Wissenschaftliche Dienste

Deutscher Bundestag

Ausarbeitung

Rechtsschutzmöglichkeiten gegen die Verletzung von Persönlichkeitsrechten bei der Facebook-Gesichtserkennung unter Berücksichtigung der europäischen Facebook-Niederlassung in Irland und deren Zuständigkeitsbereich

[redacted]

WD 10 – 3000-034/12

Rechtsschutzmöglichkeiten gegen die Verletzung von Persönlichkeitsrechten bei der Facebook-Gesichtserkennung unter Berücksichtigung der europäischen Facebook-Niederlassung in Irland und deren Zuständigkeitsbereich

Verfasser/in: [redacted]
Aktenzeichen: WD 10 – 3000-034/12
Abschluss der Arbeit: 29. März 2012
Fachbereich: WD 10: Kultur, Medien und Sport
Telefon: [redacted]

Ausarbeitungen und andere Informationsangebote der Wissenschaftlichen Dienste geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Der Deutsche Bundestag behält sich die Rechte der Veröffentlichung und Verbreitung vor. Beides bedarf der Zustimmung der Leitung der Abteilung W, Platz der Republik 1, 11011 Berlin.

Inhaltsverzeichnis

1. Einleitung

Onlinedienste haben sich zu einem festen Bestandteil unseres Alltags entwickelt. Sie werfen eine Reihe umfassender datenschutzrechtlicher Fragen auf.

Mit Suchmaschinen wie etwa Google werden Informationen im Internet abgerufen. Über Netzwerke wie Facebook tauschen sich zahlreiche Menschen mit Bekannten in der ganzen Welt aus und werden Teil ihres sozialen Alltags. Diese Onlinedienste und viele mehr sind zu einem festen Bestandteil unseres Lebens geworden.

Bei ihrer Nutzung hinterlassen wir allerdings freiwillig oder ungewollt zahllose Informationen, die Aufschluss über Vorlieben, Freizeitgestaltung, Konsumverhalten, politische und religiöse Ansichten oder die Privatsphäre geben. Doch wer diese Daten sammelt, wo sie gespeichert werden und vor allem wer unter welchen Voraussetzungen auf sie zugreifen darf, ist wegen des globalen Charakters des Internet oftmals unklar. Zudem hat der Datenschutz in verschiedenen Staaten der Welt einen unterschiedlichen Stellenwert, sodass aus der Sicht der Nutzer und Anbieter bedeutsam ist, wann ihre Angebote den Vorgaben des deutschen Datenschutzrechts entsprechen müssen.[1] Bei Ereignissen oder Entwicklungen, mit denen die Politik nicht gerechnet hat, heißt es daher häufig, das Internet dürfe kein rechtsfreier Raum sein.[2]

Das Thema betrifft eine **Materie**, die in rechtlicher Hinsicht ebenso **umfangreich** wie **inhaltlich komplex** ist. Aufgrund der Aktualität der Problematik sind nur **wenige relevante Entscheidungen der Rechtsprechung** vorhanden und ihre Ergebnisse auch nur eingeschränkt auf den vorliegenden Fall übertragbar. Weiterhin wird die Beurteilung des vorliegenden Sachverhaltes von einer Vielzahl internationaler wie auch nationaler Rechtsgebiete beeinflusst, deren Verhältnis untereinander wiederum unter Berücksichtigung spezieller europäischer Vorgaben abzuwägen ist.

Diese Arbeit muss sich daher auf die Vermittlung eines **kursorischen Überblickes** über die mit der Fragestellung verbundenen Problemfelder beschränken und kann damit lediglich eine vorläufige Einschätzung liefern. Dies gilt insbesondere unter dem Aspekt, dass die europäische Gesetzgebung der ständigen Veränderung unterliegt.[3]

Ausgangspunkt der Aufgabenstellung ist die Frage, unter welchen rechtlichen Voraussetzungen eine Privatperson sich gegen die Veröffentlichung einer bildlichen Darstellung ihrer Person im Rahmen der **Facebook-Gesichtserkennung** wenden kann, soweit diese ohne ihre Einwilligung auf einem fremden Facebook-Profil von einer anderen Person eingestellt wurde. Des Weiteren zielt die Aufgabenstellung auf die Frage nach der Anwendbarkeit des irischen Landesrechts ab.

---

1 Jotzo, MMR 2009, 232 (232).

2 Kemper, Wo bleibt der Netz-Minister?, Internet World Business, 19.12.2011, S. 34.

3 Siehe insbesondere unten: „6. Ausblick – Neue europäische Datenschutzvorgaben“.

Die Beantwortung der Aufgabe ist in mehrere Abschnitte unterteilt:

Zunächst werden **Probleme** aufgezeigt, die durch die **Facebook-Gesichtserkennungsfunktion** entstehen können. Dann erfolgt eine kurze **Darstellung der möglichen Anspruchsgrundlagen** die das deutsche Recht dem Betroffenen zur Seite stellt. Begleitend wird die **Frage nach der Anwendbarkeit der deutschen Normen** erörtert, was aufgrund des grenzüberschreitenden Charakters der Internetnutzung unerlässlich ist.

Sodann werden insbesondere unter Bezugnahme der **Besonderheiten des europäischen EU-Rechts** die **Zuständigkeit der deutschen Gerichte,** sowie **die Anwendbarkeit der irischen Gesetze** und die sich aus ihnen ergebenden **Rechtsschutzmöglichkeiten zur Wahrung von Persönlichkeitsrechten** erläutert und aufgezeigt, aus welchen maßgeblichen Hintergründen das irische Recht im Rahmen einer Gesamtbetrachtung herangezogen werden muss.

Auch werden die **unterschiedlichen Anspruchsgegner,** zum Einen das Unternehmen Facebook Irland[4] selbst und zum Anderen die Person, die die Abbildung auf der Internetseite Facebook eingestellt hat (sog. Uploader), aufgezeigt.

Schließlich wird ein **Fazit** bezüglich der aufgezeigten Rechtsschutzmöglichkeiten gezogen und eine Einschätzung in Form eines **Ausblicks zur Entwicklung der künftigen Rechtslage** gegeben.

2. Probleme bei der Facebook-Gesichtserkennung und öffentlich geäußerte Kritik

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Johannes Caspar, hat Facebook aufgefordert, die über die Gesichtserkennung gespeicherten biometrischen Daten der Nutzer zu löschen. Die Funktion der Gesichtserkennung sei an europäische und nationale Datenschutzstandards anzupassen oder abzuschalten.[5] In diesem Zusammenhang wurde insbesondere Folgendes problematisiert:

Die **Gesichtserkennung diene der automatischen Erkennung von Freunden,** die auf Fotos der Nutzer abgebildet sind. Hierfür werte Facebook die von Nutzern auf ihren Fotos markierten Gesichter nach biometrischen Merkmalen aus und speichere sie. So entstehe die vermutlich **weltweit größte Datenbank mit biometrischen Merkmalen einzelner Personen**. Lade ein Nutzer neue Fotos hoch, folge ein Abgleich mit diesen Informationen. Sobald die Software auf diesen Fotos

4 Facebook Ireland Limited, Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland.

5 Juris GmbH, Löschung biometrischer Daten bei Facebook gefordert, 02.08.2011; vgl. Heise Online, Gesichtserkennung bei Facebook: Hamburgs Datenschützer macht Ernst, 2011, abrufbar unter: http://www.heise.de/newsticker/meldung/Gesichtserkennung-bei-Facebook-Hamburgs-Datenschuetzer-macht-Ernst-1376696.html [Stand: 07.02.2012].

Übereinstimmungen mit Freunden erkenne, werde automatisch ein Vorschlag für die namentliche Markierung der erkannten Person generiert. Dabei sei nicht der Einsatz der Gesichtserkennungssoftware zur Erleichterung des sogenannten Foto-Taggings[6] von Freunden das Problem. Vielmehr sei bedenklich, dass Facebook für diese Funktion im Hintergrund eine Datenbank zur Gesichtserkennung mit Millionen von Nutzern aufbaue. Bei einer Gesamtzahl von **über 75 Milliarden hochgeladener Fotos** würden bisher nach Angaben von Facebook **mehr als 450 Millionen Personen** getaggt werden. Schätzungen zu Folge würden **pro Sekunde mehr als 1.000 Namens-Taggs eingetragen** werden. Die exorbitante Masse an Fotos wird nachvollziehbar, wenn man sich die gewaltige Mitgliederanzahl von nunmehr ca. **845 Millionen[7] Menschen** vor Augen führt. Die Risiken einer derartigen Ansammlung biometrischer Daten seien immens. So ist bereits von einem „vollständigen Kontrollverlust“[8] und dem „gläsernen Bürger“[9] die Rede. Derzeit werde jeder auf einem Foto markierte Nutzer in der Datenbank erfasst, der der Speicherung seiner Fotoinformationen nicht ausdrücklich widerspreche. Die derzeitige Möglichkeit eines sogenannten **Opt-Out[10], das durch Facebook** angeboten werde, sei dabei aus folgenden Gründen **irreführend**:

Unter den Privatsphäre-Einstellungen biete Facebook den Nutzern an, das Unterbreiten von Markierungsvorschlägen zu unterbinden durch die Option "Freunden Fotos von mir vorschlagen". Facebook habe dazu schriftlich mitgeteilt, dass nach Abschalten dieser Funktion auch eine Löschung der biometrischen Daten erfolge.[11] Allerdings könne man anhand des Facebooks Online-Hilfesystem erkennen, dass dies lediglich die Markierungsvorschläge unterdrücke. Es sei davon auszugehen, dass die biometrischen Daten gespeichert bleiben. Wenn Nutzer ihre bereits gespeicherten biometrischen Informationen löschen wollten, müssten sie zunächst das Online-Hilfesystem durcharbeiten. Darin werde zur Löschung der biometrischen Daten ein Weg über die Privatsphäre-Einstellungen gewiesen.

