Vergessen als Gefahr und Gnade

Das Recht auf Vergessen(werden) und seine Bedeutung für den Jugendschutz

Dinah Huerkamp

A. Einführung

In der Erzählung »Tina oder über die Unsterblichkeit« beschreibt Arno Schmidt die Unfähigkeit zu vergessen bzw. vergessen zu werden als qualvolle Höllenerfahrung. Er lässt bekannte Schriftsteller so lange gemeinsam in der Unterwelt schmoren, bis ihr Name auf Erden vergessen und unwiderruflich aus allen Schriften getilgt ist. Goethe, Schiller und ihre Leidensgenossen, die sich in der von Schmidt skurril skizzierten Hölle versammeln und sich im Laufe der Jahrhunderte zahlreichen zwischenmenschlichen Herausforderungen ausgesetzt sehen, eint somit Eines: Der unbändige Wunsch, endlich vergessen zu werden.[1]

Mit der Betonung der Vorzüge des Vergessenwerdens ist Arno Schmidt wohl eher einer Minderheit zuzuordnen. Seit Jahrtausenden gilt ein gutes Erinnerungsvermögen als evolutionärer Vorteil. Vergesslichkeit wird demgegenüber meist als Schwäche interpretiert.[2] Das digitale Zeitalter mit seinen bis dahin unvorstellbaren Möglichkeiten der Datenspeicherung wurde daher lange als Chance begriffen, unsere Erinnerungsfähigkeit zu optimieren. Die ersten Schritte eines Kindes lassen sich so heute bei Myspace verfolgen, Jugendliche posten Fotos in jeder denkbaren Lebenslage bei Facebook, Google speichert jede jemals eingegebene Suchanfrage.[3] Heute sehen wir uns – und insofern erfährt die Erzählung Schmidts durch die Entwicklung der neuen Medien eine ganz neue, ungeahnte Aktualität – jedoch eher mit der umgekehrten Herausforderung konfrontiert: Gerade auch die jüngste Prism-Affäre hat das Bewusstsein der breiten Öffentlichkeit dafür geschärft, dass es nicht länger um die Frage geht, wie wir uns am besten erinnern und Erinnerungen konservieren können. Vielmehr wird zunehmend wichtig, wie wir die Verfügungsgewalt über unsere Daten behalten bzw. wiedererlangen können[4] und wie hierfür einmal im Internet preisgegebene Daten auch wieder rückstandslos entfernt werden können.

Gerade auch für die Autonomieentwicklung von Kindern und Jugendlichen ist das Vergessen des Internets von ganz maßgeblicher Bedeutung: Das Internet ist nicht nur unter dem Gesichtspunkt der Informationsbeschaffung, Freundschaftspflege und gesellschaftlichen Teilhabe für die Entwicklung von Kindern und Jugendlichen zu autonomen Wesen wichtig.[5] Für ihre Persönlichkeitsentwicklung kann es ebenso entscheidend sein, dass von ihnen preisgegebene Daten wieder aus dem Internet verschwinden.[6] Denn es gehört zum natürlichen Reifungsprozess von Kindern und Jugendlichen, sich im Laufe der Zeit von früheren Meinungsäußerungen zu distanzieren und neue Ansichten zu entwickeln.[7] Und so sollte auch das Internet auf Dauer dem Bedürfnis nach Vergessen ausreichend Rechnung tragen. Denn es kann – um in den Worten Theodor Heuss', Vergessen sei Gefahr und Gnade zugleich, zu bleiben[8] – letztlich wirklich wahre Gnade sein, im Bewerbungsgespräch nicht mit sämtlichen »Jugendsünden« aus dem Internet konfrontiert zu werden.

Dinah Huerkamp ist Justiziarin der Arbeitsgemeinschaft Kinder- und Jugendschutz Landesstelle NRW e.V. (AJS) in Köln.

B. Recht auf Vergessen(werden)

I. Begriffsdefinition

Mit dem »Recht auf Vergessen(werden)« soll das Recht des Internetnutzers, die Beseitigung seiner Daten aus dem Internet verlangen zu können, auf eine rechtliche Grundlage gestellt werden.

Dieser Vorstoß kann – ungeachtet der derzeit noch bestehenden erheblichen technischen Schwierigkeiten bei der Umsetzung[9] – jedoch von vorneherein nur dann gelingen, wenn das Recht auf Vergessen(werden) den Erinnerungsvorgängen im Internet ausreichend Rechnung trägt. Denn dem Internetnutzer wäre mit einem Recht auf Vergessen(werden) wenig gedient, das lediglich Löschungsansprüche gegen die seine personenbezogenen Daten verarbeitende Stelle – z. B. Facebook – vorsieht, aber nicht ausreichend berücksichtigt, dass eine jede Dateneingabe unzählige weitere Erinnerungsschritte im Internet nach sich zieht, durch die die personenbezogenen Daten – einem »Schneeballsystem« vergleichbar[10] – im Netz verteilt werden. So werden die Daten nicht nur auf dem Server der datenverarbeitenden Stelle gespeichert, sondern es werden von ihnen Sicherheitskopien angefertigt, sie werden in Zwischenspeichern abgelegt, an Dritte weitergegeben, sind fortan über Suchmaschinen aufspürbar etc. Bildlich gesprochen muss ein »Recht auf Vergessen(werden)« immer auch Spiegelbild der Erinnerungsvorgänge im Netz sein[11], um überhaupt das Potential zu haben, eines Tages effektiv ansetzen zu können.

