Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook

Metadaten:

Version:	1.0
Ausgabedatum:	19. August 2011
Status:	☐ in Bearbeitung ☐ in Abstimmung ☑ Freigegeben
Ansprechpartner juristisch:	Moritz Karg 0431/988-1651 ULD41@datenschutzzentrum.de
Ansprechpartner technisch:	Sven Thomsen 0431/988-1211 ULD3@datenschutzzentrum.de

1 Einleitung

Gegenstand dieses Arbeitspapiers ist die Prüfung der Übereinstimmung des Dienstes Facebook (http://www.facebook.de/) und den durch dieses Unternehmen durchgeführten Formen der Nutzungsanalyse mit den datenschutzrechtlichen Vorgaben des deutschen und teilweise des europäischen Rechts. Außerdem wird untersucht, ob die Nutzung des Dienstes Facebook durch öffentliche und nicht-öffentliche Stellen im Land Schleswig-Holstein datenschutzrechtlich zulässig ist. Grundlage der rechtlichen Bewertung sind die allgemein zugänglichen Informationen und Nutzungsbedingungen des Dienstes sowie eine durch das ULD erstellte technische Analyse.

Laut Social Media Schweiz haben von den insgesamt 689,3 Millionen registrierten Facebook-Nutzerinnen und -Nutzern sich 18,6 Millionen aus Deutschland angemeldet.[1] Facebook ist das derzeit größte Soziale Netzwerk in Deutschland. Die Datenerhebung und -verarbeitung durch das Unternehmen Facebook betrifft somit fast 36 % der 51,7 Millionen deutschen Internetznutzerinnen und -nutzer.[2]

Soziale Netzwerke werden als Kommunikationsplattformen im Online-Bereich definiert. Sie geben dem Einzelnen die Möglichkeit, mit Gleichgesinnten und Interessierten zu kommunizieren oder neue Kommunikationsnetze zu schaffen.[3]

Nach der Definition der Artikel-29-Datenschutzgruppe zeichnen sich Soziale Netzwerke durch mittels detaillierter persönlicher Daten erstellte Profile der Nutzer, durch nutzergenerierte Inhalte (Texte, Links, Bilder, Videos und sonstige virtuelle Aktionen) und Schaffung von Netzwerken aufgrund von Adressbüchern und Kontaktlisten aus.[4] In der Terminologie von Facebook werden nutzergenerierte Inhalte als „IP-Inhalte“[5] bezeichnet.

Facebook hat seinen Wirkungskreis über die eigene Internetpräsenz hinaus ausgedehnt. Die technische Plattform erlaubt es dem Unternehmen, Nutzerverhalten in Bereichen zu erfassen, die über das eigentliche Netzwerk hinaus gehen.

2 Übergreifende Darstellung der Kommunikation

Die Nutzung von Facebook über das Webinterface auf facebook.com oder über auf anderen Webseiten eingebundene sogenannte „Social-Plugins“ (wie z. B. die in deutschen Webseiten mittlerweile weit verbreiteten „Gefällt mir“- bzw. „Like“-Buttons[6]) folgt einem in seinen Grundzügen größtenteils gleichartigen Muster:

---

1 http://www.socialmediaschweiz.ch/Facebook_-_Die_Welt__Update_Mai_2011_.pdf

2 http://www.ard-zdf-onlinestudie.de/index.php?id=264.

3 Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, WP 163, S. 5, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf.

4 Ebda.

5 IP steht hier für „Intellectual Property“, also sind IP-Inhalte solche, die unter die Rechte an geistigem Eigentum fallen.

6 Andere Social-Plugins sind „Activity Feed“, „Comments“, „Facepile“, „Life Stream“, „Like Box“, „Login Button“, „Recommendations“, „Registration“ oder „Send Button“, siehe https://developers.facebook.com/docs/plugins/.

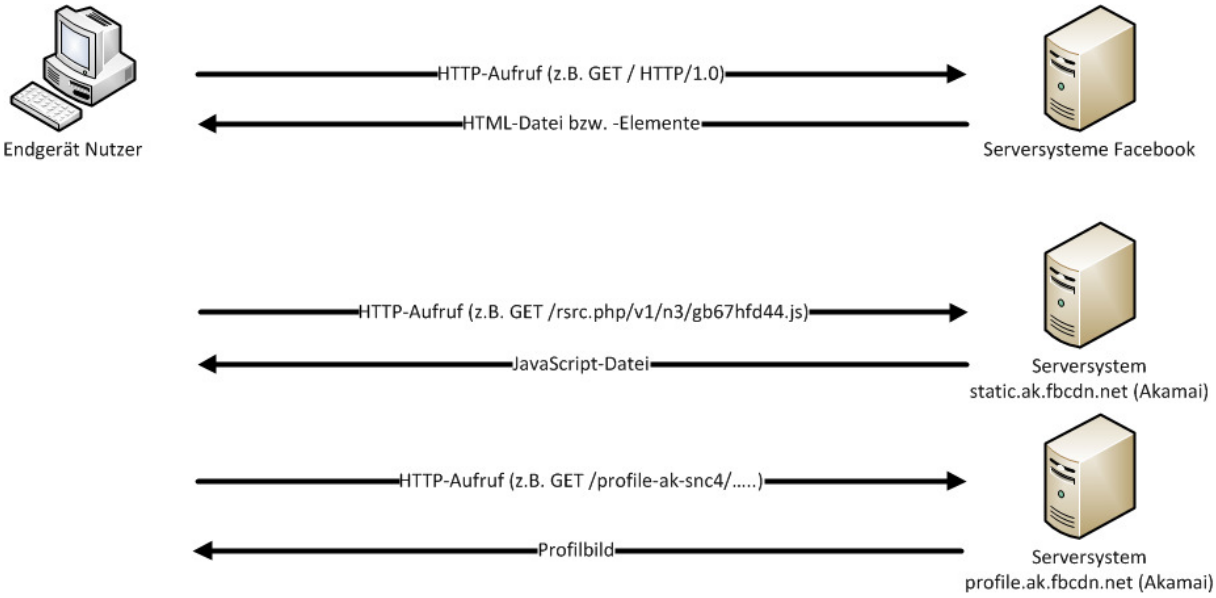

Abbildung 1: Aufteilung der Aufrufe: Facebook und Facebook Content Delivery Network

Der initiale Aufruf sowohl der Webschnittstelle facebook.com oder von Social-Plugins erfolgt stets direkt bei Servern von Facebook und nicht auf Systemen, die zum Facebook Content Delivery Network (FBCDN) gehören. Die Funktion des FBCDN wird im Folgenden genauer erläutert.

Als Antwort auf den initialen Aufruf sendet Facebook eine HTML-Seite oder einzelne HTML-Elemente zurück. In diesem HTML-Elementen finden sich dann zahlreiche Verweise auf nachzuladende Grafiken, Formatierungsangaben (Cascading Stylesheets, CSS) und Programmcode (JavaScript).

```
<script type="text/javascript">Bootloader.setResourceMap({"\/YvkZ":{"type":"css","permanent":1,"src":"https:\/\/s-
static.ak.facebook.com\/rsrc.php\/v1\/yT\/r\/5dEwtbarLZV.css"},"8UNn8":{"type":"css","permanent":1,"src":"https:\/\/s-
static.ak.facebook.com\/rsrc.php\/v1\/yJ\/r\/h7uqkYexAaR.css"},"BhxNZ":{"type":"css","permanent":1,"src":"https:\/\/s-
static.ak.facebook.com\/rsrc.php\/v1\/y9\/r\/oomdemhf9p3.css"},"P24C5":
{"type":"css","permanent":1,"nonblocking":1,"src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/y_\/r\/L2tlm-
5DPM_.css"},"\/YYg5":{"type":"css","permanent":1,"src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yu\/r\/HI-
PhS1TzB_.css"},"kkZVg":{"type":"css","permanent":1,"src":"https:\/\/s-
static.ak.facebook.com\/rsrc.php\/v1\/yf\/r\/M0ln9SVoI0F.css"}});Bootloader.setResourceMap({"SH1q\/":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yj\/r\/WRzyPEeP70R.js"},"LVwPS":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/y2\/r\/jQlKdxVr0EZ.js"},"x\/n2L":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yR\/r\/oLQht4FGzco.js"},"FfmQf":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yS\/r\/-MRj1y9SeIL.js"},"fZYUE":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/y4\/r\/eXHcpRoThZn.js"},"YxBS7":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yc\/r\/DzkM-7DYccQ.js"},"3cuzy":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yV\/r\/m1dWlBuLL4s.js"},"ZK+ek":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/y4\/r\/yGAzEWR0-5b.js"},"SOP8D":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/ym\/r\/J0NZQCRniUX.js"},"dJnMI":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yj\/r\/vBvk5ntdgBl.js"},"BaV9O":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yM\/r\/F4RSTon9cou.js"},"uKqhc":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yK\/r\/xrEeXUiCo9E.js"},"meUh+":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/y3\/r\/UPZW1aShxvn.js"},"ZQXFg":
{"type":"js","src":"https:\/\/s-static.ak.facebook.com\/rsrc.php\/v1\/yE\/r\/Or2nnTjvNOy.js"}});
Bootloader.enableBootload({"async":["fZYUE","SH1q\/","8UNn8"],"iframe-shim":
["fZYUE","SH1q\/","x\/n2L","YxBS7"],"dialog":["fZYUE","SH1q\/","8UNn8"],"dom-form":
["fZYUE","SH1q\/","8UNn8"],"PhotoTheater":["fZYUE","SH1q\/","3cuzy","8UNn8","x\/n2L"],"PhotoTagger":
["fZYUE","SH1q\/","8UNn8","ZK+ek","x\/n2L","3cuzy","SOP8D"],"TagToken":
["fZYUE","SH1q\/","dJnMI","BaV9O"],"TagTokenizer":
["fZYUE","SH1q\/","dJnMI","BaV9O","3cuzy","8UNn8","x\/n2L","ZK+ek","SOP8D"],"fb-photos-theater-css":
["\/YYg5"],"animation":["fZYUE","SH1q\/"],"uri":["fZYUE","SH1q\/"],"fb-photos-photo-css":["kkZVg"],"fb-photos-snowbox-
css":["kkZVg"],"PhotoSnowbox":["fZYUE","SH1q\/","8UNn8","ZK+ek","x\/n2L","3cuzy","SOP8D"],"Toggler":
["fZYUE","SH1q\/","8UNn8","x\/n2L"],"ajaxpipe":["fZYUE","SH1q\/","8UNn8","x\/n2L"],"dom-collect":
["x\/n2L","uKqhc"],"json":["x\/n2L"],"string-extensions":["SH1q\/"],"async-signal":["SH1q\/"],"editor":
```

