Florian Farke, Jan Rensinghoff, Markus Dürmuth, Tobias Gostomzyk

Recht auf Vergessen

Chancen und Grenzen der technischen Umsetzung

Die Forschung zum „digitalen Vergessen“ widmet sich unter anderem dem Thema, wie und in welchem Umfang personenbezogene Daten vom Internet „vergessen“ werden sollen. Durch Suchdienstleister und Online-Archive werden immer mehr Bereiche des öffentlichen und privaten Lebens im Internet auffindbar. Jan Rensinghoff und Florian Farke untersuchen diese Problematik aus rechtlicher und technischer Perspektive. In ihrem Beitrag zeigen sie Gefahren und Grenzen einer automatisierten Entfernung von Inhalten speziell in Suchmaschinen auf.

Florian Farke

Wissenschaftlicher Mitarbeiter an der Arbeitsgruppe Mobile Security an der Ruhr-Universität Bochum und Doktorand im Forschungskolleg SecHuman. Forschungsschwerpunkte: Usable Security, (Retrospective) Privacy.
E-Mail: florian.farke@rub.de

Jan Rensinghoff

Wissenschaftlicher Mitarbeiter am Lehrstuhl für Medienrecht an der Technischen Universität Dortmund und Doktorand im Forschungskolleg SecHuman. Forschungsschwerpunkte: Datenschutz- und Medienrecht.
E-Mail: jan.rensinghoff@rub.de

Markus Dürmuth

Leiter der Arbeitsgruppe Mobile Security an der Ruhr-Universität Bochum und Principal Investigator im Forschungskolleg SecHuman.

E-Mail: markus.duermuth@rub.de

Tobias Gostomzyk

Professor für Medienrecht an der Technischen Universität Dortmund und Principal Investigator im Forschungskolleg SecHuman.

E-Mail:
tobias.gostomzyk@tu-dortmund.de

1 Einleitung

Nicht das Erinnern, sondern das Vergessen war lange Zeit die Regel im gesellschaftlichen Miteinander. Der technologische Fortschritt hat diese Grundannahme teilweise umgekehrt, da es mittlerweile sehr einfach und kostengünstig möglich ist, eine große Zahl von personenbezogenen Daten über Menschen im Internet zugänglich zu machen.

Vor allem Suchmaschinen können dabei eine Gefahr für Persönlichkeitsrechte darstellen, weil sie sehr effizient im Auffinden von personenbezogenen Informationen sind. Zugleich erfreuen sie sich aufgrund ihrer Funktionalität und leichten Zugänglichkeit seit Jahrzehnten großer Beliebtheit, da sie die Weiten des Internets für den Nutzer strukturieren und auf Abruf bereithalten. Mit der Einführung des sogenannten „Rechts auf Vergessenwerden“ in Art. 17 Abs. 1 der europäischen Datenschutzgrundverordnung (DSGVO)[1] wird Betroffenen nun europaweit ermöglicht, die Entfernung der sie betreffenden personenbezogenen Informationen bei Datenverarbeitern zu beantragen. Wird einer Entfernung stattgegeben, müssen die personenbezogenen Informationen vom Datenverarbeiter umgehend gelöscht werden.

Sowohl die Technik als auch die Rechtswissenschaft werden durch das neue „Recht auf Vergessenwerden“ vor Herausforderungen gestellt, die sie nur in engem Zusammenspiel effektiv lösen können. Diese Problematik wird vor allem bei Suchmaschinen deutlich: Einerseits führt die starke Vernetzung der Suchmaschinen dazu, dass von einer Löschentscheidung im Rahmen des Rechts auf Vergessenwerden naturgemäß gleich mehrere Parteien betroffen sind. Zusätzlich zum von der personenbezogenen Information Betroffenen und dem Datenverarbeiter hat aber auch die Allgemeinheit oftmals ein legitimes Informationsinteresse daran, dass personenbezogene Daten im Internet verbleiben. Es muss somit in einer Vielzahl von Fällen kein bi- sondern ein multipolarer Ausgleich zwischen verschiedenen Interessengruppen erfolgen. Andererseits macht diese rechtliche Komponente es sehr schwer, Abwägungsergebnisse maschinell zu strukturieren – oder gar zu automatisieren. Der folgende Beitrag soll da-

1 Siehe Kubis, M., Gateway, DuD 9/2017, 583.

her die besondere Problematik des Rechts auf Vergessenwerden mit Blick auf aktuelle Suchmaschinen sowohl rechtlich als auch technisch skizzieren.

