Schleswig-Holsteinischer Landtag
Umdruck 17/2988

**Der Präsident des
Schleswig-Holsteinischen Landtages**

Wissenschaftlicher Dienst

Schleswig-Holsteinischer Landtag ▪ Postfach 7121 ▪ 24171 Kiel

An die
Parlamentarische Geschäftsführerin
der FDP-Fraktion
Frau Katharina Loedige, MdL

– im Hause –

Ihre Nachricht vom: 26.08.2011

Mein Zeichen: L 203 – 140/17

**Bearbeiter/in:
Dr. Anika D. Luch**

**Telefon (0431) 988-1133
Telefax (0431) 988-1250
anika.luch@landtag.ltsh.de**

24. Oktober 2011

„Facebook-Kampagne“ des ULD

Sehr geehrte Frau Loedige,

Ihrer Bitte um Stellungnahme, ob der Wissenschaftliche Dienst die Rechtsauffassung des ULD zur „datenschutzrechtlichen Bewertung der Reichweitenanalyse durch Facebook“ teilt, kommen wir im Folgenden gerne nach. Dabei konzentrieren sich die Ausführungen auf die für die Erfolgsaussichten von etwaigen Bußgeldverfahren maßgeblichen Fragen der Betroffenheit von personenbezogenen Daten, der datenschutzrechtlichen Verantwortlichkeit und der Frage der formellen Zuständigkeit des ULD zur Verfolgung etwaiger Ordnungswidrigkeiten bzw. Beanstandungen.

Frage 1: Ist die Rechtsauffassung des ULD korrekt, liegen – vorausgesetzt die technische Bewertung ist nicht zu beanstanden – Verstöße gegen datenschutzrechtliche Bestimmungen vor?

I. Kurzskizzierung der Ausgangslage

Im Folgenden ist stets zwischen unterschiedlichen Konstellationen zu differenzieren. Einerseits geht es zunächst um **Fanpages**, die innerhalb des Sozialen Netzwerks Facebook von angemeldeten Facebook-Nutzern angelegt werden können, um Personen der Zeitgeschichte, Unternehmen oder staatliche Stellen vorzustellen, deren Informationen zu verbreiten, „Fans“ zu sammeln und mit diesen in Diskussionen oder über Pinnwandkommentare zu kommunizieren. Andererseits stehen gewöhnliche **Websei-**

ten in Rede, auf denen unter anderem Social-Plugins von Facebook integriert werden. Sobald dieser „Gefällt mir"-Button angeklickt wird, leuchtet bei Facebook-Nutzern, die sich gleichzeitig im Netzwerk anmelden oder bereits angemeldet sind, ein Link auf deren Profilseite innerhalb von Facebook auf, der auf die Webseite mit dem Button verweist. Über das Tool „**Facebook Insight**" erfolgt durch das soziale Netzwerk eine Analyse der Reichweite der jeweiligen Seiten (Anzahl der Klicks, Geschlecht und Altersgruppen der Seitenbesucher, Feedbackstatistik zu Beiträgen), die Facebook zur unternehmensinternen Verbesserung des Angebots verwendet und in anonymisierter Form den Seitenbetreibern unaufgefordert zur Verfügung stellt.

Neben dieser Differenzierung zwischen facebookinternen Fanpages und Webseiten mit integrierten Social-Plugins ist ferner danach zu unterscheiden, ob solche Fanpages oder Webseiten von **Facebook-Nutzern**, die mit Facebook einen Nutzervertrag geschlossen haben und damit auch deren Datenschutzbestimmungen grds. akzeptieren, oder von **Nichtnutzern**, die keinerlei vertragliche Bindungen zu Facebook unterhalten, aufgerufen werden.

Ungeklärt ist bislang, bei welchen Interaktionen im Netz bezogen auf die beschriebenen Fanpages oder Webseiten welche Daten erhoben und gespeichert werden und inwiefern sich dabei Unterschiede im Hinblick auf Facebook-Nutzer und Nichtnutzer ergeben. Das ULD geht jedenfalls davon aus, dass bei beiden Personengruppen bei Aufruf einer Fanpage ebenso wie beim Aufruf einer Webseite mit integriertem Social-Plugin IP-Adressen erhoben und gespeichert werden sowie – nach einmaliger Interaktion mit Facebook (Betätigung des „Gefällt mir"-Buttons oder Einloggen ins Netzwerk) – Cookies zum Einsatz kommen[1] (zu deren Einordnung siehe unten).

II. Personenbezogene Daten

Für die Eröffnung des Anwendungsbereichs des Datenschutzrechts ist eine maßgebliche Vorfrage, ob überhaupt personenbezogene Daten, deren Schutz das Datenschutzrecht vornehmlich zu dienen bestimmt ist, betroffen sind.

[1] Siehe dazu ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 7 f.

Im Kontext der vom ULD in seinem Arbeitspapier zur Reichweitenanalyse durch Facebook „beanstandeten“[2] Datenverarbeitungsprozesse wird ausschließlich auf die Erhebung von IP-Adressen und das Setzen von Cookies abgestellt. Fraglich ist daher, ob es sich bei diesen Informationen um personenbezogene Daten handelt.

1. IP-Adressen

Zu prüfen ist daher zunächst, ob die Einschätzung des ULD, dass es sich bei der im Rahmen des Dienstes „Facebook Insight“ erhobenen IP-Adresse des Nutzers, der eine Fanpage oder Webseite mit Social-Plugin besucht, um ein solches personenbezogenes Datum im Sinne des § 3 Abs. 1 BDSG bzw. § 2 Abs. 1 LDSG[3] handelt, zutrifft. In der rechtlichen Bewertung des ULD heißt es dazu – ohne Aufführung von Nachweisen – lediglich:

> *„Durch den Dienst ‚Facebook Insight’, der bei Fanpages und den Social-Plugins zum Einsatz kommt, werden personenbezogene Daten erhoben und verarbeitet. (…) Dazu gehört die IP-Adresse, die nach einhelliger Auffassung der europäischen und deutschen Aufsichtsbehörden Personenbezug besitzt.“*[4]

Die Legaldefinition des § 3 Abs. 1 BDSG besagt, dass personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) sind.

Im Einzelnen ist es höchst umstritten, ob es sich bei der IP-Adresse um ein personenbezogenes Datum handelt, das den Anwendungsbereich des BDSG eröffnet. Der Diskussionsstand befindet sich insoweit auch weiterhin im Fluss. Dabei steht das Merkmal der „Bestimmbarkeit“ im Vordergrund. Vielfach wird für eine „relative“ Betrachtungsweise plädiert.[5] Ein und dasselbe Datum kann nach dieser Auffassung bei der

---

[2] Nicht im Rechtssinne von § 42 LDSG.

[3] Zu den Anwendungsbereichen: Das BDSG ist gem. § 1 Abs. 1 BDSG grundsätzlich auf öffentliche Stellen des Bundes (§ 1 Abs. 1 Nr. 1 BDSG), öffentliche Stellen der Länder (§ 1 Abs. 1 Nr. 2 BDSG) und nichtöffentliche Stellen (§ 1 Abs. 1 Nr. 3 BDSG) anwendbar. Für öffentliche Stellen der Länder ist es jedoch nur dann anwendbar, wenn der Datenschutz nicht durch Landesgesetz geregelt ist. In Schleswig-Holstein wurde dafür das Landesdatenschutzgesetz (LDSG SH) geschaffen. Dieses ist gem. § 3 Abs. 1 S. 2 LDSG SH auf öffentliche Stellen anzuwenden und genießt somit Anwendungsvorrang vor dem BDSG.

[4] ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 15.

[5] *Gola*/*Schomerus*, BDSG, 10. Aufl. 2010, § 3 Rn. 10; *Eckhardt*, CR 2011, 339; *Abel*, DSB 2011, 14 f.; ders., Recht und Politik 4/2011, 14 ff.; *Krüger*/*Maucher*, MMR 2011, 433 ff. unter Verweis auf *Ambs*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 179. Erg.lfrg. 2010, § 3 BDSG Rn. 3; *Eckhardt*, K&R

einen verantwortlichen Stelle (vgl. § 3 Abs. 7 BDSG) aufgrund ihrer Nachforschungsmöglichkeiten ein personenbezogenes Datum sein und bei einer anderen Stelle nicht.[6] Die Gegenauffassung lehnt – meist unter pauschalem Hinweis auf den Grundrechtsschutz der Betroffenen – jegliche Relativierung ab und lässt es ausreichen, dass (theoretisch-abstrakt) Möglichkeiten denkbar sind, die das Datum mit einer natürlichen Person in Verbindung bringen.[7]

Bei der Diskussion um die Personenbezogenheit der IP-Adressen kann insbesondere zwischen statischen und dynamischen Adressen unterschieden werden. Eine feste **(statische) IP-Adresse**, mit der sich jeder Rechner bei der Kommunikation im Internet identifiziert, bestimmt in der Regel dessen Inhaber, begründet mithin Personenbezug, falls dies eine natürliche Person ist. Während statische IP-Adressen bisher im Wesentlichen dem professionellen Bereich vorbehalten waren, ist unter dem neuen Internet-Protokoll IPv6 wohl eine generelle Verwendung absehbar. Der Anschlussinhaber lässt sich über eine Onlinedatenbank wie „www.ripe.net“ oder „who-is“ ermitteln. Die bisher weit überwiegend verwendeten, vom Service-Provider pro Wählverbindung vergebenen **dynamischen IP-Nummern**, sind wohl jedenfalls für diesen personenbezogen, da er anhand der von ihm in der Regel geführten Bestands- und Verbindungsdaten die Zuordnung zum Inhaber des Rechners vornehmen kann. Für die in den Logfiles der Anbieter von Telemediendiensten, so von Webseitenbetreibern oder Suchmaschinen, enthaltenen mit IP-Adressen verknüpften Daten über die Internet-Nutzung ist der Personenbezug nach der strengeren Auffassung ebenfalls zu bejahen. Das gelte auch, wenn zur Zuordnung weitere Angaben seitens des Betreibers einer Firewall o.Ä. herangezogen werden müssen (Auskünfte des IP-Providers seien bspw. über § 101 Abs. 2 UrhG[8] zu erreichen). Da diese Auskünfte aber an Bedingungen ge-

---

2007, 602; *Köcher*, MMR 2007,801; *Meyerdierks*, MMR 2009, 8 (13); *Moos*, K&R 2008, 139; *Schmitz*, in: Hoeren/Sieber, Handbuch Multimedia-Recht, 26. Erg.lfrg. 2010, Teil 16.2 Datenschutz im Internet Rn. 84; *Schmittmann*, in: Hoeren/Sieber, Handbuch Multimedia-Recht, 26. Erg.lfrg. 2010, Teil 9 Portalrecht Rn. 107; *Spindler*/*Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 11 TMG Rn. 5b; *Zscherpe*, in: Traeger/Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2010, § 15 TMG Rn. 23; so wohl auch *Ott*, MMR 2009, 448 (452); *Gabriel*/*Cornels*, MMR 2008, S. XV; *Heckmann*, jurisPK-Internetrecht, 2. Aufl. 2009, Kap. 1.12 Rn. 29; *Buchner*, in: Traeger/Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2010, § 3 BDSG Rn. 13.

