Dennis-Kenji Kipker, Friederike Voskamp

Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung

Die Nutzung sozialer Netzwerke wirft aus datenschutzrechtlicher Perspektive zahlreiche Probleme auf. Der europäische Entwurf einer Datenschutz-Grundverordnung versucht, sich dieser durch verschiedene, teils auch neue Regelungsinstrumente anzunehmen. Der folgende Beitrag stellt einige der Ansätze des Entwurfes für die Nutzung sozialer Netzwerke in einem Vergleich zu den Vorgaben der Richtlinie 95/46/EG dar und orientiert sich dabei an den einzelnen Stationen der Netzwerkbenutzung in Form von Registrierung, Nutzung und Abmeldung.

1 Die Registrierung im sozialen Netzwerk

Die Nutzung eines sozialen Netzwerkes beginnt stets mit der Registrierung. Im Wesentlichen erfolgt der Registrierungsvorgang bei den meisten Anbietern ähnlich; so wird neben der Angabe personenbezogener Daten, wie etwa Name, Geburtsdatum und Email-Adresse, eine Erklärung des Nutzers verlangt, wonach dieser mit den Allgemeinen Geschäfts- bzw. Nutzungsbedingungen sowie den Datenschutzrichtlinien bzw. der Datenschutz-Erklärung einverstanden ist. Aus datenschutzrechtlicher Perspektive stellen die zu erteilenden „Einverständniserklärungen" Einwilligungserklärungen im Sinne der Art. 7 lit. a, Art. 2 lit. h der Richtlinie 95/46/EG (EG-Datenschutzrichtlinie, im Folgenden EG-DSRl) dar. Für jede Datenverarbeitung gilt das Verbotsprinzip mit Erlaubnisvorbehalt nach Art. 7 EG-DSRl, welches die grundsätzliche Unzulässigkeit einer Datenerhebung und -verarbeitung statuiert, es sei denn, eine Rechtsvorschrift erlaubt diese ausdrücklich oder der Betroffene hat eingewilligt.

Dennis-Kenji Kipker

Wissenschaftlicher Mitarbeiter und Doktorand am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen

E-Mail: kipker@uni-bremen.de

Friederike Voskamp

Wissenschaftliche Mitarbeiterin und Doktorandin am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen

E-Mail: voskamp@uni-bremen.de

1.1 Gemeinsame Voraussetzungen wirksamer Einwilligung

Im Rahmen einer Einwilligungserteilung ist vom Netzwerkbetreiber zu beachten, dass diese den Voraussetzungen des Art. 2 lit. h EG-DSRl genügt: So muss die Einwilligung freiwillig erteilt werden, der Einwilligende muss bei Erteilung in ausreichender Form informiert sowie die Erklärung hinreichend bestimmt sein. Der Entwurf der Verordnung[1] (im Folgenden als DS-GVO-E bezeichnet) regelt die Zulässigkeit der Datenverarbeitung in Art. 6, wobei die Erteilung einer datenschutzrechtlichen Einwilligung als eine Erlaubnistatbestandsalternative in Art. 6 Abs. 1 lit. a DS-GVO-E benannt wird. Hiernach ist, ebenso wie in der EG-DSRl, ausgehend vom Verbotsprinzip mit Erlaubnisvorbehalt, die Datenverarbeitung nur dann rechtmäßig, wenn die betroffene Person „ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere genau festgelegte Zwecke gegeben" hat.

Unter welchen Voraussetzungen diese Einwilligung wirksam ist, regeln Art. 4 Nr. 8 und Art. 7 DS-GVO-E. Wesentliches entspricht hier den bereits genannten Vorgaben des Art. 2 lit. h sowie Art. 7 lit. a EG-DSRl. So setzt auch der Verordnungsentwurf voraus, dass die Einwilligung freiwillig, d.h. ohne jeden Zwang und für den konkreten Fall, d.h. hinreichend bestimmt, erklärt wird. Der Grundsatz der Informiertheit der Einwilligung findet sich ebenfalls in Art. 4 Nr. 8 DS-GVO-E wieder, wenn bestimmt wird, dass die Einwilligungserteilung „in Kenntnis der Sachlage" zu erfolgen hat. Art. 7 Abs. 2 DS-GVO-E enthält zudem ein Hervorhebungsgebot: Falls die Einwilligung durch eine Erklärung erfolgen soll, „die noch einen anderen Sachverhalt betrifft, muss das Erfordernis der Einwilligung äußerlich erkennbar von

1 Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM (2012) 11 endg.

dem anderen Sachverhalt getrennt werden". Während die EG-DSRl kein ausdrückliches Hervorhebungsgebot vorsieht, eröffnet sie aber einen Umsetzungsspielraum für die Mitgliedstaaten, der die Einführung eines solchen Gebots, wie etwa durch § 4a Abs. 1 S. 4 BDSG geschehen, durch die Mitgliedstaaten auf nationaler Ebene ermöglicht.