2 Hintergrund – Digitales Vergessen

Im Vergleich zu digitalen Speichermedien wie Festplatten oder Flashspeichern erscheint das menschliche Gedächtnis in vielerlei Hinsicht eingeschränkt. Erinnerungen sind oft vage, fehlerhaft oder sogar nicht mehr zu erreichen. Zwar ist der willkürliche Verlust von Information auch bei digitalen Speichermedien ein Problem. Durch die Möglichkeit Information präzise zu speichern, abzurufen und zu kopieren sind diese Einschränkungen im Vergleich mit dem menschlichen Gedächtnis aber zu vernachlässigen. Allerdings stellt die Vorstellung des menschlichen Gedächtnisses als Informationsspeicher, ähnlich einer Computerfestplatte, eine zu grobe Vereinfachung dar, da hier ein passives „Speichermodel" angenommen wird, wohingegen Erinnern und Vergessen aktive Prozesse sind [1, 2].

Da Menschen inhärent kein perfektes Gedächtnis besitzen und Vergessen für Individuen und Gesellschaften von wichtiger Bedeutung sind – z. B. bei der Rehabilitation von Straftätern oder zur Verarbeitung von Traumata – ist *digitales Vergessen* ein Sammelbegriff für Konzepte, Ideen und Ansätze, um Informationstechnologie um eine Art „Vergessen" von Information zu erweitern. Hierbei wird jedoch häufig zu sehr vereinfacht und der Begriff des digitalen Vergessens mit dem Löschen von Daten gleichgesetzt. Aus technischer Sicht sind jedoch auch andere Ansätze außer zu löschen möglich, um „Vergessen" zu realisieren [2].

Kryptographie-basierte Ansätze

Die Grundidee bei kryptographischen Ansätzen zum digitalen Vergessen ist, die Daten vor der Veröffentlichung zu verschlüsseln und in dieser Form zusammen mit dem Schlüssel zu veröffentlichen. Der Schlüssel wird dabei beispielsweise auf einem speziellen Server geladen, der den Schlüssel nach einer Zeit „vergisst". Auch dezentrale Lösungen für die Schlüsselspeicherung und Löschung sind möglich. Nachdem der Schlüssel gelöscht wurde, können die Daten nicht mehr gelesen werden und gelten damit als „vergessen". Allerdings funktionieren diese Ansätze nur, solange keine unverschlüsselten Kopien von den Daten existieren. Solange diese Daten jedoch noch lesbar sind, kann jedoch jederzeit auch von Dritten eine Kopie gespeichert werden.

Ansätze zur Täuschung und Verschleierung

Anstatt zu versuchen, einmal im Internet veröffentlichte Daten zu entfernen oder unleserlich zu machen, kann versucht werden, die Daten zu verstecken oder unglaubwürdig zu machen. Dies kann z. B. über die gezielte Veröffentlichung von Falschinformationen geschehen, welche dann die korrekten Daten sozusagen „überdecken". Auch kann durch Manipulation der Online-Identität Unsicherheit beim Betrachter der Daten erzeugt werden, so dass dieser die Daten nicht mehr zweifelsfrei einer Person zuordnen kann. Besonders Namen sind häufig nicht eindeutig, daher können mehrere Personen unter gleichem Namen gefunden werden. Allerdings können solche Ansätze unter Umständen ethisch fragwürdig sein – besonders im Hinblick auf Diffamierung oder Fake-News.

Filterung durch Suchmaschinen

Eine weitere Möglichkeit um ein digitales Vergessen zu realisieren besteht darin, Suchmaschinenanbieter in die Pflicht zu nehmen und dadurch Daten schwerer auffindbar zu machen. Da zum Finden von Daten im Internet meist Suchmaschinen eingesetzt werden, kann hier ein „Vergessen" durch das Verbergen bestimmter Suchergebnisse erreicht werden. Technisch sind diese Arten von Filter für Suchmaschinen keine große Herausforderung, da das Filtern von Suchergebnissen ohnehin die Hauptaufgabe von Suchmaschinen ist. Allerdings ist die Entscheidung, ob diesen „Löschanfragen" stattgegeben wird oder nicht, die eigentliche Herausforderung.