Abbildung 2: Code-Beispiel, Nachladen zahlreicher JavaScript-Dateien

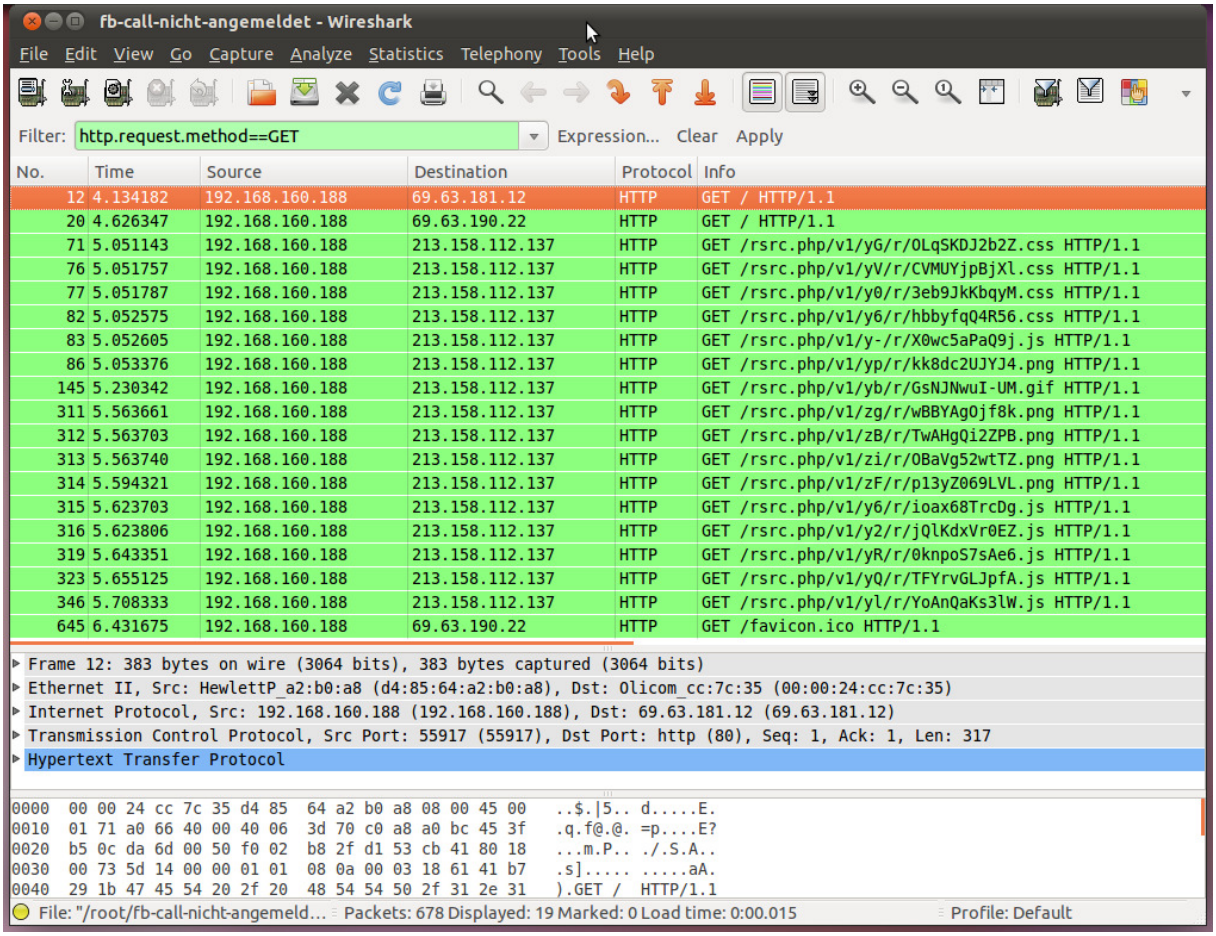

Abbildung 3: Wireshark, Darstellung der Anfragen zum Nachladen von JavaScript-Dateien

Diese Daten werden nach dem initialen Aufruf aus dem Facebook Content Delivery Network (FBCDN) geladen.

Hierbei werden unterschiedliche Systeme verwendet. Über die Systeme „static.ak.fbcdn.net“ werden wahrscheinlich vor allem nicht-personenbezogene Daten wie Grafiken und Icons, Zusammenstellungen von HTML-Elementen und die JavaScript-Bibliotheken ausgeliefert.

Die Systeme „profile.ak.fbcdn.net“ liefern großvolumige Daten aus den Profilen der Facebook-Nutzerinnen und -Nutzer, wie die Profilbilder, Videos, Fotoalben etc.

3 Technische Beschreibung der verschiedenen Tracking-Optionen durch Facebook

Facebook stellt eine Plattform zur Verfügung, auf der die Analyse des Nutzungsverhaltens angemeldeter und nicht-angemeldeter Nutzerinnen und Nutzer ermöglicht wird. Insoweit muss Facebook neben den Elementen des Sozialen Netzwerks auch als eine technische Infrastruktur zur Messung des Gebrauchs von Angeboten im Internet verstanden werden. Dabei sind drei Bereiche zu trennen, für die jeweils unterschiedliche technische Verfahren zum Einsatz kommen:

1. Der erste Bereich dient der Analyse des Verhaltens angemeldeter Nutzerinnen und Nutzer auf der Internetpräsenz des Unternehmens, d. h. derjenigen Nutzerinnen und Nutzern, die sich bei Facebook registriert und ein Nutzerkonto erhalten haben. Gemäß der unternehmensseitig veröffentlichten Privacy Policy – genannt „Facebook-Datenschutzrichtlinien“ – protokolliert Facebook das Verhalten seiner Nutzerinnen und

Nutzer auf der Webseite.[7] Welchen konkreten Umfang diese Protokollierung erreicht, erläutern die Facebook-Datenschutzrichtlinien nicht.

2. Protokolliert wird auch die Interaktion nicht-angemeldeter Internet-Nutzerinnen und -Nutzer (in Bezug auf Facebook: „Nichtnutzer"). Dies geschieht zum einen dann, wenn nicht-angemeldete Nutzerinnen oder Nutzer die Webseite von Facebook aufrufen. Eine Erhebung von Nutzungsinformationen erfolgt zum anderen durch die Social-Plugins. Die Nutzung von Internetdiensten, die Social-Plugins von Facebook in ihr Angebot eingebunden haben, wird durch das Unternehmen registriert und ausgewertet.
3. Eine Analyse des Nutzungsverhaltens authentifizierter (aktiv angemeldeter) Nutzerinnen und Nutzer über die Social-Plugins ist über die bereits im ersten Bereich erwähnte Nutzungsanalyse ebenfalls möglich.

Unklar bleibt, welche konkreten Zwecke Facebook mit der Analyse des Nutzungsverhaltens vor allem bei nicht-authentifizierten Nutzerinnen und Nutzern verfolgt. Unter Ziffer 5 der Facebook-Datenschutzrichtlinien werden die Zwecke der Nutzung nur vage beschrieben. Neben der „Verwaltung des Dienstleistungsangebots", zu der die inhaltliche Kontrolle gezählt wird, „um potenziell rechtswidrige Handlungen zu unterbinden", wird auch die Nutzung zu Werbezwecken erwähnt. Hinsichtlich der Erfassung des Nutzungsverhaltens nicht-authentifizierter Nutzerinnen und Nutzer finden sich in der Datenschutzerklärung und in der sonstigen durch Facebook zur Verfügung gestellten Dokumentation zum aktuellen Zeitpunkt keine Hinweise.

3.1 Nutzungsanalyse auf der Webseite von Facebook

3.1.1 CavalryLogger

In nahezu jeder JavaScript-Datei, die beim Aufruf eines Social-Plugins oder der Webschnittstelle facebook.com übertragen wird, wird zu Beginn eine Protokollierung (Logging) durchgeführt. Die Protokollierung wird für jede JavaScript-Datei mit einer für die jeweilige JavaScript-Datei eindeutigen Identifikationszeichenkette (ID) durchgeführt.

```
if (window.CavalryLogger) {
    CavalryLogger.start_js([ "zDo3Y" ]);
}
```

Abbildung 4: Quellcode-Beispiel CavalryLogger

Facebook gibt über die Verwendung dieser Logdaten in der Datenschutzerklärung oder in anderen Nachweisen keine detaillierte Auskunft. Es kann vermutet werden, dass es sich hierbei um eine Protokollierung zur Performance-Analyse handelt. Beim Aufruf eines Social-Plugins oder der Webschnittstelle wird eine Vielzahl von JavaScript-Dateien nachgeladen (bei Aufruf der Webschnittstelle als authentifizierter Nutzer zum Beispiel 26 JavaScript-Dateien). Erst danach (d. h. wenn diese „Kavallerie" von Dateien „vor Ort" ist, vielleicht daher der Name „CavalryLogger") kann die Ausführung des Social-Plugins oder der Webschnittstelle starten.

3.1.2 EagleEye-Logging

Facebook führt außerdem für zahlreiche Nutzeraktionen eine Protokollierung durch. Diese Protokollierung wird an mehreren Stellen verwendet.

Die Verteilung der Logfunktionen folgt keinem erkennbaren Muster; nicht alle über die Webschnittstelle oder die Social-Plugins abrufbaren Aktionen in der Nutzeroberfläche sind mit Logfunktionen ausgestattet.

[7] „Informationen über Verhalten auf der Webseite", Ziffer 2, und „Zur Verwaltung des Dienstleistungsangebots", Ziffer 5, Facebook-Datenschutzrichtlinien vom 22.12.2010, https://www.facebook.com/policy.php.

```
if (window.EagleEye && d) {
    var h = {
        app: this._application_id,
        is_game: this._is_game,
        client_start_ts: +(new Date)
    };
    if (b) h.impression_id = b;
    this._timers.push(setInterval(function(j) {
        h.client_ts = +(new Date);
        EagleEye.log("canvas-heartbeat", h);
    }, d));
```

Abbildung 5: EagleEye-Logging canvas-heartbeat

```
window.EagleEye && EagleEye.log("chat-tab", {
    id: b
```

Abbildung 6: Logging im Bereich Chat, Beispiel 1

```
this._log = EagleEye.createLogger("chat-buddylist", .1);
```

Abbildung 7: Logging im Bereich Chat, Beispiel 2

3.1.3 Nectar-Logging

An verschiedenen Stellen wird eine Protokollierung ausgeführt, die nach aktuellem Kenntnisstand eher der Nutzungsanalyse als technischen Zwecken dient.

```
o.src = n + "/ajax/nectar.php?asyncSignal=" + (Math.floor(Math.random() * 1e4) + 1) + p + "&" + (!q ? "" : "s=") + +(new Date);
```

Abbildung 8: Nectar-Initialisierung

```
setNectarImpressionIdSafe: function() {
    if (this.setNectarImpressionId) this.setNectarImpressionId();
    return this;
},
```

Abbildung 9: Nectar-Impression-Handler

3.2 Nutzungsanalyse bei nicht-authentifizierten Nutzenden in der Webschnittstelle facebook.com

Auch bei nicht-angemeldeten und somit nicht-authentifizierten Nutzerinnen und Nutzern erfolgt eine Analyse der Nutzung von Internetdienstleistungen.

3.2.1 Webschnittstelle von facebook.com

Beim Aufruf der Webschnittstelle setzt Facebook mehrere Cookies:

- Cookie „datr“ mit zufälliger ID, Cookie ist 2 Jahre gültig;
- Cookie „lsd“ mit kurzer ID, Cookie ist nur für die Sitzung gültig;
- Cookie „reg_fb_gate“ mit Domain, Cookie ist nur für die Sitzung gültig;
- Cookie: „reg_fb_ref“ mit Domain und Referrer, Cookie ist nur für die Sitzung gültig.