1.2 Schriftformerfordernis

Die EG-DSRl sieht kein explizites Schriftformerfordernis für die Einwilligungserteilung vor. Bei der Umsetzung in nationales Recht verbleibt den Mitgliedstaaten aber ein Gestaltungsspielraum. Der deutsche Gesetzgeber hat in diesem Rahmen ein grundsätzliches Schriftformerfordernis für die Einwilligungserteilung vorgesehen, welches in § 4a Abs. 1 S. 3 BDSG normiert ist. Der Entwurf der Datenschutzgrundverordnung sieht ebenso wie die EG-DSRl für die wirksame Einwilligungserteilung kein zwingendes Schriftformerfordernis vor, jedoch gibt es in diesem Falle für die Mitgliedstaaten keinen Umsetzungsspielraum, vielmehr entfaltet die Verordnung unmittelbare Rechtswirkung, ohne dass es eines weiteren Umsetzungsaktes der einzelnen Staaten bedarf.

Für die Einwilligungserteilung im Rahmen der Registrierung bei Netzwerkportalen ist diese Neuerung in der Praxis aber unbeachtlich: Bereits jetzt sieht § 13 Abs. 2 TMG für die Verwendung von Bestands- und Nutzungsdaten im Sinne der § 14 f. TMG die Möglichkeit einer elektronischen Einwilligungserklärung vor. Nichts anderes gilt im Ergebnis für die Verwendung von Inhaltsdaten, also solchen Daten, die bei der Benutzung des Netzwerkes zwischen den jeweiligen Nutzern anfallen wie beispielsweise Online-Gästebucheinträge („Pinnwand"); entweder gelten auch für diese Daten die Vorgaben des TMG entsprechend[2] oder aber gem. § 4a Abs. 1 S. 3 2. Hs. BDSG kann aufgrund „besonderer Umstände" vom Schriftformerfordernis abgewichen werden.[3]

Insbesondere für die Einwilligungserteilung mittels anklickbaren Kontrollkästchens ist positiv hervorzuheben, dass der DS-GVO-E nunmehr vorsieht, dass die Zustimmung des Nutzers nur mittels opt-in erklärt werden kann, da Art. 4 Nr. 8 des Entwurfes verlangt, dass die Einwilligung als „explizite Willensbekundung" erfolgt.[4] Bislang war in diesem Bereich die Einwilligungserteilung noch mittels des opt-out-Verfahrens zulässig.[5] Durch die opt-in-Einwilligung wird dem Nutzer vor Abschluss des Registrierungsvorganges nochmals deutlich vor Augen geführt, dass er eine Erklärung abgibt, welche das Netzwerkunternehmen zur Verarbeitung seiner personenbezogenen Daten legitimiert.

1.3 Freiwilligkeitsvorgabe

Sowohl nach der EG-DSRl als auch nach dem DS-GVO-E ist für eine wirksame Einwilligungserklärung erforderlich, dass diese freiwillig erfolgt. Diese Freiwilligkeitsvorgabe konkretisiert sich bislang u.a. im Koppelungsverbot, nach dem DS-GVO-E des Weiteren in einer Ungleichgewichtsregelung.

So stellt das datenschutzrechtliche Koppelungsverbot eine spezielle Ausprägung der Freiwilligkeit einer Einwilligung dar. Nach dem Koppelungsverbot darf der Abschluss eines Vertrages nicht von einer Einwilligungserteilung abhängig gemacht werden, wenn für den Betroffenen ohne diese Einwilligungserklärung kein anderer Zugang zu gleichwertigen vertraglichen Leistungen möglich ist. Ein Eingreifen des Koppelungsverbots kann bei sozialen Netzwerken unter dem Gesichtspunkt in Erwägung gezogen werden, dass diese regelmäßig anzeigenfinanziert sind und eine Aufnahme des Nutzungsverhältnisses deshalb meist unter der Bedingung der Einwilligung in die Verwendung der Daten zu Werbezwecken steht. Gleichzeitig verlangen nahezu alle vergleichbaren Netzwerkangebote zur Ermöglichung zielgruppengerichteter Werbeeinblendungen und -nachrichten ebenfalls umfassende Einwilligungserklärungen seitens der Nutzer.

Das Koppelungsverbot hat durch den deutschen Gesetzgeber in § 28 Abs. 3b BDSG Eingang in das nationale Recht gefunden. Auch wenn die EG-DSRl selbst kein ausdrückliches Koppelungsverbot vorsieht, ermöglicht sie aufgrund des Handlungsspielraums der Mitgliedstaaten die Einführung des Koppelungsverbots auf nationaler Ebene. Der DS-GVO-E enthält ebenfalls kein ausdrückliches Koppelungsverbot. Aufgrund seines Verordnungscharakters bleibt aber unter dem DS-GVO-E kein Spielraum mehr für eine Normierung des Koppelungsverbots auf nationaler Ebene. Im Ergebnis ist dies jedoch unerheblich, da das Koppelungsverbot trotz fehlender ausdrücklicher Normierung als Bestandteil des allgemeinen Freiwilligkeitsgebotes im Rahmen der Auslegung in Art. 4 Nr. 8 DS-GVO-E hineingelesen werden kann. Auf diese Weise kann dessen Schutzfunktion auch ohne explizite Erwähnung im Gesetzeswortlaut eingreifen.

