Neue Zeitschrift für Verwaltungsrecht – Extra

In Zusammenarbeit mit der Neuen Juristischen Wochenschrift

Gegründet von Rechtsanwalt Prof. Dr. Hermann Weber, Schriftleiter von 1982–2001

21 2015

Seite 1–16

34. Jahrgang

1. November 2015

Professor Dr. Mario Martini/Saskia Fritzsche*

Mitverantwortung in sozialen Netzwerken

Facebook-Fanpage-Betreiber in der datenschutzrechtlichen Grauzone

„Alles, was Spaß macht, macht entweder dick, ist verboten oder unmoralisch", klagte einst Alexander Woollcott. Auf den ersten Blick scheint Facebook dafür ein Beleg: Das soziale Netzwerk macht Spaß. Dick macht es zwar nicht, wiewohl es auf einem Zuckerberg gewachsen ist. Manchen gilt es aber jedenfalls als unmoralisch, beruht sein Geschäftsmodell doch auf der exzessiven Datenausbeutung seiner Mitglieder. Facebook ist vieles: Klatschcafé, Beichtstuhl, Kiosk, Nachrichtenagentur und Ball der Eitelkeiten. Eines ist es aber nicht: ein Gralshüter der Privatsphäre. Kritiker geißeln das soziale Netzwerk als Vorhut eines digitalen Imperialismus, ja als Abrissbirne informationeller Selbstbestimmung. Die gesetzliche Forderung, den Nutzern durch Transparenz die Selbstbestimmung über ihre digitalen Fußspuren zu ermöglichen, prallt an dem Internetgiganten aus dem Silicon Valley weitgehend ab. Von Facebooks Datenschutzverstößen unbeeindruckt, machen sich Fanpage-Betreiber die mediale Reichweite und infrastrukturelle Professionalität der Online-Plattform für ihre geschäftlichen Zwecke zunutze. Ob sie deshalb als Ausfallbürgen datenschutzrechtliche Mitverantwortung tragen, harrt einer Klärung. Dieser Frage geht der Beitrag nach. Er entwickelt einen neuen Lösungsvorschlag für die Verantwortungszurechnung in arbeitsteiligen Kooperationsstrukturen sozialer Netzwerke.

I. Facebook und der Datenschutz – eine spannungsreiche Beziehung

Prüfen ist erlaubt, widersprechen nicht! Dieser Losung hatte sich Facebook verschrieben, als es am 30.1.2015 die Nutzungsbedingungen für sein soziales Netzwerk änderte. Seinen Mitgliedern ließ es keine echte Wahl: Wer sein Facebook-Alter-Ego nicht zu Grabe tragen und die kollektive Autobiografie weiter nutzen wollte, musste die neuen AGB akzeptieren. Ob erweiterte Auswertung von Standortdaten, umfassendes Tracking auf allen Internetseiten mit Facebook-Plugins (wie zB Like-Button oder Facebook-Login)[1] oder Datenaustausche mit den Facebook-Schwestern WhatsApp und Instagram:[2] Das erste Einloggen wertete Facebook automatisch als Zustimmung des jeweiligen Nutzers zu allen Änderungen. Die nach § 4 a BDSG geforderte informierte Einwilligung wird so zur Fiktion. Landauf, landab üben Datenschützer harsche Kritik.[3]

Die Informationen zu den Vorlieben und dem Verhalten seiner Nutzer, die Facebook sammelt, wertet es umfassend aus. Dazu setzt das soziale Netzwerk insbesondere Cookies[4]

* *Mario Martini* ist Inhaber eines Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer. *Saskia Fritzsche* ist Forschungsreferentin am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer im Programmbereich „Digitale Transformation des Staates".

Die Autoren danken *Michael Kolain* und *Benjamin Kühl* für ihre hilfreiche Unterstützung. Die Internetquellen wurden zuletzt am 30.7.2015 aufgerufen.

1 Der entsprechende Passus in der Facebook-Datenschutzrichtlinie (abrufbar unter https://de-de.facebook.com/about/privacy/) lautet: „Wir sammeln Informationen, wenn du Webseiten und Apps Dritter besuchst, die unsere Dienste nutzen (zB wenn sie unsere „Gefällt mir"-Schaltfläche oder die Facebook-Anmeldung anbieten oder unsere Bewertungs- und Werbedienste nutzen)".

2 Vgl. die Klauselüberschrift „Teilen innerhalb der Facebook-Unternehmen" der Facebook-Datenschutzrichtlinie (vgl. o. Fn. 1).

3 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat ein Prüfverfahren eingeleitet (vgl. *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, Facebooks neue Datenrichtlinie tritt heute in Kraft, 30.1.2015, https://www.datenschutz-hamburg.de/news/detail/article/facebooks-neue-datenrichtlinie-tritt-heute-in-kraft.html), der Verhandlungsführer des Europäischen Parlaments für die Datenschutz-Grundverordnung *Jan-Philipp Albrecht* kritisiert das Vorgehen Facebooks als „schlichte Erpressung und mit den Datenschutzbestimmungen in der EU unvereinbar" (vgl. *Albrecht*, Facebook missbraucht seine Stellung als quasi-Monopolist!, 29.1.2015, http://www.janalbrecht.eu/presse/pressemitteilungen/facebook-missbraucht-seine-stellung-als-quasi-monopolist.html) und der frühere Bundesdatenschutzbeauftragte *Peter Schaar* ist seit dem 30.1.2015 nicht mehr Mitglied in dem sozialen Netzwerk (vgl. *Schaar*, Facebook: Jede große Reise beginnt mit einem kleinen Schritt, 2.2.2015, http://www.eaid-berlin.de/?p = 571). Er zeigt dem Zuckerberg-Konzern auf diese Weise eine persönliche rote Karte dafür, im Spiel um Nutzerdaten die Außenlinien des datenschutzrechtlichen Graubereichs (erneut) überschritten zu haben.

4 Cookies sind kleine Datensätze, die ein Webserver auf dem Rechner des Internetnutzers bzw. in dessen Browser speichert. Besucht der Internetnutzer die Website erneut oder ruft er ein anderes von dem Webserver gehostetes Element auf, so ermöglicht der Cookie eine Wiedererkennung des Nutzers.

und speichert IP-Adressen sowie Browser-Fingerprints[5] – gleichgültig ob es sich bei den Besuchern um angemeldete Facebook-Mitglieder handelt oder nicht. Bei der Analyse dieser Nutzungsdaten[6] greift Facebook auch großvolumig auf die als Profilinformationen gespeicherten Bestands- und Inhaltsdaten[7] (bspw. Adressen, Beziehungsstatus, Geschlecht, Chat-Nachrichten, Fotos, Freundschaftsanfragen, Pinnwand-Einträge) der registrierten Fanpage-Besucher zu.[8]

Persönlichkeitsanalysen registrierter Facebook-Nutzer kommen so schon heute den Persönlichkeitsbeschreibungen durch Freunde, Familienangehörige oder sogar Ehepartner nicht nur gleich – sie sind diesen ab einer kritischen Schwelle von Facebook-Likes sogar überlegen.[9] Aus den „Gefällt mir"-Klicks lassen sich durch entsprechende Algorithmen mit hoher Treffsicherheit Geschlecht, ethnische Zugehörigkeit, sexuelle Orientierung und politische Einstellung herauslesen.[10]

1. Facebooks Datenschutzverstöße

Facebooks Datenverarbeitungspraktiken weisen in vielerlei Hinsicht datenschutzrechtliche Mängel auf: Weder informiert das Unternehmen die Nutzer in hinreichend transparenter und detaillierter Form über die im Nutzerprofil gespeicherten Daten bzw. Datenarten (§ 13 I TMG),[11] noch räumt es ihnen eine Möglichkeit ein, der Erstellung pseudonymisierter Nutzungsprofile zu widersprechen (§ 15 III 1 aE, 2 TMG).[12] Der Internetgigant nutzt die Profildaten ohne hinreichende Einwilligung, um die Zugehörigkeit zu einer merkmals- oder kundendatendefinierten[13] Zielgruppe für Werbezwecke zu ermitteln.[14] Entgegen § 15 III 3 TMG verknüpft Facebook Daten aus Nutzungsprofilen mit den Trägern von Pseudonymen zu einem Klarnamen-Personenprofil.

Facebook kann sich auch nicht mehr (wie in der Vergangenheit)[15] mit Erfolg auf die Unanwendbarkeit deutschen Datenschutzrechts berufen. Vielmehr ist das Unternehmen jedenfalls in der Deutung des *EuGH* den Vorgaben des nationalen Datenschutzrechts unterworfen.[16] In seinem so genannten Google-Urteil[17] etabliert dieser faktisch ein datenschutzrechtliches Marktortprinzip: Für die Anwendbarkeit nationalen Datenschutzrechts reicht eine zwar andernorts in der EU stattfindende, aber auf das Inland gerichtete Datenverarbeitungstätigkeit eines Unternehmens aus, sofern es in dem Mitliedstaat über eine Niederlassung verfügt, die der Förderung des Verkaufs personalisierter Werbeeinblendungen verschrieben ist.[18]

2. Fanpage-Betreiber und die Ernte vom Baum der Erkenntnis

Zu dem virtuellen Schlaraffenland seiner Daten gewährt Facebook – neben seinen Werbekunden[19] – einer Nutzergruppe privilegierten Zutritt: den Betreibern von Fanpages. Fanpages sind die Benutzeraccounts von Unternehmen, Prominenten oder öffentlichen Einrichtungen, die für ihre Firma, Marke,

5 Der so genannte Browser-Fingerprint bildet die Spuren ab, die der Nutzer in seinen Browser-Einstellungen hinterlässt. Anhand der Vorgaben, die der Nutzer für den Umgang mit Cookies, installierten Plugins, Spracheinstellungen etc trifft, lassen sich Rückschlüsse auf seine Identität ziehen. Schätzungen zufolge sind 93 % aller Browser-Fingerprints auf Grund ihrer Einzigartigkeit einer Identifizierung zugänglich (vgl. *Tillmann*, Browser Fingerprinting: Tracking ohne Spuren zu hinterlassen, 20.10.2013, 85, 103). Zur Einzigartigkeit von Fingerprints s. auch die von *Eckersley*, How Unique Is Your Web Browser?, in *Atallah/Hopper*, Privacy Enhancing Technologies, 2010, 1 vorgestellten Ergebnisse des Panopticlick-Forschungsprojekts der Electronic Frontier Foundation (EFF). 83,6 % von 470.161 getesteten Browsern wiesen danach einen einzigartigen Fingerprint auf. Unter denjenigen Browsern, die Adobe Flash oder Java installiert hatten, zeichneten sich sogar 94,2 % durch einen unverwechselbaren Fingerabdruck aus. Zwar haben die Forscher dabei auch eine hohe Veränderungsdynamik der Fingerprints festgestellt. Der Wiedererkennbarkeit stand dies aber nicht entgegen: Mithilfe eines Algorithmus ließen sich die veränderten Fingerprints in 99,1 % dem ursprünglichen (Stamm-)Fingerprint zuordnen (*Eckersley*, 1 ff.). Vgl. auch die Informationen des Vereins *europe-v-facebook.org* zum Facebook-Datensatz „Recent Activities", abrufbar unter http://europe-v-facebook.org/DE/Datenbestand/datenbestand.html.

6 Unter Nutzungsdaten versteht das TMG alle Daten, die bei der Inanspruchnahme eines Telemediendienstes notwendig anfallen bzw. die Bereitstellung des Telemediendienstes und seine Abrechnung ermöglichen (§ 15 I TMG), vgl. *Runte* in *Lehmann/Meents*, HdB d. Fachanwalts Informationstechnologierecht, 2. Aufl. 2010, Kapitel 20 Rn. 191 ff.; *Spindler/Nink* in *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 15 TMG Rn. 2.

7 Inhaltsdaten sind (im Unterschied zu Nutzungsdaten) solche personenbezogenen Angaben, die nicht die Inanspruchnahme des Telemediendienstes ermöglichen oder für die Abrechnung des Telemediendienstes erforderlich sind, sondern den Inhalt der Kommunikation selbst bilden (vgl. *Heckmann* in *Heckmann*, jurisPK-Internetrecht, 4. Aufl. 2014, Kapitel 9 – Datenschutz Rn. 172; *Hullen/Roggenkamp* in *Plath*, BDSG, 2013, § 15 TMG Rn. 12). Vgl. zur Abgrenzung zwischen den dadurch jeweils berührten gesetzlichen Regelungsmaterien auf der Grundlage des Schichtenmodells etwa *Martini*, Datenschutz und Sicherheit bei der elektronischen Rechnung in *Rogall-Grothe*, Leitfaden Elektronische Rechnung in der öffentlichen Verwaltung, 2014, 51 (72 f.); *Spindler/Nink* (vgl. o. Fn. 6), 15 TMG Rn. 3.

8 Vgl. dazu insgesamt *Karg/Thomsen*, DuD 2012, 729.

9 Vgl. *Youyoua/Kosinski/Stillwell*, PNAS 112 (2014), 1036 ff.

10 Vgl. *Stillwell/Graepel*, PNAS 110 (2013), 5802 (5803 f.). Dabei handelt es sich (bis auf das Merkmal „Geschlecht") um besondere personenbezogene, also sensitive Daten iSv § 3 IX BDSG.

11 Vgl. dazu die Ausführungen in der Klagschrift des Sammelklageverfahrens *Schrems/Facebook Ireland Ltd.* Rn. 67 ff., abrufbar unter http://www.europe-v-facebook.org/sk/sk.pdf.

12 Dazu *Karg/Thomsen*, DuD 2012, 729 (735 f.). Ob Facebook auch nach den Vorgaben des zukünftigen europäischen Datenschutzrechts zur Einräumung einer Widerspruchsmöglichkeit und entsprechender Belehrung verpflichtet ist, hängt davon ab, ob die Verarbeitung von Nutzungsdaten zu pseudonymisierten Nutzungsprofilen zum Zwecke der personalisierten Werbung als Direktwerbung iSv Art. 19 II DSGVO-E einzustufen ist. Die Funktionalität des Widerspruchsrechts als datenschutzrechtliches Werkzeug im Zusammenhang mit dem Profiling unterstreichend *Härting*, CR 2014, 528 (533).

13 Vgl. dazu die Facebook-Targeting-Funktionen „Custom Audiences" (https://de-de.facebook.com/business/learn/facebook-ads-custom-audiences/) und „Lookalike-Audiences" (https://de-de.facebook.com/business/learn/facebook-ads-lookalike-audiences/).

14 Vgl. *Karg/Thomsen*, DuD 2012, 729 (735) sowie das laufende Auskunftsersuchen des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, das insbesondere die Wirksamkeit der Nutzereinwilligung in Facebooks Datenverarbeitung infrage stellt, vgl. die Pressemitteilung der Behörde v. 28.7.2015, https://www.datenschutz-hamburg.de/news/detail/article/facebooks-neue-datenrichtlinie-tritt-heute-in-kraft.html?tx_ttnews[backPid] = 188&cHash = 79550ce104a2f3cb9fd62dddb739b5ea.

15 Vgl. *OVG Schleswig*, NJW 2013, 1977; *VG Schleswig*, ZD 2013, 245.

16 Daher sieht sich Facebook trotz der im Jahr 2013 erfolgreich abgewehrten Verwaltungsanordnung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein erneut unter Berufung auf § 13 VI 1 TMG mit einer Anordnung zur Aufhebung der Klarnamenpflicht des Netzwerks (diesmal des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit) konfrontiert, vgl. *Redaktion beck-aktuell*, Hamburger Datenschützer geht wegen Klarnamen-Pflicht gegen Facebook vor, becklink 2000713 v. 29.7.2015.

17 *EuGH*, NJW 2014, 2257 = NVwZ 2014, 857.

18 *EuGH*, NJW 2014, 2257 Rn. 45 ff. = NVwZ 2014, 857. Die Facebook Germany GmbH ist laut Eintragung im Handelsregister für die Akquise von Anzeigen und die Bereitstellung von Marketingfunktionen für das soziale Netzwerk in Deutschland zuständig (vgl. Bekanntmachung des *AG Hamburg* v. 16.12.2009 zum Az. HRB 111963 im Gemeinsamen Registerportal der Länder, https://www.handelsregister.de/rp_web/direct-download.do; jsessionid = 661BB3C285D99558F791D3DE8E6968FA. tc04n04?id = 0). Sie fungiert damit ähnlich wie Google Spain als Bindeglied zum datennachfragenden Werbemarkt. Es handelt sich bei ihr folglich um eine Inlandsniederlassung iSv § 1 V 1 BDSG, für die deutsches Recht gilt und für die eine Zuständigkeit deutscher Aufsichtsbehörden besteht. Das gilt nicht nur für das allgemeine, sondern auch für das bereichsspezifische Datenschutzrecht (vgl. § 3 III Nr. 4 iVm § 12 III TMG), vgl. dazu auch die Ausführungen zu II. 2. a) bb) (2) mit Fn. 120; ferner *Petri*, ZD 2015, 103 (104).

19 Vgl. dazu die Facebook-Informationen zu Seitenstatistiken unter https://de-de.facebook.com/help/336893449723054 sowie Nr. 10 der Facebook-Erklärung der Rechte und Pflichten, abrufbar unter https://de-de.facebook.com/terms.php?locale = DE.

Person oder Organisation einen Facebook-Auftritt betreiben. Ihnen stellt Facebook unaufgefordert eine fortlaufende Reichweitenanalyse, so genannte Facebook Insights,[20] zur Verfügung. Sie enthält in aggregierter und anonymisierter Form insbesondere Informationen zur Demographie der Nutzer, zu Zugriffshäufigkeiten (so genannte „Pageviews") sowie zur Viralität einzelner Beiträge.

Fanpage-Betreiber machen sich Facebooks Reichweite und infrastrukturelle Professionalität für ihre geschäftlichen Zwecke[21] zunutze. Sie bedienen sich des sozialen Netzwerks somit auch, um über seine Datenmaschinerie an Informationen zu gelangen, die sie selbst in der Regel nicht oder jedenfalls nicht zu gleichen Kosten generieren könnten. Sie sind einerseits Nutznießer des datenfinanzierten Geschäftsmodells, zugleich aber auch Hilfsmotoren für das Datenaufkommen des sozialen Netzwerks. Die Marketing-, PR- und Marktforschungseinsparungen, die Fanpage-Betreiber mit der kostenfreien Nutzung der Facebook-Infrastruktur erzielen, finanzieren ihre Besucher in einem Dreiecksverhältnis durch die Preisgabe zahlreicher personenbezogener Daten gegen. Der Informationsfluss, den Fanpages als Mittel der Öffentlichkeitsarbeit und Kundenkommunikation erzeugen, fördert Facebooks Besuchs- und Klickzahlen nachhaltig.

Das darin liegende Pfund ihres Droh- und Druckpotenzials werfen weder Unternehmen noch Behörden als Fanpage-Betreiber im Interesse des Datenschutzes in die Waagschale. Im Gegenteil: Die Bundesregierung hat ihre Fanpage just drei Wochen im Nachgang zur AGB-Änderung gelauncht.[22] „Profitieren statt Protestieren" lautet das Leitmotiv der Social-Media-Manager im privatwirtschaftlichen wie im öffentlichen Bereich.