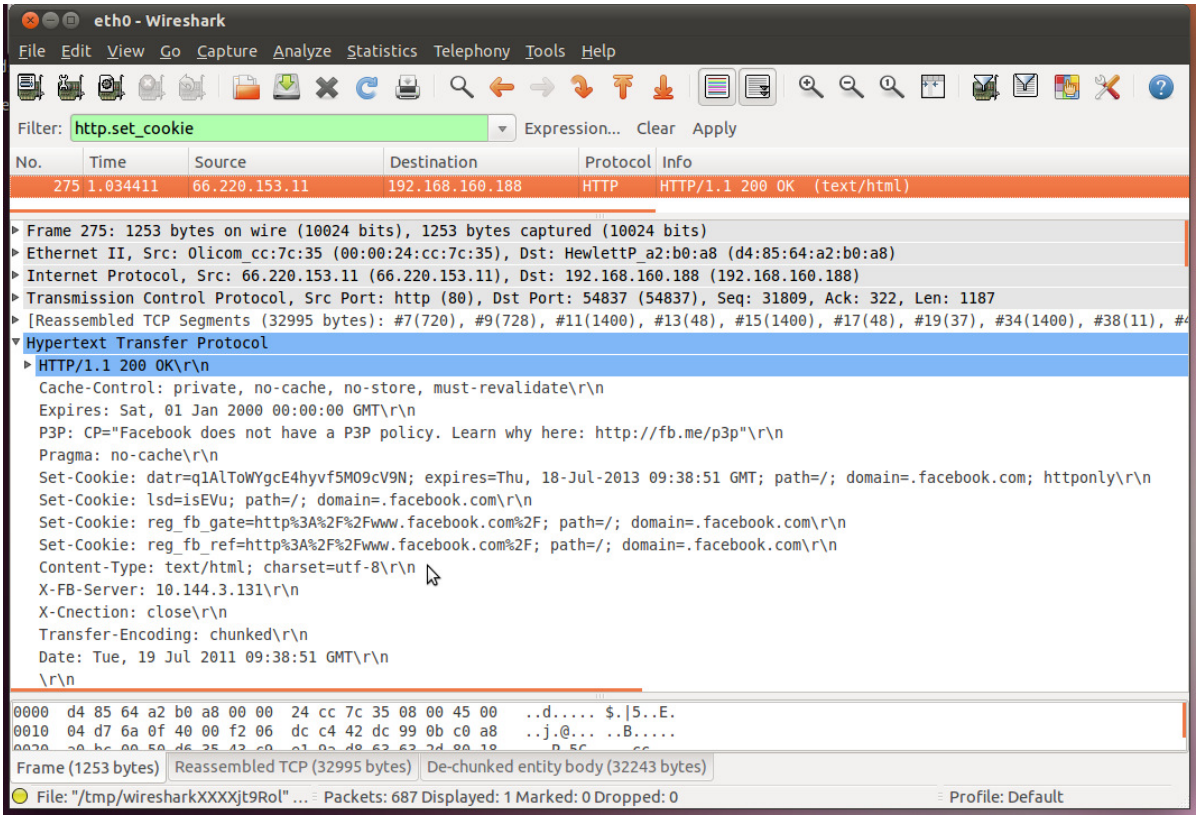

Abbildung 10: Wireshark-Darstellung von Facebook-Cookies

Der Cookie „datr“ enthält eine ID, die nachfolgend bei jeder Kommunikation mit Facebook, unabhängig davon, ob es sich um die Webschnittstelle oder ein Social-Plugin handelt, gesendet wird und zumindest 2 Jahre erhalten bleibt.

Der Cookie „lsd“ wird unter anderem zur Initialisierung der Protokollierungskomponenten genutzt und dient wahrscheinlich zur Session-Verwaltung.

Die Cookies „reg_fb_gate“ und „reg_fb_ref“ werden wahrscheinlich genutzt, um die Einstiegsseite und verweisende Seite für die Registrierung zu speichern. Der Verwendungszweck ist unklar. Denkbar ist, dass Facebook hierüber Kampagnen erkennt oder im Rahmen von Partnermodellen die über diese Partnerseiten durchgeführten Registrierungen unterscheidet.

3.2.2 Webseiten Dritter

Facebook bietet über Social-Plugins die Möglichkeit, einzelne Funktionen der Facebook-Plattform auf eigenen Webseiten einzusetzen.

Social-Plugins werden durch kurze Fragmente von HTML- oder JavaScript-Anweisungen in die Webseiten eingebunden.

Die Kommunikation verläuft hier ähnlich wie oben beschrieben: Einem Aufruf bei Facebook folgen zahlreiche Aufrufe bei dem FBCDN.

```
<meta property="fb:page_id" content="78766664651" />
<meta property="fb:app_id" content="163201030393605" />
```

Abbildung 11: Einbindung der Webseiten-ID

Bei der Nutzung der Social-Plugins wird stets die einbindende Webseite mit einer eindeutigen, von Facebook vergebenen ID und teilweise auch der URL angegeben. Diese Informationen werden an Facebook übertragen.

Werden diese Funktionen eingebunden, so wird ohne weitere Interaktion des Nutzers kein Cookie gesetzt. Erst wenn der Nutzer die eingebetteten Facebook-Funktionen aufruft, erfolgt das Setzen eines Cookies.

Facebook erhält generell bei jedem Aufruf eines in einer Webseite eingebundenen Social-Plugins:

- die „Grunddaten" eines Webseitenaufrufs:
  IP-Adresse, Browserstring
- erweiterte Daten aus dem Social-Plugin:
  Adresse der Webseite, eindeutige ID der Webseite
- aktiv abgefragt:
  Ablaufumgebung des Browsers, Bildschirmauflösung, installierte Browser-Plugins, Sprache
- nach einmaliger Interaktion mit Facebook:
  über „datr"-Cookie eine zwei Jahre gültige, eindeutige ID der Browserinstanz, im allgemeinen einer Nutzer-ID gleichzusetzen

3.3 Nutzungsanalyse bei authentifizierten Nutzenden

Bei authentifizierten Nutzerinnen und Nutzern werden mehr JavaScript-Funktionen ausgeführt sowie zusätzliche Cookies gesetzt.

Name	Value	Domain	Path	Expires	Size	HTTP	Secure
s	Aa6LF6-nUx5Lpsq7	.facebook.com	/	Sat, 20 Aug 2011 07:51:14 GMT	17	✓	✓
locale	de_DE	.facebook.com	/	Wed, 27 Jul 2011 11:26:05 GMT	11		
csm	1	.facebook.com	/	Sat, 20 Aug 2011 07:51:14 GMT	4	✓	
datr	4uouTTk_I2RLyU8N0UNyDKPX	.facebook.com	/	Sat, 20 Jul 2013 07:51:14 GMT	28	✓	
L	2	.facebook.com	/	Session	2	✓	
lu	ggTJAfdKcii-JU4vCvUOh_AA	.facebook.com	/	Sat, 20 Jul 2013 07:51:14 GMT	26	✓	
c_user	100000164615067	.facebook.com	/	Sat, 20 Aug 2011 07:51:14 GMT	21		✓
sct	1311234674	.facebook.com	/	Sat, 20 Aug 2011 07:51:14 GMT	13	✓	✓
xs	2%3Afb597d7622dfe6d6df59c3f2db62f4c8%3A1	.facebook.com	/	Sat, 20 Aug 2011 07:51:14 GMT	42	✓	✓
e	n	.facebook.com	/	Session	2	✓	
act	1311237090855%2F1	.facebook.com	/	Session	20		
presence	EM311237182L33REp_5f1B00164615067F7X311237006268Y0OQ0EsF0CEbIFDacF4G311237182PCC	.facebook.com	/	Session	88		

Abbildung 12: Facebook-Cookies

Neben den bereits bei nicht-authentifizierten Nutzerinnen und Nutzern verwendeten IDs wie z. B. „datr" kommen hier zusätzliche Cookies zum Einsatz. Die Cookies „s", „sct", „xs" und „c_user" dienen der Authentifizierung. Diese Cookies sind einen Monat lang gültig. Meldet sich die Nutzerin oder der Nutzer nicht aktiv ab, werden diese Cookies zumindest für einen Monat bei Aufruf der Webschnittstelle oder von Social-Plugins an Facebook übertragen.

Social-Plugins werden bei authentifizierten Nutzerinnen und Nutzern personalisiert. So werden beispielsweise die Profilbilder von Freunden bevorzugt eingeblendet.

4 Analyse aus Sicht von Webseitenbetreibern und Anwendungsentwicklern[8]

4.1 Graph-API

Neben dem Zugriff über die Webschnittstelle auf facebook.com bietet die Facebook-Plattform einen direkten Datenzugriff über eine Programmschnittstelle (Application Programming Interface, API) an. Die sogenannte „Graph-API"[9] ermöglicht es Webseitenbetreibern und Anwendungsentwicklern, Informationen über Facebook-Nutzer direkt abzufragen.

---

[8] *<<<Baustelle: Dieses Kapitel wird in einer der nächsten Versionen um eine Kurzdarstellung der Technik hinter den Social-Plugins ergänzt. Der datenschutzrechtliche Teil des Arbeitspapiers wird zudem um eine Analyse der Spezifika der jeweiligen Social-Plugins erweitert.>>>*

[9] https://developers.facebook.com/docs/reference/api/ (Zugriff teilweise nur nach Registrierung bei Facebook möglich, für einen Großteil der Informationen ist ein eigenes Konto bei Facebook erforderlich).

Der Zugriff ist hierbei nicht wahlfrei möglich, es gelten die vom Nutzer definierten oder initial von Facebook vergebenen Berechtigungen.

Abbildung 13: Empfohlene Berechtigungen

Die Nutzung der Graph-API kann direkt im Web-Browser nachvollzogen werden.

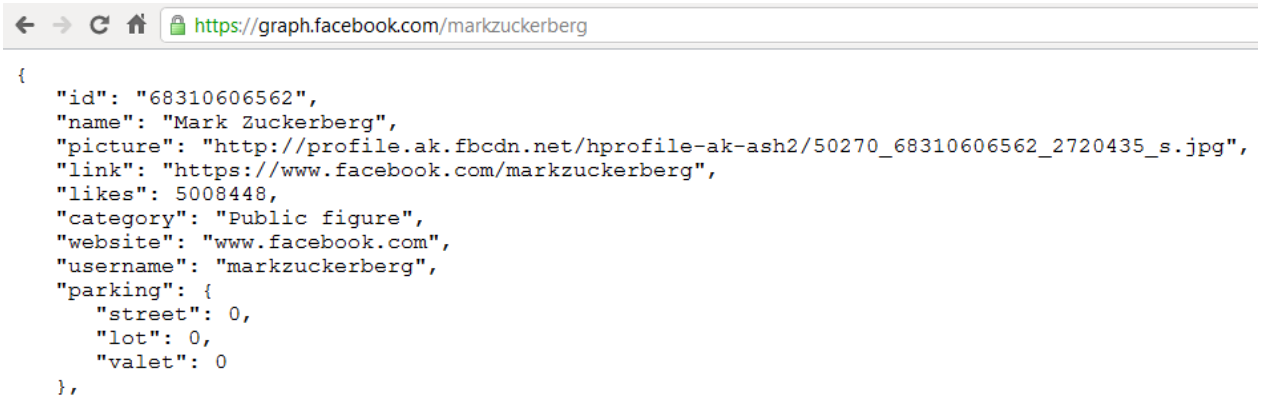

Abbildung 14: Zugriff auf die Graph-API über einen Web-Browser

Anwendungen können zusätzliche Rechte für den Zugriff anfordern.

Abbildung 15: Anforderungen erweiterter Rechte durch eine Test-Anwendung

Der Zugriff ist hierbei unabhängig davon möglich, ob die Nutzerin oder der Nutzer über die Webseite angemeldet ist. Solange die Anwendung eine gültige Zugriffskennung hat (sogenanntes „Access Token"), kann diese auf die personenbezogenen Daten der Nutzerin oder des Nutzers zugreifen.

Die Facebook-Plattform bietet darüber hinaus die Möglichkeit, Anwendungen aktiv zu benachrichtigen, wenn sich die mit der Nutzerin oder dem Nutzer verknüpften Daten ändern. Beispielsweise kann eine Anwendung automatisiert benachrichtigt werden, wenn ein Nutzer neue „Freunde" hinzufügt oder eine Nutzerin den „Gefällt mir"-Button auf einer Webseite geklickt hat. Zitat aus der Dokumentation der sogenannten Realtime-API[10]:

> *„Here are the list of user connections to which you can subscribe: feed, friends, activities, interests, music, books, movies, television, likes, checkins."*

Nutzerinnen und Nutzer haben die Möglichkeit, einzelne Zugriffe über die Graph-API zu kontrollieren und die Zugriffserlaubnis teilweise auf Anwendungsebene wieder entziehen.

[10] https://developers.facebook.com/docs/reference/api/realtime/ (Zugriff teilweise nur nach Registrierung bei Facebook möglich, für einen Großteil der Informationen ist ein eigenes Konto bei Facebook erforderlich).

