzung, keine taugliche Legitimationsgrundlage sowie keine ausreichende Prüfmöglichkeit hinsichtlich der weiteren Verwendung der Daten bestehe. Dabei wird auch darauf hingewiesen, dass Microsoft im laufenden Betrieb selbst entscheiden kann, welche weiteren Telemetriedaten erhoben und übermittelt werden, ohne dass dies für den Nutzer transparent ist.

Die vom Justizministerium beauftragten Berater folgern, dass eine Stellung als gemeinsam Verantwortliche vorliegt, sodass eine Vereinbarung hierüber mit Microsoft abzuschließen wäre:

> “Because Microsoft determines the purposes, and the government organisations enable Microsoft to process personal data, they are factually joint controllers for the diagnostic data processing.“

Demgegenüber qualifiziert sich Microsoft selbst als (eigenständig) Verantwortlicher und führt in seinen Datenschutzbestimmungen 16 relevante Zwecke für die Verarbeitung der Daten auf, einschließlich

> „the use of personal data for personalised advertising in Windows 10 and in apps, to present commercial offers, and to use the contact data for promotional communications via email, SMS, physical mail and telephone".

Welche Daten Microsoft hier tatsächlich "abgreift", wurde seit 2017 zunehmend dokumentiert und der „Diagnostic Data Viewer" kann diese Daten auch innerhalb von Windows anzeigen. Ob weitere, undokumentierte Datentypen erhoben und übermittelt werden, wird vermutlich nie restlos aufgeklärt werden können, da Teile der Daten verschlüsselt und in kleinere Datenmengen aufgeteilt werden könnten.

In der bisherigen Kommunikation zwischen dem Justizministerium und Microsoft ging es nicht darum, derartige Datenerhebungen abschaltbar auszugestalten (bzw. an die Einholung einer Einwilligung zu koppeln), sondern darum, den Transfer auf ein Niveau zu reduzieren, dass vom Justizministerium als akzeptabel angesehen werden kann. Informationen von Microsoft gegenüber dem Justizministerium zu den Untersuchungsergebnissen wurden als „vertraulich" eingestuft und daher nicht veröffentlicht.

Es steht zu vermuten, dass viele Softwareprodukte Diagnosedaten versenden. Nur bei einem Teil davon wird dieser Umstand transparent sein. Und nur bei einem Teil dieses Teils wird die Versendung von Diagnosedaten im Vorhinein abschaltbar sein.

Folgewirkungen 3 – Whatsapp?

Mittlerweile ist allgemein bekannt, dass die App „Whatsapp“, einmal in Betrieb genommen, das Kontakteverzeichnis eines Mobiltelefons ausliest – sofern diese Berechtigung nicht ausgeschlossen wird –, gleich, ob der jeweilige Kontakt ebenfalls über ein Vertragsverhältnis mit Whatsapp verfügt oder nicht. Facebook (als Betreiber von Whatsapp) erhebt und übermittelt daher über diese App personenbezogene Daten Dritter, ohne dass diese davon Kenntnis erlangen, Pflichtinformationen erhalten oder eine Rechtsgrundlage besteht. Wer als Inhaber des Mobiltelefons den Zugriff (aktiv) sperrt, kann selbst keine neuen Konversationen in Whatsapp beginnen, sondern nur angeschrieben werden (und hierauf antworten), d. h. er kann die Funktionalität von Whatsapp nur in einer (sehr) beschränkten Form nutzen.

Wie im Like-Button-Fall ist hier der Inhaber des Mobiltelefons, der Whatsapp – letztlich einen etwas größerer „Codeschnipsel“ – installiert, Verantwortlicher im datenschutzrechtlichen Sinne für die Kontaktdaten und zugleich (aus der Perspektive von Whatsapp) „Lockvogel“ für diese personenbezogenen Daten Dritter. Allerdings übermitteln die Betroffenen diese Kontaktdaten im Regelfall nicht selbst an den Inhaber des Mobiltelefons, sondern der Inhaber des Mobiltelefons erhebt diese Daten selbst – üblicherweise mit Einverständnis des Dritten, wobei die datenschutzrechtliche Qualität dieses Einverständnisses hier nicht vertieft werden soll – von den Dritten. Es gibt natürlich auch Fälle, in denen jemand „an eine Telefonnummer gelangt“, ohne dass der Dritte hiervon weiß, aber die Konsequenzen hiervon sind im vorliegenden Kontext nicht relevant.