[6] Vgl. *Härting*, Internetrecht, 4. Aufl. 2010, Rdnr. 39; *Krüger/Maucher*, MMR 2011, 433 (436 ff.).

[7] Zum Ganzen *Härting*, Öffentlichkeitsarbeit einer Landesbehörde – Warum die „*Facebook*-Kampagne“ des ULD verfassungswidrig ist, S. 3 – abrufbar unter: http://www.computerundrecht.de/media/2011_08-22_Haerting_Oeffentlichkeitsarbeit_einer_Landesbehoerde.pdf (Stand: 20.09.2011) unter Verweis auf *Weichert*, in: Däubler/Klebe/Wedde/Weichert, BDSG, 1996, § 3 Rdnr. 3; *Schaar*, Datenschutz im Internet, 2002, Rdnr. 174; *Pahlen-Brandt*, K&R 2008, 288 (288) als Vertreter der Gegenauffassung.

[8] Siehe bspw. auch § 101 Abs. 9 UrhG, §§ 161 Abs. 1 Satz 1, 163 StPO für richterliche oder staatsanwaltliche Anordnungen oder auch §§ 96 Abs. 1, 113 Abs. 1 TKG.

knüpft sind, betrachtet die Gegenmeinung das Zusatzwissen als grundsätzlich nicht legal zugänglich und damit den Aufwand als unverhältnismäßig. Dem wird jedoch wiederum entgegengehalten, dass wegen der breiten Streuung der IP-Adresse während einer lang andauernden Session (flatrate) unter oft hunderten von Anbietern besuchter Seiten, von denen eine Vielzahl die Identität des Betroffenen kennen würden und die wegen entsprechender Nutzungsbedingungen oder ihres Standorts in Drittländern faktisch oder rechtlich nicht gehindert seien, diese weiterzugeben, die Personenbestimmung nicht mit so hoher Wahrscheinlichkeit ausgeschlossen werden könne oder der Aufwand unverhältnismäßig erscheine.[9]

Gerade in der jüngeren **Rechtsprechung** sind Belege zu finden, dass die Einstufung der IP-Adresse als personenbezogenes Datum abgelehnt wird, wenn es im Beschluss des OLG Hamburg heißt:

> *„Dass das Ermitteln der IP-Adresse nach deutschem Datenschutzrecht rechtswidrig sein könnte, ist nicht ersichtlich, da bei den ermittelten IP-Adressen ein Personenbezug mit normalen Mitteln ohne weitere Zusatzinformationen nicht hergestellt werden kann.“*[10]

Ähnlich argumentiert das AG München:

> *„Die den Nutzern einer Website zugeordneten dynamischen IP-Adressen stellen mangels Bestimmbarkeit einer Person kein personenbezogenes Datum i.S.d. § 3 Abs. 1 BDSG dar. Deshalb besteht kein Anspruch auf Unterlassung der Speicherung der IP-Adressen gemäß §§ 15 Abs. 1 und 4 TMG, 1004 BGB. Bestimmbarkeit ist dann gegeben, wenn die datenspeichernde Stelle die hinter der Einzelangabe stehende Person mit den ihr normalerweise zur Verfügung stehenden Kenntnissen und Hilfsmitteln und ohne unverhältnismäßigen Aufwand identifizieren kann.“*[11]

---

[9] *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 63.
[10] OLG Hamburg, Beschl. v. 3. November 2010 – Az: 5 W 126/10, Rn. 9 – zit. nach Juris.
[11] AG München, Urteil v. 30. September 2008, Az: 133 C 5677/08. So auch LG Wuppertal, Beschl. v. 19. Oktober 2010, Az: 25 Qs 10 Js 1977/08 – 177/10, 25 Qs 177/10, Rn. 10 – zit. nach Juris. Siehe auch LG Frankenthal, Beschl. v. 21. Mai 2008, Az: 6 O 156/08, Rn. 15 ff. – zit. nach Juris, wo der lediglich relative Personenbezug dynamischer IP-Adressen herausgestellt wird.

Demgegenüber wird die IP-Adresse von anderen Gerichten aber auch als personenbezogenes Datum eingeordnet.[12] Der BGH und das BVerfG stufen die IP-Adressen als Verkehrsdaten im Sinne des Telekommunikationsgesetzes (TKG) ein. Diese einschlägigen Regelungen (§§ 96 Abs. 1, 100 Abs. 1 TKG) erfassen dabei explizit ausschließlich „personenbezogene Daten“ (siehe § 91 Abs. 1 Satz 1 TKG; der Abschnitt 2 wird insofern auch mit „Datenschutz“ überschrieben). Allerdings beziehen sich diese Entscheidungen nur auf die jeweils fragliche Einordnung der dynamischen IP-Adressen als Bestands- oder Verkehrsdaten, ohne dass auf die davor liegende Frage des Personenbezugs eingegangen wird. In den Entscheidungen findet sich zur Einordnung der IP-Adressen als personenbezogenes Datum kein eindeutiger Hinweis, ob bei der implizit festgestellten Einordnung der IP-Adressen als personenbezogenes Datum der jeweils vorhandene relative Personenbezug ausschlaggebend gewesen sein soll, der im jeweiligen Einzelfall zu bejahen war. Die jeweils agierende bzw. speichernde Stelle konnte den Personenbezug mit den ihr normalerweise zur Verfügung stehenden Mitteln und Möglichkeiten ohne unverhältnismäßigen Aufwand herstellen (der Access-Provider selbst über seine Protokolle[13] und die staatlichen Stellen aufgrund staatsanwaltlicher Anordnung[14]). So heißt es auch in einer Entscheidung des AG Berlin:

> *„Bei einer dynamischen IP-Adresse handelt es sich um personenbezogene Daten im Sinne des Telemediengesetzes, da es sich um Einzelangaben über eine bestimmbare natürliche Person handelt. Darauf, ob diese Bestimmbarkeit dabei nur mit legalen Mitteln möglich ist, kommt es in diesem Zusammenhang nicht an.“*[15]

Darüber hinaus ist festzuhalten, dass aus dem Umstand, dass eine bestimmte IP-Adresse einem Anschluss zugeordnet werden kann, noch nicht folgt, dass der Inhaber

---

[12] So z.B. AG Darmstadt, Urteil v. 30. Juni 2005, Az: 300 C 397/04, Rn. 28 – zit. nach Juris; implizit wohl auch LG Berlin, Beschl. v. 14. März 2011, Az: 91 O 25/11.
[13] BGH, Urteil v. 13. Januar 2011, Az: III ZR 146/10.
[14] Über §§ 161 Abs. 1 Satz 1, 163 StPO im Falle der Einordnung als Bestandsdaten (BGH, Urteil v. 12. Mai 2010, Az: I ZR 121/08, Rn. 29 – zit. nach Juris) bzw. über §§ 96 Abs. 1, 113a TKG i.V.m. §§ 100g Abs. 2, 100b Abs. I StPO auf richterliche Anordnung als Verkehrsdaten (BVerfG, Urteil v. 2. März 2010, Az: 2 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, nunmehr auch BGH, Urteil v. 13. Januar 2011, Az: III ZR 146/10).
[15] AG Berlin, Urteil vom 27. März 2007, Az: 5 C 314/06, LS – zit. nach Juris.

dieses Anschlusses den Anschluss auch in diesem Zeitpunkt verwendet hat (Familie, Wohngemeinschaft, Bürogemeinschaft etc.).[16]

Demzufolge ist noch keine gefestigte Linie der Rechtsprechung oder auch des Schrifttums auszumachen,[17] die für die behördliche Einschätzung durch das ULD leitend sein könnte oder müsste. Vor diesem Hintergrund kann die pauschale Einordnung einer IP-Adresse durch das ULD als personenbezogenes Datum im Sinne des § 3 Abs. 1 BDSG zwar nicht als rechtsfehlerhaft oder willkürlich angesehen werden.[18] Jedoch kann die Einschätzung eines im Falle des Widerspruchs gegen die Verhängung eines Bußgelds entscheidenden Gerichts nicht prognostiziert werden.