Abbildung 16: Bearbeiten von genehmigten Anwendungen

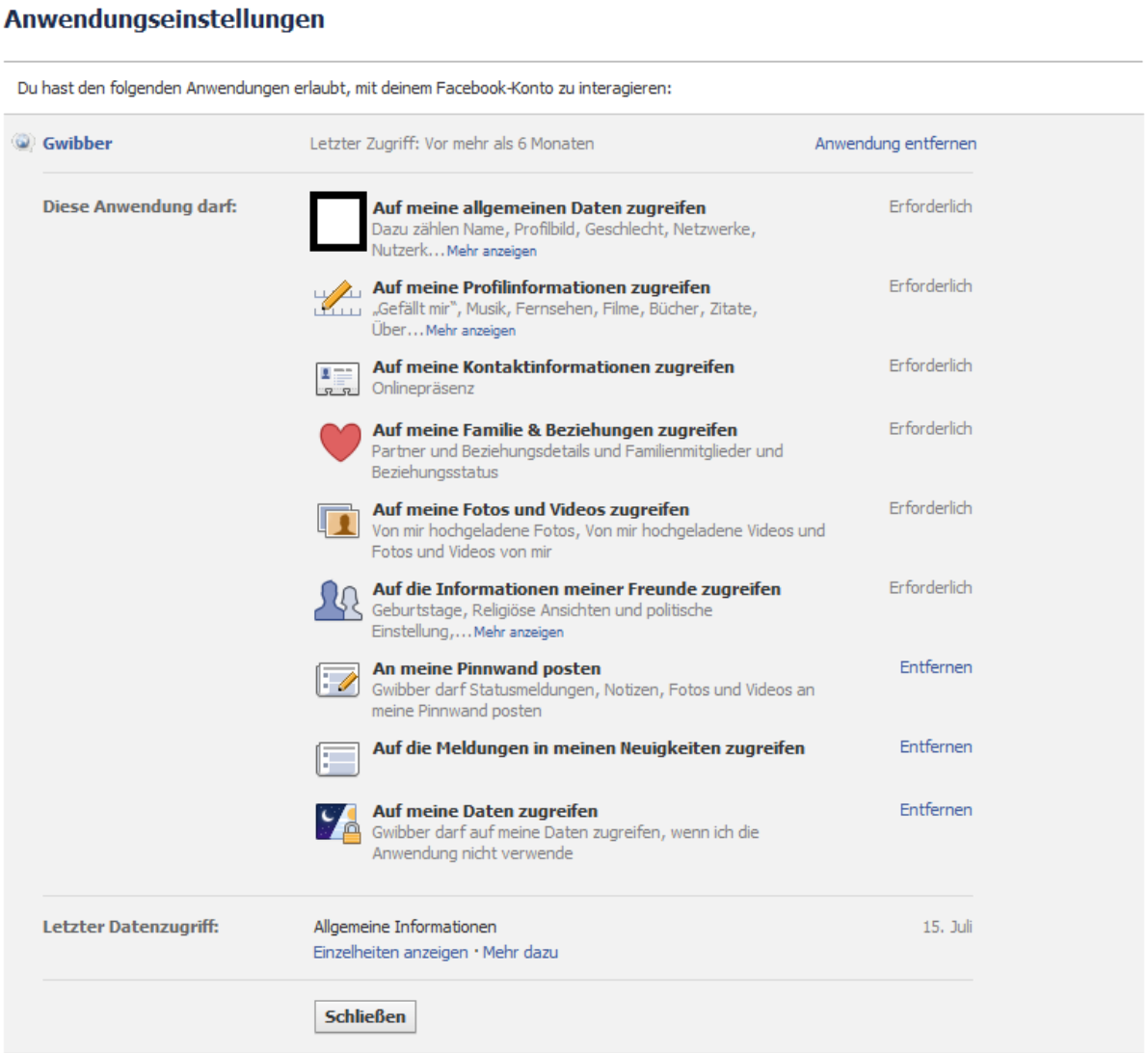

Abbildung 17: Bearbeiten von einzelnen Anwendungsberechtigungen

4.2 Facebook Insights

Facebook stellt mit Hilfe des Werkzeugs „Insights“ detaillierte Statistikinformationen über Nutzerinnen und Nutzer zur Verfügung, die von Betreibern von Facebook-Seiten (Administratoren von sog. Fanpages) und Facebook-Plattform-Anwendungsentwicklern sowie Webseitenbetreibern, die Funktionen der Facebook-Plattform in ihrer Webseite per Social-Plugin wie dem Like-Button integrieren, abrufbar sind. Diese Statistiken beziehen sich auf authentifizierte Nutzende und die ihnen zugeordneten Facebook-Seiten, -Anwendungen oder Webseiten. Sie sind von dafür eingetragenen Administratoren mit Facebook-Konto über https://facebook.com/insights/ abrufbar.[11]

Die durch Facebook erstellte Statistik erlaubt Rückschlüsse auf die Nutzung der Angebote. Zu diesen Bereichen gehören laut Facebook Angaben über den Nutzerzuwachs, Demographie, Nutzung und Erstellung von Inhalten.[12]

Die Statistik-Funktion wird durch Facebook kostenfrei auf sämtlichen Facebook-Seiten und Plattform-Anwendungen sowie Webseiten mit Open Graph-Protokoll durch das Unternehmen zur Verfügung gestellt. Der Zugang zu den statistischen Daten kann über verschiedene Wege erfolgen.[13]

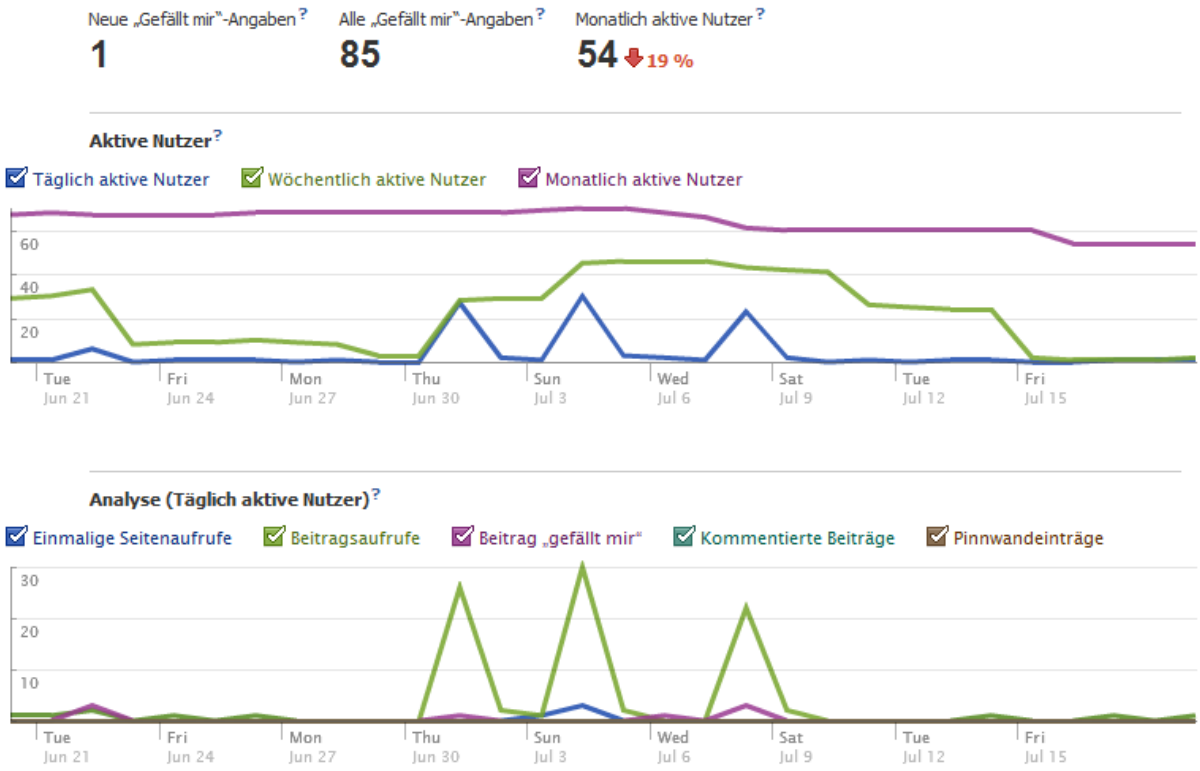

Abbildung 18: Facebook Insights: Nutzeraktivität

---

[11] Die Statistiken sind in einer Facebook-Fanpage vom jeweiligen Administrator auch über die Funktion „Statistiken anzeigen“ direkt aufrufbar.
Laut https://www.facebook.com/help/?faq=211934668839900 sind solche Statistiken „für Seiten verfügbar, die mindestens 30 Personen gefallen“.

[12] http://www.facebook.com/help/?faq=116512998432353.

[13] Ebda.: „Zusätzlich zur Statistikkonsole sind die Daten auch im Diagramm-API verfügbar.“