II. De lege lata

1. Deutschland

a) einfaches Recht

Entsprechende Regelungen sind auch dem deutschen Recht grundsätzlich nicht fremd, das sowohl Lösch- als auch Informationspflichten gegenüber Dritten kennt (vgl. z. B. §§ 20 Abs. 2 und 8, 35 Abs. 2 und 7 BSDG, § 13 Abs. 4 Nr. 2 Telemediengesetz). Löschungsbegehren können teilweise zudem mithilfe von Unterlassungs- und Beseitigungsansprüchen durchgesetzt werden.[12] Informationspflichten gegenüber Dritten werden ferner häufig dem Äußerungs-, Wettbewerbs- und Urheberrecht entnommen.[13]

b) Verfassungsrecht und verfassungsgerichtliche Rechtsprechung

Besondere Bedeutung für die Frage der Verfügungsgewalt über die eigenen Daten im Netz kommt dem »Grundrecht auf informationelle Selbstbestimmung« zu, welches das Bundesverfassungsgericht (BVerfG) in seinem »Volkszählungsurteil« als Fallgruppe des Allgemeinen Persönlichkeitsrechts, Artikel 1 Abs. 1 GG i.V.m. Artikel 2 Abs. 1 GG, herausgebildet hat.[14] Das Recht auf informationelle Selbstbestimmung gewährleistet »die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen«.[15]

Als Grundrecht schützt das Recht auf informationelle Selbstbestimmung grundsätzlich erst einmal nur Private vor Eingriffen durch den Staat. Allerdings entfaltet es auch in Verhältnissen, an denen

lediglich Private beteiligt sind – und bei der Dateneingabe im Internet stehen sich im Normalfall nur Private gegenüber – Wirkungen. Denn unabhängig davon, ob man diese Wirkungen unter dem Oberbegriff der »mittelbaren Drittwirkung«[16] oder der »Schutzpflicht des Staates«[17] diskutiert, ist das Verfassungsrecht auch bei der Auslegung einfach-gesetzlicher Normen, die zwischen Privaten Anwendung finden, zu berücksichtigen. Insofern ist die Weiterentwicklung des Rechts auf informationelle Selbstbestimmung durch die Gerichte auch für Konstellationen, in denen nur Private handeln, interessant. Allerdings lässt sich die für Staat-Bürger-Konstellationen ergangene Rechtsprechung nicht immer problemlos auf Verhältnisse übertragen, an denen lediglich Private beteiligt sind.[18] Umso bedeutsamer sind einige jüngere Entscheidungen der Obergerichte, die das informationelle Selbstbestimmungsrecht im Verhältnis von Privaten zu konkretisieren versuchen.

aa) BGH: Lebach III

In seiner Lebach III-Entscheidung[19] hatte der Bundesgerichtshof (BGH) zu entscheiden, inwiefern das Allgemeine Persönlichkeitsrecht es gebietet, Berichte über eine Straftat unter namentlicher Nennung des Täters aus einem Online-Archiv zu löschen. Im Rahmen der vorzunehmenden umfassenden Interessenabwägung stellte der BGH heraus, dass insbesondere der »Verbreitungsgrad eines Mediums« dafür entscheidend sei, ob dem allgemeinen Persönlichkeitsrecht/dem Recht auf Achtung des Privatlebens oder der ebenfalls betroffenen Meinungs- und Medienfreiheit der Vorrang einzuräumen sei. Bei einem Online-Archiv sei der Verbreitungsgrad eher gering, da die Artikel gezielt durch Interessenten aufgesucht werden müssten und sich auch nicht auf der aktuellen Seite des Internetauftritts befänden. Ferner müsse auch das Interesse der Nutzer an der Recherchierbarkeit zeitgeschichtlicher Themen Berücksichtigung finden. Eine Verpflichtung zur Löschung aller früheren, den Straftäter identifizierenden Darstellungen in Onlinearchiven führe ferner dazu, »dass Geschichte getilgt und der Straftäter vollständig immunisiert würde«. Insofern müsse hier das allgemeine Persönlichkeitsrecht/das Recht auf Achtung des Privatlebens zurücktreten.

bb) BGH: Autocomplete-Funktion von Google

In seiner Entscheidung vom 14.05. 2013[20] hat der BGH festgestellt, dass die Autocomplete-Funktion von Google zu Verletzungen des allgemeinen Persönlichkeitsrechts führen kann. Die Autocomplete-Funktion ergänzt zum Zwecke der Suchvereinfachung eingegebene Suchbegriffe um weitere Suchbegriffe, die mithilfe eines Algorithmus aus dem Suchverhalten anderer Nutzer abgeleitet werden. Den Suchmaschinenbetreiber treffe in den Fällen eine rechtliche Verantwortlichkeit, in denen die Verknüpfung der Begriffe zu einem »unwahren Aussagegehalt« führe. Eine Verantwortlichkeit bestehe jedoch auch nur dann, wenn der Suchmaschinenbetreiber Kenntnis von der Rechtsverletzung habe, eine präventive Prüfpflicht habe er – etwas anderes könne in Bereichen wie der Kinderpornografie gelten – jedoch nicht. Ab Kenntniserlangung treffe den Suchmaschinenbetreiber dann auch eine Verpflichtung zur Verhinderung künftiger Rechtsverstöße.

2. Europa

Auf europäischer Ebene werden personenbezogene Daten insbesondere durch Artikel 8 Absatz 1 Grundrechtecharta, Artikel 16 Abs. 1 AEUV, Artikel 8 Abs. 1 EMRK und Artikel 12 Datenschutzrichtlinie (Richtlinie 95/46 EG) geschützt. Artikel 12 b) der Datenschutzrichtlinie sieht einen Anspruch auf Löschung bzw. Sperrung von Daten vor, deren Verarbeitung nicht den Bestimmungen der Richtlinie entspricht, insbesondere wenn die Daten unvollständig oder unrichtig sind. Artikel 12 c der Datenschutzrichtlinie verpflichtet den Datenanwender außerdem dazu, jede Löschung oder Sperrung Dritten, denen die Daten übermittelt wurden, mitzuteilen, sofern sich dies nicht als unmöglich erweist und kein unverhältnismäßiger Aufwand damit verbunden ist. Generalanwalt Niilo Jääkinen hat im Zusammenhang mit der derzeit noch beim Europäischen Gerichtshof (EuGH) anhängigen Rechtssache C-131/12[21] erst kürzlich darauf hingewiesen[22], dass sich ein allgemeines Recht auf Vergessenwerden der Datenschutzrichtlinie jedoch nicht – auch nicht in ihrer Auslegung im Einklang mit der Charta der Grundrechte der Europäischen Union – entnehmen lasse. Ein Löschungs- bzw. Sperrungsanspruch bestehe nur im Hinblick auf Daten, deren Verarbeitung nicht den Bestimmungen der Richtlinie entspreche oder wenn ein Widerspruch aus überwiegenden, schutzwürdigen und sich aus der besonderen Situation des Nutzers ergebenden Gründen erfolge. Eine subjektive Präferenz einer Datenlöschung sei jedoch nicht als überwiegender schutzwürdiger Grund zu qualifizieren.