---

6 Englisch „to tag“, meint: Mit einem Anhänger, Schild o.Ä. versehen; Vgl. Duden – Das große Wörterbuch der deutschen Sprache in 10 Bänden. Bibliographisches Institut F. A. Brockhaus AG, Mannheim. Der Begriff „taggen“ wird neudeutsch verwendet, wenn etwa Facebook-Mitglieder Freunde oder Bekannte auf Fotos markieren; vgl. Welt Online, Foto-Tagging, Gesichtserkennung ist nicht nur auf Facebook üblich, 2011, abrufbar unter: http://www.welt.de/wirtschaft/webwelt/article13426306/Gesichtserkennung-ist-nicht-nur-auf-Facebook-ueblich.html [Stand: 09.02.2012].

7 Laut eigenen Angaben von Facebook, abrufbar unter: http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 [Stand: 31.01.2012].

8 Seemann, c´t 2010, 114 (115).

9 Heckmann, K&R 2011, 1 (4).

10 Engl. „to opt out“ meint: Etwas nicht mitmachen, vgl. Duden – Das Große Fremdwörterbuch. 4., aktualisierte Auflage. Mannheim, Leipzig, Wien, Zürich: Dudenverlag 2003. Allgemein bedeutet es aus etwas aussteigen oder austreten. Vgl. auch: http://www.pcgameshardware.de/aid,701180/Facebook-aendert-seine-Privatsphaeren-Voreinstellungen-auf-Opt-out-Modell/Internet/News/ [Stand: 09.02.2012].

11 Juris GmbH (Fn. 5).

Die entsprechende Funktion "Daten aus Fotovergleich löschen" existiere jedoch nicht. An einer anderen Stelle im Hilfesystem finde sich ein Link, über den der Nutzer das "Facebook Foto-Team" kontaktieren könne.[12] Dort solle er um die Entfernung aller bisher über ihn selbst in der biometrischen Datenbank gespeicherten Fotoinformationen bitten. Eine Opt-Out-Möglichkeit sei damit zwar vorhanden, für den normalen Nutzer aber kaum zu finden und eine eigene Umsetzung des gewünschten Datenschutzes dementsprechend kompliziert. Angesichts dessen scheine besonders bedenklich, dass sogar für minderjährige Nutzer die Gesichtserkennung voreingestellt sei.

Aber selbst wenn Facebook ein nutzerfreundliches Verfahren zum Opt-Out anböte, würde es aus folgenden Gründen weder nationalen noch europäischen Datenschutzanforderungen genügen[13]: Für eine Speicherung von biometrischen Merkmalen sei eine **vorab erteilte, unmissverständliche Einwilligung der Betroffenen erforderlich**. Zu unterstellen, durch bloßes Nichteinlegen eines Widerspruchs läge eine Zustimmung vor, reiche hierfür nicht aus. Auch die Art.-29-Datenschutzgruppe[14], der Zusammenschluss der Datenschutzbeauftragten Europas, habe deutlich gemacht, dass die Beibehaltung von Voreinstellungen in sozialen Netzwerken keinen eindeutigen Erklärungsgehalt habe.

Dazu **Johannes Caspar**, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: "Wir haben Facebook wiederholt aufgefordert, die Funktion der Gesichtserkennung abzuschalten und die bereits gespeicherten Daten zu löschen. Sollte Facebook diese Funktion weiterhin aufrechterhalten, muss sichergestellt werden, dass nur Daten von Personen in die Datenbank eingehen, die zuvor wirksam ihre Einwilligung zur Speicherung ihrer biometrischen Gesichtsprofile erklärt haben. Die automatische Gesichtserkennung ist ein schwerer **Eingriff in das informationelle Selbstbestimmungsrecht**[15] des Einzelnen. Das muss auch ein global agierendes Unternehmen berücksichtigen. Daher darf Facebook nicht lediglich auf ein intransparentes Widerspruchsverfahren verweisen. Eine selbstbestimmte Entscheidung macht die Einwilligung des informier-

12 Vgl. Homepage des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Gesichtserkennungsfunktion von Facebook verstößt gegen europäisches und deutsches Datenschutzrecht, abrufbar unter: http://www.datenschutz-hamburg.de/news/detail/article/gesichtserkennungsfunktion-von-facebook-verstoesst-gegen-europaeisches-und-deutsches-datenschutzrech.html [Stand: 02.02.2012].

13 Juris GmbH (Fn. 5).

14 Die Gruppe wurde durch Artikel 29 der Richtlinie 95/46/EG (Datenschutzrichtlinie) vom 24. Oktober 1995 eingesetzt. Ihre amtliche Bezeichnung lautet Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten.

15 Entwickelt aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und dem daraus entnommenen Allgemeinen Persönlichkeitsrecht; siehe Fn. 33.

ten Nutzers erforderlich. Facebook sollte dies erkennen und unseren Forderungen schnell nachkommen."[16]

Ähnlich kritisch beurteilt die Bundesministerin für Ernährung, Landwirtschaft und Verbraucherschutz, **Ilse Aigner,** die Gesichtserkennungsfunktion. Sie hält das Einführen der automatischen Gesichtserkennung bei Facebook für datenschutzrechtlich bedenklich.[17] Um dem Einhalt zu gebieten, wende sie sich jetzt direkt an die US-Behörden. Sogar eine diesbezüglich Beschwerde bei der **US-Handelskommission FTC**[18] sei in Erwägung gezogen worden. Gegenstand sei hierbei insbesondere, dass Facebook eine große Datenbank mit biometrischen Daten der Nutzer aufbaue, ohne zuvor für die Speicherung und Verarbeitung das Einverständnis der betroffenen Nutzer eingeholt zu haben. Dadurch verstoße Facebook nicht nur gegen deutsches und europäisches, sondern auch gegen amerikanisches Recht in Form des **Safe-Harbor-Abkommens**[19] über den Datenaustausch zwischen Europa und den USA.[20]

Neben dem Verbraucherschutzministerium versuchen noch zwei weitere Bundesministerien – die für Inneres und Justiz – den Datenschutz im Internet zu verbessern. Der frühere Bundesminister des Inneren, **Thomas de Maizière**, hatte unter anderem einen Gesetzesentwurf zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht erarbeiten lassen.[21] Diese Initiative steht im Zusammenhang mit dem Versuch, Grundsätze für eine „Netzpolitik" der Bundesregierung festzulegen. Auch die Bundesministerin der Justiz beteiligt sich an der Diskussion. So schreibt Justizministerin **Sabine Leutheusser-Schnarrenberger**, das Datenschutzrecht müsse „ausgleichen zwischen einer möglichst freien Kommunikation und dem Recht, selbst zu bestim-

16 Vgl. Veröffentlichung auf der Homepage des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, abrufbar unter: http://www.datenschutz-hamburg.de/news/detail/article/gesichtserkennungsfunktion-von-facebook-verstoesst-gegen-europaeisches-und-deutsches-datenschutzrech.html [Stand: 02.02.2012].

17 Heise Online, Gesichtserkennung bei Facebook: Ilse Aigner reicht Beschwerde ein, 2011, abrufbar unter: http://www.heise.de/newsticker/meldung/Gesichtserkennung-bei-Facebook-Ilse-Aigner-reicht-Beschwerde-ein-1393446.html [Stand: 12.01.2012].

18 Federal Trade Commission, zu Deutsch etwa „Bundeshandelskommission".

19 Englisch für „Sicherer Hafen" - ist eine besondere Datenschutz-Vereinbarung zwischen der Europäischen Union und den Vereinigten Staaten, die es europäischen Unternehmen ermöglicht, personenbezogene Daten legal in die USA zu übermitteln.

20 Siehe Fn. 17.

21 Gesetzesentwurf abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf;jsessionid=A76467562C6FAB0A0B9CC63B6E5B7C24.2_cid165?__blob=publicationFile [Stand: 10.01.2012].

men, was über die eigene Person veröffentlicht wird“, und plädiert deshalb für eine „umfassende gesetzliche Regelung“.[22]

„Entwarnung“ hingegen gab die **irische Datenschutzbehörde**[23], die eine dreimonatige umfangreiche Untersuchung gegen das soziale Netzwerk Facebook nunmehr abgeschlossen und in Form eines **Prüfungsberichts** am 21. Dezember 2011 veröffentlicht hat.[24] Besonders hervorzuheben ist dabei, dass keine Verstöße gegen geltendes irisches Recht festgestellt wurden.[25] Die Untersuchung hat das soziale Netzwerk in so fern auch entlastet, als die Behörde keine Hinweise auf die Speicherung von Daten solcher Nutzer fand, die nicht Mitglied bei Facebook sind. Allerdings werden verschiedene Nachbesserungen von Facebook gefordert, die innerhalb von sechs Monaten umgesetzt werden sollen. Facebook habe sich bereits dazu bereit erklärt, Anwender zukünftig besser über die Erhebung von Daten und über verschiedene Techniken, wie beispielsweise die Gesichtserkennung in Bildern, zu informieren. Darüber hinaus wolle Facebook zukünftig gelöschte Nutzerdaten schneller von den Servern entfernen. So sollen beispielsweise gespeicherte Klicks auf Werbeanzeigen nach spätestens zwei Jahren gelöscht werden.[26]

Die irischen Datenschützer haben darüber hinaus von Facebook gefordert, dass die Nutzung von Facebook-Apps anderer Anbieter transparenter gestaltet wird. Auch die Verwendung von Nutzerdaten für gezielte Werbung soll klarere Grenzen erhalten. Die irische Behörde will im Juli 2012 prüfen, wie die Forderungen und Vorgaben von Facebook angenommen und umgesetzt worden sind.[27]

Zweifellos lassen sich etliche positive wie auch negative Aspekte zum Thema „Soziale Netzwerke“ feststellen.[28] Kommt es zu einer ungewollten Veröffentlichung der eigenen Person in Form

---

22 Leutheusser-Schnarrenberger, Den Datenschutz rundum erneuern, Hamburger Abendblatt v. 06.12.2010, S. 2. Abrufbar unter: http://www.abendblatt.de/hamburg/article1717839/Den-Datenschutz-rundum-erneuern.html [Stand: 09.02.2012]; Bull, NVwZ 2011, 257 (257).

