Europäische Hochschulschriften

Sabine Himmels

Behavioural Targeting im Internet – Datenschutz durch lauterkeitsrechtlich gestützte Selbstregulierung?

PETER LANG

Einleitung

I. Problemdarstellung

Google, Facebook, Amazon – diese US-amerikanischen Internetunternehmen sind längst zum Synonym und Abbild für die Recherche, das soziale Leben und den Handel im Internet geworden. Dabei ist das Angebot der Unternehmen nicht auf die einzelnen Dienste beschränkt. Um die Internetnutzer immer enger an das eigene Unternehmen zu binden, werden neue Dienste entwickelt, vorhandene Funktionen ausgebaut und die einzelnen Angebote miteinander verzahnt. Daneben sind unzählige weitere kleinere oder nationale Unternehmen im Internet vertreten, die den Nutzern ihre Dienste anbieten.

So unterschiedlich die einzelnen Angebote im Internet auch ausgestaltet sind, so basieren sie doch alle überwiegend auf der umfassenden Nutzung und Verarbeitung von Informationen und Daten über die Internetnutzer. Eine umfassende Datensammlung und Auswertung dient zum einen der stetigen Verbesserung von Diensten und der Entwicklung neuer Funktionen. Zum anderen werden die zumeist kostenlosen Online-Dienste durch zielgruppenspezifische Werbung refinanziert und so wirtschaftlich ertragreich.

Die gezielte Werbeansprache, die nicht gegenüber jedem Besucher einer Webseite erfolgt, sondern nur gegenüber einer genau ausgewählten Zielgruppe, wird als Targeted Advertising bezeichnet.[1] Obwohl es nicht notwendigerweise auf den Nutzer als Individuum ankommt, sondern vielmehr auf seine Zugehörigkeit zu einer bestimmten Zielgruppe, ist die Sammlung individueller Daten notwendige Voraussetzung für den Erfolg von Online-Werbung.[2] Denn je umfassender die Informationen über einen Internetnutzer und seine Zugehörigkeit zu einzelnen Zielgruppen sind, umso effektiver kann Onlinewerbung platziert werden.

Dem wirtschaftlichen Interesse der Unternehmen, soviel wie möglich über den Nutzer zu erfahren, stehen die Bedenken der Datenschutzbehörden entgegen, die darin eine Gefährdung der Persönlichkeitsinteressen der Nutzer sehen.[3] Diese versuchen die umfassende Erhebung, Speicherung und Verknüpfung der

---

1 Grether/Markarian, in: Schwarz, Online-Marketing I, S. 297, 298; Engelken, in: Schwarz, Online-Marketing II, S. 326; Weichert, MR-Int 2007, 188, 193.

2 Vgl. Peifer, K&R 2011, 543; vgl. auch Anand/Shachar, QME 2009, 237, 238.

3 Zu den Gefahren der Profilbildung vgl. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ vom 18.03.2010, S. 11.

Daten durch die mehr oder weniger strikte Anwendung der – in seinen Grundzügen bereits vor 30 Jahren formulierten – Grundsätze des Bundesdatenschutzgesetzes (BDSG) und der bereichsspezifischen Regelungen des Telemediengesetzes (TMG) zu unterbinden. Die Aufsichtsbehörden orientieren sich dabei regelmäßig an dem maximalen Schutz des Betroffenen.[4] In diesem Sinne bewerten sie neue Dienste oder Funktionen, wie die Einbindung des „Like"-Buttons von Facebook,[5] die Bewertung von Lehrern auf einer Internetplattform[6] oder die Aufnahme von Häuserfassaden durch Google Street View[7] als mit dem Datenschutzrecht kollidierend. Inwieweit ihre Einschätzungen tragbar sind, ist mit Ausnahme der Lehrerbewertungsportale, bei der der Fokus letztlich auf einer Abwägung zwischen der Meinungsäußerungsfreiheit und beleidigender Schmähkritik lag,[8] höchstrichterrechtlich nicht endgültig entschieden. Dies ist nicht zuletzt dem Umstand geschuldet, dass sich die Tätigkeiten der Aufsichtsbehörden regelmäßig auf öffentliche Kritik beschränken, während eine Untersagung oder Sanktionierung durch Bußgelder unterbleibt.

