Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

7/8
K&R

Editorial: Weckruf für deutsche Großunternehmen? – Der neue Entwurf des IT-Sicherheitsgesetz 2.0 · *Dr. Alexander Golland*

469 Der neue Medienstaatsvertrag – Was gilt für Medienplattformen, Benutzeroberflächen und Medienintermediäre?
Dr. Christoph Enaux und *Dr. Lucas Wüsthof*

476 Datenschutz im Homeoffice – Ein Überblick
Dr. Jan Verheyen und *Daniel Elgert*

479 Datengestützte Wahlwerbung wie Microtargeting aus datenschutzrechtlicher Perspektive · *Tristan Radtke*

486 Beweislastverteilung und Haftungsgrundsätze beim Filesharing
Christian Galetzka und *Erik Stamer*

493 Die Entwicklung des Urheberrechts seit Mitte 2019
Dr. Alexander R. Klett und *Dr. Natascha M. Leyendecker*

500 Aktuelle Herausforderungen für Telekommunikations-überwachungsmaßnahmen durch die Nachrichtendienste
Prof. Dr. Franziska Schneider

506 Länderreport Österreich · *Prof. Dr. Clemens Thiele*

509 EuGH: Verfügbare Telefonnummer im Impressum muss in Widerrufsbelehrung genannt werden

511 BVerfG: Recht auf Chancengleichheit der Parteien durch Veröffentlichung auf Ministeriums-Webseite verletzt

533 BGH: Metall auf Metall IV: Keine Verletzung des Vervielfältigungsrechts durch Übernahme von Audiofragmenten

537 BGH: Rückabwicklung eines Amazon-Marketplace-Kaufvertrags

547 OLG Köln: SmartLaw: Generator für Rechtsdokumente stellt keine erlaubnispflichtige Rechtsdienstleistung dar

553 LG Köln: Unerlaubte TV-Werbung für Online-Glücksspiel
mit Kommentar von *Carsten Bringmann*

564 Glosse: Onlinezensur via Haftung · *Clemens Kochinke*

23. Jahrgang Juli/August 2020 Seiten 469 – 564

dfv Mediengruppe · Frankfurt am Main

der mit ihm in häuslicher Gemeinschaft zusammenlebenden Personen umfasst sein muss und der Datenschutzbeauftragte einzubeziehen ist.[48]

IX. Auftragsverarbeitung

Sofern jemand als Auftragsverarbeiter i. S. d. Art. 28 DSGVO wirkt, ist vor dem Einsatz von Mitarbeitern im Homeoffice zwingend zu prüfen, ob der mit dem Verantwortlichen geschlossene Auftragsverarbeitungsvertrag eine derartige Tätigkeit der eigenen Mitarbeiter und unter welchen Voraussetzungen gestattet.[49] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit empfiehlt dabei in seinem Muster zur Auftragsverarbeitung eine „vorherige ausdrückliche Zustimmung des Verantwortlichen, die erst nach Festlegung angemessener technischer und organisatorischer Maßnahmen für die Verarbeitungssituation erteilt werden kann".[50]

X. Fazit

Datenschutz endete auch schon vor dem Ausbruch der Corona-Krise nicht an der Haustür. Jedoch wird – bedingt durch die Krise – vielen Unternehmen und Unternehmern, die „Umzüge" ins Homeoffice bewerkstelligen mussten, nun erst aufgezeigt worden sein, dass hier nicht nur logistische Herausforderungen warteten und warten, sondern auch rechtliche. Neben dem geplanten Gesetz zur Etablierung eines Anspruchs auf Homeoffice[51] könnten Unternehmen im Übrigen auch weiterhin ein eigenes und gesteigertes Interesse daran haben, nach dem Abklingen der Krise die Möglichkeit für Mitarbeiter, (teilweise) im Homeoffice zu arbeiten, beizubehalten. Man mag es den Verantwortlichen nachsehen, wenn sie die rechtlichen Themen, die mit der Arbeit im Homeoffice verbunden sind, ggf. vernachlässigt haben, um zunächst den Betrieb am Laufen zu halten. (Bewusste) Versäumnisse sollten aber umgehend nachgeholt werden. Denn es ist ebenfalls zu vermuten, dass die Aufsichtsbehörden den verstärkten Wechsel ins Homeoffice aufarbeiten werden.[52] Verantwortliche sind daher gut beraten, sich dem Thema Datenschutz im Homeoffice eingehend zu widmen.

48 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit – „Telearbeit und Mobiles Arbeiten", S. 17, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html.

49 Bereits der Wortlaut von Art. 28 DSGVO gebietet eine entsprechende Vorgehensweise, da er schon zu Beginn festlegt, dass die Auftragsverarbeitung hinreichend Garantien dafür bieten muss, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

50 Abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html., dort § 3 Abs. 9.

51 https://www.handelsblatt.com/politik/deutschland/kein-rechtsanspruch-arbeitgeber-veraergert-ueber-geplantes-recht-auf-homeoffice/25774730.html?ticket=ST-1822245-udtEIBeVWmK4 YV3wpRZp-ap1; https://www.faz.net/aktuell/finanzen/corona-krise-hubertus-heil-will-home-office-per-gesetz-16742512.html.

52 Für eine mögliche Zunahme von Datenschutzgeldbußen im Allgemeinen *Behr/Tannen*, CCZ 2020, 120 ff.

Tristan Radtke, Freiburg i. Br.*

Datengestützte Wahlwerbung wie Microtargeting aus datenschutzrechtlicher Perspektive

Sei es im Bundestagswahlkampf 2017, im Europawahlkampf 2019 oder in den jüngsten Landtagswahlkämpfen: Die deutschen Parteien setzen vermehrt auf einen datengestützten Online- und Haustür-Wahlkampf und dabei auch auf die gezielte Wähleransprache (Microtargeting). Der Beitrag gibt einen Überblick über die Erscheinungsformen datengestützter Wahlwerbung und die datenschutzrechtlichen Implikationen.

I. Der Trend zum datengestützten Wahlkampf

Neben den noch immer nicht vollständig aufgeklärten,[1] zwischenzeitlich durch Netflix verfilmten Vorgängen rund um Cambridge Analytica[2] und den Erfolg von Persönlichkeitsanalysen im Wahlkampf auf Grundlage von Facebook-Profil-Daten, gibt es ihn tatsächlich in den USA: den datengestützten Wahlkampf. Über soziale Netzwerke, Online-Kampagnen, per Telefon und mittels datengestützten Haustürwahlkampfs werden Wähler für einen effizienteren[3] Wahlkampf möglichst zielgerichtet angesprochen[4] – das sog. (politische) Microtargeting.[5]

Auch hierzulande ist der datengestützte Wahlkampf mit seinen unterschiedlichen Facetten angekommen, wenngleich das europäische und deutsche Datenschutzrecht regelmäßig die Ansprache kleiner Gruppen statt einzelner Wähler notwendig werden lässt.

* Der Beitrag wurde anlässlich eines Vortrags des Verfassers im Rahmen der Veranstaltung „Von Brexit bis Bundestagswahl: Wie Microtargeting den Wahlkampf revolutioniert" am 30. 10. 2019 in Passau verfasst und basiert auch auf den dort geschilderten Ausführungen zum Wahlkampf. Internet-Verweise in diesem Beitrag wurden zuletzt abgerufen am 2. 6. 2020. Der Verfasser forscht zur Vornahme einer Systematisierung der Kriterien der gemeinsamen Verantwortlichkeit im Rahmen seines Dissertationsvorhabens. Mehr über den Autor erfahren Sie auf S. VIII.

1 Etwa *Confessore/Hakim*, https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html; *Reinbold/Schnack*, https://www.spiegel.de/netzwelt/netzpolitik/donald-trump-und-die-daten-ingenieure-endlich-eine-erklaerung-mit-der-alles-sinn-ergibt-a-1124439.html.

2 S. die aktualisierte Version des ursprünglichen Artikels *Grassegger/Krogerus*, https://www.tagesanzeiger.ch/ausland/europa/Ich-habe-nur-gezeigt-dass-es-die-Bombe-gibt/story/17474918. Zur rechtlichen Bewertung *Söbbing*, InTeR 2018, 182.

3 *Jungherr/Schoen*, Das Internet in Wahlkämpfen, 2013, S. 123.