3. Bewertung aus kinder- und jugendschutzrechtlicher Perspektive

Die bestehenden deutschen und europäischen Regelungen, mit deren Hilfe die Löschung von Daten bzw. die Information Dritter verlangt werden kann, müssen aus kinder- und jugendschutzrechtlicher Perspektive und vor dem Hintergrund der Bedeutung und Gefahren der Internetnutzung für die Persönlichkeitsentwicklung von Minderjährigen als defizitär bewertet werden. Weder das Bundesdatenschutzgesetz noch das Telemediengesetz sehen speziell auf Minderjährige zugeschnittene Regelungen vor. Zwar können sich Minderjährige auf das Recht auf informationelle Selbstbestimmung berufen[23] und Letzteres dürfte sie im Falle erhöhter Schutzbedürftigkeit sogar weitergehend schützen als Erwachsene.[24] Allerdings sind für den Schutz Minderjähriger vor der Datensammlung und -nutzung durch Dritte noch keine hinreichend präzisen Kriterien entwickelt worden. Dass der BGH in seinem Urteil zu Googles Autocomplete-Funktion feststellt, Suchmaschinenbetreiber könnten in bestimmten Bereichen, z. B. der Kinderpornografie, präventive Prüfpflichten treffen, ist aus kinder- und jugendschutzrechtlicher Perspektive zwar begrüßenswert. Insgesamt bleibt das Urteil an dieser Stelle jedoch zu vage.

Insofern ließe sich überlegen, inwiefern sich Grundsätze zum Persönlichkeitsschutz Minderjähriger im Kontext medialer Berichterstattung auf die vorliegende Konstellation übertragen lassen. Die Gefahrenlage erscheint bei einer Veröffentlichung personenbezogener Daten Minderjähriger im Internet den Gefahren, die von einer medialen Berichterstattung über Minderjährige ausgehen, zumindest vergleichbar. Für die Persönlichkeitsentwicklung Minderjähriger kann die dauerhafte Zugriffsmöglichkeit auf problematische Daten über Suchmaschinen im Zweifel noch sehr viel verheerendere Auswirkungen haben als eine mediale Berichterstattung. Dies gilt umso mehr, als Seiten, die im Internet Aufmerksamkeit erregen, aufgrund ihrer leichten Zugänglichkeit häufig innerhalb kürzester Zeit von einer großen Anzahl von Internetnutzern aufgerufen werden und somit einen sehr großen Verbreitungsgrad erreichen können. Die von Beater entwickelten Grundsätze zur Berücksichtigung des Vorverhaltens Minderjähriger ließen sich vor diesem Hintergrund gut auf die Konstellation eines geltend gemachten Löschungsbegehrens übertragen. Anders als bei Erwachsenen soll bei Minderjährigen bei der persön-

lichkeitsrechtlichen Prüfung ein etwaiges Vorverhalten des Betroffenen nicht mit der gleichen Selbstverständlichkeit zu berücksichtigen sein, wie es im Zusammenhang mit Erwachsenen der Fall sei. Vielmehr seien die Schutzinteressen der Minderjährigen stärker zu berücksichtigen.[25] Auch wenn ein Minderjähriger selbst seine personenbezogenen Daten ins Internet geladen hat, scheint es nach diesen Grundsätzen schwierig, seinem geltend gemachten Löschungsanspruch beispielsweise pauschal entgegenzuhalten, er habe seine Daten doch schließlich in das Netz geladen und sich so der Verfügungsgewalt über seine Daten begeben bzw. ein besonderes Interesse der Öffentlichkeit an seinen Daten nun selbst zu verantworten.

Übertragbar scheinen auch die durch das Bundesverfassungsgericht entwickelten Maßstäbe zur Prüfung der »Schwere der Beeinträchtigung«: Genauso wie öffentliche Berichte über Minderjährige potentiell stärker in die Persönlichkeitsinteressen Minderjähriger eingreifen als Berichte über Erwachsene, weil Erstere sehr viel leichter in ihrer Persönlichkeitsentfaltung gestört werden können[26], beeinträchtigt das Vorhalten personenbezogener Daten im Internet Minderjährige potentiell stärker als Erwachsene. Insofern sollten Minderjährige durch eine großzügigere Handhabung des Kriteriums der Beeinträchtigungsschwere weitergehend geschützt werden als Erwachsene.

Um Rechtsklarheit und -sicherheit zu schaffen, scheint es dennoch vorzugswürdig, die Problematik einer einfachgesetzlichen Klärung zuzuführen. So könnten auch weitere Unsicherheiten, die in Bezug auf Löschungsansprüche Minderjähriger bestehen – beispielsweise die Voraussetzungen eines Widerrufs der Einwilligung in eine Datenverarbeitung vonseiten Minderjähriger[27] – einer abschließenden Klärung zugeführt werden. Aus kinder- und jugendschutzrechtlicher Perspektive wäre eine europäische Regelung wünschenswert. Da es sich beim Internetverkehr häufig um grenzüberschreitende Vorgänge handelt, könnte so eine Rechtsharmonisierung und ein einheitliches Schutzniveau erreicht werden. Bei einheitlichen europäischen Schutzstandards würde es dem Internetanbieter erschwert, durch eine Serververlagerung ins EU-Ausland die Anwendbarkeit nationaler Normen und somit deren Regelungen zum Schutze Minderjähriger zu umgehen.[28] Ein wirklich effektiver Minderjährigenschutz kann letztlich aber nur dann gelingen, wenn er mithilfe weltweit durchsetzbarer Abkommen vereinbart wird.[29] Entsprechende europäische Regelungen wären aber zumindest als erster Schritt in die richtige Richtung zu bewerten.