Abbildung 19: Facebook Insights: „Gefällt mir"-Quellen

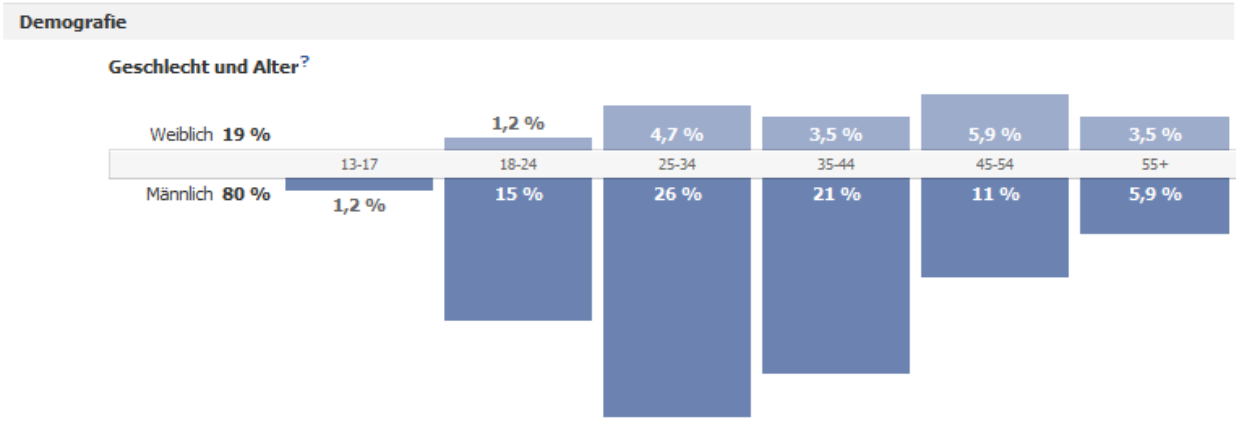

Abbildung 20: Facebook Insights: Demographische Daten

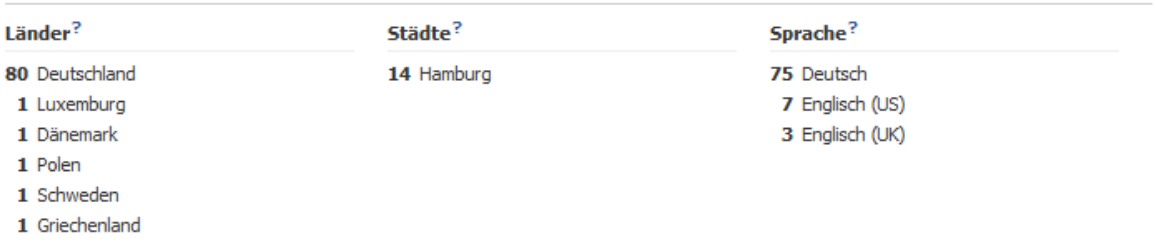

Abbildung 21: Facebook Insights: Geographische Daten

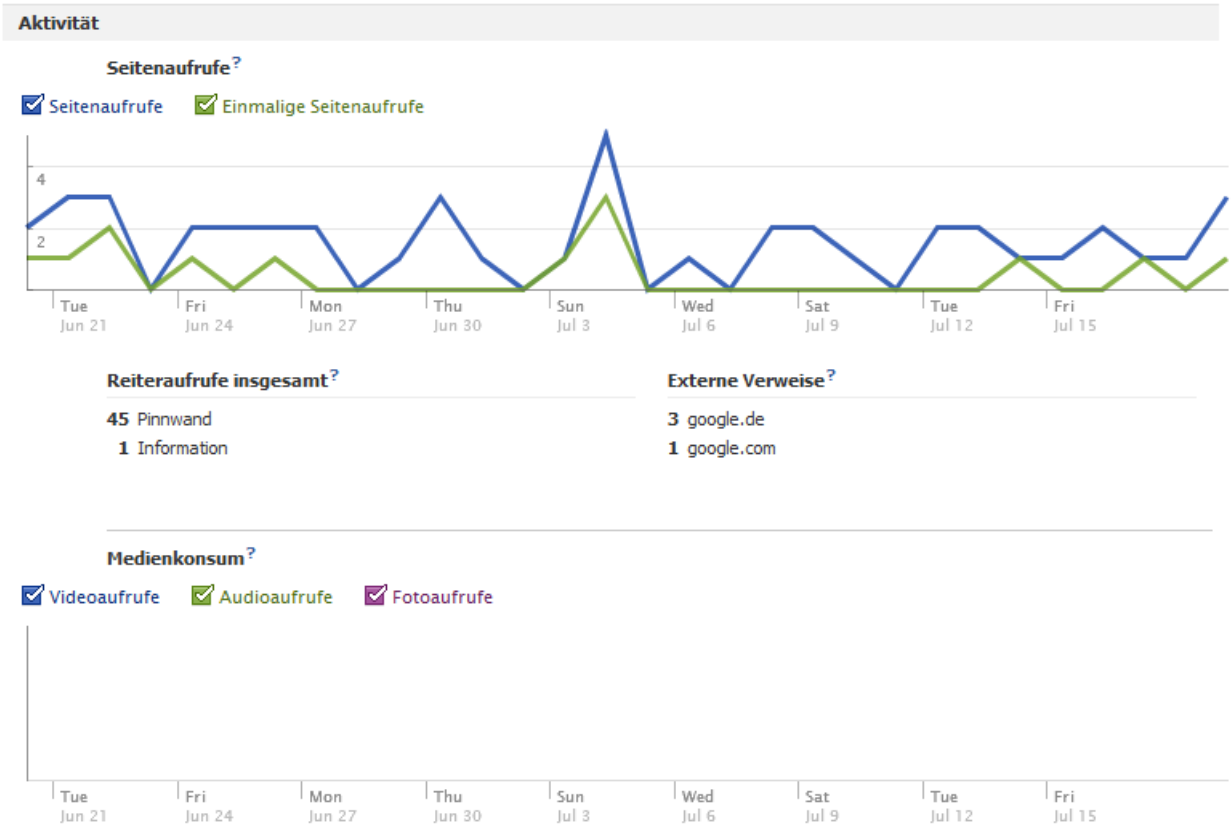

Abbildung 22: Facebook Insights: Aktivitäten wie Seitenaufrufe sowie Video-, Audio- und Fotoaufrufe

Abbildung 23: Facebook Insights: Aktivitäten wie „Gefällt mir", „Kommentare", „Abmeldungen"

Seitenbeiträge

Nachricht senden	Gepostet ▼	Impressionen	Feedback
[redacted]	08. Juli um 16:56	117	0,85 %
	08. Juli um 16:24	85	1,2 %
	04. Juli um 20:14	139	0 %
	01. Juli um 18:56	132	0 %

Abbildung 24: Facebook Insights: Seitenaufrufe detailliert, nachbearbeitet

5 Datenschutzrechtliche Bewertung

Die technisch beschriebenen Abläufe und Datenverarbeitungsprozesse sind als Webanalyse (Reichweitenanalyse) einzustufen. Webanalyse (auch Web Analytics, Web Controlling, Traffic-Analyse, Clickstream-Analyse oder Reichweitenanalyse) umfasst das Sammeln, Analysieren und Rapportieren der Nutzung einer oder mehrerer Websites und des Verhaltens ihrer Besucher.[14]

5.1 Personenbezug der erhobenen Daten

Durch den Dienst „Facebook Insight", der bei Fanpages und den Social-Plugins zum Einsatz kommt, werden personenbezogene Daten erhoben und verarbeitet. Personenbezogene Daten sind Angaben über die persönlichen und sachlichen Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 Bundesdatenschutzgesetz (BDSG)). Neben den bei der Anmeldung durch die Nutzerinnen und Nutzer im Netzwerk gespeicherten persönlichen Informationen werden auch bei der Nutzung von externen Diensten und den Fanpages Angaben mit Personenbezug erhoben und verarbeitet. Dazu gehört die IP-Adresse, die nach einhelliger Auffassung der europäischen und deutschen Aufsichtsbehörden Personenbezug besitzt. Außerdem nutzt Facebook Cookies, mit denen Nutzerinnen und Nutzer individualisiert werden können. Zusätzlich zu diesen Informationen erhebt und verarbeitet Facebook weitere Angaben, die zu einer umfassenden Profilierung der/des jeweiligen Nutzerin/Nutzers führen. Im Zusammenhang mit den durch die Nutzerinnen und Nutzer eingestellten Informationen ergeben sich somit Persönlichkeitsprofile, deren Detaillierungsgrad je nach Intensität der Nutzung von Facebook oder der Angebote, die Social-Plugins von Facebook einsetzen, variiert.

5.2 Verantwortlichkeit

An der Erhebung, Verarbeitung und Nutzung personenbezogener Daten innerhalb Sozialer Netzwerke allgemein und Facebook im Besonderen lassen sich u. a. vier Arten von Beteiligten beschreiben, denen unterschiedliche technische und datenschutzrechtliche Verantwortlichkeiten zukommen:

1. Facebook;
2. Content Delivery Networks (CDNs);
3. Webseitenbetreiber mit einem Facebook-Konto, die Social-Plugins einbinden oder darüber hinausgehende Facebook-Funktionalität nutzen, z. B. eine Fanpage bei Facebook betreiben.
4. Nutzerinnen und Nutzer.

Zusätzlich sind Anbieter von Drittprogrammen (Apps) in die Verarbeitung personenbezogener Daten involviert. Deren Rolle wird im Rahmen dieser Analyse noch nicht untersucht.

Eine weitere noch nicht bearbeitete Kategorie sind Unternehmen, die weitergehende Kooperationen mit Facebook eingegangen sind und hierzu personenbezogene Daten austauschen, so wie dies z. B. bei den E-Mail-Anbietern web.de oder GMX der Fall ist, die Zugriffe von Facebook auf Daten der Nutzerinnen und Nutzern dieser E-Mail-Dienste erlauben, etwa auf deren Adressbuch.[15]

Verantwortliche Stelle ist gemäß § 3 Abs. 7 BDSG die Stelle, die „personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt", bzw. nach Art. 2 Buchst. d) S. 1 EU-DSRL die Stelle, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Für Diensteanbieter von Telemedien gelten die §§ 2 S. 1 Nr. 1, 3 Abs. 1 Telemediengesetz (TMG).

---

[14] Hassler/Oostlander, Web Analytics – Zielorientierte Nutzung zur Erfolgssteigerung, März 2007, S. 7, http://blog.namics.com/2007/namics_Whitepaper_WebAnalytics_v1-0.pdf.

[15] http://www.gmx.net/presse/zusammenarbeit-facebook.html.

Bei der Bestimmung der Verantwortlichkeit sind nicht allein die rechtlichen, sondern auch die tatsächlichen Umstände entscheidend. Verantwortlich ist danach, wer maßgeblich die inhaltlichen Entscheidungen über die Art, den Umfang und vor allem Zweck der Datenverarbeitung trifft. Diese Interpretation entspricht dem Verständnis der Artikel-29-Datenschutzgruppe zur Auslegung des Begriffes „Verantwortliche Stelle" gemäß Art. 2 Buchst. d) der europäischen Datenschutzrichtlinie 95/46/EG (EU-DSRL).[16]

Das deutsche TMG, das vor dem BDSG auf Telemediendienste anzuwenden ist, § 12 Abs. 1 TMG, weist die Zuständigkeit für die Einhaltung datenschutzrechtlicher Bestimmungen dem Diensteanbieter zu. Dieser ist jede natürlich oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt, § 2 S. 1 Nr. 1 TMG. Die datenschutzrechtlichen Vorgaben des TMG erfassen nicht nur juristische Personen des Privatrechts, sondern auch Behörden und öffentlich-rechtlich organisierte Körperschaften.

Die Zuweisung datenschutzrechtlicher Verantwortlichkeit im Zusammenhang Sozialer Netzwerke erstreckt sich nicht nur auf den Diensteanbieter. Bereits in der durch die Artikel-29-Datenschutzgruppe erlassenen Stellungnahme 05/2009 zur Nutzung Sozialer Netzwerke stellte diese fest, dass je nach inhaltlicher Beteiligung mehrere Personen eine datenschutzrechtliche Verantwortlichkeit bei der Nutzung derartiger Dienste übernehmen. Entsprechend dem jeweiligen inhaltlichen Beitrag zur Nutzung und dem Einsatz eines derartigen Dienstes müssen die Rollen jeweils individuell bestimmt werden.

5.2.1 Dienstbetreiber – Facebook

Das Unternehmen Facebook hat seinen Stammsitz in den USA (Facebook, 1601 S. California Avenue, Palo Alto, CA 94304, USA). Seine Niederlassung in der Europäischen Union ist Facebook Ireland Limited, Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland (http://www.facebook.com/help/contact.php?show_form=impressum_contact oder impressum-support@support.facebook.com).[17] Zwar hat Facebook auch Mitarbeiter in Deutschland, insbesondere in Hamburg. Diese Personen oder Stellen sind aber nicht für die Datenverarbeitung verantwortlich und werden folgerichtig auch nicht im Impressum nach §§ 5, 6 TMG genannt. Ihnen kommen anscheinend lediglich Aufgaben im Bereich des Vertriebs bzw. der Öffentlichkeitsarbeit zu.

Facebook ist im telemedienrechtlichen Sinn zugleich Diensteanbieter für kommerzielle Kommunikation (§ 2 S. 1 Nrn. 1, 5 TMG), für den Bereich der Telekommunikation Anbieter von Telekommunikationsdiensten (§ 3 Nrn. 6, 24 Telekommunikationsgesetz (TKG)) und somit datenverarbeitende Stelle i. S. d. BDSG und der EU-DSRL.

5.2.2 Content Delivery Network – Akamai[18]

Facebook nutzt für die Diensteerbringung sog. „Content Delivery Networks" (CDN)[19] und nimmt hierfür die Dienste der Firma Akamai in Anspruch. Weitere CDNs konnten bei einer technischen Analyse nicht festgestellt werden. Sitz der Unternehmenszentrale von Akamai ist die USA: Akamai Corporate Headquarters, 8 Cambridge Center, Cambridge, MA 02142. Akamai bietet ein globales Netzwerk, das eine Verteilung von Inhalten in möglichst hoher netztopologischer Nähe zum Nutzer ermöglicht. Ziel des Einsatzes ist es, die Ladezeiten von Internet-Inhalten zu verringern. Für Deutschland verantwortliches Tochterunternehmen ist Akamai Technologies GmbH, Betastraße 10B, 85774 Unterföhring. Akamai betreibt eigene Data-Center, hat aber auch in verschiedenen

---

16 Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter, 16.02.2010, WP 169, S. 8, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf.

17 http://www.facebook.com/terms.php?ref=pf.

18 http://de.wikipedia.org/wiki/Content_Distribution_Network.

19 Auch „Content Distribution Network" genannt.

Rechenzentren anderer Anbieter Systeme zur Inhaltsverteilung untergebracht. So bedient sich Akamai u. a. des Kieler Internetproviders TNG.