Eine Neuerung stellt die Ungleichgewichtsregelung des Art. 7 Abs. 4 DS-GVO-E dar. Hiernach kann die Einwilligung keine wirksame Rechtsgrundlage für eine Datenverarbeitung darstellen, wenn sie durch eine Zwangslage herbeigeführt wurde, die in einem erheblichen Ungleichgewicht zwischen der Position der betroffenen Person und derjenigen des für die Verarbeitung Verantwortlichen besteht. Als Beispiele für solch ein erhebliches Ungleichgewicht nennt der Entwurf im Erwägungsgrund 34 für den nicht-öffentlichen Bereich das Verhältnis zwischen Arbeitgeber und Arbeitnehmer. Im öffentlichen Bereich sollen Fälle des „klaren" Ungleichgewichts dann gegeben sein, wenn die Behörde aufgrund ihrer obrigkeitlichen Befugnisse dem Betroffenen eine Verpflichtung auferlegen kann, mithin ein subordinationsrechtliches Verhältnis besteht. Beiden Beispielen ist folglich das unmittelbare Angewiesensein auf die Entscheidungen der verantwortlichen Stelle gemeinsam.

Sicherlich wird man, ausgehend von der Formulierung des Erwägungsgrundes 34 („vor allem"), die Fälle des erheblichen Ungleichgewichts nicht allein hierauf beschränken können. Dennoch wird davon auszugehen sein, dass die Ausnahmevorschrift des Art. 7 Abs. 4 DS-GVO-E nur auf im Ergebnis von der Zwangslage gleichermaßen schwerwiegende Konstellationen anwendbar sein soll. Entsprechend wird man ein erhebliches Ungleichgewicht im Sinne des Art. 7 Abs. 4 DS-GVO-E nur dann annehmen können, wenn der Betroffene von der verantwortlichen Stelle derart abhängig ist, dass er sich als vernünftig denkender Mensch Sorgen über mögliche Konsequenzen machen müsste, sollte er der Aufforderung, seine Einwilligung in die Datenverarbeitung zu erteilen, nicht nachkommen. Bezüglich der Nutzer eines sozialen Netzwerkes und der Seitenbetreiber wird von einem solch

2 In diesem Sinne Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht (5. Aufl.), S.396

3 In diesem Sinne Taeger in: Taeger/Gabel (Hg.), BDSG, § 4a Rn. 37.

4 So auch Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht (5. Aufl.), S. 358.

5 So (allerdings für einen Offline-Sachverhalt) die Payback-Entscheidung des BGH, DuD 2008, 818- 824.

erheblichen Ungleichgewicht im Regelfall wohl nicht auszugehen sein. Zwar wird man argumentieren können, dass sich das Betreiberunternehmen und der Nutzer nicht auf einer Ebene der Gleichordnung befinden, wenn durch Allgemeine Geschäftsbedingungen Einwilligungen vorgegeben werden, ohne die der Zutritt zum sozialen Netzwerk versagt bleibt. Ein erhebliches Ungleichgewicht dürfte hingegen abzulehnen sein, denn die Vorteile der Nutzung eines sozialen Netzwerkes sind für den Normalverbraucher zumeist verzichtbar, da weder ein persönliches noch ein wirtschaftliches Abhängigkeitsverhältnis zum Seitenbetreiber besteht.[6]

Die Ungleichgewichtsregelung stellt von seinem Grundgedanken her somit zwar einen guten, wenn nicht sogar dem Koppelungsverbot überlegenen Ansatz zur Absicherung der Freiwilligkeit der Einwilligung dar, seine Anwendbarkeit auf soziale Netzwerke erscheint aber aufgrund seiner derzeitig engen Fassung fraglich.

1.4 Minderjährige Nutzer

Soziale Netzwerke werden gerade auch von Kindern und Jugendlichen genutzt. Für die Einwilligungserteilung bei der Registrierung solch minderjähriger Nutzer gelten besondere Anforderungen, um deren erhöhter Schutzbedürftigkeit gerecht zu werden. Die Einwilligungserteilung durch Kinder und Jugendliche ist dann möglich, wenn sie die entsprechende Einsichtsfähigkeit zur Abgabe einer solchen Erklärung besitzen.[7] Bei Kindern mit einem Alter von unter 12 Jahren dürfte die Einsichtsfähigkeit im Regelfall abzulehnen sein. Erst ab einem Alter von 13 Jahren bedarf die Beurteilung der Einsichtsfähigkeit näherer Untersuchung.[8] Gerade für soziale Netzwerke gilt dabei, dass an die Einsichtsfähigkeit besondere Anforderungen gestellt werden müssen: Die Seitenbetreiber animieren zur Angabe möglichst vieler, auch sensibler personenbezogener Daten, die, soweit keine besonderen Einstellungen vorgenommen werden, einem großen Kreis von Nutzern zugänglich, darüber hinaus teils sogar durch Suchmaschinen im Internet für jedermann einsehbar sind. Man wird im Generellen auch nicht davon ausgehen können, dass Jugendliche sich detailliert mit den umfänglichen und teils unübersichtlichen Privatsphäreeinstellungen des Netzwerkbetreibers auseinandersetzen.