III. De lege ferenda

Sowohl auf nationaler als auch auf europäischer Ebene ist der Bedarf erkannt worden, das Vergessen des Internets auf eine rechtliche Grundlage zu stellen und hierbei auch die Interessen Minderjähriger besonders zu schützen.[30]

1. Deutschland

Während zunächst überlegt wurde, bei besonders schweren Persönlichkeitsrechtsverletzungen im Internet den Betroffenen einen immateriellen Schadensersatzanspruch an die Hand zu geben,[31] wird derzeit im Bundestag eine Änderung des Telemediengesetzes (TelemedienG-E)[32] diskutiert. Gemäß § 13 Abs. 4 Satz 1 Nr. 3 TelemedienG-E sollen Anbieter von Telemediendiensten zur Installation von leicht erkennbaren, unmittelbar erreichbaren und ständig verfügbaren Löschknöpfen verpflichtet werden, mit denen Nutzer die Löschung ihres Nutzerkontos jederzeit selbst veranlassen können. Flankiert wird diese Regelung von Löschpflichten des Diensteanbieters, § 13 Abs. 4 Satz 1 Nr. 2 und 4 und Abs. 2 TelemedienG-E. Letzterer ist grundsätzlich gehalten, nach Betätigung des Löschknopfes unverzüglich das Nutzerkonto zu löschen. Ferner soll er anfallende personenbezogene Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach dessen Beendigung löschen oder sperren müssen. Für Telemediendienste mit nutzergenerierten Inhalten[33] werden die Löschungspflichten in § 13 a Abs. 3 TelemedienG-E durch die Verpflichtung zur Löschung aller durch den Nutzer erzeugten Inhalte bzw. – wenn die Inhalte in Zusammenhang mit nutzergenerierten Inhalten anderer Nutzer stehen – durch die Pflicht zur Anonymisierung ergänzt. Diese Pflichten sollen gemäß § 13 a Abs. 3 TelemedienG-E nur dann nicht bestehen, wenn eine Löschung oder Anonymisierung nach dem Verwendungszweck nicht möglich ist oder einen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. §§ 13 Abs. 4 Satz 1 Nr. 4 und Satz 3 TelemedienG-E sehen außerdem vor, dass ein Nutzerkonto ein Jahr nach der letzten Nutzung zu löschen bzw. zu sperren ist, wobei der Nutzer vier Wochen vorher hiervon zu unterrichten ist. Flankiert werden diese Regelungen von Bußgeldvorschriften und einer Pflicht des Diensteanbieters, »in allgemein verständlicher Form, leicht erkennbar und unmittelbar erreichbar« zu Beginn des Nutzungsvorgangs über die Datenverwendung zu informieren.

2. Europa

Auf europäischer Ebene wird derzeit die Einführung eines »Rechts auf Vergessen(werden) (»right to be forgotten«) in Artikel 17 der geplanten Datenschutz-Grundverordnung (DSGV-E), die die Datenschutzrichtlinie (RL 95/46 EG) ablösen soll, diskutiert. Die Vorschrift sieht insbesondere einen Löschungs- und einen Informationsanspruch vor, die in der Folge beleuchtet werden sollen.

a) Löschungsanspruch

Artikel 17 DSGV-E enthält in Absatz 1 einen Anspruch des Internetnutzers, die Löschung von personenbezogenen Daten bzw. die Unterlassung ihrer Weiterverarbeitung von der für die Datenverarbeitung verantwortlichen Stelle verlangen zu können, wenn es zu einem Zweckfortfall, zu einem Widerruf der Einwilligung, einem Ablauf der Speicherfrist oder einem Widerspruch gegen die Verarbeitung gekommen ist oder die Datenverarbeitung nicht mit der Datenschutzgrundverordnung vereinbar ist bzw. es an einer anderen Rechtsgrundlage für die Verarbeitung der Daten fehlt. Da Artikel 17 DSGV-E mit »Recht auf Vergessenwerden *und auf Löschung*« übertitelt ist, wird häufig darauf hingewiesen, unter dem europäischen Recht auf Vergessenwerden könne nicht der Löschungsanspruch, sondern allenfalls der in Artikel 17 Abs. 2 DSGV-E geregelte Informationsanspruch verstanden werden.[34]

b) Informationsanspruch

Der Löschungsanspruch wird ergänzt durch einen Informationsanspruch in Artikel 17 Absatz 2 DSGV-E. Hat der für die Datenverarbeitung Verantwortliche die Daten öffentlich gemacht, so muss er »alle vertretbaren Schritte« unternehmen, um datenverarbeitende Dritte über den geltend gemachten Löschungsanspruch zu informieren.

c) Regelungen zum Schutze Minderjähriger

Die Datenschutz-Grundverordnung sieht eine Vielzahl von Regelungen vor, die einen besonderen Schutz Minderjähriger sicherstellen sollen. So heißt es bereits in den Gründen der Verordnung,

die personenbezogenen Daten Minderjähriger müssten besonderen Schutz genießen, »da Kinder sich der Risiken, Folgen, Vorsichtsmaßnahmen und ihrer Rechte bei der Verarbeitung personenbezogener Daten weniger bewusst sein dürften«. Eine Legaldefinition des Kindesbegriffes findet sich in Artikel 4 Abs. 18 DSGV-E: Danach ist jede Person bis zur Vollendung des 18. Lebensjahres ein Kind.

Für den in Artikel 17 Abs. 1 DSGV-E geregelten Löschungsanspruch gilt, dass dieser »speziell, wenn es sich um personenbezogene Daten handelt, die die betroffene Person im Kindesalter öffentlich gemacht hat«, bestehen soll. Bei einer vorzunehmenden Interessen- und Rechteabwägung kommt den Kinderinteressen somit ein besonderes Gewicht zu.