3. Datenschutzrechtliche Mitverantwortlichkeit als Kehrseite des Nutzungsvorteils?

Das Szenario, in dem Facebook den Fanpage-Betreibern Reichweitenanalysen zur Verfügung stellt, erinnert – in den Worten von *Heinrich Heine* – ein wenig an „das alte Liedchen von der Schlang' im Paradies, die durch (…) Apfelgabe unsern Ahn' ins Elend stieß". Während Datenschützer noch mahnen: „Von dem Baum der Erkenntnis […] sollst du nicht essen",[23] lassen die Fanpage-Betreiber sich stärker von Facebooks Lockruf inspirieren: „An dem Tage, da ihr davon esst, werden eure Augen aufgetan".[24]

Inwieweit dürfen aber Fanpage-Betreiber die Früchte vom Baum der Erkenntnis unbekümmert ernten? Verlieren sie durch ihre Datenlese die rechtliche Unschuld – oder sind sie nur unbescholtener Gast bei Facebooks All-you-can-eat-Datenbuffet? Indem Fanpage-Betreiber von den Früchten der Datenschutzpraxis des Internetkonzerns profitieren, sind sie womöglich für dessen Rechtsverstöße im Umgang mit personenbezogenen Daten mitverantwortlich.

Die Zuweisung einer solchen Mitverantwortlichkeit halten viele Datenschützer für einen wirksamen Appetitzügler, um dem sorglosen Griff nach Facebook-Daten Einhalt zu gebieten. Denn sie senkt nicht nur für die Betreiber die Attraktivität der kostenlosen Portalnutzung. Die drohenden Reichweitenverluste und wirtschaftlichen Einbußen setzen auch Facebook Anreize, seine Verarbeitungspraxis datenschutzkonform zu gestalten.

4. Der Fanpage-Rechtsstreit vor dem VG und OVG Schleswig

Ob den Fanpage-Betreibern im System des Datenschutzrechts *de lege lata* eine Mitverantwortung zukommt, ist bislang nicht geklärt. Auch insoweit verhält es sich ähnlich wie in der Schöpfungsgeschichte: Adam verweist auf Eva und Eva auf die Schlange. Das Unabhängige Landeszentrum für den Datenschutz in Schleswig-Holstein (ULD) wollte sich mit dem Verweis auf die „Schlange" Facebook nicht abfinden. Es hat, da Facebook in seiner datenschutzrechtlichen Forum-Shopping-List bislang nur schwer zu greifen war, Fanpage-Betreiber gleichsam als Ausfallbürgen zur Verantwortung gezogen. Zu diesem Zweck hat es ein Musterverfahren gegen die Wirtschaftsakademie Schleswig-Holstein GmbH angestrengt. Seit 2010 bietet diese ihren Ausbildungsinteressenten, Schülern, Ehemaligen und Partnern die Möglichkeit, sich nicht nur über die offizielle Unternehmenswebsite, sondern auch auf einem Facebook-Profil der Akademie über Neuigkeiten auf dem Laufenden zu halten.

Über ihre Fanpage erreicht die Wirtschaftsakademie, die den Aus- und Weiterbildungsauftrag der Industrie- und Handelskammern Flensburg, Kiel und Lübeck wahrnimmt, insbesondere diejenigen Altersgruppen, für die ihre Bildungsangebote von besonderem Interesse sind. Hier postet sie Veranstaltungstermine, informiert über Weiterbildungs- und Stellenangebote, gratuliert Absolventen zum erfolgreichen Abschluss und bietet eine Plattform für Nutzerbeiträge, -kommentare und -likes. Die Facebook-Fanpage ist ein wichtiger Kommunikations- und Vertriebskanal des Kieler Bildungsunternehmens.

So verwundert es auch nicht, dass lauter Protest erschallte, als das ULD Ende 2011 die Deaktivierung der Fanpage verfügte und die Wirtschaftsakademie damit von Facebooks Datenfluss abschneiden wollte. Auf der Grundlage des § 38 V BDSG legte die Datenschutzaufsichtsbehörde dem Bildungsunternehmen die Verpflichtung auf, den Betrieb der Fanpage einzustellen. Für die Wirtschaftsakademie war das ein Schlag ins Kontor ihrer Kommunikationsstrategie. Sie fürchtete eine Benachteiligung im Wettbewerb mit anderen Unternehmen.

Das *VG Schleswig* hielt den Bescheid des ULD für rechtswidrig und hob ihn auf.[25] Dabei ließ es offen, ob die Daten, die Facebook erhebt, personenbezogener Natur sind und ob das Fanpage-Angebot gegen datenschutzrechtliche Informationspflichten verstößt. Es sprach der Wirtschaftsakademie jedenfalls eine (Mit-)Verantwortlichkeit für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch Facebook ab.[26]

Das *OVG Schleswig*[27] ist dieser Einschätzung uneingeschränkt gefolgt. Es zeichnete die Fanpage-Betreiber von einer datenschutzrechtlichen Mitverantwortlichkeit frei. Zwar attestierte es dem sozialen Netzwerk Rechtsverstöße bei der Datenverarbeitung. Eine Grundlage dafür, Unternehmen eine Deaktivierung ihrer Fanpage abzuverlangen, vermochte es jedoch nicht zu erkennen. Die Herrschaft über die Daten sah das Gericht alleine in den Händen der Facebook Ireland Limited, des europäischen Headquarters des Internetkon-

20 Zu diesem Tool s. *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (123); *Sebastian*, Facebook Fanpages plus, 2012, 248 ff.; *Weinberg*, Social Media Marketing, 4. Aufl. 2014, 239 f.

21 Für rein persönliche und familiäre Tätigkeiten greift die Bereichsausnahme des § 1 II Nr. 3 BDSG. Anders als kommerzielle Fanpage-Betreiber sind sie dem BDSG grundsätzlich nicht unterworfen.

22 Seit dem 20.2.2015 ist die Bundesregierung unter https://de-de.facebook.com/Bundesregierung in dem sozialen Netzwerk vertreten.

23 Genesis 2, 17.

24 Genesis 3, 5.

25 Vgl. *VG Schleswig*, ZD 2014, 51. Dazu etwa *Karg*, ZD 2014, 54; *Pieper/Krügel*, ZD-Aktuell 2013, Heft 21, 3831.

26 *VG Schleswig*, ZD 2014, 51 (52 f.).

27 *OVG Schleswig*, ZD 2014, 643.

zerns. Sie allein bestimme, „ob“, „warum“ und „wie“ sie (Nutzungs-)Daten erhebt und verarbeitet.[28]

„Eine Katastrophe und ein Rückschlag für den Datenschutz,“ kommentierte der seinerzeitige Leiter des ULD, *Thilo Weichert*, die Entscheidung.[29] Sowohl Fanpage-Betreiber als auch Medienrechtler spendeten dem Urteil des *OVG Schleswig* demgegenüber Beifall.[30] „Statt der Juristen und Datenschützer sitzen jetzt die Kommunikations- und Marketingfachleute auf den Fahrersitzen. Gefällt mir“, würdigte etwa der IT-Rechtsanwalt *Niko Härting* die erstinstanzliche Entscheidung.[31]

Doch noch ist der Urteilsspruch aus dem hohen Norden nicht das letzte Wort der Vertreibung aus dem Facebook-Datenparadies. Das ULD hat gegen das Urteil Revision eingelegt. Voraussichtlich im Dezember wird das *BVerwG* letztinstanzlich entscheiden, ob Fanpage-Betreiber zu dem Kreis der datenschutzrechtlich Verantwortlichen zählen.

Der Präzedenzfall gibt Anlass, die Figur der Mitverantwortlichkeit in sozialen Netzwerken unter das analytische Mikroskop zu legen. Am Beispiel der Facebook-Fanpage ordnet der Beitrag die Verantwortungsstrukturen bei arbeitsteiligen Verarbeitungsprozessen sozialer Netzwerke in den Kontext allgemeiner Verantwortungstatbestände des Ordnungsrechts ein. Er unternimmt einen Streifzug durch die Zurechnungskategorien, insbesondere die Störer- sowie die ordnungsrechtliche Zweckveranlasserhaftung. Auf dieser Grundlage entwickelt der Beitrag einen neuen, zwischen privaten und öffentlichen Fanpage-Betreibern differenzierenden Lösungsansatz für die Mitverantwortlichkeit in sozialen Netzwerken.

II. Fanpage-Betreiber als Ausfallbürgen für Datenschutzverstöße?

Wer eine Fanpage betreibt, bietet einen Telemediendienst an (§ 2 S. 1 Nr. 2 TMG).[32] Sein Handeln unterwerfen die §§ 12 ff. TMG bereichs- bzw. medienspezifischen datenschutzrechtlichen Bindungen. Soweit der Diensteanbieter *selbst* personenbezogene Daten erhebt, ist er insbesondere den Informationspflichten und dem Widerspruchsrecht der §§ 13 I, III, 15 III TMG ausgesetzt.

Greift er auf *Leistungen Dritter*, etwa Facebooks, zurück, reicht seine Verantwortlichkeit allerdings nur so weit, wie das allgemeine Datenschutzrecht sie ihm zuordnet. Das ergibt sich aus der Verweisung des § 12 III TMG auf das allgemeine Datenschutzrecht.[33] Für Facebooks Datenschutzverstöße bei der Verarbeitung von Nutzungsdaten ist der Fanpage-Betreiber also grundsätzlich nur dann mitverantwortlich, wenn das BDSG (bzw. das jeweils einschlägige LDSG) eine entsprechende Verantwortlichkeit auslöst.

1. Fanpage-Betreiber als verantwortliche Stelle iSv § 3 VII BDSG

Das BDSG versteht die datenschutzrechtliche Verantwortlichkeit grundsätzlich weit. Verantwortlich ist nicht nur, wer den Datenumgang formal nach außen vertritt, sondern jeder, der in tatsächlicher Hinsicht als „Herr der Daten“ auf den Verarbeitungsvorgang steuernd einzuwirken in der Lage ist.[34] Das Gesetz verlangt eine Einflussnahme- und Kontrollmöglichkeit über Zweck und Mittel der Datenverarbeitung, also über das „Warum“ (dh das erwartete und beabsichtigte Ergebnis) und das „Wie“ (dh die Art und Weise, das Ziel zu erreichen).[35]

a) *Fanpage-Betreiber als Verarbeiter von Nutzungsdaten?* Fanpage-Betreiber können weder auf die Funktionen der Fanpage noch auf die Steuerung des Datenflusses oder die Verarbeitung der Datenspuren, welche ihre Besucher hinterlassen, einwirken.[36] Nur Facebook selbst ist bekannt, in welcher Weise und in welchem Ausmaß es Nutzungsdaten verarbeitet. Anders als der Anbieter einer selbstständigen Online-Präsenz, der aus eigener Entscheidung Werbenetzwerken die Platzierung von Tracking-Pixeln auf seiner Website zwecks personalisierter Werbung erlaubt (so genanntes Behavioural Online Targeting)[37] oder Facebook-Plugins wie den „Gefällt mir“-Button in sein Online-Angebot einbindet,[38] hat der Fanpage-Betreiber auch nicht die Wahl, seine Fanpage ohne Facebook-Cookies anzubieten oder den Datenfluss an Facebook mittels einer Zwei-Klick-Lösung[39] von der Bestätigung des Nutzers abhängig zu machen.[40] Der Einfluss des Fanpage-Betreibers beschränkt sich vielmehr auf die grundsätzliche Entscheidung, eine Fanpage bereitzustellen, sowie

28 *OVG Schleswig*, ZD 2014, 643 (644).
29 Vgl. *ULD Schleswig-Holstein*, OVG Schleswig: Rechtssicherheit für Betreiber – nicht für die Betroffenen, 5.9.2014, https://www.datenschutzzentrum.de/presse/20140905-ovg-sh-urteil-facebook.htm.
30 Vgl. etwa *Dammann* in *Simitis*, BDSG, 8. Aufl. 2014, § 3 Rn. 224; *Moos*, Update Datenschutz in *Taeger*, Big Data & Co, 2014, 525 (536 ff.); *Werkmeister/Schröder*, ZD 2014, 645.
31 *Härting*, K & R 2013, 828 aE.
32 *OVG Schleswig*, ZD 2014, 643 (644); vgl. auch *OLG Düsseldorf*, MMR 2014, 393; *LG Aschaffenburg*, MMR 2012, 38 (38); *LG Regensburg*, MMR 2013, 246 (246 f.); Dazu auch *Martini* in *Gersdorf/Paal*, BeckOK InfoMedR, Ed. 7 (Stand: 1.2.2015), § 2 TMG Rn. 18 mwN; *Micklitz/Schirmbacher* in *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 5 TMG Rn. 19.
33 Vgl. *OVG Schleswig*, ZD 2014, 643 (644). Siehe dazu auch *Heckmann* (vgl. o. Fn. 7), Kap. 9 Rn. 186 ff.; *Hullen/Roggenkamp* in *Plath*, BDSG, 2013, § 12 TMG Rn. 32; *Piltz*, K & R 2014, 80 (84); *Spindler/Nink* in *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 12 TMG Rn. 8; *Weichert* in *Däubler/Klebe/Wedde/Weichert*, BDSG, 4. Aufl. 2013, Einl. Rn. 72 f.
34 Deshalb ist auch der Betreiber eines Internetforums für Datenübertragungen verantwortlich, selbst wenn nicht er selbst, sondern außenstehende Dritte die personenbezogenen Daten einstellen, vgl. *OLG Hamburg*, NJW-RR 2011, 1611 (1612) = GRUR-RR 2012, 40. Zum funktionellen Konzept der Verantwortlichkeit iSd § 3 VII BDSG auch *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortliche“ und „Auftragsverarbeiter“, WP 169, 16.2.2010, 12 und 14.
35 *OVG Schleswig*, ZD 2014, 643 (644); *VG Schleswig* ZD 2014, 51 (53).
36 Vor einem daraus abgeleiteten „datenschutzrechtlichen Blanko-Dispens“ warnend *Caspar*, ZD 2015, 12 (13).
37 In dieser Konstellation eine datenschutzrechtliche (Mit-)Verantwortlichkeit des Inhalteanbieters bejahend *Artikel-29-Datenschutzgruppe* (vgl. o. Fn. 34), 13 f. Zum Behavioural Targeting s. auch *Artikel-29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, WP 171, 22.6.2010; *Arning/Moos*, ZD 2014, 242 (243 f.); *Himmels*, Behavioural Targeting im Internet, 2013; *Zeidler/Brüggemann*, CR 2014, 248.
38 Zur datenschutzrechtlichen Bewertung dieser Konstellation s. etwa *Ernst*, NJOZ 2010, 1917 (1917 ff.) = NJW 2010, 2989; *Laue*, DSB 6/2011, 11; *Heckmann* (vgl. o. Fn. 7), Kap. 9 Rn. 489 ff. sowie mit umfangreicher technischer Analyse, aber nur teilweiser Differenzierung zwischen Fanpage-Betrieb und Social-Plugin-Einbindung *Karg/Thomsen*, DuD 2012, 729 (731 ff.). Die datenschutzrechtliche Verantwortlichkeit der Website-Betreiber verneinend *Piltz*, CR 2011, 657 (662). Mit besonderem Augenmerk auf die Einbindung von Social Plugins in Behördenwebsites demgegenüber *Martini/Fritzsche*, VerwArch. 104 (2013), 449 (453 ff.). Unter Berufung auf die Verantwortlichkeit der Website-Betreiber gehen neben den Aufsichtsbehörden unterdessen auch einige Verbraucherschutzverbände gegen zahlreiche Unternehmen vor, die den „Gefällt mir“-Button ohne zusätzliche Datenschutzvorkehrungen integriert haben, vgl. die Pressemitteilung der Verbraucherzentrale Nordrhein-Westfalen vom 21.5.2015 zum Vorgehen gegen Unternehmen (http://www.vz-nrw.de/webseiten-von-sechs-unternehmen-abgemahnt–daumen-runter-fuer-gefaellt-mir-button). Ob § 13 TMG eine das Marktverhalten regelnde Norm iSd § 8 III Nr. 2 UWG ist, also (jedenfalls auch) die wettbewerbliche Entfaltung des Mitbewerbers schützt, ist freilich umstritten; dazu *KG*, MMR 2011, 464 (465) = NJW-RR 2011, 1264; *OLG Hamburg*, GRUR-RR 2013, 482 (484); *LG Frankfurt a. M.*, ZD 2015, 136.
39 Zu dieser s. *Solmecke*, Teil 21. 1 – Social Media in *Hoeren/Sieber/Holznagel*, Handbuch Multimedia-Recht, 41. EL (März 2015) Rn. 30; *Venzke-Caprese*, DuD 2013, 775; *Venzke*, DuD 2011, 387 (391).
40 Vgl. zu dieser Differenzierung auch *OVG Schleswig*, ZD 2014, 643 (644).

auf die Auswahl der Inhalte, die er darauf veröffentlicht. Er tritt grundsätzlich nur als Front-End-Inhalteanbieter und Datenlieferant ohne Entscheidungsmacht über die Back-End-Datenverarbeitung des eigentlichen Datenherrn Facebook in Erscheinung.[41] Der tatsächliche Einfluss, den die Fanpage-Betreiber ausüben, genügt – mit der Elle des § 3 VII BDSG gemessen – mithin nicht den Anforderungen an eine Entscheidung über die Datenverarbeitung. Vielmehr trifft Facebook seine Entscheidung über das „Ob" und „Wie" der Datenerhebung unabhängig von der Bedeutung, welche der einzelnen Fanpage als Anziehungsfaktor des sozialen Netzwerks zukommt.

aa) *Eigener Geschäftszweck als Anknüpfungspunkt einer datenschutzrechtlichen Mitverantwortlichkeit der Fanpage-Betreiber?* Während das BDSG das komplexe Zusammenspiel von Diensteanbietern, technischer Infrastrukturebene und Inhalterstellern im Web 2.0 entlang linearer Vertrags-, Nutzungs- und Auftragsbeziehungen konstruiert,[42] ist Art. 2 Buchst. d EG-Datenschutz-RL für kollaborative Verantwortungsstrukturen offener.[43] Er lässt eine gesamthänderische Verantwortung arbeitsteilig agierender Diensteanbieter ausdrücklich zu: Es genügt, dass die Stelle „allein oder gemeinsam mit anderen über Zweck und Mittel der Datenverarbeitung entscheidet". Jedenfalls bei richtlinienkonformer Auslegung ist dementsprechend auch nach deutschem Recht eine *gesamthänderische* Verantwortlichkeit bzw. eine pluralistische Kontrolle[44] denkbar.[45]

Die Entscheidungsgewichte können dabei auch ungleichmäßig verteilt sein. Ein *rein tatsächlicher Einfluss* auf die Erhebung und Verarbeitung personenbezogener Daten kann ausreichen[46] – nicht aber eine bloße Mitursächlichkeit für das Aufkommen bzw. tatsächliche Anfallen personenbezogener Daten.[47]

Immerhin verfolgt der Betreiber einer Fanpage regelmäßig auch das Ziel, zusätzliches Marktwissen über Kunden, Interessenten und Fans in Erfahrung zu bringen. Diese Motivation korrespondiert mit der Erwartung, Facebook werde die bei Nutzung der Fanpage anfallenden Daten iSv § 30 I BDSG geschäftsmäßig erheben und verarbeiten, um sie (als Facebook Insights) in aggregierter, anonymisierter Form ua an die Fanpage-Betreiber zu übermitteln. Die Einrichtung der Fanpage verbinden ihre Betreiber also *subjektiv* mit der (Neben-) Zweckbestimmung, Facebooks Datenverarbeitung zu ermöglichen. Die damit verbundenen Datenschutzverstöße nehmen sie billigend in Kauf. Das genügt in der Wahrnehmung zahlreicher Datenschützer, allen voran des ULD,[48] um eine datenschutzrechtliche Mitverantwortlichkeit der Fanpage-Betreiber auszulösen.[49] Der Fanpage-Betreiber partizipiere an Facebooks Datenerhebung und -verarbeitung, die er intendiere,[50] und entscheide demnach über die Zwecke der (Nutzungs-) Datenverarbeitung mit.

