Möglichkeiten und Grenzen der sogenannten „Facebookfahndung“

Von Privatdozent Dr. **Sönke Gerhold**, Bremen*

Schon längst nutzen die Polizeibehörden das Internet und auch soziale Plattformen wie Facebook zur Unterstützung von Sach- und Personenfahndungen. Gerade die Fahndung auf Facebook bietet dabei wegen des großen Nutzerkreises im Vergleich zu einer einfachen Internetfahndung überdurchschnittliche Erfolgschancen. Auf der anderen Seite birgt die Facebookfahndung aber auch im gleichen Maße Risiken und wird insbesondere aus datenschutzrechtlichen Gründen massiv kritisiert. Ob und unter welchen Voraussetzungen sie dennoch zulässig ist, ist Gegenstand des vorliegenden Beitrags.

I. Einleitung

Die Landespolizeibehörden, die Landeskriminalämter und das Bundeskriminalamt nutzen schon seit längerem die neuen Fahndungsmöglichkeiten, die das Internet eröffnet.[1] Überwiegend werden die Daten dabei auf speziell hierfür eingerichteten Internetseiten der Behörden veröffentlicht[2], teilweise aber auch im „na-presseportal“[3] oder in sozialen Netzwerken wie Facebook[4].

Unter den sozialen Netzwerken hat Facebook derzeit den größten Marktanteil[5] und ist aus diesem Grund besonders geeignet, um Fahndungsaufrufe schnell und unkompliziert zu verbreiten. Ein Modellprojekt, das 2011 in Hannover durchgeführt worden ist, hat bestätigt, dass die Fahndungserfolge gegenüber herkömmlichen Fahndungsmethoden „wesentlich erhöht“[6] sind.[7] Im Hinblick auf die großen Chancen der Facebookfahndung haben sich neben den Sprechern verschiedener Polizeibehörden[8] auch die Justizminister auf der Justizministerkonferenz am 14.11.2013 in Berlin für ein Festhalten an dieser Methode entschieden und wollen zu diesem Zweck die Richtlinien über die Inanspruchnahme von Publikationsorganen und die Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung nach Personen im Rahmen von Strafverfahren[9] überarbeiten.[10]

Die große Zahl der Personen, die den Fahndungsaufruf wahrnehmen, bringt nun jedoch nicht nur positive Effekte mit sich, sondern sie führt umgekehrt auch zu einem im Vergleich zur klassischen Fahndung schwerer zu bewertenden Eingriff in das Allgemeine Persönlichkeitsrecht der Gesuchten. Zudem wirft gerade die Fahndung im sozialen Netzwerk Facebook im Vergleich mit der Fahndung in anderen sozialen Netzwerken erhebliche datenschutzrechtliche Probleme auf, weshalb sich der vorliegende Beitrag auf die Facebookfahndung konzentriert.[11] Ebenfalls soll das Thema auf die

---

* Der *Autor* vertritt derzeit die Professur für Strafrecht an der Universität Bremen.

[1] Vgl. *Schiffbauer*, NJW 2014, 1052.

[2] Vgl. beispielhaft die Fahndungsseite der hessischen Polizei, abzurufen unter: http://www.polizei.hessen.de/icc/internetzentral/nav/965/96570ee1-825a-f6f8-6373-a91bbcb63046.htm (9.3.2015), oder die des BKA, abzurufen unter: http://www.bka.de/nn_198404/DE/Fahndungen/Personen/personen__node.html?__nnn=true (9.3.2015).

[3] Vgl. http://www.presseportal.de/polizeipresse/p_dienststellen.htx (9.3.2015); es handelt sich beim „na-presseportal“ um ein Tochterunternehmen der dpa mit Sitz in Hamburg; vertiefend zur Nutzung des „na-presseportals“ zu Fahndungszwecken *Schiffbauer*, NJW 2014, 1052 (1053 f.).

[4] So z.B. das LKA Niedersachen, vgl. https://www.facebook.com/LandeskriminalamtNiedersachsen?fref=ts (9.3.2015), oder die Polizei Düsseldorf, vgl. https://www.facebook.com/Polizei.NRW.D?fref=ts (9.3.2015). Vertiefend zu den tatsächlichen Hintergründen *Ihwas*, Strafverfolgung in Sozialen Netzwerken, 2014, S. 266 ff.

[5] Facebook hatte Anfang 2015 ca. 28 Millionen aktive Nutzer in Deutschland, wohingegen XING und LinkedIn im Vergleich dazu nur, aber im Vergleich mit anderen sozialen Netzwerken immerhin noch, geschätzte 8 bzw. 6 Millionen aktive Nutzer in Deutschland vorweisen konnten. Twitter oder StudiVZ nutzten sogar nur ca. zwei bzw. eine Million Menschen in Deutschland, vgl. zu den Nutzerzahlen: https://buggisch.wordpress.com/2015/01/07/social-media-und-soziale-netzwerke-nutzerzahlen-in-deutschland-2015 (9.3.2015).

[6] So die Beschlussniederschrift über die 198. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 4. bis 6.12.2013 in Osnabrück, abzurufen unter: http://www.rdv-online.com/aktuelles/private_fahndungsfotos_im_internet (9.3.2015).

[7] Umfassend *Lohmeier u.a.*, Onlinefahndung in sozialen Netzwerken, 2014, S. 3 ff., abzurufen unter: http://smtu-berlin.de/wp-content/uploads/2014/10/Öffentlichkeitsfahndung-in-sozialen-Netzwerken-Forschungsbericht-SMTU.pdf (9.3.2015); vgl. auch *Hawellek/Heinemeyer*, ZD Aktuell 2012, 02730.

[8] Vgl. beispielhaft die Pressemitteilung des LKA Niedersachsen v. 18.6.2014, online abzurufen unter: http://www.presseportal.de/polizeipresse/pm/105578/2763814/lka-ni-facebook-fahndung-im-lka-feiert-2jaehrigen-geburtstag-23-106-facebook-fans (9.3.2015).

[9] Anlage B zu den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) v. 1.1.1977, zuletzt geändert mit Wirkung zum 1.9.2014 durch Bekanntmachung v. 23.7.2014, BAnz AT v. 18.8.2014 B1.

[10] Vgl. ZD-Aktuell 2013, 03824; LT-Drs. RP 16/3387, S. 2 ff., sowie den Beschluss zu TOP II. 2., abzurufen unter: http://www.justiz.nrw.de/JM/justizpolitik/jumiko/beschluesse/2013/herbstkonferenz13/zw1/TOP_II_2.pdf (9.3.2015).

[11] Vgl. zur Erforderlichkeit, zwischen den einzelnen Diensteanbietern zu differenzieren, *Mergel u.a.*, Praxishandbuch Soziale Medien in der öffentlichen Verwaltung, 2013, S. 75 f.

Fahndung durch Strafverfolgungsorgane, d.h. Ausschreibung und Öffentlichkeitsfahndung i.S.d. §§ 131 ff. StPO, beschränkt bleiben. Die zahlreichen Probleme und Fragen, die private Fahndungsaufrufe[12] und staatliche Onlineermittlungen im Übrigen[13] aufwerfen, werden ausgeklammert.

II. Die grundsätzliche Zulässigkeit des Betreibens öffentlich-rechtlicher Fanpages

Damit eine Polizeibehörde überhaupt einen Fahndungsaufruf auf Facebook online stellen kann, muss sie zunächst eine eigene Facebookseite einrichten. Im behördlichen und gewerblichen Kontext spricht man insofern von einer Fanpage.[14]

Ob Behörden befugt sind, Fanpages einzurichten, ist umstritten und noch nicht abschließend geklärt. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD SH) klagt derzeit in der Revision vor dem BVerwG, nachdem es vor dem VG Schleswig[15] und dem OVG Schleswig[16] mit seiner Rechtsauffassung, dass Behörden und Unternehmen keine Fanpages betreiben dürfen, unterlegen war.[17] Das OVG Schleswig hatte die Revision zugelassen, weil entscheidende Rechtsfragen bislang „nicht höchstrichterlich geklärt“ seien.

Die rechtliche Zulässigkeit des Betreibens einer Fanpage wird dabei in der gegenwärtigen Diskussion unter zwei Aspekten kritisch gesehen. Zum einen wird problematisiert, ob das Einrichten einer Fanpage nicht zu einer datenschutzrechtlichen Verantwortlichkeit des Betreibers für einen unzulässigen Datenverarbeitungsvorgang führe, zum anderen, ob ein ggf. bestehender datenschutzrechtlicher Verstoß des Unternehmens Facebook der Nutzung der angebotenen Dienste durch die öffentliche Verwaltung entgegenstehe.[18] Die folgende Darstellung widmet sich nun zunächst der Frage nach der unmittelbaren datenschutzrechtlichen Verantwortlichkeit der Fanpagebetreiber für mögliche Rechtsverstöße durch Facebook und dann der nach ihrer mittelbaren Verantwortlichkeit.

1. Die unmittelbare Verantwortlichkeit der Polizeibehörden für Datenschutzverstöße

Möglicherweise sind die Fanpagebetreiber unmittelbar für alle datenschutzrechtlichen Verstöße verantwortlich, die im Zusammenhang mit der von ihnen eingerichteten Seite stehen. So wird es u.a. vom ULD SH vertreten.

a) Die Position des ULD SH

Das ULD SH steht auf dem Standpunkt, dass der Betreiber einer Fanpage Diensteanbieter i.S.d. § 2 Nr. 1 TMG und zugleich nach § 3 Abs. 7 BDSG i.V.m. Art. 2 lit. d) EU DSRL[19] bzw. den entsprechenden landesgesetzlichen Regelungen[20] die für die Einhaltung der Datenschutzvorschriften verantwortliche Stelle sei.[21] Der Betreiber einer Webpage könne sich seiner datenschutzrechtlichen Verantwortung für die durch oder die über seine Seite vorgenommene Verarbeitung personenbezogener Daten[22] nicht durch die Inanspruchnahme externer Dienstleister entziehen.[23] Wem es als Verantwortlichem aber nicht möglich sei, die datenschutzrechtlichen Pflichten einzuhalten, dürfe – frei zusammengefasst – auch keine Fanpage betreiben.[24]

aa) Die Begründung der Stellung der Fanpagebetreiber als Diensteanbieter und für den Datenschutz verantwortliche Stelle durch das ULD SH

Das ULD SH führt zur Begründung seiner Rechtsposition aus, dass in Fällen, in denen das TMG Anwendung finde, der Diensteanbieter die datenschutzrechtliche Verantwortung trage (§ 12 TMG).[25] Diensteanbieter i.S.d. § 2 Nr. 1 TMG sei „jede natürliche oder juristische Person, die eigene oder

---

[12] Vgl. hierzu *Schiffbauer*, NJW 2014, 1052 (1056 f.); *Lohmeier u.a.* (Fn. 7), S. 26, sowie zu Lynchaufrufen und organisiertem Internetmobbing als möglicher Konsequenz privater Fahndungsaufrufe *Ostendorf/Frahm/Doege*, NStZ 2012, 529 (531 ff.).

[13] Vgl. hierzu *Graf*, in: Graf (Hrsg.), Beck’scher Online-Kommentar, Strafprozessordnung, Stand: 8.9.2014, § 100a Rn. 32 ff., und speziell zu sozialen Netzwerken Rn. 32g ff., sowie *Rosengarten/Römer*, NJW 2012, 1764 (1766 f.), und *Schulz/Hoffmann*, DuD 2012, 7 (8 ff.).

[14] Vgl. VG Schleswig, DuD 2014, 120; vertiefend *Mergel u.a.* (Fn. 11), S. 75 f., und *Hoffmann/Schulz/Brackmann*, in: Schliesky/Schulz (Hrsg.), Transparenz, Partizipation, Kollaboration, Web 2.0 für die öffentliche Verwaltung, 2012, S. 177.

[15] VG Schleswig DuD 2014, 120.

[16] OVG Schleswig, Urt. v. 4.9.2014 – 4 LB 20/13 (juris).

[17] Vgl. https://www.datenschutzzentrum.de/presse/20140929-ovg-urteil-facebook-fanpages.htm (9.3.2015).

[18] *Mergel u.a.* (Fn. 11), S. 75 f.

[19] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. EG 1995 Nr. L 281, S. 31 ff.

[20] Beispielsweise § 2 Abs. 3 LDSG SH.

[21] Vgl. VG Schleswig DuD 2014, 120, sowie Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD SH), Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook v. 19.8.2011, S. 17 f., mit umfassender Begründung, abzurufen unter: https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf (9.3.2015).
Ebenso *Polenz*, VuR 2012, 207 (211).

[22] Vgl. zum Begriff der personenbezogenen Daten speziell im Zusammenhang mit Facebook den Bericht des Wissenschaftlichen Dienstes des Bundestages v. 7.10.2011 – Az.: WD 3 – 3000 – 306/11 neu, Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins, S. 5 ff.; den Bericht des Wissenschaftlichen Dienstes des Landtages Schleswig-Holstein v. 24.10.2011 – Az.: L 203 – 140/17, Umdruck 17/2988, S. 2 ff., sowie *Polenz*, VuR 2012, 207 (209 f.).

[23] ULD SH (Fn. 21), S. 17.

[24] Vgl. VG Schleswig DuD 2014, 120.

[25] So ULD SH (Fn. 21), S. 16 ff.

fremder Telemedien zur Nutzung bereit[halte] oder den Zugang zur Nutzung vermittel[e]“[26].

Zudem sei nach § 3 Abs. 7 BDSG diejenige Stelle für den Datenschutz verantwortlich, „die personenbezogene Daten für sich selbst erheb[e], verarbeite[e] oder nutz[e] oder dies durch andere im Auftrag vornehmen [lasse].“[27] Nach Art. 2 lit. d) EU DSRL sei verantwortlich, wer „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheid[e].“[28]

Im Rahmen dieser Bestimmungen seien neben den rechtlichen auch tatsächliche Umstände zu beachten.[29] Es komme also darauf an, ob die Stelle „nach Würdigung aller Gesamtumstände aufgrund des tatsächlichen Einflusses den Prozess der Datenverarbeitung steuer[e].“[30] Zu beachten sei bei der Prüfung, dass diese Voraussetzungen ebenfalls durch die „Einbindung ‚fremder‘ Verarbeitungsprozesse in das eigene Angebot des Diensteanbieters“ erfüllt werden könnten, etwa wenn „durch die Konfiguration z.B. einer Webseite ein Verarbeitungsprozess bei einem weiteren Dienstleister ausgelöst“ werde.[31] Dies gelte umso mehr, wenn der Diensteanbieter die Dienste Dritter – wie etwa bei verhaltensbasierter Online-Werbung oder beim Erstellen einer Reichweitenanalyse für die jeweilige Fanpage – für eigene Zwecke nutze. Schon das Einbinden von Social-Plugins würde daher die Verantwortlichkeit des Seitenbetreibers begründen, da dieser zwar nicht selbst Daten erhebe oder speichere, aber „durch die Gestaltung seiner Webseite die Datenweitergabe an Facebook initiier[e] und in der Hand ha[be].“ Entsprechendes gelte im Hinblick auf das Tool „Insights“, mit dessen Hilfe Facebook den Betreibern von Fanpages detaillierte Statistiken über die Nutzer der jeweiligen Seite zur Verfügung stelle.[32] Darüber hinaus sei der Fanpagebetreiber aber auch nach den §§ 11 BDSG, 17 LDSG SH (Auftragsdatenverarbeitung) für die Handlungen des Dienstleisters datenschutzrechtlich verantwortlich.[33]

bb) Die Begründung des Verstoßes gegen datenschutzrechtliche Pflichten durch das ULD SH

In der Eigenschaft als für den Datenschutz verantwortliche Stelle müsste der Seitenbetreiber die Nutzer seiner Angebote gemäß § 13 Abs. 1 TMG über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten unterrichten und die Vorschrift des § 13 Abs. 3 TMG, in der die Einwilligung in die Datenverarbeitung geregelt sei, einhalten.[34] Nutzungsprofile dürften nur nach Maßgabe des § 15 Abs. 3 TMG erstellt werden.[35] Die Nutzer müssten daher ausdrücklich in die Profilerstellung einwilligen und wären auf die Erstellung des Nutzerprofils und auf ihre Möglichkeit zum Widerspruch hinzuweisen.[36] Sollten Nutzer widersprechen, dürften ihre Daten nicht zur Profilerstellung verwendet werden.[37] Die Betreiber von Fanpages hätten jedoch keine Möglichkeit, auf die Profilerstellung durch Facebook Einfluss zu nehmen. Zudem würden die Nutzungsprofile mit Daten über die Träger der Pseudonyme zusammengeführt.[38]

Auch über die Verwendung von Cookies müsste zumindest nach der E-Privacy-Richtlinie[39], deren unmittelbare Geltung tatsächlich umstritten ist, aufgeklärt und der Verwendung zugestimmt werden. Art. 5 Abs. 3 der Richtlinie bestimme, dass „die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert [seien], nur gestattet [sei], wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u.a. über die Zwecke der Verarbeitung er[halte], seine Einwilligung gegeben ha[be].“ Hiernach gelte also das sogenannte „Opt-in“-Prinzip, wenn der Cookie nicht unverzichtbar sei, um das gewünschte Angebot zu nutzen.[40]

Schließlich rügt das ULD SH, dass die Fanpagebetreiber der in § 13 Abs. 4 Nr. 2 TMG normierten Pflicht, „durch technische und organisatorische Vorkehrungen sicherzustellen, dass die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht“ würden, nicht nachkommen könnten.[41] Unternehmen und Behörden dürften nach alledem keine Fanpages bei Facebook betreiben.

