

**Ergebnisbericht der Arbeitsgruppe des AK I „Staatsrecht  
und Verwaltung“ zum Datenschutz in Sozialen Netzwerken  
vom 4. April 2012**

**Inhaltsverzeichnis**

<b>I. Einleitung</b>	<b>3</b>
<b>II. Öffentlichkeitsarbeit in sozialen Netzwerken als Gegenstand datenschutzaufsichtlicher Diskussion</b>	<b>4</b>
<b>III. Berichtsbitte der CdS-Jahreskonferenz vom 22./23. September 2011</b>	<b>4</b>
<b>IV. Aktuelle Entwicklungen</b>	<b>5</b>
<b>V. Ausblick – weitere Entwicklung</b>	<b>26</b>
<b>IV. Gemeinsame Vorschläge des AK I</b>	<b>27</b>

Der Ergebnisbericht beruht auf den Arbeiten einer vom AK I anlässlich der Berichtsbitte der CdS-Jahreskonferenz vom 22./23. September 2011 eingerichteten länderoffenen Arbeitsgruppe. Eine Sitzung der Arbeitsgruppe unter Federführung des Landes Berlin und des Freistaats Bayern fand am 17. Februar 2012 statt.

## I. Einleitung

Ein Grund für die Popularität von Sozialen Netzwerken liegt darin, dass deren Betreiber durch neue Funktionen die Kommunikationsmöglichkeiten für die Nutzer ausbauen und dadurch die „soziale Vernetzung“ weiter steigern. Den Nutzern wird ermöglicht, ihr Leben immer schneller und einfacher mit ihren „Freunden“ in Sozialen Netzwerken zu teilen.

In letzter Zeit geschieht dies auch dadurch, dass Soziale Netzwerke ihren Wirkungskreis über die eigene Internetpräsenz hinaus mittels „Social Plugins“ ausdehnen. Insbesondere der Like-Button von Facebook hat sich rasant über das gesamte Internet verbreitet. Durch dessen Einbettung können Betreiber von Webseiten Facebook-Nutzern individualisierte Nutzungsmöglichkeiten für ihre Webseite anbieten. Ein Facebook-Nutzer kann durch einen Klick auf den Like-Button seine Facebook-Freunde auf seiner Profilseite auf die Webseite aufmerksam machen. Zudem wird einem eingeloggten Facebook-Nutzer, der eine Webseite mit Like-Button besucht, personalisierter Inhalt angeboten: er erfährt, welche seiner Facebook-Freunde die Webseite ebenfalls empfohlen haben und ggf. welche Kommentare sie über die Webseite gepostet haben.

Die Funktionsweise des Like-Buttons verdeutlicht, dass damit nicht nur die Kommunikationsmöglichkeiten der Facebook-Nutzer erweitert werden, sondern für einen Webseitenbetreiber durch die Empfehlung im Facebook-Profil des klickenden Mitglieds ein neuer Marketingweg für seine Seite (und damit für die angebotenen Produkte und Dienstleistungen) eröffnet wird. Soziale Netzwerke werden daher für öffentliche und private Institutionen im Hinblick auf Öffentlichkeitsarbeit und Marketing immer bedeutender.

Neben Social Plugins bieten die Betreiber von sozialen Netzwerken in zunehmendem Maß auch innerhalb der eigenen Internetpräsenz privaten und öffentlichen Institutionen Möglichkeiten für Öffentlichkeitsarbeit. Prominentestes Beispiel sind die Fanpages von Facebook. Dies sind Seiten auf der Plattform Facebook, welche von Unternehmen und Institutionen zur Eigendarstellung betrieben werden können und Facebook-Nutzern die unmittelbare Kommunikation mit dem Unternehmen unter Einbindung ihrer Facebook-Freunde ermöglichen.

Eine anlässlich der Erstellung dieses Berichts initiierte Umfrage im Länderkreis hat ergeben, dass öffentliche Stellen insbesondere Fanpages, aber auch in geringerem Maße Social Plugins für ihre Öffentlichkeitsarbeit vielfältig nutzen. Aus dem Polizeibereich wurde neben klassischer Öffentlichkeitsarbeit auch die Nutzung von Fanpages als Veröffentlichungsplatt-

form für Fahndungsaufrufe und Vermisstensuche genannt. Die sich hieraus ergebenden besonderen Fragestellungen bedürfen einer gesonderten polizeifachlichen Prüfung und sind nicht Gegenstand dieses Berichts.

## **II. Öffentlichkeitsarbeit in sozialen Netzwerken als Gegenstand datenschutzaufsichtlicher Diskussion**

Im August 2011 hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) alle Webseitenbetreiber in Schleswig-Holstein aufgefordert, ihre Fanpages bei Facebook und Social Plugins auf ihren Webseiten zu entfernen. Diese verstießen in ihrer gegenwärtigen Ausgestaltung gegen Bestimmungen des Telemediengesetzes (TMG).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 28./29. September 2011 hervorgehoben, dass die direkte Einbindung des Like-Buttons und anderer Social Plugins in die Webseiten deutscher Anbieter momentan ohne hinreichende Information der Nutzer über die ausgelösten Datenverarbeitungsvorgänge und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang stehe. Öffentliche Stellen sollten daher von der Nutzung absehen; gleiches gelte für Fanpages.

Der Düsseldorfer Kreis hat am 8. Dezember 2011 beschlossen, dass die Betreiber von Fanpages und von Webseiten mit Like-Button eine Mitverantwortung für die Einhaltung der Datenschutzvorschriften treffe. Hierzu gehöre die umfassende Aufklärung der Nutzer über die erhobenen Daten. Insbesondere beim Like-Button seien den Webseitenbetreibern die Datenflüsse an Facebook nicht in vollem Umfang bekannt, sodass sie diesen nicht ohne weiteres in das eigene Angebot einbinden dürften.

## **III. Berichtsbitte der CdS-Jahreskonferenz vom 22./23. September 2011**

Die Chefinnen und Chefs der Staats- und Senatskanzleien der Länder haben auf ihrer Jahreskonferenz vom 22./23. September 2011 die Diskussion über die Verbesserung des Datenschutzes in sozialen Netzwerken begrüßt, insbesondere wenn Webseitenbetreiber Fanpages z.B. bei Facebook oder Social Plugins auf ihren Webseiten eingerichtet haben (Ziffer 1 des CdS-Beschlusses). Sie stellen fest, dass die Sozialen Netzwerke von öffentlichen Stellen auf allen Ebenen, von privaten Institutionen und von Unternehmen als neue Form der Kommunikation genutzt würden. Zur Förderung der Belange des Datenschutzes sei ein zwischen Bund und Ländern abgestimmtes gemeinsames Handeln erforderlich, das europäi-

sche und internationale Bezüge berücksichtige und hierbei auch die Notwendigkeit der Änderung gesetzlicher Regelungen einbeziehe (Ziffer 2 des CdS-Beschlusses). Sie haben die Konferenz der Innenminister und -senatoren der Länder gebeten

- über die aktuellen Entwicklungen zu berichten und
- unter Einbeziehung von Initiativen der Bundesregierung sowie der Ergebnisse der Konferenz der Datenschutzbeauftragten erste gemeinsame Vorschläge zu machen (Ziffer 3 des CdS-Beschlusses).

Zur Erstellung des Berichts hat der Arbeitskreis I „Staatsrecht und Verwaltung“ der Innenministerkonferenz eine Arbeitsgruppe einberufen.

#### **IV. Aktuelle Entwicklungen**

##### **1. Sachstand Schleswig-Holstein**

Nach einer Pressemitteilung des ULD hat es hinsichtlich des Betriebens von Fanpages gegenüber sechs öffentlichen Stellen Beanstandungen ausgesprochen sowie gegenüber drei nicht-öffentlichen Stellen eine Anordnung nach § 38 Abs. 5 des Bundesdatenschutzgesetzes (BDSG) erlassen. Gegen die Anordnungen nach § 38 Abs. 5 BDSG wurde jeweils Anfechtungsklage zum VG Schleswig erhoben.

##### **2. Gutachten, Untersuchungen und Gremienbefassung**

###### **2.1. Nationale Ebene**

Neben Veröffentlichungen in der datenschutzrechtlichen Literatur liegen mittlerweile eine Vielzahl von technischen und rechtlichen Analysen zur Nutzung von Fanpages sowie der Einbindung des Like-Buttons vor. Hervorzuheben sind:

- Arbeitspapier des ULD „*Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook*“ vom 19. August 2011
- Ausarbeitung des Wissenschaftlichen Dienstes Dt. Bundestag „*Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins*“ vom 7. Oktober 2011
- Ausarbeitung des Wissenschaftlichen Dienstes Landtag Schleswig-Holstein vom 24. Oktober 2011

Zu technischen Fragen ist zudem eine umfassende Korrespondenz zwischen dem ULD und dem Unternehmen Facebook öffentlich zugänglich.

## **2.2. Europäische Ebene**

Die irische Datenschutzaufsichtsbehörde hat anlässlich einer Betriebsüberprüfung bei „Facebook Ireland Ltd.“ neben der Konzernstruktur des Unternehmens Facebook eine Vielzahl von Funktionen von Facebook (darunter auch den Like-Button) untersucht und bewertet. Der Untersuchungsbericht vom 21. Dezember 2011 enthält als Anlage auch eine technische Analyse der Funktionen. Der Bericht soll voraussichtlich in der Art-29-Datenschutzgruppe beraten werden. Diese hat sich in der Vergangenheit zudem bereits mit dem Datenschutz in sozialen Netzwerken beschäftigt (Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke vom 12. Juni 2009, WP 163).