2. Cookies

Neben den IP-Adressen werden nach Darstellung des ULD bei Fanpages und Social-Plugins auch sog. Cookies von Facebook gesetzt und ausgelesen:

> *„Außerdem nutzt Facebook Cookies, mit denen Nutzerinnen und Nutzer individualisiert werden können. Zusätzlich zu diesen Informationen erhebt und verarbeitet Facebook weitere Angaben, die zu einer umfassenden Profilierung der/des jeweiligen Nutzerin/Nutzers führen. Im Zusammenhang mit den durch die Nutzerinnen und Nutzer eingestellten Informationen ergeben sich somit Persönlichkeitsprofile, deren Detaillierungsgrad je nach Intensität der Nutzung von Facebook oder der Angebote, die Social-Plugins von Facebook einsetzen, variiert.“*[19]

---

[16] LG Saarbrücken, MMR 2008, 562; LG München, MMR 2008, 561; vgl. auch OLG Frankfurt/M., MMR 2008, 169 ff.

[17] So auch *Sachs*, CR 8/2010, 547 (551).

[18] Zur Kritik an der Sachlichkeit und Richtigkeit der Informationstätigkeit des ULD vor dem Hintergrund der Rspr. zu den Voraussetzungen staatlicher Informationstätigkeit (BVerfGE 105, 252 ff. – Glykol-Warnung, 279 ff. – Jugendsekte: Osho-Bewegung) siehe *Härting*, Öffentlichkeitsarbeit einer Landesbehörde – Warum die „*Facebook*-Kampagne“ des ULD verfassungswidrig ist, S. 6 f. – abrufbar unter: http://www.computerundrecht.de/media/2011_08-22_Haerting_Oeffentlichkeitsarbeit_einer_Landesbehoerde.pdf (Stand: 20.09.2011); *Strunk*/*Dirks*, Medien-Information: Stellungnahme zum „Facebook“-Boykott-Aufruf vom 19. August 2011 durch die schleswig-holsteinische Datenschutzbehörde ULD, S. 8 f., abrufbar unter: http://blawg.legalit.de/wp-content/uploads/2011/08/PM-SDP_ULD201108251.pdf (Stand 12.10.2011).

[19] ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 15.

Fraglich ist daher, ob Cookies einen Personenbezug im Sinne des Datenschutzrechts aufweisen.

Cookies sind kleine Dateien, die von einem Webserver eines Internet-Anbieters erzeugt und über einen mit ihm in Verbindung stehenden Web-Browser auf der Festplatte des Rechners eines Internet-Nutzers meist ohne dessen Wissen abgelegt werden, um diesen bei einer späteren erneuten Verbindung wieder erkennen (nicht notwendig: identifizieren) zu können. Soweit der Nutzer nicht bekannt ist, fungieren die Cookies als Pseudonym. Durch die mögliche Verknüpfung von Daten eignen sich Cookies unter Umständen zur Profilbildung. Bspw. kann ein in den Dateien des Anbieters eines Online-Shops oder sozialen Netzwerks bereits vorhandener oder ein bei einer künftigen Verbindung vom Benutzer – etwa anlässlich eines Vertragsschlusses – gelieferter Personenbezug genutzt werden. Cookies liefern demnach durch ihre verknüpfende Eigenschaft in manchen Situationen aktuell (zusätzliche) personenbezogene Daten, in anderen solche, die zunächst anonym sind, im weiteren Verlauf aber Personenbezug erhalten können, ohne dass der Nutzer sich dessen bewusst ist.[20]

Zum Teil wird vertreten, dass solche potentiell personenbezogenen Daten von Anfang an wie personenbezogene Daten behandelt werden müssten, um eine Sorgfaltspflichtverletzung und ein Verstoß mit Eventualvorsatz in jedem Fall zu vermeiden.[21]

Maßgeblich ist insofern auch im Bereich der Cookies die Auslegung des Merkmals der Bestimmbarkeit einer Person anhand des erhobenen Datums. Die Vertreter der relativen Theorie (siehe oben) gehen daher wiederum davon aus, dass für die Einordnung von Cookies als personenbezogenes Datum entscheidend darauf abzustellen ist, welche Daten in Form von Cookies im Einzelfall verarbeitet werden und welches Zusatzwissen dem Diensteanbieter über den Nutzer zur Verfügung steht. Ist ein Nutzer, bei dem ein Cookie abgelegt wird, anhand vorhandener Bestandsdaten bereits eine bestimmte oder bestimmbare Person, handele es sich bei Cookies um personenbezogene Daten. Dies ist etwa bei registrierten Kunden eines Online-Angebots der Fall. Keine personenbezogenen Daten liegen hingegen demnach vor, wenn durch den Cookie lediglich Daten übertragen werden, die es gerade nicht ermöglichen, einen Personen-

[20] *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 65 m.w.N.
[21] *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 65 m.w.N.

bezug herzustellen, und im Übrigen kein Zusatzwissen über den Nutzer vorhanden ist.[22]

Facebook-Cookies, die bei jedem Login zum Sozialen Netzwerk lokal hinterlegt werden, enthalten eine eindeutige Anmeldekennnummer. Anhand dieser Kennnummer ist Facebook mit Hilfe eingebetteter Social Buttons in der Lage, jeden Facebook-Nutzer im Internet eindeutig zu indentifizieren. Diese Cookies stellen daher auch nach der relativen Theorie personenbezogene Daten – zumindest konkret für Facebook – dar.[23] Gleiches muss gelten, falls auch bei Nichtnutzern im Falle des Aufrufens von Fanpages oder Webseiten mit „Gefällt mir"-Button Cookies hinterlegt werden, die längerfristig gespeichert werden („datr-Cookies") und spätestens bei einer nachträglichen Registrierung im Netzwerk zu einer nachträglichen Identifizierung durch Facebook führen. Laut eigenen Angaben von Facebook wird beim Besuch von Webseiten mit „Gefällt mir"-Schaltfläche in Deutschland weder bei Nichtnutzern noch bei nicht angemeldeten Nutzern ein Cookie gesetzt; es werde lediglich eine generische IP-Adresse im Impressionsprotokoll aufgezeichnet, die Aufschluss darüber gebe, dass der Aufruf aus Deutschland heraus erfolgte.[24]

3. Ergebnis

Nach der relativen Betrachtungsweise des Personenbezugs von Daten i.S.d. § 3 Abs. 1 BDSG kann bei dynamischen IP-Adressen weder im Hinblick auf Facebook noch auf die Webseiten- bzw. Fanpagebetreiber von einer Eröffnung des Anwendungsbereichs des Datenschutzrechts ausgegangen werden, da sie nicht über das nötige Zusatzwissen zur Identifizierung der jeweils dahinter stehenden Personen verfügen. Anders verhält sich dies für Cookies, die, soweit sie von dem sozialen Netzwerk tatsächlich entsprechend eingesetzt werden, Facebook ohne Inanspruchnahme weiterer Hilfen zur Identifizierung einzelner Personen dienen können. Nach der absoluten Theorie vom Personenbezug können sowohl dynamische IP-Adressen als auch Cookies als personenbezogene Daten eingeordnet werden.

---

[22] *Maisch*, ITRB 1/2011, 13 (15) m.w.N.
[23] *Maisch*, ITRB 1/2011, 13 (15) m.w.N.
[24] Umdr. 17/2781, S. 3.

III. Datenschutzrechtliche Verantwortlichkeit

Ausschlaggebend bleibt, ob für die personenbezogenen Daten – ob IP-Adressen oder Cookies – und deren Erhebung, Verarbeitung oder Nutzung die Verantwortlichkeit ausschließlich bei Facebook oder auch bei den öffentlichen und privaten Stellen liegt, die Social Plugins in ihre Homepages integrieren oder Fanpages bei Facebook gestalten.

Unstreitig scheint dabei zu sein, dass Daten ausschließlich von Facebook direkt erhoben und für die Reichweitenanalyse verarbeitet werden. Die hierbei erzielten Ergebnisse werden dann für die Verbesserung des Angebots durch Facebook genutzt und in anonymisierter Form unaufgefordert den jeweiligen Fanpage- bzw. Homepage-Betreibern zur Verfügung gestellt.

Die (Un-)Zulässigkeit der Datenverarbeitung richtet sich dabei nach Ansicht des ULD vornehmlich nach § 15 Abs. 3 TMG[25] (Trennungsgebot) in Verbindung mit § 11 BDSG (Auftragsdatenverarbeitung).[26] Insofern müsste es sich bei den Fanseitenbetreibern sowie den Betreibern von Webseiten, auf denen der „Gefällt mir"-Button eingebunden wird, einerseits um Diensteanbieter i.S.d. § 2 Satz 1 Nr. 1 TMG sowie um die verantwortliche Stelle für die Einhaltung der datenschutzrechtlichen Bestimmungen handeln.

1. Diensteanbieter i.S.d. TMG

Fraglich ist zunächst, ob es sich bei einem Betreiber einer Fanpage auf Facebook sowie bei einem Webseitenbetreiber, auf dessen Homepage ein „Gefällt mir"-Button integriert ist, um einen Diensteanbieter i.S.d. § 2 Satz 1 Nr. 1 TMG[27] handelt.

---

[25] Zum Anwendungsbereich: Das TMG, das für Telemedien bereichsspezifische datenschutzrechtliche Regelungen enthält und deshalb vorrangig Anwendung auf Telemediendienste findet, ist gem. § 1 Abs. 1 Satz 1 TMG auf alle Telemediendienste anwendbar. Dies gilt gem. § 1 Abs. 1 Satz 2 TMG auch für öffentliche Stellen, unabhängig davon, ob für die Nutzung der bereitgestellten Dienste ein Entgelt erhoben wird.

[26] ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, insbes. S. 22 f.

[27] Bei der Eröffnung des Anwendungsbereichs ist die Abgrenzung zum TKG im Auge zu behalten. Von daher dürfen die Telemedien nach § 1 Abs. 1 Satz 1 TMG nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG sein, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind. Da der Schwerpunkt bei Fanpages und Webseiten mit „Gefällt mir"-Buttons nicht kommunikativer Natur wie beim Versenden von Nachrichten oder dem Chatten ist, bleibt das TMG vorliegend anwendbar. Vgl. auch ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 19.