Da personenbezogene Daten insbesondere dann zu löschen sein können, wenn die betroffene Person gemäß Artikel 17 Abs. 1 b) DSGV-E ihre Einwilligung widerruft, ist auch Artikel 8 Abs. 1 DSGV-E von besonderer Bedeutung, der die Einwilligung Minderjähriger in eine Datenverarbeitung im Zusammenhang mit Online-Diensten regelt. Danach ist die Verarbeitung personenbezogener Daten eines Kindes, dem direkt Dienste der Informationsgesellschaft angeboten werden, bis zum vollendeten dreizehnten Lebensjahr »nur rechtmäßig, wenn und insoweit die Einwilligung hierzu durch die Eltern oder den Vormund des Kindes oder mit deren Zustimmung erteilt ist.« Der für die Datenverarbeitung Verantwortliche wird in Artikel 8 Abs. 1 S. 2 DSGV-E dazu verpflichtet, unter Berücksichtigung der vorhandenen Technologie angemessene Anstrengungen zu unternehmen, um eine nachprüfbare Einwilligung zu erhalten.

Hinzuweisen ist überdies auf Artikel 11 Abs. 2 DSGV-E, der den für die Datenverarbeitung Verantwortlichen dazu verpflichtet, alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten – insbesondere bei Beteiligung eines Kindes an dem Datenverarbeitungsvorgang – in »klarer, einfacher und adressatengerechter Sprache« zur Verfügung zu stellen.

d) Weitere flankierende Regelungen

Um das »Recht auf Vergessenwerden« abzusichern, sieht die DSGV-E in Artikel 79 Abs. 5 c) vor, dass eine Geldbuße bis zu 500.000 Euro oder im Fall eines Unternehmens bis in Höhe von einem Prozent seines weltweiten Jahresumsatzes verhängt werden kann, wenn das Recht auf Vergessenwerden oder auf Löschung nicht beachtet wird bzw. keine Vorkehrungen getroffen werden, um die Einhaltung der Fristen zu gewährleisten. Gleiches gilt, wenn nicht alle erforderlichen Schritte unternommen werden, um Dritte von einem Antrag auf Löschung von Links zu personenbezogenen Daten sowie Kopien oder Replikationen dieser Daten gemäß Artikel 17 DSGV-E zu benachrichtigen.

3. Bewertung der neuen Regelungen aus kinder- und jugendschutzrechtlicher Sicht

a) Deutschland

Grundsätzlich scheint die in §§ 13 Abs. 4 S. 2 und 13 a Abs. 3 S. 1 TelemedienG-E vorgesehene Regelung einer Löschpflicht nach Betätigung des entsprechenden Bedienelements der Regelung eines Schmerzensgeldanspruchs bei Persönlichkeitsverletzungen vorzugswürdig. Ein Schadensersatzanspruch in Geld beseitigt eine Grundrechtsverletzung nicht[35] und es scheint insbesondere auch im Hinblick auf die Persönlichkeitsentfaltung Minderjähriger vorzugswürdig, wenn der Diensteanbieter verpflichtet wird, das Nutzerkonto und alle nutzergenerierten Inhalte eines Nutzers zu löschen. Eine entsprechende Löschpflicht geht auch insofern weiter als der ursprünglich vorgesehene Schmerzensgeldanspruch, als dieser nur bei Persönlichkeitsverletzungen – also rechtswidrigem Verhalten – greifen sollte. Insofern wird ein umfassenderer Schutz der Kinder und Jugendlichen erreicht. Allerdings sollte noch genauer konkretisiert werden, was unter der Pflicht zur Löschung zu verstehen ist. Denn dass es für ein effektives Recht auf Vergessen(werden) nicht ausreicht, die Daten von den Servern der datenverarbeitenden Stellen zu löschen, weil die Daten nach der Eingabe noch sehr viel weitgehender im Internet verteilt werden, ist bereits dargelegt worden. Hier lässt der Gesetzentwurf noch Fragen offen. Positiv an dem Löschknopf ist ferner, dass er aufwendige Abmeldungsvorgänge entbehrlich macht und so die Benutzerfreundlichkeit erhöht. Dies gilt umso mehr, als die Löschung eines Benutzeraccounts die Nutzer gerade bei Social Networks in der Praxis vor nicht unerhebliche Probleme stellt und aufgrund ihrer Komplexität gerade Kinder und Jugendliche häufig überfordern dürfte. In die Einführung eines Löschknopfes dürfen allerdings nicht allzu große Hoffnungen gesetzt werden: Zwar heißt es in der Gesetzesbegründung, eine selbstständige Löschung des Nutzerkontos und der darin enthaltenen personenbezogenen Daten durch den Nutzer dürfte technisch nicht umsetzbar sein, sodass die Betätigung des Löschknopfes dem Nutzer die Möglichkeit biete, dem Diensteanbieter auf einfache Art und Weise mitzuteilen, dass das Nutzerkonto gelöscht werden solle und Letzterer die Löschung vornehmen könne.[36] Dies darf nicht darüber hinwegtäuschen, dass auch die technischen Möglichkeiten des Diensteanbieters, die Daten rückstandslos aus dem Netz zu entfernen, derzeit noch begrenzt sind.

Ob es demgegenüber sinnvoll und vor allem verhältnismäßig ist, Nutzerkonten automatisch zu löschen, wenn sich der Nutzer über ein Jahr lang nicht eingeloggt hat, dürfte zu bezweifeln sein. Der lapidare Hinweis in der Gesetzesbegründung, man könne die entsprechenden Daten bei einem entsprechenden Bedürfnis einfach wiedereinstellen[37], verfängt so nicht, da keineswegs klar ist, ob der Internetnutzer noch über die entsprechenden Daten und Dateien verfügt. Genauso, wie eine Person unter bestimmten Voraussetzungen darüber entscheiden können soll, ob ihre personenbezogenen Daten weiterhin verwendet werden dürfen, sollte sie grundsätzlich darüber entscheiden dürfen, ob ihre Daten im Netz verbleiben sollen, ohne dass es der regelmäßigen Bestätigung ihrer Einwilligung und einer staatlichen Intervention bedarf.