Aufgrund dieser datenschutzrechtlichen Komplexität sozialer Netzwerke erscheint es fraglich, ob die Anknüpfung an ein doch recht diffuses und im Einzelfall schwer nachprüfbares Kriterium der Einsichtsfähigkeit dem Minderjährigendatenschutz gerecht wird. Der DS-GVO-E verfolgt hier einen Ansatz, welcher sich teils an starren Altersgrenzen orientiert. So ist der Begriff des Kindes in Art. 4 Nr. 18 DS-GVO-E legaldefiniert: „Kind" ist jede Person bis zur Vollendung des 18. Lebensjahres; die besondere Schutzbedürftigkeit von Minderjährigen wird damit unabhängig von ihrem Alter für alle Jugendlichen anerkannt. Art. 8 Abs. 1 DS-GVO-E enthält weitergehend spezielle Bestimmungen betreffend die Einwilligungserteilung: Falls einem Kind bis zur Vollendung des 13. Lebensjahres unmittelbar Dienste der Informationsgesellschaft angeboten werden, worunter auch das Bereithalten sozialer Netzwerke im Internet fällt, ist die Einwilligung nur dann rechtmäßig, wenn sie durch die Eltern, den Vormund oder mit deren Zustimmung erteilt wird. Hierdurch wird den in Erwägungsgrund 25 des Verordnungsentwurfes dargestellten Überlegungen Rechnung getragen, dass Kinder sich der Risiken, Folgen und Vorsichtsmaßnahmen bei der Verarbeitung ihrer personenbezogenen Daten weniger bewusst sein dürften.

Zwar erscheint diese Einordnung in starre Altersgrenzen bis zum vollendeten 13. Lebensjahr zumindest gegenüber der fließenden Beurteilung der Einsichtsfähigkeit nach bisherigem Recht begrüßenswert, dennoch ist fraglich, ob sich hierdurch in der Praxis tatsächlich Vorteile für den Minderjährigenschutz ergeben werden: Zunächst wird bereits nach derzeitiger Rechtslage, wenn auch nicht ausdrücklich gesetzlich festgeschrieben, die Einwilligungsfähigkeit Minderjähriger bis zum vollendeten 13. Lebensjahr grundsätzlich verneint. Die Bestrebung, bei Minderjährigen, denen die Einsichtsfähigkeit fehlt, die Einwilligung durch diejenige der Eltern zu ersetzen, wird ferner vor Probleme in der praktischen Umsetzbarkeit gestellt, da sich in vielen Fällen nach wie vor

6 Offener Buchner, Die Einwilligung im Datenschutzrecht, DuD 2010, 39, 41.

7 Siehe für die Einwilligungserteilung Minderjähriger bei der Benutzung von Online-Spielen Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht (5. Aufl.), S. 401 ff.

8 Vgl. zur entsprechenden Auslegung des BDSG Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht (5. Aufl.), S. 402.

Innovativer Datenschutz

Herausgegeben von

Falk Peters
Heinrich Kersten
Klaus-Dieter Wolfenstetter

Falk Peters / Heinrich Kersten / Klaus-Dieter Wolfenstetter (Hrsg.)

Zahlr. Abb.; 335 S. 2012
<978-3-428-13860-9> € 38,–
Auch als E-Book erhältlich

Die Geschichte des Datenschutzes zeigt: Für den Schutz personenbezogener Daten sind Gesetze zwar ein sehr wichtiger, aber immer nur der erste Schritt. Denn letztlich entscheidet die Umsetzung der Datenschutznormen darüber, ob die alltägliche Praxis den gesetzgeberischen Zielvorstellungen entspricht. Dabei gefährdet die immer weiter fortschreitende automatisierte Verarbeitung in IT-Systemen personenbezogene Daten in besonderer Weise und verlangt signifikante Schutzmaßnahmen. Der effektivste Schutz sind hier technische und organisatorische Maßnahmen, welche zu einem systemimmanenten Schutz personenbezogener Daten führen. Das Idealziel muss sein, eine rechtlich verbotene Datenverarbeitung unmöglich zu machen und im Rahmen eines IT-Systems nur eine solche Datenerfassung und -verarbeitung zuzulassen, die den Rechtsnormen entspricht.

Aus dem Vorwort
von *Wolfgang Bosbach* MdB

www.duncker-humblot.de

nicht nachweisen lassen wird, von wem die Einwilligung originär stammt. Was im Rahmen einer solchen Nachforschung des Verantwortlichen unter den Begriff der „angemessenen Anstrengung" im Sinne des Art. 8 Abs. 1 S. 2 DS-GVO-E fällt, bleibt auslegungsbedürftig; jedenfalls ergibt sich aus dieser Vorschrift keine effektive Kontrollverpflichtung bezüglich der Einwilligungserklärung für den Netzwerkbetreiber.

Die derzeitige Fassung des DS-GVO-E trifft darüber hinaus keine genauen Regelungen über die Einwilligungsfähigkeit Minderjähriger im Alter von 13 bis 17 Jahren. Ausgehend von Erwägungsgrund 129 des Verordnungsentwurfes soll der Kommission die Befugnis übertragen werden, delegierte Rechtsakte im Sinne des Art. 290 AEUV zur Festlegung der Kriterien und Bedingungen für die Einwilligung eines Kindes zu erlassen. Außerhalb der Erwägungsgründe findet sich hierzu jedoch keine explizite Befugnisübertragung für die Kommission im Sinne des Art. 290 Abs. 1 AEUV. Zudem stellt sich die Frage, ob für die Einwilligungsfähigkeit Minderjähriger überhaupt eine Delegationsfähigkeit gegeben sein kann, da von der Delegationsbefugnis gem. Art. 290 AEUV nur solche Rechtsakte erfasst sind, die „nicht wesentliche" Vorschriften eines EU-Gesetzgebungsaktes betreffen. Ob diese Unwesentlichkeit ohne Weiteres auch für die Ausübung der informationellen Selbstbestimmung Minderjähriger gelten kann, die gerade im Rahmen der Nutzung sozialer Netzwerke als besonders schützenswert einzustufen sind, kann angezweifelt werden.[9]