4 Dazu ausführlich *Kolany-Raiser/Radtke*, Microtargeting – Gezielte Wähleransprache im Wahlkampf, in: Hoeren (Hrsg.), Phänomene des Big-Data-Zeitalters, 2019, S. 88 - 91.

5 *Barbu*, Advertising, Microtargeting and Social Media, Social and Behavorial Sciences 2014, S. 44, 45 und ursprünglich *Agan*, Silent Marketing: Microtargeting, 2007.

II. Der Online-Wahlkampf über soziale Netzwerke

Im Wahlkampf greifen die deutschen Parteien zunehmend auf zielgerichtete Werbung über soziale Netzwerke wie Facebook oder Twitter zurück, um einzelne Nutzer oder Nutzergruppen über Parameter wie Wohnort, Alter und Interessen über Werbe-Anzeigen gezielt anzusprechen.[6] Die Kampagnen werden in Wahlkampf-Zeiten zum Teil täglich durch die Parteien optimiert. Im Europawahlkampf wurde etwa von den im Bundestag vertretenen Parteien insgesamt deutlich über 1 Million Euro für Wahlwerbung auf Facebook aufgewendet.[7] Twitter hingegen hat sich im vergangenen Jahr entschieden, keine politische Werbung mehr zuzulassen.[8]

1. Anwendbarkeit der DSGVO (Art. 2, 3, 4 Nr. 1, 2 DSGVO)

Schon unter der Datenschutz-RL 95/46/EG zeichnete sich spätestens seit der Google-Spain-Entscheidung des EuGH[9] eine Tendenz hin zu einem weiten Anwendungsbereich – im Rahmen der Entscheidung durch ein weites Verständnis des Begriffs des Verantwortlichen – ab. Die Verarbeitung personenbezogener Daten durch US-Konzerne, um gegenüber deutschen Nutzern zielgerichtet Anzeigen ausspielen zu können und im Übrigen die Nutzung des Portals zu ermöglichen, fällt aufgrund der EU-Niederlassungen nach Art. 3 Abs. 1 DSGVO oder ggf. nach Art. 3 Abs. 2 lit. a, b DSGVO in den räumlichen Anwendungsbereich der DSGVO. Soweit die deutschen Parteien mit dem sozialen Netzwerk (gemeinsam) verantwortlich sind, kann der räumliche Anwendungsbereich auch gegenüber dem sozialen Netzwerk eröffnet sein.[10]

Die Parteien – unabhängig davon, wie dies im Hinblick auf die Fraktionen im Rahmen der parlamentarischen Tätigkeiten nach Art. 2 Abs. 2 lit. a DSGVO einzuordnen ist[11] – unterfallen auch in persönlicher und sachlicher Hinsicht dem Anwendungsbereich der DSGVO. Die Bereichsausnahme aus Art. 2 Abs. 2 lit. c DSGVO für ausschließlich persönliche oder familiäre Tätigkeiten greift nicht. Andernfalls hätte sich der EU-Gesetzgeber in Erwägungsgrund 56 DSGVO nicht mit Erlaubnistatbeständen für Datenverarbeitungen durch politische Parteien im Zusammenhang mit Wahlen auseinandersetzen müssen. Insoweit ist der Anwendungsbereich nach Art. 2, 4 Nr. 1, 2 DSGVO bei der Verarbeitung der personenbezogenen Profil- und Werbe-Daten ebenfalls eröffnet.

2. Erlaubnistatbestand (Art. 6, 9 DSGVO) und Informationspflichten (Art. 13, 14 DSGVO)

Soweit sich beim Microtargeting über soziale Netzwerke Rückschlüsse auf die politische Meinung einer natürlichen Person ziehen lassen, handelt es sich nach Art. 9 Abs. 1 DSGVO um eine grundsätzlich unzulässige Verarbeitung besonderer Kategorien personenbezogener Daten. Damit ist ein besonderer Erlaubnistatbestand nach Art. 9 Abs. 2 DSGVO notwendig. Selbst wenn die Nutzer keine Angaben zu ihrer politischen Einstellung machen, können entsprechende Daten-Kategorien bei der Auswertung von Klicks auf politische Werbe-Anzeigen vorliegen.[12]

Facebook beispielsweise gibt an, dass Daten über politische Einstellungen verarbeitet werden können.[13] Zugleich wird jedoch nur auf die Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) sowie den Schutz lebenswichtiger (Art. 9 Abs. 2 lit. c DSGVO) und öffentlicher Interessen (Art. 9 Abs. 2 lit. g, i und j DSGVO) als mögliche Erlaubnistatbestände nach Art. 9 Abs. 2 DSGVO verwiesen. Das offensichtliche, d. h. auf eindeutige Veranlassung[14] der betroffenen Person, Öffentlichmachen (Art. 9 Abs. 2 lit. e DSGVO), das ohnehin nur bei einem öffentlich zugänglichen Nutzer-Profil in Betracht kommt,[15] wird schon gar nicht erwähnt. Soweit Verarbeitungen tatsächlich auf diesen Erlaubnistatbestand gestützt werden, wird mangels Erwähnung dem Erfordernis nach Art. 13 Abs. 1 lit. c, 14 Abs. 1 lit. c DSGVO nicht Genüge getan. Andernfalls bleibt im Zusammenhang mit Wahlwerbung auf dem sozialen Netzwerk nur noch die (ausdrückliche) Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO. Im Rahmen der Prüfung der Einwilligung sind angesichts der Form und der Länge der mit der Registrierung „akzeptierten" datenschutzrechtlichen Regelungen insbesondere der Transparenz der Einholung sowie Informiertheit und Freiwilligkeit der Einwilligung (vgl. Art. 4 Nr. 11, 7 Abs. 2, 4 DSGVO) besondere Beachtung zu schenken.[16]

Die Komplexität und der Umfang der Datenverarbeitungen auf den sozialen Netzwerken erhöhen das Risiko von Verstößen gegen den Transparenzgrundsatz (Art. 5 Abs. 1 lit. a DSGVO) und seine Ausprägungen, wie die Informationspflichten nach Art. 13, 14 DSGVO.

3. Gemeinsame Verantwortlichkeit (Art. 4 Nr. 7, 26 DSGVO)

Entscheidend ist aus Sicht der Parteien im Fall der Wahlwerbung, ob diese nach Art. 4 Nr. 7, Art. 26 Abs. 1 S. 1 DSGVO gemeinsam mit dem sozialen Netzwerk für die Verarbeitungen verantwortlich sind, da sie gemeinsam über Zwecke und Mittel der Datenverarbeitung entscheiden. Im Fall der gemeinsamen Verantwortlichkeit ist der Abschluss einer Vereinbarung (Art. 26 Abs. 1 S. 2, 3, Abs. 2 DSGVO) notwendig. Zudem besteht durch die Einstufung als Verantwortlicher ein erweitertes Haftungsrisiko bei Verstößen gegen datenschutzrechtliche Vorgaben aufgrund möglicher Schadensersatzansprüche betroffener Personen (Art. 82 DSGVO) und behördlicher Aufsichtsmaßnahmen (Art. 58, 83, 84 DSGVO).[17] Darüber hinaus kann sich das Haftungsrisiko im Fall einer gemeinsamen Verantwortlichkeit mit der Funktion des Verantwortlichen als weitere „Anlaufstelle" und Passivlegitimierten gegenüber der betroffenen Person (vgl. Art. 26 Abs. 3 DSGVO)

6 https://de-de.facebook.com/business/ads.

7 *Hegelich/Serrano*, https://www.medienanstalt-nrw.de/fileadmin/user_upload/Studie_Microtargeting_DeutschlandEuropawahl2019_Hegelich__1_.pdf, S. 5. S. für den Europawahlkampf https://political-dashboard.com/europe-de.html.

8 *Sterz/Borgers*, https://www.deutschlandfunk.de/twitter-verbietet-wahlwerbung-was-genau-ist-politisch.2907.de.html?dram:article_id=462315. Zu Transparenz bei sozialen Netzwerken auch *Künast*, ZRP 2019, 62, 65.

9 EuGH, 13. 5. 2014 – C-131/12, K&R 2014, 502 ff. = WRP 2014, 805 – Google Spain.

10 *Hanloser*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 31. Edition – Stand 1. 2. 2020, Art. 3 Rn. 11.

11 *Grzeszick*, NVwZ 2018, 1505, 1508.