3 Das Recht auf ein „digitales Vergessen" gegenüber Suchmaschinen

Wann solchen Anfragen auf Entfernung von personenbezogenen Daten stattgegeben werden soll, regelt nunmehr die Datenschutzgrundverordnung. Die Pflicht, wieder zu vergessen, ist durch die DSGVO nun auch unionsrechtlich verankert. Damit reagierte der europäische Gesetzgeber darauf, dass sich der Umgang mit personenbezogenen Daten durch die zunehmende Digitalisierung stark verändert hat [3]. Informationen können mittlerweile ohne größere Kosten nahezu unbegrenzt und ohne zeitliches Limit elektronisch gespeichert und bereitgehalten werden. Technischer Fortschritt ermöglicht es, aus den Datenmengen neue Zusammenhänge zu schließen [4]. Zudem erleichtern Suchmaschinen die Auffindbarkeit von Informationen in erheblichem Maße. Suchtreffer werden per Algorithmen nach Relevanz geordnet und können über eine simple Namenssuche binnen Sekunden aufgefunden werden.

Der Kodifikation des „Rechts auf Vergessenwerden" ging das sogenannte „Google Spain"-Urteil des EuGHs aus dem Jahre 2014 voraus.[2] Hintergrund der Entscheidung war die Klage eines spanischen Bürgers, der bei Eingabe seines Namens in die Suchmaschine „Google" auf erster Position eine 16 Jahre alte, amtliche Bekanntgabe über die Zwangsversteigerung seines Hauses fand. Nach einer Beschwerde des Bürgers bei der spanischen Datenschutzbehörde ordnete diese gegenüber dem Suchmaschinenbetreiber an, die Links zu entfernen. Dagegen setzte sich Google mit einer Klage zur Wehr, die durch ein Vorabentscheidungsverfahren schlussendlich dem Europäischen Gerichtshof vorgelegt wurde. Die Luxemburger Richter entschieden, dass datenschutzrechtlich Betroffene unter Umständen einen Anspruch auf Entfernung ihrer personenbezogenen Daten gegenüber Suchmaschinenbetreibern haben können. Dabei ist der Begriff des „Vergessens" terminologisch nicht korrekt, da natürlich niemand gezwungen werden kann, sich an Inhalte nicht mehr zu erinnern. Die Idee ist, dass mit dem Anspruch auf Löschung eine bestimmte Information im Ergebnis von den Menschen vergessen wird, weil die Inhalte nicht mehr zugänglich sind. Richtigerweise handelt es sich beim Recht auf Vergessenwerden im Hinblick auf Suchmaschinen um ein „Recht auf nicht mehr Gefundenwer-

2 Siehe DuD 8/2014, 559 ff.

den", weil die eigentliche Quelle von der Suchmaschine gar nicht gelöscht werden kann. Faktisch kann sich dieses Recht aber genauso stark auswirken, weil mit einer Entfernung des Suchtreffers die Information praktisch nicht mehr aufgefunden werden kann. Sie fällt somit de facto aus dem Kommunikationsprozess des Internet vollständig heraus.

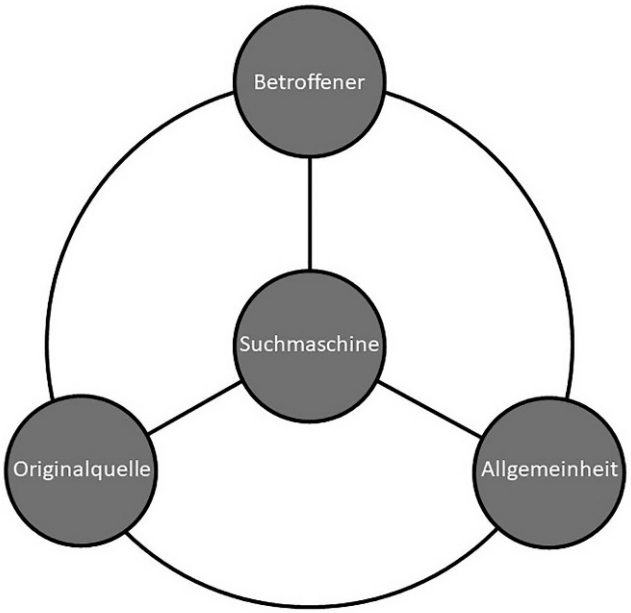
4 Probleme bei der Umsetzung des Rechts auf Vergessenwerden im Hinblick auf Suchmaschinen