Akamai nimmt funktional die Aufgaben eines Auftragsdatenverarbeiters für Facebook, das im tatsächlichen Sinn verantwortliche Stelle ist, wahr. Eine solche Auftragsdatenverarbeitung für Facebook/Irland ist datenschutzrechtlich als Auftragsdatenverarbeitung nach Art. 17 Abs. 3 EU-DSRL zu bewerten, wobei die Akamai Technologies GmbH in Erfüllung der vertraglichen Verpflichtungen für Facebook/Irland bezüglich der technisch-organisatorischen Maßnahmen zur Datensicherheit die Anforderungen nach § 9 BDSG i. V. m. der Anlage zum BDSG einhalten muss. Anders liegt der Fall, wenn die Daten nicht in Europa, d. h. im Raum der EU bzw. des Europäischen Wirtschaftsraumes (EWR), verarbeitet werden, sondern in den USA. In den Facebook-Datenschutzrichtlinien Ziffer 9 lässt sich Facebook ausdrücklich die Erlaubnis zur „Übertragung und Verarbeitung deiner persönlichen Daten in den USA" einräumen. In diesem Fall muss von einer Datenübermittlung in die USA ausgegangen werden sowie von einer Rückübermittlung an den Dienstleister Akamai. In diesem Fall wäre Akamai verantwortliche Stelle i. S. d. deutschen bzw. europäischen Datenschutzrechts. Ob dies der Fall ist bzw. inwieweit die Voraussetzungen für eine Auftragsdatenverarbeitung innerhalb von EU/EWR gegeben ist, bedarf der weiteren Klärung.

5.2.3 Webseitenbetreiber

Bei Facebook-Fanpagebetreibern und Webseitenbetreibern mit Sitz in Deutschland handelt es sich durchgängig um Diensteanbieter von Telemedien, auf die das TMG anwendbar ist. Sie sind datenschutzrechtlich verantwortlich für die über ihre Webseite vorgenommene Verarbeitung personenbezogener Daten. Auch soweit ein Webseitenbetreiber externe Dienstleister in Anspruch nimmt, kann er sich der datenschutzrechtlichen Verantwortung für die durch und über das Angebot vorgenommene Verarbeitungen und angestoßenen Prozesse nicht entziehen.

Diensteanbieter begründen eine eigene Verantwortlichkeit, soweit und solange sie nach Würdigung aller Gesamtumstände aufgrund des tatsächlichen Einflusses den Prozess der Datenverarbeitung steuern.[20] Diese Verantwortung begründet sich auch bei der Einbindung „fremder" Verarbeitungsprozesse in das eigene Angebot des Diensteanbieters. Wird durch die Konfiguration z. B. einer Webseite ein Verarbeitungsprozess bei einem weiteren Dienstleister ausgelöst, trägt der Diensteanbieter die datenschutzrechtliche Verantwortung für die dadurch ausgelöste Verarbeitung. Dies gilt umso mehr, wenn der Diensteanbieter mit seinem Angebot Dienste Dritter zu eigenen Zwecken nutzt. Dazu gehören insbesondere Dienste der Reichweitenanalyse oder der verhaltensbasierten Online-Werbung.[21]

Social-Plugins von Facebook auf der Webseite eines Drittanbieters haben zur Folge, dass bei deren Verwendung eine direkte Kommunikation zwischen dem Rechner des Nutzenden und Facebook aufgebaut wird. Eine direkte Datenerhebung und -speicherung durch den Webseitenbetreiber erfolgt nicht. Dies ändert jedoch nichts an der Verantwortlichkeit des Webseitenbetreibers, der durch die Gestaltung seiner Webseite die Datenweitergabe an Facebook initiiert und in der Hand hat. Facebook liefert mit seinem Software-Angebot eine Voraussetzung für die Datenübermittlung, trägt aber nicht die Alleinverantwortung für die konkreten Weitergaben.

Untrennbar mit dem Einsatz von Social-Plugins ist die Erstellung einer Reichweitenanalyse zugunsten des Diensteanbieters verbunden (Facebook Insights). Diesem wird nach Überschreiten einer gewissen Quantität an Page Impressions[22] eine qualifizierte Analyse der Nutzung des Angebots zur Verfügung gestellt. Diese in § 15 Abs. 3 TMG geregelte Reichweitenanalyse verortet die Verantwortlichkeit für die Nutzung der personenbezogenen Daten bei dem Diensteanbieter, der zur Erfüllung dieser Aufgabe einen Dienstleister, im konkreten Fall Facebook, heranzieht. Für

---

[20] Fn. 13, S. 14-15, Dammann, in: Simitis, Bundesdatenschutzgesetz, 7. Aufl. 2011, § 3 Rdn. 225.

[21] Artikel-29-Datenschutzgruppe, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 22.06.2010, WP 171, S. 13-14,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf.

[22] Aufruf einer Seite innerhalb eines Webseitenangebots, http://de.wikipedia.org/wiki/Seitenabruf.

die Handlungen des Dienstleisters ist nach den Maßgaben des § 11 BDSG bzw. § 17 Landesdatenschutzgesetz Schleswig-Holstein (LDSG S-H) der Diensteanbieter datenschutzrechtlich verantwortlich.

5.2.4 Nutzer als verantwortliche Stelle

Nach § 11 Abs. 2 TMG ist Nutzer im Sinne des datenschutzrechtlichen Abschnitts des Telemediengesetzes „jede natürliche Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen". Die Definitionen des Nutzers und des Betroffenen überschneiden sich. Gemäß § 2 Nr. 3 TMG ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder diese zugänglich zu machen. Nutzer im datenschutzrechtlichen Rechtsinn des Telemediengesetzes können daher Betroffene **und** gleichzeitig verantwortliche Stelle sein.[23] Für die Nutzereigenschaft spielt es keine Rolle, ob der Nutzer eine öffentliche oder eine nicht-öffentliche Stelle ist, ob dahinter eine juristische oder eine natürliche Person steckt.

Für die Verarbeitung Verantwortlicher ist diejenige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Vor diesem Hintergrund ist der Nutzer des Dienstes Facebook (auch) als Mitverantwortlicher anzusehen, soweit er z. B. personenbezogene Inhalte Dritter einstellt. Zwar sind bei Sozialen Netzwerken Ausnahmen für den Fall „ausschließlich persönlicher oder familiärer Tätigkeiten"[24] anerkannt. Allerdings räumt der Nutzer laut Ziffer 2 Nr. 1 der Facebook-Nutzungsbedingungen dem Betreiber Facebook weitgehende Rechte an den Inhalten ein, so dass der persönlich-familiäre Bereich verlassen wird.[25] Somit sind auch Betreiber von Fanpages als für die damit ausgelösten Verarbeitungsprozesse als verantwortliche Stellen anzusehen.

Als Betroffene im datenschutzrechtlichen Verständnis können nur natürliche Personen gelten. Der Schutz des Datenschutzrechts erstreckt sich nicht auf juristische Personen.

Nutzer kann auch eine natürliche Person sein, die einen Telemediendienst geschäftlich nutzt und/oder die zugleich kommerzieller Diensteanbieter i. S. v. § 2 S. 1 Nr. 5 TMG ist.

Im Anwendungsbereich des Telekommunikationsrechts ist der Nutzer bzw. der Betroffene „Teilnehmer" i. S. d. § 2 Nr. 20 TKG. Teilnehmer kann auch eine juristische Person sein.

Bedienen sich nicht-öffentliche oder öffentliche Stellen der Plattform von Facebook zur Darstellung eigener Inhalte (z. B. Fanpages), sind diese darüber hinaus verpflichtet, die jeweils geltenden gesetzlichen Vorgaben zur Auftragsdatenverarbeitung einzuhalten, § 11 BDSG, § 17 LDSG S-H.

5.3 Anwendbares Recht

Hinsichtlich des anzuwendenden Datenschutzrechts ist Folgendes zu unterscheiden:

- Die Zulässigkeit der Verarbeitung zum Datentransport (Übertragung von Signalen über Telekommunikationsnetze – Telekommunikation, § 3 Nr. 24 TKG) richtet sich nach dem Telekommunikationsgesetz (TKG) bzw. nach der E-Privacy-Richtlinie (Richtlinie 2009/136/EG als Neufassung der Richtlinie 2002/58/EG).

---

[23] Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, WP 163, S. 6-7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf; grundlegende Anerkennung findet dieses Konzept auch in der Literatur, Dammann, Fn. 19, § 3 Rdn. 226.

[24] Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, WP 163, S. 6-7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf.

[25] Bei Facebook ist es den Nutzenden zurzeit nicht zuverlässig möglich, Daten wie Fotos und Videos aus dem Sozialen Netzwerk wirklich zu löschen und den Zugriff darauf wirksam zu unterbinden. Dies ist in mehreren Fällen dokumentiert, z. B. http://www.tagseoblog.de/facebook-bilder-bei-google-loschen-praktisch-unmoglich.

- Die Interaktion zwischen Nutzer und Diensteanbieter ist im Telemediengesetz (TMG) bzw. ebenfalls in der E-Privacy-Richtlinie geregelt.
- Die Bewertung der Zulässigkeit von Inhaltsdaten, die nicht dem Telemedienrecht oder Telekommunikationsrecht unterfallen, richtet sich nach den Vorgaben des BDSG bzw. für öffentliche Stellen nach dem jeweiligen Landesdatenschutzgesetz.

Soziale Netzwerke sind zusammengesetzte Dienste, die sowohl Telekommunikations- wie auch Mediendienstleistungen enthalten. Für die rechtliche Klassifizierung von Anwendungen kommt es auf den Schwerpunkt der Diensterbringung an. Beim Versenden von privaten Nachrichten und dem Chatten in öffentlichen und geschlossenen Nutzergruppen steht in der Regel der telekommunikative Aspekt im Vordergrund, so dass das TKG anwendbar ist. Bei allen sonstigen Angeboten von Facebook und von Webseitenbetreibern (z. B. Kontaktliste, Social-Plugins, Apps, Spiele) ist das TMG anwendbar, soweit nicht Inhaltsdaten betroffen sind (s. u.).

Alle darüber hinausgehenden Datenverarbeitungen, insbesondere die Inhalte von Diensten und Kommunikation, haben sich am BDSG bzw. an der EU-DSRL zu orientieren. Inhaltsdaten sind nicht zur Vertragsabwicklung bzw. zur technischen Umsetzung eines Angebots erforderlich, sondern werden mit Hilfe des Telemediums bzw. Telekommunikationsdienstes transportiert. Hierzu zählen auch alle „freiwilligen" Angaben des Nutzers eines Sozialen Netzwerks (Name, Geschlecht, Alter, Interessen, Fotos).

Keine Anwendbarkeit des (materiellen) Datenschutzrechts ist gegeben, wenn die „Erhebung, Verarbeitung oder Nutzung der Daten … ausschließlich für persönliche oder familiäre Tätigkeiten" erfolgt (§§ 1 Abs. 2 Nr. 3, 27 Abs. 1 S. 2 BDSG). Dies ist bei vielen Nutzungen von Sozialen Netzwerken wie auch bei Facebook nicht der Fall, da diese nicht nur der privat-familiären Nutzung dienen, sondern auch Dritte einbezogen werden und soziale, berufliche und geschäftliche Zwecke bei der Datenverarbeitung eine Rolle spielen bzw. nicht ausgeschlossen werden können.[26]

Hinsichtlich der örtlichen Anwendbarkeit gilt im Datenschutzrecht grundsätzlich das Territorialitätsprinzip: Der Ort der Datenverarbeitung bestimmt, welches nationale Datenschutzrecht anwendbar ist. Beim Sitz eines Unternehmens innerhalb des Raumes der EU/EWR ist in Art. 4 EU-DSRL und in § 1 Abs. 5 BDSG eine Spezialregelung vorgesehen: Maßgebend ist für die Anwendbarkeit, in welchem Staat der Sitz der Daten verarbeitenden Stelle liegt. Dabei kommt es aber nicht auf den Hauptsitz an: Besteht in einem Staat eine Filiale oder Niederlassung, wo die geschäftliche Tätigkeit tatsächlich von einer „festen Einrichtung" aus ausgeübt wird, so ist das dortige nationale Recht anzuwenden.