12 Einzelfallabhängig *Schiff*, in: Ehmann/Selmayr (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 9 Rn. 22.

13 S. unter „Welche Arten von Informationen erfassen wir?", https://de-de.facebook.com/policy.php.

14 *Schulz*, in: Gola (Hrsg.), DSGVO, 2. Aufl. 2018, Art. 9 Rn. 26.

15 *Nebel*, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, 2015, S. 89, 103.

16 LG Berlin, 16. 1. 2018 – 16 O 341/15, K&R 2018, 269; *Rothmann/Buchner*, DuD 2018, 342; *Uecker*, ZD 2019, 248, 248 f.; *Tinnefeld/Conrad*, ZD 2018, 391, 392 und 394.

17 Vgl. das Vorgehen gegen den Facebook-Fanpage-Betreiber, EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475 – Wirtschaftsakademie Schleswig-Holstein und die Entscheidungen der Instanzgerichte.

im Hinblick auf weitere Datenverarbeitungsvorgänge erhöhen.[18]

Für den Fall von Facebook-Fanpage-Betreibern nahm der EuGH mit Blick auf die damalige Ausgestaltung der Fanpage-Funktionalität bereits eine gemeinsame Verantwortlichkeit von Facebook und dem Facebook-Fanpage-Betreiber an.[19] Der EuGH betonte die Notwendigkeit einer weiten Auslegung der Verantwortlichkeit für einen umfassenden Schutz betroffener Personen.[20] Es kommt für die Einordnung als (gemeinsam) Verantwortlicher auf einen (tatsächlichen[21]) Entscheidungsbeitrag an.[22] Diese stark einzelfallbezogene[23] und noch unter der Datenschutz-RL 95/46/EG ergangene Entscheidung lässt sich angesichts des insoweit übereinstimmenden Wortlauts im Wesentlichen auf die DSGVO übertragen.[24] Aus den Entscheidungen Zeugen Jehovas[25] und Fashion ID,[26] bei denen sich der EuGH ebenfalls zu dem Vorliegen gemeinsamer Verantwortlichkeit äußern konnte, ergibt sich insoweit nichts Abweichendes im Hinblick auf die Einordnung der Verantwortlichkeit für die mit den Werbe-Anzeigen in Zusammenhang stehenden Verarbeitungsvorgänge. Für die Einordnung bietet sich eine Differenzierung zwischen den Zwecken, Mitteln und der Gemeinsamkeit der Entscheidung an, wenngleich sich die Aussagen aus der Entscheidung diesen Kriterien nicht immer trennscharf zuordnen lassen.

a) Zwecke

Facebook verfolgt mit der Datenverarbeitung den Zweck, das Werbe-System zu verbessern.[27] Der Fanpage-Betreiber hingegen kann die Vermarktung seiner Tätigkeit leichter steuern und beispielsweise seiner Zielgruppe zukünftig relevantere Inhalte anzeigen.[28] Diese Zwecke der besseren Vermarktung sind eng miteinander verknüpft.[29]

Bei der Schaltung von Werbe-Anzeigen verfolgt das soziale Netzwerk ebenfalls den Zweck, das Werbe-System zu verbessern und die Nutzer-Interessen – namentlich die politische Einstellung – zuverlässiger einschätzen zu können. Der Werbende will die Vermarktung steuern, zielgerichtet potenziell interessierte Nutzer ansprechen und zusätzliche Besucher und „Fans" gewinnen.

b) Mittel

Facebook stellt mit der Plattform ein zentrales Mittel zur Datenverarbeitung bereit.[30] Der Fanpage-Betreiber konnte eine Parametrierung vornehmen, d. h. Kriterien festlegen, nach denen Facebook bestimmten Facebook-Nutzern Meldungen der Fanpage häufiger anzeigt.[31] Mittlerweile stellt Facebook diese, teilweise als zentral angesehene[32] Funktion nicht mehr bereit. Der Fanpage-Betreiber erhält nach wie vor Statistiken, die sog. Insights. Durch die auf seiner Fanpage bereitgestellten Inhalte und durchgeführten Interaktionen (z. B. „Liken" von Inhalten) beeinflusst er weiterhin maßgeblich die Zielgruppe und nimmt so entscheidenden Einfluss darauf, zu welchen betroffenen Personen er aggregierte Statistiken erhält.

Facebook stellt auch für die Einblendung von Werbe-Anzeigen seine Plattform bereit. Im Rahmen von Werbe-Anzeigen besteht weiterhin die Möglichkeit zur Parametrierung durch den Werbenden. Der Werbende stellt zielgerichtet, z. B. anhand von Aufenthaltsort, Alter und Interessen, ein, welcher Zielgruppe seine Werbe-Anzeigen angezeigt werden. Der Werbende kann gar – als besonders gewichtigen Beitrag – Daten eigener Kunden oder Nutzer an das soziale Netzwerk übertragen, um Facebook ähnliche Nutzer finden zu lassen (sog. Lookalike Audiences[33]).

c) Gemeinsame Entscheidung

Diese Entscheidung müsste auch gemeinsam sein. Der Beteiligung an einer Entscheidung[34] und der Gemeinsamkeit stehen nicht vertragliche Einschränkungen[35] zulasten eines Beteiligten entgegen, wonach dieser keinen Zugriff auf die personenbezogenen Daten hat.[36] Die bloße Nutzung von Facebook alleine – das jedenfalls einen bestimmenden Einfluss hat[37] – ist noch nicht ausreichend.[38] Besonders hervorgehoben wurde die öffentliche Zugänglichkeit der Fanpage als Internetseite, sodass auch personenbezogene Daten von Nicht-Facebook-Nutzern verarbeitet werden könnten.[39] Die Facebook-Fanpage ist letztlich vergleichbar mit einer selbst gehosteten Website, mit dem Unterschied, dass Facebook als Webhoster einen vergleichsweise großen Einfluss behält und (mit)entscheidet, welche verfügbaren Daten an den Facebook-Fanpage-Betreiber weitergegeben werden. Der Fanpage-Betreiber eröffnet und betreibt die Fanpage in Kenntnis der Umstände der Datenverarbeitungen.[40]

Die Verarbeitungen im Rahmen der Werbe-Anzeigen betreffen gerade keine Nutzer außerhalb von Facebook. Diese vom EuGH hervorgehobene Besonderheit entfällt, und es liegt daher auf den ersten Blick nahe, die Schaltung der Werbe-Anzeigen als bloße Nutzung von Facebook – als Werbenetzwerk und Anbieter von Online-Inhalten zugleich (Onsite-Werbung)[41] – und daher als keinen darüber hinausgehenden eigenen Entscheidungsbeitrag einzuordnen. Bei Werbe-Anzeigen besteht jedoch statt im Rahmen

18 Dafür *Hartung*, in: Kühling/Buchner (Hrsg.), DSGVO BDSG, 2. Aufl. 2018, Art. 26 Rn. 28. A. A. *Kartheuser/Nabulsi*, MMR 2018, 717, 720; *Lee/Cross*, MMR 2019, 559, 562.
19 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 44 – Wirtschaftsakademie Schleswig-Holstein. Bestätigend BVerwG, 11. 9. 2019 – 6 C 15.18, K&R 2020, 165, Rn. 23.
20 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 28 – Wirtschaftsakademie Schleswig-Holstein.
21 Generalanwalt Bot, 24. 10. 2017 – C-210/16, Rn. 54 und 57 – Wirtschaftsakademie Schleswig-Holstein.
22 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 31 – Wirtschaftsakademie Schleswig-Holstein.
23 *Marosi/Matthé*, ZD 2018, 357, 362.
24 *Marosi/Matthé*, ZD 2018, 357, 362. Krit. *Moos/Rothkegel*, MMR 2018, 591, 598.
25 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056 – Zeugen Jehovas.
26 EuGH, 29. 7. 2019 – C-40/17, K&R 2019, 562 – Fashion ID.
27 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 34 – Wirtschaftsakademie Schleswig-Holstein.
28 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 34 – Wirtschaftsakademie Schleswig-Holstein.
29 Generalanwalt Bot, 24. 10. 2017 – C-210/16, Rn. 58 – Wirtschaftsakademie Schleswig-Holstein. Zu der Notwendigkeit der Verknüpfung *Gierschmann*, ZD 2020, 69, 70; *Moos/Rothkegel*, MMR 2019, 579, 585.
30 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 40 – Wirtschaftsakademie Schleswig-Holstein.
31 Vgl. EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 36 – Wirtschaftsakademie Schleswig-Holstein; https://allfacebook.de/fbmarketing/audience-optimization.
32 *Marosi/Matthé*, ZD 2018, 357, 362; *Moos/Rothkegel*, MMR 2018, 591, 598.
33 https://allfacebook.de/fbmarketing/audience-optimization.
34 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 39 – Wirtschaftsakademie Schleswig-Holstein.
35 Generalanwalt Bot, 24. 10. 2017 – C-210/16, Rn. 61 – Wirtschaftsakademie Schleswig-Holstein.
36 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 38 – Wirtschaftsakademie Schleswig-Holstein.
37 Generalanwalt Bot, 24. 10. 2017 – C-210/16, Rn. 73 – Wirtschaftsakademie Schleswig-Holstein.
38 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 35 – Wirtschaftsakademie Schleswig-Holstein.
39 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 41 – Wirtschaftsakademie Schleswig-Holstein.
40 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 32 – Wirtschaftsakademie Schleswig-Holstein; *Moos/Rothkegel*, MMR 2018, 591, 598.
41 Artikel-29-Datenschutzgruppe, WP 171 – Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, S. 5 f.