Eine grundsätzliche Herausforderung bei der Umsetzung des Rechts auf Vergessenwerden ist, dass Art. 17 Abs. 1 DSGVO sehr abwägungsoffen formuliert ist. Die Kriterien, die für oder gegen eine Löschung von personenbezogenen Daten sprechen, sind nicht abschließend aufgeführt. Entscheidend für die Durchsetzung des Anspruches ist, ob der Betroffene den grundsätzlichen Vorrang seines Persönlichkeitsrechts geltend machen kann oder ob vorrangige, berechtigte Gründe für den Verbleib dieser Daten sprechen. Beispielsweise können etwa gesetzliche Aufbewahrungsfristen die Entfernung eines Inhaltes gesetzlich ausschließen. Der EuGH hat sich im „Google-Spain"-Urteil von 2014 nur sehr grob zu den vorzunehmenden Gewichtungen der rechtlichen Belange bei Löschentscheidungen geäußert. Maßgeblich sei zwar immer die Betrachtung des konkreten Einzelfalls. Im Grundsatz würden aber die Interessen der Betroffenen überwiegen [5]. Art. 17 DSGVO dagegen fordert grundsätzlich eine generelle Abwägung zwischen dem Löschungsinteresse der Betroffenen und den Interessen weiterer Beteiligter. Auch in einer aktuellen Vorlagefrage zum Recht auf Vergessenwerden betonte der Generalstaatsanwalt, dass das Grundrecht Achtung der Privatsphäre immer gegen das berechtigte Interesse der Öffentlichkeit am Zugang zu den gesuchten Informationen abgewogen werden müsse [6].

Suchmaschinen sind vom Recht auf Vergessenwerden in besonderem Maße betroffen. Sie indexieren unzählige Links und helfen somit, aus den Weiten des Internet die für den Nutzer relevanten Informationen herauszufiltern. Damit fungieren sie in der heutigen Zeit als eine Art „Flaschenhals" des Internet, die von vielen Millionen Menschen täglich genutzt werden. Der digitale Raum ist stark vernetzt und betrifft neben Persönlichkeitsrechten auch Kommunikationsgrundrechte anderer Teilnehmer. In der Regel sind nämlich durch die Netzwerkstruktur des Internet gleich mehrere Interessengruppen von der Löschung bestimmter, personenbezogener Informationen berührt. Dabei geht es nicht nur um den Betroffenen und um denjenigen, der die Informationen im Netz bereitgestellt hat. Suchmaschinenbetreiber verweisen oft auf personenbezogene Daten, an deren Erhalt die Öffentlichkeit regelmäßig ein legitimes Informationsinteresse hat. Diese Rolle eines „Gatekeepers" von Suchmaschinen im Internet führt dazu, dass die Entfernung eines Suchergebnisses die Allgemeinheit in diesem Informationsinteresse stark beeinträchtigen kann. Auch die Originalquelle kann stark von einer Entfernung aus Suchmaschinen betroffen sein, wenn mit der Entfernung die Besucherzahlen drastisch sinken. Diese Interessengruppen bedingen sich alle wechselseitig und gestalten eine Abwägung daher oft sehr schwierig.