[26] Zitiert wird der Wortlaut des § 2 Nr. 1 TMG.
[27] Zitiert wird der Wortlaut des § 3 Abs. 7 BDSG.
[28] Zitiert wird der Wortlaut des Art. 2 lit. d. der EU DSRL.
[29] So ULD SH (Fn. 21), S. 16.
[30] So ULD SH (Fn. 21), S. 17, unter Bezugnahme auf *Dammann*, in: Simitis (Hrsg.), Nomos Kommentar zum Bundesdatenschutzgesetz, 8. Aufl. 2014, § 3 Rn. 225.
[31] ULD SH (Fn. 21), S. 17.
[32] Vgl. ULD SH (Fn. 21), S. 12 und 17 f.
[33] ULD SH (o. Fn. 21), S. 18.
[34] VG Schleswig DuD 2014, 120; umfassend zur Einwilligung ULD SH (Fn. 21), S. 20 ff., und Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 12 f.
[35] VG Schleswig DuD 2014, 120; ULD SH (Fn. 21), S. 17; vertiefend zu dieser Frage *Mergel u.a.* (Fn. 11), S. 77 f.
[36] ULD SH (Fn. 21), S. 22 f.
[37] ULD SH (Fn. 21), S. 23.
[38] VG Schleswig DuD 2014, 120.
[39] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Abl. EG 2002 Nr. L 201, S. 37 ff., i.d.F. der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates v. 25.11.2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, Abl. EG 2009 Nr. L 337, S. 11 ff.
[40] Vertiefend zur den verwendeten Cookies VG Schleswig DuD 2014, 120, und ULD SH (Fn. 21), S. 6 ff.
[41] ULD SH (o. Fn. 21), S. 24.

b) Die Position des VG Schleswig und des OVG Schleswig

Das VG Schleswig und das OVG Schleswig gehen demgegenüber davon aus, dass der Betreiber einer Fanpage nicht die für den Datenschutz verantwortliche Stelle sei.

Die Verantwortlichkeit für die Verarbeitung personenbezogener Daten ergebe sich aus § 12 Abs. 3 TMG i.V.m. § 3 Abs. 7 BDSG und Art. 2 lit. d) EU DSRL.[42] Die Stellung als Diensteanbieter würde „keine spezialgesetzliche Verantwortlichkeit abweichend von“ diesen Vorschriften begründen.[43] Art. 1 Abs. 5 lit. b) der E-Commerce-Richtlinie (ECRL)[44], die der Gesetzgeber mit dem TMG habe umsetzen wollen, stelle nämlich ausdrücklich klar, dass die Richtlinie auf „Fragen betreffend die Dienste der Informationsgesellschaft, die von den Richtlinien 95/46/EG und 97/66/EG erfasst w[ü]rden,“ keine Anwendung finde.[45] Auch Erwägungsgrund Nr. 14 zur ECRL diene der Klarstellung. Dort heiße es: „Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ausschließlich Gegenstand der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und der Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, beide Richtlinien sind uneingeschränkt auf die Dienste der Informationsgesellschaft anwendbar.“

Eine von diesen Vorgaben abweichende Bestimmung enthalte das TMG nicht.[46] Eine Verantwortlichkeit des Fanpagebetreibers nach § 3 Abs. 7 BDSG, der im Lichte des Art. 2 lit. d) EU DSRL auszulegen sei, lasse sich jedoch nicht begründen. Weder könne davon gesprochen werden, dass der Fanpagebetreiber selbst personenbezogene Daten erhebe, verarbeite oder nutze, noch davon, dass er eine Erhebung, Verarbeitung und Nutzung in seinem Auftrag vornehmen lasse. Vielmehr würde der Nutzer die Fanpage aufrufen und dabei unmittelbar seine Daten an Facebook übermitteln.[47] Der Nutzer der Fanpage komme daher „in keinerlei direkten Kontakt zu dem Nutzer der Fanpage und dessen personenbezogenen Daten.“

Auch liege kein Fall der Auftragsdatenverarbeitung nach § 11 Abs. 1 S. 1 BDSG vor, in deren Rahmen „der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich“ sei.[48] Facebook sei nämlich im Hinblick auf die Datenverarbeitung kein Auftragnehmer der Fanpagebetreiber.[49] Eine vertragliche Beziehung zwischen Facebook und den Fanpagebetreibern bestünde nur insoweit, als die Nutzung der Fanpage selbst geregelt würde. Die Erhebung, Verwendung und Verarbeitung personenbezogener Daten von Nutzern der Fanpage sei nicht Gegenstand dieser Vereinbarung. Auch die Sammlung von Daten, um das Tool „Insights“ anbieten zu können, erfolge nicht im Auftrag der Fanpagebetreiber. Es fehle an dem für einen Auftrag konstitutiven Merkmal eines vertraglichen Weisungsrechts. Die Fanpagebetreiber seien weder allein noch gemeinsam mit Facebook „Herr[en] der Daten“. An der Entscheidung über Zweck und Mittel der Datenverarbeitung würden die Fanpagebetreiber überhaupt nicht beteiligt. Die Entscheidung der Fanpagebetreiber erschöpfe sich vielmehr in der „Annahme eines für sie unabänderlichen Angebotes, die Fanpage einzurichten und mit Inhalt zu füllen oder nicht.“ Im Hinblick auf die abschließende Regelung im BDSG könne die Verantwortlichkeit auch nicht über Zurechnungsfiguren des Polizei- und Ordnungsrechts bzw. des Privatrechts begründet werden (Haftung des Nichtstörers, Zweckveranlasser etc.).[50]

c) Stellungnahme

Da nicht Facebook selbst, sondern eine deutsche Behörde Gegenstand der Betrachtung ist, sind sowohl das BDSG bzw. die entsprechenden landesgesetzlichen Vorschriften als auch das TMG anwendbar.[51]

aa) Zur Verantwortlichkeit nach den §§ 3 Abs. 7 und 11 BDSG

Die §§ 7 ff. TMG, in denen die Verantwortlichkeit der Diensteanbieter geregelt ist, zielen nun jedoch nur auf die strafrechtliche und die deliktsrechtliche Verantwortlichkeit der Diensteanbieter, nicht aber auf deren datenschutzrechtliche Verantwortlichkeit.[52] In den §§ 11 ff. TMG finden sich Regelungen über den Datenschutz und die unmittelbare Erhebung und Verwendung personenbezogener Daten durch den Diensteanbieter, aber keine, die die Verantwortung für Handlungen Dritter in Bezug nehmen. Den §§ 3 Abs. 7, 11 BDSG entsprechende Vorschriften über die Verantwortlichkeit fehlen im TMG.[53] Es gilt insofern § 12 Abs. 3 TMG, der auf das BDSG verweist.[54] Im Ergebnis ist damit nicht jeder Telemediendiensteanbieter für alle Datenverarbeitungsprozesse verantwortlich, die mit dem von ihm bereitgehaltenen Angebot in Verbindung stehen, sondern nur für solche, für

[42] VG Schleswig DuD 2014, 120 (121).
[43] VG Schleswig DuD 2014, 120 (121); vertiefend Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 8.
[44] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates v. 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, Abl. EG Nr. L 178, S. 1 ff.
[45] VG Schleswig DuD 2014, 120 (121).
[46] VG Schleswig DuD 2014, 120 (121).
[47] VG Schleswig DuD 2014, 120 (121); *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 178.
[48] Zitiert wird der Wortlaut des § 11 Abs. 1 S. 1 BDSG.
[49] VG Schleswig DuD 2014, 120 (122).
[50] VG Schleswig DuD 2014, 120 (122 f.).
[51] Vertiefend *Mergel u.a.* (Fn. 11), S. 76 f.
[52] Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 8.
[53] *Mergel u.a.* (Fn. 11), S. 77; *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 181.
[54] Umfassend Wissenschaftlicher Dienst des Landtages Schleswig-Holstein (Fn. 22), S. 13 ff.; *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 181.

die er die Verantwortung nach den allgemeinen Regelungen des BDSG trägt.[55]

Entscheidend für die Frage, ob die Fanpagebetreiber verantwortlich für den Datenschutz sind, ist damit § 3 Abs. 7 BDSG. Unter diese Norm fallen die Betreiber von Fanpages nicht, soweit es um die Verarbeitung von Nutzerdaten durch Facebook geht. Die Fanpagebetreiber verarbeiten diese Daten nicht selbst i.S.d. Norm, da dies eine irgendwie geartete Verfügungsgewalt über die Daten voraussetzen würde.[56] Verfügungsbefugt ist aber allein Facebook.[57] Tatsächlichen Einfluss auf die Art und den Umfang der Datenverarbeitung können die Fanpagebetreiber nicht nehmen.

Die Fanpagebetreiber lassen die Daten aber auch nicht im Auftrag von Facebook verarbeiten, da es an einem ausreichenden Vertragsverhältnis mangelt.[58] Der Auftraggeber muss im Rahmen des § 11 Abs. 1 S. 1 BDSG ein Weisungsrecht gegenüber dem Auftragnehmer haben und Art und Umfang der Datenverarbeitung bestimmen können, was im Verhältnis Fanpagebetreiber – Facebook nicht der Fall ist.[59] Vielmehr verfolgt Facebook eigene Geschäftszwecke (gezielte Schaltung personalisierter Werbung) und ist somit selbst verantwortliche Stelle.[60] Einschränken, ausschalten oder kontrollieren lässt sich die Datenverarbeitung durch das Tool „Insight" nicht.[61] Der Fanpagebetreiber ist daher unmittelbar nur für die „Inhalte und selbst initiierte Datenerhebungen" verantwortlich, nicht aber für die Einhaltung der Datenschutzbestimmungen durch Facebook.[62]

bb) Zur polizeilichen Zurechnungsfigur des Zweckveranlassers

Zu Recht lehnt die Rechtsprechung auch die Übertragung polizeirechtlicher Zurechnungsfiguren auf das Datenschutzrecht ab. Die Vorschrift des § 3 Abs. 7 BDSG ist als abschließende Regelung zu verstehen, was sich zum einen aus der Formulierung und zum anderen daraus ergibt, dass § 3 Abs. 7 BDSG der Umsetzung von Art. 2 lit. d) EU DSRL dient. Daraus, dass vorliegend eine Strafverfolgungsbehörde tätig wird, kann nichts anderes folgen.

Zwar entfaltet die EU DSRL keine unmittelbare Wirkung, sofern „die Tätigkeit des Staates im strafrechtlichen Bereich" geregelt wird (vgl. Art. 3 Abs. 2 EU DSRL), doch lässt sich zum einen schon bestreiten, dass das schlichte Betreiben einer Fanpage, auf der beispielsweise Öffnungszeiten der Polizeidienststelle und Veranstaltungshinweise veröffentlicht werden, einen hinreichenden Zusammenhang zur Strafverfolgung aufweist. Zum anderen muss der Umstand Beachtung finden, dass sich der Bundes- und die Landesgesetzgeber dafür entschieden haben, den Datenschutz im öffentlichen Bereich und im nicht-öffentlichen Bereich in einheitlichen Gesetzen zu regeln und die jeweiligen Normen im BDSG bzw. in den entsprechenden LDSG nur einheitlich ausgelegt werden können. Die EU DSRL entfaltet daher eine mittelbare Wirkung im Bereich der Strafverfolgung, sofern in Deutschland allgemeine Vorschriften, die der Umsetzung der EU DSRL dienen, auch auf Strafverfolgungsbehörden anzuwenden sind. Das ist bei § 3 Abs. 7 BDSG der Fall, da die StPO keine speziellere Regelung enthält.

Die EU DSRL dient nun ausdrücklich dem Zweck, ein einheitliches Schutzniveau in Europa zu sichern, um „Hemmnisse für eine Reihe von Wirtschaftstätigkeiten auf Gemeinschaftsebene" abzubauen.[63] Eine Angleichung der Rechtsvorschriften in den einzelnen Mitgliedstaaten ist daher nach Einschätzung des Europäischen Parlaments und des Rates der Europäischen Union unerlässlich, sofern die allgemeinen Grundsätze betroffen sind.[64] Einen Spielraum sollen die Mitgliedstaaten nach Erwägungsgrund Nr. 9 der EU DSRL nur besitzen, sofern die Durchführung der Richtlinie in Frage steht; ein Punkt, der an späterer Stelle noch relevant wird.

Der EuGH geht vor diesem Hintergrund davon aus, dass die Harmonisierung der nationalen Rechtsvorschriften „nicht auf eine Mindestharmonisierung beschränkt [sei], sondern zu einer grundsätzlich umfassenden Harmonisierung führ[e]."[65] Konkret zu Art. 7 EU DSRL heißt es, es dürften daher „weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten" eingeführt noch „zusätzliche Bedingungen" für die Datenverarbeitung aufgestellt werden. Sowohl engere als auch weitere Tatbestandsvoraussetzungen für die Verarbeitung personenbezogener Daten sollen unzulässig sein (in der Entscheidung die Einschränkung des Anwendungsbereichs von Art. 7 lit. f) EU DSRL auf in öffentlich zugänglichen Quellen enthaltene Daten). Die entsprechenden Gedanken sind auch auf die Regelungen zur Verantwortlichkeit zu übertragen und Art. 2 lit. d) EU DSRL ist insoweit als abschließende Regelung zu verstehen.[66] Dies gilt insbesondere auch deshalb, weil die datenschutzrechtliche Verantwortlichkeit Anknüpfungspunkt für Maßnahmen der Aufsichtsbehörde nach § 38 Abs. 5 BDSG oder sogar die Verhängung von Bußgeldern oder Strafen nach den §§ 43 f. BDSG sein kann.

