Ansatzpunkte zum Schutz personenbezogener Daten bei Nutzung von Social Media-Diensten am Arbeitsplatz

Jürgen Karla, Björn Gronenschild

Lehrstuhl für Wirtschaftsinformatik und Operations Research
RWTH Aachen University
Templergraben 64
52056 Aachen
karla@winfor.rwth-aachen.de
bjoern.gronenschild@rwth-aachen.de

Abstract: Der vorliegende Beitrag greift verschiedene Ansätze zur Verbesserung des Datenschutzes in Social Media-Diensten am Arbeitsplatz auf. Nach einer kurzen Darstellung des typischen Umgangs mit persönlichen Daten in Social Media-Diensten erfolgt eine Betrachtung der digitalen Enthaltsamkeit, der perfekten Kontextualisierung sowie des Ansatzes der Eigentumsrechte für personenbezogene Informationen. Anschließend wird vertiefend der Ansatz eines Verfallsdatums für personenbezogene Informationen betrachtet. Dabei werden die Grundidee, eine mögliche Umsetzung, die ursprüngliche Intention sowie Vorteile und Kritikpunkte für das Verfallsdatum diskutiert. Abschließend werden Schlussfolgerungen gezogen sowie ein Ausblick auf zukünftige Forschungsfelder gegeben.

1 Datenschutz in Social Media-Diensten am Arbeitsplatz

Der Schutz der Privatsphäre wird im Rahmen des Einsatzes von Social Media-Technologien auch am Arbeitsplatz zunehmend einer grundsätzlichen Gefährdung ausgesetzt. Herausforderungen erwachsen dabei einerseits aus der Einbindung öffentlicher Social Media-Dienste in die internen Arbeitsabläufe und andererseits aus der zunehmenden Implementierung ergänzender unternehmensinterner Plattformen. Die für den Nutzer schnell offensichtlichen Annehmlichkeiten stehen dabei versteckten Herausforderungen hinsichtlich der Sichtbarkeit und Pflege der persönlichen Daten in diesen Diensten gegenüber. Die unbegrenzte Speicherdauer jeglicher bereitgestellter Information kann dabei zügig als eine zentrale Ursache ausgemacht werden. Ergänzend ist die manuelle Pflege der bereitgestellten Daten als Hürde zu nennen. [SPC09, 11ff.; Ma08, 10]. Missbrauch und falsche Interpretation der bereitgestellten Daten zählen zu den üblichlicherweise genannten resultierenden Gefahren. [Ka10a, 105]

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

Staatliche Regulierung kann im Internet keinen ausreichenden Schutz der Privatsphäre gewährleisten. Die Hauptgründe dafür sind die territorial beschränkte Gültigkeit und die international unterschiedliche Ausprägung staatlicher Regelungen. Weiterhin kann staatliche Regulierung nur schwer mit der sich schnell verändernden Welt des Internets Schritt halten und hat zu geringe Kapazitäten, um die Befolgung bestehender Regelungen im Internet wirkungsvoll zu überwachen. Die Einflussnahme unternehmensinterner Kontrollgremien bietet jedoch zumindest am Arbeitsplatz die Möglichkeit, Einfluss auf das bestehende Risiko für die Privatsphäre zu nehmen.

Bei der Untersuchung verschiedener Alternativen zur Verbesserung des Schutzes der Privatsphäre im Internet werden verschiedene Ansätze wiederholt diskutiert: Als richtungweisender Ansatz kann die Idee der Einführung von Eigentumsrechten an personenbezogenen Daten bewertet werden. Daneben verfolgt der Ansatz der Einführung eines Verfallsdatums für Informationen die Idee, die Kontrolle über persönliche Daten ebenfalls stärker in die Hände der Nutzer legen.

Ziel dieses Beitrags ist es, die Problematik des Schutzes der Privatsphäre der Nutzer in Social Media-Diensten im unternehmensinternen Einsatz hinsichtlich ihrer Ursachen und Auswirkungen darzustellen und Lösungsansätze bzgl. ihrer Eignung daraufhin zu analysieren, den Schutz der Privatsphäre verbessern zu können. Hierbei wird eine tiefer greifende Analyse der Idee durchgeführt, ein Verfallsdatum für personenbezogene Information einzuführen, welches Social Media-Diensten das Vergessen „beibringen“ will, indem es den natürlichen Vergessensprozess des menschlichen Gedächtnisses nachbildet, um dem Nutzer den Schutz seiner personenbezogenen Informationen zu erleichtern [Ma07, 17 ff.].