So überzeugend diese Argumentation auf den ersten Blick auch erscheint: Mit dem Konzept datenschutzrechtlicher Verantwortlichkeit, das Art. 2 Buchst. d EG-Datenschutz-RL und § 3 VII BDSG etablieren, stimmt sie nicht überein. Denn auch die Richtlinie legt der Verantwortlichkeit *objektive* Bezugspunkte zu Grunde. Entscheidend ist, bei wem *de facto*[51] die Verantwortung für die Verarbeitung, also die Verfügungs- oder Entscheidungsmacht, liegt.[52] Es braucht eine tatsächliche[53] oder rechtliche Einflussnahme- und Kontrollmöglichkeit über Zweck und Mittel, also über das „Warum" und das „Wie" der Datenverarbeitung.[54] Auf *subjektive* Elemente, wie die Motivation oder Erwartungshaltung des Fanpage-Betreibers, kommt es nicht an.[55] Über die Mittel und Zwecke der Datenverarbeitung entscheidet alleine Facebook. Es liefert dem Fanpage-Betreiber lediglich anonymisierte Nutzungsinformationen. Diesen fehlt der Personenbezug und damit die unmittelbare datenschutzrechtliche Sensibilität, die eine eigene Verantwortung auszulösen in der Lage ist.[56]

bb) *Datenverarbeitung im Auftrag des Fanpage-Betreibers?* Womöglich ist der Fanpage-Betreiber aber als Auftraggeber für Facebooks Datenverarbeitung verantwortlich.[57] Er muss sich Facebooks Handlungen dann zurechnen lassen, als sei das soziale Netzwerk Teil seines eigenen Unternehmens – und trägt alleine die Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen (§ 11 I 1 BDSG).[58] Für den Auftraggeber gilt insoweit, wie bei Einschaltung eines Erfüllungsgehilfen, der Rechtsgrundsatz: „Qui facit per alium,

41 Zu der datenschutzrechtlichen Relevanz dieser Rolle sub specie der damit verbundenen Erhebung von Inhaltsdaten s. unten II. 1. b).

42 Vgl. etwa *Hoffmann/Schulz/Brackmann*, Web 2.0 in der öffentlichen Verwaltung in *Schliesky/Schulz*, Transparenz, Partizipation, Kollaboration, 2012, 163 (184); *Voigt/Paul/Alich*, NJW 2011, 3541 (3543).

43 RL 95/46/EG des Europäischen Parlaments und des Rates vom 24.10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281, 31 (im Folgenden: EG-Datenschutz-RL).

44 Vgl. die Terminologie bei *Artikel-29-Datenschutzgruppe* (vgl. o. Fn. 34), 5.

45 Eine weite Bestimmung des Begriffs der Verantwortlichkeit entspricht auch der grundrechtlichen Zielsetzung, einen wirksamen und umfassenden Schutz der betroffenen Persönlichkeitsrechte sicherzustellen. Vgl. *EuGH*, NJW 2014, 2259 Rn. 34 = NVwZ 2014, 857.

46 Siehe dazu auch *VG Schleswig*, ZD 2014, 51 (54).

47 *OVG Schleswig*, ZD 2014, 643 (644); *Voigt/Paul/Alich*, NJW 2011, 3541 (3543) mwN; für die gegenteilige Ansicht *Karg*, ZD 2014, 54 (55).

48 Vgl. dazu den Vortrag des ULD bei *OVG Schleswig*, Urt. v. 4.9.2014 – 4 LB 20/13, BeckRS 2014, 55993 (insoweit in ZD 2014, 643 nicht abgedruckt); *Ernst*, NJOZ 2010, 1917 (1918) = NJW 2010, 2989; *Höppner*, Web Analytics und Datenschutz in *Taeger*, Die Welt im Netz, 2011, 477 (477 f.). Ohne eindeutige Positionierung *Schröder/Hawxwell*, Die Verletzungen datenschutzrechtlicher Bestimmungen durch so genannte Fanpages und Social-Plugins, WD 3 – 3000 – 306/11 neu (7.10. 2011), 8. Eine rein faktische Sichtweise der Verantwortlichkeit proklamierend *Dammann* (vgl. o. Fn. 30),§ 3 BDSG Rn. 224.

49 Vgl. dazu auch *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Orientierungshilfe »Soziale Netzwerke«, 14.3.2013, 11 f.

50 Vgl. insoweit auch *Krebs/Lange*, IT-Rechts-Berater 2014, 278 (280).

51 Vgl. *Artikel-29-Datenschutzgruppe* (vgl. o. Fn. 34), 11 f.

52 *Artikel-29-Datenschutzgruppe* (vgl. o. Fn. 34), 11.

53 Siehe dazu auch *VG Schleswig*, ZD 2014, 51 (54).

54 *OVG Schleswig*, ZD 2014, 643 (644); *Piltz*, K & R 2014, 80 (81). Zur Definition von „Zwecken" und „Mitteln" der Datenverarbeitung vgl. *Artikel-29-Datenschutzgruppe* (vgl. o. Fn. 34), 16.

55 Die Motivlage eines Unternehmens bei Einrichtung einer Fanpage können die Datenschutzbehörden überdies nur sehr bedingt nachvollziehen. Auch die unternehmerische Relevanz der Facebook Insights für den Fanpage-Betreiber dürfte in den seltensten Fällen offenliegen. Vielmehr besteht für sie stets die Möglichkeit, die Fanpage ausschließlich als Instrument der Außenkommunikation in Form einer digitalen Pinnwand zu nutzen – ohne Rückgriff auf die datenschutzrechtlich angreifbaren, zusätzlichen Angebote von Facebook.

56 So auch *OVG Schleswig*, Urt. v. 4.9.2014 – 4 LB 20/13, BeckRS 2014, 55993 (insoweit in ZD 2014, 643 nicht abgedruckt).

57 Ein solches Auftragsverhältnis im datenschutzrechtlichen Sinne, die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durchzuführen (Auftragsverhältnis im weiteren Sinne), kann außer als Auftrag iSv § 662 BGB auch in Gestalt aller anderen inhaltlich funktionalen Vertragsverhältnisse abgeschlossen werden, vgl. *Gola/Klug/Körffer* in *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 11 Rn. 6; *Plath* in *Plath*, BDSG, 2013, § 11 Rn. 21; *Spindler/Nink* in *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 11 TMG Rn. 7.

58 Auftragnehmer und Auftraggeber sind im Verhältnis zueinander grundsätzlich keine Dritten iSd § 3 VIII 3 BDSG. Damit geht eine Privilegierung ihres Datenaustauschs einher, sofern der Auftragnehmer seinen Sitz im Inland, in einem anderen Mitgliedstaat der EU oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat. Die Übertragung der Daten sowie deren Verarbeitung und Nutzung durch den Auftragnehmer sind dann auch ohne gesonderte Einwilligung oder gesetzliche Erlaubnis zulässig. Vgl. *Gola/Klug/Körffer* (vgl. o. Fn. 57), § 11 BDSG Rn. 4; *Plath* (vgl. o. Fn. 57), § 11 BDSG Rn. 2; *Spindler/Nink* in *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 11 BDSG Rn. 3.

facit per se".[59] Übt er auch keine physische Herrschaft über den Verarbeitungsprozess aus, bleibt er kraft Weisung doch Herr über die Daten. Derjenige, der die Entscheidungen trifft, soll dann auch die Verantwortung für alle ihre mittelbar erzeugten Folgen tragen.

Die (mit dem Zuspielen von Facebook Insights grundsätzlich vergleichbare) Einbindung von Google Analytics stuft der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) ausdrücklich als Auftragsdatenverarbeitung ein.[60] Google Analytics ist der Datenverkehrsanalyse-Dienst für Webseiten. Ebenso wie Facebook Insights analysiert er Nutzungsinformationen, etwa Verweildauern und Zugriffszahlen auf Homepages und stellt sie deren Betreibern kostenlos zur Verfügung. Dass Google mit der Auswertung der Nutzungsdaten (ebenso wie Facebook) auch bzw. vor allem eigene Verarbeitungszwecke verfolgt, schließt eine Auftragsdatenverarbeitung dabei nicht grundsätzlich aus.[61]

Der Auftragssachverhalt im Falle von Google Analytics unterscheidet sich allerdings in einem entscheidenden Punkt von Facebook Insights: Google analysiert den Besucherverkehr auf fremden Websites außerhalb seines eigenen Online-Angebots. Das ist dem Internetunternehmen nur möglich, wenn die Websites-Betreiber Google Analytics in eigener Verantwortung einbinden und auf diese Weise Google einen Analyseauftrag erteilen. Facebook kann demgegenüber auch ohne gesonderte (tatsächliche oder vertragliche) Ermächtigung der Fanpage-Betreiber auf die Nutzungsdaten der im eigenen Netzwerk gehosteten Fanpages zugreifen – und tut dies auch. Die Einrichtung der Fanpage (und die damit einhergehende Eröffnung des Nutzungsdatenkanals) genügt nicht den (Bestimmtheits-)Anforderungen an ein wirksames Angebot zur Auftragsdatenverarbeitung.[62] Auch die Fanpage-Nutzungsbedingungen enthalten kein Angebot für Facebook Insights, welches die Fanpage-Betreiber annehmen könnten. Weder fordert der Fanpage-Betreiber Facebook zur Datenanalyse auf noch verpflichtet sich Facebook rechtlich bindend dazu. Die Auswertung der Fanpage-Nutzungsdaten entspricht als Service vielmehr einer Geschäftsführung ohne klaren Auftrag; die Reichweitenanalyse gleicht unbestellter Ware.[63]

§ 11 BDSG setzt darüber hinaus tatbestandlich[64] eine Kontroll- und Entscheidungskompetenz des Auftraggebers voraus. Der Auftragnehmer darf also nur als dessen verlängerter Arm ohne eigenen Wertungs- und Entscheidungsspielraum tätig werden.[65] Einer solchen Weisungsbefugnis der Fanpage-Betreiber zu Art, Umfang und Zweck der Verarbeitung und Nutzung von Daten (§ 11 II Nr. 2 BDSG) unterwirft sich Facebook aber gerade nicht. Vielmehr setzt das Unternehmen einseitige, nicht verhandelbare[66] Nutzungsbedingungen für seine Fanpages[67] – entsprechend dem Leitmuster: „In meinem Garten Eden darf nur *Zuckerberg* befehlen".

Der Fanpage-Betreiber hat demgegenüber von der Genese der Nutzungsdaten an bis zur Veröffentlichung der aus ihnen aggregierten Nutzungsstatistiken zu keinem Zeitpunkt die volle Verfügungsgewalt über die Daten inne; er ist daher auch nicht – wie für den Auftraggeber einer Datenverarbeitung charakteristisch[68] – „Herr der Daten". In dem Verhältnis zwischen Facebook und seinen Fanpage-Betreibern fehlt es – anders als bei der Einbindung externer Webanalysetools,[69] beim Cloud Computing[70] oder der Einschaltung eines externen Rechenzentrums für die Gehaltsabrechnung – an einem Auftragsverhältnis iSd § 11 I BDSG.[71] Die Entscheidungsbefugnis über Zwecke und Mittel der Datenverarbeitung liegt vielmehr allein bei Facebook.[72]

cc) *Der Fanpage-Betreiber als Übermittler von Nutzungsdaten im Rahmen einer Funktionsübertragung?* Geht die tatsächliche Entscheidung über die Datenverwendung in wesentlichen Teilen auf den Dienstleister über, handelt es sich anstelle eines Verarbeitungsauftrags regelmäßig um eine *Funktionsübertragung*.[73] Diese zeichnet sich durch einen eigenen Entscheidungsspielraum des „Auftragnehmers" über Gegenstand, Zweck und Mittel der Datenerhebung, -verarbeitung und -nutzung aus. Er übt seine Tätigkeit nicht unter Kontrolle eines Auftraggebers aus, sondern selbstbestimmt – und ist daher selbst verantwortliche Stelle.

Das Verhältnis zwischen Facebook und einem Fanpage-Betreiber trägt charakteristische Merkmale einer solchen Funktionsübertragung: Dem Fanpage-Betreiber steht kein Weg

59 Wer durch einen anderen handelt, handelt selbst. *Ulpian*, Dig. 26, 7, 5 § 3; *Bonifatius VIII*, Liber Sextus, 1298, lib. 5, tit. 12, reg. 68 und 72.

60 Vgl. dazu etwa *Spindler/Nink* (vgl. o. Fn. 57), 11 TMG Rn. 16.

61 Vgl. auch *Artikel-29-Datenschutzgruppe* (vgl. o. Fn. 34), 18; *Karg*, ZD 2014, 54 (56).

62 Offen bleibt insbesondere der genaue Vertragsgegenstand, also die Art und Weise der beauftragten Datenverarbeitung. Vgl. allgemein zur hinreichend bestimmten Regelung der essentialia negotii etwa MüKoBGB/*Busche*, AT, 6. Aufl. 2012, § 145 BGB Rn. 6.

63 Vgl. dazu die zivilrechtliche Wertung des § 241 a I BGB.

64 Der Wortlaut des § 11 BDSG ist insoweit zwar offen. Die Vorschrift verpflichtet den Auftraggeber nicht ausdrücklich dazu, Weisungen zu erteilen. In diesem Sinne *Sutschet*, RDV 2004, 97 (101 f.). Allerdings ergibt sich aus § 11 II Nr. 3 iVm Nr. 6 der Anlage zu § 9 S. 1 BDSG, dass der Auftraggeber zur Auftragskontrolle, namentlich zur Verarbeitung entsprechend den Weisungen des Auftraggebers, verpflichtet ist. Die Auftragsdatenverarbeitung setzt damit in der Sache tatbestandlich eine Weisungsbefugnis sowie die Sachherrschaft über die zu verarbeitenden Daten voraus. Wer diese – wie der Betreiber einer Fanpage – nicht hat, kann auch einem Dritten für die Verarbeitung keinen Auftrag erteilen.

65 *Petri* in *Simitis*, BDSG, 8. Aufl. 2014, § 11 Rn. 22.

66 Standardmäßige Geschäftsbedingungen schließen umgekehrt eine Auftragsdatenverarbeitung nicht per se aus. Vgl. *Artikel-29-Datenschutzgruppe* (vgl. o. Fn. 34), 32.

67 Dies ist zwar auch bei Google Analytics der Fall. Allerdings öffnet sich Google über das bloße Akzeptieren der Nutzungsbedingungen hinaus auch dem Abschluss eines (mit dem HmbBfDI abgestimmten) schriftlichen Vertrags. Dieser räumt dem Nutzer formal eine Weisungsbefugnis gegenüber Google als Auftragsdatenverarbeiter ein (vgl. Anlage 1 Nr. 3 des unter www.google.com/analytics/terms/de.pdf abrufbaren Vertrags). Er konterkariert die Weisungsbefugnis jedoch dadurch, dass er Google das Ermessen einräumt, innerhalb von 60 Tagen nach Weisungszugang Einspruch gegen die Einzelweisung zu erheben. Das höhlt die Weisungsbindung faktisch aus. Die Weisungsbefugnis zur Datenlöschung im (fort-)laufenden Vertragsverhältnis (und damit eine entscheidende Rechtsposition, um eine datenschutzkonforme Auftragsdatenverarbeitung zu gewährleisten) fehlt sogar gänzlich. Der einzelne Google-Analytics-Nutzer ist auch nur eingeschränkt in der Lage, die nach § 11 II 4 BDSG erforderlichen Kontrollen bei der in den USA ansässigen Google Inc. durchzuführen. Google sucht diesen Bedenken dadurch zu begegnen, dass es einen von einem unabhängigen Wirtschaftsprüfer erstellten Prüfbericht bereithält, den es dem Nutzer auf entsprechende Anfrage in aktuellster Fassung (die nicht älter als 24 Monate ist) zur Verfügung stellt (vgl. Anlage 1 Nr. 5 des o. g. Vertrags).

68 Vgl. *Wedde* in *Däubler/Klebe/Wedde/Weichert*, BDSG, 4. Aufl. 2013, § 11 Rn. 5 u. 12.

69 *Petri* (vgl. o. Fn. 65), § 11 BDSG Rn. 39 unter Berufung auf den Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich vom 26./27.11.2009 Dok. F 357.

70 *Arbeitskreis Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises*, Orientierungshilfe – Cloud Computing, 2014, 9 ff.; *Artikel-29-Datenschutzgruppe*, Stellungnahme 05/2012 zum Cloud Computing, WP 196, 2012, 10; *Gola/Klug/Körffer* (vgl. o. Fn. 57), § 11 BDSG Rn. 8.

71 *Spindler/Nink* in *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 13 TMG Rn. 11.

72 So auch das *VG Schleswig*, ZD 2014, 51 (54); *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (124).

73 Im Einzelnen str.; zu Begriff und Inhalt der Funktionsübertragung insbesondere *Kramer/Herrmann*, CR 2003, 938 (939). Zum Meinungsstreit zwischen Funktionsübertragungs- und Vertragstheorie ausführlich *Gabel* in *Taeger/Gabel*, BDSG, 2. Aufl. 2013, § 11 Rn. 14 ff.; kritisch zur Abgrenzbarkeit *Sutschet*, RDV 2004, 97 (99 ff.).

offen, auf die einzelnen Phasen des Umgangs mit personenbezogenen Daten einzuwirken. Vielmehr nimmt Facebook die Verarbeitung eigenverantwortlich vor.[74] Sind beide somit nicht als einheitliche Stelle zu behandeln, braucht grundsätzlich jeder direkte Austausch personenbezogener Daten zwischen ihnen als Übermittlung von Daten iSd § 3 IV Nr. 3 BDSG eine gesetzliche Erlaubnis (zB nach § 29 II bzw. § 16 II BDSG).