Das ULD äußert sich insofern knapp:

> *„Bei Facebook-Fanpagebetreibern und Webseitenbetreibern mit Sitz in Deutschland handelt es sich durchgängig um Diensteanbieter von Telemedien, auf die das TMG anwendbar ist.“*[28]

Dieses wird jedoch insbesondere bei **Twitter**-Profilen, die eine gewisse Vergleichbarkeit mit Facebook-Fanseiten aufweisen, durchaus unterschiedlich beurteilt,[29] weil die Nutzer der Plattform Twitter selbst eben **Nutzer** und nicht **zugleich Anbieter** eines Dienstes seien. Zudem hätte die Plattform und nicht die Nutzer der angebotenen Dienste die Kontrolle über die eingestellten Angebote.

Zu den Informations- und Kommunikationsdiensten i.S.d. § 1 Abs. 1 Satz 1 TMG zählen vor allem **Webseiten** und andere im Internet verfügbare Inhaltsangebote. Facebook-Fanseiten sind in ihrer Funktion und Darstellungsart mit solchen Webseiten grundsätzlich vergleichbar.[30]

Die **Begriffsbestimmung** des Diensteanbieters in § 2 Satz 1 Satz 1 Nr. 1 TMG setzt Art. 2 lit. b) E-Commerce-Richtlinie[31] um. Der Diensteanbieter bildet demnach das Gegenstück zum „Nutzer“. § 2 Satz 1 Nr. 1 TMG nimmt dabei eine **weite Definition** des Diensteanbieters vor und erfasst jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereit hält oder den Zugang zur Nutzung vermittelt. Es ist somit nicht entscheidend, ob eigene oder fremde Telemedien Ge-

---

[28] ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 17.

[29] Gegen eine Einordnung als Telemediendienst *Stadler*, Impressumspflicht für Twitteraccount?, abrufbar unter: www.internet-law.de/2009/04/impressumspflicht-fur-twitter-account.html (Stand: 07.10.2011; *Ferner*, Impressum bei Twitter, Wikia & Co.?, abrufbar unter www.homepage-impressum.de/ impressum-bei-twitter/ (Stand: 07.10.2011). Anders *Lapp*, Blogeintrag v. 17. 04. 2009, Impressumspflicht für Twitter-Account?, abrufbar unter: www.blog.beck.de/2009/04/17/impressumspflichtfuer- twitter-account#comment-16892 (Stand: 07.10.2011); *Krieg*, K&R 2010, 73 (77 f.); *Schirmbacher*, Härting-Paper, Rechtsvorschriften für Unternehmen in Twitter, abrufbar unter: www.haerting.de/ downloads/pdfs/Rechtsvorschriften_fuer_Unternehmen_in_Twitter.pdf (Stand: 07.10.2011); *Venzke*, DuD 2011, 387 (392); zumindest für geschäftsmäßige Angebote *Rauschhofer*, Internet World BUSINESS 24/09, 30 (30).

[30] *Holznagel/Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 1 TMG Rn. 4.

[31] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), Amtsblatt Nr. L 178 v. 17/07/2000 S. 1 ff.

genstand des Angebots sind. Allein die Funktion des Anbieters, dem Kunden die Nutzung von Telemedien zu ermöglichen, genügt zur Einordnung als Diensteanbieter. Dies muss noch nicht einmal ein gewerbliches Angebot sein. Wie der Diensteanbieter das Angebot bewerkstelligt, ist ebenfalls irrelevant. Daher ist nicht nur der Content Provider, der seine Inhalte auf eigenen Rechnern speichert, Diensteanbieter i.S.d. § 2 Satz 1 Nr. 1 TMG. Auch derjenige hält Telemedien zur Nutzung bereit, der selbst nicht über einen eigenen Server verfügt, sondern fremde Speicherkapazität nutzt.[32] Diensteanbieter ist somit neben einem Portalbetreiber (z.B. Internet-Auktion, Shopping-Portal) ebenso, wer auf der durch den Dritten betriebenen Verkaufsplattform ein gewerbliches Angebot einstellt und Waren oder Dienstleistungen anbietet.[33] Auch Unterseiten einer Domain können sich zu eigenständigen Telemedien entwickeln.[34]

Hier zeigt sich, dass es insbesondere auch in der Rspr. anerkannt ist, dass ein Nutzer einer Plattform zugleich zum Anbieter eines Telemediendienstes werden kann. Werden Twitter- bzw. Facebook-Dienste nachhaltig mit dem Willen genutzt, durch ihre Gesamtheit ein **dauerhaftes inhaltliches Angebot** zu schaffen, ist eine Einordnung als Telemediendienst geboten. Anders ist dies jedoch, wenn die Dienste lediglich für die Individualkommunikation, wie bspw. in Chatrooms, genutzt werden.[35]

Sowohl Betreiber einer Facebook-Fanpage als auch einer eigenen Webseite mit einem integrierten „Gefällt mir"-Button sind somit als Diensteanbieter i.S.d. TMG einzuordnen. Insofern trifft sie die in **§§ 7 ff. TMG** normierten Verpflichtungen. In diesem Abschnitt 3 zur „Verantwortlichkeit" finden sich die Bestimmungen zur **inhaltlichen Verantwortung** für eigene und Fremdinformationen innerhalb des Telemediendienstes. Abschnitt 4 (**§§ 11 ff. TMG**) widmet sich demgegenüber dem auf Telemediendienste zugeschnittenen **Datenschutz**. Durch den Verweis in § 12 Abs. 3 TMG wird deutlich, dass im Falle fehlender Regelungen im TMG die allgemeinen datenschutz-

---

[32] *Föhlisch*, in: Hoeren/Sieber, Handbuch Multimedia-Recht, 28. Erg.lfrg. 2011, Teil 13.4 Verbraucherschutz im Internet, Rn. 53. Siehe auch *Abel*, Praxiskommentar TMG, TKG und TKÜV, 2011, § 2 TMG Erl. (1); *Brüggen*/*Meier*, Telemedienrecht, 2007, Erl. zu § 2 Ziff. 1 m.N.

[33] LG München I, WRP 2005, 1042; *LG Memmingen,* MMR 2004, 769; *LG Berlin,* WRP 2004, 1198. Zum Ganzen *Holznagel*/*Ricke*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 2 TMG Rn. 2 m.w.N.

[34] Z. B. OLG Frankfurt/M., Urt. v. 06. 03. 2007 – 6 u 115/06, MMR 2007, 379 f.; zu Unterseiten von Verkäufern beim Online-Auktionator *eBay* OLG Hamm, MMR 2010, 29; OLG Düsseldorf, MMR 2008, 682 (682 f.); *Krieg*, K&R 2010, 73 (74).

[35] *Krieg*, in: Heckmann/Bräutigam (Hrsg.), Anwalt Zertifikat Online, IT-Recht 10/2009, Anm. 3.

rechtlichen Vorschriften greifen, so dass ergänzend auf Vorschriften des BDSG oder der entsprechenden Landesgesetze zurückzugreifen ist.[36]

2. Verhältnis des TMG zum BDSG

Die vom ULD herangezogene „Verbotsnorm", auf die sich das ULD bei der Verhängung der Bußgelder bezieht, ist § 15 Abs. 3 TMG:

> *„Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden."*

Tatsächlicher Anknüpfungspunkt ist für das ULD der Umstand, dass Facebook mit dem Einsatz eines Social-Plugins ebenso wie mit einer Fanpage untrennbar die Erstellung einer von § 15 Abs. 3 TMG erfassten Reichweitenanalyse („Facebook Insight") verbindet. Diensteanbieter sind jedoch nach dem Wortlaut der Datenschutzregelungen der §§ 11 ff. TMG lediglich für die eigene Erhebung und Verwendung personenbezogener Daten verantwortlich. Diensteanbieter sind insofern nicht zwangsläufig stets auch verantwortliche Stellen für sämtliche Datenverarbeitungsprozesse, die in irgendeinen Zusammenhang mit dem von ihnen angebotenen Telemediendiensten gebracht werden können. Dies betont auch das ULD, wenn es feststellt:

> *„Diensteanbieter begründen eine eigene Verantwortlichkeit, soweit und solange sie nach Würdigung aller Gesamtumstände aufgrund des tatsächlichen Einflusses den Prozess der Datenverarbeitung steuern."*[37]

Die Datenerhebungen und -verarbeitungen im Zusammenhang mit dem Aufrufen von Fanpages oder Webseiten mit Social-Plugins werden ausschließlich von Facebook vorgenommen. Das ULD rechnet diese Fremdvorgänge den Diensteanbietern der

---

[36] Dies gilt insbesondere auch für die Begriffsbestimmungen nach § 3 BDSG, siehe *Dix*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 170. Siehe auch *Piltz*, CR 2011, 657 (662).

[37] ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 17 m.w.N.

Fanpages und Webseiten mit integrierten „Gefällt mir“-Buttons über die Grundsätze der Auftragsdatenverarbeitung zu:

> *„Diese in § 15 Abs. 3 TMG geregelte Reichweitenanalyse verortet die Verantwortlichkeit für die Nutzung der personenbezogenen Daten bei dem Diensteanbieter, der zur Erfüllung dieser Aufgabe einen Dienstleister, im konkreten Fall Facebook, heranzieht. Für die Handlungen des Dienstleisters ist nach den Maßgaben des § 11 BDSG bzw. § 17 Landesdatenschutzgesetz Schleswig-Holstein (LDSG S-H) der Diensteanbieter datenschutzrechtlich verantwortlich.“*[38]

Dies ist insofern folgerichtig, als über § 12 Abs. 3 TMG die allgemeinen datenschutzrechtlichen Regelungen herangezogen werden können. Fraglich ist jedoch, ob es sich bei den Fanpagebetreibern und den Betreibern der Webseiten mit Social-Plugins tatsächlich um die datenschutzrechtlich verantwortliche Stelle i.S.d. **§ 3 Abs. 7 BDSG** (§ 2 Abs. 3 LDSG), ggf. vermittelt über ein Auftragsdatenverhältnis nach **§ 11 BDSG** (§ 17 LDSG), handelt.