2 Digitales Zeitalter - Das Ende des Vergessens

Das digitale Universum umfasst heute mehr als 1,8 Billionen Gigabyte und soll in den nächsten Jahren exponentiell weiter wachsen. [Fu09] Die Grundidee des „Ubiquitous Computing“ trägt dazu bei, eine Welt zu erschaffen, in der alles miteinander vernetzt und in immer größerem Umfang das Speichern von Informationen in jedem Lebensbereich möglich ist. [La04, 8 f.; Ad03, 3] Neben vielen positiven Annehmlichkeiten [Bo03, 3 ff.] entwickelt sich Ubiquitous Computing daher auch zu einer immer größer werdenden Gefahr für die informationelle Selbstbestimmung. Gerade in Social Media-Diensten ist häufig die Preisgabe persönlicher Information festzustellen. [SPC09, 14; Ze09, 31; Re09, 28; Pö07, 53]

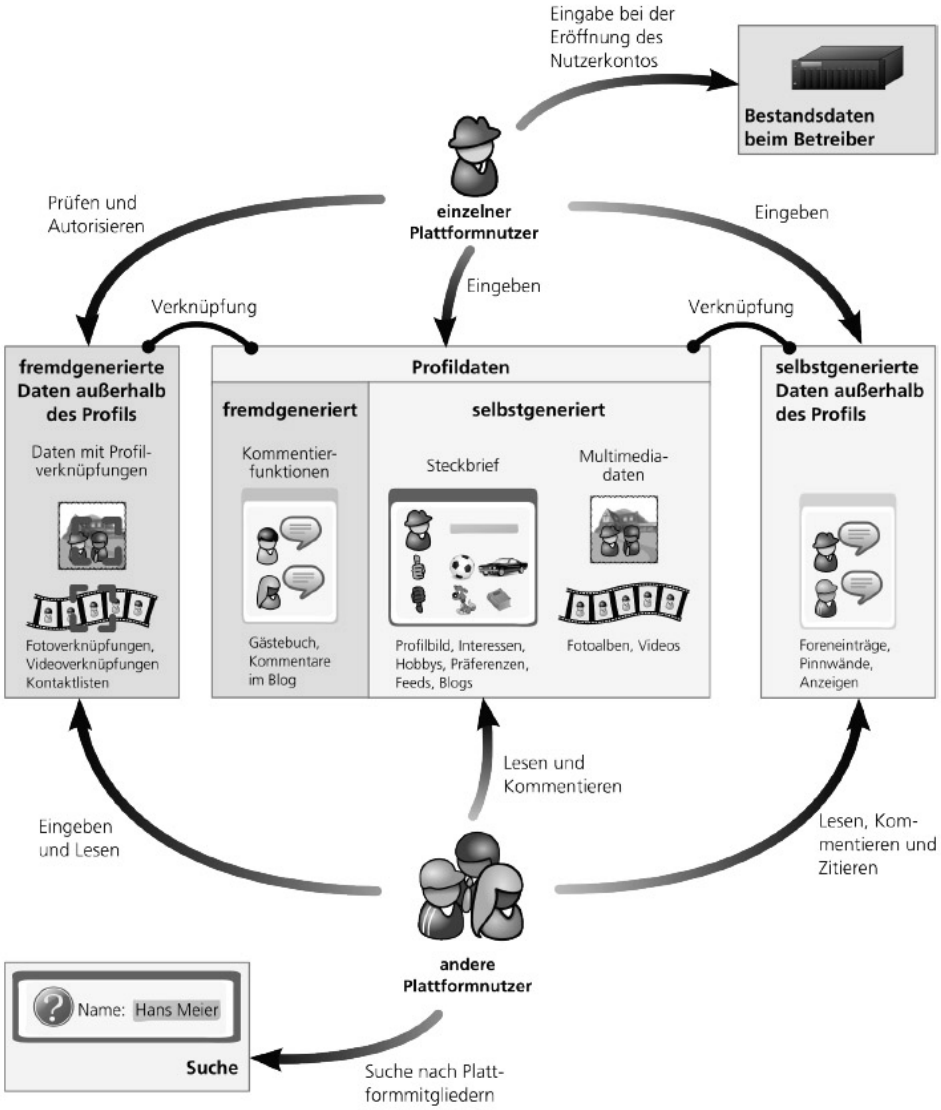

Abbildung1: Datenarten und mit ihnen verbundene Nutzeraktionen [HKP08, 19]

2.1 Die gespeicherten Daten in Social Media-Diensten

Die in Social Media-Diensten zu einem Nutzer gespeicherten Daten lassen sich hinsichtlich Quelle, Ort und Zweck kategorisieren. Hinsichtlich der Quelle lassen sich selbstgenerierte Daten und fremdgenerierte Daten unterscheiden. Fremdgenerierte Daten sind Informationen, die ein Dritter über einen Nutzer in Social Media-Diensten preisgibt.