## **3. Würdigung der Sach- und Rechtsfragen**

### **3.1. Allgemeines**

Für die datenschutzrechtliche Beurteilung ist Kenntnis der technischen Abläufe erforderlich, d.h. Kenntnis davon, welche Arten von Daten bei Social Plugins und Fanpages unter welchen Bedingungen von wem verarbeitet werden. Die unter Ziffer 2.1. zitierten Ausarbeitungen, die Korrespondenz von Facebook mit dem ULD sowie der Untersuchungsbericht der irischen Datenschutzaufsichtsbehörde tragen hier zur Klärung bei. Die technischen Abläufe werden daher im Folgenden für den Like-Button und die Facebook-Fanpages beschrieben. Jedoch verbleiben Unsicherheiten, auf deren Auswirkung bei der Würdigung der Sach- und Rechtslage nachfolgend im Einzelnen einzugehen ist.

### **3.2. Technische Abläufe beim Like-Button und bei Fanpages**

#### **(1) Grundlagen**

Die Einbindung des Like-Buttons in Webseiten erfolgt mittels eines sog. Inline-Frames, der auch bei vielen anderen Internetseiten zur Zusammenführung von Text- und Bildinhalten verschiedener Anbieter genutzt wird. Dies bedeutet, dass beim Aufruf einer Webseite mit Like-Button auch der Webserver von Facebook aufgerufen wird, ohne dass dies im Browser des Nutzers erkennbar ist. Es werden die gleichen Informationen an den Facebook-Server übertragen, die auch bei einem ausdrücklichen Aufruf der Seite durch Eingabe in den Browser übertragen werden. Dies ermöglicht es zum Beispiel, dass Cookies, welche Facebook zu einem früheren Zeitpunkt

im Browser des Nutzers gesetzt hat, beim Besuch einer Webseite mit Like-Button an Facebook übertragen werden.

Fanpages sind Webseiten von Facebook und enthalten daher auch die URL der Facebook-Seite (Beispiel: Fanpage des FC Bayern München, abrufbar unter <http://de-de.facebook.com/FCBayern>). Das Aufrufen einer Fanpage ist somit ein Aufrufen der Facebook-Seite.

## **(2) Datenflüsse**

Sowohl beim Like-Button als auch bei Fanpages ist nach Fallgruppen zu unterscheiden. Differenziert werden muss zwischen:

- Facebook-Mitgliedern und Nicht-Facebook-Mitgliedern
- Eingeloggten und nicht eingeloggten Facebook-Mitgliedern
- Klicken des Like-Buttons und bloßem Besuch einer Webseite mit Like-Button

Betreffend die Art von Daten sind die IP-Adressen der Nutzer und die von Facebook gesetzten und an Facebook übertragenen Cookies für die datenschutzrechtliche Beurteilung von Bedeutung.

### *IP-Adressen*

Sowohl beim Like-Button als auch bei Fanpages findet eine Übertragung der IP-Adresse des Nutzers an Facebook statt. Ohne Übertragung der IP-Adresse des Nutzers könnte diesem der Inhalt des Like-Buttons und der Fanpage nicht dargestellt werden. Nach Angaben von Facebook wird die IP-Adresse in den meisten Fallgruppen unmittelbar nach Übertragung in eine „*generische IP-Adresse*“ umgewandelt. Dieser Begriff ist kein IT-Fachbegriff, sondern eine Bezeichnung von Facebook, die eine Anonymisierung meint. Details hierzu sind bislang nicht bekannt.

### *Cookies*

Facebook setzt sowohl über den Like-Button als auch bei Fanpages Cookies im Webbrowser der Nutzer, wobei hier zwischen den Fallgruppen zu unterscheiden ist. Für die datenschutzrechtliche Würdigung bedeutsam sind der sog. datr-Cookie sowie der c\_user-Cookie. Der datr-Cookie, der bei jedem Aufruf der Webseite [www.facebook.com](http://www.facebook.com) gesetzt wird (Anm.: durch den Klick auf den Like-Button öffnet sich diese in einem separaten Fenster; bei Fanpages findet ein Aufruf der Facebook-Webseite statt), hat eine Gültigkeit von zwei Jahren, kann aber durch entsprechende Browsereinstellung blockiert und gelöscht werden. Er dient Facebook nach eigenen

Angaben zur Identifizierung des Webbrowsers, der die Verbindung mit der Facebook-Seite aufbaut, und spielt eine Schlüsselrolle beim Schutz des Sozialen Netzwerks vor „böswilligen Aktivitäten“. Der c\_user-Cookie wird von Facebook gesetzt, wenn sich das Facebook-Mitglied einloggt, und enthält die Anmeldekennnummer (User-ID) des Facebook-Mitglieds. Facebook kann dadurch das Mitglied identifizieren, den Aufruf der Webseite mit Like-Button oder der Fanpage einer konkreten Person zuordnen und auf diese Weise den Inhalt des Like-Buttons bzw. der Fanpage personalisieren. Die Gültigkeit des c\_user-Cookies hängt davon ab, ob das Facebook-Mitglied in seinen Kontoeinstellungen die Option „Angemeldet bleiben“ gewählt hat oder nicht. Hat es diese gewählt, verliert der Cookie seine Gültigkeit erst, wenn das Facebook-Mitglied den Facebook-Webserver 30 Tage nicht mehr aufruft. Ansonsten wird der c\_user-Cookie mit dem Schließen des Browsers gelöscht.

Die nachfolgenden Tabellen 1 und 2 stellen die Datenflüsse dar, die Facebook beim Besuch einer Webseite mit Like-Button bzw. einer Fanpage vom Nutzer erhält.

Tabelle 1: Like-Button

	<b>Fallgruppe</b>	<b>Technische Abläufe</b>
1	Nicht-Facebook-Mitglied besucht erstmalig eine Webseite mit Like-Button und klickt diesen nicht	Übertragung der IP-Adresse und Speicherung als generische IP-Adresse
2	Nicht-Facebook-Mitglied besucht erstmalig eine Webseite mit Like-Button und klickt auf diesen	Übertragung der IP-Adresse/Speicherung als generische IP-Adresse <u>und</u> Setzen des datr-Cookie
3	Nicht-Facebook-Mitglied besucht, nachdem es früher bereits auf derselben oder einer anderen Webseite auf den Like-Button geklickt hatte, erneut eine Webseite mit Like-Button und - klickt aber den Like-Button nicht erneut - klickt den Like-Button erneut	Übertragung der IP-Adresse/Speicherung als generische IP-Adresse <u>und</u> Übertragung des datr-Cookie (soweit noch gültig und noch nicht gelöscht)
4	Facebook-Mitglied, das gerade nicht eingeloggt ist, besucht eine Webseite mit Like-Button und klickt diesen nicht	Übertragung der IP-Adresse/Speicherung als generische IP-Adresse <u>und</u> Übertragung des datr-Cookie (soweit noch gültig und noch nicht gelöscht)
5	Facebook-Mitglied, das gerade nicht eingeloggt ist, besucht eine Webseite mit Like-Button und klickt auf diesen	Übertragung der IP-Adresse und Speicherung als spezifische IP-Adresse <u>und</u> Übertragung des datr-Cookie (soweit noch gültig und noch nicht gelöscht)
6	Eingeloggtes Facebook-Mitglied besucht eine Webseite mit Like-Button	Übertragung der IP-Adresse und Speicherung als spezifische IP-Adresse <u>und</u> Übertragung des datr-Cookie (soweit noch gültig und noch nicht gelöscht) <u>und</u>

	Übertragung des c_user-Cookie
--	-------------------------------

Tabelle 2: Fanpage

	Fallgruppe	Technische Abläufe
1	Nicht-Facebook-Mitglied oder Facebook-Mitglied, das gerade nicht eingeloggt ist, besucht eine Fanpage	Übertragung der IP-Adresse (unklar, ob Speicherung als generische oder spezifische IP-Adresse) <u>und</u> Setzen/Übertragen des datr-Cookie
2	Eingeloggtes Facebook-Mitglied besucht eine Fanpage	Übertragung der IP-Adresse (unklar, ob Speicherung als generische oder spezifische IP-Adresse) <u>und</u> Setzen/Übertragung des datr-Cookie <u>und</u> Übertragung des c_user-Cookies

### (3) Facebook Insights

Webseitenbetreiber, die den Like-Button einbinden, und Betreiber von Fanpages können mit Hilfe des von Facebook kostenfrei zur Verfügung gestellten Werkzeugs „Facebook Insights“ Statistkinformationen über Nutzer abrufen. Die durch Facebook erstellten Statistiken enthalten Angaben über die Nutzung der Webseite/Fanpage. Dazu gehören Informationen über den Nutzerzuwachs, die Demographie der Nutzer und über die Nutzung der einzelnen Funktionalitäten von Like-Button/Fanpage.

### 3.3. Rechtsfragen – Würdigung

Die Darstellung der Rechtsfragen behandelt ausschließlich den Like-Button und Facebook-Fanpages, über deren Funktionsweise am meisten bekannt ist.

Like-Button und Fanpages ermöglichen dem Nutzer durch entsprechende Verwendung der Funktionen eine Kommunikation, d.h. das Teilen von Inhalten mit anderen. Aufgrund seiner Funktionsweise ist der Like-Button insbesondere nicht nur eine auf eine einfache Transportfunktion von Inhalten reduzierte Leistung. Auch Fanpages bieten einem Besucher Bedienmöglichkeiten zur Interaktion mit dem Fanpage-Betreiber und den anderen Nutzern des Sozialen Netzwerks, die über eine einfache Transportfunktion von Inhalten hinausgeht. Aus diesem Grund sind Like-Button und Fanpage als Telemedien nach § 1 Abs. 1 Satz 1 TMG zu qualifizieren, sodass der sachliche Anwendungsbereich des TMG eröffnet ist.