Die Übermittlung an einen Dritten setzt aber voraus, dass die Daten aus dem datenschutzrechtlichen Verantwortungsbereich einer verantwortlichen Stelle heraus weitergegeben werden.[75] Nur wenn sich der Kreis derjenigen, die auf die Daten zugreifen, durch den Datentransfer *erweitert*, greift der Rechtsgrund für die besonderen gesetzlichen Zulässigkeitsanforderungen an das Übermitteln.[76] Bei den übermittelten Daten muss es sich daher um von der übermittelnden Stelle gespeicherte oder von ihr durch Datenverarbeitung gewonnene Daten handeln.[77]

Diese Voraussetzung ist im Verhältnis zwischen Fanpage-Betreibern und Facebook nicht erfüllt. Der Fanpage-Betreiber übermittelt – anders als bspw. in Fällen einer Hinzuziehung Dritter für die Meinungs- und Marktforschung nach § 30 a BDSG[78] – nämlich keine Nutzerdaten an Facebook iSv § 3 IV Nr. 3 BDSG. Das tun die Nutzer vielmehr selbst. Eine Datenübermittlung findet ausschließlich im Verhältnis zwischen Facebook und Nutzer statt.[79]

b) *Fanpage-Betreiber als Beschaffer von Inhaltsdaten.* Fanpage-Betreiber machen sich nicht nur Facebooks Auswertungen von Nutzungsdaten zunutze, ernten also nicht nur die Früchte vom verbotenen Baum. Sie tragen auch zu dessen Wachstum bei: Sie erheben selbst personenbezogene Daten, nämlich die Inhalte, welche die Nutzer, zB als Kommentare auf der Fanpage, hinterlassen (aa). Das macht sie insoweit zur verantwortlichen Stelle iSd § 3 VII BDSG und damit womöglich auch für Facebooks Datenschutzpraktiken mitverantwortlich (bb). Denn verantwortlich ist nicht nur, wer personenbezogene Daten verarbeitet und nutzt (bzw. dies durch andere im Auftrag vornehmen lässt), sondern auch derjenige, der Daten iSv § 3 III BDSG *erhebt*.

aa) *Datenerhebung.* Eine Datenerhebung iSd § 3 III BDSG umschließt alle der Datenverarbeitung vorgelagerten Aktivitäten, mit denen eine Stelle willentlich Kenntnis von Daten erhält oder die Verfügungsmacht über diese begründet.[80] Welcher Art die Erhebungsaktivität ist (zB Beobachtung, Befragung, Erlangung durch Übermittlung oder Zugriff auf Dateien) und welche Informationsquelle Verwendung findet, spielt grundsätzlich keine Rolle.[81] Die Datenbeschaffung muss auch nicht Teil eines weitergehenden Erhebungsplans sein oder notwendig in eine Speicherung münden.[82] Es genügt eine eigene Verfügungsmöglichkeit über die Daten.[83] Die Schwelle zum Beschaffen ist lediglich dann noch nicht überschritten, wenn es an einem aktiven und subjektiven Beschaffungsmoment fehlt und die Daten der jeweiligen Stelle ohne eigenes Zutun zuwachsen.[84] Die bloße Eröffnung eines Kommunikationskanals, zB die Vorhaltung einer E-Mail-Adresse, ist daher noch kein Beschaffungsvorgang.

Animiert der Fanpage-Betreiber Nicht-Mitglieder zur Registrierung bei Facebook oder registrierte Nutzer zum Posten von Texten, Bildern oder Videos, beschafft er sich (und Facebook) damit Daten.[85] Er wirkt aktiv und willentlich darauf hin, dass die Nutzer personenbezogene Daten bereitstellen. Die Klarnamenpflicht des Netzwerks macht jedes abgefragte Nutzerfeedback zu einem personenbezogenen Datum (§ 3 I BDSG).[86] Dieser Personenbezug entspricht dem Interesse des Fanpage-Betreibers, ermöglicht er ihm doch eine zielgruppengenaue Aufschlüsselung des Nutzerfeedbacks. Seine Intention zur Datenbeschaffung geht damit deutlich über die beim Betrieb eines anonymen oder pseudonymen Online-Forums

74 *Petri* (vgl. o. Fn. 65), § 11 BDSG Rn. 22 f. Eine Datenweitergabe ist dann eine Übermittlung iSd § 3 IV 1 Nr. 3 BDSG. Vgl. auch *Gola/Klug/Körffer* (vgl. o. Fn. 57), § 11 BDSG Rn. 9.

75 Vgl. *Dammann* (vgl. o. Fn. 30), § 3 BDSG Rn. 156.

76 Vgl. *Dammann* (vgl. o. Fn. 30), § 3 BDSG Rn. 145.

77 Vgl. dazu *Dammann* (vgl. o. Fn. 30), § 3 BDSG Rn. 159 ff.

78 Die Literatur stuft diese Konstellation regelmäßig als Fall einer Funktionsübertragung ein; vgl. *Wilken*, Datenschutz-Nachrichten 35 (2012), 104 (104). § 30 a BDSG rechtfertigt dabei lediglich die Datenerhebung und -speicherung zu Zwecken der Markt- oder Meinungsforschung, nicht aber die Einbeziehung Dritter, regelt insbesondere nicht deren Verantwortlichkeit.

79 *OVG Schleswig*, ZD 2014, 643 (644); *Moos*, jurisPR -DSR 1/2015, Anm. 6. Auch indem Facebook seine Insights bereitstellt, übermittelt es keine Daten an die Fanpage-Betreiber. Infolge ihrer Anonymisierung und Zusammenfassung unterfallen die Nutzungsdaten zu diesem Zeitpunkt nicht mehr dem Datenschutzregime des BDSG (§ 1 I BDSG), so dass Facebook sie, ohne datenschutzrechtliche Rechtfertigungsanforderungen überwinden zu müssen, an die Fanpage-Betreiber übermitteln kann.

80 Vgl. *Dammann* (vgl. o. Fn. 30), § 3 BDSG Rn. 102; *Gola/Klug/Körffer* in *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 3 Rn. 24; *Plath/Schreiber* in *Plath*, BDSG, 2013, § 3 Rn. 30; *Buchner* in *Taeger/Gabel*, BDSG, 2. Aufl. 2013, § 3 Rn. 25. Zwar knüpft Art. 2 Buchst. d EG-Datenschutz-RL seine Zurechnung von Pflichten alleine an den Vorgang der Verarbeitung an: Dort ist lediglich die Rede von dem „für die Verarbeitung Verantwortlichen" und der Entscheidung über „die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten". Allerdings liegt der Richtlinie eine andere begriffliche Systematik als dem nationalen Datenschutzrecht zu Grunde: Sie versteht den Begriff der Verarbeitung als Oberbegriff, der sämtliche Vorgänge in Zusammenhang mit personenbezogenen Daten und damit auch das Erheben umfasst (vgl. Art. 2 Buchst. b EG-Datenschutz-RL). Damit unterstreicht sie, dass auch der vorgelagerte Vorgang des Erhebens bereits Teil des Lebenszyklus eines Datums ist und die (Mit-)Entscheidung über Mittel und Zwecke der Erhebung insoweit einer (Mit-)Entscheidung über technische Vorgänge (wie das Speichern, Abfragen Auslesen oder Verknüpfen) gleichsteht. Vgl. zur jeweils gesonderten Bewertung der verschiedenen Phasen des Umgangs mit personenbezogenen Daten *Gola/Klug/Körffer*, § 3 BDSG Rn. 24; *Plath/Schreiber*, § 3 BDSG Rn. 33.

81 *Gola/Klug/Körffer* (vgl. o. Fn. 80), § 3 BDSG Rn. 24; *Weichert* in *Däubler/Klebe/Wedde/Weichert*, BDSG, 4. Aufl. 2013, § 3 Rn. 30; *Wehr*, BPolG (2013), § 21 Rn. 3.

82 *OVG Münster*, Urt. v. 22.11.2001 – 1 A 4855/99, BeckRS 2002, 21134; *Plath/Schreiber* (vgl. o. Fn. 80), § 3 BDSG Rn. 30; *Weichert* (vgl. o. Fn. 81), § 3 BDSG Rn. 30.

83 *Dammann* (vgl. o. Fn. 30), § 3 BDSG Rn. 107.

84 Statt vieler vgl. *Dammann* (vgl. o. Fn. 30), § 3 BDSG Rn. 104.

85 Die Fanpage ist als interaktives soziales Medium auf einen Informationsrückfluss angelegt und dient dazu, mehr von und über Interessenten, Kunden und Zielgruppen zu erfahren. Auf Fanpages testen die Betreiber Kampagnen und fordern die Besucher zur Abstimmung über Design- und Produktinnovationen mittels Like-Button auf. Die auf jeder Fanpage für nicht-eingeloggte Besucher angezeigte Aufforderung „Um dich mit […] zu verbinden, registriere dich noch heute für Facebook" und die unter jedem Chronik-Eintrag platzierten „Gefällt mir"- und „Teilen"-Buttons sowie die Kommentarfunktion sind ein Appell zur Preisgabe personenbezogener Daten. Diese Funktionen stellt zwar nicht der Fanpage-Betreiber selbst zur Verfügung, sondern Facebook. Der Fanpage-Betreiber macht sich mit seiner Facebook-Präsenz aber die Registrierungsaufforderung und die Folgen-, Teilen- und Bewerten-Tools seiner Fanpage zu eigen. Er steuert über die Content-Veröffentlichung auch die Häufigkeit entsprechender Funktionseinblendungen auf den Nutzerprofilen: Je mehr Posts, desto mehr „Gefällt-mir-Buttons" und Kommentarspalten. Außerdem beeinflusst er durch den Inhalt und die Formulierung seiner Beiträge, ob und welche Informationen die Nutzer preisgeben. Konkrete Fragestellungen, wie „An was erinnert euch die neue Geschmacksrichtung Vanille" oder die Aufforderung „Postet uns Fotos, auf denen ihr unser Produkt benutzt" stimulieren und strukturieren das Nutzer-Feedback und sind daher (mit-)entscheidend für die Datenbeschaffung. In der Einrichtung und inhaltlichen Bespielung der Fanpage liegt dann regelmäßig eine eigene Datenbeschaffungsaktivität der Fanpage-Betreiber bzw. ein arbeitsteiliges Zusammenwirken mit Facebook bei der Datenerhebung. Mit diesem Nudging schafft der Fanpage-Betreiber zusätzliche Anreize, sich dem Datensammler Facebook zu öffnen. Denn mit jedem eingestellten Inhalt ermöglicht der Betreiber der Fanpage, dass Facebook die Daten der Seitenbesucher zu Werbezwecken mittels Cookies erfasst.

86 So etwa auch *Solmecke/Wahlers*, ZD 2012, 550 (552).

mit inhaltlich offener Beitragsmöglichkeit hinaus. Letztere ist keine Datenerhebung,[87] die Beschaffung von Informationen über Fanpage-Besucher demgegenüber schon.[88] Der Fanpage-Betreiber trifft insoweit nicht nur eine eigene Entscheidung über die Mittel der Inhaltsdatenerhebung, sondern auch darüber, dass diese Daten durch die Erhebung via Fanpage Facebook für dessen geschäftsmäßige Datenverarbeitung zur Verfügung stehen.[89]

bb) *Konnexität zwischen der Erhebung von Inhaltsdaten und der Verarbeitung von Nutzungsdaten.* Die Inhaltsdaten der Fanpages sind notwendige Voraussetzung dafür, dass Facebook überhaupt Nutzungsdaten destillieren kann. Ohne ihren Datenregen würde der Baum der Erkenntnis auf Dauer verkümmern. Die Inhaltsdatenerhebung des sekundären Diensteanbieters (Fanpage-Betreiber) begründet so womöglich dessen (Mit-)Verantwortung für die Nutzungsdatenverarbeitung des primären Diensteanbieters (Facebook).

Die rechtliche Konnexität zwischen den Phasen der Datenerhebung und der Datenverarbeitung bringt das nationale Recht insbesondere in seinem § 28 I 2 BDSG zum Ausdruck: Die Zwecke, für die Daten später verarbeitet oder genutzt werden sollen, sind bereits bei der Erhebung konkret festzulegen. Die Inhaltsdaten erhebende Stelle ist auch Adressat einer korrespondierenden datenschutzrechtlichen Unterrichtungspflicht, nämlich der des § 4 III 1 Nr. 2 BDSG[90] – und dementsprechend verpflichtet, die Betroffenen über die Zweckbestimmungen der Erhebung, einschließlich der (Nutzungs-)Datenverarbeitung durch Facebook, zu informieren. In gleicher Weise geben § 4a I 2 BDSG und § 13 I 1 TMG vor, dass bei einer auf eine Einwilligung gegründeten Datenerhebung und -verarbeitung schon die (zu Beginn der Erhebung bzw. des Nutzungsvorgangs gebotene) datenschutzrechtliche Unterrichtung die Zweckbestimmung enthalten muss, um informiert über die Datenpreisgabe entscheiden zu können.[91]

Das Informationsbedürfnis der Nutzer entfällt nicht etwa (gleichsam rückwirkend) dadurch, dass sie ihr Feedback via „Gefällt mir"- und Kommentarwerkzeug allgemein zugänglich machen,[92] statt (wie bei einer postalischen Umfrage) die Daten dem Fanpage-Betreiber im Wege der Individualkommunikation zuzuspielen. Vielmehr müssen die Nutzer gerade auch über die Öffentlichkeitswirkung ihrer Beiträge und die von dem Fanpage-Betreiber verfolgten bzw. durch seine Vertragsbindung mit Facebook unterstützten Zwecke der Datenerhebung informiert werden. Denn für die Entscheidung über das öffentliche Zugänglichmachen ist durchaus auch relevant, welche Zwecke der Fanpage-Betreiber mit der Erhebung verfolgt oder ermöglicht.

Eine eigene Datenschutzerklärung des Fanpage-Betreibers, die über die Zwecke der Datenerhebung informiert, ist nur dann entbehrlich, wenn die Fanpage-Besucher bereits anderweitig über die Zwecke der Erhebung informiert sind. Eine solche anderweitige Information liegt zwar mit der Datenrichtlinie von Facebook[93] vor. Die registrierten Facebook-Nutzer haben ihr zugestimmt und nicht-registrierte Fanpage-Besucher können sie über einen Link in der Fußzeile jeder Fanpage aufrufen. Allerdings weist Facebooks Datenschutzerklärung Unzulänglichkeiten bei der Zweckbestimmung der Datenerhebung und -verarbeitung auf.[94] Verlassen sich die Fanpage-Betreiber, statt eine eigene Datenschutzerklärung auf ihrer Fanpage-Informationsseite vorzuhalten, darauf, dass die Nutzer bereits via Facebook Kenntnis von den Zwecken der Datenerhebung erlangt haben, sind ihnen daher die Unterrichtungsmängel der Facebook Datenschutzrichtlinie als eigener Datenschutzverstoß vorzuwerfen.

Die Unzulänglichkeiten der Datenschutzrichtlinie des sozialen Netzwerks Facebook schlagen auf diese Weise womöglich auf die Zulässigkeit der *Inhaltsdaten*erhebung durch, welche die Fanpage-Betreiber vornehmen. Dasselbe gilt für die fehlende Widerspruchsbelehrung hinsichtlich der Erstellung pseudonymer Nutzungsprofile.

Mit den Augen der strafrechtlichen Dogmatik betrachtet, weist das Verhalten des Fanpage-Betreibers Ähnlichkeiten zum *Gehilfen* auf. Der Fanpage-Betreiber wirkt mit dem sozialen Netzwerk arbeitsteilig und in Kenntnis datenschutzrechtlicher Verstöße zusammen: „Wer die Leiter hält, ist so schuldig als der Dieb", sagt ein altes Sprichwort. Nicht zuletzt steht der Fanpage-Betreiber als telemedienrechtlicher Diensteanbieter auch selbst in der Verantwortung für die Einhaltung der Pflichten des § 15 TMG.

Das alleine begründet indes noch nicht ohne Weiteres eine Verantwortung für Datenerhebungen, die Facebook selbst vornimmt, indem es Nutzungsdaten zu Nutzungsprofilen verschneidet. Denn verantwortlich ist der Fanpage-Betreiber grundsätzlich nur für das, was er *selbst mitentscheiden* kann.

87 Vgl. dazu *Dammann* (vgl. o. Fn. 30), § 3 BDSG Rn. 110.

88 Allerdings handelt es sich bei dem durch den Fanpage-Betreiber erhobenen personenbezogenen Nutzerfeedback nicht um Nutzungsdaten iSv § 15 TMG und somit auch nicht um Daten, deren Verarbeitung das ULD zum Ausgangspunkt seines Bescheids an die Wirtschaftsakademie Schleswig-Holstein (oben I. 4.) gemacht hat. Vielmehr sind die auf Aktivitäten des Fanpage-Betreibers zurückgehenden Kommentare und Likes der Nutzer als so genannte Inhaltsdaten zu qualifizieren (so auch *Der Bayerische Landesbeauftragte für den Datenschutz*, Fanpages bayerischer öffentlicher Stellen in sozialen Netzwerken zum Zweck der Öffentlichkeitsarbeit, 28.3.2013, https://www.datenschutz-bayern.de/technik/orient/oh_fanpages.html, unter 2. 3). Dementsprechend thematisiert weder die erstinstanzliche noch die Berufungsentscheidung die Konsequenzen einer Verantwortlichkeit der Fanpage-Betreiber für die Inhaltsdatenerhebung auf ihrer Fanpage.

89 Siehe auch *Jandt/Roßnagel*, ZD 2011, 160 (161).

90 Die Zulässigkeit des Umgangs mit Inhaltsdaten und die einschlägigen Betroffenenrechte sowie korrespondierende Pflichten der verantwortlichen Stelle bestimmen sich (mangels Spezialregelung im TMG) nach dem allgemeinen Datenschutzrecht des BDSG und der LDSGe, vgl. *Hullen/Roggenkamp* (vgl. o. Fn. 7), § 15 TMG Rn. 12; *Spindler/Nink* (vgl. o. Fn. 6), § 15 TMG Rn. 2; aA bei einer Online-Leistungserbringung *Schmitz*, Teil 16.2 Datenschutz im Internet in *Hoeren/Sieber/Holznagel*, Handbuch Multimedia-Recht, 41. EL (März 2015), Rn. 262.

91 Im Hinblick auf besondere Arten personenbezogener Daten (§ 3 IX BDSG) sind Fanpage-Betreiber als Inhalteanbieter zudem besonderen Schranken unterworfen (vgl. insbesondere § 13 II, § 28 VI und V BDSG). Sie sind auch für die Löschung entsprechender Inhaltsdaten (§ 35 II, BDSG, § 13 IV Nr. 2 TMG) und für Auskunftspflichten im Hinblick auf Daten, die über die Person des Betroffenen gespeichert sind (§ 34 I 1 Nr. 1 iVm § 13 VII TMG), verantwortlich. Sie haben überdies die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Erfüllung der datenschutzrechtlichen Pflichten sicherzustellen (§ 12 III TMG iVm § 9 S. 1 BDSG in Verbindung mit der Anlage zum BDSG). Die Daten sind aber auf Servern von Facebook gespeichert, auf die der Fanpage-Betreiber keine Einfluss- und Kontrollmöglichkeit ausüben kann. Für solche Fälle der Datenübermittlung begrenzt § 35 VII BDSG sub specie der Löschung die Verantwortlichkeit auf eine Unterrichtungspflicht.

92 Die Verpflichtung des § 4 III 1 Hs. 1 BDSG greift de lege lata nur, wenn die Daten direkt beim Betroffenen erhoben werden, nicht aber beim Auswerten allgemein zugänglicher Datenquellen ohne Zutun des Betroffenen. Allgemein zugänglich sind auf der Fanpage veröffentlichte Inhaltsdaten dann, wenn der Zugang zu ihnen nicht auf eine bestimmte Zielgruppe beschränkt ist, sondern potenziell jedermann sie zur Kenntnis nehmen kann (vgl. zum Begriff der allgemein zugänglichen Daten zB *Venzke-Caprese*, DuD 2013, 775 [776]). Das ist bei „Gefällt mir"-Angaben und Kommentaren regelmäßig der Fall, da der kommentierende Facebook-Nutzer die Sichtbarkeit seiner Likes und Comments nicht individuell einschränken kann. Vielmehr sind sie für jeden sichtbar, den die Fanpage adressiert und der daher die Inhalte auf der Fanpage lesen kann. Da Fanpage-Betreiber für ihre Fanpage-Inhalte entsprechend ihrer PR-Zielrichtung regelmäßig die Zielgruppeneinstellung „öffentlich" auswählen, kann in der Regel jeder Internetnutzer – unabhängig von einer Facebook-Registrierung – Kommentare und Likes zur Kenntnis nehmen. Demnach handelt es sich bei „Gefällt mir"-Angaben und Kommentaren auf Fanpages nach ihrer Veröffentlichung um allgemein zugängliche Daten. In dem Zeitpunkt, in dem der Fanpage-Betreiber einen Beitrag postet und so das Social-Media-Feedback der Fanpage-Besucher abfragt, liegt die alleinige Entscheidungshoheit darüber, ob sie entsprechende Inhaltsdaten preisgeben wollen freilich noch bei den Betroffenen. Der Fanpage-Betreiber erhebt die Inhaltsdaten somit direkt beim Betroffenen. Dass dieser sie mit der Übermittlung auf Grund seiner Voreinstellungen publik macht, ändert daran rechtlich nichts.