23 Office of the Data Protection Commissioner. Canal House, Station Road, Portarlington, Co. Laois, Ireland, unter der Leitung des Datenschutzbeauftragten (Data Protection Commissioner), Billy Hawkes.

24 Report of Data Protection Audit of Facebook Ireland, published 21 December 2011, abrufbar unter: http://dataprotection.ie/viewdoc.asp?m=f&fn=/documents/Facebook Report/final report/report.pdf [Stand: 31.01.2012].

25 Dieses Ergebnis wurde auch von Facebook unter dem Titel: „Facebook and the Irish Data Protection Commission „ veröffentlicht, vgl.: https://www.facebook.com/notes/facebook-public-policy-europe/facebook-and-the-irish-data-protection-commission/288934714486394 [Stand: 31.01.2012].

26 Office of the Data Protection Commissioner Ireland, Report of Data Protection Audit of Facebook Ireland, published 21 December 2011, abrufbar unter: http://dataprotection.ie/viewdoc.asp?m=f&fn=/documents/Facebook Report/final report/report.pdf [Stand: 31.01.2012].

27 Siehe Fn. 26.

28 Vgl. etwa eine Zusammenstellung positiver wie negativer Aspekte im Rahmen der Initiativstellungnahme des Europäischen Wirtschafts- und Sozialausschusses vom 04.11.2009, dort unter 3.3. und 3.4. aufgeführt, abrufbar

eines vielleicht sogar kompromittierenden Fotos auf einer weltweit zugänglichen und für jeden zugreifbaren Internetseite zählt dies sicherlich zu den weniger positiven Aspekten des „Social Networks“. Somit stellt sich die Frage, wie der Betroffene in einem solchen Fall vorgehen kann.

3. Rechtsschutzmöglichkeiten des Betroffenen - Ansprüche aus deutschem Recht und deren Anwendbarkeit

Für eine betroffene Privatperson kommen insbesondere folgende Ansprüche in Betracht:

- Ansprüche aus dem BDSG[29] und dem TMG[30] insbesondere auf Löschung der Bilddaten als personenbezogene Daten im Sinne des § 35 Abs. 2 S. 2 Nr. 1 BDSG

- Anspruch auf Unterlassung gemäß § 1004 Abs. 1 S. 2 analog i.V.m. § 823 Abs. 2 BGB[31] i.V.m. §§ 22, 23 KUG[32]

- Anspruch auf Beseitigung gemäß §§ 823 Abs. 2 i.V.m. 249 ff. BGB i.V.m. §§ 22, 23 KUG

- Anspruch auf Schadensersatz gemäß § 823 Abs. 2 BGB i.V.m. §§ 22, 23 KUG

- Anspruch auf Schadensersatz in Form von Schmerzensgeld gemäß § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[33]

---

unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:128:0069:0073:DE:PDF [Stand: 22.01.2012).

29 Bundesdatenschutzgesetz in der Fassung der Bekanntmachung v. 14.01.2003, BGBl. I S. 66, zuletzt geändert durch Art. 1 des Gesetzes v. 14.8.2009, BGBl. I S. 2814.

30 Telemediengesetz in der Fassung der Bekanntmachung v. 26.02.2007, BGBl. I S. 179, zuletzt geändert durch Art. 1 des Gesetzes v. 31.06.2010, BGBl. I S. 692.

31 Bürgerliches Gesetzbuch (BGB) in der Fassung der Bekanntmachung v. 02.01.2002, BGBl. I S. 42, ber. S 2909 und BGBl. I 2003 S. 738, zuletzt geändert durch Art. 1 des Gesetzes v. 27.07.2011, BGBl. I S. 1600.

32 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturhebergesetz - KUG) vom 9. Januar 1907 (RGBl. S. 7), BGBl. III/FNA 440-3. Das Gesetz wurde durch § 141 Nr. 5 Urheberrechtsgesetz vom 9.9.1965 (BGBl. I S. 1273); Nr. 65 mit Wirkung vom 1.1.1966 aufgehoben, soweit es nicht den Schutz von Bildnissen betrifft und zuletzt geändert durch Art. 145 Einführungsgesetz zum Strafgesetzbuch vom 2.3.1974 (BGBl. I S. 469) und Art. 3 § 31 Gesetz zur Beendigung der Diskriminierung gleichgeschlechtlicher Gemeinschaften: Lebenspartnerschaften vom 16.2.2001 (BGBl. I S. 266).

33 Grundgesetz für die Bundesrepublik Deutschland (GG) v. 23.05.1949, BGBl. 1949 S. 1, in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 1 des Gesetzes v. 21.07.2010, BGBl. I S. 944.

- Anspruch auf Herausgabe des Bildmaterials gemäß § 1004 Abs. 1 S. 2 analog i.V.m. §§ 823 Abs. 1, 249 S. 1 BGB

3.1. Anspruch auf Löschung der Bilddaten gem. § 35 Abs. 2 S. 2 Nr. 1 BDSG – Anwendbarkeit des BDSG und des TMG

§ 35 Abs. 2 S. 2 BDSG knüpft die Pflicht der verantwortlichen Stelle (in diesem Fall das Unternehmen Facebook), gespeicherte Daten zu löschen, an die Unzulässigkeit der Speicherung dieser Daten.

Fraglich ist zunächst die **Anwendbarkeit** der Vorschrift:

Das BDSG regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Unter dem Begriff der personenbezogenen Daten versteht man gem. § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. Der Begriff erfasst auch fotografische Ablichtungen einer Person, da durch sie unter anderem das Aussehen und Erscheinungsbild der betroffenen Person und somit auch persönliche Verhältnisse im Sinne der Vorschrift vermittelt werden.[34]

Das BDSG folgt grundsätzlich dem **Territorialprinzip.**[35] Nach diesem Grundsatz gelten für alle verantwortlichen Stellen, die personenbezogene Daten in Deutschland erheben, verarbeiten oder nutzen, die Vorschriften des BDSG.[36] Vorausgesetzt, das Anbieten und Verwalten der Dienste eines sozialen Netzwerkes durch Facebook erfülle die Merkmale des „Erhebens, Verarbeitens oder Nutzens“, käme die Anwendbarkeit deutscher Rechtsvorschriften in Betracht.

Eine **Ausnahme zu diesem Grundsatz** besteht jedoch für den **grenzüberschreitenden Datenverkehr innerhalb der EU bzw. des EWR**[37], da gem. Art. 4 Abs. 1 lit. 1) der **Richtlinie 95/46/EG** (sog. Datenschutzrichtlinie[38]) die europäischen Mitgliedstaaten ihre jeweiligen **nationalen Daten-**

34 VG Hamburg, DuD 1981, 57; VG Wiesbaden, DVBl. 1981, 790 (792).

35 Gola/Schomerus, BDSG § 1 Rn. 28.

36 RegE zum BDSG, BT-Drs. 14/4329, S. 31 f.

37 Europäischer Wirtschaftsraum.

38 Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html [Stand: 31.01.2012].

schutzvorschriften auf alle datenschutzrelevanten Tätigkeiten anzuwenden haben, die ein Verantwortlicher durch eine Niederlassung in ihrem Hoheitsgebiet ausführt.[39]

Unter Berücksichtigung dieses Aspektes käme mit Blick auf das Unternehmen Facebook und dessen irischer Niederlassung die Anwendbarkeit der irischen Datenschutzvorschriften in Betracht, da für den grenzüberschreitenden Datenverkehr im Binnenmarkt der EU diese Richtlinie das Territorialprinzip aufhebt und das anwendbare Recht an den Ort der Niederlassung des Verantwortlichen knüpft (sog. **Sitz- bzw. Niederlassungsprinzip**).[40]

Die Anwendbarkeit des BDSG, und somit auch die Entscheidung über das jeweils anzuwendende Zuständigkeitsprinzip bestimmt sich insbesondere nach **§ 1 Abs. 5 BDSG**.[41]

Der Vorschrift entsprechend sind drei verschiedene Fallkonstellationen zu unterscheiden:

a) ein Unternehmen, das nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, führt datenschutzrelevante Handlungen in Deutschland aus (Satz 2, Anwendung des **Territorialprinzips**, Geltung des BDSG)[42],

b) ein in einem Mitgliedstaat der EU/EWG belegenes Unternehmen, das eine funktionale und effektive (Haupt-)Niederlassung in Deutschland selbst unterhält, führt datenschutzrelevante Handlungen in Deutschland aus (Satz 1 a.E., Geltung des BDSG),

c) Ein in einem Mitgliedstaat der EU/EWG belegenes Unternehmen, das keine maßgebende Niederlassung in Deutschland selbst unterhält, führt datenschutzrelevante Handlungen[43] in Deutschland aus (Satz 1, Anwendung des **Sitzprinzips**, keine Geltung des BDSG).

Von einer **Niederlassung** ist nach Erwägungsgrund 19 der EU-Datenschutzrichtlinie auszugehen, wenn die Tätigkeit effektiv und tatsächlich von einer **„festen Einrichtung“** ausgeübt wird[44], das Unternehmen also von diesem Standpunkt aus in funktionaler Hinsicht agiert.

---

39 Jotzo, MMR 2009, 232 (237).

40 Gola/Schomerus, § 1 Rn. 28.

41 Ausführlich hierzu: Simitis, BDSG § 1 Rn. 7.

42 Vgl. auch Anmerkung zum Urteil vom 02.08.2011, Az. 7 U 134/10 des OLG Hamburg 7. ZS von Dr. Hans-Werner Moritz in JurisPR-ITR 24/2011 Anm. 5.