Im Überblick stellen sich dann bei der Nutzung von Like-Button und Fanpage auf der Grundlage des Telemediengesetzes folgende Rechtsfragen, die nachfolgend im Einzelnen zu würdigen sind.

Tabelle 3: Überblick zu den Rechtsfragen

Aufgeworfene Rechtsfrage	Würdigung unter
Internationales Datenschutzrecht: Anwendbarkeit deutschen Rechts?	(1)
Personenbezug der erhobenen Daten?	(2)
Verantwortlichkeit der Betreiber von Webseiten mit Like-Button und der Betreiber von Fanpages?	(3)
Verstoß gegen § 15 Abs. 3 TMG wegen Facebook Insights und/oder Setzen/Übertragen von Cookies?	(4)
Cookies nur noch mit Einwilligung des Nutzers?	(5)
Zulässigkeit der Übertragung und Speicherung der <u>generischen IP-Adresse</u> ?	(6)
Zulässigkeit der Speicherung der <u>spezifischen IP-Adresse</u> ?	(7)
Zulässigkeit des Setzens/der Übertragung des <u>dat-Cookie</u> ?	(8)
Zulässigkeit der Übertragung des <u>c User-Cookie</u> ?	(9)

### (1) Internationales Datenschutzrecht: Anwendbarkeit deutschen Rechts?

Dies wird kontrovers diskutiert. Facebook ist der Auffassung, dass seine irische Niederlassung *Facebook Ireland Ltd.* verantwortliche Stelle für die Datenverarbeitung seiner deutschen (und europäischen) Mitglieder sei und daher irisches Datenschutzrecht Anwendung finde. Das ULD sieht die Verantwortlichkeit bei *Facebook Inc.* in den USA, sodass deutsches Datenschutzrecht anwendbar sei. Die irische Niederlassung sei lediglich eine Anlauf- und Beschwerdestelle, trage jedoch für die Datenverarbeitung keine Verantwortlichkeit.

### Würdigung

Die Anwendbarkeit deutschen Datenschutzrechts kann aufgrund des Untersuchungsberichts der irischen Datenschutzaufsicht kritisch hinterfragt werden. Die Befassung der Art-29-Datenschutzgruppe und v.a. die in Schleswig-Holstein anhängigen Gerichtsverfahren können diesbezüglich zur Klärung beitragen.

Im Einzelnen:

Die Datenschutzvorschriften des TMG (§§ 11ff.) finden gemäß § 3 Abs. 3 Nr. 4 TMG, § 1 Abs. 5 Satz 2 BDSG nur Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt.

Im Fall des Like-Buttons und der Fanpage wäre dies der Fall, wenn

- die Betreiber deutscher Webseiten mit Like-Button/Fanpages die Daten erheben und sie dann an Facebook übermitteln oder
- Facebook die Daten durch seine US-Niederlassung *Facebook Inc.* erhebt.

Übermitteln ist gemäß § 12 Abs. 3 TMG, § 3 Abs. 4 Satz 2 Nr. 3 BDSG das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abrufen. Erforderlich ist neben einem Bereithalten der Daten, dass Gegenstand der Übermittlung „gespeicherte“ oder „durch Datenverarbeitung gewonnene“ personenbezogene Daten sind.

Im Hinblick auf den Betreiber einer Webseite mit Like-Button oder einer Fanpage ist dies aber nicht der Fall, da diese den Datenbestand, der Facebook zur Kenntnis gelangt, nicht auf einem Datenträger festhalten, d.h. also nicht „speichern“. Der Datenbestand, den Facebook in Bezug auf die IP-Adresse von Nutzern zur Kenntnis erhält, mag inhaltlich der gleiche sein wie ihn auch der Webseitenbetreiber erhält. Er ist jedoch nicht „durch die Hände“ des Webseitenbetreibers gegangen und besteht unabhängig von dessen Datensatz. Besonders evident ist die fehlende Speicherung bei den von Facebook gesetzten Cookies. Auf diese hat nur Facebook Zugriff; der Webseitenbetreiber kann sie weder einsehen noch verändern. Die von Facebook empfangenen Daten stellen auch keine unmittelbar „durch Datenverarbeitung gewonnenen“ Daten dar, da sie vom Webseiten-/Fanpagebetreiber in keiner Weise für Facebook aufbereitet werden. Ein Übermitteln durch den Webseitenbetreiber erfolgt somit nicht.

Für die Frage, ob Facebook die Daten durch seine US-Niederlassung *Facebook Inc.* erhebt, ist entscheidend, ob die irische Niederlassung *Facebook Ireland Ltd.* eine für die Datenerhebung verantwortliche Stelle ist. Wird dies bejaht, findet gemäß § 1 Abs. 5 Satz 1 BDSG irisches Datenschutzrecht Anwendung, welches die deutschen Datenschutzaufsichtsbehörden gemäß § 1 Abs. 5 Satz 5, § 38 Abs. 1 Satz 1 BDSG ihrer datenschutzrechtlichen Beurteilung zugrunde legen müssten. Gemäß § 12 Abs. 3 TMG, § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt, wobei es darauf ankommt, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (vgl. Art. 2 lit. d RL 95/46/EG). Die irische Datenschutzauf-

sichtsbehörde hat die Struktur und die Aufgaben von *Facebook Ireland Ltd.* – v.a. im Verhältnis zu *Facebook Inc. USA* – eingehend untersucht. Aus dem Untersuchungsbericht sind folgende Gesichtspunkte besonders hervorzuheben:

- Zwischen *Facebook Ireland Ltd.* und *Facebook Inc. USA* besteht ein „*Data Transfer and Processing Agreement*“, in dem Facebook Ireland für Daten von Mitgliedern außerhalb der USA und Kanada als „data exporter“ und Facebook Inc. als „data importer“ bezeichnet wird.
- *Facebook Ireland Ltd.* hat *Facebook Inc.* durch ein „*Data hostings service agreement*“ als Serviceprovider mit der Datenverarbeitung beauftragt.
- Sowohl das „*Data Transfer and Processing Agreement*“ als auch das „*Data hostings service agreement*“, die beide seit September 2010 gelten, werden als rechtsgültig und wirksam betrachtet.
- *Facebook Ireland Ltd.* (400 Mitarbeiter) führt für Mitglieder außerhalb der USA und Kanada u.a. die Bereiche „Developer Relations“, „Site Reliability Operations“, „User Operations“, „Network Operations“ und „Database Operations“.

Gerade die (von der irischen Datenschutzaufsicht gewürdigten) vertraglichen Vereinbarungen zwischen *Facebook Ireland Ltd.* und *Facebook Inc.* könnten die Schlussfolgerung zulassen, dass die irische Niederlassung über Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der europäischen Nutzer entscheidet und daher auch für deutsche Nutzer eine datenschutzrechtliche Beurteilung nach irischem Recht erfolgen muss. Die Frage ist bislang noch nicht abschließend geklärt, das ULD ist anderer Auffassung.

Unabhängig von der endgültigen Beantwortung der Frage des anwendbaren Rechts werden nachfolgend die zu prüfenden Fragen auf der Grundlage des deutschen Rechts bewertet. Denn sowohl das ggf. auf Facebook anzuwendende irische als auch das deutsche Recht setzen EU-Recht um, so dass in jedem Fall die gleichen Schutzziele zugrunde liegen.

## **(2) Personenbezug der erhobenen Daten?**

Das ULD ist der Auffassung, dass mit dem Like-Button und bei Fanpages folgende personenbezogenen Daten im Sinne des § 3 Abs. 1 BDSG erhoben und verarbeitet werden:

- die durch die Facebook-Mitglieder gespeicherten persönlichen Informationen,

- die IP-Adressen von Besuchern der Fanpages bzw. der Webseiten mit Like-Button (sowohl bei Facebook-Mitgliedern als auch bei Nicht-Facebook-Mitgliedern),
- die durch Facebook genutzten/gesetzten Cookies (sowohl bei Facebook-Mitgliedern als auch bei Nicht-Facebook-Mitgliedern)

### Würdigung

Die durch die Facebook-Mitglieder gespeicherten persönlichen Informationen und der c-user-Cookie sind personenbezogene Daten.

Ob dynamische IP-Adressen generell personenbezogene Daten sind, ist gerichtlich nicht abschließend geklärt. Eine richtlinienkonforme Auslegung könnte für eine Bejahung des generellen Personenbezugs sprechen, sodass für deren Übertragung §§ 11ff. TMG gelten.

Ob der datr-Cookie als personenbezogenes Datum qualifiziert werden kann, für dessen Nutzung dann §§ 11ff. TMG gilt, ist aufgrund des Untersuchungsberichts der irischen Datenschutzaufsicht fraglich, kann aber aufgrund des gegenwärtigen Sachstands nicht mit Sicherheit ausgeschlossen werden. Eine Offenlegung des Inhalts des datr-Cookies durch Facebook gegenüber den deutschen Datenschutzaufsichtsbehörden wäre zu begrüßen.