der *Herkunft* der Besucher im Rahmen des *Ziels* der Besucher eine Besonderheit: Bei der Weiterleitung auf eine Website erfährt der Website-Betreiber, in der Regel also der Werbende, die IP-Adresse und ggf. auch die Kampagnen-Nummer.[42] Er kann also dem konkreten Nutzer[43] die im Rahmen der Kampagne definierte Zielgruppe zuordnen. Da der Werbende sowohl anfangs durch die Parametrierung – und ggf. auch über die Bereitstellung von Nutzer-Daten – als auch nach dem Werbe-Klick über den Kreis potenziell betroffener Personen mitentscheidet und nach dem Werbe-Klick den betroffenen Personen weitere Informationen zuordnen kann, handelt es sich um eine gemeinsame Entscheidung im Hinblick auf den gesamten Anzeigen-Vorgang. Ein Übergang zu einer „Phase"[44] getrennter Verantwortlichkeit ab dem Werbe-Klick scheidet angesichts der sich durchgehend auswirkenden Parametrierung im Vorfeld aus.[45]

d) Folgen gemeinsamer Verantwortlichkeit

Die gemeinsame Verantwortlichkeit von Facebook und dem Werbenden führt nicht zwangsläufig zu einer gleichwertigen Verantwortlichkeit.[46] Zudem erstreckt sich die gemeinsame Verantwortlichkeit nicht auf Verarbeitungsprozesse auf Facebook über die konkreten Werbe-Anzeigen hinaus.[47] Im Hinblick auf etwaige Sanktionen wie Bußgelder – etwa bei unzureichender Information der Betroffenen – sind neben dem Grad der Verantwortung (Art. 83 Abs. 2 S. 2 lit. d DSGVO) auch etwaige Maßnahmen zur Minderung der Folgen des Verstoßes zu berücksichtigen (Art. 83 Abs. 2 S. 2 lit. c DSGVO). Sollte etwa die von Facebook zur Verfügung gestellte Vereinbarung[48] und die Information hierüber nicht den Anforderungen des Art. 26 Abs. 1 S. 2, Abs. 2 DSGVO entsprechen, wären Bemühungen, mit Facebook eine den Anforderungen entsprechende Vereinbarung abzuschließen und den Nutzern das Wesentliche der Vereinbarung zur Verfügung zu stellen, im Hinblick auf diesen konkreten Verstoß zu berücksichtigen.

III. Der datengestützte Haustürwahlkampf

In dem datengestützten Haustürwahlkampf in Deutschland zeigen den Parteien sog. Potenzial-Analysen, in welchen Gruppen mehrerer (in der Regel mindestens sechs)[49] zusammengefasster Haushalte und in welchen Straßenzügen Wahlkampf-Teams eingesetzt werden sollten.[50] Das konkrete Feedback der Wahlkampf-Helfer zu einzelnen Haustürbesuchen ermöglicht die Optimierung der Analysen.

1. Wähler-Daten

Die Parteien verwenden besondere Anstrengungen darauf, schon gar nicht dem sachlichen Anwendungsbereich der DSGVO (Art. 2 DSGVO) zu unterfallen.

a) Sachliche Anwendbarkeit der DSGVO (Art. 2, 4 Nr. 1, 2 DSGVO)

Angesichts des weiten Begriffs der Verarbeitung nach Art. 2 Abs. 1, Art. 4 Nr. 2 DSGVO und der Anwendbarkeit auf jegliche (teil-)automatisierte Verfahren wäre diese Hürde für die Anwendbarkeit ohne Weiteres genommen.

Entscheidend kommt es im Rahmen der Anwendbarkeit darauf an, ob personenbezogene Daten vorliegen. Nach Art. 4 Nr. 1 DSGVO müssten die im Wahlkampf verarbeiteten Informationen „sich auf eine identifizierte oder identifizierbare natürliche Person" beziehen. Als Beispiel wird unter anderem die Zuordnung mittels Namen oder Standortdaten genannt. Ein positives Gesprächsfeedback in Kombination mit einer Anschrift[51] lässt sich auf eine natürliche Person zurückführen. Dies gilt jedenfalls dann, wenn nicht mehrere natürliche Personen unter dieser Anschrift wohnen.

Die Wahlkampf-Apps der Parteien ermitteln daher bereits auf dem Smartphone des Wahlkampf-Helfers anhand des Standorts einen Straßenzug und übermitteln nur diesen, nicht aber die genaue Anschrift, an die Server der Partei.[52] Solange und soweit sichergestellt ist, dass tatsächlich mehrere natürliche Personen in diesem Straßenzug wohnen, handelt es sich um nicht-personenbezogene, mithin anonyme[53] Daten. Abhängig von den Einzelheiten des angewendeten Verfahrens kann die DSGVO ggf. auf die Anonymisierung selbst Anwendung finden.[54] Zumindest nach der Anonymisierung ist die DSGVO sachlich nicht anwendbar, Art. 2 Abs. 1 DSGVO.

Anders kann es zu beurteilen sein, wenn Daten verschiedener Quellen kombiniert werden und Daten über mehrere Wahlkämpfe hinweg zusammengeführt werden. Je mehr Datenquellen kombiniert werden, desto größer ist die Wahrscheinlichkeit, dass sich Rückschlüsse auf einzelne natürliche Personen ziehen lassen. Man denke beispielsweise an einen Straßenzug, in dem sich über zwei Wahlkämpfe hinweg nur ein positives Gesprächsfeedback erzielen ließ. Alle anderen Gespräche in diesem Straßenzug wurden als neutral oder negativ bewertet. Zieht nun eine natürliche Person aus und wird im dritten Wahlkampf kein einziges positives Gesprächsfeedback mehr erfasst, lässt sich unter Zuhilfenahme weiterer, den Parteien möglicherweise zugänglicher Datenquellen ermitteln, wer der der Partei positiv Gesinnte war. Unter Berücksichtigung dieser den Parteien womöglich zustehenden „Hilfsmittel" liegt dann ein Personenbezug vor.[55] Mit einer steigenden Anzahl an Microtargeting-Wahlkämpfen können sich diese Einzelfälle häufen und zu einer vermehrten sachlichen Anwendbarkeit der DSGVO führen.