Die öffentliche Kritik der Datenschutzbehörden hat das Interesse an datenschutzrechtlichen Themen bei den Nutzern geweckt und sie für den Umgang mit den Daten durch die Betreiber von Online-Diensten zunehmend sensibilisiert.[9] Die Vorstellung des Beobachtetwerdens im Netz führt bei ihnen zu Unbehagen.[10] Sie wollen nicht, dass ihre Daten im Hintergrund erhoben werden, ohne

---

4 So die Kritik bei Höppner, in: Taeger, Die Welt im Netz, 477, 489.

5 Vgl. https://www.datenschutzzentrum.de/presse/20111209-facebook-duesseldorfer-kreis.htm (letzter Abruf am 19.01.2013).

6 Vgl. http://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2008/080422_Datenschutz.pdf (letzter Abruf am 19.01.2013); a. A.: BGH, NJW 2009, 2888, 2893 („spickmich"); für die Übertragung auf Ärzteportale Gundermann, VuR 2010, 329, 333.

7 Vgl. https://www.datenschutzzentrum.de/geodaten/20081118-dk.html (letzter Abruf am 19.01.2013); Casper, DÖV 2009, 965, 969, 973.

8 Vgl. BGH, NJW 2009, 2888, 2891 („spickmich"); hierzu Spickhoff, LMK 2009, 287789.

9 BFDI 23. Tätigkeitsbericht 2009-2010, S. 15; Spindler, Persönlichkeitsschutz im Internet, F-11.

10 Von 3360 befragten US-amerikanischen Konsumenten über 18 Jahren wussten 69 %, dass ihr Browser-Verhalten protokolliert und für Werbezwecke ausgewertet werden kann; 51 % der Befragten gaben zudem an, mit Unbehagen auf die kommerzielle Nutzung ihrer Verhaltensdaten zu reagieren, selbst wenn die erhobenen Informationen ihnen nicht persönlich zugeordnet werden können, vgl. 2009 Study: Consumer Attitudes about Behavioural Targeting, S. 3, 6; abrufbar unter http://de.scribd.com/doc/18050719/TRUSTeTNS-Study-Consumer-Attitudes-about-Behavioral-Targeting- (letzter Abruf am 19.01.2013).

dass sie wissen, ob sie beobachtet werden oder in welchem Ausmaß die Beobachtung erfolgt.[11]

Der Druck der Datenschutzbehörden und die Entwicklung des gesellschaftlichen Bewusstseins haben dazu geführt, dass die Betreiber der Online-Dienste datenschutzrechtliche Anforderungen nicht mehr einfach ignorieren können. Selbst ehemalige „selbsternannte Totengräber“[12] des Datenschutzes wie der CEO von Sun Microsoft Scott Nelly, der gerne mit seiner im Jahr 1999 getätigten Aussage „You have zero privacy – get over it!“[13] zitiert wird, hat seine Einstellung zum Datenschutz geändert. So betonte er bereits im Jahr 2006 die Wichtigkeit des Datenschutzes für den Erfolg von Online-Diensten, indem er feststellte:

> „It’s going to get scarier if we don’t come up with data technology and rules to protect appropriately privacy and secure the data, and the most important asset we have is obviously the data on people (...). And if we can`t protect that, people (…) are not going to go online“[14].

Möchten die Betreiber der Online-Dienste einerseits das Vertrauen von Nutzern und Aufsichtsbehörden gewinnen, sich aber andererseits nicht ihrer wirtschaftlichen Grundlagen berauben, muss eine Kompromisslösung gefunden werden. Die Lösung stellt nicht nur Anforderungen an die Werbewirtschaft, sondern schafft möglicherweise auch bei den Datenschützern ein Umdenken dahingehend, dass die Unternehmen nicht mehr nur als regulierungsbedürftige Daten-Sünder, sondern auch als mitwirkungsberechtigte Akteure wahrgenommen werden.