93 Vgl. die Facebook-Datenschutzrichtlinie (vgl. o. Fn. 1).

94 Dazu oben I. 1.

Steuern kann er eigene Erhebungen personenbezogener *Inhalts*daten, nicht hingegen Facebooks Verarbeitung von *Nutzungs*daten. Es fehlt an einer – über die bloße Stimulierung der Facebook-Nutzung und den damit verbundenen Nutzungsdatenzuwachs hinausgehenden – Klammer der Steuerung, welche die Beschaffung von Inhaltsdaten zugleich zur Mitentscheidung über die Verarbeitung von Nutzungsdaten macht. Facebook und der Betreiber der Fanpage agieren insoweit in getrennten Verantwortungssphären.

Beide Vorgänge stehen zwar in einem Konnex, sind aber unterschiedlichen Rechtsregimes unterworfen: Die Beschaffung von Inhaltsdaten des Fanpage-Betreibers bestimmt sich regelmäßig nach § 28 BDSG, die Verarbeitung von Nutzungsdaten durch Facebook ist hingegen an § 15 TMG zu messen. TMG und BDSG bauen grundsätzlich auf einer Trennung der Vorgänge auf: Jede datenverarbeitende Stelle ist nur für die Einhaltung derjenigen Datenschutzvorschriften heranzuziehen, die ihren eigenen Verarbeitungsvorgang betreffen.[95] Die datenschutzrechtliche Verantwortlichkeit ist mit anderen Worten für einen Datenverarbeitungsvorgang nicht notwendig gebündelt zu beurteilen, sondern regelmäßig phasenspezifisch anhand der konkreten Einwirkungsmöglichkeiten der jeweils beteiligten Akteure.[96] Die datenschutzrechtliche Verantwortung des Fanpage-Betreibers bezieht sich nur auf *eigene* Datenerhebungen von *Inhalts*daten, erstreckt sich aber nicht auf die Verarbeitung von *Nutzungs*daten, die Facebook selbst wahrnimmt. Die Legaldefinition der Verantwortlichkeit in § 3 VII BDSG deutet das dadurch an, dass sie ausdrücklich zwischen „erheben", „nutzen" und „verarbeiten" trennt.

c) *Zwischenergebnis.* Fanpage-Betreiber sind für die Verarbeitung personenbezogener *Nutzungs*daten nicht verantwortlich. Der tatsächliche Einfluss, den sie auf das entsprechende Datenaufkommen haben, bleibt hinter der gesetzlich geforderten (Mit-)Entscheidung über Mittel und Zwecke der Datenverarbeitung zurück. Auch die Erwartung der Fanpage-Betreiber, Facebook werde die über die Fanpage anfallenden Nutzungsdaten erheben und verarbeiten, um sie ihnen anschließend in aggregierter, anonymisierter Form als Facebook Insights zur Verfügung zu stellen, entfaltet als Handlungsmotivation keinen einer Mitentscheidung äquivalenten Einfluss. Rein subjektiven Zweckbestimmungen fehlt die tatsächliche und rechtliche Entscheidungsmacht zur Bestimmung des „Wie" und „Warum" der Datenverarbeitung.

Eine datenschutzrechtliche Verantwortlichkeit lässt sich auch nicht aus einem *Datenverarbeitungsauftrag* zwischen Fanpage-Betreiber und Facebook herleiten. Anders als beim Einsatz von Google Analytics fehlt es an der für ein Auftragsverhältnis iSd § 11 I BDSG erforderlichen Beauftragung, Weisungsbefugnis und Verfügungsgewalt des Fanpage-Betreibers. Er ist nicht – wie für den Auftraggeber einer Datenverarbeitung charakteristisch – „Herr der (Nutzungs-)Daten", sondern überlässt deren Erheben, Speichern und Verarbeiten in Gänze Facebook. Auch die darin liegende *Funktionsübertragung* zieht keinen datenschutzrechtlich rechtfertigungsbedürftigen Übermittlungsvorgang nach sich, der eine Verantwortlichkeit auslöst. Denn zwischen Fanpage-Betreiber und Facebook findet keine Übermittlung personenbezogener Daten statt. Vielmehr sind es die Nutzer selbst, die ihre personenbezogenen Daten an Facebook übermitteln. Der Daten(rück)fluss an die Fanpage-Betreiber in Gestalt der Facebook Insights erfolgt ausschließlich anonymisiert, also datenschutzrechtlich neutral.

Eine Verantwortlichkeit des Fanpage-Betreibers für Facebooks rechtswidrige Verarbeitung der Nutzungsdaten resultiert auch nicht daraus, dass er zumindest für die Erhebung der auf seiner Fanpage veröffentlichten *Inhalts*daten verantwortlich ist. Sowohl die Einrichtung der Fanpage als auch alle Posts und Einträge des Fanpage-Betreibers sind zwar regelmäßig als Datenerhebung zu qualifizieren. Denn sie zielen auf Grund Facebooks Klarnamen-Policy notwendig auf die Preisgabe und Bereitstellung personenbezogener Daten.[97] Diese Inhaltsdaten sind auch die notwendige Voraussetzung dafür, dass Facebook Daten über das aktive Nutzungsverhalten erheben kann. Aus dieser rein kausalen Verknüpfung der Beiträge erwächst indes noch keine rechtliche Mitverantwortung iSd § 3 VII BDSG. Denn auf die Erhebung und Verarbeitung der Nutzungsdaten hat der Fanpage-Betreiber keinen Einfluss.

2. Gesetzlicher Spielraum für aufsichtsrechtliche Maßnahmen nach § 38 V BDSG jenseits § 3 VII BDSG

Gemessen an der Figur der verantwortlichen Stelle des § 3 VII BDSG können Fanpage-Betreiber Facebooks datenschutzwidrige digitale Infrastruktur risiko- und rechtsfolgenlos nutzen. Womöglich ergibt sich ihre Mitverantwortung aber aus allgemeinen Zurechnungskategorien der Rechtsordnung jenseits des § 3 VII BDSG (a). Die aufsichtsrechtliche Befugnisnorm des § 38 V BDSG ist in ihrem Wortlaut insoweit grundsätzlich offen. Sie knüpft lediglich an einen Verstoß gegen eine datenschutzrechtliche Verhaltenspflicht an[98] (b). Ob eine Heranziehung des Nutznießers eines Datenschutzverstoßes Verhältnismäßigkeitsanforderungen entspricht, steht jedoch auf einem anderen Blatt (c).

a) *(Mit-)Verantwortlichkeit der Fanpage-Betreiber als mittelbare Verursacher nach allgemeinen Grundsätzen?* Wenn der Fanpage-Betreiber sich via Facebook Insights Angaben zur Demografie seiner Fans und zur Wirkung seiner Posts verschafft, erntet er von den „Früchten des verbotenen Baumes".[99] Er beschafft sich Informationen, die unter Missachtung des deutschen Datenschutzrechts, insbesondere der Bestimmungen des § 15 TMG,[100] ermittelt worden sind.[101] Ihm dann auch eine Verantwortung dafür zuzuweisen, dass die Daten in rechtmäßiger Weise erlangt sind, entspricht einer plausiblen normativen Wertung.

Die zivilrechtliche Störerdogmatik kennt eine solche Fernwirkung der Tat. Sie erlaubt eine Inanspruchnahme desjenigen, der – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat zur Verletzung eines geschützten Guts beigetragen hat.[102] Zivilrechtliche Störerkategorien

95 Vgl. auch *Jandt/Roßnagel*, ZD 2011, 160 (164).
96 *Dammann* (vgl. o. Fn. 30), § 3 BDSG Rn. 227.
97 Vgl. etwa *Grabs/Bannour*, Follow me!, 2. Aufl. 2013, 36 ff., 270 ff.
98 Trifft eine aufsichtsbehördliche Ermächtigung keine Aussage über den Adressatenkreis der von ihr geregelten aufsichtsrechtlichen Maßnahmen, greifen einige Gerichte auf die allgemeinen Grundsätze der Verhaltens- und Zustandsverantwortlichkeit des Gefahrenabwehrrechts bzw. die telemedienrechtlichen Verantwortlichkeitskategorien zurück. Vgl. etwa *OVG Münster*, MMR 2009, 286 (287), das die allgemeinen ordnungsrechtlichen Verantwortlichkeitsgrundsätze für die Bestimmung des Adressatenkreises von § 67 I 1 TKG heranzieht.
99 Die Lehre entstammt der strafprozessualen Dogmatik. Sie beschäftigt sich mit der Frage, ob jemand zB wegen Steuerhinterziehung verurteilt werden kann, wenn er seiner Taten nur durch rechtsstaatswidrig erhobene Beweise, zB durch gestohlene Steuer-CDs, überführt werden kann. Die Unzulässigkeit der Beweiserhebung führt im Strafprozess nicht ohne Weiteres zur Fernwirkung eines Beweisverwertungsverbotes, sofern der Verfahrensverstoß nicht planmäßig oder systematisch erfolgt. *BVerfG*, NJW 2011, 2417 (2418) = NStZ 2011, 103 Rn. 42 ff.
100 Dazu im Einzelnen oben I. 1., Seite 3.
101 Bedenklich daher die Wertungen bei *Hoffmann/Schulz/Brackmann*, ZD 2013, 122 (125).
102 *BGH*, NJW-RR 2002, 832 (833) = GRUR 2002, 618; MMR 2013, 733 (736) = NJW 2013, 3245 Rn. 58); GRUR 2015, 485 = NJW 2015, 2122 Ls. = CR 2015, 386 (387).

– wie vermehrt erwogen[103] – in das Datenschutzrecht zu übertragen, insbesondere bei hoheitlichen Aufsichtsmaßnahmen heranzuziehen, geht allerdings an der gesetzlichen Systematik vorbei.[104] Denn sie folgen dem Grundgedanken der Abwehr von Besitz- und Eigentumsstörungen unter Privaten (§ 1004 I 1 und § 862 BGB). Eine ordnungsrechtliche Verantwortlichkeit im Subordinationsverhältnis vermögen sie nicht zuzuordnen.

Ein Rückgriff auf die zivilrechtliche Störerhaftung genügt überdies nicht rechtsstaatlichen Bestimmtheitsanforderungen. Das Handeln der Verwaltung muss für den Bürger in hinreichendem Ausmaß voraussehbar sein.[105] Mit hoheitlichen Maßnahmen auf zivilrechtlicher Zurechnungsgrundlage braucht er nicht zu rechnen.[106] Hätte der Gesetzgeber das gewollt, so hätte er dies durch entsprechenden Verweis auf die zivilrechtlichen Haftungsnormen klarstellen müssen.[107]

Anwendung können daher allenfalls allgemeine ordnungsrechtliche Grundsätze der Verhaltens- und Zustandsverantwortlichkeit finden.

aa) *Die Zweckveranlassung als datenschutzrechtliche Verantwortungskategorie?* Dem praktischen Bedürfnis, den Hintermann eines Störers ordnungsrechtlich verantwortlich machen zu können, trägt das Gefahrenabwehrrecht mit der Kategorie des Zweckveranlassers Rechnung. Er muss sich die Fernwirkungen seines Handelns zurechnen lassen.

Der Zweckveranlasser überschreitet nicht selbst die Gefahrenschwelle, sondern nimmt – isoliert betrachtet – eine rechtmäßige Handlung vor. Allerdings setzt er durch sein Verhalten eine Kausalkette in Gang, an deren Ende ein anderer die Gefahrenschwelle in zurechenbarer Weise überschreitet. Seine Handlung ist daher eine Bedingung im Sinne der Condicio-sine-qua-non-Formel für die abzuwehrende Gefahr oder Störung. Wer bspw. durch eine offensive Schaufensterreklame einen Massenauflauf vor seinem Geschäft verursacht, der den Verkehr gefährdet, setzt den letzten Schritt zur polizeirechtlichen Gefahr nicht selbst. Er veranlasst aber objektiv die Überschreitung der Gefahrenschwelle durch Dritte – und ist damit Zweckveranlasser.[108]

Nicht jeder kausale Beitrag zum Handlungsverlauf löst aber schon als solcher eine Haftung als Zweckveranlasser aus. Hinzukommen muss ein objektives[109] (1) oder subjektives[110] (2) Zurechnungselement.[111]

(1) *Objektiver Ansatz.* Mit der Einrichtung seiner Facebook-Seite gibt der Fanpage-Betreiber nicht den Anstoß dafür, dass Facebook Daten unter Verstoß gegen deutsches Datenschutzrecht verarbeitet und so die Gefahrenschwelle überschreitet. Er nutzt vielmehr ein Verhalten aus, das Facebook ohnehin an den Tag legt: Facebook ist – strafrechtlich gewendet – ein omnimodo facturus.

Dass der Zweckveranlasser beim unmittelbaren Störer den Tatentschluss hervorruft, hält die Rechtsprechung aber nicht für konstitutiv. Es soll vielmehr ausreichen, dass der Zweckveranlasser dem unmittelbaren Störer die tatsächliche Möglichkeit verschafft, dessen vorgefassten Entschluss in die Tat umzusetzen.[112]

Mit der Einrichtung einer Facebook-Seite erhöht der Fanpage-Betreiber das Datenaufkommen in dem sozialen Netzwerk: Fanpages sind regelmäßig darauf angelegt, möglichst hohe Klickraten zu erzielen. Als Kommunikations- und Vertriebskanal fördern sie objektiv die Breitenwirkung Facebooks geschäftsmäßiger Datenschutzverstöße. Sie legen insbesondere den Grundstein dafür, dass Facebook seine Verstöße in vorhersehbarer Weise auch auf Betroffene ausdehnen kann, die allein auf Grund des Informationsangebots des Fanpage-Betreibers das soziale Netzwerk besuchen. Das begründet einen Wirkungs- und Verantwortungszusammenhang, der eine Zurechnung rechtfertigen kann.

(2) *Subjektiver Ansatz.* Der Fanpage-Betreiber nimmt regelmäßig zumindest als Nebenfolge auch in Kauf, eine ordnungsrechtliche Störung des Datenschutzrechts hervorzurufen. Indem Fanpage-Betreiber Facebooks (öffentlich breit diskutierte und kritisierte) Nutzungsbedingungen akzeptieren,[113] bringen sie zum Ausdruck, dass sie sich der datenschutzwidrigen Praktiken bewusst sind und diese billigen.

(3) *Anforderungen des Datenschutzrechts.* Fanpage-Betreiber sind dem ordnungsrechtlichen Zweckveranlasser strukturell ähnlich. Sie tragen in zurechenbarer Weise dazu bei, dass Facebook die datenschutzrechtliche Gefahrenschwelle überschreitet.

Für eine kollektive datenschutzrechtliche Verantwortlichkeit lässt das unionsrechtliche Datenschutzrecht zwar Raum. Anders als dem Polizeirecht, das (in engen Grenzen) eine mittelbare Verursachung – und damit eine Zweckveranlassung – ausreichen lässt, genügt dem Datenschutzrecht als Sonder-

103 *LG Potsdam*, MMR 2013, 662 mit Anm. *Timm*; vgl. dazu etwa auch *Mantz*, ZD 2014, 62; *Piltz*, K & R 2014, 80 (83 ff.); *Spindler*, GRUR 2013, 996 (1003). Das Gericht verurteilte den Admin-C einer Website wegen Datenschutzverstößen des Websitebetreibers analog § 1004 I 1 BGB als Störer zur Unterlassung. Der Admin-C (administrativer Ansprechpartner) ist der bei der DENIC (Registrierungsstelle für Domains unterhalb der Top-Level-Domain „.de") registrierte Bevollmächtigte des Domaininhabers (vgl. Nr. VIII 1 der DENIC-Domainrichtlinien).

104 Dies hebt auch das *VG Schleswig*, ZD 2014, 51 (54) hervor.

105 Siehe hierzu etwa *BVerfGE* 110, 33 (53 ff.) = NJW 2004, 2213 = NVwZ 2004, 1223 Ls. mwN.

106 Vgl. zu den engen Voraussetzungen einer analogen Anwendung zivilrechtlicher Vorschriften als Rechtsgrundlage für das Verwaltungshandeln bspw. *Wall*, Die Anwendbarkeit privatrechtlicher Vorschriften im Verwaltungsrecht, 1999, 100 ff.

107 Vgl. dazu auch die Ausführungen des *OVG Schleswig*, ZD 2014, 643 (645).

108 Vgl. zu den Merkmalen der Zweckveranlassung *Schenke*, Polizei- und Ordnungsrecht, 8. Aufl. 2013, Rn. 244 ff.; *Schoch*, Jura 2009, 360 (361). Zur Grundlegung der Rechtsfigur des Zweckveranlassers vgl. *Preußisches OVG*, PrOVG 40, 216 [217]).

109 Maßgeblich ist insoweit, ob aus der Perspektive eines objektiven Dritten zwischen dem Verhalten einer Person und dem Eintritt der Gefährdung oder Störung ein erkennbarer Wirkungs- und Verantwortungszusammenhang besteht: Je weniger das tatsächliche Geschehen von dem üblicherweise zu Erwartenden abweicht, desto eher steht der Betreffende dann in der Pflicht, hiergegen einzuschreiten (vgl. *OVG Lüneburg*, Beschl v. 26.2.2008 – 1 ME 4/08, BeckRS 2008, 33633; *Heckel*, NVwZ 2012, 88 [91]; *Schoch*, *Polizei-* und Ordnungsrecht in *ders*., Besonderes Verwaltungsrecht, 15. Aufl. 2013, 125 Rn. 189 f.).

110 In diesem Fall knüpft der Zurechnungstatbestand an die Intention des mittelbaren Verursachers an, also dessen – zumindest billigendes – Wissen und Wollen der Gefahrschwellenüberschreitung durch Dritte (so genannte subjektive Theorie, vgl. *Selmer*, JuS 1992, 97 [99 f.]). *Schenke* plädiert für einen Mittelweg: Er will dem Hintermann das gefahrenschwellenüberschreitende Verhalten des Dritten zurechnen, wenn er dieses entweder bezweckt oder es sich zwangsläufig aus seinem neutralen Vorverhalten ergibt, *Schenke* (vgl. o. Fn. 108), Rn. 245.

111 Mit dieser Prämisse befürwortet die ganz ü. M. die Rechtsfigur des Zweckveranlassers, vgl. etwa *VGH Kassel*, NVwZ 1992, 1111 (1113); *OVG Münster*, NVwZ 1997, 804 (805); *Schenke* (vgl. o. Fn. 108), Rn. 244; *Schoch*, (vgl. o. Fn. 109), Rn. 188. Allerdings finden sich auch zahlreiche Stimmen, die verfassungsrechtliche und rechtsmethodische Bedenken an der Heranziehung des Zweckveranlassers äußern, vgl. statt vieler *Beaucamp*, JA 2007, 577 (578 ff.); *Erbel*, JuS 1985, 257 (257 ff.); *Rühl*, NVwZ 1988, 577 (577 f.) mwN.