3. Verantwortliche Stelle i.S.d. BDSG

Fraglich ist, ob die datenschutzrechtliche Verantwortlichkeit der Fanpage- und Webseitenbetreiber über die Regelungen des BDSG konstruiert werden kann.

a) Verantwortlichkeitsbegriff und Auftragsdatenverarbeitung

Die maßgeblichen Normen im Datenschutzrecht zur Verantwortlichkeit lauten:

§ 3 Abs. 7 BDSG:

> *„Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.“*

---

[38] ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 17 f.

§ 2 Abs. 3 LDSG:

> *„Daten verarbeitende Stelle ist jede öffentliche Stelle im Sinne von § 3 Abs. 1, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.“*

Den genannten Bestimmungen liegt die entsprechende Begriffsbestimmung aus der gemeinschaftsrechtlichen Datenschutzrichtlinie (EU-DSRL) zugrunde; Art. 2 lit. d) EU-DSRL (Begriffsbestimmungen):

> *„‚für die Verarbeitung Verantwortlicher' die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. (…)“.*

Maßgeblicher Anknüpfungspunkt ist nach all diesen Regelungen stets ein gewisser Grad an Einflussmöglichkeit auf die tatsächlich erfolgenden Datenverarbeitungsprozesse.

Die Verarbeitungsregelungen des Datenschutzrechts setzen stillschweigend voraus, dass es für jede gesetzlich geregelte Aktivität **mindestens einen Verantwortlichen** gibt, so dass „unverantwortete“ Aktivitäten ausgeschlossen sind. Die Verantwortlichkeit ist nicht streng an den Besitz und die physische Herrschaft über den Verarbeitungsprozess gebunden.[39] Sie bleibt daher insbesondere bei Auftragsdatenverarbeitung erhalten. Dies wird ausdrücklich auch in den gesetzlichen Begriffsbestimmungen deutlich, wenn es hier heißt „oder durch andere verarbeiten lässt“ / „dies durch andere im Auftrag vornehmen lässt“. Entsprechend einem allgemeinen Rechts- und Organisationsgrundsatz wird dadurch klargestellt, dass die Verantwortlichkeit einer Person oder Stelle nicht davon abhängt, ob sie Daten selbst erhebt und verarbeitet oder ob sie sich dazu eines anderen, z.B. eines Service-Rechenzentrums oder eines Datenerfassungsbüros, bedient; sie bleibt auch dann verantwortliche Stelle. Dieses Prinzip liegt

[39] *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 225.

auch den Regelungen des **§ 11 Abs. 1 BDSG** (§ 17 LDSG) für die **Datenverarbeitung im Auftrag** zugrunde.[40]

Das BDSG spricht die „verantwortliche Stelle“ stets im Singular an. Dies entspricht üblicher Gesetzesredaktion. Das Gesetz schließt aber weder ausdrücklich noch sinngemäß aus, dass **mehrere** natürliche oder juristische **Personen** mit personenbezogenen Daten in **gemeinsamer Verantwortung** umgehen.[41] Zum Teil wird im Rahmen der Auftragsdatenverarbeitung vertreten, dass die beauftragte Stelle selbst gerade keine verantwortliche Stelle sei, weil sie die Daten nicht für sich selbst, sondern nur für jemand anderes verarbeitet.[42] Dies ist zunächst vom Wortlaut der Begriffsbestimmungen gedeckt, tatsächlich werden die Rechte und Pflichten der Auftrag gebenden sowie beauftragten Personen und Stellen jedoch vom Gesetz ausdrücklich im Einzelnen bestimmt und gegeneinander abgegrenzt (§ 11 BDSG). Die **Verantwortlichkeit des Auftragsverarbeiters** ist **eingeschränkt**, aber nicht aufgehoben.[43]

Eine **Auftragsdatenverarbeitung** liegt nach ganz überwiegender Auffassung nur vor, wenn der Auftraggeber nicht nur rechtlich, sondern zumindest prinzipiell auch tatsächlich in der Lage ist, dem Auftragnehmer **jeden Arbeitsschritt vorzuschreiben** und letztlich auch die **korrekte Durchführung** des Datenumgangs zu **kontrollieren**. Teilweise wird daher die Auftrag gebende Stelle als „Herrin des Verfahrens“ und die Auftrag nehmende Stelle als „verlängerter Arm“ bezeichnet. Typisches Merkmal einer Auftragsdatenverarbeitung ist der Umstand, dass sich der Auftraggeber die Entscheidungsbefugnis vorbehält und dem Auftragnehmer keinerlei inhaltlichen Bewertungs- und Ermessensspielraum gestattet.[44] Erfüllt der externe Datenverarbeiter **überwiegend eigene Geschäftszwecke**, dann ist er nicht mehr bloßer Auftragnehmer, sondern wird selbst zur insoweit verantwortlichen Stelle. Eine Datenweitergabe des „Auftraggebers“ wäre dann als Übermittlung anzusehen.[45]

---

[40] *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 227.
[41] *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 226.
[42] Siehe *Auerhammer*, BDSG, 3. Aufl. 1993, § 2 Rn. 15; *Giesen*, CR 2007, 543 f.
[43] *Dammann*, in: Simitis, BDSG, 7. Aufl. 2011, § 3 Rn. 228 unter Verweis auf *Wedde*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, S. 529; *Marx*, DSWR 1979, 88.
[44] *Petri*, in: Simitis, BDSG, 7. Aufl. 2011, § 11 Rn. 20 m.w.N.
[45] *Petri*, in: Simitis, BDSG, 7. Aufl. 2011, § 11 Rn. 22 unter Verweis auf *Gützmacher*, ITRB 2997, 183.

b) Keine Auftragsdatenverarbeitung durch Facebook

Bei der vorliegenden Konstellation scheint unstreitig, dass die Fanpage- und Webseitenbetreiber selbst keine personenbezogenen Daten erheben oder verarbeiten.[46] Soweit Facebook auf eigene Initiative die für die Reichweitenanalyse erforderlichen Daten erhebt und verarbeitet, kann von einem Verhältnis der Auftragsdatenverarbeitung keine Rede sein. Den Fanpage- oder Webseiten-Betreibern ist es nicht möglich, auf die Reichweitenanalyse zu verzichten, geschweige denn Facebook im Einzelnen vorzuschreiben, wie die Datenverarbeitungsvorgänge im Detail abzuwickeln sind. Es bleibt lediglich die Möglichkeit, die anonymisiert übermittelten Ergebnisse der Reichweitenanalyse zu ignorieren und nicht zur Kenntnis zu nehmen. Der Fanseiten- oder Webseitenbetreiber hat grundsätzlich keine Entscheidungsbefugnis darüber, ob und in welcher Weise personenbezogene Daten von Facebook erhoben werden,[47] geschweige denn einzelne Arbeitsschritte zu kontrollieren.

Das **ULD** veröffentlichte am 30. September 2011 eine **ergänzende Stellungnahme** zur Frage der Verantwortlichkeit bei Facebook-Fanpages und Social-Plugins. Hierbei stützt sich das ULD zur Begründung der gemeinsamen Verantwortung von Facebook und den Betreibern der jeweiligen Seiten auf Arbeitspapiere der Artikel-29-Datenschutzgruppe, die sich explizit mit Fragen der „geteilten" oder „gemeinsamen" Verantwortlichkeit, auch speziell im Kontext der sozialen Netzwerke, auseinandersetzen. In diesen Arbeitspapieren sind jedoch auch nur abstrakt gehaltene Maßstäbe für die Verteilung von Verantwortlichkeiten im Kontext von sozialen Netzwerken enthalten. Eine konkrete Zuordnung bestimmter Datenverarbeitungsprozesse zum Plattformbetreiber oder zum Nutzer wird nicht vorgenommen. Es wird zwar betont, dass allein die Nutzung eines sozialen Netzwerks, welches von einem Dritten betrieben wird, nicht zum Ausschluss der Verantwortlichkeit führt. Dies wird auch hier nicht bestritten, da die Verantwortlichkeit für eigene Inhalte und selbst initiierte Datenerhebungen stets auf Seiten des Fanpage- oder Webseitenbetreibers mit Social-Plugin verbleibt. Es bleibt aber dabei, dass für die Annahme einer Verantwortlichkeit, selbst einer (Teil-) Verantwortlichkeit, stets ein Anknüpfungspunkt bestehen muss. Der Mitverantwortliche muss in irgendeiner Form maßgeblich die inhaltlichen Entscheidungen über die Art, den Umfang und vor allem den Zweck der Datenverarbeitung treffen kön-

[46] Siehe dazu auch *Laue*, Datenschutz-Berater 6/2011, 11 (12); *Strunk*/*Dirks*, Medien-Information: Stellungnahme zum „Facebook"-Boykott-Aufruf vom 19. August 2011 durch die schleswig-holsteinische Datenschutzbehörde ULD, S. 5, abrufbar unter: http://blawg.legalit.de/wp-content/uploads/2011/08/PM-SDP_ULD201108251.pdf (Stand 12.10.2011).

[47] So auch Facebook selbst in der Stellungnahme zum Arbeitspapier des ULD, Umdr. 17/2684.

nen. Soweit die Datenverarbeitung, wie die für die Reichweitenanalyse, allein nach Art und Maß durch Facebook und ohne Einflussmöglichkeiten des Nutzers gestaltet wird, muss eine Verantwortlichkeit der Fanpage- oder Webseitenbetreiber ausscheiden, ohne dass diese Ansicht in Widerspruch zur Artikel-29-Datenschutzgruppe steht.