Hierzu zählen, neben eigenständigen Beiträgen, auch Kommentierungen oder Verlinkungen zu möglichen Inhalten wie Fotos, Videos oder Blogeinträgen dieses Nutzers. [HKP08, 17] Selbst generierte Daten sind hingegen Daten, die ein Nutzer selbst in Social Media-Diensten veröffentlicht. Einen detaillierten Überblick über die verschiedenen Datenarten und deren Beziehungen untereinander gibt Abbildung 1.

2.2 Motive der Privatsphärenpreisgabe in Social Media-Diensten

Im Wesentlichen lassen sich die Motive zur Preisgabe persönlicher Informationen in Social Media-Diensten auf einige Hauptaspekte zurückführen. Social Media-Dienste zeichnen sich durch einfache Bedienbarkeit aus und erreichen durch User Generated Content eine starke Einbindung des Nutzers. In Verbindung mit der Neuartigkeit und neuen Möglichkeiten der Kommunikation ist die Nutzung der Social Media-Dienste für die Nutzer sehr attraktiv. Im privaten Umfeld wird die Befriedigung einer Vielzahl menschlicher Bedürfnisse erleichtert, wie z.B. das Streben nach Gemeinschaft und Austausch, den Hang zur Selbstoffenbarung und den Wunsch nach der Flucht vor dem Alltag. [HKW08, 9ff.] Sowohl interne Anreizsysteme als auch bestehender Gruppendruck verstärken dabei den Willen zur Preisgabe persönlicher Information. [SPC09, 11; Ze09, 29 und 56ff; HKW08, 11] Leichtsinn und Unbekümmertheit im Umgang mit diesem neuartigen Medium in Verbindung mit dem Fehlen unmittelbarer Konsequenzen fördern die Preisgabe persönlicher Informationen dabei noch zusätzlich. [Re08, 29; SPC09, 14] Zwar nicht in dieser Umfänglichkeit gegeben, sind Social Media-Dienste dennoch auch am Arbeitsplatz mittlerweile etabliert und für gezielt ausgewählte Einsatzbereiche im Einsatz. So finden sich Social Media-Dienste beispielsweise auch im Umfeld des Personalmanagements im Einsatz. [Mü07a; Mü02] Demzufolge sind auch einige der genannten Aspekte auf die Nutzung von Social Media-Diensten am Arbeitsplatz zu übertragen.

3 Alternative Möglichkeiten zum Schutz personenbezogener Daten in Social Media-Diensten

Im folgenden werden einige Ansätze zum Schutz der Privatsphäre in Social Media vorgestellt und bezüglich ihrer Eignung zur Verbesserung der bestehenden Situation diskutiert. Ein weiterer Ansatz wird im folgenden Kapitel 4 vertieft betrachtet.

ISBN 978-3-88579-286-4

3.1 Digitale Enthaltsamkeit

Eine Maßnahme zum Schutz persönlicher Information in Social Media-Diensten ist der Vorschlag zu digitaler Enthaltsamkeit. Kerngedanke dieses Vorschlags ist, auf die Benutzung dieser Dienste zu einem großen Teil oder sogar ganz zu verzichten, um so zu verhindern, dass große Mengen personenbezogener Informationen überhaupt veröffentlicht werden. [Li08; Pö07, 55] Zur Beurteilung dieses Ansatzes ist jedoch festzuhalten, dass es für den Großteil der betrachteten Nutzer in der heutigen Zeit nicht mehr einfach möglich ist, diesen Verzicht auszuüben. Das Internet hat sich schneller als jedes Medium zuvor in der Gesellschaft verbreitet. Es ist heute in jeden Lebensbereich integriert und für viele Menschen unverzichtbar geworden. Weiterhin hat sich das Internet zu einer unverzichtbaren Informationsquelle entwickelt. Es ist komfortabeler als andere Medien zuvor und ermöglicht die leichte Beschaffung nahezu beliebiger Informationen. [KÖG08, 5 ff.] Gerade auch im Unternehmenskontext mit einer ggf. verbindlich vorgeschriebenen Nutzung ausgewählter Social Media-Dienste ist dieser Ansatz demnach nicht praktikabel.

Der Vorschlag zur digitalen Enthaltsamkeit zum Schutz persönlicher Information lässt sich vor den beschriebenen Hintergründen nur bedingt durchsetzen. In Anbetracht der aufgeführten Gründe ist in den meisten Fällen daher allerhöchstens eine Reduktion der Verwendung von Social Media-Diensten realisierbar. Hierdurch kann allerdings nur eine geringe Verbesserung des Schutzes persönlicher Informationen erreicht werden, da auch bei der eingeschränkten Nutzung noch eine große Menge persönlicher Informationen preisgegeben wird [Os07].