2 Die Nutzung des sozialen Netzwerkes

Erscheint dem Nutzer eines sozialen Netzwerkes im Laufe der Zeit ein anderes Netzwerk als attraktiver, kann sich ein Wechsel des Services beziehungsweise die Anlegung eines weiteren Accounts bei dem alternativen Netzwerk aufgrund der Datenmengen, die der Nutzer bereits auf den Server seines sozialen Netzwerkes hochgeladen hat, als schwierig erweisen. Oftmals wird der Nutzer auf seine bereits angesammelten Fotos, Videos, Beiträge oder Kontaktdaten nicht verzichten wollen, die manuelle Übertragung der Daten auf das alternative Netzwerk aber als impraktikabel empfinden,[10] so dass er unter Umständen auf einen Wechsel oder ein weiteres Nutzerkonto verzichtet.

2.1 Recht auf Datenportabilität

Gerade auch im Hinblick auf soziale Netzwerke, auf die in Erwägungsgrund 55 des DS-GVO-E ausdrücklich hingewiesen wird, sieht der Grundverordnungsentwurf nunmehr das Recht auf Datenportabilität gem. Art. 18 vor, welches sich in der EG-DSRl nicht findet. Die Regelung des Art. 18 DS-GVO-E ist weniger auf den Datenschutz im engeren Sinne als vielmehr auf den Schutz der Verbraucherrechte ausgerichtet.[11] Es soll den Wettbewerb stärken, indem es dem Betroffenen bei einer Datenverarbeitung in strukturierten gängigen elektronischen Formaten das Recht an die Hand gibt, eine Kopie seiner verarbeiteten Daten in einem von ihm weiter verwendbaren strukturierten gängigen elektronischen Format zu verlangen (Abs. 1). Gem. Abs. 2 muss es dem Betroffenen zudem möglich sein, seine personenbezogenen Daten an einen anderen Verarbeiter zu überführen, ohne dabei vom ursprünglichen Datenverarbeiter, dem die personenbezogenen Daten entzogen werden, behindert zu werden. Dem Betroffenen wird damit die Möglichkeit eröffnet, sich ohne größeren Aufwand auch nach erfolgter Wahl eines bestimmten sozialen Netzwerkes für ein anderes, ihm unter Umständen als besser geeignet Erscheinendes zu entscheiden und bei einem Wechsel seine Daten zu exportieren und möglichst problemlos auf dieses Netzwerk zu übertragen.

In Hinblick auf die mit Art. 18 Abs. 2 DS-GVO-E verfolgten Ziele ist zudem davon auszugehen, dass das Recht auf Datenportabilität auch eingreifen soll, wenn der Nutzer das ursprüngliche Netzwerk nicht endgültig verlassen, sondern vielmehr lediglich ein weiteres Nutzerkonto bei einem alternativen Netzwerkanbieter anlegen und seine Daten auch auf dieses übertragen möchte. Der Wortlaut des Art. 18 Abs. 2 DS-GVO-E ist diesbezüglich jedoch missverständlich, da von einem „Entziehen" der Daten bei dem ursprünglichen Datenverarbeiter die Rede ist. Hier bedarf es der Konkretisierung des Normtextes, unter Umständen sollte auf den Begriff des Entziehens vollständig verzichtet werden.[12]

2.2 Technische Umsetzung

Nach Art. 18 Abs. 1 und 2 DS-GVO-E sind die Daten vom Seitenbetreiber in einem gängigen elektronischen Format zur Verfügung zu stellen, so dass ein Einlesen etwa in einem anderen sozialen Netzwerk grundsätzlich ermöglicht wird. Dabei ist jedoch zu beachten, dass die meisten großen sozialen Netzwerke bereits jetzt die Möglichkeit des Exports der Nutzerdaten anbieten[13], wobei jedoch zum Teil elektronische Formate verwendet werden, die zwar als gängig zu werten, jedoch nicht zur Übertragung der Daten auf ein anderes Netzwerk geeignet sind.[14] Da sich zudem anders als etwa im Bereich der Email-Diensteanbieter bezüglich sozialer Netzwerke bisher noch kein einheitliches elektronisches Format durchgesetzt hat, erfordert das Recht auf Datenportabilität zu seiner wirksamen Umsetzung einer Präzisierung bezüglich des erforderlichen Formats sowie technische Neuerungen. Nach Art. 18 Abs. 3 DS-GVO-E kann die europäische Kommission die näheren Modalitäten zur Ausgestaltung des Rechts auf Datenportabilität wie die technischen Standards, Modalitäten und Verfahren für die Überführung der personenbezogenen Daten nach Art. 18 Abs. 2 DS-GVO-E festlegen.