Hinzu kommt, dass die Wahlkampf-Helfer, je nach Partei, frei in ihrer Entscheidung sind, welche Haushalte sie besuchen. Dies birgt ein Missbrauchspotenzial, indem in einem Straßenzug unter Umständen gar nicht mehrere, sondern beispielsweise nur ein Haushalt besucht und dessen Feedback erfasst wird. Unter Zuhilfenahme weiterer Informationen, z. B. wenn erkennbar nur jeweils das erste Haus in mehreren Straßenzügen angesteuert wurde, steigt

42 Vgl. Artikel-29-Datenschutzgruppe, WP 171 – Stellungnahme 2/2010 zur Basis von Behavioural Targeting, S. 15.
43 Vgl. EuGH, 19. 10. 2016 – C-582/14, K&R 2016, 811, Rn. 48 f. – Breyer.
44 EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 43 – Wirtschaftsakademie Schleswig-Holstein.
45 Einer solchen getrennten Phase zugeneigt Artikel-29-Datenschutzgruppe, WP 171 – Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, S. 15.
46 Vgl. EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 43 – Wirtschaftsakademie Schleswig-Holstein.
47 Vgl. *Moos/Rothkegel*, MMR 2018, 591, 597.
48 https://de-de.facebook.com/legal/terms/page_controller_addendum.
49 Dazu und auch zu dem zeitweise öffentlich zugänglichen Wahlkampf-Portal der FDP mit Analysen *Hegelich*, http://politicaldatascience.blogspot.com/2017/08/fdpleaks-hype-und-hybris-im.html.
50 *Keller/Schlieter*, https://www.berliner-zeitung.de/politik/bundestagswahl/microtargeting-im-bundestagswahlkampf-nah-am-waehler-und-anfaellig-fuer-manipulation-28137412.
51 Vgl. *Klar/Kühling*, in: Kühling/Buchner (Fn. 18), Art. 4 Nr. 1 Rn. 18.
52 Dazu auch Abgeordnetenhaus Berlin, Drs. 18/1253, S. 129.
53 Vgl. Erwägungsgrund 26 S. 5 DSGVO.
54 Vgl. BfDI, Öffentl. Konsultationsverfahren – Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 10. 2. 2020, S. 5 f.
55 Vgl. EuGH, 19. 10. 2016 – C-582/14, K&R 2016, 811, Rn. 48 f. – Breyer.

die Wahrscheinlichkeit eines Personenbezugs. Soweit ein Personenbezug vorliegt, ist die DSGVO auch sachlich und räumlich anwendbar. Insbesondere greift im Hinblick auf keinen Beteiligten die Ausnahme nach Art. 2 Abs. 2 lit. c DSGVO, da die Daten potenziell zahlreichen Wahlkampf-Helfern und -Organisatoren zugänglich sind[56] und die Tätigkeit des Haustürwahlkampfs die Ansprache von Personen umfasst, die nicht zu dem Haushalt der Wahlkämpfer gehören.[57] Daher wären die weiteren Vorgaben – insbesondere die im Folgenden dargestellten – zu beachten.

b) Besonderer Erlaubnistatbestand (Art. 9 DSGVO)

Da das Gesprächsfeedback Rückschlüsse auf die politische Meinung einer natürlichen Person zulässt, kommen erneut nur die besonderen Erlaubnistatbestände aus Art. 9 Abs. 2 DSGVO in Betracht.

Die Wahlkampf-Helfer holen im Vertrauen auf die erfolgreiche Aggregation der Daten keine ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) der betroffenen Personen an der Haustür ein. Im Übrigen würde ein derartiges Vorgehen mangels Bereitschaft der betroffenen Personen die Zahl der verfügbaren Datensätze vermutlich erheblich reduzieren und ist daher nicht gewollt. Der besondere Erlaubnistatbestand der ausdrücklichen Einwilligung kommt mithin nicht in Betracht.

Nach dem Privileg für Tendenzbetriebe (Art. 9 Abs. 2 lit. d DSGVO) dürfen beispielsweise Parteien als Organisationen ohne Gewinnerzielungsabsicht im Rahmen ihrer Tendenz (nur)[58] politische Daten verarbeiten. Das Privileg ist auf die interne Verarbeitung der Daten von Mitgliedern und nachhaltig Interessierten beschränkt.[59] Eine Verarbeitung zu Werbezwecken unterfällt regelmäßig nicht dem Tatbestand.[60] Selbst Parteien handeln bei (Wahl-)Werbung nicht mehr im Rahmen ihrer Tendenz bzw. „im Zusammenhang mit [ihrem] Tätigkeitszweck" (Art. 9 Abs. 2 lit. d DSGVO), obwohl diese Wahlwerbung zu ihrem Kerngeschäft zählt. Dies zeigt in systematischer Hinsicht der Erwägungsgrund 56 DSGVO – der Erwägungsgrund 51 a. E. DSGVO konkretisiert –, wonach die Verarbeitung politischer Daten im Zusammenhang mit Wahlen zugelassen werden *kann* („may be permitted"), nicht aber zugelassen ist. Für eine Bezugnahme des Erwägungsgrunds 56 DSGVO stattdessen auf die Öffnungsklausel des Art. 9 Abs. 2 lit. g DSGVO spricht nicht zuletzt, dass nach dem Erwägungsgrund geeignete Garantien notwendig sind. Dies erinnert eher an den Wortlaut des lit. g als an den des lit. d. Auch der Erlaubnistatbestand aus Art. 9 Abs. 2 lit. d DSGVO steht den Parteien mithin nicht zur Seite.

Art. 9 Abs. 2 lit. e DSGVO ist ebenfalls nicht einschlägig. Bloße Mitteilungen in einem „Haustürgespräch" sind mangels Mitteilung an einen unbestimmten Personenkreis[61] und damit mangels Öffentlichmachens nicht erfasst. Eine Veröffentlichung von Feedback-Daten über die Partei hinaus ist auch durch die Parteien nicht gewollt.[62] Andernfalls würden jedenfalls eine beiläufige Erwähnung des beabsichtigten Öffentlichmachens und die einfache Zustimmung des Betroffenen nicht ausreichen, da sonst die Anforderungen an eine Einwilligung aus Art. 4 Nr. 11, 7 DSGVO unterlaufen werden würden.

Sieht man in Wahlwerbung durch die Parteien in Zusammenschau mit dem Erwägungsgrund 56 DSGVO ein erhebliches öffentliches Interesse, kommt Art. 9 Abs. 2 lit. g DSGVO als besonderer Erlaubnistatbestand in Betracht.[63] Es fehlt allerdings, abgesehen von § 50 Abs. 1 BMG, an entsprechenden Regelungen, die die Verarbeitungen zu Zwecken der zielgerichteten Wahlkampf-Werbung zulassen.[64]

Es würde daher an einem besonderen Erlaubnistatbestand fehlen und die Verarbeitung wäre nach Art. 9 Abs. 1 DSGVO unzulässig.

c) Informationspflichten (Art. 13, 14 DSGVO)

Auch bei ungewolltem, „zufälligem" Personenbezug handelt es sich im Umkehrschluss zu Erwägungsgrund 26 S. 6 DSGVO um personenbezogene Daten und die betroffenen Personen sind grundsätzlich nach Art. 13, 14 DSGVO zu informieren. Während Art. 13 DSGVO die Direkterhebung („bei der betroffenen Person") voraussetzt, ist Art. 14 DSGVO in den übrigen Fällen – insbesondere also bei Erlangung aus einer anderen Quelle – einschlägig.[65] Das Gesprächsfeedback wird im Anschluss des Gesprächs auf Basis einer Bewertung des Wahlkampf-Helfers erfasst. Die betroffene Person ist sich diesbezüglich also gerade nicht, wie in der Situation des Art. 13 DSGVO, bewusst, dass sie Informationen über sich „aus der Hand gibt".[66] Stattdessen stammen die Feedback-Daten aus einer anderen Quelle und Art. 14 DSGVO ist maßgeblich, sodass nach Art. 14 Abs. 5 DSGVO ein umfangreicher(er) Katalog an Ausnahmetatbeständen in Betracht kommt.

Zunächst ist daran zu denken, dass die Erteilung der Informationen sich als unmöglich erweisen oder einen unverhältnismäßigen Aufwand erfordern könnte (Art. 14 Abs. 5 lit. b Var. 1 und 2 DSGVO), wobei ggf. stattdessen eine Information der Öffentlichkeit notwendig sein kann (Art. 14 Abs. 5 lit. b a. E. DSGVO). Selbst wenn die Parteien mit zusätzlichen Informationen – an die sie z. B. mithilfe des Einwohnermeldeamts nach § 50 Abs. 1 BMG gelangen können – Betroffene vollständig identifizieren könnten, ist dies zum einen mit einem erheblichen Aufwand verbunden, da Zehntausende Datensätze geprüft werden müssten, um einzelne betroffene Personen ausfindig zu machen. Zum anderen wäre dies mit weiteren Verarbeitungen verbunden, die nach der Wertung des Art. 11 Abs. 1 DSGVO womöglich nicht gewollt sind.[67]

Art. 14 Abs. 5 lit. b Var. 2 DSGVO (Unverhältnismäßigkeit) ist jedoch eng auszulegen.[68] Im Rahmen der Unverhältnismäßigkeit sind die Risiken für die betroffenen Personen und das Informationsinteresse dieser zu berücksichtigen.[69] Die Zahl der betroffenen Personen kann ebenfalls berücksichtigt werden.[70] Wenn ein Verantwortlicher zahlreiche Datenquellen über mehrere Wahlkämpfe hinweg