43 Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten.

44 RegE zum BDSG, BT-Drs. 14/4329, S. 31; Gola/Schomerus, § 1 Rn. 28.

Der **deutsche Geschäftssitz des Unternehmens Facebook in Hamburg**[45] ist ausschließlich mit der Akquisition und Betreuung von Werbekunden betraut. Eine Verarbeitung, Nutzung oder Erfassung personenbezogener Daten der Nutzer findet an diesem Ort nicht statt. Somit kommt als Niederlassung im Sinne des § 1 Abs. 5 BDSG lediglich die **europäische Hauptniederlassung in Irland** (Facebook Ireland Limited) in Betracht und somit Fall c).

Demnach ist zu unterscheiden, ob **Facebook Ireland Ltd.** als eine in einem anderen Mitgliedstaat der EU bzw. EWG belegene verantwortliche Stelle gemäß Satz 1 der Vorschrift personenbezogene Daten in Deutschland erhebt, verarbeitet oder nutzt. In diesem Fall käme das Sitzlandprinzip zur Anwendung und die Rechtmäßigkeit der Handlungen wäre **nicht** an den deutschen Normen des BDSG und des TMG zu messen. Sofern allerdings diese datenschutzrelevante Handlungen von einem **außerhalb** der EU/EWG belegenen Unternehmen ausgehen, etwa dem anderen Hauptsitz des Unternehmens: **Facebook Inc. in den USA**[46], käme das Territorialprinzip zur Anwendung und die deutschen Rechtsvorschriften wären zu beachten.

Entscheidend ist somit, welche Niederlassung (Hauptkonzernsitz in den USA oder aber die europäische Niederlassung in Irland) für die Nutzerdatensammlung verantwortlich ist.

Eine Anwendung irischer Rechtsvorschriften kommt nur dann in Betracht, wenn Facebook Ireland Ltd.[47] die verantwortliche Stelle im Sinne des § 1 Abs. 5 BDSG ist und nicht Facebook Inc. in den USA. Dies wäre dann der Fall, wenn die Niederlassung in Irland sich lediglich der Mittel wie beispielsweise der Serverleistungen des Konzerns in den USA zur Nutzerdatensammlung bedient und diese dort im Auftrag für Facebook Ireland Ltd. **weisungsgebunden** verwaltet werden (**sog. Auftragsdatenverwaltung**, § 11 BDSG).

Genau dies trifft auf den vorliegenden Fall zu:

Nach eigenen Angaben[48] von Facebook sind die Zeiten längst vorbei, in denen das Unternehmen noch in den Kinderschuhen steckte und vollständig durch den damals einzigen Hauptverwaltungssitz Facebook Inc. in den USA geleitet wurde. Spätestens **2009 mit Gründung eines neuen Hauptquartiers in Dublin, Irland**[49] wurde durch den neuen zusätzlichen Sitz in Europa die Unternehmensstruktur maßgeblich verändert. Facebook Ltd. in Irland unterliegt der dortigen Daten-

45 Facebook Germany GmbH, Großer Burstah 50-52, 20457 Hamburg.

46 Facebook Incorporated, 1601 S California Ave, Palo Alto, California, Vereinigte Staaten. Facebook, Inc. ist eine nach dem Recht des Staates Delaware gegründete und registrierte Gesellschaft.

47 Facebook Ireland Limited, Hanover Reach, 5-7 Hanover Quay, Dublin 2 Ireland.

48 Allan, Richard, Facebook's director of policy in Europe, Email vom 16. November 2011 an einen Abgeordneten des Deutschen Bundestages.

49 Im Folgenden auch Facebook Ltd.

schutzkommission[50] und **verwaltet selbständig persönliche Daten von deutschen Facebook-Nutzern**. Von den etwa 3000 Facebook-Mitarbeitern weltweit[51] sind mit ca. 350 Angestellten eine gewichtige Anzahl für die Niederlassung in Irland tätig. Auch ist die Facebook Ltd. für sämtliche Facebook-Nutzer europaweit der maßgebliche Vertragspartner. Entscheidend ist, dass die **Facebook Ltd. in Irland unabhängig** von der amerikanischen Facebook Inc. Entscheidungen über die Nutzung und Verwendung der Datenverarbeitung aller Daten europäischer Facebook-Nutzer trifft.

Facebook Ltd. stellt somit eine „**Niederlassung" nach Erwägungsgrund 19 der EU-Datenschutzrichtlinie** dar, da die maßgeblichen Tätigkeiten in einem EU-Mitgliedsstaat selbständig, effektiv und tatsächlich durch diesen Verwaltungssitz von einer „festen Einrichtung" ausgeübt werden und das weltweit agierende Unternehmen Facebook von diesem Standpunkt aus auch in funktionaler Hinsicht europaweit agiert.

Ein Unternehmen, das datenschutzrelevante Handlungen von seiner Niederlassung im innereuropäischen Ausland aus vornimmt, unterliegt nicht den Datenschutzbestimmungen des BDSG und TMG, § 1 Abs. 5 Satz 1 BDSG (s.o.). Ein Unternehmen erhebt dann Daten im Inland, wenn es normativ betrachtet hierzu auf im Inland belegene Computer der Nutzer zurückgreift. Das ist der Fall, wenn sich das Angebot äußerlich erkennbar (auch) an deutsche Nutzer richtet. So verhält es sich mit dem deutschen Internetauftritt von Facebook.

Da Unternehmen erst dann in den Anwendungsbereich von BDSG und TMG gelangen, wenn der Datenumgang zumindest auch über eine in Deutschland belegene Niederlassung erfolgt,[52] und wie bereits erwähnt der Geschäftssitz von Facebook in Hamburg keine diesbezüglichen datenschutzrelevanten Handlungen vornimmt, fehlt in Deutschland eine Niederlassung als notwendige Voraussetzung für die Anwendbarkeit des BDSG und TMG.

Dies führt zu folgendem Ergebnis:

Die internationale Anwendbarkeit deutschen Datenschutzrechts richtet sich nach § 1 Abs. 5 BDSG. Das gilt auch für die in §§ 11 ff. TMG enthaltenen Datenschutzbestimmungen.

§ 1 Abs. 5 BDSG beruht auf dem Territorialprinzip. Für den grenzüberschreitenden Datenverkehr innerhalb der EU bzw. des EWR knüpft § 1 Abs. 5 in Umsetzung der europäischen Datenschutz-

---

50 Office of the Data Protection Commissioner. Canal House, Station Road, Portarlington, Co. Laois, Ireland, unter der Leitung des Datenschutzbeauftragten (Data Protection Commissioner), Billy Hawkes.

51 Laut eigenen Angaben von Facebook, abrufbar unter: http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 [Stand: 31.01.2012].

52 Vgl. Jotzo, MMR 2009, 232 (234).

richtlinie das anwendbare Recht allerdings an den Ort der Niederlassung der verantwortlichen Stelle (Sitz- oder Niederlassungsprinzip).

Facebook erhebt, nutzt und speichert als innerhalb der EU aber nicht im Inland belegenes Unternehmen in Deutschland personenbezogene Daten und unterliegt somit gem. § 1 Abs. 5 S. 2 BDSG unter Anwendung des Niederlassungsprinzips den deutschen Vorschriften des BDSG und TMG nicht.[53] Ansprüche aus diesen Gesetzen sind demnach nicht durchsetzbar.

3.2. Andere zivilrechtliche Ansprüche - Anwendbarkeit des BGB

Anders als bei Ansprüchen aus dem BDSG und TMG, ist für sämtliche zivilrechtlichen Ansprüche, die sich aus dem unerlaubten Umgang mit personenbezogenen Daten ergeben und somit in den Bereich der „**unerlaubten Handlung**“ fallen, das anwendbare Recht nach dem allgemeinen **Deliktstatut** zu bestimmen (**Art. 40 Abs. 1 EGBGB**[54]).[55]

Dies bedeutet, dass anders als bei den speziell datenschutzrechtlichen Ansprüchen hier die Ansprüche aus deutschem Recht vor deutschen Gerichten durchsetzbar sind, allerdings nur, wenn zwei Voraussetzungen erfüllt werden:

Zum Einen muss es sich um Ansprüche aus „unerlaubter Handlung“, also deliktische Ansprüche handeln, zum Anderen muss der Ersatzpflichtige in Deutschland gehandelt haben.

Letztere Voraussetzung ist wie oben dargelegt jedenfalls dann erfüllt, sofern sich der Betroffene gegen die Facebook Ltd. als Anspruchsgegner wendet, da Facebook als innerhalb der EU aber nicht im Inland belegenes Unternehmen in Deutschland personenbezogene Daten erhebt, nutzt und speichert (s.o.). Aber auch bezüglich des Uploaders[56] werden die Voraussetzungen erfüllt, wenn dieser Bilder in Deutschland hochgeladen hat.

Somit ist zu klären, ob die genannten zivilrechtlichen Ansprüche des BGB deliktische Ansprüche i.S.d. Art. 40 Abs. 1 EGBGB sind.

---

53 Vgl. Hoeren, Risiken für Unternehmen und Privatnutzer, Deutscher AnwaltSpiegel 2011, 9 (10).

54 Einführungsgesetz zum Bürgerlichen Gesetzbuche v. 21.09.1994, BGBl. I S. 2494; 1997 I S. 1061, zuletzt geändert durch Art. 2 des Gesetzes v. 27.07.2011, BGBl. I S. 1600, 1942.