Soweit also beispielsweise *Polenz* argumentiert, Facebook würde die konkreten Nutzungsdaten nicht erhalten, wenn der Fanpagebetreiber keine Seite eingerichtet hätte,

[55] *Mergel u.a.* (Fn. 11), S. 77; *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 181.
[56] Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 8; *Jotzo*, MMR 2009, 232 (233).
[57] Vgl. *Mergel u.a.* (Fn. 11), S. 78.
[58] Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 9; *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 182.
[59] Vertiefend Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 9; Wissenschaftlicher Dienst des Landtages Schleswig-Holstein (Fn. 22), S. 16 ff.; *Mergel u.a.* (Fn. 11), S. 78.
[60] Wissenschaftlicher Dienst des Landtages Schleswig-Holstein (Fn. 22), S. 16; *Mergel u.a.* (Fn. 11), S. 78.
[61] *Mergel u.a.* (Fn. 11), S. 78.
[62] *Mergel u.a.* (Fn. 11), S. 79.
[63] Vgl. Erwägungsgrund Nr. 7f der EU DSRL.
[64] Vgl. Erwägungsgrund Nr. 9 und Art. 5 der EU DSRL.
[65] EuGH NZA 2011, 1409 (1410).
[66] Für eine durch die EU DSRL angestrebte Vollharmonisierung auch KG BeckRS 2014, 03648; vertiefend *Brühann*, EuZW 2009, 639 (641 ff.).

ließe sich allenfalls eine Störerhaftung i.w.S. begründen, nicht aber eine der Tatbestandsvoraussetzungen des § 3 Abs. 7 BDSG/Art. 2 lit. d) EU DSRL.[67] Ebenfalls kann es nicht entscheidend sein, ob die Fanpagebetreiber die von Facebook zur Verfügung gestellten Informationen tatsächlich nutzen,[68] da ein Nutzen i.S.d. § 3 Abs. 7 BDSG/Art. 2 lit. d) EU DSRL nach ganz h.M. ein Mitentscheidungsrecht über den Zweck und die Mittel der Verarbeitung voraussetzt.[69] Unter dem Zweck der Datenverarbeitung wird gemeinhin das zu erwartende Ergebnis der Datenverarbeitung verstanden, das Grund der Datenverarbeitung ist („Warum“ der Datenverarbeitung).[70] Die Entscheidung über die Mittel der Datenverarbeitung umfasst die Entscheidung über die technischen und organisatorischen Fragen und damit Fragen nach der zu verwendenden Hard- und Software („Wie“ der Datenverarbeitung).[71] Es genügt daher nicht, dass eine Person Nutznießer der von dritter Seite veranlassten und gesteuerten Datenerhebung ist. Mögliche Zwecke, die die Fanpagebetreiber mit ihrer Fanpage verfolgen, bleiben ohne jeden Einfluss auf die Ausgestaltung des Tools „Insight“. „Den Fanpage- oder Webseiten-Betreibern ist es nicht möglich, auf die Reichweitenanalyse zu verzichten, geschweige denn Facebook im Einzelnen vorzuschreiben, wie die Datenverarbeitungsvorgänge im Detail abzuwickeln sind.“[72] Hierauf käme es aber an! Allein die Entscheidung über die Einrichtung einer Fanpage, mit der im Falle des Aufrufs zwingend von Facebook gesteuerte Datenverarbeitungsprozesse einhergehen, ist nicht ausreichend, um eine datenschutzrechtliche Verantwortlichkeit zu begründen.[73] Der geleistete Beitrag zur Datenverarbeitung ist ohne Einfluss auf Art, Zweck und Umfang derselben.[74] Damit sind Fanpagebetreiber nicht unmittelbar dafür verantwortlich, dass die Vorschriften der §§ 13, 15 TMG bei Aufruf ihrer Seite eingehalten werden. Mangels diesbezüglicher Verpflichtung ist die Einrichtung einer Fanpage durch Polizeibehörden auch nicht aus diesem Grund rechtswidrig.

2. Die mittelbare Verantwortlichkeit der Polizeibehörden für Datenschutzverstöße

Prüft man die datenschutzrechtliche Zulässigkeit des Betreibens einer Fanpage durch Behörden, darf bei der Feststellung, dass diese nicht unmittelbar für Datenschutzverstöße durch Facebook verantwortlich sind, jedoch nicht stehengeblieben werden. Der Gesetzgeber darf es nicht in der Hand haben, die Reichweite des Grundrechtsschutzes einfachgesetzlich, hier durch die Verantwortlichkeitszuweisung in TMG und BDSG, zu bestimmen. Für die öffentliche Verwaltung gelten daher „andere Maßstäbe für die Nutzung sozialer Medien […] als bei Privatpersonen.“[75]

Zunächst haben Behörden die anerkannten Grundsätze zur Nutzung des Internets für Verwaltungszwecke zu beachten (Barrierefreiheit, Impressumspflicht u.a.) und müssen ihr Verhalten im Internet am deutschen Recht ausrichten.[76] Die Fanpage ist insoweit als „ausgelagerte Behördenhomepage“ zu betrachten.[77]

Darüber hinaus ist die öffentliche Verwaltung aber auch gemäß Art. 20 Abs. 3 GG in besonderem Maße an Recht und Gesetz gebunden und zum Schutz beispielsweise der Persönlichkeitsrechte von Nutzern verpflichtet.[78]

Aus dieser strengen Rechtsbindung und dem staatlichen Schutzauftrag wird nun teilweise abgeleitet, dass die öffentliche Verwaltung ohne Ausnahme keinen Dienst in Anspruch nehmen dürfe, der rechtswidrig – dies wird in der folgenden Prüfung unterstellt[79] – Daten verarbeite.[80]

Diese Schwarz-Weiß-Betrachtung verschiedener Datenschutzbehörden wird in der Literatur überwiegend kritisiert.[81] Sie soll „ausgehend von allgemeinen Rechtsgrundsätzen“ einer Abwägung der widerstreitenden Interessen weichen.[82] Nur so ließen sich sachgerechte Ergebnisse erzielen, „die sowohl rechtsstaatlichen Grundsätzen genüg[t]en als auch eine Überdehnung der Haftung der öffentlichen Stellen für

[67] Vgl. *Polenz*, VuR 2012, 207 (210).
[68] In diesem Sinne aber *Polenz*, VuR 2012, 207 (210).
[69] Wissenschaftlicher Dienst des Landtages Schleswig-Holstein (Fn. 22), S. 16 f.
[70] OVG Schleswig, Urt. v. 4.9.2014 – 4 LB 20/13, Rn. 78 (juris).
[71] OVG Schleswig, Urt. v. 4.9.2014 – 4 LB 20/13, Rn. 79 (juris); *Polenz*, VuR 2012, 207 (210).
[72] So Wissenschaftlicher Dienst des Landtages Schleswig-Holstein (Fn. 22), S. 17.
[73] Wissenschaftlicher Dienst des Landtages Schleswig-Holstein (Fn. 22), S. 18.
[74] Wissenschaftlicher Dienst des Landtages Schleswig-Holstein (Fn. 22), S. 18.
[75] So *Mergel u.a.* (Fn. 11), S. 45; entsprechend *Schulz*, in: Schliesky/Schulz (Fn. 14), S. 122.
[76] Vertiefend *Mergel u.a.* (Fn. 11), S. 67 ff. und 75 ff., sowie Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 14 f.
[77] So die Terminologie von *Mergel u.a.* (Fn. 11), S. 67.
[78] *Mergel u.a.* (Fn. 11), S.75 und 82.
[79] Eine dezidierte Untersuchung aller möglichen Datenschutzverstöße würde den Rahmen dieses Beitrags sprengen. Es muss daher auf weitergehende Untersuchungen verwiesen werden: Umfassend zur Rechtswidrigkeit bzw. Rechtmäßigkeit der Datenerhebung durch Facebook beispielsweise *Weichert*, in: Möllers/van Ooyen (Hrsg.), Jahrbuch Öffentliche Sicherheit, 2012, S. 379 (380 f.) m.w.N., und *Erd*, NVwZ 2011, 19 ff.
[80] Vgl. ULD SH, Verantwortlichkeit für Facebook-Fanpages, zugleich eine parteiische Besprechung von Schulz/Schliesky (Hrsg.), Transparenz, Partizipation, Kollaboration, Web 2.0 für die öffentliche Verwaltung, 2012, online abzurufen unter: https://www.datenschutzzentrum.de/facebook/20120222-web20-in-verwaltung.html (9.3.2015); bayerischer Landesdatenschutzbeauftragter, Soziale Netzwerke, Fanpages bayerischer öffentlicher Stellen in sozialen Netzwerken zum Zwecke der Öffentlichkeitsarbeit, 2013, S. 11 f., online abzurufen unter: https://www.datenschutz-bayern.de/technik/orient/oh_fanpages.pdf (9.3.2015).
[81] Vgl. *Mergel u.a.* (Fn. 11), S. 82; *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 187 ff.
[82] So *Mergel u.a.* (Fn. 11), S. 82.

Drittinhalte und -aktivitäten verhinder[te]n."[83] Es bedürfe einer Abwägung von Risiko und Nutzen. Eine rechtliche Begründung dieses Ergebnisses fehlt in den meisten Fällen.

Häufig scheint bereits der Grundrechtseingriff selbst verneint zu werden. Dies lässt sich im Falle der rechtswidrigen Datenverarbeitung ohne Weiteres begründen, wenn entgegen der ganz herrschenden Meinung auf den sogenannten „klassischen Eingriffsbegriff" zurückgegriffen wird, der Finalität, Unmittelbarkeit, Rechtsförmigkeit und Imperativität verlangt.[84] Ein Rückgriff auf den klassischen Eingriffsbegriff wird für die allgemeine Handlungsfreiheit gelegentlich befürwortet, nicht jedoch für Eingriffe in das Allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung.[85]

Näher dürfte es daher liegen, sich am sogenannten modernen Eingriffsbegriff zu orientieren, der jede durch staatliches Handeln hervorgerufene Schutzbereichsbeeinträchtigung erfasst, solange sie eine gewisse Intensität erreicht und dem Staat zugerechnet werden kann, insbesondere also vorhersehbar ist.[86] Hiernach muss nach verbreiteter Auffassung wohl ein mittelbar-faktischer Grundrechtseingriff durch das Verwenden einer Fanpage seitens der Behörden bejaht werden,[87] ohne dass vorliegend auf die im Verfassungsrecht stark umstrittene Frage nach den exakten Kriterien eines solchen Eingriffs eingegangen werden soll.[88] Solange der Eingriff gerechtfertigt wäre, bedarf es nämlich keiner eigenen Positionierung.

a) Das Vorliegen einer ausreichenden Ermächtigungsgrundlage

Fraglich ist, ob ein solcher mittelbar-faktischer Grundrechtseingriff gerechtfertigt wäre. Die Vorschriften über die Öffentlichkeitsfahndung kommen dabei nicht als Ermächtigungsgrundlage zum Betreiben einer Fanpage in Betracht, da über den Einzelfall hinaus Informationen vorrätig gehalten werden müssen und die Fanpage nur dann sinnvoll für einen Fahndungsaufruf genutzt werden kann, wenn sie über eine hohe Zahl gut vernetzter „Fans" verfügt, die die Seite „gelikt" haben und den sogenannten „Newsfeed" verfolgen. Mit dem Sinn und Zweck der Facebookfahndung wäre es daher unvereinbar, nur im Zusammenhang mit einem bestimmten Fahndungsaufruf eine Fanpage anzulegen.[89] Das dauerhafte Betreiben einer polizeilichen Informationsseite einschließlich des Veröffentlichens einer Vielzahl von Informationen, die dazu dienen, die Seite für Nutzer attraktiv zu machen, kann daher nicht auf die §§131 ff. StPO gestützt werden.[90]

Zu beachten ist jedoch, dass das BVerfG schon wiederholt betont hat, dass im Zusammenhang mit mittelbar-faktischen Grundrechtseingriffen, die aus staatlicher Informationstätigkeit erwachsen, auch allgemeine Zuständigkeitsnormen als Ermächtigungsgrundlage genügen können.[91] Der Vorrang des Gesetzes ist dann allerdings besonders zu beachten. Das Ergebnis entspricht daher in etwa dem derjenigen, die einen Grundrechtseingriff von vornherein verneinen.

Schon das BVerwG hat in diesem Zusammenhang ausgeführt, dass es bei der Öffentlichkeitsarbeit um eine Staatsaufgabe gehe, die „ihrer Art nach nur tatsächlich, nicht rechtsförmlich erfüllbar [sei] und bei deren Wahrnehmung der Staat dem Einzelnen kein – notfalls zwangsweise durchzusetzendes – Handeln verbindlich auf[gebe] oder verbiet[e]".[92] In solchen Fällen stehe das Rechtsstaatsprinzip einem Schluss von der Aufgabe auf die Zulässigkeit von Individualrechtsbeschränkungen, die mit der Aufgabenwahrnehmung zwangsläufig oder typischerweise verbunden seien, nicht von vornherein entgegen. Dies folge „aus dem jeder Staatsaufgabe

[83] *Mergel u.a.* (Fn. 11), S. 82.
[84] Vgl. BVerfG NJW 2002, 2626 (2628).
[85] Vgl. *Lang*, in: Epping/Hillgruber (Hrsg.), Beck'scher Online-Kommentar, Grundgesetz, Stand: 1.12.2014, Art. 2 Rn. 23, 51.
[86] Vgl. BVerfGE 66, 39 (60), und *Oermann/Staben*, Der Staat 2013, 630 (637). Die Einzelheiten sind freilich umstritten, vertiefend *Isensee*, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. 5, 3. Aufl. 2007, § 111 Rn. 65 ff.; *Sachs*, in: Sachs (Hrsg.), Grundgesetz, Kommentar, 6. Aufl. 2011, Vor Art. 1 Rn. 83 ff.; *Bleckmann/Eckhoff*, DVBl. 1988, 373 (374 f.); *Cremer*, Freiheitsgrundrechte, 2003, S. 150 f. Nach *Sachs*, a.a.O., ist lediglich das Kausalitätserfordernis als Voraussetzung der Zurechnung allgemein anerkannt.
[87] Für eine Zurechnung sprechen insbesondere die Parallele zum Gnadenschussfall und das sichere Wissen der Fanpagebetreiber, dass Daten der Nutzer gespeichert werden.
[88] Vgl. zum Streit Fn. 86 sowie *Lenski*, ZJS 2008, 13 (14 ff.). Für einen sehr weiten Eingriffsbegriff sprechen sich z.B. *Oermann/Staben*, Der Staat 2013, 630 (640 ff.), aus; deutlich enger und einen Eingriff ohne Finalität ablehnend z.B. *Ossenbühl*, NVwZ 2011, 1357 (1359). *Bleckmann/Eckhoff*, DVBl. 1988, 373 (380, in Bezug auf Dreieckskonstellationen mit Privaten auch 377 f.), stellen die Zurechnung in den Vordergrund. Umfassend zu möglichen Zurechnungskriterien *Petersen*, ZÖR 2012, 459 (467 ff.).
[89] Vgl. hierzu auch *Ihwas* (Fn. 4), S. 271.
[90] Abhängig von der jeweils handelnden Behörde kommen neben der allgemeinen Aufgabenzuweisungsnorm teilweise auch Generalklauseln in Betracht (z.B. § 3 Abs. 1 EGovG oder § 11 Abs. 3 IFG), deren Regelungsgehalt aber noch nicht abschließend geklärt ist und die im Vergleich zur allgemeinen Aufgabenzuweisungsnorm als Ermächtigungsgrundlage auch nicht zu einem Mehr an Bestimmtheit beitragen (vgl. zum IFG beispielhaft *Hoffmann/Klessmann*, in: Schliesky/Schulz [Fn. 14], S. 50 ff.; kritisch zu § 11 Abs. 3 IFG als Ermächtigungsgrundlage zur eigenständigen Informationsveröffentlichung ohne vorangegangenen Antrag BMI, Referat O2, Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften, 2013, S. 16).
[91] Vgl. konkret zum Einrichten von Fanpages auch *Schliesky*, in: Schliesky/Schulz (Fn. 14), S. 8, sowie allgemein zur Nichtgeltung des Gesetzesvorbehalts bei mittelbar-faktischen Eingriffen *Isensee* (Fn. 86), § 111 Rn. 68.
[92] BVerwG NJW 1991, 1770 (1771).