Mit der Verabschiedung des Telemediengesetzes sollte – da im Falle einer Kollision mit europäischem Recht eine Unwirksamkeit der nationalen Vorschriften die Folge wäre – gewartet werden. Dies gilt umso mehr, als Generalanwalt Niilo Jääkinen bereits die Ansicht geäußert hat, dass nationale Löschungsansprüche gegen Suchmaschinenbetreiber in Bezug auf in die öffentliche Sphäre gelangte legitime und rechtmäßige Inhalte mit der Meinungsäußerungsfreiheit unvereinbar seien, da sie letztlich eine Zensur bedeuteten.[38] Zu begrüßen wäre aus kinder- und jugendschutzrechtlicher Sicht jedoch, wenn von der Diskussion über eine Änderung des Telemediengesetzes auch Impulse für die geplante Datenschutzgrundverordnung ausgingen.

b) Europarecht

Dass die geplante DSGV die Interessen der Kinder in besonderem Maße berücksichtigen soll und so den Gefahren der Internetnutzung begegnet, ist grundsätzlich ein sehr begrüßenswertes Novum. Insbesondere in Bezug auf die zu erteilende Einwilligung in die Datenverarbeitung und die Widerrufsmöglichkeit hätten

jedoch weitergehende Regelungen erfolgen sollen. Die Einwilligungsregelung des Artikel 8 Abs. 1 DSGV-E beschränkt sich auf Online-Dienste, wäre jedoch auch im Zusammenhang mit anderen Datenverarbeitungsvorgängen sinnvoll.[39] In der rechtswissenschaftlichen Literatur wird teilweise begrüßt, dass die DSGV – anders als das deutsche Recht – klare Altersgrenzen für die Einwilligung Minderjähriger enthält.[40] Denn klare Altersstufen bedeuten auch immer mehr Rechtssicherheit und eine bessere Handhabbarkeit in der Praxis. Kehrseite ist jedoch ein Weniger an Passgenauigkeit und Flexibilität, sodass den Entwicklungsstufen und der Autonomieentwicklung – anders als bei einer Einwilligung, die sich nach der Einsichtsfähigkeit richtet – weniger Rechnung getragen wird. Ein vermittelnder Ansatz könnte darin bestehen, eine Einwilligung ab 13 Jahren als im Zweifel wirksam erteilt zu sehen (mit entsprechender Widerlegungsmöglichkeit). Alternativ könnte man auch unterschiedliche Altersstufen dergestalt festlegen, dass zwischen 13 und 16 Jahren die Zweifelsregelung gilt und ab 16 eine Einwilligung ohne Einschränkung wirksam ist.

Dass Artikel 17 Abs. 1 b) DSGV-E einen Löschungsanspruch grundsätzlich auch im Falle eines Widerrufes der Einwilligung vorsieht, ist grundsätzlich zu befürworten. Allerdings enthält Artikel 8 DSGV-E für den Widerruf keine speziellen Regelungen für Minderjährige. Ob an den Widerruf als actus contrarius die gleichen Anforderungen zu stellen sind wie an eine Einwilligung oder ob der Widerruf als einseitiges Rechtsgesschäft § 110 BGB entsprechend bis zur Volljährigkeit immer der Einwilligung des gesetzlichen Vertreters bedarf, bleibt offen. Hier wären weitergehende, für Rechtsklarkeit sorgende Regelungen wünschenswert gewesen. Eine Regelung zur verpflichtenden Einführung eines Löschknopfes für Social Networks, wie sie für das Telemediengesetz angedacht wird, könnte man auch hier sinnvollerweise diskutieren.

Schwierigkeiten bereitet auch die sogenannte »Household-Exemption« in Artikel 2 Abs. 2 d) DSGV-E. Danach ist die DSGV-E nicht anwendbar auf die Verarbeitung personenbezogener Daten, die durch natürliche Personen zu ausschließlich persönlichen oder familiären Zwecken ohne jede Gewinnerzielungsabsicht vorgenommen wird. Gerade im Zusammenhang mit Social Networks dürfte diese Vorschrift eine weitgehende Unanwendbarkeit der DSGV zur Folge haben, und das, obwohl sie gerade im Zusammenhang mit Online-Diensten besonderen Schutz vermitteln möchte, vgl. Artikel 8 Abs. 1 DSGV-E. Wenn jemand nun beispielsweise bei einem Social Network personenbezogene Daten über eine andere Person einstellt und diese nicht der Öffentlichkeit, sondern nur seinem Freundeskreis zugänglich macht, so besteht aufgrund von Artikel 2 Abs. 2 d) DSGV-E mangels Anwendbarkeit der DSGV kein Löschungsanspruch gegen den Nutzer des Social Networks. Ob die von der Datenverarbeitung betroffene Person einen Löschungsanspruch gegen den Anbieter des Social Networks hat, ist auch noch nicht abschließend geklärt.[41] Gerade für Minderjährige, die Social Networks besonders stark frequentieren, könnten sich hieraus Schutzlücken ergeben.

IV. Sonstige Alternativen

Da sich ein »Recht auf Vergessenwerden« derzeit technisch noch nicht zufriedenstellend umsetzen lässt, werden vielfach Alternativen angedacht, die bereits zu einem früheren Zeitpunkt ansetzen. Teilweise wird ein rechtliches Verfallsdatum vorgeschlagen[42], teilweise soll der Problematik mit technischen Anwendungen wie dem »Digitalen Radiergummi« und dem »Digitalen Wasserzeichen« begegnet werden. Von einem digitalen Radiergummi spricht man, wenn Daten verschlüsselt und der für die Entschlüsselung benötigte Schlüssel für einen vorher festgelegten Zeitraum auf einem anderen Server abgespeichert wird. Nach Ablauf dieses Zeitraums ist der Schlüssel nicht mehr abrufbar und somit die elektronisch verschlüsselte Datei nicht mehr zu öffnen.[43] Mithilfe des digitalen Wasserzeichens erfolgt eine Kennzeichnung von Dateien und eine Festlegung der Dauer ihrer Nutzbarkeit. Bevor nun ein Server eine mit einem Wasserzeichen gekennzeichnete Datei überträgt, wird überprüft, ob die Datei zu diesem Zeitpunkt noch freigegeben oder bereits als gelöscht markiert ist. Ist Letzteres der Fall, wird die Datei nicht mehr ausgeliefert.[44] Häufig wird an diesen technischen Lösungen jedoch ihre leichte Umgehbarkeit kritisiert. So ist es beispielsweise ein Einfaches, Screenshots von aufgerufenen Dateien zu fertigen. Diese lassen sich auch nach Ablauf des vorgesehenen Zeitfensters noch problemlos öffnen.[45]