Man könnte nun sagen, dass die „gutgläubige“ – datenschutzrechtlich: auf den Zweck der unmittelbaren Kontaktaufnahme beschränkte – Mitteilung der Kontaktdaten durch den Betroffenen an den „Lockvogel“ (den Inhaber des Mobiltelefons) es Whatsapp ermöglicht, die Daten des Kontaktverzeichnisses „abzugreifen“. Eine Kausalität bzw. Ermöglichung – und damit nach Auffassung des EuGH eine Überschneidung der Mittel der Verarbeitung – liegt also durchaus vor. Daran anknüpfend stellt sich aber die Frage, ob ein ausreichendes „Interessen-Austauschgeschäft“ vorliegt. In diesem Zusammenhang ist darauf hinzuweisen, dass die vollständige kostenlose Nutzung von Whatsapp nur dadurch ermöglicht wird, dass Whatsapp der Kontaktabzug ermöglicht wird. Die vollständige kostenlose Nutzungsmöglichkeit sämtlicher Whatsapp-Funktionen könnte einen „geldwerten“ und damit wirtschaftlichen Vorteil darstellen, auch wenn es eine kostenpflichtige, datenabzugsfreie Variante der App nicht gibt (und damit auch keinen Maßstab für die Bemessung dieses Vorteils). Voll funktionsfähige Messenger-Alternativen oder SMS sind gewöhnlich kostenpflichtig. Im Gegenzug hat Whatsapp jedenfalls das wirtschaftliche Interesse, so viele Kontakte wie möglich zu erlangen, zumindest, um als Plattform attraktiver zu werden. Das Geschäftsmodell von Whatsapp war lange unklar, doch nun soll ab 2020 zielgerichtet Werbung eingeblendet werden. Es ist davon auszugehen, dass die Analyse (auch) der

Kontaktbeziehungen – ähnlich wie bei Facebook selbst – die Werbeeinblendungen beeinflusst und „zielgerichteter“ macht.

Man könnte aber auch sagen, dass das Interesse des Inhabers des Mobiltelefons an einer unbeschränkten Nutzung der App nicht „geldwert“ bzw. wirtschaftlicher Natur, sondern nur ideeller Natur ist und damit kein Austauschverhältnis zweier wirtschaftlicher Interessen vorliegt. Ob auch ideelle Interessen im Rahmen eines Austausches gleichwertig zu einer Zwecküberschneidung führen, hatte der EuGH in der Like-Button-Entscheidung nicht zu bewerten. Es wäre dann auch die Frage der Trennlinie zwischen beiden Interessensarten zu stellen. Immerhin ist auch in der Like-Button-Entscheidung der wirtschaftliche Vorteil von Fashion ID, nämlich die „bessere Sichtbarkeit auf sozialen Netzwerken“, nicht wirklich messbar. Allenfalls könnten hier die Kosten einer herkömmlichen Marketing-Kampagne mit ähnlichem Erfolg als Vergleichsmaßstab dienen.

Eine Stellung als gemeinsam Verantwortliche von einerseits Facebook (als Whatsapp-Betreiber) und andererseits dem Mobiltelefon-Inhaber, der Kontakte Dritter speichert, kann damit aus der „Formel“ der EuGH-Entscheidung nicht zwangsläufig gefolgert werden. Würde man Facebook und den Mobiltelefon-Inhaber als gemeinsam Verantwortliche einzustufen haben, müsste bei jeder Whatsapp-Installation ein „Joint Controllership Agreement“ zwischen diesen beiden abgeschlossen werden. Die Verantwortlichkeit des Inhabers des Mobiltelefons, eine (datenschutzrechtlich einwandfreie) Einwilligung der Betroffenen für die Erhebung und Übermittlung ihrer Kontaktdaten durch bzw. an Whatsapp einzuholen und die entsprechenden Pflichtinformationen zu erteilen, wurde allerdings unabhängig von der datenschutzrechtlichen „Gesamtschuld“ schon bisher attestiert.

Folgewirkungen 4 – Veranstaltungen?