55 Jotzo, MMR 2009, 232 (237).

56 Person, die die Abbildung auf der Internetseite Facebook eingestellt hat.

Neben dem zuvor besprochenen Anspruch aus dem BDSG, handelt es sich bei den restlichen oben aufgeführten Ansprüchen[57] vollumfänglich um Anspruchsgrundlagen, die sich insbesondere auch auf § 823 BGB stützen. Der § 823 BGB ist deliktischer Natur. Er stellt im Bereich der „unerlaubten Handlungen“ des BGB an vorderster Stelle stehend schon rein systematisch die wichtigste **deliktische Norm** dar. Sofern der Ersatzpflichtige in Deutschland gehandelt hat, käme nach Art. 40 Abs. 1 EGBGB folglich deutsches Recht zur Anwendung.[58]

3.2.1. Anspruch auf Unterlassung gem. § 1004 Abs. 1 S. 2 analog i.V.m. § 823 Abs. 2 BGB i.V.m. §§ 22, 23 KUG

Dieser Anspruch ist auf die Beseitigung der Rechtsbeeinträchtigung gerichtet; im vorliegenden Fall käme das einer **Löschung der beanstandeten Datensätze, also des Bildes** gleich, sogenannte „Verbreiterhaftung“, um die Erstveröffentlichung des Bildes oder eine wiederholte Veröffentlichung zu verhindern.

Fraglich sind zunächst die örtliche gerichtliche Zuständigkeit (sog. **Gerichtsstand**) und damit zusammenhängend auch die Frage des anzuwendenden Rechtsgebietes. Grundsätzlich richtet sich der Gerichtsstand vorliegend gemäß § 32 ZPO[59] i.V.m. Art. 40 Abs. 1 EGBGB nach der **sog. Tatortregel**, wonach das Recht des Landes anzuwenden ist, in dem der Tatort der Persönlichkeitsrechtsverletzung liegt.[60] Als Tatort kommen sowohl der **Ort der Handlung** als auch der **Ort des Erfolges** in Betracht, sog. **Ubiquitätsprinzip**.[61]

Bezogen auf **Persönlichkeitsrechtsverletzungen im Internet** ist Handlungsort der Ort, an dem der Täter die unerlaubte Handlung ausgeführt hat, also die persönlichkeitsrechtsverletzende Information in das Netz eingespeist hat[62] – im vorliegenden Fall also Deutschland. Als Erfolgsort gilt

57 Siehe Ausführungen oben: „3. Rechtsschutzmöglichkeiten des Betroffenen – Ansprüche aus deutschem Recht und deren Anwendbarkeit“.

58 Vgl. Thorn, in: Palandt, Art. 40 EGBEB, Rn. 10; es bestehe weitgehende Einigkeit darüber, dass Ansprüche aus Persönlichkeitsrechtsverletzungen regelmäßig deliktsrechtich qualifiziert werden (Deliktsstatut). Dies gelte nicht nur für Schadensersatzansprüche, sondern auch für die Ansprüche auf Unterlassung und Beseitigung.

59 Zivilprozessordnung (ZPO) in der Fassung der Bekanntmachung v. 5.12.2005, BGBl. I S. 3202 (2006 I S. 431) (2007 I S. 1781), zuletzt geändert durch Art. 3 des Gesetzes vom 22.12.2011, BGBl. I S. 3044. geändert worden ist. § 32 erfasst in der sog. doppelfunktionalen Auslegung sowohl die Frage des internationalen wie nationalen Gerichtsstandes und ist darüber hinaus auch auf Unterlassungsansprüche anwendbar, vgl. BGH, AfP 2010, 167 (168).

60 Gounalakis/Rhode, S. 7 Rn. 12.

61 Hoffmann, § 11 Rn. 23; s.a. Art. 2 ff. EuGVVO = Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen. Bezüglich deliktischen Ansprüchen s. insb. Art. 5 Nr. 3 EuGVVO.

62 BGH NJW 1994,2888 (2890); Gounalakis/Rhode (Fn. 60).

prinzipiell der Ort, an dem die Persönlichkeitsrechtsverletzung eintritt, also die Abbildung der beeinträchtigten Privatperson abrufbar ist.[63] Dabei steht es dem Betroffenen gem. **Art. 40 Abs. 1 S. 2 EGBGB** frei, unter den verschiedenen Orten das ihm **günstigste Recht** zur Anwendung zu bringen.[64]

Speziell in Fällen der Persönlichkeitsrechtsverletzung durch Informationen im Internet ist umstritten, vor welchen Gerichten die damit verbundenen Ansprüche durchgesetzt werden können, da im Internet vermittelte Inhalte üblicherweise **weltweit abrufbar** sind und somit auch eine unüberschaubare Vielzahl von in Betracht zu ziehenden Erfolgsorten zu einem **uneingeschränkten Haftungsrisiko** führt.[65]

Die höchstrichterliche Rechtsprechung stellt in solchen Fällen darauf ab, ob die als rechtsverletzend beanstandeten Inhalte objektiv einen deutlichen **Bezug zum Inland** in dem Sinne aufweisen, dass eine **Kollision der widerstreitenden Interessen** (Interesse des Klägers an der Achtung seiner Rechte, Interesse des Beklagten an der freien Gestaltung der Inhalte auf Facebook) im Inland tatsächlich eintreten kann.[66]

Davon ausgehend, dass sowohl der Abgebildete als auch der Uploader den überwiegenden Teil ihrer auf Facebook mit ihnen verknüpften sozialen Kontakte im Inland haben und somit die Abbildung einen Inlandsbezug aufweist und darüber hinaus eine **Persönlichkeitsbeeinträchtigung im Inland** eintritt, begründet bereits dieses Merkmal den Erfolgsort und somit die **Zuständigkeit deutscher Gerichte**.

Die weiteren **Voraussetzungen** des Anspruchs sind vergleichsweise unproblematisch, so dass im Folgenden lediglich die wichtigsten Erwägungen **kurz skizziert** werden:

Durch die Veröffentlichung der Abbildung ohne die Einwilligung des Berechtigten liegt grundsätzlich eine Beeinträchtigung des **Rechtes am eigenen Bild gemäß §§ 22, 23 KUG** vor.

Weiterhin ist die **sog. Störerhaftung** eines Online-Dienstanbieters zu berücksichtigen, die die Rechtswidrigkeit davon abhängig macht, inwiefern er Kenntnis von den rechtswidrigen Handlungen hat.[67] Erforderlich ist daher, dass der anspruchstellende Benutzer vor einer gerichtlichen Geltendmachung des Anspruchs die zuständige Stelle des Unternehmens Facebook auf die

63 LG München I, RIW 2000, 466 (467); BGH NJW 2001, 624; Gounalakis/Rhode (Fn. 60), Rn. 14.

64 Heldrich, in: Palandt, Art. 40 EGBEB, Rn. 4.

65 Vgl. zum Ganzen auch: Roth, S. 254 f.

66 BGH, GRUR 2005, 431 (433); BGH, MMR 2010, 167 (169); Pichler, in: Hoeren/Sieber, Handbuch Multimedia-Recht, Kap. 25 Rn. 210.

67 BGH, MMR 2004, 68; Hoeren, in Hoeren/Sieber, aaO. Rn. 68.

Rechtsverletzung aufmerksam macht. Sofern diese **innerhalb der ihr zustehenden Möglichkeiten** (sowohl in technischer als auch zeitlicher Hinsicht) keine Vorkehrungen zur Beseitigung trifft (sog. „notice and take down approach“) und zumutbare Prüfungspflichten verletzt[68], liegt eine anspruchsbegründende **rechtswidrige Beeinträchtigung** vor.

3.2.2. Anspruch auf Beseitigung gemäß §§ 823 Abs. 2 i.V.m. 249 ff. BGB i.V.m. §§ 22, 23 KUG

Bezüglich der Anwendbarkeit der Normen wird auf die Ausführungen zum Anspruch auf Unterlassung gem. § 1004 Abs. 1 S. 2 BGB (s.o. 3.2.1.) verwiesen.

Im Unterschied zum Anspruch auf Löschung gem. § 35 Abs. 2 BDSG ist der Anspruch gem. §§ 823 Abs. 2 BGB **verschuldensabhängig**, erfordert also **zumindest fahrlässiges Verhalten** und somit gemäß § 276 Abs. 2 BGB ein „Außerachtlassen der im Verkehr erforderlichen Sorgfalt“.

Auch an dieser Stelle sind die **Grundsätze der Störerhaftung** im Zusammenhang mit der Frage des Täterbegriffs des § 823 BGB zu berücksichtigen; bezüglich der Ausführungen zu diesem Punkt kann inhaltlich im Wesentlichen auf das voran Gesagte verwiesen werden.

Die weiteren Anspruchsvoraussetzungen liegen ebenfalls vor. Der Anspruch ist inhaltlich darauf gerichtet, den Zustand wiederherzustellen, der ohne das beeinträchtigende Ereignis (die Veröffentlichung der Abbildung auf Facebook) bestehen würde (sog. **Grundsatz der Naturalrestitution**), § 249 Abs. 1 BGB. In der Praxis bedeutet dies auf den konkreten Fall übertragen, dass der Geschädigte insbesondere die Löschung des Fotos verlangen kann.

3.2.3. Weitere in Betracht kommende Anspruchsgrundlagen

Die unter 3.2.1. und 3.2.2. vorgestellten Ansprüche ermöglichen mit ihrer Rechtsfolge das wohl wichtigste Ziel des Betroffenen, nämlich die Löschung der beanstandeten Datensätze, also des unerwünschten Bildes.

Daneben seien noch drei weitere ebenfalls denkbare Ansprüche, mit jeweils anderen Rechtsfolgen, erwähnt.

68 Ohrmann, 113, (208 ff.).

Anspruch auf Schadensersatz gemäß § 823 Abs. 2 BGB i.V.m. §§ 22, 23 KUG:

Hier ist neben dem Ersatz des konkreten Schadens nach der sogenannten Lizenzanalogie (aus § 97 Abs. 1 S. 1 UrhG) eine fiktive Lizenzgebühr für die Verwendung des Bildes zu bezahlen und ein etwaiger Gewinn (etwa wegen der Steigerung der Auflage) herauszugeben. Dabei gestaltet sich bereits die Berechnung der fiktiven Lizenzgebühr als relativ kompliziert, ist in der Praxis jedoch die am häufigsten vorkommende Berechnungsmethode.[69]

Ob dieser Schadensersatzanspruch, der vorrangig im Zusammenhang mit Veröffentlichungen von Fotos bekannter Personen[70] in Zeitungen und anderen Printmedien seitens des Betroffenen herangezogen wird, auch im Rahmen der aufgezeigten Facebook-Problematik durchgreifen kann, sei der künftigen Rechtsprechung überlassen.