V. Fazit/Ausblick

Die Hauptschwierigkeit im Zusammenhang mit der Regelung eines »Rechtes auf Vergessen(werden)« besteht derzeit noch darin, dass es sich momentan noch nicht technisch zufriedenstellend umsetzen lässt. Damit auf lange Sicht eine effiziente Regelung gelingen kann, ist eine enge Zusammenarbeit zwischen Juristen und Informatikern essentiell: Nur wenn Juristen die Bereitschaft entwickeln, die technischen Voraussetzungen des Erinnerns und Vergessens des Internets zu durchdringen[46] und Informatiker bei ihrer Programmentwicklung berücksichtigen, wo das Recht auch ihnen Grenzen setzt, kann das grundsätzlich begrüßenswerte Projekt, das Vergessen des Internets auf eine rechtliche Grundlage zu stellen, auf Dauer von Erfolg gekrönt sein.

Und auch wenn sich das »Recht auf Vergessen(werden)« derzeit noch Defiziten rechtlicher und technischer Natur ausgesetzt sieht, kann es als wichtiger Schritt in die richtige Richtung bewertet werden. Dies gilt umso mehr, als sich durch die Kombination unterschiedlicher Maßnahmen bereits jetzt ein recht hohes Schutzniveau erreichen lässt: Einerseits lässt sich durch die Verhängung hoher Unternehmensgeldbußen in Einzelfällen, die Artikel 79 Abs. 5 c) DSGV-E erlaubt und die man bereits aus dem Kartellrecht kennt, ein hohes Maß an Regelkonformität erreichen. Drohen Unternehmensgeldbußen bis zu 500.000 Euro bzw. im Fall eines Unternehmens bis in Höhe von einem Prozent des weltweiten Jahresumsatzes, werden Compliance-Anwälte den großen Internetfirmen dazu raten, die Einhaltung der Anforderungen des »Rechts auf Vergessen(werden)« organisatorisch abzusichern. Die so evozierte Selbstregulierung dürfte faktisch einen Anstieg des Schutzniveaus zur Folge haben.[47] Und auch die Möglichkeit der Geltendmachung von Löschungsansprüchen wird – trotz technischer Schwierigkeiten bei der Umsetzung – Wirkungen entfalten und kann durch den Einsatz digitaler Radiergummis und Wasserzeichen sinnvoll ergänzt werden. Derzeit ist jedoch vor allem zu Datensparsamkeit zu raten. Eine gute Medienerziehung, die Minderjährige für die Gefahren des Internets und die Schwierigkeit einer rückstandslosen Datenlöschung sensibilisiert, ist vor diesem Hintergrund das Gebot der Stunde.[48]

---

1 *Schmidt*, Tina oder über die Unsterblichkeit, Insel-Bücherei Nr. 1387, 2013.

2 *Mayer-Schönberger*, Delete. Die Tugend des Vergessens in digitalen Zeiten, 2011, S. 33; *Nolte* ZRP 2011, 236.

3 *Mayer-Schönberger*, aaO, S. 16.

4 Angeblich wollen 75 Prozent der Europäer die Verfügungsgewalt über ihre Daten im Netz behalten, so *Hornung/Hofmann* JZ 2013, 170. Das BVerfG hat bereits in sei-

nem Volkszählungsurteil [BVerfGE 65, 1, 41 f.] darauf hingewiesen, dass die Verfügungsgewalt über die eigenen Daten nicht uneinschränkbar sei. So auch *Nolte* aaO, 237.

5 Zu den Funktionen des Internets vgl. BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, Rz. 87 ff. [Online-Durchsuchung].

6 Die Bedeutung der Verfügungsgewalt über die eigenen Daten für die individuelle Persönlichkeitsentwicklung hat das Bundesverfassungsgericht bereits 1983 herausgearbeitet [BVerfGE 65, 1 ff.] und darüber hinausgehend auch noch den Gemeinwohlbezug betont: »Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Dies würde nicht nur die individuellem Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine allgemeine Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.«

7 Ähnlich *Hornung/Hofmann* aaO, 164; *Jandt/Kieselmann/Wacker* DuD 2013, 237.

8 http://www.kas.de/wf/de/71.7356/ (abgerufen am: 19.08.2013)

9 *Wybitul/Fladung* BB 2012, 512; *Härting* BB 2012, 464; *Hornung/Hofmann* aaO, 169; *Jandt/Kieselmann/Wacker* aaO, 237 f.; *Kalabis/Selzer* DuD 2012, 675.

10 *Jandt/Kieselmann/Wacker* aaO, 236.

11 *Huerkamp* DPolBl 2013, im Erscheinen.

12 ausführlich hierzu *Nolte* aaO, 238; *Bull* NVwZ 2011, 261; *Hornung/Hofmann* aaO, 165.

13 *Hornung/Hofmann* aaO, 165.

14 BVerfGE 65, 1 ff. [Volkszählung].

15 BVerfGE 65, 43. *Grimm* betont in diesem Zusammenhang, dass personenbezogene oder »personenbeziehbare« Daten dem Schutz des keinesfalls als Datenschutzgrundrecht zu bezeichnenden Persönlichkeitsrechts unterfielen, aufgrund des Auffangcharakters des allgemeinen Persönlichkeitsrechts allerdings nur solche Daten, die nicht bereits durch ein spezielleres Grundrecht geschützt würden, vgl. *Grimm* JZ 2013, 585 f.

16 So *Nolte* aaO, 237.

17 *Grimm* aaO, 586, scheint den Fragenkomplex primär als Schutzpflichtproblematik zu sehen.

18 *Grimm* aaO, 587.