innewohnenden Postulat einer wirksamen Aufgabenwahrnehmung und […] aus der Vielgestaltigkeit der Eingriffslagen und -wirkungen“ solch „informalen Staatshandelns“. Je vielgestaltiger nämlich die zu regelnden Sachverhalte seien, desto geringer seien auch die Anforderungen, die an die Bestimmtheit der gesetzlichen Eingriffsermächtigung gestellt werden könnten. Ausdrücklich bezieht das BVerwG seine Argumentation dabei auch auf die gesetzlichen Aufgaben der Polizeibehörden.[93]

Entsprechend positioniert sich das BVerfG in der sogenannten Osho-Entscheidung.[94] Zunächst stellt das BVerfG fest, dass die Anforderungen an eine gesetzliche Ermächtigung u.a. dadurch bestimmt würden, ob diese dazu beitragen könne, „die im Rechtsstaats- und im Demokratieprinzip wurzelnden Anliegen des Gesetzesvorbehalts zu erfüllen“. Ob und inwieweit der Sachbereich staatlicher Normierung zugänglich sei, lasse sich nur mit Blick „auf den jeweiligen Sachbereich und auf die Eigenart des betroffenen Regelungsgegenstandes beurteilen“. Weiter heißt es, „die Aufgabe staatlichen Handelns k[ö]nn[e] der Gesetzgeber ohne weiteres normativ festlegen. Ebenso k[ö]nn[e] er die Voraussetzungen gezielter und unmittelbarer Eingriffe normieren. Für die faktisch-mittelbaren Wirkungen staatlichen Handelns g[e]lt[e] dies regelmäßig nicht. Hier lieg[e] die Beeinträchtigung nicht in einem staatlicherseits geforderten Verhalten des Normadressaten, sondern in den Wirkungen staatlichen Handelns für einen Dritten, die insbesondere vom Verhalten anderer Personen abh[i]ngen. Die Beeinträchtigung entsteh[e] aus einem komplexen Geschehensablauf, bei dem Folgen grundrechtserheblich w[ü]rden, die indirekt mit dem eingesetzten Mittel oder dem verwirklichten Zweck zusammenh[i]ngen. Derartige faktisch-mittelbare Wirkungen entz[ög]en sich typischerweise einer Normierung. […] Ob und welche nachteiligen Konsequenzen diese Tätigkeit im Einzelfall für den Grundrechtsträger ha[be], häng[e] im Allgemeinen von einer Vielzahl unterschiedlichster Faktoren und deren Zusammenwirken ab.[95] Häufig [sei] hierfür das Verhalten Dritter ausschlaggebend, das, weil es auf deren freier Entscheidung beruhe, regelmäßig nicht abschätzbar [sei] und hinsichtlich seiner Folgen nur schwer kalkuliert werden k[ö]nn[e]. Weder die rechtsstaatliche, grundrechtsschützende und den Rechtsschutz gewährleistende noch die demokratische Funktion des Gesetzesvorbehalts forder[e] unter diesen Umständen eine über die Aufgabenzuweisung hinausgehende gesetzliche Ermächtigung. Gegenstand und Modalitäten staatlichen Informationshandelns [seien] so vielgestaltig, dass sie angesichts der eingeschränkten Erkenntnis- und Handlungsmöglichkeiten des Gesetzgebers allenfalls in allgemein gehaltenen Formeln und Generalklauseln gefasst werden könnten. Ein Gewinn an Messbarkeit und Berechenbarkeit staatlichen Handelns [sei] für den Bürger auf diesem Wege regelmäßig nicht zu erreichen oder nur in einer Weise, die den Erfordernissen staatlicher Informationstätigkeit nicht gerecht [würde. …] Angesichts der zwangsläufig weiten und unbestimmten Fassung einer einfachgesetzlichen Ermächtigung zum Informationshandeln wäre mit einer solchen Ermächtigung eine Entscheidung zur Sache in Wirklichkeit nicht verbunden.“ Die vom BVerwG und vom BVerfG angestellten Erwägungen lassen sich nun ohne Weiteres auf die hier interessierende Fallkonstellation übertragen. Will man folglich einen mittelbar-faktischen Grundrechtseingriff durch das schlichte Anlegen einer Fanpage bejahen, genügt die allgemeine Aufgabenzuweisung in § 163 StPO, der Ermittlungsgeneralklausel, als Ermächtigungsgrundlage und das Einrichten einer Fanpage fällt auch in die festgelegte Zuständigkeit der Polizeibehörden.

b) Verhältnismäßigkeit des Einrichtens einer Fanpage

Im Rahmen der Verhältnismäßigkeitsprüfung hat sodann eine umfassende Güterabwägung stattzufinden.[96] Dabei ist zu beachten, dass der mittelbar-faktisch veranlasste Eingriff[97] in das Recht auf informationelle Selbstbestimmung von geringem oder allenfalls mittlerem Gewicht ist, da die Daten, die beim Besuch der Behördenfanpage gespeichert werden, weder dem Kernbereich privater Lebensgestaltung noch einem engen Bereich privater Lebensgestaltung zuzurechnen sind.[98] Zudem soll bereits bei der Beurteilung des Eingriffsgewichts von Bedeutung sein, ob der Grundrechtsberechtigte Kenntnis über die Erhebung und weitere Verarbeitung seiner Daten hat, da er im Falle der Kenntnis sein künftiges Verhalten an dieser ausrichten könne.[99] Dass Facebook die Nutzerdaten in weitem Umfang speichert und zu Werbezwecken nutzt, ist allgemein bekannt.

Des Weiteren sollen das Bestehen einer Pflicht zur Datenpreisgabe oder ein besonderer Motivationsdruck für einen schweren Eingriff sprechen, die freiwillige Preisgabe dagegen.[100] Vorliegend ist von einer freiwilligen Datenpreisgabe auszugehen. Von einem heimlich oder zwangsweise erstellten Persönlichkeitsprofil kann daher nicht gesprochen werden, was ebenfalls für einen Eingriff von geringem Gewicht spricht.

Nach dem VerfGH Rheinland-Pfalz steht es der Einordnung eines Eingriffs als Maßnahme von nur geringem Ge-

[93] Vgl. BVerwG NJW 1991, 1770 (1771).
[94] BVerfG NJW 2002, 2626.
[95] BVerfG NJW 2002, 2626 (2630).

[96] Umfassend zu dieser Abwägung *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 187 ff.
[97] Zu beachten ist überdies, dass die Grundrechte in Privatrechtsverhältnissen nur eingeschränkt wirken, vgl. dazu *Mergel u.a.* (Fn. 11), S. 82.
[98] Vgl. auch VerfGH Rheinland-Pfalz NJW 2014, 1434 (1437 und 1440), zum Grundrechtseingriff durch den Ankauf von Steuerdaten-CDs. Dabei wird nicht verkannt, dass es für die Bestimmung der Eingriffsintensität nicht allein auf die Art des Datums ankommt, sondern auch auf die Nutzbarkeit und die Verwendungsmöglichkeiten, sodass es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum mehr“ gibt, vgl. BVerfGE 65, 1 (45).
[99] Vgl. *Polenz*, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 32. Lfg., Stand: August 2013, Teil 13 II Rn. 16.
[100] Vgl. *Polenz* (Fn. 99), Teil 13 II Rn. 16, sowie Rn. 17 zu weiteren Kriterien wie dem Grad der Missbrauchsgefahr oder der Dauer der Speicherung.

wicht auch nicht entgegen, dass „eine große Zahl von Personen betroffen ist“, weil „die Schwere des Eingriffs in das jeweilig betroffene Grundrecht“ des Einzelnen dieselbe bliebe.[101]

Zumindest muss aber im Rahmen der Rechtfertigung berücksichtigt werden, dass Facebook jedenfalls allgemein und seit dem 1.1.2015 umfassender als zuvor[102] über die Datenverarbeitung informiert und die Nutzer eine, wenn auch datenschutzrechtlich möglicherweise unwirksame, Einwilligung zur Datenverarbeitung durch Facebook erteilen.[103] Darüber hinaus sind die hohe Zahl an Interaktionen und die schnelle Verbreitung von Informationen zu berücksichtigen, die sowohl auf die Größe des Netzwerks als auch auf das typische Nutzerverhalten zurückzuführen sind.[104] Im Durchschnitt loggt sich jeder Facebooknutzer mindestens einmal im Monat bei Facebook ein, die Hälfte der Nutzer sogar täglich.[105] Mit einer Fanpage können daher mit geringem Zeit- und Kostenaufwand weit mehr Menschen erreicht werden als über eine Behördenhomepage, deren Inhalte aktiv aufgerufen werden müssen und sich auch nicht über standardisierte Funktionen weiterverbreiten lassen.[106] Zudem lassen sich bestimmte Personenkreise (insbesondere die sogenannten „Digital Natives“) kaum noch über klassische Medien wie die Tageszeitung erreichen.[107] Es müssen jedoch alle Bürger gleichermaßen an den zur Verfügung gestellten staatlichen Informationen partizipieren, da der staatliche Informationsauftrag Verfassungsrang genießt.[108] Facebook ist daher zur Informationsverbreitung im Vergleich zu sonstigen Medien überdurchschnittlich gut geeignet und für die behördliche Aufgabenerfüllung von großem Nutzen. Die verbleibenden Risiken können durch Hinweise zum Datenschutz auf der eigenen Fanpage weiter reduziert werden.

Sofern eine Abwägung zugelassen wird, entspricht es daher der ganz herrschenden Meinung, dass diese zugunsten der Fanpagebetreiber ausgeht.[109] Dieser Einschätzung ist nach den gängigen Bewertungskriterien zuzustimmen.

Auch die staatliche Schutzpflicht erfordert nur eine Beachtung des Untermaßverbotes, sodass der Staat in zumutbaren Grenzen nicht zum Eingreifen verpflichtet ist. Wären diese Grenzen überschritten, müsste mit Hilfe der datenschutzaufsichtsrechtlichen Instrumente (u.a. Maßnahmen zur Beseitigung datenschutzrechtlicher Verstöße nach § 38 Abs. 5 BDSG oder Bußgeldbescheide nach den §§ 16 TMG, 43 BDSG) reagiert werden.[110]

Ob also tatsächlich deutsches Datenschutzrecht anwendbar ist,[111] nach diesem Datenschutzverstöße vorliegen[112] und die E-Privacy-Richtlinie nach Ablauf der Umsetzungsfrist in Deutschland unmittelbare Geltung beansprucht,[113] muss daher nicht abschließend entschieden werden. Selbst die vom ULD SH in Übereinstimmung mit dem Schrifttum angenommenen Rechtsverstöße unterstellt,[114] dürfen Fanpages im Grundsatz von Polizeibehörden betrieben werden.[115] Entsprechend den Fällen des Agent Provocateurs oder im Falle des Ankaufs einer Steuerdaten-CD ist das Verhalten des Staates

[101] VerfGH Rheinland-Pfalz NJW 2014, 1434 (1437); vgl. aber auch *Oermann/Staben*, Der Staat 2013, 630 (646 ff.).

[102] Vgl. die neuen Datenrichtlinie sowie die neue Cookies-Richtlinie von Facebook, online abzurufen unter: https://www.facebook.com/about/privacy/update (9.3.2015) und https://www.facebook.com/help/cookies/update (9.3.1015). Auch ein Löschungsanspruch bezogen auf das gesamte Konto wurde nun aufgenommen.

[103] *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 189; umfassend zur Einwilligung ULD SH (Fn. 21), S. 20 ff.; Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 12 f.

[104] *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 188.

[105] *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 188, m.w.N.

[106] Vertiefend *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 188 f.

[107] Vgl. zum Bedeutungsverlust klassischer Medien für die Fahndung *Irlbauer*, Kriminalistik 2012, 764 (764 und 766).

[108] Vgl. BVerfGE 105, 252 (268). Aus dieser Erkenntnis folgt auch, dass Inhalte nicht exklusiv über soziale Medien zur Verfügung gestellt werden dürfen, vgl. *Schulz*, in: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, 2015, Kap. 10 Rn. 55.

[109] In diesem Sinne *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 188.

[110] Vgl. OVG Schleswig, Urt. v. 4.9.2014 – 4 LB 20/13, Rn. 73 (juris).

[111] Umfassend zum anwendbaren Recht im Zusammenhang mit grenzüberschreitendem Datenverkehr bei der Nutzung von Onlinediensten *Jotzo*, MMR 2009, 232. Vgl. zur Anwendbarkeit des deutschen Datenschutzrechts auf Facebook ULD SH, Replik v. 21.7.2014 – Az.: LD4-61.45/11.001, S. 1 ff.; *id.* (Fn. 21), S. 19; Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 11; *Polenz*, VuR 2012, 207 (208), und KG BeckRS 2014, 03648, sowie zum Begriff der Niederlassung EuGH NJW 2014, 2257 (2259 ff.); für die Anwendbarkeit irischen Datenschutzrechts demgegenüber VG Schleswig BeckRS 2013, 46930; OVG Schleswig NJW 2013, 1977 (1979).

[112] Kritisch *Härting*, CR 2011, 585 ff.; vgl. auch Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 5 ff. und 12 ff.; Bericht des Irischen Datenschutzbeauftragen, zitiert nach ZD-Aktuell 2012, 02708 und 02724.

[113] Vgl. zum Streit um die unmittelbare Anwendung https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (9.3.2015), S. 20 f.

[114] So heißt es bei *Hoffmann/Schulz/Brackmann* (Fn. 14), S. 187, es sei problematisch, dass personenbezogene Daten durch Facebook „am Maßstab des deutschen Datenschutzrechts gemessen in unzulässiger Weise“ genutzt würden.

[115] Gestützt wird dieses Ergebnis nicht zuletzt durch eine Erwägung des Wissenschaftlichen Dienstes des Landtages Schleswig-Holstein. Sollte nämlich die zwingend mit der Einrichtung einer Homepage zusammenhängende Datenverarbeitung zur datenschutzrechtlichen Verantwortung führen, gälte dies auch für eine „klassische Homepage“ bei deren Besuch die IP-Adresse durch den jeweiligen Accessprovider verarbeitet würde (so Wissenschaftlicher Dienst des Landtages Schleswig-Holstein [Fn. 22], S. 18 f.).

rechtmäßig, obwohl es in einem engen Zusammenhang zu einem ggf. rechtswidrigen Verhalten eines Dritten steht.

II. Die Voraussetzungen und Grenzen der Nutzung einer Fanpage für die Öffentlichkeitsfahndung zum Zwecke der Strafverfolgung

Im Anschluss an die eben beantwortete Frage nach der grundsätzlichen Zulässigkeit des Betreibens einer Fanpage ist nun der Frage nachzugehen, ob und unter welchen Voraussetzungen die Fanpage für Fahndungen zum Zwecke der Strafverfolgung genutzt werden darf. Die AGB von Facebook schließen die Nutzung des Netzwerkes zu Fahndungszwecken jedenfalls nicht aus.[116]

1. Die Fahndungsvorschriften im Überblick

Die Fahndung zum Zwecke der Strafverfolgung ist in den §§ 131 ff. StPO geregelt. Sofern sich der Fahndungsaufruf dabei an Behörden richtet, spricht das Gesetz von einer Ausschreibung, im Übrigen von einer Öffentlichkeitsfahndung.[117] § 131 StPO ermöglicht insofern die Fahndung nach einem Beschuldigten zum Zwecke der Festnahme. § 131a StPO gestattet die Fahndung nach Beschuldigten oder Zeugen zum Zwecke der Aufenthaltsermittlung sowie die Fahndung nach Beschuldigten zum Zwecke der Sicherstellung seines Führerscheins und zur Durchführung einiger weiterer prozessualer Maßnahmen. § 131b StPO regelt schließlich die Veröffentlichung von Abbildungen eines Beschuldigten oder Zeugen, um deren Identität zu klären oder die Aufklärung einer Straftat zu erleichtern (sogenannte Identitätsfeststellungs- oder Aufklärungsfahndung)[118] und die Zuständigkeiten für entsprechende Anordnungen ergeben sich aus den Normen selbst oder aus § 131c StPO.