Im Einzelnen:

#### *Gespeicherte persönliche Informationen der Facebook-Mitglieder:*

Die bei der Facebook-Registrierung durch die Nutzer gemachten Angaben wie Name, Alter, Geschlecht und Beruf sind personenbezogene Daten. Beim Besuch einer Webseite mit Like-Button bzw. beim Besuch einer Fanpage durch ein eingeloggtes Facebook-Mitglied kommt es zu einer Verknüpfung mit seinem Account, weswegen eine Identifizierung möglich ist (vgl. Tabelle 1 Fallgruppe 6 und Tabelle 2 Fallgruppe 2) In-soweit werden beim Like-Button und beim Besuch einer Fanpage personenbezogene Daten verarbeitet.

#### *IP-Adressen:*

Die Frage nach dem Personenbezug von dynamischen IP-Adressen ist weder auf nationaler noch europäischer Ebene höchstrichterlich entschieden. Die Rechtsprechung der Instanzgerichte ist nicht einheitlich.

Eine Auffassung prüft den Personenbezug relativ und bejaht ihn nur für diejenige datenverarbeitende Stelle, die über Kenntnisse, Mittel und Möglichkeiten (dementsprechend ein etwaiges Zusatzwissen) zur Zuordnung zu einer bestimmten Person verfügt. Dies trifft i.d.R. nur für den Access-Provider (Anbieter des Internetzugangs) zu, da dieser dem Nutzer mit jeder Einwahl die IP-Adresse zuweist und daher über die Mittel und Möglichkeiten der Zuordnung verfügt. Die Anbieter des Webseiteninhalts (wie Facebook und die Betreiber der Webseite mit Like-Button/Fanpagebetreiber) haben dieses Zusatzwissen hingegen nicht. Die andere Auffassung lässt bereits die theoretische Möglichkeit der Bestimmbarkeit einer Person genügen, um generell von einem personenbezogenen Datum auszugehen, auch wenn die Person nur durch einen Dritten bestimmt werden kann und dieser das notwendige Zusatzwissen nicht an die verarbeitende Stelle weitergibt.

Zumindest Erwägungsgrund 26 der EG-Datenschutzrichtlinie 95/46/EG könnte für letztgenannte Auffassung sprechen. Darin heißt es zum Begriff des personenbezogenen Datums in Art. 2 a) der Richtlinie, dass bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen. Daher könnte folglich die Identifizierbarkeit allein durch einen Dritten für eine Bestimmbarkeit ausreichen und ein genereller Personenbezug von dynamischen IP-Adressen zu bejahen sein, sodass die IP-Adresse auch für Facebook und die Webseitenbetreiber/Fanpagebetreiber ein personenbezogenes Datum wäre.

Auch der von der Europäischen Kommission vorgelegte Entwurf einer EU-Datenschutzgrundverordnung lässt insoweit bislang keine eindeutige Festlegung erkennen (Wortlaut des Art. 4 Abs. 1 und Abs. 2 sowie Erwägungsgrund 24).

#### *Cookies:*

Ob bei der Nutzung von Cookies von einer Erhebung/Verarbeitung personenbezogener Daten auszugehen ist, hängt davon ab, ob im Cookie als einem Datenpaket/Textdatei personenbezogene Informationen über den Nutzer gespeichert sind. Wenn Cookies personenbezogene Daten enthalten und dem Zweck dienen, personenbezogene Daten zu sammeln, gelten für die Nutzung die Datenschutzvorschriften des TMG.

Der c\_user-Cookie enthält die Anmeldekennnummer des Facebook-Mitglieds, d.h. dessen personenbezogene Informationen. Damit kann Facebook eingeloggte Mitglieder identifizieren, was auch gewollt ist, um den Like-Button und die Fanpage mit personalisiertem Inhalt anbieten zu können. Für den c\_user-Cookie gelten daher §§ 11ff. TMG.

Nach Angaben von Facebook ist alleiniger Zweck des datr-Cookie, „böswillige Aktivitäten zu verhindern und unsere Nutzer zu schützen“. Er werde nicht dazu eingesetzt, personenbezogene Daten zu sammeln. Ob die Verwendung des datr-Cookies tatsächlich nur die Abwehr missbräuchlicher Nutzung des sozialen Netzwerks bezweckt, wird von den deutschen Aufsichtsbehörden kritisch hinterfragt. Es werden zum einen erhebliche Zweifel an der Effektivität zur „Missbrauchsabwehr“ geäußert. Zum anderen könne bei entsprechender inhaltlicher Gestaltung insbesondere bei Nicht-Facebook-Mitgliedern, bei denen der datr-Cookie einmal gesetzt wurde und die später Mitglied werden, durchaus die Möglichkeit bestehen, personenbezogene Daten zu erheben und Nutzerprofile unter Einbeziehung und Zuordnung der besuchten Webseiten mit Like-Button und Fanpages (vor Mitgliedschaft) zu erstellen; v.a. die zweijährige Geltungsdauer könnte dies nahelegen. Allerdings ist die Einschätzung der irischen Datenschutzaufsicht zur alleinigen „Sicherheitsrelevanz“ des datr-Cookie wohl eine andere: diese hat bei ihrer Prüfung keine Anhaltspunkte dafür feststellen können, dass der datr-Cookie der Sammlung personenbezogener Daten dient. Jedoch ist dabei nicht zu verkennen, dass Facebook den genauen Inhalt des datr-Cookie bislang zumindest gegenüber den deutschen Aufsichtsbehörden nicht offengelegt hat.

### **(3) Verantwortlichkeit der Betreiber von Webseiten mit Like-Button und der Betreiber von Fanpages?**

Das ULD ist der Auffassung, dass diese neben Facebook die rechtliche Verantwortung für die Einhaltung der Datenschutzvorschriften des TMG tragen. Diese Verantwortung stellt auch der Beschluss des Düsseldorfer Kreises zu Sozialen Netzwerken vom 8. Dezember 2011 heraus.

#### **Würdigung**

Beim Like-Button ist für die Webseitenbetreiber zumindest eine datenschutzrechtliche Mitverantwortung gut begründbar. Bei Fanpages kann man diese in Frage stellen, allerdings lässt sich nicht ausschließen, dass deutsche Gerichte auf die Einflussnahmemöglichkeit hinsichtlich des Ob der Datenverarbeitung abstellen.

Im Einzelnen:

Eine Verantwortlichkeit, die sich für die Datenschutzvorschriften des TMG nach § 3 Abs. 7 BDSG richtet, kommt für Webseitenbetreiber/Fanpage-Betreiber in Betracht, wenn

- sie selbst personenbezogene Daten erheben, verarbeiten oder nutzen,
- Facebook durch den Like-Button bzw. mit der Fanpage im Auftrag der Webseitenbetreiber/Betreiber von Fanpages personenbezogene Daten erhebt oder
- Facebook und die Webseitenbetreiber/Betreiber von Fanpages eine gemeinsame Verantwortung tragen.

*Erhebung/Verarbeitung durch Webseitenbetreiber/Fanpage-Betreiber:*

Die Datenflüsse erfolgen unmittelbar an Facebook. Eine Verarbeitung in Form einer Datenübermittlung durch den Webseitenbetreiber/Fanpage-Betreiber findet wie oben dargelegt nicht statt.

*Auftragsdatenverarbeitung durch Facebook:*

Beim Like-Button könnte dies deshalb in Betracht kommen, weil Facebook den Webseitenbetreibern den Dienst „Facebook Insights“ zur Verfügung stellt, mit dem diese Informationen zur Reichweite der Nutzung ihrer Webseite erlangen können. Allerdings ist die Bereitstellung von „Facebook Insights“ im Hinblick auf die sonstigen Funktionen des Like-Buttons nicht Hauptzweck der Vertragsbeziehung. Insbesondere steht für Facebook beim Like-Button im Vordergrund, seinen Mitgliedern Zusatzfunktionen im Sinne einer erleichterten Kommunikation mit Facebook-Freunden und einer Personalisierung von Webseiteninhalten anzubieten, und durch die zunehmende Präsenz des Like-Buttons verstärkt neue Mitglieder zu werben. Die Tätigkeit von Facebook im Zusammenhang mit dem Like-Button wird damit nicht nur durch die für die Auftragsdatenverarbeitung kennzeichnenden Merkmale eines Über-/Untersetzungsverhältnisses oder bloßer Hilfsfunktionen für einen Webseitenbetreiber geprägt.

Bei den Fanpages spricht für eine Auftragsdatenverarbeitung, dass ein eigener Internetauftritt des Betreibers unter der Oberfläche von Facebook vorliegt und dass Facebook die technischen Möglichkeiten zur Verfügung stellt, damit z.B. Kommentare auf der Pinnwand gepostet werden können. Gegen eine Auftragsdatenverarbeitung spricht, dass der Betreiber nur sehr geringe Einflussmöglichkeiten auf die optische Gestaltung einer Fanpage und v.a. die ihm zur Verfügung stehenden Funktionen hat. Zudem ist die Fanpage eine Facebook-Domain, der Dienst „Facebook Insights“ wird

kostenlos zur Verfügung gestellt. Allerdings wurde das rechtliche Verhältnis zwischen Fanpage-Betreiber und Facebook von den deutschen Aufsichtsbehörden – soweit ersichtlich – noch nicht näher untersucht. Deren Einschätzung, dass Facebook die Nutzungsbedingungen für Fanpages strikt vorgibt und keine Abweichungen verhandelbar sind, dürfte jedoch schwer widerlegbar sein. Hierfür sprechen die Marktmacht von Facebook sowie dessen bestehende Intention einer einheitlichen Optik und Funktionalität von Facebook-Seiten.