Anhand der technischen Präzisierung durch die Kommission wird sich die Realisierbarkeit des Rechts auf Datenportabilität zeigen. Es ist zudem abzuwarten, inwieweit es, gemessen an den Hürden der Umstellung von einem zum anderen sozialen Netzwerk, einen tatsächlichen Bedarf für ein solches Recht gibt. Denn ein vollständiger automatischer Umzug eines Nutzerkontos mit allen Daten in ein anderes soziales Netzwerk wird in der Regel

9 So auch Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht (5. Aufl.), S. 402.

10 So auch Hornung, Eine Datenschutz-Grundverordnung für Europa?, ZD 2012, 99, 103; Wybitul/Fladung, EU-Datenschutz-Grundverordnung – Überblick und arbeitsrechtliche Betrachtung des Entwurfs, BB 2012, 509, 512.

11 Härting, Starke Behörden, schwaches Recht – der neue EU-Datenschutzentwurf, BB 2012, 459, 465.

12 Vgl auch LDA, Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder v. 11. Juli 2012 zur Datenschutz-Grundverordnung, S. 12, abrufbar unter: http://www.datenschutz.hessen.de/download.php?download_ID=252 (Stand: 21.06.2012)

13 Vgl. etwa zur Möglichkeit des Datenexports aus dem sozialen Netzwerk Google Plus: http://www.dataliberation.org/ (Stand: 05.06.2012).

14 Facebook bietet etwa auf der Seite „Kontoeinstellungen" dem Nutzer die Möglichkeit, eine Kopie seiner Daten herunterzuladen, wobei er eine HTML-Datei erhält, die sich kaum zur Übertragung auf ein anderes Netzwerk eignet.

auch unter der Geltung eines Rechts auf Datenportabilität und bei Verwendung eines zur Übertragung geeigneten elektronischen Formats nicht möglich sein, da die Services der verschiedenen Netzwerke meist sehr unterschiedlich aufgebaut sind.[15]

3 Die Abmeldung aus dem sozialen Netzwerk

Kündigt der Betroffene den Nutzungsvertrag mit dem Betreiber des sozialen Netzwerkes und schließt er sein Konto endgültig, so stellt sich oftmals die Frage, wie die Spuren seiner Netzwerktätigkeit wieder gelöscht werden können. Nicht selten wollen Internetnutzer sich von ihren früheren Aktivitäten und Beiträgen im Nachhinein distanzieren, Spuren der Tätigkeit im Netzwerk sollen nach der Abmeldung nicht mehr im Internet auffindbar sein. Dies gilt insbesondere für jüngere Nutzer, die dem Bedürfnis folgen, sich online Altersgenossen gegenüber möglichst umfassend zu präsentieren. Die Besonderheit und Problematik sozialer Netzwerke liegt dabei darin, dass persönliche Informationen schnell und unter Umständen unüberlegt einem großen Kreis von Personen gegenüber veröffentlicht werden können, so dass sich anders als bei herkömmlichen Kommunikationsformen das Problem der Rückgängigmachung der informationellen Spuren in besonderem Maße stellt.

3.1 Recht auf Löschung

Art. 12 lit. b EG-DSRl sieht hierfür eine Pflicht zur Löschung der personenbezogenen Daten vor, wenn die Datenverarbeitung nicht den Bestimmungen der Richtlinie entspricht. Eine Löschungspflicht besteht danach unter anderem bei Unzulässigkeit der Speicherung nach Art. 7 EG-DSRl. Eine solche unzulässige Speicherung ist bezüglich Daten, die im Rahmen der Nutzung eines sozialen Netzwerkes angefallen sind, bei einer Vertragskündigung und einem dabei zumindest konkludent erklärten Widerruf der Einwilligungserklärung anzunehmen, so dass den Seitenbetreiber in diesem Fall eine Löschungspflicht trifft.

Auch nach dem DS-GVO-E ist ein Recht auf Löschung vorgesehen: Art. 17 Abs. 1 DS-GVO-E gibt dem Betroffenen das Recht, von dem für die Verarbeitung Verantwortlichen die Löschung seiner Daten sowie das Unterlassen ihrer weiteren Verbreitung zu verlangen, soweit einer der in Art. 17 Abs. 1 genannten Fälle einschlägig ist. Unter anderem besteht nach Art. 17 Abs. 1 lit. b DS-GVO-E ein Recht auf Löschung bei Widerruf der Einwilligungserteilung nach Art. 7 Abs. 3 DS-GVO-E. Das Recht auf Widerruf steht dem Betroffenen nach Art. 7 Abs. 3 DS-GVO-E nunmehr ausdrücklich jederzeit zu, so dass die Pflicht zur Löschung seiner Daten ebenfalls jederzeit durch den Betroffenen herbeigeführt werden kann.

Da auch nach der EG-DSRl bei einer Vertragsbeendigung und einem dabei zumindest konkludent erklärten Widerruf der Einwilligung eine Pflicht zur Löschung besteht, ist bezüglich sozialer Netzwerke keine wesentliche Verbesserung der Position des Nutzers durch das Recht auf Löschung nach Art. 17 Abs. 1 DS-GVO-E gegeben.

Die Rechtslage für den Betroffenen verschlechtert sich vielmehr insofern, als er zwar nach Art. 14 Abs. 1 lit. d vom Verantwortlichen auf das Bestehen des Rechts auf Löschung hingewiesen werden muss, nach Art. 17 Abs. 1 DS-GVO-E die Löschung dann aber explizit verlangen muss. Nach der EG-DSRl wird den Mitgliedsstaaten durch Art. 12 lit. b dagegen die Möglichkeit eingeräumt, die Löschungsverpflichtung qua Gesetz eintreten zu lassen, wovon etwa der deutsche Gesetzgeber mit § 35 Abs. 2 S. 2 BDSG Gebrauch gemacht hat[16].