56 Vgl. EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 42 und 45 – Zeugen Jehovas.
57 Vgl. EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 42 und 44 – Zeugen Jehovas.
58 Vgl. *Weichert*, in: Kühling/Buchner (Fn. 18), Art. 9 Rn. 74.
59 *Frenzel*, in: Paal/Pauly (Hrsg.), DSGVO BDSG, 2. Aufl. 2018, Art. 9 Rn. 34.
60 *Weichert*, in: Kühling/Buchner (Fn. 18), Art. 9 Rn. 74.
61 *Schiff*, in: Ehmann/Selmayr (Fn. 12), Art. 9 Rn. 45.
62 Vgl. *Hegelich*, https://www.berliner-zeitung.de/politik/bundestagswahl/microtargeting-im-bundestagswahlkampf-nah-am-waehler-und-anfaellig-fuer-manipulation-28137412.
63 *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 9 Rn. 68.
64 Vgl. *Weichert*, in: Kühling/Buchner (Fn. 18), Art. 9 Rn. 168.
65 Vgl. Erwägungsgrund 61 S. 1 DSGVO.
66 Vgl. *Franck*, in: Gola (Fn. 14), Art. 13 Rn. 4.
67 Differenziert *Bäcker*, in Kühling/Buchner (Fn. 18), Art. 14 Rn. 54.
68 *Knyrim*, in: Ehmann/Selmayr (Fn. 12), Art. 14 Rn. 45.
69 *Bäcker*, in Kühling/Buchner (Fn. 18), Art. 14 Rn. 55. Vgl. auch Art. 14 Abs. 5 lit. b a. E. DSGVO.
70 Vgl. Erwägungsgrund 62 S. 3 DSGVO, wenngleich sich dieser nicht ausdrücklich auf Art. 14 Abs. 5 lit. b Var. 2 DSGVO im Allgemeinen bezieht.

kombiniert und damit sehenden Auges – und damit auch entgegen Art. 24 Abs. 1 S. 1 DSGVO – die Gefahr „zufälliger" Personenbezüge schafft, liegt regelmäßig kein unverhältnismäßiger Aufwand vor, sodass die Ausnahme nach Art. 14 Abs. 5 lit. b Var. 2 DSGVO nicht greift. Angesichts der Verarbeitung besonderer Kategorien personenbezogener Daten ist das Informationsinteresse nämlich höher zu gewichten. Zudem wird die Zahl der betroffenen Personen (auch) bezüglich der neu erhobenen Daten[71] mit jedem Wahlkampf steigen. Der Aufwand lässt sich durch den Einsatz von Big-Data-Techniken[72] bei der Identifizierung der entsprechenden Datensätze reduzieren.

d) Weitere Pflichten

Daneben bestehen weitere Pflichten der Verantwortlichen.[73] Die Verarbeitung besonderer Kategorien personenbezogener Daten erhöht das Risiko für die Rechte und Freiheiten natürlicher Personen und lässt daher die Anforderungen, etwa an zu treffende technische und organisatorische Maßnahmen nach Art. 32 DSGVO, steigen.[74]

e) (Gemeinsame) Verantwortlichkeit (Art. 4 Nr. 7, 26 DSGVO)

Im Rahmen des Haustürwahlkampfs sind neben der Partei auch die Wahlkampf-Helfer, die von Tür zu Tür gehen, beteiligt. Daher stellt sich die Frage nach den Rollen der Beteiligten unter der DSGVO.

Für die Einordnung bietet sich ein Vergleich mit der Konstellation der Verkündungstätigkeit der Zeugen Jehovas an. Diese unter der Datenschutz-RL 95/46/EG ergangene EuGH-Entscheidung lässt sich im Hinblick auf das Vorliegen gemeinsamer Verantwortlichkeit auf die DSGVO übertragen.[75]

Bei der Verkündungstätigkeit der Zeugen Jehovas ist der Zweck eng verbunden mit dem Eigeninteresse des Verkündenden[76] und dem Interesse der Gemeinschaft an einer Weiterverbreitung des Glaubens.[77] Bei den Haustürbesuchen der Parteien und der Feedback-Aufzeichnung (z. B. positiv, neutral oder negativ sowie ggf. Schätzung des Alters)[78] besteht ein Eigeninteresse des Wahlkampf-Helfers aus politischer Überzeugung und ggf. aufgrund von Belohnungseffekten durch Gamification-Elemente[79] in der App. Zugleich erfolgen diese im Interesse der Partei.

Der einzelne Verkünder nutzt keine bereitgestellten Formulare (mehr),[80] sondern fertigt eigene (Papier-)Aufzeichnungen an[81] und gestaltet insoweit die Mittel der Datenverarbeitung mit. Die Gemeinschaft der Zeugen Jehovas organisiert die Verkündungstätigkeit durch die Einteilung von Bezirken[82] und das Führen von Listen mit Haushalten, die einen Besuch nicht wünschen.[83] Zudem gibt die Gemeinschaft Anleitungen[84] und ermuntert die Verkünder.[85] Bei dem Haustürwahlkampf stellt die Partei durch Wahlkampf-Vorbereitungen und die Bereitstellung einer Smartphone-App oder eines Portals zentrale Mittel bereit. Der Anteil der Wahlkampf-Helfer beschränkt sich auf die Eingabe des Feedbacks und ggf. Auswahl der konkret anzusteuernden Haustüren. Dabei bleibt ihm jedoch weiterhin ein gewisser, ausreichender Spielraum und er ist nicht strikt weisungsgebunden.

Für das Vorliegen einer gemeinsamen Entscheidung sind weder der Zugriff durch die Wahlkampf-Helfer auf etwaige personenbezogene Daten[86] noch schriftliche Anweisungen einer Stelle notwendig.[87] Gerade demokratisch aufgebaute Parteien (Art. 21 Abs. 1 S. 3 GG) sind ein Beispiel par excellence für das (demokratische) Zusammenwirken zahlreicher Entscheidungsträger. Dies zeigt sich besonders im Haustürwahlkampf, bei dem das Mitglied nicht nur im Rahmen der möglichen Übernahme einer Parteifunktion für die übergeordnete Wahlkampf-Organisation, sondern auch als Wahlkampf-Helfer mitentscheiden kann, welche Haushalte angesteuert werden und wie ein Gespräch geführt, eingeschätzt und bewertet wird.

Es ist daher von einer gemeinsamen Entscheidung mit der Partei über Zwecke und Mittel der Datenverarbeitung und damit von einer gemeinsamen Verantwortlichkeit (vgl. Art. 4 Nr. 7, 26 DSGVO) auszugehen. Die Verantwortlichkeit der Parteien scheint angesichts der Zusammenarbeit der Parteien mit den Datenschutzbehörden auch nicht in Frage gestellt zu werden.

2. Wahlkampf-Helfer-Daten

Die Frage, ob überhaupt personenbezogene Daten verarbeitet werden, lässt sich im Hinblick auf die registrierten Wahlkampf-Helfer bejahen.

a) Besonderer Erlaubnistatbestand (Art. 9 DSGVO)

Für die Wahlkampf-Helfer der CDU wird auf der CDU-Connect-Internetseite[88] öffentlich ein Formular bereitgestellt, über das sich Unterstützer registrieren können. Neben Kontaktdaten werden optional auch Stärken abgefragt wie „Ich kann von Tür zu Tür gehen" oder „Ich unterstütze in sozialen Netzwerken". Dabei wird der Nutzer auf die Verarbeitung von Informationen über seine politische Meinung und auf die Datenschutzbestimmungen hingewiesen und muss diese über eine Checkbox akzeptieren. Bei anderen Parteien wird ähnlich vorgegangen, wobei die Registrierung regelmäßig nur für Partei-Mitglieder möglich ist und, soweit ersichtlich, kein öffentlich zugängliches Anmeldeformular zur Verfügung steht. Wie die CDU-Internetseite beispielhaft zeigt, sind sich die Parteien der Verarbeitung von besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) bewusst.