Hinsichtlich der Tatbestandsvoraussetzungen wird jeweils strikt zwischen der Ausschreibung in den Fahndungshilfsmitteln der Strafverfolgungsbehörden und der Öffentlichkeitsfahndung differenziert. Einheitliche Voraussetzungen der Öffentlichkeitsfahndung sind, dass (dringender)[119] Tatverdacht bezüglich einer Straftat von erheblicher Bedeutung vorliegt und dass andere Formen der Aufenthaltsermittlung bzw. der Sachaufklärung erheblich weniger Erfolg versprechen oder wesentlich erschwert wären. Die Subsidiaritätsklausel verlangt daher, dass mildere Maßnahmen nicht erst bei gleicher Eignung zu ergreifen sind, „sondern auch wenn sie weniger, jedoch nicht erheblich weniger, Erfolg versprechen oder die Aufenthaltsermittlung etwas, aber nicht erheblich erschweren.“[120]

Bei der Fahndung nach einem Zeugen i.S.d. § 131a Abs. 4 S. 3 StPO darf zudem kein überwiegendes schutzwürdiges Interesse des Zeugen entgegenstehen und die Subsidiaritätsklausel wird bei der Veröffentlichung von Abbildungen eines Zeugen gemäß der §§ 131a Abs. 4 S. 4, 131b Abs. 2 StPO dahingehend eingeengt, dass die Erreichung des Fahndungsziels ohne die Öffentlichkeitsfahndung aussichtslos erscheinen oder wesentlich erschwert sein muss.

Bezüglich des Inhalts der Ausschreibung regelt § 131 Abs. 4 StPO, auf den die §§ 131a Abs. 4 S. 1 und 131b Abs. 3 StPO verweisen, dass der Beschuldigte möglichst genau zu bezeichnen ist und auch eine Abbildung beigefügt werden darf, wenn dies zur Zielerreichung erforderlich ist. Zudem können die Tat, derer er verdächtig ist, Ort und Zeit ihrer Begehung sowie Umstände, die für die Ergreifung von Bedeutung sein können, angegeben werden. Bei der Fahndung nach einem Zeugen ist gemäß der §§ 131a Abs. 4 S. 2 und 131b Abs. 2 S. 2 StPO erkennbar zu machen, dass die gesuchte Person nicht Beschuldigter ist.

Eine Straftat von erheblicher Bedeutung muss mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, wobei das Gewicht der Straftat im Einzelfall nach dem jeweiligen Deliktstypus, der Art der Ausführung und der Schuldschwere zu bestimmen ist.[121] Auch generalpräventive Erwägungen können zur Bestimmung der Bedeutung einer Straftat herangezogen werden.[122] Ob die Subsidiaritätsklausel eingreift, ist von den konkreten Umständen des Einzelfalles abhängig. Zudem ist eine allgemeine Verhältnismäßigkeitsprüfung durchzuführen, die sich an den Vorgaben der Nr. 1.2 der Anlage B zur RiStBV zu orientieren hat.

Darüber hinaus bestimmt Nr. 3.2 der Anlage B zur RiStBV in Abs. 1 S. 1, dass die staatlichen Fahndungsaufrufe im Internet grundsätzlich auf speziellen Seiten gebündelt werden sollen, „um die Aufmerksamkeit der Internetbenutzer für die Öffentlichkeitsfahndung zu erlangen“. Weiter heißt es in Abs. 1 S. 2: „Private Internetanbieter sollen grundsätzlich nicht eingeschaltet werden.“ Die Norm verfolgt damit das Ziel, „die Vermeidung einer unkontrollierten Weitergabe sowie die Sicherstellung einer abschließenden Löschung von personenbezogenen Daten“ zu gewährleisten.[123] Ausnahmen kommen nur bei auch im Einzelfall sehr schwerwiegenden Straftaten in Betracht. Eine entsprechende Einschränkung ergibt sich jedoch schon aus allgemeinen Verhältnismäßigkeitserwägungen.[124]

Schlussendlich bestimmt Nr. 3.2 der Anlage B zur RiStBV in Abs. 2 S. 1, dass „die Nutzung des Internets zu Fahndungszwecken unverzüglich“ eingestellt werden muss, wenn das Fahndungsziel erreicht worden ist oder die Fahndung aus sonstigen Gründen beendet wurde. Abs. 2 S. 2 enthält die Pflicht, das Vorliegen der Ausschreibungsvoraussetzungen regelmäßig zu überprüfen.

---

[116] Vertiefend *Ihwas* (Fn. 4), S. 270 ff.

[117] Vertiefend zu den Begriffen der Ausschreibung und der Öffentlichkeitsfahndung *Gerhold*, in: Kudlich (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 1, 2014, § 131 Rn. 4 u. 11.

[118] Vgl. BR-Drs. 961/96, S. 20; BT-Drs. 14/1484, S. 21.

[119] Bei § 131b StPO ist einfacher Tatverdacht ausreichend.

[120] So bereits *Gerhold* (Fn. 117), § 131 Rn. 15.

[121] Vertiefend *Gerhold* (Fn. 117), § 131 Rn. 14.

[122] *Gerhold* (Fn. 117), § 131 Rn. 14.

[123] So LT-Drs. RP 16/3387, S. 2.

[124] Vgl. zur Verhältnismäßigkeit der Fahndung in sozialen Netzwerken auch *Lohmeier u.a.* (Fn. 7), S. 23 ff.

2. Die zentralen Rechtsfragen

Vor dem Hintergrund der eben genannten Voraussetzungen stellen sich nun einige konkrete Rechtsfragen, von deren Beantwortung die Zulässigkeit der Facebookfahndung abhängig ist.

a) Die grundsätzliche Anwendbarkeit der Fahndungsvorschriften auf die Facebookfahndung

Zunächst sind Zweifel zu entkräften, dass das Verbreiten eines Fahndungsaufrufs in einem sozialen Netzwerk, das auf Interaktivität zielt, nicht mehr mit dem Wesen der Öffentlichkeitsfahndung vereinbar ist, das klassisch durch einseitige Öffentlichkeit gekennzeichnet war.[125] Rückmeldungen der Bürger konnten lange Zeit lediglich im Rahmen der Individualkommunikation erfolgen. Der Hinweisgeber wurde zwar als einer von vielen angesprochen, konnte jedoch nicht seinerseits durch beispielsweise ein Flugblatt auf den Fahndungsaufruf reagieren, sondern musste persönlich bei einer Polizeidienststelle vorstellig werden oder zumindest dort anrufen.

Es ließe sich also argumentieren, dass die unkontrollierte Gefahr, dass im Rahmen der Fahndung in sozialen Netzwerken Dritte den Fahndungsaufruf kommentieren, Namen von Verdächtigen veröffentlichen oder gar Verlinkungen vornehmen, die von der verantwortlichen Strafverfolgungsbehörde weder kontrolliert noch entfernt werden können, den Anwendungsbereich der Norm überdehne und die Öffentlichkeitsfahndung in sozialen Netzwerken daher einer noch spezielleren Ermächtigung bedürfe.

Tatsächlich unterscheidet sich die allgemeine Onlinefahndung insofern aber nicht von der Facebookfahndung und auch die Wortlautgrenze des Begriffs der Öffentlichkeitsfahndung wird nicht überschritten.

Unter dem Begriff der Öffentlichkeitsfahndung wird heute der Aufruf an einen größeren, nicht überschaubaren Personenkreis verstanden, die allgemeine oder gezielte Suche nach einer Person oder Sache zum Zwecke der Strafverfolgung durch sachdienliche Hinweise zu unterstützen. Auf das Verteilungsmedium soll es nicht mehr ankommen.

Vor dem Jahr 2000 sprach das Gesetz demgegenüber ausschließlich von der Verfolgung eines Beschuldigten mittels Steckbrief.[126] Dieser Begriff wurde bewusst aufgegeben, da er „die heutigen differenzierten Fahndungsmethoden nicht mehr adäquat kennzeichn[e].“[127]

Streitpunkte vor der Reform waren insbesondere die Fahndung über Fernsehsendungen und die Fahndung über das Internet.[128] Beide Fahndungsmethoden sollten durch die Neufassung des Abschnitts 9a ermöglicht werden.[129] Der Begriff der Öffentlichkeitsfahndung sollte neueren technischen Entwicklungen und Trends offenstehen. Hierfür spricht auch die erst im Vermittlungsausschuss gefundene Fassung des § 131c Abs. 2 StPO, nach der „in Fällen andauernder Veröffentlichung in elektronischen Medien“ im Ermittlungsnotstand getroffene Anordnungen der Staatsanwaltschaft und ihrer Ermittlungspersonen der richterlichen Bestätigung binnen Wochenfrist bedürfen.[130] Unter den Wortlaut des §§ 131 ff. StPO lässt sich die Facebookfahndung mithin subsumieren.

Zudem birgt die Fahndung in sozialen Netzwerken dieselben Risiken wie die Internetfahndung im Allgemeinen. Lediglich der Verbreitungsgrad wird beträchtlich erhöht.

Jede Internetseite kann in sozialen Netzwerken geteilt und kommentiert werden. Es lassen sich Personen mit der geteilten Seite verlinken und Namen von Beschuldigten veröffentlichen. Entsprechendes gilt für eine Verbreitung des Fahndungsaufrufs über Onlineportale, -magazine und -zeitungen.

Die Praxis belegt zudem, dass der Einfluss der Behörde auf das Geschehen im sozialen Netzwerk schwindet, wenn sie nicht selbst einen Link in das Netzwerk einstellt, sondern Dritte unmittelbar die jeweiligen Fahndungsseiten teilen. Diese Beobachtung fußt darauf, dass der Fanpagebetreiber im Rahmen der Nutzungsbedingungen entscheiden kann, ob der geteilte Link mit einem Foto versehen werden soll, ob die Möglichkeit eröffnet wird, die Inhalte zu kommentieren, und ob Personen auf dem Foto verlinkt werden dürfen. Stellt also die Polizeibehörde den Ursprungslink in das soziale Netzwerk ein, entscheidet sie selbst über die konkreten Voraussetzungen, unter denen dieser Link geteilt werden kann. Verzichtet die Polizei demgegenüber auf das Einstellen des Links in das soziale Netzwerk, finden sich regelmäßig private Dritte, die diese Verteilungsfunktion übernehmen, ohne die erforderlichen Netzwerkeinstellungen zum Datenschutz vorzunehmen.[131] Die Verteilung von Fahndungsaufrufen durch Dritte lässt sich also faktisch in keinem Fall der Onlinefahndung verhindern und die Anzahl der Fans privater Fanpagebetreiber steht der Anzahl der Fans staatlicher Fahndungsseiten in nichts nach. So hat die Seite „PolizeiNews Fahndungen“ über 35.000 Fans und teilt Fahndungsmeldungen ohne dabei die erforderlichen Netzwerkeinstellungen zum Schutz personenbezogener Daten vorzunehmen. Entsprechend werden Fahndungsmeldungen auch außerhalb von sozialen Netzwerken von Onlinemedienanbietern kopiert und veröffentlicht, die eine Kommentarfunktion anbieten.[132] Der Unterschied zwischen der allgemeinen Onlinefahndung und der Fahndung in sozialen Netzwerken besteht folglich nicht da-

[125] Vgl. *Hawellek/Heinemeyer*, ZD-Aktuell 2012, 02730.

[126] Geändert durch das Gesetz zur Änderung und Ergänzung des Strafverfahrensrechts v. 2.8.2000 (StVÄG 1999), BGBl. I 2000, S. 1253.

[127] So BR-Drs. 961/96, S. 19, und BT-Drs. 14/1484, S. 19.

[128] Vgl. *Pätzel*, NJW 1997, 3131 (3132); *Hilger*, in: Rieß (Hrsg.), Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 2, 25. Aufl. 2004, § 131 Rn. 1 und 32.

[129] Vgl. BT-Drs. 14/1484, S. 21; BT-Drs. 14/2595, S. 27 f.

[130] Vgl. BT-Drs. 14/3525, S. 2.

[131] Vertiefend hierzu *Schiffbauer*, NJW 2014, 1052 (1056 f.). Vgl. als Beispiel einer privatbetriebenen Fahndungsseite: https://www.facebook.com/fahndungennrw?fref=ts (9.3.2015).

[132] Vertiefend zu den Missbrauchsgefahren der allgemeinen Onlinefahndung *Seitz*, Strafverfolgungsmaßnahmen im Internet, 2004, S. 384 f.

rin, dass Dritte nicht unmittelbar im Netz auf den Fahndungsaufruf reagieren können, sondern allein in dem wahrscheinlichen Verbreitungsgrad, der im Durchschnitt geringer ist, wenn eine Meldung nur auf der Homepage der Polizei veröffentlicht wird, etwas größer, wenn er in einem sozialen Netzwerk veröffentlicht wird, aber das Teilen des Beitrags technisch ausgeschlossen ist, und am größten, wenn er in sozialen Netzwerken geteilt werden kann. Diese Aspekte sind jedoch lediglich für die Frage der Verhältnismäßigkeit von Bedeutung und nicht für die Frage, ob die Facebookfahndung den §§ 131 ff. StPO unterfällt.

Will der Staat daher ein Mindestmaß an Einfluss auf die Verbreitung von Fahndungsaufrufen in sozialen Netzwerken behalten, darf er die sozialen Netzwerke nicht den privaten Anbietern überlassen. Im Rahmen der eigenen Angebote lässt sich dann der Grad der Interaktivität durch entsprechende Einstellungen regulieren und jeder Fahndungsaufruf kann mit dem Hinweis versehen werden, dass Zeugen sich nicht über das soziale Netzwerk an die Polizei wenden sollen, sondern eine Kontaktaufnahme nur über klassische Kommunikationswege zulässig ist. Auf diese Weise wird das Risiko minimiert, dass personenbezogene Daten von den Hinweis gebenden Nutzern an Facebook gelangen.

Im Ergebnis ist die Facebookfahndung daher unter den Begriff der Öffentlichkeitsfahndung zu fassen. Der eben entkräftete Einwand ist jedoch nicht der einzige, der gegen die Zulässigkeit der Facebookfahndung ins Feld geführt wird. Dem Datenschutzrecht kommt in diesem Zusammenhang erneut eine erhebliche Bedeutung zu.

b) Die mit dem Hochladen einer Fahndungsmeldung auf Facebook verbundenen datenschutzrechtlichen Probleme

Nicht nur in Bezug auf das schlichte Einrichten einer Fanpage, sondern auch im Rahmen der Öffentlichkeitsfahndung selbst spielt das Datenschutzrecht eine entscheidende Rolle. Anders als beim schlichten Einrichten einer Fanpage und Einstellen bestimmter nicht personenbezogener Informationen enthält ein Fahndungsaufruf personenbezogene Daten, für deren Verarbeitung der Fanpagebetreiber unmittelbar nach TMG und BDSG verantwortlich ist. Da die Verarbeitung personenbezogener Daten in das Recht auf informationelle Selbstbestimmung eingreift, muss jeder Verarbeitungsschritt von einer Ermächtigungsgrundlage gedeckt sein.[133] Eine Einwilligung des Gesuchten nach den §§ 4, 4a BDSG bzw. 12, 13 TMG kommt dabei von vornherein nicht in Betracht.[134]

Die Übermittlung der Daten ins Ausland müsste daher ebenfalls von den §§ 131 ff. StPO gestattet werden, ohne dass die Voraussetzung einer Auslandsfahndung erfüllt wären.

Der niedersächsische Landesbeauftrage für den Datenschutz geht diesbezüglich davon aus, dass die §§ 131 ff. StPO keine taugliche Ermächtigungsgrundlage für die Facebookfahndung darstellen würden, da die Daten auf Server in den USA übermittelt und dort von Facebook ausgewertet werden würden.[135] Eine Datenübermittlung nach Amerika sei aber unzulässig.