Bei Telemedien wird hinsichtlich der Anwendbarkeit des TMG gemäß § 3 Abs. 1 TMG auf das Herkunftsland abgestellt. § 1 Abs. 5 TMG stellt klar, dass daneben die jeweiligen privatrechtlichen Kollisionsregeln anzuwenden sind. Haben Telemedienanbieter Töchter oder Filialen in Deutschland und zielt deren Angebot auf den deutschen Markt, z. B. indem ein deutschsprachiges Angebot bereitgehalten wird, so verfolgen diese Unternehmen gezielt die Erhebung und Verarbeitung von deutschen Nutzerdaten. In diesem Fall kann bei einer außereuropäischen Datenverarbeitung an die Verarbeitung auf den Nutzerrechnern (z. B. durch Setzen von Cookies) angeknüpft werden, und deutsches Recht ist anwendbar.

Da Facebook in Irland eine verantwortliche Niederlassung betreibt und keine Niederlassung in Deutschland besteht, ist für die Datenverarbeitung von Facebook zwar gemäß den gesetzlichen Zuständigkeitsregelungen irisches Recht anwendbar (§ 3 Abs. 1 u. 3 Nr. 4 TMG i. V. m. § 1 Abs. 5 BDSG). Jedoch dient Facebook Irland nach den vorliegenden Informationen nur als Anlauf- und Beschwerdestelle. Nur hierfür ist dann irisches Datenschutzrecht anwendbar. Hinsichtlich der Datenverarbeitung des Sozialen Netzwerks Facebook selber ist Facebook Inc. Betreiber bzw.

[26] Artikel-29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke, 12.06.2009, WP 163, S. 7, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf.

verantwortliche Stelle. Damit ist für die Datenverarbeitung von Facebook wieder direkt deutsches Datenschutzrecht anwendbar.

Etwas anderes gilt für private Webseitenbetreiber und Nutzer des Dienstes von Facebook sowie für öffentliche Stellen des Bundes in Deutschland. Soweit diese die Plattform Facebook für eigene Zwecke nutzen und Facebook in deren Auftrag tätig wird, sind diese Nutzer i. S. d. § 2 S. 2 Nr. 3 TMG bzw. verantwortliche Stelle i. S. d. § 3 Abs. 7 BDSG. Für öffentliche Stellen der Länder gilt das jeweilige Landesdatenschutzgesetz (z. B. § 3 Abs. 1 LDSG S-H).

Für eine unmittelbare Anwendung deutscher datenschutzrechtlicher Bestimmungen spricht auch die durch Facebook verwendete Ergänzung zu den Nutzungsbedingungen, die für deutsche Nutzerinnen und Nutzer die Anwendung deutschen Rechts vorsieht bzw. vorsah.[27]

5.4 Zulässigkeit der Datenverarbeitung

Stellen, die mittels Facebook personenbezogene Daten zur Erfüllung eigener Zwecke verarbeiten, müssen sicherstellen, dass diese Datenverarbeitung datenschutzrechtlich zulässig ist (§ 12 Abs. 1 TMG, § 4 Abs. 1 BDSG). Die Zulässigkeit kann sich aus gesetzlichen Regelungen ergeben oder aus einer ausdrücklichen Einwilligung des Betroffenen. Die Zulässigkeit muss hinsichtlich jedes einzelnen Verarbeitungsschritts festgestellt werden.

5.4.1 Einwilligung

Eine Datenverarbeitung ist zulässig, wenn die betroffene Person hierin eingewilligt hat (§ 4 Abs. 1 BDSG, § 12 Abs. 1 TMG, Art. 7 Buchst. a) EU-DSRL). Eine Einwilligung ist nur wirksam, wenn dieser eine vorherige Information über die konkrete Erhebung und Verwendung von Daten vorausgegangen ist. Nach § 4a BDSG muss diese Erklärung auf der freien Entscheidung des Betroffenen beruhen, weshalb er auf den vorgesehenen Zweck der Verarbeitung hingewiesen werden muss. Die erteilte Einwilligung muss bestimmt sein. Die Einwilligung muss den konkreten Zweck, Umfang, die Art der erhobenen Daten und die daraus resultierenden Konsequenzen erkennen lassen. Unwirksam wären daher alle pauschalen Erklärungen, in denen der Betroffene seine Zustimmung zu nicht klar definierten Verarbeitungsprozessen erteilt.[28]

Weitere Anforderung an die Wirksamkeit der Einwilligung ist die Kenntnis der einwilligenden Person in die Sachlage.

> *„‚In Kenntnis der Sachlage' bedeutet Einwilligung der betroffenen Person nach der bewussten Erfassung und Würdigung der Fakten und Auswirkungen einer Handlung. Sie muss in klarer und verständlicher Form genau und umfassend über alle relevanten Aspekte, […] wie Art und Zweckbestimmung der verarbeiteten Daten, Personen, an die die Daten möglicherweise weitergegeben werden, und ihre Rechte, aufgeklärt werden. Hierzu gehört auch die Aufklärung über die möglichen Folgen bei Verweigerung der Einwilligung zu der jeweiligen Verarbeitung."*[29]

Die Einwilligung bedarf nach § 4a Abs. 1 S. 2 BDSG der Schriftform, wenn nicht wegen besonderer Umstände eine andere Form angemessen ist. Hiervon kann bei Einwilligungen im Online-Bereich regelmäßig ausgegangen werden. Für die Verarbeitung von Nutzerdaten sieht § 13 Abs. 2 TMG eine elektronische Form alternativ zur Schriftform vor. Danach kann die Einwilligung „elektronisch erklärt werden, wenn der Diensteanbieter sicherstellt, dass

1. der Nutzer seine Einwilligung bewusst und eindeutig erklärt hat,

---

[27] https://www.facebook.com/terms/provisions/german, Stand des Abrufs 26. Juni 2011; am 17. August 2011 war diese Klausel nicht verfügbar.

[28] Artikel-29-Datenschutzgruppe, Opinion 15/2011 on the definition on consent, 13.07.2011, WP 187, S. 17, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf; Simitis, in ders., Bundesdatenschutzgesetz, 7. Aufl., 2011, § 4a Rdn. 77.

[29] Artikel-29-Datenschutzgruppe, Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten, 15.02.2007, WP 131, S. 26,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_de.pdf; Simitis, ebda, § 4a Rdn. 72.

2. die Einwilligung protokolliert wird,
3. der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
4. der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann."

Facebook fingiert die Erteilung der Einwilligung mit der Einrichtung des Nutzerkontos. Während des Anmeldeprozesses erfolgt keine klare Information über die Art, den Umfang und den Zweck der Erhebung, Verarbeitung und Nutzung der Daten. Das „Registrieren" bei Facebook kann nicht mit einer datenschutzrechtlich wirksamen Einwilligung gleichgesetzt werden, weil damit keine ausdrückliche Einbeziehung des Willens der Nutzerinnen und Nutzer in sämtliche vorgesehenen und als Standard konfigurierten Formen der Datenverarbeitung erfolgt. Vielmehr wird lediglich pauschal auf eine Vielzahl von Dokumenten verwiesen, die durchzuarbeiten keinem Nutzenden zumutbar ist:

- Nutzungsbedingungen mit weiteren Verweisen u. a. auf Facebook-Grundsätze, Privatsphäre- und Anwendungseinstellungen, Richtlinien für Promotions, Zahlungsbedingungen, Grundsätze und Richtlinien für Entwickler, Werberichtlinien, Nutzungsbedingungen für Facebook-Seiten, Facebook Site Governance, Besondere Regeln für deutsche Nutzer,
- Facebook-Datenschutzrichtlinien mit weiteren Verweisen auf u. a. Safe Harbor[30]-Bestimmungen, Privatsphäre- und Anwendungseinstellungen, Nutzungsbedingungen, Facebook-Werbeanzeigen, Facebook Site Governance.

Facebook bietet damit den interessierten Nutzerinnen und Nutzern zwar teilweise sehr weitgehende Informationen über die durchgeführten Datenverarbeitungen. Diese Informationen sind aber nicht hinreichend bestimmt und genügen nicht den Mindestanforderungen an Transparenz. Denn es werden vage Formulierungen gewählt, die den Umfang und Art der Datenverarbeitung nicht hinreichend erkennen lassen. So formuliert Facebook zum Beispiel zur Erfassung der Nutzeraktivitäten:

> *„Wir verwenden die von uns erfassten Informationen, um dir unsere Dienstleistungen und Funktionen zur Verfügung zu stellen, diese Dienstleistungen und Funktionen zu analysieren, zu messen und zu optimieren und dir eine Kundenbetreuung anzubieten. Wir verwenden die Informationen, um potenziell rechtswidrige Handlungen zu unterbinden und die in unserer „Erklärung der Rechte und Pflichten" verankerten Nutzungsbedingungen durchzusetzen. Wir arbeiten auch mit einer Vielzahl technischer Systeme zur Erkennung anomaler Aktivitäten und Prüfung von Inhalten, um Missbrauch wie Spam zu verhindern."*[31]

Unklar bleibt, welche Daten zu Verfolgung der sehr vage genannten Ziele erfasst und ausgewertet werden. Rechtlich unbestimmt ist u. a. die Formulierung *„potenziell rechtswidrige Handlungen"*. Nutzerinnen und Nutzern wird nicht deutlich gemacht, welche Handlungen dies sein könnten.

---

30 Das Safe Harbor-Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem diese sich verpflichten, die Safe Harbor-Grundsätze zu beachten. Dies ist die Voraussetzung dafür, dass europäische Stellen personenbezogene Daten an diese Unternehmen übermitteln dürfen. Im April 2010 hat der Düsseldorfer Kreis allerdings festgestellt, dass sich deutsche Stellen nicht auf die Behauptung einer Safe Harbor-Zertifizierung einer US-amerikanischen Organisation verlassen dürfen, sondern überprüfen müssen, wie das US-amerikanische Unternehmen die Safe Harbor-Grundsätze einhält. Dazu gehört insbesondere die Informationspflicht darüber, zu welchem Zweck das Unternehmen die Daten über die Betroffenen erhebt und verwendet, wie die Betroffenen die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege das Unternehmen den Betroffenen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken,
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf.

31 Ziffer 5 der Facebook-Datenschutzrichtlinien.

Denn es wird nicht auf die Rechtswidrigkeit der Handlungen, sondern das Potenzial derselben abgestellt.

Zugleich werden wesentliche Formen der Datenverarbeitung nicht erwähnt (z. B. Einbindung von CDN) oder nur angesprochen, ohne dass die Funktionen genauer und verständlich erläutert werden (z. B. Reichweitenanalyse per Insights und Werbenutzung). Die Informationen werden nicht so in die eingeforderte Erklärung inkorporiert, dass die Betroffenen die Bedeutung ihrer Erklärung übersehen können. Die notwendige Hervorhebung nach § 4a Abs. 1 S. 3 BDSG erfolgt nicht. Zudem sind die Anforderungen der § 13 Abs. 2 Nrn. 1, 3 und 4 TMG nicht erfüllt. Stattdessen wird bei der Registrierung nur auf zahlreiche weitere Dokumente verwiesen.

Nicht ausreichend für die Erteilung einer wirksamen Einwilligung ist eine reine Information über eine standardmäßig stattfindende personenbezogene Datenverarbeitung, verbunden mit der Möglichkeit, diese durch Anklicken eines Buttons zu unterbinden (Opt-out statt Opt-in). Ein solches Opt-out von Standardeinstellungen, die eine weitgehende Datenverarbeitung erlauben, ist bei Facebook weit verbreitet, z. B. bzgl. der Weiterleitung von Daten an Webseitenbetreiber.[32]

Bei den Nutzungsbedingungen von Facebook handelt es sich um Allgemeine Geschäftsbedingungen (AGB). Die Anforderungen an die rechtliche Bindungswirkung derartiger AGB sind in den §§ 305 ff. BGB geregelt. Diesen Anforderungen genügen die Facebook-Regeln inhaltlich wie formal nicht. So ist nach deutschem Recht schon der Verweis auf die englischsprachige Version der AGB als maßgebliche Version unzulässig, da AGB in der Regel in deutscher Sprache abgefasst sein müssen, um in Deutschland gegenüber Verbrauchern wirksam zu sein bzw. deshalb nur die deutsche Version gültig sein kann. Die Regelung in Ziffer 2 Nr. 1 der Nutzungsbedingungen räumt Facebook umfangreiche Rechte an vom Nutzer eingestellten Inhalten wie Fotos, Videos etc. ein, die sogar eine Unterlizenzierung erlauben sollen. Dies stellt eine überraschende Klausel im Sinne des § 305c BGB dar und ist damit unwirksam.