Soweit sichergestellt ist, dass sich nur Mitglieder oder Personen mit regelmäßigem Kontakt zu der Partei registrieren, greift für die parteiinterne Verarbeitung der Wahlkampf-Helfer-Daten Art. 9 Abs. 2 lit. d DSGVO. Bei der Neuregistrierung von in Zukunft womöglich aktiven Unterstützern fehlt es (noch) an dem notwendigen regelmäßi-

71 Auf eine Nachholung kommt es damit nicht an, dazu *Schmidt-Wudy*, in: Wolff/Brink (Fn. 10), Art. 14 Rn. 100.
72 Vgl. *Werkmeister/Brandt*, CR 2016, 233, 237.
73 Dazu auch EDPB, Erklärung 2/2019 v. 13. 3. 2019.
74 *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 63), Art. 32 Rn. 30.
75 *Petri*, EuZW 2018, 897, 903.
76 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 68 – Zeugen Jehovas.
77 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 71 – Zeugen Jehovas.
78 *Hein*, https://rp-online.de/nrw/landespolitik/big-data-im-wahlkampf-eine-app-hilft-der-cdu-beim-klinken-putzen_aid-20611285; Abgeordnetenhaus Berlin, Drucks. 18/1253, S. 129.
79 Vgl. https://www.cdu-connect.de/app/.
80 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 16 – Zeugen Jehovas.
81 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 15 – Zeugen Jehovas; Generalanwalt Mengozzi, 1. 2. 2018 – C-25/17, Rn. 14 – Zeugen Jehovas.
82 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 71 – Zeugen Jehovas.
83 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 70 – Zeugen Jehovas.
84 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 16 – Zeugen Jehovas; Generalanwalt Mengozzi, 1. 2. 2018 – C-25/17, Rn. 15 – Zeugen Jehovas
85 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 70 – Zeugen Jehovas.
86 Vgl. EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 69 – Zeugen Jehovas; EuGH, 5. 6. 2018 – C-210/16, K&R 2018, 475, Rn. 38 – Wirtschaftsakademie Schleswig-Holstein.
87 EuGH, 10. 7. 2018 – C-25/17, WRP 2018, 1056, Rn. 67 – Zeugen Jehovas.
88 https://www.cdu-connect.de/.

gen Kontakt, sodass insgesamt die ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO vorzugswürdig ist. Diese verlangt eine unmittelbare Bezugnahme auf die Verarbeitung und schließt konkludentes Handeln aus.[89] Zudem ist darauf zu achten, dass ein bereits gesetztes Ankreuzkästchen nicht ausreichend ist[90] und der Nutzer „in der Lage ist, die Einwilligung zu verweigern […], ohne Nachteile zu erleiden",[91] die Einwilligung also freiwillig erteilt wurde (vgl. Art. 7 Abs. 4 DSGVO). Wird, wie im Fall des CDU-Connect-Unterstützer-Formulars, die Einwilligung als Pflichtfeld ausgestaltet, können Zweifel aufkommen, ob die Einwilligung tatsächlich freiwillig erfolgt. Beachtet man jedoch, dass der einzige Zweck und Vorteil der Registrierung als Unterstützer darin besteht, dass die eigenen Daten für Unterstützerkampagnen im Wahlkampf genutzt werden, besteht ein derart enger Zusammenhang zwischen Registrierungs- und Einwilligungszweck, dass die Verweigerung der Einwilligung mit der Verweigerung der Registrierung einhergehen darf[92] – bzw. dass die Datenverarbeitungen, soweit ein Vertrag geschlossen wird, für die Erfüllung des Vertrags erforderlich sind (vgl. Art. 7 Abs. 4 DSGVO).

b) Informationspflichten (Art. 13, 14 DSGVO)

Den Informationspflichten nach Art. 13, 14 DSGVO wird regelmäßig Genüge getan, wenn die Parteien in einer gut zugänglichen Datenschutz-Erklärung entsprechend den Anforderungen informieren. In der Vergangenheit, auch noch vor Anwendbarkeit der DSGVO, kam es dabei etwa mit Blick auf die Registrierung über Facebook und im Rahmen eines für alle Nutzer sichtbaren Rankings, das personenbezogene Daten enthielt, zu Verstößen.[93]

IV. Datenschutzrechtliche Implikationen des Telefonwahlkampfs

Der Telefonwahlkampf spielt hierzulande eine deutlich geringere Rolle als beispielsweise in den USA. Ein herkömmlicher Telefon-Anruf unterfällt mangels ausreichenden Automatisierungsgrades ggf. nicht dem Anwendungsbereich nach Art. 2 Abs. 1 DSGVO.[94] Die vorbereitende Speicherung der Telefonnummer und das Anlegen eines Gesprächsprotokolls hingegen unterfallen dem Anwendungsbereich der DSGVO, sodass dafür im Wesentlichen die oben genannten Anforderungen zu beachten sind. Der Nachweis einer etwaigen Einwilligung nach Art. 7 Abs. 1 DSGVO muss dabei auch den Nachweis der Zuordnung der Telefonnummer zu der Person – und nicht etwa nur der E-Mail-Adresse wie im double-opt-in-Verfahren[95] –, die die Einwilligung erklärt, umfassen.

Unabhängig von datenschutzrechtlichen Anforderungen wird regelmäßig eine Einwilligung – zwar nicht nach UWG mangels geschäftlicher Handlung bei Wahlkampf-Werbung (§ 2 Abs. 1 Nr. 1 UWG) – als Anforderung aus dem allgemeinen Persönlichkeitsrecht der betroffenen Person (Art. 1 Abs. 1, 2 Abs. 1 GG i. V. m. §§ 823, 1004 BGB analog) vor Durchführung eines Telefon-Anrufs erforderlich sein.[96]

V. Datenschutzrechtliche Implikationen des Wahlkampfs über die Partei-Internetseite

Die datenschutzrechtliche Betrachtung der Internetseiten der Parteien unter Einschluss etwaiger Marketing-Maßnahmen gestaltet sich regelmäßig nicht anders als die anderer Internetseiten. Wie auch für andere Internetseiten gilt es die DSGVO nebst gesonderten Anforderungen, z. B. aus der geänderten eCommerce-RL 2002/58/EG, zu beachten. Eine Besonderheit ergibt sich jedoch erneut aus der Partei-Eigenschaft des Website-Betreibers aufgrund von Art. 9 DSGVO.

Für das Merkmal des Hervorgehens im Sinne von Art. 9 Abs. 1 DSGVO kommt es auf die Umstände des Einzelfalls an.[97] Bereits die Verarbeitung von Daten über eine nur mögliche Parteiaffinität im Rahmen statistischer Analysen kann unter Art. 9 Abs. 1 DSGVO fallen.[98] Lediglich eine hinreichende Wahrscheinlichkeit für die inhaltliche Richtigkeit ist vorauszusetzen.[99] Da bereits aus dem Besuch einer Partei-Website politische Meinungen hervorgehen können, namentlich ein Interesse an der jeweiligen Partei der entsprechenden politischen Richtung, könnten, auch abhängig von den aufgerufenen Unterseiten, die erhöhten Anforderungen aus Art. 9 DSGVO gelten.

In dieser Konsequenz wäre Parteien die Verarbeitung beispielsweise aus Gründen der Informationssicherheit in sog. Logdateien faktisch ohne ausdrückliche Einwilligung, mangels anderer einschlägiger Erlaubnistatbestände aus Art. 9 Abs. 2 DSGVO, versperrt. Derartige Interessen will der EU-Gesetzgeber jedoch privilegieren, indem sie – soweit unbedingt notwendig und verhältnismäßig – als berechtigtes Interesse in Betracht kommen sollen.[100] Auch losgelöst von politischen Parteien wird eine einschränkende Auslegung unter Berücksichtigung des Schutzzwecks gefordert.[101] Art. 9 Abs. 1 DSGVO muss daher so verstanden werden, dass aus einem einfachen Besuch einer Partei-Website noch nicht die politische Meinung hervorgeht. Sobald aber parteispezifische Verarbeitungen erfolgen, die weitere Rückschlüsse über das bloß allgemeine Informationsinteresse durch den Besuch der Website zulassen – wie etwa die Anmeldung zum Partei-Newsletter –, ist Art. 9 DSGVO mit seinen erhöhten Anforderungen einschlägig.

VI. Schlussbetrachtung

Die deutschen Parteien beginnen gerade erst das Microtargeting und generell den datengestützten Wahlkampf für sich zu entdecken. Dabei sind regelmäßig die erhöhten Anforderungen aus Art. 9 DSGVO aufgrund des Hervorgehens politischer Meinungen zu beachten.