19 BGH, Urt. vom 15.12.2009 – Az. VI ZR 227/08.

20 BGH, Urt. vom 14.05.2013 – Az. VI ZR 269/12.

21 Derzeit verhandelt der Europäische Gerichtshof (Rechtssache C-131/12) den Fall eines Spaniers, der Löschungsansprüche gegen den Suchmaschinenbetreiber »Google« geltend macht, weil dieser einen Zeitungsartikel über eine Jahre zurückliegende Pfändung beim Kläger als Suchergebnis präsentiert.

22 Vgl. http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077de.pdf (abgerufen am 19.08.2013).

23 BVerfG, Beschlüsse vom 23. Mai 2013 – 1BvR 2059/12 und vom 23. Januar 2013 – 2 BvR 2392/12.

24 Dass das allgemeine Persönlichkeitsrecht Minderjährige aufgrund seines Schutzanliegens im Falle einer erhöhten Schutzwürdigkeit weitergehend als Erwachsene schützen kann, hat das Bundesverfassungsgericht bereits vor einigen Jahren festgestellt, BVerfGE 101, 385 [Caroline von Monaco].

25 *Beater* JZ 2013, 113.

26 BVerfGE 101, 361 [Caroline von Monaco]; *Beater* JZ 2013, 112.

27 Zu den Unsicherheiten vgl. B)III)3b).

28 Für eine europäische Regelung spricht sich auch die Bundesregierung in ihrer Stellungnahme zum Gesetzentwurf des Bundesrates für ein Gesetz zur Änderung des Telemediengesetzes aus, vgl. http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/bundesregierung-verabschiedet-stellungnahme-aenderung-telemediengesetzes,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, S. 6 f. (abgerufen am 19.08.2013).

29 Selbstverständlich kann ein weitergehender Schutz auch durch Aufgabe des Territorialprinzips erreicht werden, wie es jetzt bei der neuen Datenschutzgrundverordnung geplant ist. Künftig soll die Datenschutzgrundverordnung auch dann Anwendung finden, wenn Unternehmen mit Sitz im außereuropäischen Ausland Daten von in der Union ansässigen Personen verarbeiten, vgl. Artikel 3 Abs. 2 DSGV-E. Eine gewisse Berechtigung scheint die Aussage Härtings zu haben, der Geltungsanspruch des europäischen Datenschutzrechts gehe bedenklich weit. Man solle sich einmal vorstellen, die Regierung der Volksrepublik China erließe Verbotsvorschriften mit ähnlichem Geltungsanspruch und drohte europäischen Online-Anbietern, die die Filterung, Sperrung oder Unterdrückung bestimmter Inhalte verweigerten, mit drakonischen Bußgeldern oder anderen Sanktionen, vgl. *Härting* aaO, 462.

30 Für das Telemediengesetz vgl. Stellungnahme der Bundesregierung, abrufbar unter http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/bundesregierung-verabschiedet-stellungnahme-aenderung-telemedien gesetzes,property=pdf,bereich= bmwi2012,sprache=de,rwb=true.pdf (abgerufen am 19.08.2013).

31 vgl. die Ankündigung des Bundesinnenministeriums vom 1. Dezember 2010, einen Gesetzentwurf zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht im Internet einzubringen, http://www.bmi.bund.de/ShareDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf?__blob= publicationFile (abgerufen am 19.08.2013).

32 http://dipbt.bundestag.de/dip21/btd/17/067/1706765.pdf (abgerufen am 19.08. 2013).

33 Von einem Telemediendienst mit nutzergenerierten Inhalten spricht man dann, wenn der Diensteanbieter dem Nutzer die Möglichkeit bietet, den Telemediendienst durch eigene Inhalte mit personenbezogenen Daten zu erstellen und zu gestalten und diese Inhalte anderen Nutzern zugänglich zu machen, vgl. § 13 a Abs. 1 S. 1 TelemedienG-E.

34 statt aller *Hornung/Hofman*n aaO, 167.

35 *Huerkamp/Wielpütz* JZ 2011, 141.

36 Vgl. http://dipbt.bundestag.de/dip21/brd/2011/0156-11.pdf, Entwurf eines Gesetzes zur Änderung des Telemediengesetzes, S. 8 f. (abgerufen am 19.08.2013).

37 Vgl. http://dipbt.bundestag.de/dip21/brd/2011/0156-11.pdf, Entwurf eines Gesetzes zur Änderung des Telemediengesetzes, S. 9 (abgerufen am 19.08.2013).

38 Vgl. http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077de.pdf (abgerufen am 19.08. 2013).

39 *Härting* aaO, 464.

40 *Härting* aaO, 464.

41 *Hornung/Hofmann* aaO, 167 f. unter Verweis auf *Dix*, in Simitis, BDSG, 7. Auflage 2011, § 35 Rn. 8, Art.-29-Datenschutzgruppe. Stellungnahme Nr. 163, S. 9 f. und Koops SCRIPTed 8:3 (2011), 229, 237 f.

42 *Hornung/Hofmann* aaO, 170.

43 *Jandt/Kieselmann/Wacker* aaO, 240; ein guter Überblick zu den technischen Möglichkeiten findet sich bei *Hornung/Hofmann* aaO, 168 f.

44 *Jandt/Kieselmann/Wacker* aaO, 241.

45 *Nolte* aaO, 237 f., der auf die Möglichkeit von Screenshots und auf die Ungeeignetheit des digitalen Radiergummis für Social Networks hinweist; weitere Kritik bei *Kalabis/Selzer* aaO, 672.

46 *Nolte* aaO, 238 sieht die Gefahr einer Kapitulation der Rechtswissenschaften vor den technischen Herausforderungen.

47 Dies deutet auch *Grimm* aaO, 589 an.; *Kalabis/Selzer* aaO, 675 sprechen sich ebenfalls für strengere Strafen aus, sehen die Sanktionsmöglichkeit jedoch durch die »household exemption« konterkariert.

48 So auch *Nolte* aaO, 240. Eine Anleitung zur sicheren und verantwortungsvollen Nutzung des World Wide Web enthält die Broschüre »Persönlichkeit stärken und schützen, Jugendschutz im Internet – Information für Eltern« von Susanne Philipp, die bei der Arbeitsgemeinschaft für Kinder- und Jugendschutz Landesstelle Nordrhein-Westfalen e.V. angefordert werden kann. ◆