Ein weiteres Beispiel für die Rechtswidrigkeit der Klauseln ist die Regelung in Ziffer 10 Nr. 3 der Nutzungsbedingungen, wonach sich Facebook vorbehält, Werbung („bezahlte Dienstleistungen und Kommunikation") nicht als solche zu kennzeichnen. Dies widerspricht § 6 Abs. 1 Nr. 1 TMG, wonach kommerzielle Kommunikationen stets klar als solche erkennbar sein müssen.

Bisher sind keine Einwilligungen von anderen Unternehmen und Anbietern bekannt, die Daten mit Facebook austauschen, die den oben genannten rechtlichen Anforderungen genügen.

Aus dem oben Gesagten ergibt sich, dass die personenbezogene Datenverarbeitung bei Facebook in keinem Fall durch eine nach deutschem bzw. europäischem Recht wirksame Einwilligung legitimiert werden kann. Hinzuweisen ist zudem darauf, dass eine Einwilligung nur durch die betroffene Person erteilt werden kann. Eine Einwilligung zur Verarbeitung von Daten Dritter ist rechtlich ausgeschlossen.

5.4.2 Zulässigkeit der Reichweitenanalyse - Facebook Insights

Der durch Facebook für die Einbindung von Social-Plugins und Fanpages angebotene Reichweitenanalysedienst „Facebook Insights" kann nicht über die von Facebook eingeholte „Einwilligung" datenschutzrechtlich gerechtfertigt werden. § 15 Abs. 3 TMG sieht jedoch zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien vor, dass Nutzungsprofile bei Verwendung von Pseudonymen erstellt werden dürfen. Dies gilt jedoch nur, sofern der Nutzer dem nicht widerspricht. Außerdem hat der Diensteanbieter den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 TMG hinzuweisen. Die erstellten Nutzungsprofile dürfen im Übrigen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.[33]

---

[32] Feature „Überprüfte Webseiten und Anwendungen".

[33] Vgl. dazu auch Beschluss des Düsseldorfer Kreises vom 27. November 2009, Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten,

Betreiber von Fanpages und Webseitenbetreiber, die Social-Plugins von Facebook auf ihren Seiten einbinden, sind nach § 15 Abs. 3 TMG verpflichtet, bei der Erstellung von Nutzungsprofilen auf pseudonymer Basis die Nutzer hierüber sowie über ihre Möglichkeit zum Widerspruch zu unterrichten. Im Fall eines Widerspruchs muss die Profilerstellung unterlassen werden. Dies setzt voraus, dass technisch die Möglichkeit der Widerspruchserteilung implementiert ist. Für Betreiber von Fanpages ist dies nach derzeitigem Wissensstand nicht möglich. Webseitenbetreiber, die Social-Plugins verwenden, müssen sicherstellen, dass eine Übermittlung von identifizierenden Angaben gegenüber Facebook unterbleibt, sobald Nutzerinnen oder Nutzer der Reichweitenanalyse widersprechen.

Werden von einem Webseitenbetreiber Social-Plugins eingebunden, so initiiert Facebook beim Anklicken das Setzen des Cookies „datr" mit einer Lebensdauer von mindestens zwei Jahren auch bei nicht-authentifizierten und nicht-angemeldeten Nutzern mit einer ID, die bei jeder Kommunikation mit Facebook oder mit dem Anklicken eines Social-Plugins wiedererkannt wird. Bei Facebook führt dies zu einer Profilbildung. Hierüber werden die Betroffenen nicht informiert. Auch über das gesetzlich vorgesehene Widerspruchsrecht werden sie nicht informiert. Ein solches Widerspruchsrecht mit der Möglichkeit des Ausschlusses einer Profilbildung besteht auch gar nicht. Die erstellten Profile werden dafür genutzt, dem jeweiligen Webseitenbetreiber Nutzungsanalysen zu ermöglichen, ihm die sog. „Insights" zu geben.

5.4.2.1 Missachtung der E-Privacy-Richtlinie

Über § 15 Abs. 3 TMG hinausgehend verlangt Art. 5 Abs. 3 E-Privacy-Richtlinie beim Setzen von Cookies, die nicht allein für die Erbringung des Dienstes erforderlich sind und genutzt werden, die Einwilligung des Nutzers. Diese inzwischen direkt anwendbare Regelung geht über die Anforderungen des § 15 Abs. 3 TMG insofern hinaus, dass hier nicht nur eine Information mit einer Opt-out-Möglichkeit gefordert wird, sondern ein Opt-in. Diesen Anforderungen wird die Nutzung von Facebook-Social-Plugins nicht gerecht.

5.4.2.2 Verstoß gegen das Trennungsgebot des § 15 Abs. 3 S. 3 TMG

Wegen der Missachtung des in § 15 Abs. 3 TMG festgelegten Trennungsgebotes ist das Einbinden von Social-Plugins von Facebook in deutschen Webseiten und das Betreiben von „Facebook Insights" auf Fanpages innerhalb von Facebook unzulässig. Ein Verstoß gegen das Gebot § 15 Abs. 3 S. 3 TMG stellt zugleich eine Ordnungswidrigkeit nach § 16 Abs. 2 Nr. 5 TMG dar, die mit einer Geldbuße bis zu 50.000 Euro geahndet werden kann.

Bei authentifizierten und angemeldeten Nutzern werden neben den standardmäßig gesetzten Cookies, die aus jeder Interaktion mit Facebook hervorgehen, weitere Cookies gesetzt. Diese werden für die Authentifizierung und die Profilbildung genutzt.

Der Cookie „datr" ist als Identifikator ein personenbezogenes Datum. Dies gilt in Bezug auf sämtliche bei Facebook angemeldeten Nutzende. Denn Facebook kann die hierüber erlangten Nutzungsdaten einem individuellen angemeldeten Facebook-Nutzenden namentlich zuordnet.

Dies gilt auch für nicht-angemeldete Nutzer, wenn die Cookie-ID innerhalb des mindestens zweijährigen Bestehens als Pseudonym im Fall einer späteren Anmeldung bei Facebook eindeutig zugeordnet werden kann. Darüber hinausgehend erhält Facebook weitere Angaben, über die eine Identifizierung des Nutzers grundsätzlich möglich ist (IP-Adresse, Browserstring, eindeutige Webseiten-ID, Ablaufumgebung des Browsers mit Zusatzinformationen). Auf der Grundlage dieser Daten erfolgt die Reichweitenanalyse.

Der Reichweitenanalysedienst wird allen zur Verfügung gestellt, die Entwickler oder Betreiber einer Anwendung oder Seite auf der Facebook-Plattform sind. Eine Möglichkeit, diese Funktionalität abzustellen, ist nicht vorgesehen und nicht bekannt. Facebook erstreckt damit die Erfassung der

---

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.html?nn=409242.

Nutzerdaten über sein eigenes Angebot auch auf die Angebote Dritter, die Social-Plugins anbieten. Facebook ist somit in der Lage nachzuvollziehen, welche anderen Angebote (mit Social-Plugin) die eigenen Nutzer außerhalb von Facebook besuchen, wenn diese nicht aktiv eine Verfolgung über die Session Cookies durch Löschen und bewusstes Abmelden vom Netzwerk unterbinden.

Bei angemeldeten und authentifizierten Nutzerinnen und Nutzern wird zur Erstellung der demographischen Nutzungsanalyse auf Informationen aus dem Facebook-Nutzerkonto zugegriffen. Facebook als funktionaler Auftragsdatenverarbeiter führt für die Webseitenbetreiber und Fanpagebetreiber die Nutzungsinformationen aus der Reichweitenanalyse, die unter dem Pseudonym des Cookies erstellt werden, mit den Angaben über den angemeldeten und authentifizierten Nutzer aus dem Nutzerkonto zusammen. Dies verstößt gegen das gesetzliche Verbot, die erstellten Nutzerprofile dahingehend zu qualifizieren, dass sie Aussagen über die konkrete und namentlich erkennbare Person zu lassen. Facebook ist dazu jedoch mit dem Dienst „Facebook Insights" in der Lage und realisiert dies. Dadurch, dass Webseitenbetreibern und Fanpagebetreibern eine eigene datenschutzrechtliche Verantwortung für deren Angebote zukommt, schlägt diese Unzulässigkeit auch auf sie durch.

5.5 Weitere gesetzliche Regelungen für deutsche Webseitenbetreiber

5.5.1 Informationspflichten

Nach § 5 Abs. 1 TMG sind Webseitenbetreiber verpflichtet, ein Impressum auch auf Unterseiten von Social Media-Plattformen wie Facebook zu führen. Ein Verweis auf das Impressum des Plattformbetreibers genügt nicht.

Nach § 13 Abs. 1 TMG sind Webseitenbetreiber verpflichtet, „den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten […] zu unterrichten." Diesen Anforderungen kommt nach den bisherigen Erfahrungen kein Webseitenbetreiber, der Social-Plugins von Facebook nutzt und dadurch Datenübermittlungen an Facebook initiiert, nach.[34]

Verstöße gegen § 5 Abs. 1 oder § 13 Abs. 1 TMG stellen jeweils eine Ordnungswidrigkeit nach § 16 Abs. 2 Nrn. 1 u. 2 TMG dar, die mit einem Bußgeld bis zu 50.000 Euro geahndet werden kann.

5.5.2 Datensicherheit

Nach § 13 Abs. 4 TMG ist ein Telemedienanbieter verpflichtet, „durch technische und organisatorische Vorkehrungen sicherzustellen, dass […]

> 2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des Satzes 2 gesperrt werden,
>
> 3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann, […]
>
> 6. Nutzungsprofile nach § 15 Abs. 3 nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können."

Nach § 13 Abs. 5 TMG ist die Weitervermittlung zu einem anderen Diensteanbieter dem Nutzer anzuzeigen. Diesen Anforderungen genügen die Webseitenbetreiber mit Social-Plugins von Facebook nicht. Ein Verstoß gegen § 13 Abs. 4 Nrn. 1-4 oder 5 TMG stellt nach § 16 Abs. 2 Nr. 3 TMG eine Ordnungswidrigkeit dar, die mit einer Geldbuße bis zu 50.000 Euro geahndet werden kann.

[34] Kammergericht Berlin v. 29.04.2011, Az. 5 W 88/11.

5.6 Schlussfolgerungen

5.6.1 Konsequenzen für Webseiten- und Fanpagebetreiber

Als erster Schritt sind die Seitenbetreiber allgemein darauf hinzuweisen, dass das Betreiben einer Fanpage und die Einbindung von Social-Plugins von Facebook zwangsläufig zu Datenschutzverstößen führt, verbunden mit der Aufforderung, die Nutzung dieser Facebook-Anwendungen für die Zukunft zu unterlassen. Anwender in Schleswig-Holstein können nach einer Umsetzungsfrist von einem Monat im Einzelfall aufgefordert werden, die rechtswidrige Datenverarbeitung über deren Webseite einzustellen, verbunden mit dem Hinweis auf die Möglichkeiten einer Untersagung nach § 38 Abs. 5 BDSG und eines Bußgeldverfahrens nach § 16 TMG und/oder § 43 BDSG bei privaten Stellen bzw. einer Beanstandung nach § 42 Abs. 2 LDSG S-H bei öffentlichen Stellen.

5.6.2 Sonstige Konsequenzen

Weitere behördliche Maßnahmen gegen Facebook selbst und gegen CDN-Anbieter sind noch zu prüfen.

Die Nutzerinnen und Nutzer sind über die für diese bestehenden Risiken hinsichtlich ihres Datenschutzes zu informieren. Zudem sind sie darauf hinzuweisen, wie sie im umfassenden Kontext der Facebook-Datenverarbeitung ihre Rechte wahrnehmen können.