Allein die Entscheidung für die Eröffnung einer Fanpage oder die Einbindung eines Social-Plugins, mit der unwillkürlich Datenverarbeitungsprozesse der Netzwerkbetreiber einhergehen, ist für die Begründung einer datenschutzrechtlichen Verantwortlichkeit nicht ausreichend.[48] Denn eine Steuerung der Datenverarbeitungsprozesse, wie sie das ULD selbst zur Begründung einer Verantwortlichkeit von Diensteanbietern verlangt,[49] liegt gerade nicht vor. Sie haben insofern durch die Nutzung der Facebook-Angebote allenfalls das „Ob" einer Datenerhebung und -verarbeitung durch das soziale Netzwerk in der Hand, keinesfalls Art, Umfang oder Zweck der Prozesse.

Das Zusammenspiel von TMG und allgemeinen Datenschutzbestimmungen macht deutlich, dass das Regelungswerk nicht auf die Verteilung der Verantwortlichkeiten im Zeitalter des Web 2.0 ausgerichtet ist.[50] Insbesondere die Vorschriften des TMG zielten ursprünglich darauf ab, dass Diensteanbieter schlicht die Infrastruktur „Internet" zur Verbreitung eines eigenen Teledienstes nutzen; zwischenzeitlich ist jedoch eine zweite Infrastrukturebene wie Facebook, Google-plus, Twitter oder Ebay, die für die Erstellung eigener (Unter-) Dienste genutzt werden, hinzugetreten. Insofern drängt sich der Vergleich auf, dass auch Betreiber gewöhnlicher Homepages ohne Nutzung anderer Plattformen oder Social-Plugins nicht für die Datenerhebungen und -verarbeitungsprozesse des „Internets" (in Form von Service-Providern) allein durch die Errichtung der eigenen Webseite generell in die datenschutzrechtliche Mitverantwortung genommen werden, nur weil beispielsweise die Verwendung der IP-Adresse durch den Provider erfolgt, die für die Aufrechterhaltung der Verbindung mit der jewei-

---

[48] So wohl auch *Strunk*/*Dirks*, Medien-Information: Stellungnahme zum „Facebook"-Boykott-Aufruf vom 19. August 2011 durch die schleswig-holsteinische Datenschutzbehörde ULD, S. 5, abrufbar unter: http://blawg.legalit.de/wp-content/uploads/2011/08/PM-SDP_ULD201108251.pdf (Stand 12.10.2011).

[49] ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 17 m.N.

[50] Siehe auch *Karg*/*Fahl*, K&R 2011, 453 (458), die ebenfalls anmerken: „wie wenig passend die bisher geltenden Regelungen und die mittlerweile artifizielle Trennung der Fachgesetze in Hinblick auf den Datenschutz ist. Je stärker die Verwendung personenbezogener Daten intermedial erfolgt, desto schwieriger wird es, Rechtssicherheit für Betreiber und Nutzer zu schaffen. Die vor allem in der Rechtspraxis entstehenden Unsicherheiten bereits bei der Beantwortung der Frage, welches Rechtsregime überhaupt einschlägig ist, können weder durch die Aufsichtsbehörden noch durch die Judikative beseitigt werden."

ligen Homepage im Übrigen unumgänglich ist. Es bieten sich daher differenzierende Lösungen an.

c) Facebook als verantwortliche Stelle

Die Verneinung der datenschutzrechtlichen Verantwortlichkeit der Fanpage- und Webseitenbetreiber in der vorliegenden Konstellation führt zu keiner regelungswidrigen Schutzlücke. In Form von Facebook ist eine verantwortliche Stelle eindeutig zu identifizieren. Eine unverantwortete Datenverarbeitung, die über das Datenschutzrecht in jedem Fall ausgeschlossen werden soll, findet insofern nicht statt.[51] Zudem zeigt sich, dass die Annahme eines Auftragsdatenverarbeitungsverhältnisses mit Facebook als Auftrag nehmende Stelle mit dem unbefriedigenden Ergebnis einherginge, dass dessen Verantwortlichkeit im Gegensatz zu der jeweils Auftrag gebenden Stelle eingeschränkt wäre, obwohl sich der Eindruck aufdrängt, dass Facebook zumindest als Haupt(mit-)verantwortlicher zu identifizieren ist.

Soweit man anerkennt, dass Facebook überwiegend eigene Geschäftszwecke verfolgt, scheidet eine Einordnung als Auftragnehmer ohnehin aus (siehe oben). In diesem Fall wäre jede Datenweitergabe des „Auftraggebers“ als Übermittlung anzusehen.[52] Vorliegend werden aber keinerlei Daten von den Fanpage- oder Webseitenbetreibern erhoben, die anschließend an Facebook übermittelt werden; vielmehr erfolgen sämtliche Datenverarbeitungsprozesse unmittelbar durch Facebook.

4. Berücksichtigung der mittelbaren Verantwortlichkeit außerhalb des TMG/BDSG

Die mittelbar zu konstruierende Verantwortung wegen der nicht zu leugnenden Kausalität für den Datenverarbeitungsprozess allein durch den Umstand der Eröffnung von Fanpages oder der Einbindung eines Social-Plugins in eigene Homepages kann insoweit interessengerecht aufgefangen werden, indem aus der **staatlichen Schutzpflicht** der öffentlichen Stellen aus den **Grundrechten** sowie der **Verpflichtung zum gesetzmäßigen Verhalten** aus Art. 20 Abs. 3 GG die Pflicht entnommen wird, auch

[51] Offen bleibt in diesem Zusammenhang, ob auf die Aktivitäten von Facebook deutsches oder irisches Datenschutzrecht Anwendung findet. Siehe dazu ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 18 ff.; *Stadler*, ZD 2011, 57 ff., die für die Anwendung des deutschen Datenschutzrechts votieren, a.A. Stellungnahme von Facebook, Umdr. 17/2781, S. 1.

[52] *Petri*, in: Simitis, BDSG, 7. Aufl. 2011, § 11 Rn. 22 unter Verweis auf *Gützmacher*, ITRB 2997, 183.

ohne unmittelbare datenschutzrechtliche Verantwortlichkeit zwischen den positiven Nutzungseffekten von Fanpages und Social-Plugins (hoher Verbreitungsgrad, wirtschaftliches, kostenloses Angebot, einfach erreichbare Informationen, schnelle Veränderbarkeit etc.) und den datenschutzrechtlichen Belangen der potentiellen Seitenbesucher (Recht auf informationelle Selbstbestimmung; Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme etc.) **abzuwägen**, um zu entscheiden, ob eine Nutzung des Facebook-Angebots angemessen im Sinne des allgemeinen Verhältnismäßigkeitsprinzips ist. Dabei kommt es auch maßgeblich auf die Ermittlung der tatsächlich stattfindenden Datenerhebungs- und -verarbeitungsprozesse durch Facebook an, insbesondere ob und welche Daten wann bei Nichtnutzern erhoben und verarbeitet werden, um ein mögliches Gefahrenpotential angemessen einschätzen zu können. Bei Nutzern bliebe zu klären, ob die seitens Facebook bei Abschluss des Nutzungsvertrages abgegebenen Einwilligungserklärungen auf Grundlage der von Facebook zur Verfügung gestellten Datenschutzrichtlinien und Allgemeinen Geschäftsbedingungen eine die Datenverarbeitungsprozesse rechtfertigende Funktion zukommt oder ob diese zu intransparent und/oder als zu umfangreich bezeichnet werden können.[53] Selbst im letzteren Fall könnte dem Umstand einer tatsächlich abgegebenen Einwilligung und dem damit zum Ausdruck kommenden grundsätzlichen Willen zur Nutzung von Facebook im Rahmen des Abwägungsprozesses durch die öffentlichen Stellen Rechnung getragen werden.

Ein Ergebnis einer solchen Abwägung könnte insbesondere im Zusammenhang mit der Einbindung von **Social-Plugins** auf eigenen Webseiten sein, dass hier eine „**Zwei-Klick-Lösung**“ genutzt werden sollte, bei der zunächst eine Aufklärung desjenigen erfolgt, der den Social-Plugin betätigt. Stimmt dieser den dort genannten Nutzungsbedingungen zu, erfolgt die tatsächliche Aktivierung des „Gefällt mir“-Buttons mit den damit verbundenen Datenverarbeitungsprozessen, die über Facebook ausgelöst werden. Dies gilt umso mehr, als die mittelbare Verantwortlichkeit des Webseitenbetreibers bei der Integration von Social-Plugins deutlicher ausgeprägt ist, weil die jeweilige Webseite autonom existiert und nicht prinzipiell wie bei der Fanpage von der genutzten Infrastrukturebene Facebook als Plattform abhängt.

[53] Das ULD mahnt beides an, wobei unklar bleibt, wie einerseits dem Erfordernis nach umfassenderer Aufklärung und zugleich kürzeren Ausführungen nachgekommen werden könnte.

Dass eine ähnliche Verpflichtung **private Unternehmen oder andere Stellen** nicht trifft, muss unter dem Aspekt der diese ebenfalls berechtigenden Grundrechte (Art. 12, 14, 2 Abs. 1 GG) und dem Grundsatz der Entscheidungsfreiheit der die Fanpages und Webseiten mit Social-Plugins besuchenden Nutzer sowie der Tatsache, dass Facebook zumindest den europäischen Datenschutzstandards unterfällt,[54] als unschädlich eingestuft werden.

IV. Andere mögliche Verstöße: §§ 5 und 13 TMG

Das ULD mahnt neben der Unzulässigkeit der Reichweitenanalyse nach § 15 Abs. 3 TMG auch Verstöße der Webseitenbetreiber gegen § 5 Abs. 1 TMG (Impressum) sowie weitere Verpflichtungen aus § 13 Abs. 1, 4 und 5 TMG an.