*Gemeinsame datenschutzrechtliche Verantwortung:*

In richtlinienkonformer Auslegung von § 3 Abs. 7 BDSG kann ein Selbsterheben, -verarbeiten und -nutzen auch vorliegen, wenn die Erhebung, Verarbeitung oder Nutzung zwar durch eine andere Stelle erfolgt, jedoch diese nicht allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, sondern eine gemeinsame Entscheidung vorliegt (vgl. Art. 2 lit. d RL 95/46/EG).

Die Art-29-Datenschutzgruppe hat sich zur gemeinsamen Verantwortlichkeit eines Webseitenbetreibers geäußert, der den Betreibern sog. Werbenetzwerken seine Webseite zur Verfügung stellt. Für die Datenerhebung durch die Betreiber der Werbenetzwerke wurde für die Webseitenbetreiber, die die Werbung technisch ermöglichen, eine datenschutzrechtliche Mitverantwortung hinsichtlich der Verpflichtungen zur Unterrichtung der Nutzer über die Zwecke und Mittel der Datenverarbeitung bejaht. Beim Like-Button ist die Konstellation vergleichbar. Die Dienstleistungen von Facebook sind zwar kostenlos, der Platz für das Social Plugin wird daher auch nicht „vermietet“, allerdings trifft ein Webseitenbetreiber durch die Einbindung eines Like-Buttons die technischen Voraussetzungen für die Datenerhebung durch Facebook, welches zumindest bei eingeloggten Mitgliedern eine personalisierte Einblendung des Like-Buttons zur Steigerung der Attraktivität des Netzwerks bezweckt. Bei Fanpages ist die Konstellation hingegen nicht vergleichbar. Hier werden die technischen Voraussetzungen für die Datenerhebung durch Facebook selbst geschaffen; lediglich der Inhalt der Fanpage stammt von deren Betreiber. Jedoch lehnt die Art-29-Datenschutzgruppe in einer weiteren Stellungnahme eine (gemeinsame) Verantwortung nur ab, wenn eine Stelle weder rechtlichen noch tatsächlichen Einfluss auf die Entscheidung hat, wie personenbezogene Daten verarbeitet werden. Bei den Fanpages ist zumindest ein tatsächlicher Einfluss vorhanden, weil die Betreiber auf die Errichtung der Fanpage verzichten und dadurch das Ob der Datenerhebung maßgeblich steuern können. Ob dies die Art-29-Datenschutzgruppe in ihrer Einschätzung auch so sieht, ist aber eher fraglich. Sie setzt wohl die Entscheidung über das Ob der

Datenverarbeitung voraus und stellt auf den rechtlichen und tatsächlichen Einfluss auf das Wie der Datenverarbeitung ab. Ein solcher Einfluss des Fanpage-Betreibers ist aber wie oben dargelegt mehr als fraglich. Allerdings lässt sich nicht ausschließen, dass deutsche Gerichte in einem Erst-Recht-Schluss auf die Einflussnahmemöglichkeit hinsichtlich des Ob der Datenverarbeitung abstellen könnten.

#### **(4) Verstoß gegen § 15 Abs. 3 TMG wegen „Facebook Insights“ und/oder Setzen/Übertragen von Cookies?**

Das ULD bejaht im Hinblick auf den beim Like-Button und bei Fanpages angebotenen Dienst „Facebook Insights“ die Anwendbarkeit der Profilbildungsregelung in § 15 Abs. 3 TMG. Zum einen sieht es mangels unstreitig nicht angebotener Widerspruchsmöglichkeit einen Verstoß gegen § 15 Abs. 3 Satz 1 und 2 TMG. Zum anderen bejaht das ULD einen Verstoß gegen § 15 Abs. 3 Satz 3 TMG, d.h. eine unzulässige Zusammenführung der Nutzungsprofile mit den Daten über den Träger des Pseudonyms. Zudem äußert auch der Hamburgische Beauftragte für den Datenschutz aufgrund einer Prüfung den Verdacht, dass durch die Nutzung des datr-Cookies Trackingprofile der Nutzer erstellt würden, die ohne entsprechenden Hinweis auf das hiergegen bestehende Widerspruchsrecht nicht zulässig seien.

#### **Würdigung**

Die Anwendbarkeit von § 15 Abs. 3 TMG in Bezug auf „Facebook Insights“ ist noch nicht abschließend geklärt.

Hinsichtlich des Setzens und Übertragens von Cookies stehen sich die Befunde der irischen Datenschutzaufsicht und des Hamburger Datenschutzbeauftragten gegenüber. Eine Offenlegung des Inhalts des datr-Cookies durch Facebook gegenüber den deutschen Aufsichtsbehörden wäre zu begrüßen.

Insgesamt darf nicht verkannt werden, dass seitens des ULD der Verstoß gegen § 15 Abs. 3 TMG den Hauptvorwurf bildet und insoweit eine erste gerichtliche Klärung in den bereits in Schleswig-Holstein anhängigen Verfahren noch aussteht.

Im Einzelnen:

Ob mit „Facebook Insights“ ein pseudonymisiertes Nutzungsprofil im Sinne von § 15 Abs. 3 Satz 1 TMG verbunden ist, welches auch für die Anwendbarkeit des § 15 Abs. 3 Satz 3 TMG zwingende Voraussetzung ist, ist unklar. Ein Profil ist eine zielgerichtete Verknüpfung von personenbezogenen Daten durch ein logisches zueinander in Beziehung setzen, wodurch zumindest eine Wiedergabe des Teilabblids der Persön-

lichkeit erfolgt. Die im ULD-Arbeitspapier vom 19. August 2011 enthaltenen Auszüge aus „Facebook Insights“ zeigen, dass Einzelstatistiken zu verschiedensten Punkten der Nutzung von Like-Button und Fanpage zur Verfügung gestellt werden und diese jeweils auf die Gesamtheit der Nutzer bezogen sind. Ein Profil als (pseudonymisierte) Wiedergabe des Teilabbilds der Persönlichkeit eines Nutzers ist hiermit wohl nicht verbunden. Dies wäre eher der Fall, wenn z.B. Informationen darüber bereitgestellt würden, wie viele männliche deutsche Nutzer der Altersgruppe XX aus X eine Seite mit Like-Button oder eine Fanpage auf welche Weise bedienen (Beitragsaufrufe, Beitrag „gefällt mir“, Kommentierte Beiträge, Pinnwandeinträge etc.). „Facebook Insights“ ist eher eine Nutzungsstatistik, aber kein Nutzungsprofil.

In Bezug auf beim Like-Button gesetzte und übertragene Cookies hat die irische Datenschutzaufsicht ausgeführt, dass es damit technisch sowohl bei Facebook-Mitgliedern (unabhängig, ob eingeloggt oder nicht) als auch bei Nicht-Facebook-Mitgliedern möglich sei, Profile der Nutzer zu erstellen. Man habe jedoch bei einer technischen Analyse keine Anhaltspunkte für eine solche Nutzung feststellen können. Sollte sich dieser Befund als zutreffend herausstellen, würde zumindest ein Verstoß gegen § 15 Abs. 3 Satz 3 TMG unabhängig von der Frage, ob „Facebook Insights“ überhaupt ein Nutzungsprofil darstellt, ausscheiden, da dann eine Zusammenführung im Sinne dieser Bestimmung ausgeschlossen werden könnte. Der Hamburgische Datenschutzbeauftragte kommt hier zu einem anderen Ergebnis (Pressemitteilung vom 2. November 2011). Die Erörterung des irischen Untersuchungsberichts in Rahmen der Art-29-Datenschutzgruppe wird hier möglicherweise Klarheit bringen. Es sollte jedoch nicht verkannt werden, dass Facebook insbesondere den genauen Inhalt des datr-Cookie bislang zumindest gegenüber den deutschen Aufsichtsbehörden nicht offengelegt hat.

#### **(5) Cookies nur noch mit Einwilligung des Nutzers?**

Hintergrund ist die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, die u.a. die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (E-Privacy-Richtlinie) ändert und die von den Mitgliedstaaten bis zum 25. Mai 2011 umzusetzen war.

Art. 5 Abs. 3 RL 2002/58/EG i.d.F. der RL 2009/136/EG in Verbindung mit Erwägungsgrund 66 der RL 2009/136/EG sieht für die Verwendung von Cookies grundsätzlich das Erfordernis einer Einwilligung des Nutzers vor, es sei denn, dass diese unbedingt erforderlich sind, damit der Anbieter eines Dienstes der Informationsge-

sellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann. Wenn es technisch durchführbar und wirksam ist, kann die Einwilligung des Nutzers über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausgedrückt werden.