II. Stand der Forschung

Die Sammlung und Auswertung personenbezogener Daten zum Zwecke der personalisierten Werbung wird schon seit Längerem in der datenschutzrechtlichen Literatur diskutiert. So befasst sich der derzeitige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter *Schaar* bereits 2001 mit den datenschutzrechtlichen Gefahren im Internet und betont den Wert von Nutzungs-

---

11 So Härting, Internetrecht, Rn. 102; ders.: CR 2008, 743, 747 f.

12 Hansen, in: de Meer/Herkenhöner, 23, 24.

13 Sprenger, Polly (1999): Sun on Privacy: ‚Get Over it‘; Wired Magazine, abrufbar unter http://www.wired.com/politics/law/news/1999/01/17538 (letzter Abruf am 19.01.2013).

14 Lemos, Robert (2006): Private identities become a corporate focus, Security Focus; abrufbar unter http://www.securityfocus.com/news/11377 (letzter Abruf am 19.01.2013).

profilen für die Werbewirtschaft.[15] Eine umfassende datenschutzrechtliche Bewertung der Erstellung von Nutzerprofilen durch Cookies nimmt *Merati-Kashani*[16] vor.

In der aktuellen Literatur wird die Profilbildung von Nutzern durch den Einsatz von Cookies beim sogenannten Online Behavioural Targeting diskutiert.[17] Beim Online Behavioural Targeting wird das Nutzerverhalten im Internet über einen längeren Zeitraum verfolgt und der Nutzer einem bestimmten Zielgruppenprofil zugeordnet. Hierin wird eine besondere Bedrohung der Selbstbestimmung gesehen.[18] Zur Beschränkung des Online Behavioural Targeting, wurden auf europäischer Ebene die Vorgaben der E-Privacy-Richtlinie (RL 2002/58/EG)[19] verschärft. Nach Auslegung durch die Art.-29-Datenschutzgruppe[20] ist Online Behavioural Targeting nur zulässig, wenn das Einverständnis der Nutzer eingeholt wurde. Dieser Ansatz wird auch im Entwurf einer Datenschutz-Grundverordnung[21] verfolgt.[22] Diese Regelung des EU-Datenschutz-

---

15 Schaar, Datenschutz im Internet, Rn. 36; ders.: DuD 2001, 383, 384 f.

16 Merati-Kashani, Datenschutz im E-Commerce, insbesondere S. 59 ff., 139 ff.

17 Thürauf, ZD 2011, 24, 28, Rammos, K&R 2011, S. 692; Lienemann, K&R 2011, 609, 610 f.

18 Vgl. Art.-29-Datenschutzgruppe, WP 171.

19 Richtlinie 2002/58/EG des europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. Nr. L 201 S. 37 (Datenschutzrichtlinie für elektronische Kommunikation); zuletzt geändert durch Richtlinie 2009/136 des Europäischen Parlaments und des Rates vom 25. November 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.

20 Die Art.-29-Datenschutzgruppe setzt sich aus Vertretern der nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten und der Europäischen Kommission zusammen. Ihre Aufgaben bestehen primär in der fachlichen Beratung der Europäischen Kommission, der Förderung der einheitlichen Anwendung der Richtlinie 95/46/EG sowie der Beratung der Kommission auf alle EG-Rechtsvorschriften, die sich auf das Recht auf den Schutz personenbezogener Daten beziehen.

21 Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung); KOM 2012 (11) endg. 2012/0011 (COD).