Anspruch auf Schadensersatz in Form von Schmerzensgeld gemäß § 823 Abs. 2 i.V.m. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG:

Wurde durch die Veröffentlichung schwerwiegend in das „Recht am eigenen Bild“[71] eingegriffen, beispielsweise durch die Veröffentlichung von Nacktfotos, kann auch ein Anspruch auf Entschädigung in Geld für einen immateriellen Schaden (Schmerzensgeld) bestehen. Dieser Anspruch soll neben der Genugtuungsfunktion für das Opfer auch eine Präventionsfunktion für den Verletzer haben und stützt sich auf das aus dem Grundgesetz aus Art. 1 Abs. 1 (Menschenwürde) in Verbindung mit Art. 2 Abs. 1 GG (freie Entfaltung der Persönlichkeit) abgeleitete „Allgemeine Persönlichkeitsrecht“.[72] Auch hier bleibt die Übertragbarkeit auf den vorliegenden Fall klärungsbedürftig.

---

69 Wanckel, Foto- und Bildrecht, S. 182 Rn. 282.

70 Insbesondere in Bezug auf sogenannte „Absolute und relative Personen der Zeitgeschichte“ in diversen juristischen Veröffentlichungen betreffend Caroline von Monaco/Hannover diskutiert, vgl. etwa BGH Urteil vom 29.10.09 - I ZR 65/07, dort m.w.N.

71 Speziell zum „Recht am eigenen Bild“ und zum „Bildnisschutz in Europa“ allgemein siehe: Neukamm, Bildnisschutz in Europa.

72 Vergleiche die vom Bundesverfassungsgericht hergeleiteten Fallgruppen des Allgemeinen Persönlichkeitsrechts, insbesondere das „Recht auf informationelle Selbstbestimmung“ (s. etwa BVerfG, 1 BvR 209/83 vom 15.12.1983) und das „Recht am eigenen Bild“ (s. etwa BVerfG, 1 BvR 1168/04 vom 22.8.2006).

Anspruch auf Herausgabe des Bildmaterials gemäß § 1004 Abs. 1 S. 2 analog i.V.m. §§ 823 Abs. 1, 249 S. 1 BGB

Letztlich käme auch ein Anspruch auf Herausgabe des Bildmaterials in Betracht. Dieser Anspruchs stützt sich innerhalb der Verweisungskette ebenfalls auf den deliktischen § 823 BGB, so dass die nötige deliktische Natur ebenfalls begründet werden kann. Ob der Anspruch auch in den speziellen Fällen der Facebook-Bildveröffentlichung durchgreifen kann, bleibt klärungsbedürftig, so dass auch diesbezüglich künftige Urteile der Judikative abzuwarten sind.

3.2.4. Mögliche Anspruchsgegner

Zusammenfassend stehen dem Betroffenen für die Löschung von Bildern somit vorrangig folgende Ansprüche zu:

- Anspruch auf Unterlassung gem. § 1004 Abs. 1 S. 2 analog i.V.m. § 823 Abs. 2 BGB i.V.m. §§ 22, 23 KUG

- Anspruch auf Beseitigung gem. §§ 823 Abs. 2 i.V.m. 249 ff. BGB i.V.m. §§ 22, 23 KUG

Für beide Ansprüche kommen **jeweils zwei Personen als Anspruchsgegner** in Betracht.

Zum einen das **Unternehmen Facebook** in Form des irischen Hauptquartiers in Dublin, das als englische „Limited“ im Rechtsverkehr auftritt. Die Limited, als Rechtsform eine eigenständige „juristische Person“, hat die Fähigkeit eigenständiger Träger von Rechten und Pflichten sein zu können. Daher kann sie selbst verklagt werden und für den von der ungewollten Bildveröffentlichung Betroffenen der richtige Anspruchsgegner sein.

Zum anderen kann die Person, die die Abbildung auf der Internetseite Facebook eingestellt hat (sog. **Uploader**) richtiger Anspruchsgegner sein.

Inhaltlich weisen diese Ansprüche auch unter Berücksichtigung der unterschiedlichen Anspruchsgegner keine Besonderheiten auf, so dass im Wesentlichen auf die vorangehende Argumentation verwiesen werden kann. Dies gilt insbesondere in Bezug auf die Anwendbarkeit der Normen. Da in der Konstellation Betroffener -> Nutzer die Frage der internationalen Gerichtszuständigkeit keine Rolle spielt (s.o.), liegen sowohl der Erfolgs- als auch der Handlungsort regelmäßig im Inland. Klarstellend sei noch ergänzend hinzugefügt, dass in diesem Verhältnis der Betroffene im Rahmen des Löschungsbegehrens vom Uploader selbstverständlich nicht die Löschung der Daten vom Facebook-Server selbst verlangen kann, sondern nur die Löschung des Bildes, das sich im von Facebook zur Verfügung gestellten Zugangsbereich des Uploaders befindet.

Im Unterschied zu den Ansprüchen gegen Facebook selbst beurteilt sich die Frage der Rechtswidrigkeit im Rahmen des Unterlassungsanspruches (§ 1004 Abs. 1 BGB) bzw. die Frage des Verschuldens im Rahmen des Beseitigungsanspruches (§ 823 Abs. 2 BGB) allerdings nicht unter dem Aspekt der Störerhaftung, sondern nach den allgemeinen Grundsätzen der Deliktshaftung (Haftung für Verschulden bzw. Fahrlässigkeit, s.o. 3.2.2.).

Demzufolge obliegt es dem Betroffenen bzw. Verletzten, gegen welchen Anspruchsgegner er vorgehen will. Die aufgezeigten Ansprüche bleiben dabei grundsätzlich inhaltsgleich.

4. Zuständigkeit deutscher Gerichte und Vorgaben des Europäischen Gerichtshofs[73] - Klagemöglichkeiten des Betroffenen unter Berücksichtigung des Facebook-Sitzes in Irland

Nach der Verordnung über die gerichtliche Zuständigkeit[74] sind Personen, die ihren Wohnsitz im Hoheitsgebiet eines Mitgliedstaats haben, grundsätzlich vor den Gerichten dieses Mitgliedstaats zu verklagen. Bilden jedoch eine unerlaubte Handlung, eine Handlung, die einer unerlaubten Handlung gleichgestellt ist, oder Ansprüche aus einer solchen Handlung den Gegenstand des Verfahrens, so kann eine Person auch in einem anderen Mitgliedstaat vor dem Gericht des Ortes, an dem das schädigende Ereignis eingetreten ist oder einzutreten droht, verklagt werden. So hat ein Betroffener bei **Ehrverletzungen** durch einen in mehreren Mitgliedstaaten verbreiteten Artikel in Printmedien für die Erhebung einer Schadensersatzklage gegen den Herausgeber zwei Möglichkeiten: Zum einen kann er die Gerichte des Staates anrufen, in dem der Herausgeber ansässig ist, wobei diese Gerichte für die Entscheidung über den Ersatz **sämtlicher** durch die Ehrverletzung entstandener Schäden zuständig sind. Zum anderen kann er sich an die Gerichte jedes Mitgliedstaats wenden, in dem die Veröffentlichung verbreitet worden ist und in dem das Ansehen des Betroffenen nach dessen Vorbringen beeinträchtigt worden ist (Ort der Verwirklichung des Schadenserfolgs). In diesem Fall sind die nationalen Gerichte jedoch **nur** für die Entscheidung über den Ersatz der Schäden zuständig, die in dem Staat verursacht worden sind, in dem sie ihren Sitz haben.

Der **Bundesgerichtshof** hat den **EuGH** im Rahmen eines **Vorabentscheidungsverfahrens**[75] um Klärung ersucht, inwieweit diese Grundsätze auf Verletzungen von Persönlichkeitsrechten durch Inhalte auf einer Website übertragbar sind.[76]

---

73 Im Folgenden auch mit EuGH abgekürzt.

74 Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (ABl. 2001, L 12, S. 1).

75 Im Wege eines Vorabentscheidungsersuchens können die Gerichte der Mitgliedstaaten in einem bei ihnen anhängigen Rechtsstreit dem Gerichtshof Fragen nach der Auslegung des Unionsrechts oder nach der Gültigkeit

Das Urteil des EuGH[77]:

In seinem hierauf ergangenen Urteil vom 25. Oktober 2011 stellt der Europäische Gerichtshof fest, dass sich die **Veröffentlichung von Inhalten auf einer Website** von der gebietsabhängigen Verbreitung eines Druckerzeugnisses dadurch unterscheidet, dass die Inhalte von einer unbestimmten Zahl von Internetnutzern überall auf der Welt unmittelbar abgerufen werden können. Somit kann die weltumspannende Verbreitung zum einen die Schwere der Verletzungen von Persönlichkeitsrechten erhöhen, und zum anderen ist es dadurch sehr schwierig, die Orte zu bestimmen, an denen sich der Erfolg des aus diesen Verletzungen entstandenen Schadens verwirklicht hat.[78] Unter diesen Umständen – und da die Auswirkungen eines im Internet veröffentlichten Inhalts auf die Persönlichkeitsrechte einer Person am besten von dem Gericht des Ortes beurteilt werden können, an dem das Opfer den Mittelpunkt seiner Interessen hat – erklärt der Gerichtshof dieses Gericht für zuständig, über den gesamten im Gebiet der Europäischen Union verursachten Schaden zu entscheiden. In diesem Zusammenhang stellt der Gerichtshof klar, dass der Ort, an dem eine Person den **Mittelpunkt ihrer Interessen** hat, im Allgemeinen ihrem gewöhnlichen Aufenthalt entspricht.