Des Weiteren sehen sich datenschutzrechtlich Verantwortliche nun mit der Aufgabe konfrontiert, selbst entscheiden zu müssen, wann ein Anspruch auf Entfernung rechtmäßiger Weise besteht und wann nicht. Daher ist die Umsetzung des Recht auf Vergessenwerden mitunter der Kritik ausgesetzt, dass die Rechtsdurchsetzung durch diese Regelungen faktisch privatisiert wird, da die Entscheidung in erster Instanz nicht mehr den Gerichten obliegt, sondern den Suchmaschinen selbst [7]. Diese Entscheidungen über die Entfernung von Inhalten können zudem – je nach Größe des Verantwortlichen – in sehr großer Zahl von den Unternehmen gefordert werden. Aus Googles Transparenzbericht zum „Recht auf Vergessenwerden" geht hervor, dass sich das Unternehmen zwischen dem 01.01.2015 und dem 01.01.2019 den Löschanfragen zu über 1,9 Millionen URLs ausgesetzt sah, die es zu bearbeiten galt [8].

Abbildung 1 | Interessengruppen, die bei der Abwägungsentscheidung von Suchmaschinen miteinbezogen werden müssen.



5 Technische Aspekte des Rechts auf Vergessenwerden

Suchmaschinenanbieter betreiben unter Umständen einen nicht unerheblichen Aufwand zur Überprüfung von Löschanfragen. So wird bei Google jede einzelne Anfrage von mindestens einem menschlichen Gutachter geprüft und entschieden [3]. Dabei soll keinerlei Automatisierung des Entscheidungsprozesses stattfinden.

Ein solches Vorgehen ist für große Internetunternehmen mit entsprechenden Ressourcen möglich. Für mittelständische Unternehmen oder Startups ist eine vollständig manuelle Prüfung höchstwahrscheinlich keine Option – besonders im Hinblick darauf, dass auch kleinere Unternehmen Dienste mit einer hohen Nutzeranzahl anbieten können, welche aber wiederum auch potenziell eine hohe Anzahl an Löschanfragen nach sich ziehen können.

Aus diesem Grund könnte eine Automatisierung der Löschung für viele Unternehmen eine praktikablere Lösung darstellen. Al-

lerdings zeigt das Beispiel Google, dass eine vollständige oder selbst nur eine Teilautomatisierung nicht oder nur schwer zu realisieren ist. Im Folgenden sollen deswegen der Prozess zur Bearbeitung von Löschanfragen, die Möglichkeiten zur Automatisierung und die damit verbundenen Probleme am Beispiel von Suchmaschinen diskutiert werden. Zwar ist das Beispiel einer Suchmaschine recht speziell, allerdings ist die Beschreibung allgemein gehalten und mit entsprechenden Anpassungen auch auf andere Internetdienstleister übertragbar.

Bei der Modellierung des Prozesses können drei Phasen unterschieden werden. In der ersten Phase wird eine Anfrage zur Löschung von Daten gestellt, diese Anfrage wird dann in der zweiten Phase geprüft und auf Grundlage dieser Prüfung wird in der dritten Phase eine Entscheidung getroffen.

Phase 1 – Anfrage zur Löschung

In der ersten Phase wird eine Anfrage zur Löschung von Daten mit Personenbezug gestellt (z. B. ein Suchergebnis bei einer Suchmaschine). Entsprechend muss vom Antragsteller angegeben werden, um welche Daten es sich handelt und auf wen sich diese beziehen. Bereits diese Phase stellt einen automatisierten Ansatz vor große Herausforderungen. So muss festgestellt werden, ob die betroffene Person überhaupt ein Recht auf Löschung hat (also z. B. ob die Person Bürger der EU ist) und ob der/die Antragssteller/in im Sinne dieser Person handelt (falls es sich nicht um dieselbe Person handelt).

So verlangt Google bspw. als Identitätsnachweis die Kopie eines Dokuments, welches die Identität der Person bestätigt (es muss sich nicht um ein amtlich ausgestelltes Dokument handeln), zu der Suchergebnisse gelöscht werden sollen. Allerdings ist eine automatische Prüfung solcher Dokumentenkopien schwer umzusetzen, weswegen die Legitimationsprüfung eventuell auf andere Art und Weise umgesetzt werden sollte, z. B. durch Verwendung von persönlichen Identifikationsverfahren wie *Postident* oder über elektronische Ausweisdokumente wie den elektronischen Personalausweis. Allerdings existiert EU-weit kein einheitliches Verfahren, sodass im Zweifel für jeden Mitgliedsstaat ein gesondertes Prozedere angeboten werden müsste. Weiterhin ist problematisch, wie Dritte legitimerweise einen Antrag zur Löschung stellen können, da nicht immer der Betroffene selbst einen Antrag stellen kann (bspw. bei verstorbenen Personen).