112 Vgl. *OVG Magdeburg*, Beschl. v. 24.4.2006 – 2 M 174/06, BeckRS 2008, 32935.

113 Fanpage-Betreiber verpflichten sich in Nr. I. E. der Nutzungsbedingungen für Facebook-Seiten (abrufbar unter https://de-de.facebook.com/page_guidelines.php), keine Bestimmungen für ihre Facebook-Seite einzuführen, die im Widerspruch zu den Datenverwendungsrichtlinien von Facebook stehen.

ordnungsrecht eine *Mitverursachung* für die Begründung einer datenschutzrechtlichen Verantwortlichkeit iSv § 3 VII BDSG aber nicht. Es verlangt eine *Mitentscheidung* – und modifiziert damit die Anforderungen des allgemeinen Ordnungsrechts an die Verhaltensverantwortlichkeit. Für einen allgemeinen Rückgriff auf die Rechtsfigur des Zweckveranlassers bleibt im Regime des Datenschutzrechts daher kein Raum.

bb) *Telemedienrechtliche Störerhaftung.* Anstelle der allgemeinen ordnungsrechtlichen Störerdogmatik bilden womöglich die §§ 7 ff. TMG einen normativen Ansatzpunkt für eine Mitverantwortung der Fanpage-Betreiber in sozialen Netzwerken.[114] Immerhin sind sie als telemedienrechtliche Diensteanbieter[115] auch selbst Adressat der Pflichten des § 15 TMG. Die §§ 7 ff. TMG – insbesondere die Überschrift zum Abschnitt 3 des TMG – sprechen sogar ausdrücklich von „Verantwortlichkeit".

(1) *Inhalt.* Vereinfacht ausgedrückt etablieren die §§ 7 ff. TMG ein Notice-and-take-down-Prinzip:[116] Wer, wie zB eBay oder Youtube, Dritte dazu veranlasst, auf seiner Plattform Inhalte einzustellen, ist für deren Rechtmäßigkeit nicht uneingeschränkt verantwortlich. Erlangt er aber von rechtswidrigen Fremdinhalten, insbesondere Marken- oder Urheberrechtsverletzungen bzw. Beleidigungen, positive Kenntnis, dann ist er zum Einschreiten verpflichtet (§ 7 II 2, § 10 TMG). Ebenso nimmt das TMG auch die absichtliche Zusammenarbeit mit einem Nutzer, um rechtswidrige Handlungen zu begehen, von der Privilegierung aus (§ 8 I 2 TMG).

(2) *Anwendbarkeit.* Der allgemeine Regelungsgedanke, der den §§ 7 ff. TMG zu Grunde liegt, lässt sich grundsätzlich auch für die Zurechnung in arbeitsteiligen Datenverarbeitungsprozessen in normativ stimmiger Weise fruchtbar machen: Fanpage-Betreiber sind danach dann verantwortlich, wenn sie sich die Datenverarbeitung durch Facebook über die bloße Fanpage-Einrichtung hinaus durch Nutzung von Facebook Insights zu eigen machen.

Allerdings sind die §§ 7 ff. TMG in ihrem Normzweck nicht darauf ausgerichtet, datenschutzrechtliche Primärpflichten – gleich welcher Rechtsnatur – zu *begründen;* sie lösen keine „allgemeine telemedienrechtliche Garantenstellung der Diensteanbieter" aus.[117] Sie *setzen* vielmehr eine *anderweit gesetzlich begründete* Verantwortlichkeit *voraus* – und modifizieren sie. Eine solche anderweitige ordnungsrechtliche Verantwortlichkeit des Fanpage-Betreibers besteht aber nicht.

Hinter eine Anwendung der §§ 7 ff. TMG auf datenschutzrechtliche Verantwortlichkeiten setzen auch Art. 1 V Buchst. b und Erwägungsgrund Nr. 14 S. 1 und 2 E-Commerce-Richtlinie[118] ein Fragezeichen:[119] Der Anwendungsbereich der E-Commerce-RL lässt die Regelungen der EG-Datenschutz-RL ausdrücklich unberührt.[120] Die §§ 7 ff. TMG, welche auf Art. 12 ff. E-Commerce-RL zurückgehen, regeln entsprechend lediglich haftungsrechtliche Sekundäransprüche, die Folge rechtswidriger Handlungen Dritter sind. Sie modifizieren aber nicht zugleich auch die datenschutzrechtliche Verantwortlichkeit der Diensteanbieter (vgl. auch Erwägungsgrund Nr. 14 S. 3 E-Commerce-Richtlinie). Im Unterschied dazu zielen die §§ 12 ff. TMG auf die Verarbeitung und Nutzung personenbezogener Daten durch den Anbieter selbst und damit auf dessen eigene Handlungen.[121]

Auch für eine *analoge Anwendung* der §§ 7 ff. TMG auf die datenschutzrechtliche Mitverantwortung ist kein Raum. Es fehlt insoweit an einer Regelungslücke. Denn für die Zuweisung datenschutzrechtlicher Verantwortlichkeit verweist der Gesetzgeber in § 12 III TMG auf das BDSG und die LDSGe, nicht aber auf die §§ 7 ff. TMG. Das sperrt den Rückgriff auf die §§ 7 ff. TMG. Der Begriff des Diensteanbieters schafft insbesondere keine spezialgesetzliche Verantwortlichkeitskategorie.[122] (Wahrgenommene) Regelungsdefizite des bereichsspezifischen Datenschutzrechts lassen sich insoweit nicht durch datenschutzfremde Rechtsgedanken beheben.[123]

cc) *Auswahlverantwortung aus § 11 II 1 und 4 BDSG a maiore ad minus.* Dass der Wortlaut des § 3 VII BDSG Fanpage-Betreiber nicht unmissverständlich für solche Verarbeitungsvorgänge in die Pflicht nimmt, die sie bei Dritten veranlassen, kann Schutzlücken für das Recht auf informationelle Selbstbestimmung aufreißen. Zwar ist mindestens einer der Beteiligten datenschutzrechtlich verantwortlich. Das verkleinert die drohende datenschutzrechtliche Schutzlücke,[124] schließt sie aber nicht. Denn die rechtliche Verantwortlichkeit läuft im Ergebnis leer, wenn bei Online-Portalen mit mehrschichtiger Anbieterstruktur der die Datenverarbeitung kontrollierende primäre Diensteanbieter sich deutschem Datenschutzrecht faktisch zu entziehen in der Lage ist.[125] Das setzt bedenkliche Umgehungsanreize: Der sekundäre Diensteanbieter kann so Verarbeitungsvorgänge zu seinem Nutzen veranlassen, die ihm selbst verboten wären. Ein Dritter macht sich die Hände schmutzig; der Fanpage-Betreiber wäscht die eigenen in Unschuld. Es eröffnet sich ein Weg arbeitsteiliger Verletzung deutschen Datenschutzrechts.

Dem Risiko einer Schädigung Dritter durch die Einbeziehung von Hilfspersonen tritt die Rechtsordnung mit der Figur der Auswahlverantwortlichkeit entgegen: Bei der Auswahl von Kooperationspartnern kann den am Rechtsverkehr Teilnehmenden die Verpflichtung treffen, nur solche Partner zu wählen, die nicht offensichtlich gegen Recht und Gesetz verstoßen.

114 Dies ebenfalls prüfend, im Ergebnis aber ablehnend *OVG Schleswig*, ZD 2014, 643 (645); *VG Schleswig*, ZD 2014, 51 (54).

115 Vgl. *VG Schleswig*, ZD 2014, 51 (52). Dazu auch *Jandt/Roßnagel*, ZD 2011, 160 (162), die zwischen gewerblichen und privaten Plattformnutzern unterscheiden; *Kroschwald*, ZD 2013, 388 (389); *Moos*, IT-Rechts-Berater 2012, 226 (227) sowie o. Fn. 32.

116 Vgl. etwa *Ohly*, ZUM 2015, 308 (310).

117 Vgl. *Hoffmann* in *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, vor §§ 7–10 TMG Rn. 25; *Paal* in *Gersdorf/Paal*, BeckOK InfoMedR, Ed. 7 (Stand: 1.2.2015), § 7 TMG Rn. 5 f.; *Roggenkamp/Stadler* in *Heckmann*, jurisPK-Internetrecht, 4. Aufl. 2014, Kap. 10 Rn. 70.

118 RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6. 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABl. Nr. L 178, 1.

119 In diesem Sinne bspw. *VG Schleswig*, ZD 2014, 51 (52 f.).

120 Selbst wenn man diese unionsrechtliche Abschichtung von Normkategorien nicht zwingend auch auf die – Zweckmäßigkeitskategorien folgende – Trennung des Anwendungsbereichs des BDSG und des TMG durchschlagen sieht, kommt ihr zumindest Indizwirkung zu.

121 *Spindler*, Persönlichkeitsschutz im Internet, Verhandlungen des 69. Deutschen Juristentages, 2013, F1 (F83).

122 Vgl. auch die Nachweise oben Fn. 32.

123 Das gilt auch für die Sekundärebene der zivilrechtlichen Haftung wegen rechtswidriger Datenverarbeitung. Diese hat in § 7 f. BDSG eine allgemeine datenschutzrechtliche Regelung erfahren. Die §§ 7 ff. TMG sind insoweit nicht leges speciales. Bereichsspezifisches Datenschutzrecht enthält das TMG entsprechend seiner Gesetzessystematik nur im vierten Abschnitt (also in den §§ 11 ff. TMG).

124 Darauf eine fehlende Verantwortlichkeit des Fanpage-Betreibers stützend *OVG Schleswig*, ZD 2014, 643 (645).

125 Vgl. auch die Befürchtung von Karg, ZD 2013, 54 (56) sowie die bestehende Rechtsunsicherheit, ob und in welchem Umfang die Facebook Germany GmbH oder die Facebook Ireland Ltd und ihr Mutterkonzern datenschutzrechtlichen Aufsichtsbefugnissen welcher Aufsichtsbehörde unterliegen; dazu Fn. 172.

(1) *Inhalt und dogmatische Herleitung.* Eine Auswahlverantwortlichkeit desjenigen, der sich Dritter bedient, die er im eigenen Pflichtenkreis mit einer bestimmten Aufgabe betraut und von deren Leistungen er profitieren will, verankert insbesondere § 11 II 1 und 4 BDSG normativ – allerdings nur für den Auftraggeber einer Auftragsdatenverarbeitung.

An einem Auftragsverhältnis iSv § 11 BDSG mangelt es beim Betrieb von Fanpages.[126] Das schließt eine Pflichtenbindung des Fanpage-Betreibers für eine ordnungsgemäße Auswahl des Kooperationspartners aber nicht aus. Der Fanpage-Betreiber profitiert wie ein Auftraggeber von der Verarbeitung, die ein Dritter für ihn vornimmt. Zwar fehlt ihm die Möglichkeit der Steuerung des Verarbeitungsprozesses. Der Handlungsablauf ist für ihn aber in Grundzügen bereits in dem Moment voraussehbar, in dem er sich des Werkzeugs Facebook bedient.

Wäre er als Nutzer fremder technischer Infrastruktur nicht mehr für Rechtsverstöße verantwortlich, für die er nach §§ 12 ff. TMG verantwortlich wäre, wenn er die Infrastruktur selbst betriebe, könnte er durch geschickte Auswahl eines Betreibers von datenschutzrechtswidrigen Praktiken profitieren. Er könnte Verarbeitungsvorgänge, die ihm selbst untersagt sind, dadurch im Ergebnis für sich verwerten, dass er sich bewusst des rechtswidrigen Handelns eines Dritten bedient. Kein Apfel schmeckt dann besser als der vom verbotenen Baum.

Diese dysfunktionale Anreizstruktur kann es legitimieren, den Fanpage-Betreiber ähnlichen Bindungen zu unterwerfen wie den Auftraggeber einer Auftragsdatenverarbeitung. Bedient sich ein Diensteanbieter zur Diensterbringung keines Auftragsdatenverarbeiters, sondern eines Dritten und gesteht er diesem eine größere Freiheit zu, als er sie einem Auftragnehmer bei der Auftragsdatenverarbeitung einräumen dürfte, unterliegt er bei konsequenter Fortschreibung des gesetzgeberischen Schutzkonzepts erst recht den Anforderungen an eine sorgfältige Auswahl: Wenn schon die Auftragsdatenverarbeitung einer strengen Auswahlkontrolle unterliegt, dann umso mehr die Einbindung eines Dritten für eigene Zwecke bei Nichtbeachtung der Voraussetzungen des § 11 BDSG. Das deutet auch die materielle Wertung des Bußgeldtatbestandes des § 43 I 1 Nr. 2 b BDSG an: Er schlägt die ordnungswidrigkeitenrechtliche Verantwortlichkeit für Versäumnisse bei der Auftragserteilung – auch bei der Auswahl des Auftragnehmers – dem Auftraggeber zu.[127] Jede Form der Einschaltung Dritter für Datenverarbeitungen will das Gesetz damit sehr strengen Schranken unterwerfen, insbesondere Umgehungen des gesetzlichen Schutzinstrumentariums einen Riegel vorschieben.

Legt man diese Rechtsgedanken zu Grunde, befreit sich ein Fanpage-Betreiber, der via Facebook Insights unter Verstoß gegen deutsches Datenschutzrecht in eigenem Interesse Verarbeitungsvorgänge vornehmen lässt, nicht von seiner Auswahlverantwortung.[128] Dies ergibt sich aus einer *Anwendung des § 11 II 1 und 4 BDSG a maiore ad minus*. Selbst wenn den Diensteanbieter bei arbeitsteiligen Verarbeitungsstrukturen im digitalen Raum keine unmittelbare Verantwortung für die *Verarbeitung* der Nutzungsdaten trifft, so doch sehr wohl eine Verpflichtung zur ordnungsgemäßen *Auswahl* seines Kooperationspartners.

(2) *Das verwaltungsrechtlichen Analogieverbot als Schranke.* Eine entsprechende Anwendung des § 11 II 1 und 4 BDSG tritt in eine Spannungslage mit dem verwaltungsrechtlichen Analogieverbot.[129] Der Vorbehalt des Gesetzes schließt nämlich eine Ausweitung von Befugnissen über den Tatbestand hinaus grundsätzlich aus.[130] Eine solche geht mit einer Auswahlverantwortlichkeit des telemedienrechtlichen Diensteanbieters jedoch nicht einher. Vielmehr liegt die Auswahlverantwortlichkeit in der Konsequenz des gesetzlichen Regelungskonzepts.

Ein Blick auf die Funktion des § 11 BDSG macht das deutlich. Der Tatbestand der Auftragsdatenverarbeitung privilegiert eine Gruppe von datenschutzrechtlichen Sachverhalten: Ein Auftraggeber darf Dritte in die Datenverarbeitung einbinden, ohne den Anforderungen an eine Übermittlung von Daten genügen zu müssen.[131] Er muss dafür aber strengen Auswahl- und Kontrollpflichten genügen. Sind die Voraussetzungen des § 11 BDSG – wie im Falle des Facebook-Fanpage-Betreibers – nicht eingehalten, ist die Kooperation mit dem Dritten als Funktionsübertragung dafür regelmäßig den Anforderungen an eine Datenübermittlung unterworfen. Im Falle des Fanpage-Betriebs greifen diese Anforderungen der §§ 4 ff. BDSG aber nicht, weil der Nutzer die fraglichen Daten direkt an Facebook übermittelt und nicht über den Umweg des Fanpage-Betreibers. Die Verortung der Kooperation in der Web-2.0-Infrastruktur des Netzwerkbetreibers macht eine Datenübermittlung entbehrlich.

Eine solche Möglichkeit der Informationsgewinnung durch Aufgabenauslagerung auf soziale Netzwerke hatte der Gesetzgeber nicht im Blick. Sein normatives Programm hat sie aber in der Sache mitgedacht. Indem er eine Auftragsdatenverarbeitung strengen Bindungen unterwirft, muss das für eine Verarbeitung durch einen Dritten, die nicht mit einer Übermittlung einhergeht, erst recht gelten. Sonst wäre einem Race-to-the-bottom-Wettbewerb Tür und Tor geöffnet, der das legislative Konzept contra legem auszuhöhlen in der Lage ist. Die Kooperation eines Fanpage-Betreibers mit Facebook erhöht insbesondere in gleicher Weise die Gefahr für die informationelle Selbstbestimmung wie die (datenschutzrechtlich als Übermittlung zu wertende) Zusammenarbeit zwischen Facebook und einem Webseiten-Betreiber, der den Facebook „Gefällt-mir"-Button in sein Angebot einbindet und dafür datenschutzrechtlich verantwortlich ist.[132]

(3) *Umfang der Einstandspflicht privater und öffentlicher Stellen.* Eine Auswahlverantwortlichkeit impliziert kein Einstehenmüssen für jeden Fehler des Dritten. Sie findet ihre Grenze in der Zumutbarkeit.[133] *Private Stellen* verletzen ihre Auswahlverantwortlichkeit nur, wenn sie um Datenschutzverstöße des ausgewählten Kooperationspartners entweder positiv wissen oder aber infolge ihrer Offensichtlichkeit wissen müssen.

126 Siehe dazu oben II. 1. a) bb), Seite 9 f.

127 Vgl. etwa *Gola/Klug/Körffer* in *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 43 Rn. 6 b.

128 Die Ordnungspflicht des Fanpage-Betreibers tritt zu derjenigen von Facebook vielmehr hinzu. Vgl. *Dammann* (vgl. o. Fn. 30), § 3 BDSG Rn. 228; *Plath* (vgl. o. Fn. 57), § 11 BDSG Rn. 40. In diesem Sinne auch *Artikel-29-Datenschutzgruppe* (vgl. o. Fn. 34), 31. Wann das der Fall sein soll, lässt das Gesetz (anders als zukünftig Art. 26 IV iVm Art. 24 EU-Datenschutz-Grundverordnung) offen.

129 Vgl. dazu *BVerfG*, NJW 1996, 3146 = NVwZ 1997, 53 Ls.; *Beaucamp*, AöR 134 (2009), 83 ff.; *Konzak*, NVwZ 1997, 872; *Sachs* in *Stelkens/Bonk/Sachs*, VwVfG, 8. Aufl. 2014, § 44 Rn. 54; *Schmidt*, VerwArch. 96 (2006), 139 ff.

130 Vgl. *Bach*, Das Analogieverbot im Verwaltungsrecht, 2011, 104 ff.

131 Dazu auch Fn. 58.

132 In diesen Fällen überträgt der Homepage-Betreiber selbst personenbeziehbare Daten an Facebook. Wer die Schnittstelle in seine Homepage einbindet, entscheidet über den Zweck und die Mittel der Datenverarbeitung mit. Denn er steuert bewusst einen Datenfluss an einen Dritten. Insbesondere löst er die Übermittlung der IP-Adresse an den Dritten aus (zum [umstrittenen] Personenbezug von IP-Adressen s. den Vorlagebeschluss des *BGH* an den *EuGH*: *BGH*, ZD 2015, 80). Vgl. auch Fn. 38.

133 Zum Merkmal der Offensichtlichkeit und Zumutbarkeit bei der telemedienrechtlichen Haftung s. etwa *BGH*, GRUR 2015, 485 = NJW 2015, 2122 Ls. = CR 2015, 386 (388 Rn. 50 f.) mwN.