Im August 2011 wurde vom Bundesrat der Entwurf eines Gesetzes zur Änderung des TMG eingebracht (BT-Drs. 17/6765). In der Stellungnahme der Bundesregierung äußerte diese, dass derzeit geprüft werde, wie durch eine Regelung im TMG Art. 5 Abs. 3 der (geänderten) E-Privacy-Richtlinie umgesetzt werden könne. Die Bundesregierung werde dem Bundestag hierzu im Zuge der bereits im parlamentarischen Verfahren befindlichen Novellierung des Telekommunikationsgesetzes (TKG) eigene Vorschläge unterbreiten. Die Novellierung des TKG wurde mittlerweile nach Anrufung des Vermittlungsausschusses Anfang Februar 2012 abgeschlossen (BT-Drs. 17/5707, BT-Drs. 17/7521, BT-Drs. 17/8569). Vorschläge der Bundesregierung zur TMG-Änderung wurden in diesem Verfahren nicht vorgelegt. Im ursprünglichen Gesetzentwurf der Bundesregierung zur TKG-Novellierung heißt es, dass Einzelfragen der Umsetzung der Änderung von Art. 5 Abs. 3 E-Privacy-Richtlinie derzeit Gegenstand umfangreicher Konsultationen auf europäischer Ebene seien, die auch Selbstregulierungsansätze umfassten. Das Ergebnis dieses Prozesses werde vor einer Entscheidung über weitergehenden gesetzgeberischen Handlungsbedarf abgewartet. Bei der Beratung des Gesetzentwurfs zur TKG-Änderung im federführenden Ausschuss für Wirtschaft und Technologie wurden seitens der Fraktionen SPD und Bündnis 90/DIE GRÜNEN ein Entschließungsantrag zur Umsetzung der Änderungen der E-Privacy-Richtlinie gestellt und festgestellt, dass die von der Bundesregierung angekündigten Vorschläge zur Umsetzung von Art. 5 Abs. 3 E-Privacy-Richtlinie nicht vorlägen (Ausschussdrucksache 17(9)684). Der Antrag fand im Ausschuss keine Mehrheit. Ein aktueller Gesetzentwurf der Fraktion der SPD vom Januar 2012 zur Änderung des TMG mit dem Ziel der Umsetzung des Art. 5 Abs. 3 der E-Privacy-Richtlinie (BT-Drs. 17/8454) wurde Ende Januar 2012 eingebracht. Nach Empfehlung des Wirtschaftsausschusses vom 1. März 2012 wird Ablehnung vorgeschlagen (BT-Drs. 17/8814).

Vor diesem Hintergrund ist zumindest für die nachfolgende Beurteilung der Rechtsfragen Folgendes festzuhalten:

1. Eine unmittelbare Wirkung der Richtlinie 2009/136/EG kann nach Ablauf der Umsetzungsfrist weder sicher angenommen noch ausgeschlossen werden. Nach der ständigen Rechtsprechung des EuGH kann sich zwar der Einzelne in Fällen, in de-

nen die Bestimmungen einer Richtlinie inhaltlich unbedingt und hinreichend genau sind, vor den nationalen Gerichten gegenüber dem Mitgliedstaat auf diese Bestimmungen berufen, wenn der Mitgliedstaat die Richtlinie nicht fristgemäß oder unzulänglich in nationales Recht umgesetzt hat. Eine unmittelbare Wirkung einer Richtlinie wurde bislang jedoch ausgeschlossen, wenn sie nicht nur eine Begünstigung des Bürgers bedeutet, sondern auch zu einer Verpflichtung oder Belastung einer nicht-staatlichen Stelle führen würde. Der Grundsatz der Rechtssicherheit, so bislang der EuGH, steht der Begründung von Verpflichtungen für den Einzelnen durch Richtlinien entgegen, sodass gegenüber dem Einzelnen die Bestimmungen einer Richtlinie nur Rechte begründen können. Die Rechtsprechung des EuGH geht bislang davon aus, dass der Einzelne sich nicht gegenüber einem Mitgliedstaat auf eine Richtlinie berufen kann, wenn mit der Erfüllung dieser Richtlinie eine unmittelbare Inpflichtnahme eines Dritten verbunden ist (EuGH, Urteil vom 07.01.2004, Rs. C-201/02 – Wells – Rn. 56 m.w.N.). Bei einer direkten Anwendung von Art. 5 Abs. 3 RL 2002/58/EG in der Fassung der RL 2009/136/EG käme es aber gerade zu einer solchen unmittelbaren Inpflichtnahme.

Die Richtlinien, deren unmittelbare Horizontalwirkung der EuGH bislang mit Verweis auf den Grundsatz der Rechtssicherheit abgelehnt hatte (s.o.), datieren jedoch – soweit ersichtlich – aus der Zeit vor Inkrafttreten des Vertrags von Maastricht, als eine Veröffentlichung von Richtlinien im Amtsblatt der EU nicht vorgesehen war. Es ist nicht auszuschließen, dass nunmehr, nachdem auch für Richtlinien die Veröffentlichung im Amtsblatt zwingend vorgeschrieben (Art. 297 Abs. 1 AEUV) und damit Publizität hergestellt ist, der EuGH eine unmittelbare Horizontalwirkung von Richtlinien bejaht, soweit auch die übrigen Voraussetzungen für eine unmittelbare Geltung erfüllt sind.

**2.** Die (geänderte) E-Privacy-Richtlinie ist wohl dahingehend auszulegen, dass eine Einwilligung zum Setzen von Cookies nicht erforderlich ist, wenn dies nicht die Erhebung personenbezogener Daten bezweckt, d.h. Cookies keine personenbezogenen Daten enthalten. Dies ergibt sich aus deren Anwendungsbereich, der die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation umfasst.

**3.** Eine Einwilligung ist zumindest dann nicht erforderlich, wenn ein Cookie unverzichtbar ist, um die Nutzung eines vom Nutzer ausdrücklich angeforderten Dienstes zu ermöglichen.

## **(6) Zulässigkeit der Übertragung und Speicherung der generischen IP-Adresse?**

Die Übertragung und Speicherung der generischen IP-Adresse ist nach gegenwärtigem Sachstand nach § 15 Abs. 1 Satz 1 TMG zulässig. Sehr zweifelhaft ist jedoch, ob diesbezüglich auch die Unterrichtungspflicht nach § 13 Abs. 1 Satz 1 TMG insbesondere gegenüber Nicht-Facebook-Mitgliedern ausreichend erfüllt wird.

Im Einzelnen:

Rechtsgrundlage für die nicht-anonymisierte Übertragung der IP-Adresse des Nutzers an Facebook ist § 15 Abs. 1 TMG. Danach darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Wie oben dargelegt kann – obwohl gerichtlich nicht abschließend geklärt – die Einordnung der IP-Adresse als generell personenbezogenes Datum nicht ausgeschlossen werden. Aus technischer Sicht ist die Übertragung der IP-Adresse erforderlich. Nur durch die Übertragung kann Facebook den Like-Button und die Fanpage mit Inhalt darstellen. Dass einem Nicht-Facebook-Mitglied die (Facebook-)Funktion durch den Besuch der Webseite mit Like-Button oder der Fanpage letztlich „aufgedrängt“ wird, ändert an der Erforderlichkeit nichts. Ein Vertragsverhältnis zwischen Telemedienanbieter und Nutzer muss bei § 15 Abs. 1 Satz 1 TMG – im Gegensatz zu § 14 TMG – nicht vorliegen. Durch die über das Ende des Nutzungsvorgangs hinausgehende Speicherung als generische IP-Adresse liegt auch kein Verstoß gegen § 15 Abs. 4 Satz 1 TMG vor, weil durch die Anonymisierung keine Nutzungsdaten gemäß § 15 Abs. 1 Satz 1 TMG mehr vorliegen. Nur diese wären nach Ende des Nutzungsvorgangs zu löschen. Hier darf jedoch nicht verkannt werden, dass die Anonymisierung von Facebook vorgetragen wird und noch nicht abschließend verifiziert ist.

Auch bei einer Datenerhebung nach § 15 Abs. 1 Satz 1 TMG hat der Diensteanbieter die Unterrichtungspflicht nach § 13 Abs. 1 Satz 1 TMG zu erfüllen. Unabhängig von der Frage des anwendbaren Rechts auf Facebook trifft diese Pflicht mitverantwortlich auch den Webseitenbetreiber, der den Like-Button einbettet, und – auch wenn man dies eher in Frage stellen kann – den Betreiber der Fanpage. Gerade ein Nicht-Facebook-Mitglied wird jedoch beim Besuch einer Webseite mit Like-Button oder einer Fanpage mangels Kenntnis der Datenschutzerklärung und den Nutzungsbedingungen von Facebook jedenfalls keine Kenntnis über die Übertragung der IP-Adresse an Facebook erlangen.

### **(7) Zulässigkeit der Speicherung der spezifischen IP-Adresse?**

Die Speicherung der spezifischen IP-Adresse bedarf wohl einer informierten Einwilligung und kann nicht auf § 14 oder § 15 TMG gestützt werden. Die Zustimmung zu den Datenverwendungsrichtlinien von Facebook kann als Einwilligung gelten, wobei allerdings die Wahrung der auch diesbezüglich geltenden Unterrichtungspflichten nach § 13 Abs. 1 Satz 1 TMG unterschiedlich beurteilt werden kann.

Im Einzelnen:

Für die Speicherung der spezifischen IP-Adresse bei zunächst nicht-eingeloggten Facebook-Mitgliedern, die einen Like-Button bestätigen (und sich dadurch i.d.R. einloggen werden), sowie bei eingeloggten Facebook-Mitgliedern, die eine Webseite mit Like-Button besuchen, ist wohl eine (informierte) Einwilligung des Facebook-Mitglieds erforderlich. § 14 Abs. 1 TMG, wonach der Diensteanbieter personenbezogene Daten eines Nutzers erheben und verwenden darf, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten), scheidet als Rechtsgrundlage aus. Die Erforderlichkeit der Erhebung und Verwendung von Bestandsdaten wird von der herrschenden Auffassung eng ausgelegt und nur bejaht, wenn sie für die Gestaltung des Telemediendienstevertrags unerlässlich ist. Für die Inanspruchnahme der Funktionalität Like-Button ist die Speicherung der spezifischen IP-Adresse jedoch nicht unerlässlich, da diese auch ohne sie technisch umsetzbar ist. Auch § 15 Abs. 1 TMG kommt für die Speicherung nicht in Betracht, da die spezifische IP-Adresse als Nutzungsdatum nach Ende des Nutzungsvorgangs zu löschen ist (§ 15 Abs. 4 Satz 1 TMG); aufgrund der Unentgeltlichkeit von Facebook ist die Speicherung gerade nicht für Zwecke der Abrechnung mit dem Nutzer erforderlich.