22 Nach Artikel 20 der Grundverordnung sollen auf der Erstellung von Nutzerprofilen basierende Maßnahmen nur noch zur Erfüllung eines Vertrags, durch ausdrückliche Erwähnung in einer Rechtsvorschrift oder auf der Grundlage einer Einwilligung zulässig sein.

rechts soll für jeden Internetdienstanbieter gelten, der das Surfverhalten der Webseiten-Besucher zwecks zielgerichteter Werbung auswertet.[23]

Demgegenüber hält sich der deutsche Gesetzgeber mit der Umsetzung der europäischen Vorgaben und dem Erlass imperativer Regelungen bislang zurück.[24] Es wird zunächst der Dialog mit der Werbewirtschaft gesucht, deren favorisierte Lösung in der Einführung selbstregulierender Mechanismen liegt.[25] Erste Ansätze finden sich beispielsweise in der Vereinbarung eines „Datenschutzkodex für Geodatendienste“[26], der Vereinbarung von Selbstkontrollrichtlinien durch die Europäische Online-Werbeindustrie[27] oder in der Erklärung des sozialen Netzwerks Facebook, sich an einer Selbstregulierung der Branche zum Schutz der Nutzer zu beteiligen[28].

Die Vorstellung einer Selbstregulierung zur Verbesserung des Datenschutzes im nicht-öffentlichen Bereich ist der datenschutzrechtlichen Forschung nicht unbekannt. So fordern bereits *Roßnagel/Pfitzmann/Garstka*[29] in ihrem Modernisierungsgutachten 2001, dass es den betroffenen Branchen ermöglicht werden

---

23 Kritisch hierzu Härting, BB 2012, 459, 462; die materiellen Regelungen entsprechen in weiten Teilen 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, Abl. Nr. L 281, S. 31, und damit dem deutschen Datenschutzrecht, was nicht zuletzt dem Umstand geschuldet sein dürfte, dass Ziel der Datenschutz-Grundverordnung sein soll, das Schutzniveau in Europa an das geltende Schutzniveau in Deutschland anzupassen, vgl. hierzu Reding, ZD 2012, 195, 197; Schneider/Härting, ZD 2012, 199, 203.

24 Vgl. zur Notwendigkeit der Änderung des § 15 Abs. 3 TMG, der keine Einwilligung, sondern die Widerspruchslösung vorsieht, Beschluss des Düsseldorfer Kreises vom 24/25.11.2010: abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.pdf?__blob=publicationFile (letzter Abruf am 19.01.2013).

25 Vgl. BR-Drs 129/11, S. 69.

26 Vgl. http://www.bitkom.org/de/themen/50792_66098.aspx (letzter Abruf am 19.01.2013).

27 Das Selbstregulierungskonzept mit dem Namen „European Self-Regulation for OBA“ (im Folgenden IAB OBA) vom 14.4.2011 ist abrufbar unter: http://www.iabeurope.eu/media/62483/2012-02-20%20iab%20europe%20oba%20framework.pdf (letzter Abruf am 19.01.2013)

28 Vgl. http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/facebook/nach-gespraechen-mit-dem-innenministerium-facebook-zu-selbstregulierung-bei-datenschutz-bereit-11134098.html (letzter Abruf am 19.01.2013).

29 Roßnagel/Pfitzmann/Garstka, S. 153 f.; ebenso für die Stärkung einer ergänzenden Selbstregulierung u.a.: Weichert, DuD 2001, 264, 268; ders., RDV 2005, 1; Schaar, DuD 2003, 421, 425 f.; Abel, RDV 2003, 11, 15.

soll, Verhaltensregeln aufzustellen, die die datenschutzrechtlichen Vorgaben praxistauglich und angepasst auf die aktuellen technischen Entwicklungen umsetzen. Es fehlt bisher an klaren Rahmenvorgaben, wie das Konzept der Selbstregulierung ausgestaltet sein muss, welche Maßnahmen zwingend umzusetzen und welche Grenzen einzuhalten sind. Die von der FDP angestrebte Etablierung einer „Stiftung Datenschutz“[30] hat noch keine konkreten Formen angenommen.