Öffentliche Stellen sind insoweit strengeren Sorgfaltsmaßstäben ausgesetzt. Denn sie trifft beim Umgang mit Daten der Bürger eine unmittelbare Grundrechtsbindung.

Ihnen sind Facebooks Datenschutzrechtsverstöße zum einen jedenfalls dann als eigener mittelbar-faktischer Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen zuzurechnen, wenn sie die Verstöße zum Zwecke staatlichen Informationshandelns nicht nur begünstigen, sondern bei der Profil- und Nutzungsdatenauswertung jedenfalls billigend in Kauf nehmen.[134]

Zum anderen ist die besondere Auswahlverantwortung öffentlicher Stellen Ausfluss ihrer verfassungsrechtlichen Pflicht, die informationelle Selbstbestimmung der Bürger vor Übergriffen Privater zu schützen.[135] Das Gebot effektiver Durchsetzung der einfachgesetzlichen Normen des Datenschutzrechts steuert die sachgerechte Ausübung des behördlichen Entschließungs- und Auswahlermessens bei der ordnungsrechtlichen Aufgabenwahrnehmung.[136] Öffentliche Stellen sind dazu verpflichtet, Datenschutzrechtsverstöße Privater nicht durch eigenes Verhalten zu fördern und so die Durchsetzung des Datenschutzrechts zu erschweren. Sie trifft insoweit eine informatorische Verkehrssicherungspflicht im virtuellen Raum, aus der sich eine Auswahlverantwortlichkeit für diejenigen ergibt, welche die öffentliche Stelle auf diesen Raum als Kooperationspartner einwirken lässt. Darüber hinaus nehmen öffentliche Stellen bei der Teilnahme am Datenverkehr eine besondere Vorbildfunktion wahr.

Die Sorgfaltspflichten öffentlicher Stellen sind auch nicht deshalb weniger streng, weil sie durch ihre Fanpage Öffentlichkeitsarbeit bzw. amtliches Informationshandeln ausüben.[137] Die Rechtsprechung legt an solches Handeln zwar niedrigere Zulässigkeitsanforderungen an.[138] Diese berühren aber nur die Rechtsbeziehungen zwischen der staatlichen Stelle und dem von der Information (bspw. einer Warnung) mittelbar grundrechtlich Betroffenen, nicht hingegen die Beziehung zu den durch das Informationsmedium unmittelbar adressierten Dritten.

b) *Adressatenkreis von Ordnungsmaßnahmen nach § 38 V BDSG*. Gegen den Fanpage-Betreiber ist eine Datenaufsichtsbehörde nur dann vorzugehen befugt, wenn § 38 V BDSG den Kreis der Ordnungspflichtigen nicht auf verantwortliche Stellen iSv § 3 VII BDSG beschränkt. Denn den Fanpage-Betreiber trifft zwar eine Auswahlverantwortlichkeit, er ist aber nicht verantwortliche Stelle iSd § 3 VII BDSG.[139] Ob der Adressatenkreis der Norm auch Dritte iSd § 3 VIII 1 BDSG erfasst,[140] ist bislang ungeklärt.

aa) *Wortlaut*. § 38 V BDSG selbst schweigt sich zu der Person des Anordnungsadressaten aus.[141] Die Norm hat zwar unausgesprochen vorrangig den datenschutzrechtlich Verantwortlichen im Auge. Statt einen bestimmten Adressaten zu benennen, richtet die Norm ihr normatives Programm auf den Erfolg aus: Sie erklärt die „Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten“ zum aufsichtsrechtlichen Handlungsauftrag. Das impliziert, auch Dritte iSv § 3 VIII 2 BDSG in die Pflicht zu nehmen.[142] Denn sie können, etwa durch Deaktivierung ihres den Datenfluss stimulierenden Angebots, ebenfalls in der Lage sein, eine datenschutzrechtliche Störung zu beseitigen, auch wenn sie nicht unmittelbar an der Datenverarbeitung mitwirken.

bb) *Historische Auslegung*. Die Gesetzesinitiative des Bundesrates, auf welche die aktuelle Fassung des § 38 V BDSG zurückgeht, deutet prima facie auf eine andere Sichtweise hin.[143] Sie regt auf der Grundlage bekannt gewordener Datenschutzverstöße und von Erfahrungen beim Gesetzesvollzug an, die Anordnungsbefugnisse der Aufsichtsbehörden zur Beseitigung materiell rechtswidriger Datenverarbeitung zu erweitern. Bis dato konnte die Aufsichtsbehörde von ihren Befugnissen lediglich bei technischen und organisatorischen Mängeln der Datenverarbeitung, also bei formellen Verstößen, Gebrauch machen.[144]

Daraus ergibt sich allerdings nicht zwingend, dass die Norm nur die verantwortliche Stelle iSv § 3 VII BDSG in die Pflicht nimmt.[145] War Zielsetzung des Gesetzes eine Effektivierung des Gesetzesvollzugs, ist dem nicht ein enger, sondern ein weiter Zuschnitt des Adressatenkreises zuträglich.

cc) *Systematik*. Auch der systematische Zusammenhang zwischen § 38 V BDSG und § 3 VII BDSG[146] begrenzt den Adressatenkreis der Aufsichtsbehörde nicht auf verantwortliche Stellen. Entsprechend seiner Stellung im Gesetz *definiert* § 3 VII BDSG den Begriff der verantwortlichen Stelle; er bestimmt, wer für die Einhaltung der Datenschutzbestimmungen verantwortlich ist und gegenüber wem Betroffene Rechte geltend machen können.[147] Die Reichweite der Rechte und Pflichten, welche das materielle Datenschutzrecht begründet, legt er aber nicht abschließend fest. Vielmehr aktiviert er seine Wirkung nur, wenn die einzelnen datenschutzrechtlichen Anspruchs- und ordnungsrechtlichen Ermächtigungsnormen den für die Datenverarbeitung Verantwortlichen in Bezug nehmen.

Regelmäßig benennt das BDSG die verantwortliche Stelle in den Verpflichtungsnormen explizit als Adressaten datenschutzrechtlicher Pflichten.[148] In einigen Tatbeständen verzichtet das BDSG aber darauf[149] bzw. weist Dritten iSv § 3 VIII 2 BDSG datenschutzrechtliche Pflichten zu.[150] In

134 In diese Richtung auch *Caspar*, ZD 2015, 12 (15) der die öffentliche Stelle auch unabhängig von einer datenschutzrechtlichen Verantwortlichkeit als verpflichtet ansieht, das informationelle Selbstbestimmungsrecht der Bürger nicht mittelbar zu verletzen.

135 Zu dieser Schutzpflicht vgl. *BVerfGE* 117, 202 (229) = StAZ 2007, 113 = NJW 2007, 753; *BVerfG*, MMR 2007, 93 (93 f.). Siehe außerdem *Gurlit*, NJW 2010, 1035 (1040 f.); *Kühling*, DV 40 (2007), 153; *Kutscha*, ZRP 2010, 112 (113); *Schliesky/Hoffmann/Luch/Schulz/Borchers*, Schutzpflichten und Drittwirkung im Internet, 2014, 104 ff. jew. mwN.

136 Vgl. allgemein zu den Wirkungsdimensionen grundrechtlicher Schutzpflichten *Isensee*, § 191 – Das Grundrecht als Abwehrrecht und staatliche Schutzpflicht in *Isensee/Kirchhof*, HdbStR IX, 3. Aufl. 2011, Rn. 267, 281 ff.

137 Das gilt unabhängig davon, ob der Betrieb einer Fanpage als informelles hoheitliches Handeln oder aber als privatrechtliches Handeln der öffentlichen Hand einzustufen ist. Vielmehr verhindert das allgemeine Verbot der Flucht aus der Verantwortung durch Formenwahl (*BVerfGE* 128, 226 [244 f.] = NJW 2011, 1201) eine Umgehung grundrechtlicher Schutzpflichten. Das Datenschutzrecht macht die Anwendung der Datenschutzvorschriften für den öffentlichen Bereich entsprechend nicht von der Handlungs-, sondern von der öffentlich-rechtlichen Organisationsform der verantwortlichen Stelle abhängig.

138 Vgl. BVerfGE 105, 252 (268 ff.) = NJW 2002, 2621 = NVwZ 2002, 1495 Ls.

139 Dazu oben II. 1., Seite 7 ff.

140 Dies verneinend *OVG Schleswig*, ZD 2014, 643 (644 f.).

141 Nichts anderes gilt für die Kommentarliteratur. Sie geht auf die Frage nach dem richtigen Adressaten regelmäßig nicht ein. Anders aber (zutreffend) *Petri* (vgl. o. Fn. 65), § 11 BDSG Rn. 21: § 38 V „kennt keine Beschränkung aufsichtsbehördlicher Maßnahmen auf verantwortliche Stellen“.

142 Anders aber das *OVG Schleswig*, ZD 2014, 643 (645).

143 *OVG Schleswig*, ZD 2014, 643 (645).

144 Vgl. *Bundesrat*, Stellungnahme zum Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BT-Drs. 16/12011 vom 18.2.2009, Anlage 3, 44.

145 In diesem Sinne aber *OVG Schleswig*, ZD 2014, 643 (645).

146 Nichts anderes gilt für die unionsrechtlichen Normendeterminanten des Art. 2 Buchst. d und Art. 28 III Datenschutz-RL.

147 Vgl. *Artikel-29-Datenschutzgruppe* (vgl. o. Fn. 34), 6.

148 Vgl. ua § 4 III, § 4 d I, § 19 I, §§ 33, 34 BDSG.

149 Vgl. §§ 4, 6 a, 6 b, 13 ff. ua BDSG.

150 Vgl. etwa §§ 6 c, 10 II BDSG.

adressatenoffen formulierten Tatbeständen wie § 38 V BDSG besteht dann Auslegungsspielraum für Verantwortlichkeiten jenseits des § 3 VII BDSG. In diese Richtung deutet ein Stück weit mittelbar auch § 11 IV Nr. 2 BDSG. Er stellt durch seinen Verweis auf § 38 BDSG klar, dass neben dem für die Verarbeitung verantwortlichen Auftraggeber ebenso der Auftragnehmer der Datenschutzaufsicht unterliegt. Auch nicht verantwortliche Stellen können also Adressaten einer Verfügung iSd § 38 V BDSG sein. Der Verweis lässt sich freilich auch anders deuten: nämlich dahin, dass die Einbeziehung nicht verantwortlicher Stellen in den Zugriffsradius des § 38 V BDSG stets einer ausdrücklichen normativen Grundlage bedarf. Zwingend ist dieser Schluss aber nicht. Näher liegt ein Verständnis der Regelung als gesetzgeberische Klarstellung, die eine normativ ohnedies bestehende Aufsichtsbefugnis unmissverständlich, aber ohne Anspruch auf abschließenden Charakter zum Ausdruck bringt (nicht zuletzt erweitert § 11 IV BDSG nach seinem Wortlaut nicht den Reigen der auf den Auftragnehmer anzuwendenden datenschutzrechtlichen Regelungen, sondern schränkt ihn ein [„für den Auftragnehmer gelten (…) nur"]).

Der weite Begriff des Diensteanbieters iSd § 2 S. 1 Nr. 1 TMG[151] überschreibt zwar nicht den bundesdatenschutzgesetzlichen Begriff der verantwortlichen Stelle. Er erweitert aber den Kreis der *Aufsichtspflichtigen* dort, wo das BDSG – wie in § 38 V BDSG – die Aufsichtsbefugnis nicht auf Maßnahmen gegenüber dem datenschutzrechtlich Verantwortlichen beschränkt. Aufsichtsbefugnis und Handlungs-, insbesondere datenschutzrechtliche Beseitigungspflicht, müssen insoweit miteinander korrelieren. Adressiert eine datenschutzrechtliche Vorschrift einen Handlungsträger nicht, ist er grundsätzlich auch keiner ordnungsrechtlichen Beseitigungspflicht unterworfen. Voraussetzung einer Beseitigungspflicht iSd § 38 V BDSG ist danach eine datenschutzrechtliche Verhaltenspflicht. Eine solche folgt für den Fanpage-Betreiber aus § 11 II 1 BDSG a maiore ad minus.[152] Die Aufsichtsbehörde kann daher aus systematischer Perspektive bei Verstößen gegen § 15 III, § 13 I TMG iVm § 11 II 1, 4 BDSG auch gegenüber dem Fanpage-Betreiber als Diensteanbieter zu Aufsichtsmaßnahmen nach § 38 V BDSG greifen.

dd) *Teleologische Auslegung.* Die grundrechtliche Schutzpflicht aus Art. 2 I iVm Art. 1 I GG[153] fordert dem Gesetzgeber eine wirksame Ausgestaltung des aufsichtsrechtlichen Datenschutzinstrumentariums ab. Der Gesetzgeber verfügt insoweit über weitreichende Spielräume, um gegenläufige Grundrechtspositionen angemessen auszubalancieren.[154] Die zunehmende Verschiebung des Gefährdungsschwerpunkts informationeller Selbstbestimmung aus dem hoheitlichen in den nicht-öffentlichen Bereich[155] unterstreicht allerdings die Notwendigkeit abwehrgeeigneter Aufsichtsbefugnisse, insbesondere gegenüber datenschutzwidrig agierenden privaten Internetkonzernen und den Multiplikatoren ihrer Verstöße.

Mit der ordnungsrechtlichen Ermächtigungsnorm des § 38 V BDSG gibt der Gesetzgeber den Aufsichtsbehörden seit 2009 die hierfür geforderten Kontroll- und Durchsetzungsmechanismen an die Hand. Dabei zielt er – mit Blick auf das Untermaßverbot als äußerste Grenze seines Gestaltungsspielraums[156] – auf eine effektive Bewehrung der Aufsichtsbehörden. Dies erfordert hinreichende Möglichkeiten zur Durchbrechung schadensbegründender Kausalverläufe. Es entspricht daher einer zweckgerechten Auslegung des § 38 V BDSG, den adressatenbezogenen Interpretationsspielraum im Interesse effektiver Schutzpflichtverwirklichung (zusätzlich zum unmittelbaren Verhaltensstörer iSd § 3 VII BDSG) auch auf Dritte zu erstrecken.[157]

ee) *Unionsrechtlicher Rahmen.* Auch das Unionsrecht beschränkt die Befugnis zur Anordnung aufsichtsrechtlicher Maßnahmen nicht auf bestimmte Adressaten (Art. 28 III Spstr. 2 der Datenschutzrichtlinie).[158] Das tut es explizit nur für die Befugnis zum Erlass einer Verwarnung oder Ermahnung – in allen anderen Fällen[159] im Umkehrschluss aber nicht.[160]

Die EG-Datenschutz-RL zielt grundsätzlich nicht auf eine Mindest-, sondern auf eine Vollharmonisierung des unionalen Datenschutzniveaus.[161] Den Mitgliedstaaten ist es daher grundsätzlich nicht nur verwehrt, die in der EG-Datenschutz-RL vorgesehenen Schutzstandards zu unterschreiten; sie dürfen auch nicht über sie hinausgehen. Das hindert das deutsche Recht aber nicht, neben dem datenschutzrechtlich Verantwortlichen auch weitere Personen als Störer zu

151 Zum personellen Anwendungsbereich des TMG vgl. *Martini* in *Gersdorf/Paal*, BeckOK InfoMedR, Ed. 7 (Stand: 1.2.2015), § 1 TMG Rn. 16 f. § 11 I TMG modifiziert den allgemeinen Anwendungsbereich des TMG für dessen datenschutzrechtlichen Abschnitt nur in sachlicher Hinsicht (er nimmt namentlich die Bereitstellung solcher Dienste vom Anwendungsbereich aus, die im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder innerhalb von bzw. zwischen nicht-öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von Arbeits- oder Geschäftsprozessen erfolgt). Der personelle Anwendungsbereich, den § 1 I 2 TMG bestimmt, erstreckt sich auch auf die Datenschutzvorschriften der §§ 12 ff. TMG und ist somit bereichsspezifisches Datenschutzrecht, dessen Anwendung nicht durch die unionsrechtlich vorgegebene Abschichtung telemedien- und datenschutzrechtlicher Normkategorien (dazu oben Seite 22) gesperrt ist. Diese Normen gehen dem allgemeinen Datenschutzrecht vor.

152 Dazu im Einzelnen oben II. 2. a) cc), Seite 22 ff.

153 Vgl. hierzu Fn. 135.

154 Vgl. *BVerfGE* 117, 202 (227) = *StAZ* 2007, 113 = NJW 2007, 753; sowie allgemein für die Schutzpflichtverwirklichung *BVerfGE* 77, 170 (214) = NJW 1988, 1651. Siehe auch *Nettesheim*, VVDStRL 70 (2011), 7 (40).

155 Dazu *Gurlit*, NJW 2010, 1035 (1039 ff.); *Masing*, NJW 2012, 2305 (2306 f.); *Nettesheim*, VVDStRL 70 (2011), 7 (32 f., 38).

156 Dazu grundlegend *BVerfGE* 88, 203 (254 f.) = NJW 1993, 1751 sowie zu seiner Herleitung und Operationalisierung auch *Calliess*, FS Starck, 2007, 201 (202 ff.).

157 Zur Relevanz der grundrechtlichen Schutzpflicht bei der Normanwendung und –auslegung einfachen Rechts vgl. *Di Fabio* in *Maunz/Dürig*, GG, Ed. 39 (Stand: Juli 2011), Art. 2 Rn. 136.

158 Dass für die Bestimmung des aufsichtsrechtlichen Adressatenkreises in erster Linie Art. 28 III maßgeblich ist, lässt das *OVG Schleswig* unberücksichtigt: Es stellt in seiner Entscheidung ua darauf ab, dass nach Art. 23 I Schadensersatz wegen Datenschutzverstößen nur von dem für die Verarbeitung Verantwortlichen verlangt werden kann (vgl. *OVG Schleswig*, Urt. v. 4.9.2014 – 4 LB 20/13, BeckRS 2014, 55993 (insoweit in ZD 2014, 643 nicht abgedruckt). Art. 23 I der Richtlinie bezieht sich allerdings allein auf die zivilrechtliche Haftung. Deshalb lassen sich der Norm nicht als Minus auch Aussagen zum Adressatenkreis ordnungsrechtlicher Unterlassungsverfügungen entnehmen. Anderer Ansicht *Piltz*, K & R 2014, 80 (84).

159 Insbesondere für die Anordnung einer Sperrung, Löschung oder Vernichtung von *Daten* oder eines vorläufigen oder endgültigen Verarbeitungsverbots.

160 Immerhin lässt sich argumentieren, dass die Ermahnung oder Verwarnung im Verhältnis zu den anderen genannten Maßnahmen ein weniger scharfes Schwert ist und daher nicht davon auszugehen ist, dass tiefer eingreifende Maßnahmen dann gegen jeden Dritten verhängt werden dürfen, wenn die mildere Maßnahme schon auf den Verantwortlichen beschränkt ist. In diesem Sinne *OVG Schleswig*, Urt. v. 4.9.2014 – 4 LB 20/13, BeckRS 2014, 55993 (insoweit in ZD 2014, 643 nicht abgedruckt). Allerdings gestaltet die Richtlinie das Verhältnis der einzelnen Maßnahmen im Gesetz insoweit nicht eindeutig aus. Die Verwarnung enthält einen Schuldvorwurf und setzt insoweit eine Verantwortlichkeit voraus; die Löschung oder Sperrung von Daten zielt demgegenüber auf einen Erfolg, der im Interesse umfassenden Persönlichkeitsschutzes auch Dritten eine Handlungspflicht abverlangen kann.