Maßgeblich für die hiernach erforderliche Einwilligung sind die „Datenverwendungsrichtlinien“ von Facebook, denen bei Registrierung zugestimmt werden muss. Diese enthalten verschiedene Themenrubriken mit anklickbaren und z.T. untereinander verlinkten Untermenüs. Unter den Rubriken „*Daten, die wir über dich erhalten*“, „*Wie wir uns bereitgestellte Daten verwenden*“ und „*Teilen von Inhalten mit anderen Webseiten und Anwendungen – Über soziale Plug-ins*“ werden Informationen u.a. über die Speicherung der mit den sozialen Plug-ins gesammelten Daten (hierzu gehören auch die IP-Adressen) bereitgehalten. Über den Verwendungszweck werden pauschale Aussagen getroffen, die v.a. auf die Ermöglichung eines sozialeren und persönlichen Nutzungserlebnisses abstellen. Ob dies den auch für die Einwilligung geltenden An-

forderungen an die Transparenz einer Unterrichtung nach § 13 Abs. 1 Satz 1 TMG genügt, wird unterschiedlich beurteilt. Allerdings sollten an eine Unterrichtung in allgemein verständlicher Form auch keine zu hohen Anforderungen gestellt werden: gerade eine zu große Detailliertheit wäre für die allgemeine Verständlichkeit eher abträglich.

#### **(8) Zulässigkeit des Setzens/der Übertragung des datr-Cookie?**

Die Einordnung des datr-Cookie als personenbezogenes Datum kann nach gegenwärtigem Sachstand nicht ausgeschlossen werden. Bejaht man den Personenbezug, ist die Übertragung eines gesetzten datr-Cookies beim Like-Button ohne Einwilligung unzulässig, wenn Nutzer (Facebook-Mitglieder und Nicht-Mitglieder) in der Folge beim Besuch von Webseiten mit Like-Button diesen nicht klicken.

Ansonsten ist das Setzen und Übertragen des datr-Cookies nach § 15 Abs. 1 TMG zulässig, sofern sich die Befunde der irischen Datenschutzaufsicht zur ausschließlichen Sicherheitsrelevanz des datr-Cookies als zutreffend erweisen. Der Hamburger Datenschutzbeauftragte ist hier anderer Auffassung. Eine Offenlegung des Inhalts des datr-Cookies durch Facebook gegenüber den deutschen Datenschutzaufsichtsbehörden wäre zu begrüßen.

Im Einzelnen:

Wie oben darlegt kann die Einordnung des datr-Cookie als personenbezogenes Datum nach gegenwärtigem Sachstand nicht ausgeschlossen werden.

Für den Fall, dass weitere Untersuchungen einen Personenbezug des datr-Cookie bestätigen sollten, gilt neben den unter (4) dargelegten Fragen zur Nichtanwendbarkeit der Profilbildungsregelung in § 15 Abs. 3 TMG Folgendes:

- Bei Nicht-Facebook-Mitgliedern, die mehrmals Like-Buttons klicken oder Fanpages besuchen, sowie bei Facebook-Mitgliedern, die sich anlässlich der Bestätigung des Like-Buttons oder der Bedienung einer Fanpage einloggen, bzw. im eingeloggten Zustand Webseiten mit Like-Button oder Fanpages besuchen, mag das Setzen und die spätere Übertragung des datr-Cookies nach § 15 Abs. 1 Satz 1 TMG zulässig sein. Mit dem Klicken des Like-Buttons bzw. dem Besuch der Fanpage wird die Facebook-Plattform geöffnet mit der Möglichkeit, sich zu registrieren und einzuloggen, und damit auch mit der Möglichkeit, sich mit der Identität eines Facebook-Mitglieds missbräuchlich einzuloggen. Mit dem Übertragen des datr-Cookies will Facebook solche Versuche verhindern, um dadurch seine re-

gistrierten Nutzer zu schützen. Insoweit ließe sich von einer Erforderlichkeit zur Ermöglichung der Inanspruchnahme von Facebook sprechen, da hierzu auch die Nutzung unter Ausschluss von Missbrauch gehört.

- Vor diesem Hintergrund ist dann aber beim Like-Button nicht ersichtlich, dass eine Übertragung des beim ersten Klicken eines Like-Buttons sowohl bei Facebook-Mitgliedern als auch bei Nicht-Facebook-Mitgliedern gesetzten datr-Cookies auch erforderlich ist, wenn bei späteren Besuchen von Webseiten mit Like-Buttons diese nicht geklickt werden. Hier erfolgt nämlich jeweils kein Anmeldeversuch bei Facebook, der die Gefahr einer missbräuchlichen Nutzung herbeiführen würde. § 15 Abs. 1 Satz 1 TMG kann daher nicht als Rechtsgrundlage herangezogen werden. Vielmehr bedarf es – unabhängig von den Vorgaben der E-Privacy-Richtlinie – einer Einwilligung des Nutzers.

### **(9) Zulässigkeit der Übertragung des c\_User-Cookie?**

Die Übertragung des c\_User-Cookie kann auf § 15 Abs. 1 Satz 1 TMG gestützt werden. Es gilt die spezielle Unterrichtungspflicht nach § 13 Abs. 1 Satz 2 TMG. Hier besteht unter dem Gesichtspunkt der Transparenz Verbesserungsbedarf.

Im Einzelnen:

Die Übertragung des c\_user-Cookies bei eingeloggten Facebook-Mitgliedern (beim Like-Button als auch bei Fanpages) kann auf § 15 Abs. 1 Satz 1 TMG gestützt werden, da sie gerade erforderlich ist, um für Facebook-Mitglieder die personalisierte Nutzung des Like-Button/der Fanpage zu ermöglichen. Unabhängig von der – abzulehnenden – horizontalen Drittwirkung der E-Privacy-Richtlinie ist das Setzen/Übertragen des c-user-Cookie weiter auf der Grundlage von § 15 Abs. 1 Satz 1 TMG möglich und nicht erst aufgrund einer Einwilligung zulässig. Damit Facebook die von seinen Nutzern ausdrücklich gewünschte personalisierte Darstellung einer Fanpage zur Verfügung stellen kann, ist der c\_user-Cookie unverzichtbar, sodass auch nach der Richtlinie eine Ausnahme vom Einwilligungserfordernis greift.

Für den c\_user-Cookie ist die spezielle Unterrichtungspflicht nach § 13 Abs. 1 Satz 2 TMG einschlägig. Der c\_user-Cookie ermöglicht nämlich eine spätere Identifizierung des Facebook-Mitglieds und dient daher auch der Vorbereitung der Erhebung/Verwendung personenbezogener Daten. Insoweit kommt es darauf an, ob Facebook seine Mitglieder zu Beginn des Verfahrens über solche personalisierten Inhalte mit Hilfe der Nutzung von Cookies unterrichtet oder dies bei der Registrierung bereits in allgemeiner Form getan hat. Solche Hinweise gibt Facebook tatsächlich; diese

sind aber unter dem Gesichtspunkt der Transparenz verbesserungswürdig. In den „Datenverwendungsrichtlinien“ erhält der Nutzer diese Hinweise nur versteckt unter der Rubrik „*Was du sonst noch wissen solltest*“, Unterrubrik „*Cookies*“ mit einem Link auf „*Hilfereich*“ unter der Rubrik „*Etwas funktioniert nicht - Cookies*“ (dort allerdings in gut verständlicher Form).

## **V. Ausblick – weitere Entwicklung**

Neben Social Plugins und Fanpages sind weitere technische Entwicklungen und Änderungen der Geschäftspraktiken der Sozialen Netzwerke Gegenstand intensiver datenschutzrechtlicher Diskussionen. So untersucht die Art-29-Datenschutzgruppe mit dem Ziel eines abgestimmten Vorgehens der europäischen Datenschutzaufsichtsbehörden die Änderungen der Nutzungsbedingungen bei Google, die für die Nutzer eine Zusammenführung der über sie bei den einzelnen Google-Diensten – darunter auch das Soziale Netzwerk Google+ – gespeicherten Daten ohne Widerspruchsmöglichkeit vorsehen. Bei Facebook ist zu erwarten, dass die jetzt eingefügte Funktion einer umfassenden digitalen Nutzerbiographie („Timeline“) noch eingehender datenschutzrechtlicher Untersuchung unterzogen wird. Das gleiche gilt für die von Facebook beabsichtigte, von vielen Nutzern abgelehnte und von Datenschützern kritisierte Änderung der Nutzungsbedingungen („Datenverwendungsrichtlinien“).

Die Ergebnisse dieser laufenden Untersuchungen der zuständigen unabhängigen Datenschutzaufsichtsbehörden sind derzeit weder auf nationaler noch auf europäischer Ebene absehbar. So steht die endgültige Entscheidung der irischen Datenschutzaufsicht über die konkret zu einzelnen Funktionen von Facebook erhobenen Beschwerden noch aus. Der Untersuchungsbericht zeigt aber bereits auf, dass in vielen Bereichen Verbesserungen bei der Transparenz der Datenerhebung angemahnt werden, hinsichtlich derer Facebook erste Zusagen gemacht hat. Ebenfalls noch nicht abgeschlossen sind die vom Bundesminister des Innern im November 2011 initiierten, unter Federführung der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (FSM) geführten Verhandlungen über eine Selbstverpflichtung der Betreiber Sozialer Netzwerke.

Vor diesem Hintergrund beschränken sich die nachfolgenden gemeinsamen Vorschläge des AK I auf die in der Berichtsbitte der CdS-Jahreskonferenz in den Mittelpunkt gestellte Nutzung von Social Plugins und Fanpages.