Abgesehen davon, ob überhaupt Verstöße gegen die aus **§ 5 TMG** resultierenden allgemeinen Informationspflichten vorliegen, ist festzustellen, dass hierauf gestützte Ordnungswidrigkeitenverfahren (§ 16 Abs. 2 Nr. 1 TMG) in die Zuständigkeit der Medienanstalt Hamburg/Schleswig-Holstein fallen (siehe unten).

Im Rahmen des § 13 TMG ist ebenfalls wie bei § 15 Abs. 3 TMG (siehe oben) auf die datenschutzrechtliche Kategorie der Verantwortlichkeit abzustellen. Da keinerlei Datenerhebungs- und -verarbeitungsprozesse auf Veranlassung des Fanpage- oder Webseitenbetreibers stattfinden, treffen die in **§ 13 Abs. 1 und Abs. 4 Nr. 2 und 6 TMG** genannten Pflichten ebenfalls Facebook als verantwortliche Stelle. Anderes mag allerdings zum einen für die Verpflichtung aus **§ 13 Abs. 5 TMG** gelten. Hiernach muss dem Nutzer die Weitervermittlung zu einem anderen Diensteanbieter angezeigt werden. Im Falle der Einbindung von Social-Plugins wird der Nutzer bei Aktivierung des Buttons direkt zur Anmeldeseite von Facebook weitergeleitet. Erkennbar ist dies allenfalls an dem Design des Buttons, der mit einem blauen „f“ für Facebook verbunden ist. Insofern würde wiederum eine „Zwei-Klick-Lösung“ Abhilfe von einem möglichen Verstoß schaffen. Ähnliches gilt für die Pflicht gemäß **§ 13 Abs. 4 Nr. 3 TMG**, wonach der Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen hat, dass der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann. Soweit Facebook als Dritter (vgl. § 3 Abs. 8 BDSG) eingestuft werden kann, ist fraglich, ob bereits die Einbindung des „Gefällt mir“-Buttons auf einer Webseite zur Erhebung von personenbezogenen Daten durch Fa-

[54] Siehe Fußnote 51.

cebook führt, ohne dass der Button durch den jeweiligen Webseitenbesucher angeklickt werden muss. Ist dies der Fall, könnte ggf. durch eine in dieser Hinsicht Abhilfe schaffende „Zwei-Klick-Lösung“ ein Verstoß gegen die Datensicherheitsnorm des § 13 Abs. 4 Nr. 3 TMG vermieden werden.

Frage 2: Ist es daher zwingend erforderlich, dass alle Stellen in Schleswig-Holstein ihre Fanpages bei Facebook und „Social-Plugins“ auf ihren Webseiten entfernen?

Aufgrund der obigen Ausführungen ist festzustellen, dass es sich bei der vom ULD vertretenen Rechtsauffassung zur Auslegung der einfachgesetzlichen Normen, die Grundlage der anvisierten Ordnungswidrigkeitenverfahren sein sollen, um eine im Ergebnis vertretbare, aber äußerst umstrittene Position handelt, deren Erfolgsaussichten unter Zugrundelegung der bisherigen Rechtsprechung und der im Schrifttum vorherrschenden Ansichten vom Wissenschaftlichen Dienst als gering eingeschätzt werden. Dies gilt insbesondere für die Annahme einer unmittelbaren datenschutzrechtlichen Verantwortlichkeit der Fanpage- und Webseitenbetreiber.[55] Eine Entfernung von Fanpages und Social-Plugins ist allerdings vor dem Hintergrund des in jedem Fall bestehenden Prozessrisikos zu erwägen, sobald individualisierte Aufforderungen des ULD einzelne Stellen erreichen. Mit Blick auf die unschwer zu realisierende „Zwei-Klick-Lösung“ im Falle der Einbindung von „Gefällt mir“-Buttons und der möglicherweise mit der Einbindung einhergehenden Verstöße gegen § 13 Abs. 4 Nr. 3 sowie Abs. 5 TMG, sollten solche „Zwei-Klick-Lösungen“ auf den eigenen Webseiten vorgeschaltet werden. Dieses Modell wird bspw. bereits vom SWR3 auf dessen Internetseite „SWR3.de“ genutzt. So heißt es bereits in den dortigen Datenschutzbestimmungen:

> *„Für die Gefällt-mir- (Facebook) und +1-Knöpfe (Google) – die du unter vielen Seiten findest – haben wir eine zweistufige Lösung eingerichtet: Damit du bei einer Seite auf WR3.de ‘Gefällt mir’ oder ‘+1’ drücken kannst, musst du erst auf den Button klicken und ihn aktivieren; nur dann wird eine Verbindung mit den*

[55] Vgl. jüngst *Piltz*, CR 2011, 657 (662).

Facebook- oder Google-Servern aufgebaut und du kannst mit einem zweiten Klick den Beitrag deinen Freunden empfehlen.“[56]

Im Übrigen ist die Grundrechts- und Gesetzmäßigkeitsbindung der öffentlichen Stellen zu beachten, die zu einer Abwägung von Nutzen und Risiken im Einzelfall des Rückgriffs auf Angebote von Facebook veranlasst.

Frage 3: Haben die den Webseitenbetreibern angedrohten Bußgeldverfahren Aussicht auf Erfolg, wenn der Aufforderung des ULD nicht bis Ende September 2011 nachgekommen wird?

Insofern ist auf das Ergebnis zu Frage 1 sowie auf die Ausführungen zu Frage 2 zu verweisen. Um die Erfolgsaussichten etwaiger Ordnungswidrigkeitenverfahren zu beurteilen, sei im Folgenden ergänzend auf die formellen sowie die allgemeinen materiellen Voraussetzungen solcher Verfahren hingewiesen.

I. Zuständigkeit

Eine wichtige Frage im Zusammenhang mit den Erfolgsaussichten der Bußgeldverfahren ist die streitige Frage,[57] ob das ULD überhaupt für die Ahndung von Ordnungswidrigkeiten in diesem Umfang zuständig ist.

Die Bußgeldverfahren richten sich nach eigenen Angaben des ULD „nach § 16 TMG und/oder § 43 BDSG bei privaten Stellen“; daneben werden Beanstandungen gemäß § 42 Abs. 2 LDSG bei öffentlichen Stellen in Aussicht gestellt.[58]

Für **Ordnungswidrigkeiten** im Sinne des **§ 43 BDSG** ergibt sich die Zuständigkeit des ULD über Ziffer **3.5.2** der Anlage zur Ordnungswidrigkeiten-

[56] Datenschutzbestimmungen des SWR3, abrufbar unter: www.swr3.de/startpage/Hinweise-zum-Datenschutz/-/id=47310/did=906402/3052t/index.html#Facebook (Stand: 11.10.2011).
[57] Bspw. bestritten von *Härting*, Öffentlichkeitsarbeit einer Landesbehörde – Warum die „*Facebook*-Kampagne“ des ULD verfassungswidrig ist, S. 7 – abrufbar unter: http://www.computerundrecht.de/media/2011_08-22_Haerting_Oeffentlichkeitsarbeit_einer_Landesbehoerde.pdf (Stand: 20.09.2011).
[58] ULD, *Karg*/*Thomsen*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 19. August 2011, S. 25.

Zuständigkeitsverordnung (**OWi-ZustVO**). Aufgabe des ULD ist gemäß § 39 Abs. 1 LDSG die Überwachung der Einhaltung der Vorschriften des LDSG sowie anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen; bei nichtöffentlichen Stellen kontrolliert das ULD den Datenschutz nach dem BDSG und fungiert als Aufsichtsbehörde im Sinne des § 38 BDSG (§ 39 Abs. 3 LDSG). Das ULD ist damit sowohl für den öffentlichen als auch den privaten Bereich zuständige Aufsichtsbehörde für den Datenschutz[59].

In den Kompetenzbereich des ULD fallen auch Maßnahmen der **Beanstandung** gemäß **§ 42 LDSG** für den Sektor der öffentlichen Stellen. Dem ULD spricht das LDSG damit, anders als das BDSG der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich, keine Befugnis zu, selbst verbindlich Maßnahmen zur Verbesserung des Datenschutzes anzuordnen (siehe § 38 Abs. 5 BDSG). Allerdings eröffnet die mit der förmlichen Beanstandung verbundene Unterrichtung der Aufsichtsbehörde die Möglichkeit, den Sachverhalt noch einmal rechtlich zu prüfen und bei Übereinstimmung zwischen Landesbeauftragten und Aufsichtsbehörde ggf. die Maßnahmen durch die Aufsichtbehörde zu veranlassen, die dem Landesbeauftragten versagt sind.[60] Für die Ahndung von Ordnungswidrigkeiten nach § 44 LDSG wäre dann gemäß Ziffern 1.1.1.1, 1.2.2 und 2.5.1.1 der Anlage zur OWi-ZustVO entweder die jeweils oberste Landesbehörde, das Innenministerium als Kommunalaufsichtsbehörde oder die Landrätinnen und Landräte als untere Fachaufsichts- oder Kommunalaufsichtsbehörde, zuständig.

Die Regelung des § 59 des Staatsvertrages für Rundfunk und Telemedien (RStV) schreibt die Kompetenz für die Überwachung der Einhaltung der Datenschutzbestimmungen des TMG den nach den allgemeinen Datenschutzgesetzen des Bundes oder der Länder zuständigen Kontrollbehörden zu. In Ermangelung einer spezialgesetzlichen Regelung im **TMG** richtet sich die zuständige **Aufsichtsbehörde** für Telemediendiensteanbieter nach § 38 BDSG.[61] Über § 39 Abs. 3 LDSG kommt diese Aufgabe dem ULD zu, so dass dieses in jedem Fall für die inhaltliche Überwachung der datenschutzrechtlichen Anforderungen aus den §§ 11 ff. TMG zuständig ist.