161 Das ergibt sich daraus, dass die Richtlinie auf einen freien Binnenmarktverkehr personenbezogener Daten bei gleichzeitiger Herstellung eines hohen und äquivalenten Schutzniveaus für die Rechte der von der Datenverarbeitung Betroffenen in allen Mitgliedstaaten zielt, vgl. Erwägungsgrund Nr. 3 ff. (insbesondere Nr. 8 und 10) EG-Datenschutz-RL. StRspr des *EuGH*, ECLI:EU:C:2003:294 = Slg. 2003, I-4989 = BeckRS 2004, 77378 Rn. 96 – Österreichischer Rundfunk ua; *EuGH*, ECLI:EU:C:2008:724 = Slg 2008, I-9705 (9725) = NVwZ 2009, 379 Rn. 51 – Huber.

adressieren.[162] Denn die Richtlinie eröffnet den Mitgliedstaaten dort gesetzgeberische Freiräume, wo sie – wie in Art. 28 III – mit interpretationsoffenen Rechtsbegriffen oder beispielhaft aufgezählten Optionen (anstelle eines abschließenden Befugniskatalogs) hantiert.[163]

Insbesondere ist es dem Unionsrecht ein Anliegen, für seinen wirksamen Vollzug gegenüber all denjenigen zu sorgen, die sich über unionsrechtliche Datenschutzpflichten hinwegsetzen. Die RL 95/46 zielt – wie sich aus ihrem Art. 1 und ihrem 10. Erwägungsgrund ergibt – darauf ab, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihrer Privatsphäre, bei der Verarbeitung personenbezogener Daten zu gewährleisten.[164] Es entspricht daher dem Telos des Unionsrechts, das „Durchdrücken teils niedrigerer amerikanischer Datenschutzstandards“[165] auch durch eine weite Interpretation der datenschutzrechtlichen Ordnungspflicht entgegenzutreten. Dass Art. 28 III Spstr. 2 weitere Personen neben dem für die Datenverarbeitung Verantwortlichen nicht ausdrücklich nennt, steht dem nicht entgegen. Die Figur der Auswahlverantwortlichkeit schafft nämlich keinen neuen, von der EG-Datenschutz-RL nicht vorgesehenen Haftungsgrund, sondern konkretisiert die personelle Zurechnung im Zusammenhang mit kontrollbehördlichen Befugnissen nach Art. 28 III EG-Datenschutz-RL.

c) *Verhältnismäßigkeit, insbesondere ermessensgerechte Störerauswahl.* § 38 V BDSG nimmt den Auswahlverantwortlichen nur in den Grenzen der Verhältnismäßigkeit in Haftung; ihm liegt ein Konzept gestufter Verantwortlichkeit zu Grunde – und zwar unter mehreren Gesichtspunkten: dem Gedanken eigenverantwortlicher Selbstgefährdung (aa), der Störerauswahl und dem Stufenverhältnis zwischen § 38 V 1 und 2 BDSG (bb).

aa) *Eigenverantwortung.* Der Besuch von Fanpages ist Ausdruck einer privatautonomen Selbstgefährdung. Facebook-Nutzer nehmen die Datenschutzlücken des sozialen Netzwerks insoweit grundsätzlich bewusst in Kauf. Die Eigenverantwortung der Betroffenen setzt einer Verkehrssicherungspflicht Grenzen.

Auf Nichtmitglieder des sozialen Netzwerks trifft das allerdings nur bedingt zu. Denn diese gelangen oftmals über eine Suchmaschine oder einen Link auf einer Webseite mehr oder minder unbewusst auf die Fanpage.

Ebenso wie der Betrieb eines Ladengeschäfts in der analogen Welt muss der Betrieb einer Online-Präsenz zugleich aber nicht absolut gefahrlos sein. Die (hinter der Auswahlverantwortlichkeit stehende) informatorische Verkehrssicherungspflicht virtueller Räume erstreckt sich nur auf diejenigen Maßnahmen, die ein umsichtiger und verständiger, in vernünftigen Grenzen vorsichtiger Mensch für notwendig und ausreichend erachtet, um andere vor Schäden zu bewahren.[166] Zusätzliche Datenschutzinformationen auf der Fanpage, welche die Defizite der Datenschutzrichtlinie von Facebook ausgleichen, oder eine Platzierung einer Warnung vor dem gefahrenträchtigen Zustand können insoweit genügen.[167] Das kann einer sachgerechten Abwägung des Publikumsinteresses an einem Facebook-Auftritt und der grundsätzlichen Eigenverantwortlichkeit der Nutzer von Telemedien mit der besonderen Vertrauenserwartung an Informationsangebote und den staatlichen Schutzpflichten genügen. Facebooks Infrastruktur lässt für solche Maßnahmen technisch allerdings nur sehr beschränkt Raum.

bb) *Störerauswahl sowie Stufenverhältnis zwischen § 38 V 1 und 2 BDSG.* Kommen zur Beseitigung eines Datenschutzverstoßes mehrere Störer als Ordnungspflichtige in Betracht, hat die Aufsichtsbehörde ihr Auswahlermessen – entsprechend allgemeinen ordnungsrechtlichen Grundsätzen – am Prinzip effektiver Gefahrenabwehr auszurichten.[168] Daraus ergibt sich das Gebot, vorrangig gegen Facebook vorzugehen. Denn nur das soziale Netzwerk kann durch Änderung seiner Datenverarbeitungspraxis die ordnungsrechtliche Störung flächendeckend beseitigen. Die Deaktivierung einzelner Fanpages behebt Facebooks strukturelle Datenschutzrechtsverstöße demgegenüber nicht. Die Fanpage ist nicht des Übels Wurzel, sondern seine Frucht.

Diesen Verhältnismäßigkeitsüberlegungen trägt auch das Stufenverhältnis des § 38 V 1 und 2 BDSG Rechnung. Es lässt Untersagungsanordnungen nur bei Erfolglosigkeit einer vorherigen Beseitigungsanordnung zu.[169] Die Inanspruchnahme des Fanpage-Betreibers kommt daher nur als Ultima Ratio in Betracht, wenn zuvor eine Beseitigungsanordnung gegen Facebook[170] ergangen, aber erfolglos geblieben ist.[171]

162 So *Mantz*, ZD 2014, 62 (64 f.).
163 Vgl. dazu *Brühann*, EuZW 2009, 639 (642 f.).
164 Vgl. zB *EuGH*, NJW 2014, 2257 Rn. 66 = NVwZ 2014, 857.
165 Vgl. *Kühling*, EuZW 2014, 527 (527).
166 Vgl. für die stRspr *BGHZ* 195, 30 = NJW 2013, 48 mwN.
167 Technisch vorstellbar ist grundsätzlich auch eine Zwei-Klick-Lösung, die den Weg zur Fanpage nur nach Bestätigung öffnet und damit Unzulänglichkeiten von Datenschutzerklärungen durch eigene Information ausgleicht. Eine entsprechende Programmierung ist dem Fanpage-Betreiber aber nur möglich, wenn die Fanpage über einen Link auf seiner eigenen Webseite aufgerufen wird. Greifen die Nutzer hingegen – wie in der Mehrzahl der Fälle – über die Facebook-Suche oder einen Suchmaschineneintrag bei Google & Co. auf die Fanpage zu, hat der Fanpage-Betreiber technisch derzeit keine Möglichkeit, dem Zugriff ein Informations-Plugin vorzuschalten.
168 Zum Gebot effektiver Gefahrenabwehr als vorrangigem Maßstab für die Störerauswahl vgl. *Schoch* (vgl. o. Fn. 109), Rn. 227 ff. Vgl. dazu im Hinblick auf die Auswahl zwischen unmittelbar Verhaltensverantwortlichem und Zweckveranlasser *VGH Kassel*, NVwZ 1992, 1111 (1113).
169 Vgl. dazu *OVG Schleswig*, ZD 2014, 643.
170 Für öffentliche Stellen bestehen insoweit Besonderheiten: Die datenschutzrechtliche Kontrolle ihrer Fanpage-Angebote obliegt gem. § 24 BDSG bzw. den entsprechenden landesdatenschutzrechtlichen Regelungen zwar ebenso dem Bundes- bzw. den Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Allerdings können sie Datenschutzmängel bei der Tätigkeit öffentlicher Stellen lediglich formell beanstanden; sie verfügen über keine Handhabe, um festgestellte Verstöße hoheitlich zu unterbinden oder zu beseitigen. Diese beschränkte Aufsichtsgewalt ist Ausdruck der fehlenden bzw. eingeschränkten Polizeipflicht von Hoheitsträgern (zur Polizeipflichtigkeit öffentlicher Stellen vgl. *Britz*, DÖV 2002, 891). Die „störende“ Behörde muss und kann selbst entscheiden, wie sie dem Datenschutz im Rahmen ihrer Aufgabenerfüllung und diesbezüglicher Rechtspflichten genügt. Anders als die Aufsichtsbehörde bei Maßnahmen gegenüber privaten Störern kann sie allerdings kein Auswahlermessen gegenüber sich selbst ausüben und die Beseitigung der eigenen Störung von der vorrangigen (erfolglosen) Inanspruchnahme Facebooks abhängig machen. Denn zum einen ist die störende öffentliche Stelle selbst nicht zu Aufsichtsmaßnahmen gegenüber Facebook befugt und zum anderen gilt ihre Gesetzesbindung unabhängig von Rechtsverletzungen Dritter bzw. deren effektiverer Möglichkeit zur Störungsbeseitigung. Darüber hinaus kann sie haftungsrechtlichen Ersatzansprüchen der Nutzer ausgesetzt sein (vgl. insbesondere § 7 S. 1 BDSG).
171 Ob das Vollzugsinstrumentarium des deutschen Datenschutzrechts als solches stark genug ist, um es mit den wirtschaftlichen Triebkräften aufzunehmen, welche die Datenschutzschwäche von Facebook & Co. bedingen, muss sich allerdings noch beweisen. Zweifel hieran schürt insbesondere die gegenwärtige Bußgeldbemessungsgrenze des § 43 III 1 Hs. 1 BDSG. Sie beträgt 50.000 Euro. Verglichen mit Facebooks Quartalsgewinnen (im Quartal 1/2015 weltweit 512 Mio. US-Dollar) handelt es sich hierbei um einen Handkassenbetrag, der keine substanzielle Sanktionswirkung auslöst. Von der Möglichkeit, ausnahmsweise ein Bußgeld oberhalb von 50.000 Euro festzusetzen (§ 43 III 3 BDSG), haben die Aufsichtsbehörden bislang keinen Gebrauch gemacht. Solange aber aus einem niedrigen Datenschutzniveau keine wirtschaftlichen Nachteile, sondern stattdessen ökonomische Vorteile erwachsen, bleibt die Vollzugsschwäche deutschen Datenschutzrechts bestehen. Zur deshalb geforderten Stärkung des Datenschutzrechts durch einen geeigneten Geldausgleich für immaterielle Schäden in Folge von Datenschutzverstößen vgl. *Härting*, BB 2010, 839 (842). Zur Durchsetzbarkeit des Datenschutzrechts im Internetzeitalter auch *Klar*, DÖV 2013, 103 (108); *Kühling/Sivridis/Schwuchow/Burghardt*, DuD 2009, 335; *Lepperhoff/Petersdorf/Thursch*, DuD 2012, 195.

Zwar ist das ULD für ein Vorgehen gegenüber Facebook nicht örtlich zuständig. Das legitimiert die Aufsichtsbehörde aber nicht, die dem eigenen Zuständigkeitsbereich unterworfenen Fanpage-Betreiber hoheitlich in die Pflicht zu nehmen. Das gilt jedenfalls so lange, wie der (stattdessen als Aufsichtsbehörde für die Facebook Germany GmbH örtlich zuständige) HmbBfDI, die Facebook als unmittelbaren Handlungsstörer herantritt.[172] Erst wenn er sich dauerhaft verschließt, ist der Weg frei für ein Vorgehen gegenüber Fanpage-Betreibern.

III. Zusammenfassung und rechtspolitische Desiderate

Die Rechtsordnung tut sich schwer damit, die Vielschichtigkeit der Mitwirkungsbeiträge an kooperativ generierten Angeboten im Internet abzubilden und steuerbar zu machen. Das arbeitsteilige Zusammenwirken eines sozialen Netzwerks und seiner Inhalteanbieter ermöglicht ihnen eine symbiotische Datenernte: Facebook stellt mit seiner Infrastruktur Land und Saatgut zur Verfügung, der Fanpage-Betreiber gießt es mit seinem Datenkännchen, im Anschluss veredelt und verarbeitet Facebook die Früchte zu einem süßen Saft und lässt den Fanpage-Betreiber unentgeltlich davon kosten. Beide agieren als Teil einer Win-Win-Gemeinschaft – auf Kosten gesetzlicher Schutzbestimmungen.

Auf dieses kooperative Spiel mit verteilten Rollen ist das Drehbuch des nationalen Datenschutzrechts nicht gut vorbereitet. Seine normativen Regieanweisungen sind primär auf lineare Verarbeitungsvorgänge ausgerichtet. Die Möglichkeit einer Aufgabenverlagerung auf soziale Netzwerke jenseits einer Auftragsdatenverarbeitung oder Datenübermittlung war vom analogen Regelungshorizont des historischen nationalen und europäischen Gesetzgebers aus noch nicht zu erkennen.

Arbeitsteilige Aktionseinheiten inszenieren nun ein Regie-Theater unter Leitung von Internetgiganten, die dem europäischen Datenschutzmodell die Rolle des sterbenden Schwans zuweisen möchten. Die konfuzianische Regel „Wenn Du ein fremdes Land betrittst, frage, was dort verboten ist." lässt sie unbeeindruckt. Sie orientieren sich vielmehr an dem arabischen Sprichwort: „Wenn Du jedes Mal stehen bleibst, wenn ein Apfel vom Baum fällt, wirst Du Deine Reise nie beenden."

Dass § 3 VII BDSG de lege lata bislang allein Facebook als primären Diensteanbieter erfasst, nicht aber Fanpage-Betreiber, heißt allerdings nicht, dass sie datenschutzrechtlicher Pflichten gänzlich enthoben sind. Zwar lässt sich die Verantwortlichkeitslücke aus rechtssystematischen Gründen weder durch einen Rückgriff auf die Figur des Zweckveranlassers noch durch Verweis auf die zivilrechtliche Störerhaftung oder die §§ 7 ff. TMG schließen. Allerdings ist dem Regelungskonzept des BDSG im Wege eines Erst-recht-Schlusses eine Auswahlverantwortlichkeit zu entnehmen: Wer als Diensteanbieter seine Inhalte in eine fremde digitale Kommunikationsinfrastruktur integriert und sich deren Datenschutzbedingungen unterwirft, darf keinen Kooperationspartner auswählen, der offensichtlich deutsches Datenschutzrecht verletzt. § 11 II 1, 4 BDSG begründet a maiore ad minus eine ordnungsrechtliche, auf der Grundlage des § 38 V BDSG durchsetzbare Verhaltenspflicht. Vorrangig ist aber Facebook als unmittelbar datenschutzrechtlich verantwortlicher Störer heranzuziehen.

Die in der Entstehung begriffene Datenschutz-Grundverordnung (DSGVO-E) wird für kooperativ generierte Internetangebote keine innovativen, passgenauen Regelungen zum Schutz europäischer Privatheitsvorstellungen treffen. Vielmehr verharrt sie insoweit weitgehend auf dem Stand der Datenschutzrichtlinie. Sie definiert den „für die Verarbeitung Verantwortlichen"[173] als auch den „Auftragsverarbeiter"[174] in gleicher Weise wie das bisherige Unionsrecht. Auch in Bezug auf den Adressatenkreis aufsichtsbehördlicher Maßnahmen bleiben Neuerungen weitgehend aus.[175] Im Falle mehrerer Verantwortlicher mit unklarer Verantwortungsaufteilung weist die DSGVO-E ihnen zwar eine gesamtschuldnerische Verantwortlichkeit zu.[176] Das setzt aber die grundsätzliche normative Zuweisung einer Verantwortung als verantwortliche Stelle notwendig voraus. Daran fehlt es allerdings nach dem aktuellen Verordnungsentwurf für den Fanpage-Betreiber weiterhin.

Faktische Auftragsverhältnisse ohne Auftrag, welche die Ernte vom Baum der Erkenntnis ohne eigenes Risiko ermöglichen wollen, sollte das Datenschutzrecht ausdrücklich in die Mitverantwortung einbeziehen – jedenfalls in Gestalt einer abgestuften Pflicht. Verantwortlich sollte daher in Zukunft nicht nur sein, wer allein oder gemeinsam mit anderen über die Verarbeitung mitentscheidet, sondern (subsidiär) auch derjenige, der sich offensichtlich rechtswidrig verarbeitete Daten nutzbar macht. Die bloße Verortung der Datenverarbeitung in einer fremden Infrastruktur entbindet nicht von Verantwortung. Denn Verantwortung und Freiheit gehören zusammen. Auch insoweit sollte der römisch-rechtliche Grundsatz: „Qui habet commoda, ferre debet onera"[177] Gültigkeit behalten: Wer die Vorteile genießt, muss auch die Lasten tragen. ■

172 Die Frage, ob Aufsichtsmaßnahmen wegen der Verletzung deutschen Datenschutzrechts gegen die deutsche Facebook-Niederlassung zu richten sind oder ob stattdessen die irische Facebook-Niederlassung oder gar der US-amerikanische Mutterkonzern Facebook Inc. Aufsichtsadressat sind (und ob auch in diesem Fall die Zuständigkeit einer deutschen Datenschutzbehörde gegeben ist), ist bislang nicht geklärt. Vgl. dazu aus zivilrechtlicher Perspektive *LG Berlin*, ZD 2015, 235. Zu dem möglichen Auseinanderfallen des anwendbaren Rechts und der Kontrollzuständigkeit sowie den damit zusammenhängenden kollisionsrechtlichen Fragen hat sich jüngst der *EuGH*, ECLI:EU:C:2015:639 = BeckRS 2015, 81213, geäußert – wenngleich in der umgekehrten Konstellation einer fehlenden Niederlassung des Mutterkonzerns und entsprechender Unanwendbarkeit des nationalen Rechts.

173 Vgl. Art. 4 V DSGVO-E und Art. 2 Buchst. d EG-Datenschutz-RL.

174 Vgl. Art. 4 VI DSGVO-E und Art. 2 Buchst. e EG-Datenschutz-RL.

175 Während Art. 53 DSGVO-E für einige Befugnisse der Aufsichtsbehörde ausdrücklich auf „den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter" rekurriert, nennt Art. 53 Buchst. f DSGVO-E den Adressaten einer Anordnung zur Berichtigung, Löschung oder Vernichtung von Daten nicht explizit. Dies entspricht im Wesentlichen der Gestaltung des Art. 28 III EG-Datenschutz-RL (s. dazu oben II. 2. b) ee), Seite 28).

176 Art. 24 S. 3 DSGVO-E idF des EU-Parlaments bzw. Art. 24 II idF des Rates.

177 *Paulus*, Dig. 50, 17, 10. Vgl. auch *Ulpian*, Dig. 17, 2, 55: „Cuius participavit lucrum, participet et damnum."