Kann die Rechtsprechung des EuGH zum Thema gemeinsam Verantwortliche auch auf Fallkonstellationen außerhalb von Webseiten und „Apps mit Datensammeltendenz“ angewandt werden? Abstrakt gesagt: Sind zwei Verantwortliche, nämlich einer, der ein öffentliches Forum veranstaltet und damit natürliche Personen „anlockt“, und ein weiterer, der anlässlich dieser Veranstaltung – und mit Wissen des ersteren – personenbezogene Daten erhebt, gemeinsam verantwortlich? Immerhin ist die Veranstaltung des Forums kausal für die spätere Erhebung („ohne dieses Forum nicht diese Erhebung“) und soweit sich der Veranstalter durch die Datenerhebung des anderen irgendeinen Vorteil verspricht, könnte auch bereits ein Interessen-Austauschgeschäft vorliegen. Es stellt sich dann nur die Frage, ob ein Austausch „wirtschaftlicher“ Interessen notwendig ist, wie es der EuGH in der Like-Button-Entscheidung vorfindet (s. o.), oder auch ein „ideelles“ Interesse ausreicht. Bei öffentlichen Veranstaltungen greift insbesondere die sog. „Haushaltsausnahme“ der Verarbeitung von personenbezogenen Daten für den ausschließlich privaten oder familiären Bereich nicht ein, sodass der Fotograf hier auch als Einzelperson „Verantwortlicher“ im Sinne der DSGVO mit allen Konsequenzen wäre. Dabei geht es (noch) nicht um die umstrittene Frage der datenschutzrechtlichen Legitimationsgrundlage für Fotografien und das Verhältnis zum „altehrwürdigen“ Kunsturhebergesetz, sondern nur um die Stellung als gemeinsam Verantwortliche.

Dieses Muster könnte etwa auf Festivals oder Tourismus-Veranstaltungen angewandt werden, wenn die Besucher sogar dazu aufgefordert werden, „Fotos zu machen und ins Netz zu stellen“ oder Videos anzufertigen und live im Internet zu streamen, sofern einzelne Personen auf den Aufnahmen individualisiert erkennbar sind und damit personenbezogene Daten erhoben werden. Derartige Aufnahmen dienen der (möglicherweise wirtschaftlichen, möglicherweise nur ideellen, s. dazu o.) Aufmerksamkeit („likes“), die dem Fotografen im Internet aufgrund seiner Fotografien entgegengebracht wird, und den wirtschaftlichen Interessen des Veranstalters, das Festival (bzw. die Veranstaltung) zu bewerben. Im insoweit entscheidenden Satz des Like-Button-Urteils (s. o.) müsste nur Fashion ID (der „Lockvogel“) durch den Festival-Veranstalter und Facebook (der die Daten dann erhebende und in seiner Sphäre weiter verarbeitende Verantwortliche) durch den Fotograf ersetzt werden, zumindest sofern dieser „wirtschaftliche Zwecke“ verfolgt:

> Dabei werden diese Verarbeitungsvorgänge im wirtschaftlichen Interesse sowohl des Festival-Veranstalters als auch des Fotografen durchgeführt, für den die Tatsache, über diese Daten für seine eigenen wirtschaftlichen Zwecke verfügen zu können, die Gegenleistung für den dem Festival-Veranstalter gebotenen Vorteil darstellt.

Nach dem „Phasenscheibenmodell“ des EuGH würde diese Stellung als gemeinsam Verantwortliche natürlich nur für das Anfertigen der Fotografien gelten, sprich für die Datenerhebung, während die weitere Verarbeitung – das „ins-Netz-Stellen“ – nicht mehr Teil dieser Phase wäre. Ein „Joint Controllership Agreement“ wäre dann zwischen jedem solchen Fotografen (zumindest mit wirtschaftlichen Interessen an den angefertigten Fotografien) und dem Veranstalter abzuschließen.

Oder noch weitergehend: Hat der Betreiber einer (Privat-)Schule – immerhin auch die Veranstaltung eines öffentlichen „Forums“ – ein (wirtschaftliches) Interesse daran, bei einer Schulveranstaltung angefertigte Bilder der Schüler „im Netz“ veröffentlicht zu sehen, weil das die Attraktivität der Schule erhöht, während der Fotograf mehr „likes“ erhält?