---

[59] So auch *Gola*/*Schomerus*, BDSG, 10. Aufl. 2010, § 38 Rn. 29 unter Verweis auf *Bäumler*, DuD 2000, 20.
[60] *Beilecke*, LDSG Schleswig-Holstein, 2. Aufl. 1996, § 25 Rn. 6, 8.
[61] *Köhler*/*Arndt*/*Fetzer*, Recht des Internets, 6. Aufl. 2008, Rn. 946. § 38 Abs. 1 Satz 1 BDSG: „Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit (…)."

Hinsichtlich der **Ordnungswidrigkeitenverfahren** im Bereich des **TMG** liegt eine geteilte Zuständigkeitsregelung vor. Während die **Medienanstalt** Hamburg/Schleswig-Holstein für die Ahndung von Verstößen gegen die Impressumspflicht nach **§ 16 Abs. 1, Abs. 2 Nr. 1 TMG** zuständig ist **(§ 38 Abs. 6 Medienstaatsvertrag** HSH), richtet sich die Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten nach § 16 Abs. 2 Nr. 2-5 TMG nach § 36 Abs. 2 lit. a OWiG, der allgemein die oberste Landesbehörde für die Ahndung von Ordnungswidrigkeiten zuständig erklärt. Über die Regelung des § 45 Abs. 1 LDSG wurden jedoch die Aufgaben des Innenministeriums im Bereich des Datenschutzes auf das ULD übertragen.[62] Fraglich ist insoweit jedoch, ob über diese Aufgabenübertragungsnorm sämtliche Aufgaben im Bereich des Datenschutzes – insbesondere auch die der Verfolgung von datenschutzrechtlichen Verstößen mit Bußgeldverfahren – auf das ULD übergegangen sind.[63] Problematisch ist hierbei zunächst, dass nach dem Wortlaut des § 45 LDSG lediglich „die am 30. Juni 2000 dem bei dem Präsidenten des Schleswig-Holsteinischen Landtages eingerichteten Landesbeauftragten für den Datenschutz sowie der Datenschutzaufsichtsbehörde im Innenministerium obliegenden Aufgaben (…) am 1. Juli 2000 auf die Anstalt über[gehen]“. Die Regelungen des TMG stammen jedoch erst aus dem Jahr 2007. Ausgehend vom Sinn und Zweck der Regelungen zur Errichtung des ULD und der gebündelten Aufgabenübertragung ist es möglich zu argumentieren, dass die bislang durch die beiden in § 45 LDSG genannten „Vorgängerstellen“ wahrgenommenen Aufgaben ebenso wie die in Zukunft entstehenden Aufgaben im Bereich des Datenschutzrechts auf das ULD übertragen werden sollten. Dagegen spricht jedoch, dass die OWiZustVO ausdrückliche Regelungen der Zuständigkeit für die Ahndung von Ordnungswidrigkeiten gerade für den Bereich der privaten Stellen nach § 43 BDSG in Ziffer 3.5.2 enthält. Im Umkehrschluss kann daraus gefolgert werden, dass in den übrigen Bereichen der Ahndung von Ordnungswidrigkeiten es bei der allgemeinen Zuständigkeit der obersten Landesbehörde nach § 36 Abs. 1 Nr. 2 lit. a OWiG verbleiben sollte,[64] zumal im Bereich des Ordnungswidrigkeitenrechts besondere Anforderungen an das Gebot der Normenklarheit (Bestimmtheitsgebot) zu stellen sind. Auch § 38

---

[62] So auch ULD, Fragen und Antworten zu Anfragen bzgl. der Reichweitenanalyse bei Facebook, Antwort 1 – abrufbar unter: https://www.datenschutzzentrum.de/facebook/ (Stand: 23.09.2011). Siehe auch *Spindler*/*Schuster*, Recht der elektronischen Medien, 2. Aufl. 2011, § 59 Rn. 30.

[63] Davon ausgehend ULD, Fragen und Antworten zu Anfragen bzgl. der Reichweitenanalyse bei Facebook, Antwort 1 – abrufbar unter: https://www.datenschutzzentrum.de/facebook/ (Stand: 23.09.2011). Zustimmend *Piltz*, CR 2011, 657 (663).

[64] Nach § 36 Abs. 2 OWiG können die obersten Landesbehörden die Zuständigkeit auch den direkt verantwortlichen Behörden übertragen; dies geschieht zumeist, wenn sie nicht selbst die Aufsicht wahrnehmen. Vgl. dazu *Gola*/*Schomerus*, BDSG, 10. Aufl. 2010, § 43 Rn. 28 m.w.N.

Abs. 1 BDSG macht mit der Formulierung „Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, (…) den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen (…)“, deutlich, dass nicht davon ausgegangen wird, dass die landesrechtlich bestimmten Aufsichtsbehörden zugleich mit der inhaltlichen Überwachung der datenschutzrechtlichen Anforderungen auch mit der Verfolgung von Verstößen beauftragt sind, obwohl dies sicherlich dem „Geist“ der EU-Datenschutzrichtlinie entsprechen würde, die in Art. 28 Abs. 3 verlangt, dass jede Kontrollstelle über „wirksame“ Einwirkungsbefugnisse verfügen muss.[65]

Für die seitens des ULD in Aussicht gestellten Maßnahmen nach § 43 BDSG sowie § 42 LDSG ist hingegen vom Vorliegen der sachlichen und örtlichen Zuständigkeit auszugehen. Eine Ahndung von etwaigen Verstößen gegen die Informationspflichten aus § 5 TMG über § 16 Abs. 2 Nr. 1 TMG ist dem ULD jedoch verwehrt, da die Zuständigkeit insoweit bei der Medienanstalt Hamburg/Schleswig-Holstein angesiedelt ist. Ob von einer Kompetenz zur Verfolgung von Ordnungswidrigkeiten nach § 16 Abs. 2 Nr. 5 TMG ausgegangen werden kann, ist nicht eindeutig zu beantworten. Das ULD scheint dies insoweit selbst in Betracht gezogen zu haben, wenn es Maßnahmen auf „§ 16 TMG und/oder § 43 BDSG bei privaten Stellen“ stützt. Insofern findet sich auch in der Stellungnahme des ULD zum Entwurf eines Gesetzes zur Änderung des LDSG[66] der Vorschlag eine Klarstellung hinsichtlich der Zuständigkeiten in einem neuen § 44 Abs. 3 vorzunehmen:

> *„(3) Das Unabhängige Landeszentrum für Datenschutz ist für Ordnungswidrigkeiten nach diesem Gesetz Verwaltungsbehörde im Sinne von § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG). Dies gilt auch für Ordnungswidrigkeiten nach § 43 BDSG, nach § 85 SGB X und nach Abschnitt 4 des TMG.“*

II. Verfahren

Abgesehen von den Erfolgsaussichten hinsichtlich des materiellen Gehalts der angedrohten Ordnungswidrigkeitenverfahren (siehe oben), müssten zunächst individuali-

---

[65] Vgl. *Gola*/*Schomerus*, BDSG, 10. Aufl. 2010, § 38 Rn. 32.
[66] Umdr. 17/2896, S. 2.

sierte Verfahren eingeleitet werden. Das Arbeitspapier des ULD und die Pressemitteilung mit der Aufforderung, Fanpages und Social-Plugins bis zum 30. September zu entfernen, kann nicht als Einleitung entsprechender Verfahren verstanden werden, sondern kündigt lediglich die nunmehr exemplarisch begonnenen Verfahren an. Es sind im Übrigen die Verfahrensvorschriften gemäß §§ 46 ff. OWiG einzuhalten.

Es gilt das Opportunitätsprinzip. Die Verfolgung von Ordnungswidrigkeiten liegt im Ermessen der zuständigen Behörde, § 47 Abs. 1 Satz 1 OWiG. Im Zuge des Vorverfahrens ist zu prüfen, ob die Voraussetzungen für ein Ordnungswidrigkeitenverfahren vorliegen. Bei geringfügigen Verstößen kann nach § 56 OWiG zunächst eine Verwarnung ausgesprochen werden oder auch eine Einstellung des Verfahrens über § 47 Abs. 1 Satz 2 OWiG verfügt werden. Andernfalls wird über § 65 OWiG ein Bußgeldbescheid erlassen. Dem Betroffenen steht die Möglichkeit des Einspruchs über § 67 Abs. 1 OWiG innerhalb von zwei Wochen nach Zustellung offen. Dem schließt sich das Zwischenverfahren an, in dem die Verwaltungsbehörde, die Staatsanwaltschaft und das Gericht mit der Sache befasst werden können. Kommt es in diesem Stadium zu keiner Verfahrenserledigung, erfolgt die Überleitung ins gerichtliche Hauptverfahren nach §§ 71 ff. OWiG.

III. Materielle Anforderungen

Soweit trotz der obigen Bedenken (bis auf die möglichen Verstöße gegen § 13 Abs. 4 Nr. 3 und Abs. 5 TMG), von der materiellen Rechtmäßigkeit von Zwangsmaßnahmen und Bußgeldbescheiden ausgegangen werden sollte, müsste in jedem Fall dem Grundsatz der Verhältnismäßigkeit entsprochen werden. Dies betrifft zum einen die Wahl der Mittel (Untersagung oder Bußgeld) sowie die Höhe etwaiger Bußgelder, die in einem angemessenen Verhältnis zum Rechtsverstoß stehen muss. Hierbei wäre insbesondere der in jedem Fall nicht bestreitbaren unterschiedlichen Verteilung der Verantwortlichkeiten Rechnung zu tragen.

Für Rückfragen stehen wir Ihnen selbstverständlich jederzeit gern zur Verfügung.

Mit freundlichen Grüßen
Für den Wissenschaftlichen Dienst

gez. Anika Luch