Der EuGH hebt jedoch hervor, dass das Opfer anstelle einer Haftungsklage auf Ersatz des gesamten Schadens auch die Gerichte jedes Mitgliedstaats anrufen kann, in dessen Hoheitsgebiet ein im Internet veröffentlichter Inhalt zugänglich ist oder war. In diesem Fall sind die Gerichte wie bei Schäden durch ein Druckerzeugnis nur für die Entscheidung über den Schaden zuständig, der im Hoheitsgebiet des Staates entstanden ist, in dem sie ihren Sitz haben. Ebenso kann die verletzte Person wegen des gesamten entstandenen Schadens auch die Gerichte des Mitgliedstaats anrufen, in dem der Urheber der im Internet veröffentlichten Inhalte niedergelassen ist.

Sofern eine „unerlaubte Handlung“ den Gegenstand des Verfahrens bildet, **ergeben sich für** das **betroffene Opfer**[79] für die zu untersuchende Fragestellung somit **folgende Möglichkeiten**:

---

einer Handlung der Union vorlegen. Der Gerichtshof entscheidet nicht über den nationalen Rechtsstreit. Es ist Sache des nationalen Gerichts, über die Rechtssache im Einklang mit der Entscheidung des Gerichtshofs zu entscheiden. Diese Entscheidung des Gerichtshofs bindet in gleicher Weise andere nationale Gerichte, die mit einem ähnlichen Problem befasst werden.

76 Verfahrensgang und Volltextveröffentlichungen und Veröffentlichungen der Presse abrufbar unter: http://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=EuGH&Datum=25.10.2011&Aktenzeichen=C-509/09 [Stand: 09.02.2012].

77 EuGH, 25.10.2011 - C-509/09; C-161/10. Abrufbar unter: http://lexetius.com/2011,4975 [Stand: 31.01.2012].

78 Speziell zu diesem Problem der Bestimmbarkeit des Erfolgsorts s.a.: BGH Urteil vom 29.03.11 - VI ZR 111/10, abrufbar unter: http://openjur.de/u/165165.html [Stand: 02.01.2012].

79 Unterstellt sei, dass die zu klagen beabsichtigende Person die deutsche Staatsangehörigkeit besitzt oder eine Person mit gewöhnlichen Aufenthalt in Deutschland ist, die europäische Hauptniederlassung von Facebook in

a) Klage vor einem **deutschen Gericht**
(Regulierung des gesamten im EU-Gebiet verursachten Schadens),

b) Klage vor einem **irischen Gericht** (ebenfalls gesamter Schaden),

c) Klage vor einem **Gericht eines jeden europäischen Mitgliedstaates** in dessen Hoheitsgebiet ein im Internet veröffentlichter Inhalt zugänglich ist oder war, ausgenommen Deutschland und Irland
(nur begrenzter Schaden - nämlich derjenige, der im Hoheitsgebiet des jeweiligen EU-Staates entstanden ist).

Schließlich legte der EuGH die **Richtlinie über den elektronischen Geschäftsverkehr**[80] dahin aus, dass es der Grundsatz des freien Dienstleistungsverkehrs grundsätzlich nicht zulässt, dass der Anbieter eines Dienstes des elektronischen Geschäftsverkehrs im Aufnahmemitgliedstaat strengeren Anforderungen unterliegt, als sie das Recht des Mitgliedstaats vorsieht, in dem der Anbieter niedergelassen ist.[81]

Im Ergebnis könnte ein deutscher Facebook-Nutzer als Betroffener ein deutsches Gericht um Rechtsschutz ersuchen, das deutsche Gericht dürfte aufgrund der europäischen Vorgaben jedoch nicht schärfer urteilen als das in Irland ansässige Gericht.

Demnach stellt sich die Frage welchen Beurteilungsmaßstab das irische Recht vorgibt. Jedoch unterliegen die Vorschriften des irischen Landesrechts ebenfalls dem europäischen Vorgaben bzw. der europäischen Datenschutzrichtlinie, so dass dort entsprechend eine Speicherung personenbezogener Daten ohne Einwilligung des Betroffenen grundsätzlich genau wie nach deutschem Recht für unzulässig erklärt wird.[82] Aufgrund der europäischen Vorgabe bleibt demnach ein Mindeststandart an Persönlichkeitsrechten gewahrt, ganz gleich in welchen europäischen Mitgliedsstaat das aufgezeigte Problem verortet wird.

Irland ansässig ist und die Person ungewollt von einer Veröffentlichung ihres Bildes auf Facebook im deutschen, irischen oder dem Internet eines Mitgliedsstaates der EU betroffen wird.

80 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (ABl. L 178, S. 1), abrufbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:DE:PDF [Stand: 09.02.2012].

81 Siehe Fn. 77.

82 Dies ergibt sich aus der Mitgliedschaft Irlands in der Europäischen Union bzw. der Verpflichtung der einzelnen Mitglieder, die europäischen Vorgaben zu beachten.

5. Zusammenfassung

Im Ergebnis lässt sich somit festhalten, dass ein Rückgriff auf irische Rechtsvorschriften für die Beurteilung der Rechtsschutzmöglichkeiten nicht erforderlich ist, da bereits die jeweils einschlägigen nationalen Regelungen des Bürgerlichen Gesetzbuches den Sachverhalt auch ohne einen Rückgriff auf das BDSG oder TMG abschließend zu regeln vermögen.

Auf die Frage der Anwendbarkeit der irischen Rechtsvorschriften kommt es somit inhaltlich nicht entscheidend an, da die einschlägigen Vorschriften des irischen Landesrechts ebenfalls auf der europäischen Datenschutzrichtlinie beruhen und wie das deutsche Recht eine Speicherung personenbezogener Daten ohne die Einwilligung des Betroffenen grundsätzlich für unzulässig erklären[83] (s.o. unter 4. a.E.). Ein europäischer Mindeststandart an Persönlichkeitsrechten wird folglich gewahrt, ganz gleich vor welchem europäischen Gericht der Betroffene seinen Rechtsschutz einklagt.

Dennoch muss es gemeinsames Ziel sein, auf gesamteuropäische Gesetze hinzuarbeiten.[84] Nachdem die Anwendbarkeit der einschlägigen Anspruchsgrundlagen und ein ausreichender Schutz des Betroffenen gegeben ist, hat der EuGH nun auch die Frage nach der Zuständigkeit der Gerichte zufriedenstellend beantwortet, so dass es nunmehr eine Frage der Zeit ist, bis sich die gewünschte Rechtssicherheit[85] und der gewollte Rechtsfrieden einstellen.

Dieses Ergebnis gilt umso mehr im Hinblick auf die geplante **neue EU-Datenschutzverordnung**, die eine Stärkung der Rechtsposition von Internet-Nutzern und den einzelnen nationalen Datenschutzbehörden beabsichtigt. Allerdings wird deren Umsetzung noch einige Zeit in Anspruch nehmen.

---

83 Data Protection Act 1998, Data Protecion Principle 1, Schedule 2 Nr. 1.

84 So auch Lehr, NJW 2012, 705 (710); s.a. Wiele, Warten auf Europa?, Frankfurter Allgemeine Zeitung, 26.10.2011, S. 12.

85 Den Wunsch nach Rechtssicherheit im Umgang mit den Inhaltsdaten bei „Social Communities“ äußerte nicht zuletzt das Unabhängige Landeszentrum für Datenschutz (ULD). Abrufbar unter: http://www.bundestag.de/dokumente/textarchiv/2011/36162329_kw43_pa_neue_medien/index.html [Stand: 19.01.2012].

6. Ausblick – Neue europäische Datenschutzvorgaben[86]

Nach 17 Jahren soll die europäische Datenschutzrichtlinie durch eine Verordnung abgelöst werden. Das bedeutet, dass die Regeln nicht von den Nationalstaaten individuell umgesetzt werden müssen, sondern es eine unmittelbar geltende einheitliche Vorschrift für alle 27 EU-Mitglieder geben wird. Zusätzlich soll es noch eine separate Richtlinie[87] geben, die regelt, wie Verstöße gegen den Datenschutz zu handhaben sind.

Recht auf dauerhafte Datenlöschung

Der neue EU-Datenschutz soll garantieren, dass Nutzer ihre Daten jederzeit dauerhaft bei einem Anbieter löschen können und fordert somit quasi die Einführung eines „digitalen Radiergummis“.[88] Wie der Fall des Wiener Studenten Max Schrems[89] aufgezeigt hat, der von Facebook eine genaue Aufstellung seiner Daten angefordert hat, aufgezeigt hat, halten manche Betreiber Informationen noch weiter vor, selbst wenn die Nutzer ihr Konto schon längst aufgelöst haben. Das will die EU-Kommission nun verhindern. Allerdings wird es auch weiterhin eine Einschränkung geben: Daten sollen aufbewahrt werden können, sofern es "legitimierte Gründe" dafür gibt. Nahezu unmöglich scheint es, das Ziel der dauerhaften Datenlöschung umzusetzen, sollten die Informationen einmal von einem Unternehmen heraus, etwa durch ein Datenleck, ins Internet gelangen. Denn das Internet hat ein ganz großes Defizit: Ihm fehlt der „Löschknopf“. Sind private Daten einmal unterwegs, lassen sie sich kaum noch aufhalten. Jedes Leck, jede Datenpanne – egal ob selbst verschuldet oder von einer Firma verursacht – kann zu einem irreparablen Schaden führen.[90] Das Netz vergisst nichts, wenn man nicht selbst aktiv wird.[91]

---

86 Die Europäische Kommission hat am 25. Januar 2012 den **Entwurf zur Allgemeinen Europäischen Datenschutzverordnung** veröffentlicht. Er geht jetzt im Gesetzgebungsverfahren zum Parlament und Rat; abrufbar unter: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf [Stand: 10.02.2012]. Vgl. auch den diesbezüglichen Bericht von Daniel Breuss am 26.01.2012 auf „DiePresse.com“; abrufbar unter: http://diepresse.com/home/techscience/internet/sicherheit/727035/EUDatenschutz_Das-bringen-die-neuen-Regeln [Stand: 10.02.2012].