Bevor wir aber nun anfangen, darüber nachsinnieren, ob nach der abstrakten „Formel“ des EuGH nicht auch jede Auftragsverarbeitungssituation in Wirklichkeit eine Stellung der Beteiligten als gemeinsam Verantwortliche begründet, verlassen wir lieber die – mit vielen Untiefen versehene – Spielwiese der möglichen Folgewirkungen des Like-Button-Urteils für andere Fallgestaltungen.

Zeitreise

Eine Anschlussfrage im Verhältnis von Fanpage- zur Like-Button-Entscheidung ist übrigens, ob der EuGH nicht unter Anwendung der Maßstäbe der Like-Button-Entscheidung die (vorherige) Fanpage-Entscheidung hätte anders fällen müssen. Dies betrifft nicht nur die Frage, wie sich die „Zeitphasen-Theorie“ des EuGH auf die Fanpages auswirken würde – also ob die Stellung als gemeinsam Verantwortliche über die gesamte Dauer der Datenverarbeitungstätigkeit hinweg besteht, (nur) weil der Fanpage-Betreiber „am Ende“ auf die anonymisierten Nutzungsstatistiken („Insights“) zugreifen kann. Nein, auch ganz grundsätzlich ist mit einzubeziehen, dass die in der Fanpage-Entscheidung thematisierten Cookies während des Besuchs von Facebook selbst gesetzt und ausgelesen werden – der Besucher besucht ja „nur“ eine Facebook-Seite, deren HTML-Quellcode ausschließlich von Facebook stammt (und die nur die teilweise vom Fanpage-Betreiber gestalteten Inhalte enthält). Die „Sogwirkung“ auf die Fanpage-Seite, die natürlich nicht von Facebook als solchem, sondern vom Fanpage-Betreiber ausgeht, ist vielleicht mit der Übernahme eines „Codeschnipsels“ nicht vergleichbar. Der EuGH hatte dazu ausgeführt:

> „Auch wenn der bloße Umstand der Nutzung eines sozialen Netzwerks wie Facebook für sich genommen einen Facebook-Nutzer nicht für die von diesem Netzwerk vorgenommene Verarbeitung personenbezogener Daten mitverantwortlich macht, ist indes darauf hinzuweisen, dass der Betreiber einer auf Facebook unterhaltenen Fanpage mit der Einrichtung einer solchen Seite Facebook die Möglichkeit gibt, auf dem Computer oder jedem anderen Gerät der Person, die seine Fanpage besucht hat, Cookies zu platzieren, unabhängig davon, ob diese Person über ein Facebook-Konto verfügt."

Diese Möglichkeit der Cookie-Platzierung (durch den „Codeschnipsel") hatte der Webseiten-Betreiber in der Like-Button-Entscheidung aber sogar durch eine besondere, zielgerichtete Aktion, die Übernahme des „Codeschnipsels", entscheidend ermöglicht (ohne „Codeschnipsel" keine Cookies). Entweder ist also der „Mitwirkungs"-Maßstab der Fanpage-Entscheidung strikter, indem nur das Befüllen einer Facebook-Fanpage mit Inhalten und die daraus resultierende „Sogwirkung in Richtung Facebook" inklusive des Zugriffs auf anonyme Nutzerstatistiken ausreicht. Die „Parametrisierung" dieses Zugriffs ist dem Fanpage-Betreiber nur in sehr engen Grenzen möglich; er entscheidet hier in keiner Weise über die Datenverarbeitung bei Facebook, sondern lediglich „ein bisschen" über die Präsentation der anonymisierten Ergebnisse der ihm unbekannten Verarbeitungshandlungen bei Facebook ihm gegenüber. Wäre die Fanpage-Entscheidung also strikter, so hätte in der Like-Button-Entscheidung keine eigene Argumentation entwickelt werden müssen; es hätte die kurze Aussage genügt, dass wenn schon das lediglich Befüllen einer Facebook-Seite mit Inhalten für die „Sogwirkung" ausreicht, dies erst Recht gelten muss, wenn sogar ein „Codeschnipsel" von Facebook in den eigenen Auftritt integriert wird, um zielgerichtet eine „Sogwirkung in Richtung Facebook" zu erzeugen – auf den Zugriff auf die dabei entstehenden Daten kommt es ohnehin nicht an. Oder aber die Like-Button-Entscheidung fällt hinter die Fanpages-Entscheidung zurück, indem sie höhere Anforderungen an die „Sogwirkung" formuliert. Dann würde sich der EuGH heute im Fanpage-Fall möglicherweise anders entscheiden (auch wenn er dies noch gar nicht bemerkt hat und auch nicht bemerken wird), auch wenn er sich in der Like-Button-Entscheidung auf die Fanpages-Entscheidung bezogen hat.