Etwas einfacher ist die Angabe der Daten, die gelöscht werden sollen. Beim Beispiel der Suchmaschinen handelt es sich um ein oder mehrere Suchergebnisse. Diese können unter Angabe der entsprechenden URL eindeutig bezeichnet werden. Bei anderen Diensten sind unter Umständen andere Angaben zur Identifizierung der zu löschenden Daten notwendig, wie z. B. eine Identifikationsnummer eines Nutzerkontos oder Ähnliches. In jedem Fall ist dieses Problem technisch lösbar.

Phase 2 – Prüfung der Anfrage

Nach der Verarbeitung der Angaben aus der ersten Phase findet die eigentliche Überprüfung des Antrags statt. Dabei muss geprüft werden, ob bei den zur Löschung angegeben Daten ein Personenbezug vorliegt. Dies mag von Dienst zu Dienst einfacher oder schwieriger sein. Bei dem Beispiel der Suchmaschine, muss geprüft werden, ob es eine Verbindung zwischen der Person und der beanstandeten URL gibt. Verweist die URL z. B. auf eine Website, könnte geprüft werden, ob der Name der Person auf dieser Webseite vorkommt. Die Prüfung ist für eine Suchmaschine prinzipiell einfach durchzuführen, da lediglich abgeglichen werden muss, ob die angegeben URL in den Suchergebnissen zum gegebenen Namen enthalten ist. Allerdings handelt sich hierbei nur um eine einfache Plausibilitätsprüfung; die Mehrdeutigkeit von Namen wird nicht beachtet. Grundsätzlich treten hier aber die gleichen Schwierigkeiten wie auch bei der Identitätsprüfung (5.1) auf.

Noch schwieriger ist die Bewertung, ob ein öffentliches Interesse an den zu löschenden Daten vorliegt oder nicht. Dazu muss zum einen die Bekanntheit der Person bewertet werden und zum anderen um welche Art von Daten es sich handelt bzw. in welchem Kontext diese auftauchen. Eine Metrik für die Bekanntheit einer Person könnte die Anzahl der Suchtreffer bei einer Suchmaschine sein. Hierbei muss aber immer noch festgelegt werden, ab wann jemand als „bekannt" gilt. So kann eine Person in bestimmten Bevölkerungsgruppen sehr bekannt, für andere Bevölkerungsteile aber nahezu unbekannt sein. Ab wann jemand als Person öffentlichen Interesses gilt und wann nicht, ist also nicht direkt ersichtlich. Auch haben Personen von öffentlichem Interesse immer noch ein Recht auf Privatsphäre, es muss also zwischen privaten und öffentlichkeitsrelevanten Daten unterschieden werden. Beispielsweise sind die privaten Urlaubsbilder des Vorstandsvorsitzenden eines Großkonzerns nicht relevant für die Öffentlichkeit, wohingegen berufliche Verfehlungen relevant sind.

Zusätzlich muss die Quelle der Daten geprüft werden. Diese kann ebenfalls einen großen Einfluss auf die Entscheidung zur Löschung haben. Dabei wird es für eine Suchmaschine schon einen Unterschied machen ob es sich bei dem Suchergebnis um einen Artikel auf der Webpräsenz einer renommierte Zeitung handelt oder um den privaten Blog eines „Hobbyjournalisten". Nichtsdestotrotz ist diese Bewertung nicht trivial und kann von Fall zu Fall variieren. Denn auch als vertrauenswürdig geltende Quellen können unbewusste oder bewusste Falschmeldungen herausbringen und somit im Einzelfall eine Löschung aus den Suchergebnissen rechtfertigen.

Phase 3 – Entscheidung der Anfrage

Die abschließende Entscheidung für oder gegen die Datenlöschung kann mittels regelbasiertem oder fallbasiertem Schließen umgesetzt werden. Beim regelbasierten Schließen werden im Vorfeld von Menschen Regeln definiert (üblicherweise in der Form, *Wenn-Dann-Sonst*), mit deren Hilfe eine Entscheidung getroffen werden kann [10]. Die Verwendung von einfachen Wenn-Dann-Regeln ist möglich, wenn davon ausgegangen wird, dass sämtliche unscharfe Abwägungen in Phase 2 passieren und in Phase 3 als Fakten für das regelbasierte System angenommen werden. Allerdings müssen unter Umständen die Regeln angepasst werden, wenn Rahmenbedingungen (z. B. gesetzliche Vorgaben) geändert werden oder nicht bedachte Sonderfälle auftreten.