87 Bisher handelt es sich nur um Vorschläge von Justizkommissarin Viviane Reding.

88 Lapp, ITRB 2011, 282 (286).

89 Vgl.: http://europe-v-facebook.org/DE/de.html [Stand: 31.01.2012].

90 Kuri, c´t 2010, 112 (113).

91 Bager, c´t 2010, 118 (121).

Ausdrückliches Zustimmungserfordernis

Onlinedienste, wie Facebook und Google müssen in Zukunft erst die ausdrückliche vorherige Zustimmung ihrer Nutzer einholen, wenn sie deren Daten verwenden wollen. Nur nach Einwilligung der Nutzer sollen Datenschutzeinstellungen geändert werden dürfen. Bisher war es oft so, dass Nutzern bei Änderungen am Dienst, insbesondere auf Facebook, neue Einstellungen erst vorgegeben wurden. Danach konnten Nutzer für mehr Schutz Einstellungen ändern (s.o.). Die geplanten Regelungen sollen europäische Bürger vor unangenehmen Überraschungen bewahren.

Gestärkte Informationspflicht

In Zukunft soll es Nutzern in der EU erleichtert werden, ihre gesamten Daten einsehen zu dürfen. Auch soll es leichter werden, Daten von einem Anbieter zu einem anderen übertragen zu können. Die geplanten europäischen Vorgaben beabsichtigen auch im Falle eines Anbieterwechsels, ein Recht auf dauerhafte Löschung der beim alten Anbieter befindlichen Daten zu gewähren. Dies soll ebenfalls den Wettbewerb fördern. Letztlich soll das neue Recht somit mehr Transparenz schaffen. Wie die einzelnen Unternehmen darauf im Einzelnen reagieren werden bleibt abzuwarten. Google[92] hat bereits seine bestehenden Datenschutzbestimmungen vor kurzem überarbeitet und erst kürzlich verlautbart, dass diese am 1. März 2012 in Kraft treten und den Nutzer besser schützen sollen.[93] Ob dies mit den bevorstehenden neuen EU-Vorgaben im Zusammenhang steht, kann nicht mit Sicherheit gesagt werden, doch könnte dies zumindest angenommen werden. Jedenfalls kann vermutet werden, dass andere Unternehmen den „Großen“ wie Google und Facebook folgen und durch eine Veränderung ihrer Datenschutzbestimmungen ebenfalls nachziehen werden.

Eigenständige Datenschutzbehörden in jedem Mitgliedstaat

Die Vorschläge der Justizkommissarin Viviane Reding[94] sehen vor, dass die nationalen Datenschutzbehörden sich um die Anliegen ihrer Bürger kümmern sollen. Das soll auch zutreffen, wenn die Daten in einem anderen Staat verarbeitet werden. Es zählt einzig und allein, dass es sich um Daten von EU-Bürgern handelt. Wenn also ein Österreicher ein Problem mit Google oder

92 Google Incorporated, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

93 Der Umfang der Neuerungen kann den Angaben der Google-Homepage entnommen oder direkt unter dem folgenden Link nachgelesen werden: http://www.google.de/intl/de/policies/privacy/preview/ [Stand: 31.01.2012] .

94 Seit Februar 2010 Vizepräsidentin der Europäischen Kommission, zuständig für Justiz, Grundrechte und Bürgerschaft.

Facebook hat, muss dieses Problem von der österreichischen Datenschutzbehörde aufgegriffen werden. Die Umsetzung dieser Regel dürfte sich als besonders schwierig erweisen.

Stärkung der Kompetenzen der jeweiligen (Datenschutz-)Behörde

Die nationalen Datenschutzbehörden sollen mehr Befugnisse erhalten. Es wird erwogen, dass bei Verstößen direkt Strafen gegen Unternehmen ausgesprochen werden können, die bis zu einer Million Euro oder bis zu zwei Prozent des weltweiten Umsatzes eines Unternehmens betragen könnten. Beginnen soll der Strafrahmen bei 250.000 Euro oder 0,5 Prozent[95] des Umsatzes. Als Beispiel für einen "weniger schweren Verstoß" wird genannt, dass ein Unternehmen eine Gebühr dafür verlangt, dass ein Kunde seine Daten einsehen möchte. Bei kriminellen Vergehen soll die neue Richtlinie mehr Zusammenarbeit zwischen Polizei und Gerichtsbarkeit ermöglichen. Auch soll der Datenaustausch zwischen den Behörden der Mitgliedstaaten aufgrund von harmonisierten Regelungen einfacher und sicherer werden.

Informationspflicht der Unternehmen

Im Hinblick auf die Vorgabe, Daten sicher zu verwahren, sollen Unternehmen künftig einer Meldepflicht unterliegen, falls Daten ihrer Kunden in unberechtigte Hände geraten sind. In diesem Fall sollen Unternehmen verpflichtet werden, innerhalb von 24 Stunden die jeweilige nationale Datenschutzbehörde über ein aufgetretenes Datenleck zu informieren. So sollen insbesondere Unternehmen, die eine Vielzahl an Kundendaten verwahren, generell stärker in die Pflicht genommen werden.

Dauer der praktischen Umsetzung

Bisher liegen nur die beiden Vorschläge für eine einheitliche EU-Datenschutzverordnung und die sie begleitende Richtlinie vor. Diese werden jetzt dem Europäischen Parlament und dem Rat der Europäischen Union zur Diskussion weitergeleitet. Sollten diese die Vorschläge annehmen, wird die Verordnung zwei Jahre nach der Zustimmung gültig und damit für jeden EU-Mitgliedsstaat unmittelbar rechtsverbindlich. Bezüglich der Richtlinie hätten die Staaten zwei Jahre Zeit, um diese in nationales Recht umzusetzen.

95 Vgl. Bericht auf „heise online“, abrufbar unter: http://www.heise.de/newsticker/meldung/Bericht-EU-will-Unternehmen-fuer-Datenlecks-bestrafen-1390501.html [Stand: 06.02.2012].

Erkenntnisprozess – Eine Frage der Zeit

Insgesamt ist zu erwarten, dass die Überarbeitung der Datenschutzrichtlinie zu einer besseren Harmonisierung von Recht und Aufsicht in Europa führen wird. An Hand der Vielzahl von Problemen, die durch die neuen europäischen Vorgaben gelöst werden sollen wird deutlich, dass Datenschutz im Internet kein nationales oder europäisches, sondern ein weltumfassendes Thema ist.[96]

96 Gröschel, AnwBl 4/2011, 276 (277).

7. Literatur

Bager, Jo. Privat eingestellt, c´t 2010, Heft 14, 118 ff.

Bull, Hans Peter. Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen, NVwZ 2011, 257 ff.

Gola, Peter; Schomerus, Rudolf. Bundesdatenschutzgesetz Kommentar, 9. Auflage, München 2007.

Gounalakis, Georgios; Rhode, Lars. Persönlichkeitsschutz im Internet, München 2002.

Gröschel Philippe. Bedrohen soziale Netzwerke den Datenschutz?, AnwBl 4/2011, 276 f.

Heckmann, Dirk. Smart Life – Smart Privacy Management: Privatsphäre im total digitalisierten Alltag, K&R 2011, 1 ff.

Hoeren, Thomas; Sieber, Ulrich. Handbuch Multimedia-Recht, 27. Ergänzungslieferung, München 2011.

Hoeren, Thomas. Facebook und Co. – Risiken für Unternehmen und Privatnutzer, Deutscher AnwaltSpiegel 15.06.2011, Ausgabe 12, 9 f.

Hoffmann, Bernd von; Thorn, Karsten; Firsching, Karl. Internationales Privatrecht, 8. Auflage, München 2002.

Jotzo, Florian. Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co bei grenzüberschreitendem Datenverkehr?, MMR 2009, 232 ff.

Kemper, Frank. Wo bleibt der Netz-Minister?, Internet World Business, 19.12.2011, 34.

Kuri, Jürgen. Macht und Ohnmacht, c´t 2010, Heft 14, 113 f.

Lapp, Thomas. Soziale Medien im Spiegel des Rechts, ITRB 2011, 232 ff.

Lehr, Matthias. Internationale medienrechtliche Konflikte und Verfahren, NJW 2012, 705 ff.

Leutheusser-Schnarrenberger. Den Datenschutz rundum erneuern, Hamburger Abendblatt, 06.12.2010, 2.

Moritz, Hans Werner. Unterlassungsanspruch gegen Betreiber eines Internetforums wegen Veröffentlichung personenbezogener Daten, JurisPR-ITR 24/2011 Anm. 5, Anmerkung zu: OLG Hamburg 7. Zivilsenat, Urteil vom 02.08.2011 – 7 U 134/10.

Neukamm, Katrin. Bildnisschutz in Europa, Dissertation, Berlin 2007.

Ohrmann, Christoph. Der Schutz der Persönlichkeit in Online-Medien, Düsseldorf 2009.

Palandt, Otto. Bürgerliches Gesetzbuch, Kurzkommentar, 70. Auflage, München 2011.

Roth, Isabel. Die internationale Zuständigkeit deutscher Gerichte bei Persönlichkeitsrechtsverletzungen im Internet, Frankfurt 2007.

Seemann, Michael. Archäologie der Zukunft, c´t 2010, Heft 14, 114 f.

Simitis, Spiros. Bundesdatenschutzgesetz Kommentar, 6. Auflage, Baden-Baden 2006.

Wanckel, Endress. Foto- und Bildrecht, München 2009.

Wiele, Jan. Warten auf Europa?, Frankfurter Allgemeine Zeitung, 26.10.2011, 12.