Oder sind die Fallkonstellationen deshalb gar nicht vergleichbar, weil sich der Fanpage-Betreiber die Infrastruktur Facebooks in einer ganz anderen Weise zunutze macht als der Webseiten-Betreiber, der nicht Facebook „insgesamt", sondern „nur" einen „Codeschnipsel" nutzt? Bei dieser Sichtweise wäre die Intensität von Mittel- und Zwecküberschneidung anders zu bewerten, was zeigt, wie relativ – und letztlich beliebig? – die Argumente sind.

Wie auch immer: Die Abgrenzungen und Folgen sind unklar, eine klare begriffliche Linie wird letztlich auf dem Weg zur Konkretisierung der „politisch-prinzipienbasierten Gesetzesformulierungen“ nicht herausgearbeitet. Es bleibt zudem immer unklar, inwieweit der EuGH die zugrundeliegenden technischen Vorgänge versteht. Juristen neigen bekanntlich dazu, ihre juristische Fachkenntnis in den Vordergrund zu stellen und die notwendige Sachkenntnis als vernachlässigbar zu bezeichnen. Aber möglicherweise ist das in einer immer komplexeren digitalisierten Welt nicht mehr zielführend. Vielleicht brauchen wir einen „Digital-EuGH“ – und dann auch gleich einen „Digital-Gesetzgeber“?

Fazit

Das Orakel hat gesprochen. Provokant könnte man dazu noch sagen, dass wenn eine EuGH-Entscheidung mit den folgenden Absätzen beginnt, man eigentlich schon weiß, wie sie ausgehen wird:

> Im zehnten Erwägungsgrund der Richtlinie 95/46 heißt es:
>
> „Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und -freiheiten, insbesondere des auch in Artikel 8 der [am 4. November 1950 in Rom unterzeichneten] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des [Unionsrechts] anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern muss im Gegenteil darauf abzielen, in der [Union] ein hohes Schutzniveau sicherzustellen."
>
> Art. 1 der Richtlinie 95/46 sieht vor:
>
> „(1) Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten."

Die hier zitierten Rechtsquellen sind eigentlich nicht „subsumtionsfähig" und daher als solche wenig geeignet, den Fall zu lösen (weshalb sie dann auch durch die Zitierung der einzelnen relevanten Regelungen der Datenschutzrichtlinie ergänzt werden) – aber faktisch geben sie als „politische Programmnormen" das Ergebnis vor. Die Zielrichtung des EuGH ist es, Datenschutzrecht extensiv in Richtung Datenschutz auszulegen. Die Einzelheiten der Argumentation rücken da fast schon in den Hintergrund. Jeder, der die Entscheidung in der Sache begrüßt – darunter natürlich die Datenschutzbehörden –, wird daher behaupten, sie sei natürlich vorhersehbar und alternativlos gewesen. Dass die Entscheidung, wie so häufig, „unter der Lupe" mehr Fragen aufwirft als sie beantworten kann, liegt in der Natur der Sache. Dogmatisch zwingend oder auch nur überzeugend gegen Alternativen abgewogen ist sie nicht.

PSP MÜNCHEN

In der Praxis bedeutet dies, dass „Social Plugins“ bzw. die eingebundenen „Codeschnipsel“ eigentlich erst einmal vom Netz genommen werden sollten, denn zunächst müssen die Social-Media-Anbieter „Joint Controller Agreements“, Pflichtinformationen und überzeugende Legitimationsgrundlagen liefern und letztlich auch ihre Serverfarmen für eine Überprüfung dieser Angaben öffnen. Ansonsten ist die Mithaftung eröffnet. Für die meisten wird sich da eher die Frage stellen, ob der Aufwand bzw. das Restrisiko, „für“ Facebook in die Haftung genommen zu werden, noch den erhofften Nutzen lohnt.

Was sonst noch so alles ins Visier des prinzipientreu datenschutzfreundlichen EuGH gerät, werden wir in den nächsten Jahren sehen.