Auch wenn Facebook seit Juni 2013 einen Serverpark in Schweden betreibt, muss davon ausgegangen werden, dass tatsächlich noch immer ein großer Teil der Datenverarbeitung in Amerika stattfindet.[136] Für diese Einschätzung spricht insbesondere die Nr. 16.1 (ehemals 17.1) der Nutzungsbedingungen von Facebook, in der bestimmt wird: „Du bist damit einverstanden, dass deine persönlichen Daten in die USA weitergeleitet und dort verarbeitet werden.“[137]

Es könnte daher in der Tat eine unzulässige Auslandsdatenverarbeitung und ein Verstoß gegen § 4b Abs. 2 S. 2, Abs. 3 BDSG bzw. die entsprechenden landesrechtlichen Vorschriften (z.B. § 16 LDSG SH)[138] vorliegen. § 4b Abs. 2 S. 2 BDSG (im Folgenden wird nicht weiter auf die ggf. anwendbaren, aber inhaltlich vergleichbaren landesgesetzlichen Vorschriften verwiesen, sie sind insofern mitzudenken) bestimmt, dass eine Übermittlung von personenbezogenen Daten an ausländische Stellen, die nicht Mitglieder der EU oder Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind, zu unterbleiben hat, wenn der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in S. 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Die Voraussetzungen des § 4b BDSG müssen daher bei Sachverhalten mit Auslandsbezug zu den Voraussetzungen der jeweiligen Ermächtigungsgrundlage hinzutreten. Im Datenschutzrecht spricht man insofern von einer „zweistufigen“ Prüfung.[139] Auf der ersten Stufe sind die allgemeinen Voraussetzungen der Datenübermittlung zu prüfen, auf der zweiten Stufe die Voraussetzungen der Übermittlungsverbote an die konkrete Stelle in einem Drittland.

Die Angemessenheit des Schutzniveaus richtet sich dabei nach § 4b Abs. 3 BDSG. Sie ist unter Berücksichtigung aller Umstände zu beurteilen, die bei einer Datenübermittlung von Bedeutung sind; „insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.“[140]

[133] ULD SH (Fn. 21), S. 20.

[134] Vgl. zu den Voraussetzungen der Einwilligung ULD SH (Fn. 21), S. 20; Wissenschaftlicher Dienst des Bundestages (Fn. 22), S. 12 f.

[135] Vgl. Landesbeauftragter für den Datenschutz Niedersachsen, zitiert nach *Hawellek/Heinemeyer*, ZD-Aktuell 2012, 02730.

[136] Vgl. KG BeckRS 2014, 03648. Umfassend zur Datenspeicherung bei Facebook *Ihwas* (Fn. 4), S. 57 ff.

[137] *Polenz*, VuR 2012, 207 (208); vgl. dazu: https://de-de.facebook.com/terms.php?locale=DE (9.3.2015).

[138] Vgl. zur Vergleichbarkeit *Gabel*, in: Taeger/Gabel (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 2. Aufl. 2013, § 4b Rn. 7.

[139] *Gabel* (Fn. 138), § 4b Rn. 9.

[140] Zitiert wird § 4b Abs. 3 BDSG.

aa) Die Anwendbarkeit des § 4b BDSG neben den §§ 131 ff. StPO

Zu klären ist damit, ob § 4b BDSG überhaupt neben den §§ 131 ff. StPO berücksichtigt werden muss. In diesem Zusammenhang ist anerkannt, dass das BDSG immer dann Anwendung findet, wenn „keine speziellen bereichsspezifischen Datenschutzregelungen bestehen" (vgl. § 1 Abs. 3 S. 1 BDSG).[141] Das BDSG wird nur verdrängt, „soweit" besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln. Bestehen Lücken, ist auf das BDSG zurückzugreifen.[142] Dies entspricht seiner Funktion als Auffanggesetz.

Nichts anderes gilt auch für die Anwendbarkeit des § 4b BDSG im öffentlichen Bereich, da die Norm nicht ausschließlich der Umsetzung des Art. 25 EU DSRL diente, sondern zudem den ehemaligen § 17 BDSG in der Fassung vor 2001, der gleichermaßen für den öffentlichen und den nicht-öffentlichen Bereich galt, ersetzt hat. Anstatt ausschließlich bereichsspezifische Datenschutzgesetze zu erlassen, haben sich Bund und Länder für eine einheitliche Grundlage des Datenschutzes entschieden. Das BDSG regelt daher mehr als die EU DSRL, weshalb § 4b BDSG im Grundsatz auch für die Strafverfolgungsbehörden gilt.

Speziellere Regelungen zu § 4b BDSG finden sich nun in den verschiedensten Gesetzen. Geläufige Beispiele sind § 77 SGB X (Übermittlung von Sozialdaten ins Ausland) oder § 37 StVG (Übermittlung von Fahrzeug- und Halterdaten an Stellen außerhalb des Geltungsbereichs des StVG), nicht jedoch in der StPO. Auch sind die Datenschutzvorschriften der StPO nach herrschender Auffassung nicht abschließend, sodass im Einzelfall ein Rückgriff auf das BDSG möglich ist.[143] Anerkannt ist u.a., dass die Regeln über die Datensicherheit in § 9 BDSG von allen Strafverfolgungsorganen eingehalten werden müssen.[144] Die §§ 131 ff. StPO legen nun jedoch nur die Voraussetzungen der ersten Stufe fest und betreffen damit die Frage nach der grundsätzlichen Zulässigkeit der Datenübermittlung. Zur zweiten Stufe, der Frage nach der Datenübermittlung in bestimmte Länder, verhalten sie sich nicht.

§§ 474 ff. StPO regeln ausschließlich das Ersuchen um Auskünfte aus Akten und die Datenübermittlung von Amts wegen in Konstellationen, die die Fahndung nicht betreffen.[145] Ein Ausschlussgrund für die Datenübermittlung in bestimmte Länder außerhalb der EU anlässlich einer Fahndung lässt sich auch aus ihnen nicht ableiten.

§§ 483 ff. StPO befassen sich schließlich mit der Datenübermittlung zwischen Strafverfolgungsbehörden, Strafgerichten und sonstigen mit der Strafrechtspflege befassten Stellen, nicht jedoch mit der Datenübermittlung an private Dritte.[146] Es existiert zudem auch hier keine im Vergleich mit § 4b BDSG speziellere Regelung wie sie beispielsweise die §§ 61a, 92 IRG im Bereich der internationalen Rechtshilfe darstellen oder die §§ 14 ff. BKAG, 32 ff. BPolG bezogen auf den Datenaustausch mit ausländischen Stellen, die für die Verhütung oder Verfolgung von Straftaten zuständig sind. Die Frage nach der Zulässigkeit der Datenübermittlung an private Dritte im Ausland wird im Zusammenhang mit der nationalen Fahndung schlicht ausgeklammert. Auch das TMG enthält keine im Vergleich mit § 4b BDSG speziellere Regelung über die Datenübermittlung ins Ausland, sondern verweist in § 12 Abs. 3 TMG auf das BDSG.

Entsprechend der fehlenden Regelungen über die Datensicherheit darf daher nicht davon ausgegangen werden, dass der Fahndung keinerlei Grenzen gesetzt sind. Vielmehr ist auf die allgemeinen Vorgaben der Datenschutzgesetze zurückzugreifen und § 4b BDSG findet Anwendung. Für diese Auslegung spricht auch Art. 13 des Rahmenbeschlusses über den Datenschutz in Strafsachen[147], da dort bestimmt wird, dass eine Weitergabe von Daten, die ein Mitgliedstaat von einem anderen erhalten hat, an Drittstaaten nur zulässig ist, wenn diese ein ausreichendes Datenschutzniveau gewährleisten. Ein sachlicher Grund dafür, dass Daten, die unmittelbar durch deutsche Behörden erhoben worden sind, kein entsprechender Schutz zuteilwerden sollte, ist nicht ersichtlich. Auch findet sich keine Art. 13 entsprechende Einschränkung in der StPO, sodass sie bei europarechtskonformer Auslegung dem BDSG entnommen werden muss.

bb) Das Vorliegen der Voraussetzungen des § 4b Abs. 2 S. 2, Abs. 3 BDSG

Fraglich ist daher, ob die Voraussetzungen des § 4b Abs. 2 S. 2, Abs. 3 BDSG vorliegen.

Zunächst ist festzuhalten, dass die USA nicht Mitgliedstaat der Europäischen Union oder Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum sind und die Übermittlung der Daten auch nicht im Rahmen von Tätigkeiten erfolgt, „die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen." Voraussetzung der Datenübermittlung ist daher, dass der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat, insbesondere also „ein angemessenes Datenschutzniveau" bei der empfangenden Stelle, mithin Facebook Inc., gewährleistet ist. Eine Ausnahme vom Erfordernis dieser Voraussetzungen nach den §§ 4b Abs. 2 S. 3, 4c BDSG liegt nicht vor.

[141] Vgl. *Soiné*, NStZ 1997, 166 (168 f.).

[142] Umfassend Gola/Schomerus, in: Gola/Schomerus, Bundesdatenschutzgesetz, Kommentar, 12. Aufl. 2015, § 1 Rn. 23 f.; vgl. auch *Brodersen*, NJW 2000, 2536 (2537).

[143] *Schmitt*, in: Meyer-Goßner/Schmitt, Strafprozessordnung, Kommentar, 57. Aufl. 2014, Vor §§ 474 ff. Rn. 3; *Weßlau*, in: Wolter (Hrsg.), Systematischer Kommentar zur Strafprozessordnung, GVG und EMRK, Bd. 8, 4. Aufl. 2013, Vor §§ 474 ff. Rn. 25; *Brodersen*, NJW 2000, 2536 (2537).

[144] So *Schmitt* (Fn. 138), Vor §§ 474 ff. Rn. 3.

[145] Vertiefend *Weßlau* (Fn. 143), Vor §§ 474 ff. Rn. 1.

[146] Vgl. *Weßlau* (Fn. 143), Vor §§ 483 ff. Rn. 1, und § 487 Rn. 1.

[147] Rahmenbeschluss 2008/977/JI des Rates v. 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, Abl. EU Nr. L 350, S. 60.

(1) Der Einfluss der Safe-Harbor-Zertifizierung Facebooks auf die Annahme eines „angemessenen Datenschutzniveaus“ nach der herrschenden Meinung

Für die Annahme eines angemessenen Datenschutzniveaus könnte zunächst sprechen, dass Facebook ein Safe-Harbor-Zertifikat beantragt und erhalten hat.[148] Die Safe-Harbor-Zertifizierung beruht auf einer Entscheidung der Europäischen Kommission[149] und erfordert, dass sich das antragstellende Unternehmen verpflichtet, die Safe-Harbor-Principles sowie einige weitere Voraussetzungen einzuhalten, und sich bei der Federal Trade Commission registrieren lässt. Mit der Registrierung gilt ein angemessenes Datenschutzniveau grundsätzlich als gewährleistet.

Zu beachten ist jedoch erneut, dass die EU DSRL und damit auch das Safe-Harbor-Abkommen keine Bindungswirkung im Bereich der Strafverfolgung entfalten, selbst wenn das nationale Datenschutzrecht Vorschriften, die der Umsetzung der EU DSRL dienen, auch auf Strafverfolgungsbehörden erstreckt. Den Datenschutz in Bereichen, die nicht der EU DSRL unterfallen, können die Länder – von anderen möglicherweise einschlägigen Richtlinien oder Rahmenbeschlüssen abgesehen – frei gestalten. Eine Geltung des Safe-Harbor-Abkommens im Zusammenhang mit dem Rahmenbeschluss über den Datenschutz in Strafsachen wird aber weder im Rahmenbeschluss noch andernorts angeordnet. Auch im nationalen Recht findet sich keine Bezugnahme auf die Kommissionsentscheidung, die darüber hinaus auch nach ihrer Schutzrichtung nicht auf Strafverfolgungsmaßnahmen passt. Eine Pflicht zur Beachtung der Safe-Harbor-Zertifizierung Facebooks durch die fahndende Stelle ist daher zu verneinen.

Hinzu kommt, dass eine solche Selbstzertifizierung für sich genommen „bei einem gleichzeitigen Fehlen der tatsächlichen Durchsetzung der Datenschutzgrundsätze“ nach in Deutschland herrschender Meinung auch nicht ausreichend wäre, um die Datenübermittlung zu legitimieren, sondern es müsste in gewissen Grenzen die tatsächliche Einhaltung der Selbstverpflichtung geprüft werden.[150] Entsprechend vertritt die Art. 29-Datenschutzgruppe der EU die Ansicht, „dass die Safe-Harbor-Grundsätze an sich dem Daten-Exporteur nicht die erforderlichen Mittel garantieren, um sicherstellen zu können, dass von dem […] Anbieter in den USA angemessene Sicherheitsmaßnahmen angewendet w[e]rden, wie es möglicherweise von den nationalen Rechtsvorschriften basierend auf Richtlinie 95/46/EC gefordert wird.“

Identisch haben sich der Bundes- und die Landesdatenschutzbeauftragten in Deutschland positioniert. Sie gehen davon aus, dass deutsche Stellen verpflichtet sind, die Einhaltung gewisser Mindestkriterien für den Datenschutz trotz Safe-Harbor-Zertifizierung eigenständig zu prüfen (§ 4b Abs. 5 BDSG), bevor sie personenbezogene Daten an ein zertifiziertes Unternehmen übermitteln.[151] Keinesfalls dürfe sich die übermittelnde Stelle „allein auf die Behauptung einer Safe-Harbor-Zertifizierung des Datenimporteurs verlassen“.[152] Vielmehr müsse sich die datenexportierende Stelle „nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungen vorliegen und deren Grundsätze auch eingehalten werden.“ Insbesondere auf die Einhaltung der Informationspflichten müsse geachtet werden.

Sollte man daher die Safe-Harbor-Zertifizierung von Facebook entgegen der hier vertretenen Auffassung auch im strafrechtlichen Bereich für beachtlich halten, würde dieser Umstand die Behörde nicht von einer datenschutzrechtlichen Risikobewertung entbinden.

(2) Die rechtliche Begründung der Überprüfungspflicht

Für die eben vorgestellte Rechtsauffassung der herrschenden Meinung spricht zunächst, dass Art. 25 Abs. 2 EU-DSRL, dessen Umsetzung § 4b Abs. 3 BDSG dient, eine Prüfung der Angemessenheit des Datenschutzniveaus im Einzelfall verlangt.[153] Insbesondere soll die Art der konkret übermittelten Daten von Bedeutung sein. Ob die schutzwürdigen Interessen des Betroffenen verletzt werden, kann nämlich nicht unab-

[148] Vgl. die Liste Safe-Harbor-zertifizierter Unternehmen, online abzurufen unter: https://safeharbor.export.gov/list.aspx (9.3.2015).

[149] Entscheidung 2000/520/EG der Kommission v. 26.7.2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, Abl. EG Nr. L 215, S. 7.

[150] So die Stellungnahme 01037/12/DE WP 196 der Art. 29-Datenschutzgruppe v. 1.7.2012, S. 21 f.; entsprechend Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28. und 29. April 2010 in Hannover, S. 1, abzurufen unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile (9.3.2015); *Däubler*, in: Däubler u.a. (Hrsg.), Kompaktkommentar zum Bundesdatenschutzgesetz, 4. Aufl. 2014, § 4b Rn. 16; *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 8. Aufl. 2014, § 4b Rn. 65 ff. und 78 f.; *Dammann*, in: Dammann/Simitis (Hrsg.), EG-Datenschutzrichtlinie, Kommentar, 1997, Art. 25 Rn. 30; *Hilbrans*, in: Däubler u.a. (Hrsg.), Handkommentar Arbeitsrecht, 3. Aufl. 2013, §§ 4b, 4c BDSG Rn. 2; *Marnau/Schlehahn*, DuD 2011, 311 (313 ff.); a.A. *Schantz*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, Kommentar, 2013, § 4b BDSG Rn. 31.

[151] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28. und 29. April 2010 in Hannover, S. 1, abzurufen unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile (9.3.2015).

[152] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28. und 29. April 2010 in Hannover, S. 1, abzurufen unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile (9.3.2015).