## **VI. Gemeinsame Vorschläge des AK I**

Die unter Ziffer IV.3. dargestellte Würdigung der einzelnen Sach- und Rechtsfragen zeigt, dass die datenschutzkonforme Ausgestaltung der Nutzung von Social Plugins wie dem Like-Button sowie von Fanpages sowohl in tatsächlicher Hinsicht –weitere Auskünfte von Facebook insbesondere zu Nutzung und Verwendungszweck von Cookies – als auch in rechtlicher Hinsicht – insbesondere bezüglich der Unterrichtungspflichten nach dem TMG und Erfordernis von Einwilligungen in bestimmten Fallkonstellationen – noch nicht abschließend geklärt ist. Die Würdigung bestimmter Rechtsfragen hängt dabei von der Klärung tatsächlicher Fragen ab. Der Untersuchungsbericht der irischen Datenschutzaufsichtsbehörde gibt für diese Klärung Anhaltspunkte, kann aber nicht als abschließende Klärung auch im Verhältnis zu den deutschen Aufsichtsbehörden und in den bereits anhängigen gerichtlichen Verfahren gelten.

Aufgrund dieses Sach- und Rechtsstands ergeben sich gegenwärtig folgende Vorschläge und Empfehlungen betreffend die Nutzung von Social Plugins und Fanpages durch öffentliche Stellen:

1. Öffentliche Stellen trifft bei der Öffentlichkeitsarbeit mittels Sozialer Netzwerke die Pflicht, hierbei sorgfältig auf ein hohes Datenschutzniveau zu achten. Bei Social Plugins wie dem Like-Button kann diese datenschutzrechtliche Mitverantwortung neben den Betreibern der Sozialen Netzwerke bereits aus den einfachgesetzlichen Bestimmungen des Telemediengesetzes und des Bundesdatenschutzgesetzes abgeleitet werden. Bei Fanpages sollte eine solche Mitverantwortung zumindest aufgrund einer „Vorbildfunktion“ des Staates bejaht werden, der das Recht auf informationelle Selbstbestimmung seiner Bürgerinnen und Bürger schützen sollte.
2. Diese datenschutzrechtliche Mitverantwortung legt nahe, Gefährdungen der informationellen Selbstbestimmung durch neue Technologien und Vorteile bei der sachgerechten Erfüllung öffentlicher Aufgaben wie der Wahrnehmung des Informationsauftrags öffentlicher Stellen sorgsam gegeneinander abzuwägen. Es sollte dabei nicht verkannt werden, dass für den Betreiber des Sozialen Netzwerks, der notwendigerweise in die Öffentlichkeitsarbeit der öffentlichen Stelle eingebunden ist, personenbezogene Daten und deren Nutzung für Werbezwecke die Währung sind, mit der Bürgerinnen und Bürger für die „unentgeltliche“ Bereitstellung von Sozialen Netzwerken tatsächlich bezahlen. Dies gilt umso mehr, als bei Social Plugins und Fanpages auch

Bürgerinnen und Bürger betroffen sind, die die Nutzung Sozialer Netzwerke für sich bislang nicht in Betracht ziehen.

3. Zur Minimierung der Gefährdungen für die informationelle Selbstbestimmung bei der Nutzung von Social Plugins und Fanpages trifft die Betreiber der Sozialen Netzwerke die Hauptverantwortung. Zur Wahrung dieser Verantwortung wäre ein mit den Datenschutzaufsichtsbehörden abzustimmendes Maßnahmenkonzept begrüßenswert. Für die Erarbeitung und Vorlage eines solchen Maßnahmenkonzepts bieten die gegenwärtig laufenden, vom Bundesminister des Innern im November 2011 initiierten Beratungen zu einem allgemeinen Datenschutzkodex für Soziale Netzwerke Gelegenheit. Diese Beratungen unter Federführung der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (FSM) sollten ausdrücklich um die Gesichtspunkte Social Plugins und Fanpages erweitert werden. Die Einbeziehung der Datenschutzaufsichtsbehörden in diesen Beratungsprozess ist hierbei von großer Wichtigkeit.

Ein Maßnahmenkonzept sollte insbesondere folgende Defizite aufgreifen und Lösungsmöglichkeiten aufzeigen:

- Technische Abläufe bei Social Plugins und Fanpages sind gegenüber den deutschen Aufsichtsbehörden umfassend offenzulegen (insbesondere Nutzungszweck von Cookies).
- Die Erstellung von Nutzerprofilen durch den Besuch von Webseiten mit Like-Button und von Fanpages ist insbesondere im Hinblick auf Nichtnutzer von Sozialen Netzwerken auszuschließen. Die Nachprüfbarkeit durch die Datenschutzaufsicht sollte hierbei sichergestellt sein.
- Im Interesse einer umfassenden Gewährleistung der informationellen Selbstbestimmung sollte bei jeder Art von Statistikverfahren betreffend die Reichweite der Nutzung einer Webseite ein Widerspruchsrecht nach § 15 Abs. 3 TMG bestehen, unabhängig davon, ob das Verfahren im Einzelnen als pseudonymisiertes Nutzungsprofil im Sinne dieser Vorschrift zu qualifizieren ist.
- Bei der Entscheidung über Art und Weise der Verwendung von Cookies sollten die Anforderungen der überarbeiteten E-Privacy-Richtlinie nicht unbeachtet bleiben.
- Die Verwendung personenbezogener Daten im Rahmen von Mechanismen zum Ausschluss missbräuchlicher Nutzung Sozialer Netzwerke sollte sich strikt an dem Grundsatz der Erforderlichkeit orientieren. Dies gilt insbesondere für die Bemessung von Speicherfristen.
- Die Unterrichtungspflichten nach dem Telemediengesetz (§ 13 Abs. 1 TMG) sind umfassend zur Geltung zu bringen. Social Plugins und Fanpages sind so auszu-

gestalten, dass insbesondere Nichtnutzer Sozialer Netzwerke idealerweise vor dem Datenfluss über die Erhebung und Verwendung personenbezogener Daten informiert werden.

- Im Interesse der umfassenden Gewährleistung der informationellen Selbstbestimmung sollten die Betreiber Sozialer Netzwerke bei Social Plugins aktiv oder zumindest wohlwollend unterstützend an technischen Lösungen mitwirken, bei denen personenbezogene Daten der Nutzer erst an den Betreiber übertragen werden, wenn die entsprechende Schaltfläche durch den Nutzer nach einer Information über die dann fließenden Daten und deren Verwendung freigegeben wird. Mit einer solchen Funktion werden Einwilligungslösungen ermöglicht, die neben der praktischen Handhabbarkeit der Unterrichtungspflichten auch Anforderungen aus der E-Privacy-Richtlinie und an Statistikverfahren berücksichtigen können. Bei Fanpages sollten die Betreiber Sozialer Netzwerke adäquate Lösungen entwickeln.
4. Betreiber von Webseiten mit Social Plugins können durch die (durch ein IT-Informationsportal entwickelte) Zwei-Klick-Lösung das soeben dargelegte Maßnahmenkonzept auch ohne den Betreiber des Sozialen Netzwerks in gewissem Maße bereits jetzt grundsätzlich erfüllen und dadurch Gefährdungen für die informationelle Selbstbestimmung der Nutzer minimieren. Aufgrund des bestehenden Aufklärungsbedarfs tatsächlicher Art hinsichtlich der technischen Abläufe ist insbesondere die umfassende Information der Nutzer jedoch mit Unwägbarkeiten behaftet. Bei Fanpages könnten ergänzende Nutzerinformationen über die Datenverarbeitungsprozesse, die zunächst bei Aufruf der Fanpage eingeblendet werden, einen ersten Ansatz für eine Risikominimierung darstellen. Der sofortige Datenfluss beim bloßen Besuch der Fanpage kann hier jedoch ohne Mitwirkung von Facebook nicht unterbunden werden.
  5. Die Debatte über den Einsatz von Social Plugins und Fanpages zeigt wiederum, dass insbesondere die Umsetzung folgender rechtspolitischer Forderungen dringend geboten ist:
    - völkerrechtliche Vereinbarungen zur datenschutzrechtlichen Verantwortlichkeit, die auch für nichtöffentliche Stellen, die ihren Sitz außerhalb der EU haben, verbindlich sind und deren Einhaltung von den deutschen Datenschutzaufsichtsbehörden wirksam überprüft werden können
    - Regelungen zur Verbesserung der Transparenz bei der Datenverarbeitung durch erweiterte Informations- und Auskunftspflichten der verantwortlichen Stellen

- Regelungen, die der Bildung von Persönlichkeitsprofilen (z. B. Konsumentenprofile, Bewegungsprofile, Nutzerprofile im Internet) möglichst enge Grenzen setzen
- Regelungen für soziale Netzwerke zum Schutz des Persönlichkeitsrechts der Nutzer (z. B. Verpflichtung der verantwortlichen Stelle zu datenschutzfreundlichen Voreinstellungen, zu besonderem Schutz für minderjährige Nutzer, Lösungsanspruch bei Ausscheiden aus dem Netzwerk)

Die Reform des Europäischen Datenschutzrechts und die parallel dazu auch in den Vereinigten Staaten von Amerika angelaufene Debatte über einen neuen Rechtsrahmen für den Datenschutz in der Informationsgesellschaft eröffnen die Chance, diese Forderungen in umfassend verbindlicher und zeitgemäßer Gewährleistung der informationellen Selbstbestimmung umzusetzen.