Als größter Kritikpunkt gegen ein Selbstregulierungskonzept werden Durchsetzungsschwierigkeiten genannt.[31] Eine Durchsetzung durch die Aufsichtsbehörden wird schon für die gesetzlichen Vorgaben des BDSG und TMG aufgrund der fehlenden personellen Ausstattung skeptisch gesehen.[32] Den sich selbst regulierenden Akteuren oder den betroffenen Nutzern wird eine objektive Kontrolle und Ahndung von Verstößen nicht zugetraut.[33] Zur besseren Rechtsdurchsetzung der datenschutzrechtlichen Selbstregulierung ist es denkbar, die Instrumente des Gesetzes gegen den unlauteren Wettbewerb (UWG) zu aktivieren. In diesem Sinne fordert *Spindler*[34] eine gesetzliche Klarstellung, dass Verstöße gegen Datenschutzerklärungen oder datenschutzrechtliche Verhaltenskodizes eine Irreführung des Verbrauchers nach §§ 3, 5 UWG darstellen. Eine über die Forderung hinausgehende Prüfung, wie dieser Vorschlag konkret umgesetzt werden könnte, unterbleibt. *Gola/Schomerus*[35] und *Kinast*[36] halten es schon nach geltendem Recht für möglich, dass in dem Verstoß gegen die datenschutzrechtliche Selbstregulierung zugleich eine unlautere irreführende Handlung nach §§ 3, 5 UWG liegt. Eine Ausandersetzung mit den Tatbestandsvoraussetzungen der

30 Vgl. http://www.bfdi.bund.de/SharedDocs/Publikationen/KonzeptionStiftung Datenschutz.pdf?__blob=publicationFile (letzter Abruf am 19.01.2013); hierzu Piltz/ Schulz, RDV 2011, 117, 119 ff.; kritisch Wagner, RDV 2011, 229 f.

31 Vgl. u. a. Schmidthuber, Verhaltenskodizes, S. 130; Dahm, DuD 2002, 412, 415; Christiansen, MMR 2000, 123, 126 f.

32 So sind die Aufsichtsbehörden schon heute nicht ausreichend ausgestattet, um ihre Funktionen auszuüben, zur personellen Unterbesetzung vgl. http://www.xamit-leistungen.de/downloads/Files.php?f=XamitDatenschutzbarometer2011.pdf, S. 37 (letzter Abruf am 19.01.2013); ebenso Weichert, RDV 2005, 1, 5; Peifer, K&R 2011, 543, 547.

33 Schon zum Vollzugsdefizit der aktuellen datenschutzrechtlichen Vorschriften durch die gesellschaftlichen Akteure Leppershof/Pettersdorf, DuD 2009, 15, 19; Kühling/Sivridis/ Schwuchow/Burghardt, DuD 2009, 335 f.; ebenso die Einschätzung von Peifer, K&R 2011, 543, 547.

34 Spindler, Persönlichkeitsrechtschutz im Internet, F-131.

35 Gola/Schomerus, BDSG, § 38a Rn. 3a.

36 Kinast, in: Taeger/Gabel, BDSG, § 38a Rn. 37.

§§ 3, 5 UWG findet nicht statt. Etwas ausgiebiger befasst sich nur *Schröder*[37] im Rahmen der Untersuchung der Haftungsfolgen für Unternehmen bei Verstößen gegen datenschutzrechtliche Verhaltensregeln mit möglichen Ansprüchen nach den Regelungen des UWG 2004[38].

Eine umfassende lauterkeitsrechtliche Untersuchung des konkreten Selbstregulierungsansatzes im Bereich des Datenschutzes hat es, soweit ersichtlich, noch nicht gegeben. Insbesondere fehlt es auch an einer Auseinandersetzung mit den durch die Umsetzung der Richtlinie über unlautere Geschäftspraktiken (UGP-RL)[39] eingeführten neuen Tatbeständen und Voraussetzungen.

III. Arbeitshypothesen

Diese Arbeit nimmt den Ansatz einer datenschutzrechtlichen Selbstregulierung für den Einsatz von personalisierter Werbung durch die Werbewirtschaft auf und versucht herauszufinden, wie die Interessen der Datenschutzbehörden und der Betroffenen an einem möglichst umfassenden Schutz der Privatsphäre der Nutzer effektiv umgesetzt werden können, ohne zugleich den Betreibern der Online-Dienste ihre Erlösquellen und den Nutzern die Vorteile der Datenauswertung zu entziehen. Ein maßgeblicher Schwerpunkt soll dabei auf der Gewährleistung der Durchsetzung des von den Unternehmen selbst gesetzten Regelwerks liegen. Wesentliches Ziel dieser Arbeit ist es, zu untersuchen, inwieweit ein ergänzender Rechtsschutz für die Durchsetzung einer Selbstregulierung im Bereich des Datenschutzes durch die Instrumente des Gesetzes gegen unlauteren Wettbewerb (UWG) bewirkt werden kann.