[153] *Simitis* (Fn. 150), § 4b Rn. 65.

hängig davon beurteilt werden, welcher Art die Daten sind und zu welchem Zweck die Übermittlung erfolgt. Bei *Simitis* heißt es hierzu treffend: „Sollen deshalb die Entscheidungsvorgaben der EG-Datenschutzrichtlinie und des BDSG auch weiterhin maßgeblich sein, muss die ‚Angemessenheitsliste' der EG-Kommission zwar zur Kenntnis genommen, aber nur als Anregung angesehen werden, die übermittelnde Stellen ebenso wie nationale Kontrollinstanzen nicht davon entbindet, sich am Einzelfall zu orientieren und dessen Besonderheiten zu berücksichtigen. Die ‚Angemessenheitsliste' ist, anders ausgedrückt, Entscheidungshilfe, nicht aber Entscheidungsersatz."[154]

Gestützt wird diese Erwägung auch dadurch, dass die EU DSRL und die Entscheidung der Kommission grundrechtechartakonform auszulegen sind[155] und Erwägungsgrund Nr. 10 der EU DSRL ausdrücklich auf die Pflicht zur Berücksichtigung der Grundrechte hinweist.

Art. 8 EU GRCh garantiert nun im Rahmen von Rechtsakten der EU den besonderen Schutz personenbezogener Daten. Könnten sich Datenexporteure selbst dann mit Bindungswirkung gegenüber der für die Datenschutzaufsicht verantwortlichen Stelle auf die Safe-Harbor-Selbstzertifizierung eines Daten empfangenden Unternehmens berufen, wenn deren Grundsätze offensichtlich nicht eingehalten werden, ließe sich ein angemessenes Datenschutzniveau nicht gewährleisten.[156]

Der Wortlaut der EU DSRL eröffnet entsprechende Auslegungsspielräume. Sofern Daten in andere EU-Mitgliedstaaten übermittelt werden sollen, verbietet Art. 1 Abs. 2 EU DSRL die Beschränkung oder Untersagung des freien Datenverkehrs aus Gründen des Datenschutzes ausdrücklich. Sofern die Kommission feststellt, dass ein Drittstaat kein ausreichendes Datenschutzniveau gewährleistet, verpflichtet Art. 25 Abs. 4 EU DSRL die Mitgliedstaaten ausdrücklich, die Datenübermittlung in entsprechende Länder zu verhindern. Eine entsprechend zwingende Regelung für die Feststellung, dass in einem Drittstaat das Datenschutzniveau eingehalten wird, fehlt. Es findet sich in Art. 25 Abs. 6 EU DSRL lediglich die weiche Formulierung, dass im Hinblick auf die Feststellung die „gebotenen Maßnahmen" zu ergreifen seien.

Diese Unterschiede in der Formulierung dienen ganz konkreten Zwecken. Unter den Mitgliedstaaten der EU soll der freie Verkehr personenbezogener Daten gewährleistet werden. Hierzu ist zum einen Voraussetzung, dass die Mitgliedstaaten die Datenübermittlung untereinander nicht im Hinblick auf verbleibende nationale Unterschiede im Datenschutzrecht reglementieren, zum anderen ist Voraussetzung, dass die Gefahr gebannt wird, dass die Daten von einem Mitgliedstaat in einen Drittstaat transferiert und dort unter Umgehung der europarechtlichen Vorgaben verarbeitet werden.[157] Ist das Datenschutzniveau in einem Drittstaat aber grundsätzlich angemessen, ist es für den freien Datenverkehr in Europa nicht entscheidend, ob jeder Mitgliedstaat auch jede Datenübermittlung in diesen Drittstaat zulässt.[158] Nicht ohne sachlichen Grund, so *Dammann*, sei daher die Folgeverpflichtung der Mitgliedstaaten im Falle der Bejahung des angemessenen Schutzniveaus anders formuliert worden als im Falle der Verneinung.[159] Sei im erstgenannten Fall die Verpflichtung zur Verhinderung der Datenübermittlung die logische Konsequenz der Verneinung eines angemessenen Datenschutzniveaus, greife bei Bejahung des angemessenen Schutzniveaus keine bestimmte Verpflichtung der Mitgliedstaaten ein. Ein gemeinschaftsrechtlicher Zwang, die Datenübermittlung zuzulassen, bestehe anders als bei der innergemeinschaftlichen Datenübermittlung nicht. Eine Verpflichtung, die Datenübermittlung ausnahmslos und unabhängig von den konkreten Umständen zuzulassen, kann jedenfalls nicht mit dem Ziel der Richtlinie, den freien Datenverkehr in Europa zu gewährleisten, begründet werden.[160] In Erwägungsgrund Nr. 9 der EU DSRL heißt es daher, dass bezogen auf die Datenverarbeitung bei der „Durchführung der Richtlinie" gewisse Spielräume der Mitgliedstaaten bestünden. Die daraus resultierenden Unterschiede seien hinzunehmen, sofern die „Maßgaben" des 2. Kapitels Berücksichtigung fänden (vgl. Art. 5 EU DSRL).

Die Richtlinie selbst macht also für die Einzelfallprüfung, ob bestimmte Daten an eine bestimmte Stelle übermittelt werden dürfen, eine Ausnahme von dem an anderen Stellen verfolgten Ziel der Vollharmonisierung. Dieses gilt zwar für die Voraussetzungen, an denen sich die Prüfung zu orientieren hat, kann aber die von Art. 25 Abs. 2 EU DSRL und Art. 8 GRCh geforderte Bewertung im Einzelfall nicht ersetzen.

Eine eigenständige Prüfung der Zulässigkeit der Datenübermittlung an Facebook seitens der fahndenden Behörde ist daher selbst dann nicht entbehrlich, wenn man die Safe-Harbor-Zertifizierung von Facebook im Rahmen der Fahndung für beachtlich hielte.[161]

---

[154] *Simitis* (Fn. 150), § 4b Rn. 66, ähnlich auch Rn. 78.

[155] Vertiefend zur grundrechtskonformen Auslegung von EU-Sekundärrecht *Herdegen*, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. 10, 3. Aufl. 2012, § 211 Rn. 28.

[156] *Simitis* (Fn. 150), § 4b Rn. 78.

[157] Vgl. *Draf*, Die Regelung der Datenübermittlung personenbezogener Daten in Drittländer nach Art. 25, 26 der EG-Datenschutzrichtlinie, 1999, S. 103.

[158] *Draf* (Fn. 157), S. 103.

[159] *Dammann* (Fn. 150), Art. 25 Rn. 30.

[160] In diesem Sinne *Draf* (Fn. 157), S. 103.

[161] Vgl. allgemein zur Prüfpflicht *Simitis* (Fn. 150), § 4b Rn. 79. Zu beachten ist darüber hinaus, dass Art. 25 Abs. 6 EU DSRL die Kommission lediglich zu der Feststellung ermächtigt, dass ein Staat ein angemessenes Schutzniveau gewährleistet. Innerhalb dieses Staates kann es dennoch Stellen geben, die die Regeln nicht einhalten, was im Einzelfall berücksichtigt werden können muss. Schon die Kompetenz zur Feststellung, dass eine bestimmte Stelle ein hinreichendes Datenschutzniveau einhält, ist daher fraglich. Eine solche unterstellt, wird die Einzelfallprüfung jedoch nicht entbehrlich, da es stets auf den konkreten Akt der Datenübermittlung ankommt, zu dem die Kommission keine Aussage treffen kann. Sie kann lediglich den abstrakten Rahmen prüfen.

cc) Die Anwendung der erarbeiteten Grundsätze auf die Facebookfahndung

Eine Übermittlung der personenbezogenen Fahndungsdaten an Facebook ist nach den eben dargestellten Grundsätzen also nur möglich, wenn zumindest eine summarische Prüfung bestätigt, dass Facebook auch in Bezug auf die hoch sensiblen Fahndungsdaten ein angemessenes Datenschutzniveau gewährleistet. Je größer der Eingriff in das allgemeine Persönlichkeitsrecht ausfällt, desto höher müssen dabei die Standards der Datenverarbeitung der empfangenden Stelle sein.

Dass Facebook jedoch, die tatsächlichen Feststellungen und rechtlichen Einschätzungen des ULD SH weiter zugrunde gelegt, ein angemessenes Datenschutzniveau im Hinblick auf personenbezogene Fahndungsdaten gewährleistet, lässt sich nicht annehmen.[162] Um nur den wichtigsten Aspekt zu nennen, werden die Fahndungsaufrufe bei Facebook dauerhaft gespeichert und können nach der Beendigung der Fahndung nicht von der zuständigen Behörde gelöscht werden.[163] Auch können die amerikanischen Geheimdienste nach Beendigung der Fahndung weiter auf die entsprechenden Daten bei Facebook zugreifen, woraus sich erhebliche Nachteile des ehemals Gesuchten im Falle einer geplanten Einreise in die USA ergeben können. Die erforderliche, mindestens summarische Prüfung, dass ein ausreichender Schutz für die besonders sensiblen Fahndungsdaten gewährleistet ist, dürfte den Fanpagebetreibern daher nicht möglich sein. Wird der Nachweis für die Einhaltung eines angemessenen Schutzniveaus durch Facebook nicht geführt, dürfen die Fanpagebetreiber folglich keine personenbezogenen Daten auf ihrer Fanpage veröffentlichen. Gestützt wird das Ergebnis zudem durch allgemeine Verhältnismäßigkeitserwägungen.[164]

dd) Die Konsequenzen des Ergebnisses

Daraus, dass die Polizeibehörden keine personenbezogenen Fahndungsdaten in das soziale Netzwerk Facebook einstellen dürfen, folgt nun aber keineswegs ein grundsätzliches Verbot der Facebookfahndung. Die Erfahrung zeigt vielmehr, dass es für eine erfolgreiche Facebookfahndung gar nicht erforderlich ist, den Primärdatensatz, also den Fahndungsaufruf selbst, in das soziale Netzwerk einzustellen. Vielmehr reicht es aus, dass der Fahndungsaufruf aus dem sozialen Netzwerk heraus erreichbar ist.

Zur technischen Umsetzung einer zulässigen Facebookfahndung sind daher zwei Vorgehensweisen denkbar, zum einen die sogenannte Link-Lösung und zum anderen die sogenannte i-frame-Lösung, die nun im Folgenden vorgestellt werden.

(1) Die sogenannte Link-Lösung

Bei der sogenannten Link-Lösung wird der Fahndungsaufruf ausschließlich auf polizeieigenen Servern veröffentlicht und auf der Fanpage wird lediglich ein Hinweis auf den Fahndungsaufruf und dessen Internetadresse eingestellt.[165] Durch entsprechende Einstellungen lässt es sich auch verhindern, dass eine Seitenvorschau bei Facebook angezeigt wird und auf diesem Wege Bilddateien in den Machtbereich von Facebook gelangen.

Der eingestellte Link samt einer allgemeinen, nicht personenbezogenen kurzen Beschreibung des Vorfalls wird anschließend von den Fans der Behördenseite und von deren Freunden geteilt und verbreitet sich so schnell über das gesamte soziale Netzwerk.

Wird der Link von einem Nutzer angeklickt, gelangt dieser direkt auf die polizeieigene Seite. An Facebook gelangt dabei nur die Internetadresse samt Begleittext.[166] Die Polizei bleibt damit Herrin der Daten und kann diese im Anschluss an die Fahndung von ihrem eigenen Server löschen. Die geteilten Links verweisen ab diesem Zeitpunkt ins Leere.

Bereits vom EuGH entschieden ist zudem, dass das Einstellen von Daten auf eigenen Webseiten nicht selbst eine Datenübermittlung in Drittländer gemäß Art. 25 EU DSRL und der zu seiner Umsetzung ergangenen nationalen Regelungen darstellt, solange sich die Server im Inland oder in einem Mitgliedstaat der EU befinden.[167] Dass von überall auf der Welt auf diese Daten zugegriffen werden könne, sei für den Begriff der Datenübermittlung irrelevant. Zur Begründung führt der EuGH aus, dass bei einer anderen Auslegung immer dann, wenn personenbezogene Daten auf eine Internetseite hochgeladen würden, auch eine Übermittlung von Daten in ein Drittland vorläge, da die Übermittlung unter dieser Prämisse in alle Länder erfolge, in denen die Internetseite potentiell aufrufbar sei.[168] „Damit würde die in Kap. IV Richtlinie 95/46/EG vorgesehene Sonderregelung notwendig zu einer allgemeinen Regelung für Vorgänge im Rahmen des Internets werden.“ Sobald die Kommission also nur für ein einziges Land, aus dem auf das Internet zugegriffen werden kann, feststellen würde, dass dieses kein angemessenes Schutzniveau aufweise, wären die Mitgliedstaaten verpflichtet, „jede Aufnahme personenbezogener Daten in das Internet zu unterbinden“.

[162] Vgl. ULD SH, zitiert nach ZD-Aktuell 2012, 03098, sowie *Erd*, NVwZ 2011, 19 (19 f.), mit Erläuterungen zum amerikanischen, sektoralen Datenschutzrecht.

[163] Vertiefend *Weichert* (Fn. 79), S. 379 (382).

[164] Zutreffend geht *Kolmey*, DRiZ 2013, 242 (244), davon aus, dass es nie erforderlich sein kann, die Kontrolle über die personenbezogenen Daten aus der Hand zu geben, was zwingende Konsequenz einer Einstellung von Daten in das soziale Netzwerk Facebook ist. Zudem legt *Kolmey* (a.a.O.) dar, dass es problematisch sei, die Daten ohne entsprechendes Rechtshilfeersuchen auf amerikanischen Servern zu verarbeiten. Selbst dann, wenn man § 4b BDSG im Rahmen der Fahndung für unanwendbar halten wollte, wäre das Ergebnis also dasselbe.

[165] Vgl. zur Link-Lösung insgesamt *Kolmey*, DRiZ 2013, 242 (244).

[166] Vgl. Presseinformation der Polizei Niedersachen vom 2.6.2012, online abzurufen unter: http://www.mi.niedersachsen.de/portal/live.php?navigation_id=14797&article_id=102910&_psmand=33 (9.3.2015).

[167] EuGH EuZW 2004, 245 (249 f.).

[168] EuGH EuZW 2004, 245 (250).

Ein so weitreichendes Verbot der Internetnutzung wäre jedoch mit dem Ziel der EU DSRL, den freien Datenverkehr zu ermöglichen, unvereinbar, sodass der entsprechenden Konsequenz bereits bei der Auslegung des Begriffs der Datenübermittlung in Ausland entgegenzutreten ist.[169] In den Begriff der Übermittlung wird daher ein finales Element hineingelesen.[170]

Zu beachten ist zwar erneut, dass die EuGH-Entscheidung keine unmittelbare Bindung für die Strafverfolgungsbehörden entfaltet, aber sie wirkt jedenfalls mittelbar über die im Übrigen verbindliche Auslegung des § 4b BDSG.

Das Hochladen von Fahndungsdaten auf eine Webseite stellt damit keine Datenübermittlung ins Ausland dar.[171] Eine Datenübermittlung im Inland ist nach Maßgabe der §§ 131 ff. StPO zulässig.