Beim fallbasierten Schließen werden zuvor entschiedene ähnliche Fälle zur Findung einer Entscheidung herangezogen. Dabei können sowohl Ansätze zum maschinellen Lernen als auch formale Ansätze verwendet werden, wobei die ersten häufig eher einem Blackbox-System entsprechen (es ist nicht transparent, wie bestimmte Entscheidungen zustande kommen) und letztere einen größeren Aufwand bei der Erstellung der Datenbasis er-

fordern, da die bereits entschiedenen Fälle manuell formalisiert werden müssen.

6 Fazit und Ausblick

Es sind mithin verschiedene Ansätze denkbar, um die Umsetzung des Rechts auf Vergessenwerden technisch zu unterstützen. Die Anfrage zur Löschung ist bei einigen Suchdienstleistern bereits heute teilweise automatisiert. Dies geschieht regelmäßig mithilfe von Online-Formularen, die Betroffene ausfüllen und elektronisch an den verantwortlichen Datenverarbeiter versenden können. Die Prüfung sowie die Bescheidung der Anfrage sind jedoch noch nicht vollständig automatisiert. Es ist auch fraglich, inwiefern eine abschließende technische Umsetzung in den nächsten Jahren realistisch ist. Denn es gilt zu bedenken, dass rechtlich immer eine Abwägung im konkreten Einzelfall gefordert wird, die die verschiedenen Rechte der Beteiligten möglichst schonend miteinander in Ausgleich bringt. Diese Abwägung ist nicht immer im Vorfeld technisch zu antizipieren.

Wie der Beitrag aufzeigt hat, könnten automatisierte Ansätze in naher Zukunft allerdings auch bei der Entscheidungsfindung (zumindest) eine Hilfestellung bieten. Mit steigender Zahl der Anfragen würde eine solche technische Hilfestellung zudem auch zunehmend an Relevanz gewinnen. Aktuell wird automatisierter Entscheidungsfindung zunehmend der Weg bereitet. Eine Abnahme der Anfragen zum Recht auf Vergessenwerden ist aktuell auch nicht ersichtlich. Ansatzpunkte für eine technische Umsetzung gibt es – wie der Beitrag gezeigt hat – bereits heute zur Genüge.

Literatur

[1] Bannon, L. (2006). *Forgetting as a Feature, Not a Bug: The Duality of Memory and Implications for Ubiquitous Computing*. Hardware/Software Codesign and System Synthesis (CODES+ISSS'06)

[2] Bishop, M., et al. (2013). *Forgive and Forget: Return to Obscurity*. New Security Paradigms Workshop (NSPW'13).

[3] Europäische Kommission, 1. Entwurf der DSGVO v. 25.01.2012, Drcks. KOM(2012) 11, S. 1.

[4] Grimm, R. (2012). *Spuren im Netz,* DuD 2012, S. 88.

[5] EuGH, Urt. v. 13.05.14, Rs. C-131/12, Rn. 81.

[6] EuGH, Pressemitteilung vom 10.01.19 *zu den Schlussanträgen des Generalanwalts in der Rechtssache C-507/17,* Nr.2/19, S. 1.

[7] Masing, J. (2014). *RiBVerfG Masing: Vorläufige Einschätzung der „Google-Entscheidung" des EuGH*. Verfassungsblog, online abrufbar unter: https://verfassungsblog.de/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/.

[8] Google Transparency Report 2019, *Search removals under European privacy law,* online abrufbar unter: https://transparencyreport.google.com/eu-privacy/overview

[9] Bertram, T., et al. (2018). *Three years of the Right to be Forgotten.* Under Submission.

[10] Tiwari, A., et al. (2018). *A Formal Logic Framework for the Automation of the Right to be Forgotten.* Security and Privacy in Communication Networks (SecureComm'18).