Eine gewisse Stärkung erfährt das Recht auf Löschung nach dem DS-GVO-E jedoch dadurch, dass bei Nichtbeachtung des Rechts auf Löschung empfindliche Sanktionsmöglichkeiten gem. Art. 79 Abs. 5 lit. c DS-GVO-E nunmehr zwingend vorgesehen sind. Die EG-DSRl schafft in Art. 24 lediglich die Befugnis der Mitgliedstaaten, Sanktionen für Verstöße gegen die Umsetzungsvorschriften festzulegen. Dabei wird den Mitgliedstaaten ein großer Handlungsspielraum eingeräumt, welche Tatbestände tatsächlich sanktioniert werden sollen.[17]

3.2 Recht auf Vergessenwerden

Über das Recht auf Löschung hinaus begründet Art. 17 Abs. 2 DS-GVO-E das so genannte Recht auf Vergessenwerden. Es stellt eine der wesentlichen Neuerungen des DS-GVO-E dar.[18] Art. 17 Abs. 2 DS-GVO-E besagt, dass der für die Verarbeitung Verantwortliche, der personenbezogene Daten öffentlich gemacht hat, bezüglich dieser Daten alle vertretbaren Schritte zu unternehmen hat, um Dritte, die die Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt. Die Regelung soll dem einzelnen Internetnutzer die Möglichkeit geben, seine Daten im Internet zu beherrschen und trägt damit der Problematik Rechnung, dass einmal in das Netz gestellte Informationen ständig und für den Einzelnen unkontrollierbar weiter verbreitet werden können.

Fraglich ist, ob das Recht auf Vergessenwerden auch bei sozialen Netzwerken eingreift. Das Recht auf Vergessenwerden setzt gemäß Art. 17 Abs. 2 DS-GVO-E ein Öffentlichmachen der personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen voraus, d.h. dieser selbst muss die Daten aktiv so darbieten, dass sie der Öffentlichkeit zugänglich sind. Bei sozialen Netzwerken besteht insofern die Besonderheit, dass die Daten der Nutzer regelmäßig durch diese selbst auf die Webseiten hochgeladen und zumindest in Teilen der Öffentlichkeit präsentiert und zur Verfügung gestellt werden. Die sozialen Netzwerke stellen dabei lediglich die technische Plattform zur Verfügung, die dem Nutzer das Öffentlichmachen ermöglicht bzw. erleichtert. Von einem Öffentlichmachen durch den Betreiber des sozialen Netzwerkes kann deshalb nicht ausgegangen werden, so dass bei sozialen Netzwerken ein Eingreifen des Rechts auf Vergessenwerden abzulehnen ist.

Für ein anderes Ergebnis könnte sprechen, dass die Voreinstellungen zur Nutzung der sozialen Netzwerke regelmäßig so gestaltet sind, dass die eingestellten Daten öffentlich einsehbar

15 Entscheidet sich etwa ein Nutzer zu Beginn seiner beruflichen Karriere von dem sozialen Netzwerk Facebook zu dem Anbieter Xing zu wechseln, so werden sich viele Daten als nicht mit dem neuen Service kompatibel erweisen.

16 Bergmann/Möhrle/Herb (Hg.), Datenschutzrecht (43. Ergänzungslieferung), § 35 Rn. 47.

17 Damann/Simitis, EG-Datenschutzrichtlinie, Art. 24 Rn. 5.

18 Der Gedanke, dass der Internetnutzer im Nachhinein die Spuren seiner Tätigkeit vernichten können muss, ist jedoch auch bereits auf nationaler Ebene in der Diskussion über den „digitalen Radiergummi" behandelt worden; vgl. hierzu Nolte, Zum Recht auf Vergessenwerden im Internet, ZRP 2011, 236 ff.; Federrath/Fuchs/Herrmann et al., Grenzen des „digitalen Radiergummis", DuD 2011, 403 ff.

sind. Eine Auslegung, die ein Öffentlichmachen durch den Betreiber des sozialen Netzwerkes bejaht, wäre jedoch im Ergebnis nicht interessengerecht. Zwar ist die Schaffung eines Rechts auf Vergessenwerden zunächst einmal zu begrüßen und ein Schritt in die richtige Richtung; die Ausklammerung der sozialen Netzwerke aus dem Anwendungsbereich dieser Vorschrift erscheint auch auf den ersten Blick misslich, da sich besonders bei ihrer Nutzung die Problematik der Rückgängigmachung informationeller Spuren nach der Abmeldung zeigt.