Die Link-Lösung ist daher ein gangbarer Weg, der u.a. bereits vom LKA Niedersachsen beschritten wird.[172]

(2) Die sogenannte i-frame-Lösung

Als Alternative zur Link-Lösung kommt auch die sogenannte i-frame- oder inline-frame-Lösung in Betracht. Beim i-framing „handelt es sich um eine besondere Spielart der Verlinkung zweier Webseiten", da die verlinkte Seite nicht nach anklicken eines Links in einem eigenen Browserfenster aufgerufen, sondern unmittelbar in einem speziell definierten Bereich der Ausgangsseite angezeigt wird.[173] Ein i-frame ist daher ein HTML-Element, das es ermöglicht, den Inhalt einer Internetseite auf einer anderen Internetseite anzeigen zu lassen.[174] Entsprechend der Link-Lösung werden bei dieser Art des Vorgehens keine personenbezogenen Daten an Facebook übermittelt.[175]

Ein polizeitaktischer Vorteil der i-frame-Lösung gegenüber der Link-Lösung scheint nun zu sein, dass der Fahndungsaufruf unmittelbar auf der Fanpage sichtbar wird. Da die Daten jedoch nicht auf die Facebookseite gelangen, erscheinen sie weder im Newsfeed der Seitenfans noch können sie geteilt und auf diese Weise im sozialen Netzwerk verbreitet werden. Der jeweilige Nutzer muss also entsprechend einer klassischen Homepage unmittelbar auf die jeweilige Fanpage zugreifen, um auf einen Fahndungsaufruf aufmerksam zu werden. Die i-frame-Lösung entspricht daher eher der Fahndung mittels einer klassischen Homepage, die entsprechend der Link-Lösung zwingend parallel erfolgen muss. Lediglich der Verbreitungsgrad des Fahndungsaufrufs dürfte unwesentlich erhöht sein, da sowohl Nutzer erreicht werden, die die polizeiliche Homepage aufrufen, als auch solche, die die polizeiliche Fanpage aufrufen. Der spezifische Nutzen, den die Fahndung in sozialen Netzwerken bietet, lässt sich im Rahmen der i-frame-Lösung aber nicht realisieren. Vielmehr findet die Fahndung gar „nicht ‚in' einem sozialen Netzwerk statt, sondern nur ‚über' das soziale Netzwerk".[176] Entsprechend geht beispielsweise die Polizei Hessen vor.[177]

Ein Konflikt mit dem Datenschutzrecht besteht auch bei dieser Lösung nicht. Grundsätzlich lässt sich eine datenschutzrechtlich zulässige Facebookfahndung also technisch realisieren. Es bleibt jedoch noch die Frage nach der Zuständigkeit für entsprechende Fahndungsmaßnahmen zu klären. Gelegentlich wird diesbezüglich vorgetragen, es handle sich bei jeder Onlinefahndung um eine internationale Fahndung, weshalb ausschließlich das BKA zuständig sei.

c) Facebookfahndung als internationale Fahndung

Pätzel u.a. gehen davon aus, dass jede Internetfahndung zugleich internationale Fahndung sei und sich an den entsprechenden Anforderungen messen lassen müsse.[178] Für die Durchführung internationaler Fahndungen wäre nun aber gemäß der §§ 3, 11 bis 15a BKAG ausschließlich das BKA zuständig und die besonderen Anordnungsvoraussetzungen der internationalen Fahndung nach Nr. 43 RiStBV wie z.B., dass sich die gesuchte Person im Ausland befindet und ihre Auslieferung beantragt werden soll, müssten vorliegen.[179] Das ist in typischen Fällen der Facebookfahndung, mit deren Hilfe im Inland nach bestimmten Personen gesucht wird, nicht der Fall. Fraglich ist daher, ob die Einschätzung *Pätzels* zutreffend ist.

Die internationale Fahndung zeichnet sich im Vergleich mit der nationalen oder auch nur regionalen Fahndung nun dadurch aus, dass durch die Fahndung die territoriale Souveränität eines anderen Staates berührt wird, da sich die Fahndungsaufforderung im Sinne eines Rechtshilfeersuchens un-

[169] Vgl. *Taraschka*, CR 2004, 280 (284 f.); *Roßnagel*, MMR 2004, 99 (99 f.).
[170] *Taraschka*, CR 2004, 280 (284 f.); *Roßnagel*, MMR 2004, 99 f.
[171] Sollte man bereits das Onlinestellen von Informationen als Übermittlung in Drittländer betrachten, müsste jede Internetfahndung davon abhängig gemacht werden, dass die Behörde eine sogenannte IP-Länder- oder Geo-Sperre einrichtet und über eine solche Geo-IP-Filterung verhindert, dass Fahndungsdaten in unsichere Drittländer gelangen. Entsprechend geht etwa YouTube vor. Eine bewusste Umgehung dieser Sperren durch Nutzer würde dann den Zurechnungszusammenhang durchbrechen und damit keine Übermittlung seitens der Behörde darstellen.
[172] Vgl. https://www.facebook.com/LandeskriminalamtNiedersachsen?fref=ts (9.3.2015).
[173] So LG Hamburg MMR 2003, 197 (197 f.).
[174] Vertiefend zur i-frame-Lösung *Ihwas* (Fn. 4), S. 283.
[175] *Ihwas* (Fn. 4), S. 283.
[176] So LT-Drs. RP 16/3387, S. 3.
[177] Vgl. https://www.facebook.com/PolizeiHessen/app_396393053713168 (9.3.2015).
[178] *Pätzel*, NJW 1997, 3131 (3132 f.); bayerischer Landesdatenschutzbeauftragter, 18. Tätigkeitsbericht, 1998, Nr. 7.3.1, abzurufen unter: https://www.datenschutz-bayern.de/nav/1001.html (9.3.2015). Vgl. auch Nr. 85 RiVASt, Nr. 43 RiStBV sowie die Richtlinien der Länder über die internationale Fahndung nach Personen.
[179] Vertiefend zur internationalen Fahndung allgemein *Soiné*, NStZ 1997, 321 (324); speziell zur Facebookfahndung *Ihwas* (Fn. 4), S. 284.

mittelbar an ausländische Behörden richtet.[180] Solange aber keine fremden Hoheitsrechte verletzt werden, weil weder ein anderer Staat um Unterstützung in einem Strafverfahren ersucht wird noch Personen, die sich im Ausland befinden, Zwangsmaßnahmen oder Rechtsnachteile angedroht oder für diese Rechtswirkungen herbeigeführt werden, ist ein Rechtshilfeersuchen nicht erforderlich.[181] Vielmehr erlaubt es die Gebietshoheit eines jeden Staates, Informationen auf Servern, die sich im eigenen Staatsgebiet befinden, online zu stellen.[182] Jedenfalls die Facebookfahndung mittels der Link- oder i-frame-Lösung stellt daher keine internationale Fahndung dar, weil eine Person im Inland gesucht wird und die Datensätze auf deutschen Servern durch die hierfür zuständigen Polizeibehörden eingegeben werden.[183] Es handelt sich lediglich um eine nationale Fahndung.

Für diese Sichtweise spricht auch ein Vergleich mit der Fahndung über Fernsehsendungen und Printmedien, die ebenfalls im Ausland empfangen bzw. bezogen werden können, aber unstreitig als nationale Fahndungen angesehen werden, solange die Ausstrahlung über einen deutschen Sender erfolgt oder es sich um eine in Deutschland verlegte Zeitung handelt.[184]

Die vereinzelt gebliebene Sichtweise *Pätzels* verdient folglich keine Zustimmung. Es bleibt damit nur noch eine Frage zu beantworten und zwar die nach der allgemeinen Verhältnismäßigkeit der Facebookfahndung bezogen auf die mit ihr verbundenen Missbrauchsgefahren.

d) Das Problem digitaler Kopien und persönlichkeitsrechtsverletzender Kommentareinträge

Der Umstand, dass das Internet nicht vergisst und die dort enthaltenen Daten einem sehr großen Personenkreis zugänglich sind, stellt einen im Vergleich mit analogen Fahndungsaufrufen größeren Eingriff in das Allgemeine Persönlichkeitsrecht der Gesuchten dar.[185] Gerade im Bereich der Facebookfahndung lassen sich entsprechende Aufrufe grundsätzlich teilen oder kopieren, wodurch der Fahndungsaufruf perpetuiert wird.[186]

Darüber hinaus räumt Facebook die grundsätzliche Möglichkeit ein, Profile mit Fotos zu verlinken und die Fotos zu kommentieren. Teilweise wurden diese Funktionen in der Vergangenheit auch dazu missbraucht, zur Selbstjustiz gegen eine Person aufzurufen oder diese in der Öffentlichkeit bloßzustellen.[187]

Das entsprechende Risiko lässt sich jedoch sowohl durch die Link- als auch durch die i-frame-Lösung reduzieren, da nicht der Primärdatensatz geteilt wird. Zudem ist aus Gründen der Verhältnismäßigkeit darauf hinzuweisen, dass die Informationen zwar geteilt werden dürfen, aber Private nicht berechtigt sind, den originären Fahndungsaufruf auf eigenen Facebookseiten zu veröffentlichen.[188] Anderenfalls tragen die Privaten selbst ein Haftungsrisiko und machen sich ggf. sogar strafbar.[189]

Entsprechend ist darauf hinzuweisen, „dass sachdienliche Hinweise ausschließlich außerhalb der Kommunikationsstrukturen sozialer Netzwerke übermittelt werden“ und dass Kommentare auf den offiziellen Fanpages auf persönlichkeitsrechtsverletzende Inhalte geprüft und ggf. entfernt werden.[190] Auf das Einhalten dieser Regeln haben die online fahndenden Beamten im Rahmen des Möglichen zu achten.

Nachdem die Fahndung beendet worden ist, sind die Interneteinträge gemäß Nr. 3.2 der Anlage B zur RiStBV sowie nach allgemeinen Grundsätzen zu löschen und es ist auf demselben Weg, der für die Bekanntmachung der Fahndung genutzt worden ist, darauf hinzuweisen, dass die Fahndung nun beendet ist und der Fahndungsaufruf samt Bildmaterial auch von Privaten, die ihn auf eigenen Servern veröffentlicht haben, zu löschen ist.[191] Richtigerweise weist daher das LKA Niedersachsen im Anschluss einer jeden Facebookfahndung auf das Ende der Fahndung hin und bittet darum, „den Namen des Beschuldigten und seine Beschreibung aus dem Internet zu entfernen, da die Fahndungsmaßnahme beendet ist und die Persönlichkeitsrechte des Beschuldigten zu schützen sind.“[192]

Werden diese Vorgaben eingehalten, bestehen daher bei der Facebookfahndung dieselben Risiken, die jeder Onlinefahndung innewohnen. Es wiegt lediglich der Eingriff in das Allgemeine Persönlichkeitsrecht im Hinblick auf den hohen Verbreitungsgrad der Fahndungsaufrufe schwerer. Bereits die allgemeine Onlinefahndung ist jedoch wegen der hohen Risiken nur zur Aufklärung schwerster Kriminalität statthaft.[193]

---

[180] Vertiefend *Soiné*, NStZ 1997, 166 (167 f.); *Seitz* (Fn. 132), S. 382; *Ihwas* (Fn. 4), S. 284.

[181] Vertiefend *Soiné*, NStZ 1997, 166 (167 f.).

[182] *Seitz* (Fn. 132), S. 383; vgl. zur Datenverarbeitung auf Servern in fremdem Staatsgebiet *Kolmey*, DRiZ 2013, 242 (244).

[183] So *Ihwas* (Fn. 4), S. 284; entsprechend auch schon *Gerhold* (Fn. 117), § 131 Rn. 11. Anders kann es sich verhalten, wenn mittels Facebook gezielt eine Person im Ausland gesucht werden soll.

[184] Vgl. *Ihwas* (Fn. 4), S. 284; *Gerhold* (Fn. 117), § 131 Rn. 11, *Seitz* (Fn. 132), S. 383.

[185] Vgl. *Schiffbauer*, NJW 2014, 1052 (1053).

[186] *Schiffbauer*, NJW 2014, 1052 (1053).

[187] Vgl. *Schiffbauer*, NJW 2014, 1052 (1053); umfassend zu den sogenannten negativen Netzwerkeffekten *Lohmeier u.a.* (Fn. 7), S. 10 ff.

[188] *Lohmeier u.a* (Fn. 7), S. 26.

[189] Umfassend zu den strafrechtlichen Risiken Dritter, die Fahndungsaufrufe nicht nur verlinken, sondern kopieren *Schiffbauer*, NJW 2014, 1052 (1056 f.).

[190] So LT-Drs. RP 16/3387, S. 2 f.; entsprechend die Forderungen bei *Lohmeier u.a.* (Fn. 7), S. 25.

[191] Vertiefend *Schiffbauer*, NJW 2014, 1052 (1056); *Lohmeier u.a.* (Fn. 7), S. 25.

[192] Vertiefend zum gegen die Behörde gerichteten Folgenbeseitigungsanspruch und der Pflicht, über die Beendigung der Fahndung zu informieren, *Schiffbauer*, NJW 2014, 1052 (1055 f.).

[193] So bereits *Seitz* (Fn. 132), S. 386; *Gerhold* (Fn. 117), § 131 Rn. 15; speziell für die Facebookfahndung auch *Ihwas* (Fn. 4), S. 281.

Fahndungen im Internet nach Verkehrssündern oder Sachbeschädigern, die in der Vergangenheit immer wieder vorkamen, sind ausnahmslos unverhältnismäßig.[194] Im Rahmen schwerster Delikte ist dann jeweils im Einzelfall zu entscheiden, ob der Fahndungsaufruf lediglich über die polizeieigene Homepage oder noch zusätzlich über Facebook zu verbreiten ist. Dabei ist zu berücksichtigen, dass der Eingriff in das Recht auf informationelle Selbstbestimmung bei der Verbreitung über die i-frame-Lösung bereits etwas größer ist als bei ausschließlicher Verbreitung über die polizeieigene Homepage und bei einer Verbreitung mittels der Link-Lösung noch einmal deutlich erhöht ist.[195] Ist es trotz dieser hohen Hürden verhältnismäßig, auf Facebook zu fahnden, liegt stets auch ein ausreichender Grund vor, von der Regelverpflichtung der Nr. 3.2 der RiStBV abzuweichen, nach der „grundsätzlich" nicht in Angeboten Privater gefahndet werden soll.

III. Zusammenfassung und Endergebnis

Technisch lässt sich die Facebookfahndung sowohl über die Link- als auch über die i-frame-Lösung im Einklang mit den nationalen und internationalen Datenschutzbestimmungen realisieren. Grundvoraussetzung ist, dass die personenbezogenen Daten ausschließlich auf im Verantwortungsbereich der Strafverfolgungsbehörden stehenden Servern gespeichert werden, da die Behörden auf diese Weise die größtmögliche Kontrolle über die Daten behalten und den Primärdatensatz selbständig löschen können. Dass Dritte die externen Seiten ihrerseits auf Facebook verlinken oder kopieren können,[196] ist ein generelles Problem der Internetfahndung, das im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen ist.[197] Sofern Dritte von diesen Möglichkeiten Gebrauch gemacht haben, sind sie jedoch ebenfalls zur Löschung verpflichtet und machen sich im Falle der Weigerung ggf. nach den §§ 33 KUG, 13 StGB oder wegen Ehrdelikten strafbar.[198]

Unter Beachtung der aufgestellten Grundsätze entspricht die Facebookfahndung in den möglichen Risiken also der allgemeinen Onlinefahndung, birgt jedoch größere Erfolgschancen.[199] Sie ist daher, sofern eine auch im Einzelfall sehr schwerwiegende Straftat aufgeklärt werden soll und die weiteren Voraussetzungen der §§ 131 ff. StPO vorliegen, zulässig.[200]

---

[194] So *Lohmeier u.a.* (Fn. 7), S. 24.
[195] Vgl. zur Intensität des Grundrechtseingriffs auch *Ihwas* (Fn. 4), S. 281 f.
[196] Vgl. https://www.facebook.com/fahndungennrw?fref=ts (9.3.1015).
[197] So LT-Drs. RP 16/3387, S. 3; vgl. auch *Schiffbauer*, NJW 2014, 1052 (1056 f.).
[198] Vertiefend *Schiffbauer*, NJW 2014, 1052 (1056 f.); *Lohmeier u.a.* (Fn. 7), S. 26; *Gerhold*, Das System des Cyber- und Internetstalking, 2009, S. 151 f.
[199] Vgl. *Hawellek/Heinemeyer*, ZD-Aktuell 2012, 02730.
[200] So LT-Drs. RP 16/3387, S. 3; entsprechend *Lohmeier u.a.* (Fn. 7), S. 24.