Soweit die Parteien ihren Online-Wahlkampf mit personalisierten Werbe-Anzeigen über soziale Netzwerke führen, sind die Parteien mit dem sozialen Netzwerk für Datenverarbeitungsprozesse, die unmittelbar in Zusammenhang mit der Werbe-Anzeige stehen, gemeinsam verantwort-

89 *Kampert*, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 9 Rn. 14.
90 EuGH, 1. 10. 2019 – C-673/17, K&R 2019, 705, Rn. 63 – Planet49.
91 Erwägungsgrund 42 DSGVO.
92 Vgl. Erwägungsgrund 43 DSGVO.
93 Abgeordnetenhaus Berlin, Drs. 18/1253, S. 128.
94 Vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 63), Art. 2 Rn. 16.
95 VG Saarlouis, 29. 10. 2019 – 1 K 732/19, K&R 2020, 386 ff. = WRP 2020, 128.
96 *Sosnitza*, in: Ohly/Sosnitza (Hrsg.), Gesetz gegen den unlauteren Wettbewerb, 7. Aufl. 2016, § 7 Rn. 17 f.
97 *Weichert*, in: Kühling/Buchner (Fn. 18), Art. 9 Rn. 22.
98 Österreichisches LG Feldkirch, 7. 8. 2019 – 57 Cg 30/19 b – 15, ZD 2019, 562 m. Anm. *Wirtensohn*. Insoweit nicht abweichend Österreichisches OLG Innsbruck, 13. 2. 2020 – 1 R 182/19 b.
99 *Schiff*, in: Ehmann/Selmayr (Fn. 12), Art. 9 Rn. 14.
100 Vgl. Erwägungsgrund 49 DSGVO.
101 *Schulz*, in: Gola (Fn. 14), Art. 9 Rn. 13. Nicht abgeneigt *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 63), Art. 9 Rn. 12. Wohl eine weite Auslegung präferierend *Frenzel*, in: Paal/Pauly (Rn. 59), Art. 9 Rn. 12.

lich. Dies birgt angesichts der Komplexität der Datenverarbeitungen auf sozialen Netzwerken und womöglich mangels einschlägigen Erlaubnistatbestands nach Art. 9 Abs. 2 DSGVO ein Risiko für die Parteien.

Im Haustürwahlkampf besteht vor allem bei der Kombination von Daten verschiedener Quellen und über mehrere Wahlkämpfe hinweg die Möglichkeit „zufälligen" Personenbezugs der Wähler-Daten und damit einer rechtswidrigen Verarbeitung, ggf. auch mit Blick auf eine fehlende Information der betroffenen Personen. Insoweit sind die Parteien und die Wahlkampfhelfer gemeinsam verantwortlich. Für die Verarbeitung von Wahlkampfhelfer-Daten durch die Parteien wird regelmäßig eine ausdrückliche Einwilligung notwendig sein.

Der in Deutschland kaum durchgeführte Telefonwahlkampf löst jedenfalls bei vor- und nachbereitenden Verarbeitungen ebenfalls datenschutzrechtliche Pflichten aus.

Die datenschutzrechtlichen Implikationen des Online-Wahlkampfs über die Internetseite einer Partei unterscheiden sich kaum von denen auf herkömmlichen Internetseiten. Jedenfalls ist insoweit eine restriktive Auslegung von Art. 9 DSGVO geboten, um IT-Sicherheitsinteressen der Betreiber zur Geltung zu bringen.

RA Christian Galetzka, LL.M., Würzburg und RA Erik Stamer, LL.M., Berlin*

Beweislastverteilung und Haftungsgrundsätze beim Filesharing

Der vorliegende Beitrag knüpft an den Beitrag der Autoren von 2017 (K&R 2017, 78 ff.) an und verfolgt das Ziel, die Entwicklung der BGH-Rechtsprechung zu Beweislastverteilung und Haftungsgrundsätzen beim Filesharing nachzuzeichnen sowie Folgen für die anwaltliche Beratungspraxis aufzuzeigen.

I. Einleitung

Seit der ersten BGH-Entscheidung *Sommer unseres Lebens* sind nunmehr 10 Jahre vergangen, in denen sich der BGH kontinuierlich mit dem Thema Filesharing und der Haftung von Anschlussinhabern wegen illegaler Nutzung von sogenannten Tauschbörsen im Internet befassen musste. Seit der letzten Bilanz der Autoren[1] sind in knapp drei Jahren neun weitere Entscheidungen des BGH, aber auch je eine des BVerfG und des EuGH in diesem Bereich ergangen. Dabei haben vor allem auch grundrechtliche Aspekte (insbes. Schutz der Familie) verstärkt Einzug in die Rechtsprechung gehalten.

Mehrere der Entscheidungen betreffen die sogenannte sekundäre Darlegungslast des Inhabers eines Internetanschlusses und damit die Frage, unter welchen Voraussetzungen der Anschlussinhaber einer Haftung als Täter einer über seinen Anschluss begangenen Urheberrechtsverletzung entkommen kann. Die Skizzierung der vom BGH weiterentwickelten Rechtsprechungslinie zur sekundären Darlegungslast bildet einen Schwerpunkt des Beitrags (hierzu II.). Bedenklich ist in diesem Zusammenhang die bereits vielfach kritisierte Tendenz des BGH, die sekundäre Darlegungslast zu einer sekundären Beweislast zu verdichten.

Technisch und haftungsrechtlich interessante Aspekte liefert der BGH mit seiner Entscheidung *Konferenz der Tiere*.[2] In dieser wird zum ersten Mal ausführlich dem Phänomen Beachtung geschenkt, dass jeder Tauschbörsennutzer beim Filesharing lediglich einzelne Dateifragmente eines urheberrechtlich geschützten Werkes über Tauschbörsensysteme anderen Tauschbörsennutzern öffentlich zugänglich macht und sich bereits aus diesem Grund eine Haftungsgemeinschaft der Tauschbörsennutzer bildet, die das konkrete Werk gemeinsam mit unterschiedlichen Datenfragmenten desselben zum Herunterladen anbieten (hierzu III.).

Auch zur Störerhaftung[3] und zur Rechtsfolgenseite[4] (Lizenzschadensersatz und Streitwertbemessung) sind BGH-Entscheidungen ergangen, die jedoch im Rahmen dieses Beitrags nicht weiter behandelt werden können.[5]

II. Täterhaftung und sekundäre Darlegungslast des Anschlussinhabers

1. Allgemeine Anforderungen der bisherigen Rechtsprechung des BGH

Eine Haftung des Anschlussinhabers für eine durch Filesharing begangene Urheberrechtsverletzung kann sowohl als Täter als auch als Störer in Betracht kommen. In der Entscheidung *Sommer unseres Lebens* hat der BGH hierzu den mittlerweile allseits bekannten Grundsatz aufgestellt, dass für den Fall, dass ein geschütztes Werk der Öffentlichkeit von einer IP-Adresse aus zugänglich gemacht wird, die zum fraglichen Zeitpunkt einer bestimmten Person, dem Anschlussinhaber, zugeteilt ist, eine tatsächliche Vermutung dafür spricht, dass diese Person für die Rechtsverletzung verantwortlich ist.[6]

---

* Mehr über die Autoren erfahren Sie auf S. VIII.

1 *Galetzka/Stamer*, K&R 2017, 78 ff.

2 BGH, 6. 12. 2017 – I ZR 186/16, K&R 2018, 249 ff. = MMR 2018, 303 – Konferenz der Tiere.

3 BGH, 26. 7. 2018 – I ZR 64/17, K&R 2018, 625 ff. = GRUR 2018, 1044 – Dead Island; BGH, 7. 3. 2019 – I ZR 53/18, K&R 2019, 585 – Bring mich nach Hause.

4 BGH, 22. 3. 2018 – I ZR 265/16, K&R 2018, 588 ff. = GRUR 2018, 914 – Riptide; BGH, 30. 3. 2017 – I ZR 15/16, ZUM 2018, 143.

5 Kritische Auseinandersetzungen finden sich an anderer Stelle, u. a. *Spindler*, GRUR 2018, 1012 ff.; *Nordemann*, GRUR 2018, 1016 ff. zur BGH-Entscheidung Dead Island; ferner auch *Sesing*, GRUR 2019, 898 ff. zum Sperranspruch gem. § 7 Abs. 4 TMG.

6 BGH, 12. 5. 2010 – I ZR 121/08, K&R 2010, 492 ff. = GRUR 2010, 633, Rn. 12 – Sommer unseres Lebens.