Dazu stützt sich die Arbeit primär auf die Untersuchung folgender Aspekte: Die Profilbildung zum Zwecke der personalisierten Werbung wird als Eingriff in die Privatsphäre gewertet. Der verfassungsrechtliche Schutz des Privaten nach Art. 2 Abs. 1 i. V. mit Art. 1 GG wurde von dem Gesetzgeber auch für die Bedrohungen im Verhältnis unter Privaten, insbesondere in den §§ 28 ff. BDSG,

---

37 Schröder, Haftung für Verstöße gegen Privacy Policies und Codes of Conduct, S. 134-150, 191-196, 249 f.

38 UWG v. 03.07.2004, BGBl. I. S. 1414.

39 Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinie 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken), ABl. Nr. L 149 S. 22, ber. ABl. 2009 Nr. L 253, S. 18.

konkretisiert.[40] Nach § 1 BDSG ist der Zweck des Gesetzes, den Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechts durch den Umgang mit seinen personenbezogenen Daten zu schützen. Dieser Zweck gilt für die wirtschaftsbezogenen Regelungen des TMG entsprechend.[41] Auch über das zivilrechtliche Allgemeine Persönlichkeitsrecht finden die verfassungsrechtlichen Wertungen zum Schutz der Privatheit Berücksichtigung. Einer Selbstregulierung der Werbewirtschaft kann aber nur dann Bedeutung zukommen, wenn die derzeitige gesetzliche Ausgestaltung den Konflikt zwischen dem Schutz des Persönlichkeitsrechts und den wirtschaftlichen Verwertungsinteressen nicht gerecht lösen kann. Daher wird angenommen, dass das derzeitige gesetzliche Regelungsmodell zum Schutz der Privatsphäre im Internet zu komplex, lückenhaft oder zu verbotsintensiv ist, um zu einer sachgerechten Beurteilung von Behavioural Targeting zu kommen.

Weiterhin ist kritisch zu prüfen, inwieweit der gesetzliche Rahmen Raum für eine Selbstregulierung im Bereich des Datenschutzes lässt und wie diese ausgestaltet sein muss, um den Einsatz zielgruppenspezifischer Werbung zu ermöglichen, ohne die persönlichkeitsrechtlichen Belange der Nutzer unangemessen zu benachteiligen. Es ist zu prüfen, welche Funktion den selbst gesetzten Regelungen zukommen kann, ob sie geeignet ist, möglicherweise bestehende Lücken im Gesetz zu schließen oder konkretisierend auf bestehende Regelungen einzuwirken.

Gestützt auf die Annahme, dass die gesetzlichen Regelungen im Datenschutzrecht Raum für eine Selbstregulierung durch die Werbewirtschaft lassen, soll ihre Durchsetzungsmöglichkeit geprüft werden. Dabei wird untersucht, inwieweit die Instrumente des UWG nutzbar gemacht werden können, um die Einhaltung der Vorgaben der Selbstregulierung und so im Ergebnis einen datenschutzkonformen Umgang mit personenbezogenen Daten im Internet zu gewährleisten. Es wird angenommen, dass dem Lauterkeitsrecht besondere Bedeutung zukommen kann, um Transparenz und Information beim Umgang mit personenbezogenen Daten im Internet zu bewirken.

---

40 Schwartmann, RDV 2012, 1, 2.

41 Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, § 11 TMG Rn. 1, 2; Merati-Kashani, Datenschutz im E-Commerce, S. 26.

IV. Gang der Darstellung

Der Gang der Darstellung orientiert sich an der Überprüfung der aufgestellten Arbeitshypothesen. Der Einsatz personalisierter Werbung im Internet ist bisher nicht eindeutig gesetzlich geregelt. Gerade bestehende Lücken im Gesetz, Unsicherheiten in der Auslegung oder die Vermeidung unsachgemäßer Ergebnisse können aber ein Ausweichen auf die Selbstregulierung rechtfertigen.