Gleichwohl kann im Ergebnis das Recht auf Vergessenwerden gegenüber sozialen Netzwerken nicht eingreifen, da die technische Umsetzbarkeit dieses Rechts derzeit noch äußerst problematisch, wenn nicht gar unmöglich ist. Das Internet ermöglicht ein müheloses Kopieren und Weiterverbreiten von Daten ohne Rücksicht auf entgegenstehende Betroffeneninteressen. Das Recht auf Vergessenwerden beschränkt sich entsprechend in seiner derzeitigen Fassung[19] lediglich auf eine Informationspflicht des Verantwortlichen gegenüber Dritten.[20] Aber bereits die Umsetzung dieser Informationspflichten erscheint in der Praxis problematisch, da es im Internet nicht ohne weiteres möglich ist, festzustellen, wer die veröffentlichten Daten als Dritter verarbeitet. Insbesondere durch große soziale Netzwerke erscheint eine solche Pflicht nicht umsetzbar. Soziale Netzwerke zeichnen sich vielmehr gerade dadurch aus, dass Bilder und Daten ständig kopiert und verbreitet werden. Durch wen dies jeweils erfolgt und wer deshalb über das Verlangen der Löschung gem. Art. 17 Abs. 2 DS-GVO-E zu unterrichten ist, ist für den Betreiber eines sozialen Netzwerkes im Normalfall nicht nachvollziehbar, so dass entsprechende Schritte zur Information Dritter zumindest nicht mehr als vertretbare Anstrengung im Sinne des Art. 17 Abs. 2 DS-GVO-E zu bewerten wären.

Damit ist es im Ergebnis richtig, dass das Recht auf Vergessenwerden bezüglich sozialer Netzwerke von Vornherein nicht eingreift, zumal im Hinblick auf die verschärften Sanktionsmöglichkeiten nach dem Verordnungsentwurf andernfalls ein unübersehbares Haftungsrisiko für die Verantwortlichen bestünde. Es ist zudem zu beachten, dass im Fall der Übermittlung von Daten durch den Betreiber des sozialen Netzwerkes an Dritte die sich bereits jetzt aus Art. 12 lit. c EG-DSRl ergebende Pflicht des Betreibers, den Dritten über die Löschung zu verständigen, soweit dies keinen unverhältnismäßigen Aufwand erfordert, mit Art. 13 nach dem DS-GVO-E weiterhin vorgesehen ist. Durch diese Regelung wird dem Löschungsanspruch des Betroffenen bereits zusätzliches Gewicht gegeben.

Die stets geäußerte Mahnung „das Internet vergisst nie" gilt damit trotz Einführung eines Rechts auf Vergessenwerden zunächst fort. Der Internetnutzer sollte auf den begrenzten Anwendungsbereich und die im Allgemeinen schwierige Umsetzbarkeit dieses Rechts hingewiesen werden, um zu verhindern, dass er sich insbesondere bei der Nutzung sozialer Netzwerke in falscher Sicherheit wiegt.

4 Fazit

Der DS-GVO-E enthält zahlreiche rechtliche Neuerungen zum Schutz von Nutzerdaten sowie zur Förderung der informationellen Selbstbestimmung, die das bisherige Datenschutzrecht nicht kennt. Dabei wird die Regelungsintention des EU-Gesetzgebers erkennbar, den interaktiven Austausch von personenbezogenen Daten im Internet rechtlich weitergehend zu regulieren. In Bereichen, in welchen nach der EG-DSRl und dem BDSG bisher keine Regelungsstrukturen bestanden, werden neue normative Konzepte entworfen, so die Einführung einer starren Altersgrenze im Rahmen der Einwilligung bei Minderjährigen bis zum vollendeten 13. Lebensjahr und die Ungleichgewichtsregelung gem. Art. 7 Abs. 4 DS-GVO-E; speziell für die Netzwerkbenutzung wird dem Nutzer zudem ein Recht auf Datenübertragbarkeit gem. Art. 18 DS-GVO-E eingeräumt. Darüber hinaus findet eine Stärkung des Rechts auf Löschung durch das in Art. 17 Abs. 2 DS-GVO-E normierte Recht auf Vergessenwerden statt.

Hinsichtlich dieser neuen Regelungsinstrumente bestehen aber zum Teil noch offene Fragen.

Das Eingreifen des Rechts auf Vergessenwerden auf soziale Netzwerke ist fraglich. Die besseren Argumente sprechen dafür, dieses abzulehnen. Ebenso ist die Anwendbarkeit der Ungleichgewichtsregelung für soziale Netzwerke aufgrund ihrer engen begrifflichen Fassung zweifelhaft. Daneben ist die Einwilligungsfähigkeit von Nutzern sozialer Netzwerke im Alter von 13 bis einschließlich 17 Jahren ungeklärt. Für Nutzer bis zum vollendeten 13. Lebensjahr sollten darüber hinaus effektive Kontrollinstrumente zur Nachprüfbarkeit der Einwilligung der Erziehungsberechtigten geschaffen werden. Das Recht auf Datenübertragbarkeit stellt für den Nutzer sozialer Netzwerke zwar einen Vorteilsgewinn dar, jedoch bestehen auch hier noch Fragen hinsichtlich der technischen Realisierung dieses Rechts.

19 Anders als noch die im November 2011 bekannt gewordene vorläufige Fassung des Verordnungsentwurfs, in der es in Art. 15 Abs. 2 heißt: "Where the controller referred to in paragraph 1 has made the data public, it shall in particular ensure the erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service which allows or facilitates the search of or access to this personal data.", abrufbar unter: http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf (Stand: 04.06.2012).

20 So auch Hornung, Eine Datenschutz-Grundverordnung für Europa?, ZD 2012, 99, 103.