Dementsprechend beginnt der erste Teil der Arbeit mit einer datenschutzrechtlichen und persönlichkeitsrechtlichen Bewertung des Targeted Advertising. Da sich die Bedenken der Aufsichtsbehörden insbesondere gegen Onlinewerbung auf der Basis des Online Behavioural Targeting richten, wird die Untersuchung auf diese Form der personalisierten Werbung begrenzt. Die vom Online Behavioural Targeting ausgehenden Gefahren für den Nutzer können nach den gesetzlichen Regelungen nur bewertet werden, wenn die Funktionsweise hinreichend geklärt ist. Daher wird zunächst die Funktionsweise des Online Behavioural Targeting erläutert und von anderen Formen der personalisierten Werbung im Internet abgegrenzt. Die Prüfung der Zulässigkeit des Online Behavioural Targeting nach den Vorgaben des TMG und BDSG sowie nach dem zivilrechtlichen Persönlichkeitsrecht dient einerseits der rechtlichen Einordnung. Andererseits sollen aber auch die Schwierigkeiten der derzeitigen gesetzlichen Ausgestaltung dargestellt werden, um Anknüpfungspunkte für eine Selbstregulierung aufzuzeigen. Die hier erarbeiteten Ergebnisse bilden wesentliche Vorgaben für die inhaltliche Ausgestaltung einer Selbstregulierung, für ihre Funktion und für ihre Grenzen.

Im zweiten Teil wird erörtert, unter welchen Voraussetzungen eine Implementierung von Selbstregulierungsmechanismen für den Einsatz von Online Behavioural Targeting erfolgen kann. Hierfür werden zunächst die im BDSG vorgesehenen Selbstregulierungsinstrumente sowie die bereits in der Praxis bewährten Privacy Policies erörtert. Sieht das BDSG die Vereinbarung von Verhaltenskodizes und die Zertifizierung besonders nutzerfreundlicher Datenschutzkonzepte vor, lassen sich hieraus die zwingenden Anforderungen einer Selbstregulierung für den Einsatz von Online Behavioural Targeting ableiten. Anhand der herausgearbeiteten Anforderungen werden schließlich Eckpunkte bestimmt, wie Online Behavioural Targeting unter Berücksichtigung der gegenläufigen Interessen datenschutzkonform umgesetzt werden könnte.

Im dritten Teil wird die Durchsetzbarkeit des erarbeiteten Regelwerks durch die Instrumente des UWG überprüft. Stellt der Verstoß gegen die selbst gesetzten Verhaltenspflichten zugleich eine unzulässige geschäftliche Handlung nach § 3 UWG dar, so können nach § 8 Abs. 3 UWG Verbraucherschutzverbände und Mitbewerber Ansprüche auf Unterlassung (§ 8 Abs. 1 UWG), aber auch auf

Schadensersatz (§ 9 UWG) oder Gewinnabschöpfung (§ 10 UWG) geltend machen. Die Selbstregulierung bindet regelmäßig nur die gesellschaftlichen Akteure, die sich ihr freiwillig unterworfen haben. Es fragt sich, ob die Instrumente des Lauterkeitsrechts nutzbar gemacht werden können, um auch Außenseiter zu binden. Zugleich könnten so auch die im Datenschutzrecht verfolgten Prinzipien der Information und Transparenz gestärkt werden. Da die Selbstregulierung für den Einsatz des Online Behavioural Targeting die gesetzlichen Regelungen nur konkretisieren, geht mit dem Verstoß gegen die Selbstregulierung häufig auch ein Verstoß gegen die gesetzlichen Regelungen einher. Daher liegt ein Schwerpunkt auf der Überprüfung, inwieweit Verstöße gegen die Vorgaben von BDSG und TMG einen Verstoß gegen eine Unlauterkeit wegen Rechtsbruch nach § 4 Nr. 11 UWG begründen können.