3.2 Perfekte Kontextualisierung

Der Ansatz der perfekten Kontextualisierung argumentiert in die entgegengesetzte Richtung. Dabei wird davon ausgegangen, dass der Schutz persönlicher Informationen in Social Media-Diensten dadurch verbessert werden kann, dass in noch größerem Umfang als bisher persönliche Information gespeichert wird. Die dadurch angestrebte perfekte Kontextualisierung aller verfügbaren Informationen soll dazu beitragen, Fehlentscheidungen und Missverständnisse, die aufgrund nur verfügbarer Informationsfragmente entstehen, zu vermeiden. Sind alle ergänzenden Umstände zu einer Information, wie z.B. bei einem Foto zusätzlich Entstehungsort, Anlass und Datum des Fotos, verfügbar, ist es auch im Nachhinein noch möglich, eine angemessene Bewertung dieser Information vorzunehmen und Missverständnisse zu vermeiden. Allerdings ist es somit realisierbar, eine gläserne Gesellschaft einzuführen, in welcher perfekte Überwachung möglich ist. [Ma08, 13 f.]

ISBN 978-3-88579-286-4

Eine gläserne Gesellschaft birgt jedoch naturgemäß Risiken. Menschen ändern beim Glauben daran, permanent überwacht zu werden, ihr Verhalten. Wer überwacht wird, kann verstärkt für sein Verhalten kritisiert und zur Rechenschaft gezogen werden. Dieser permanente Überwachungsdruck führt zu einer Einschränkung in der Entfaltung der Persönlichkeit. Die daraus resultierende übertriebene Selbstkontrolle führt zur Einschränkung der persönlichen Freiheit und zunehmender Fremdbestimmung. [Ba08]. Darüber hinaus kann es zu einer Störung des gesellschaftlichen Zusammenlebens kommen, da Privatsphäre und Individualität als wichtige Voraussetzungen gesellschaftlichen Zusammenlebens angesehen werden. [Bi08, 2 f.]

Perfekte Kontextualisierung kann vor dem Hintergrund der damit verbundenen Gefahren nicht als Lösung zum Schutz personenbezogener Daten bezeichnet werden. Dies lässt sich damit begründen, dass sie einerseits zu keiner deutlichen Verbesserung bestehender Probleme zum Schutz personenbezogener Daten in Social Media-Diensten beitragen und andererseits als eine Bedrohung angesehen werden kann, die den Schutz der Privatsphäre als ursprünglich angestrebtes Ziel gänzlich verfehlt. Den Schutz der Privatsphäre dadurch zu erreichen, diese weitgehend abzuschaffen, kann zusätzlich als paradox bezeichnet werden.

3.3 Eigentumsrechte für personenbezogene Information

Derzeit wird der Schutz der Privatsphäre entweder mittels staatlicher Regulierung, wie z.B. in der Europäischen Union, oder mittels Mechanismen der Selbstregulierung des Marktes, wie z.B. in den USA, gewährleistet. Beide Varianten können aber keinen zufriedenstellenden Schutz der Privatsphäre im Internet gewährleisten. Nach herrschender Auffassung ist dies damit zu begründen, dass die Nutzer, welche die Konsequenzen tragen, nicht in ausreichendem Maße in die Entscheidungen zum Schutz ihrer persönlichen Daten mit eingebunden sind. [Le01, 281 f.] Wesentliche Ursache hierfür ist das Fehlen einer geeigneten Infrastruktur, die sowohl technisch als auch organisatorisch den Nutzer in ausreichendem Maße involviert und somit eine Verwaltung der Privatsphäre ermöglichen würde.

Der folgende Ansatz beruht auf der Idee, den Schutz der Privatsphäre in Social Media-Diensten durch eine Kombination aus Gesetz und Technik zu realisieren. Dabei soll die Kontrolle über persönliche Daten nicht beim Staat und auch nicht bei den Unternehmen, sondern beim Nutzer selbst liegen. Konkret wird im Rahmen dieser Idee die Einführung eines umfassenden Digital Rights Management für personenbezogene Information (Privacy DRM) vorgeschlagen, bei dem Nutzer Eigentumsrechte an ihren persönlichen Daten halten. Dadurch sollen die Nutzer mit ihren Daten wie auf einem Markt handeln können und dabei für die Nutzung ihrer Daten einen Preis, den Zweck, die Dauer und den Umfang der Nutzung bestimmen können. [Ma07, 14 f.; Ma08, 14; Le01, 282 ff.] Natürliche Regulierungsmechanismen des Marktes sollen dabei sicherstellen, dass der Schutz personenbezogener Daten im Interesse des Nutzers gewährleistet wird.

Die Einführung eines derartigen DRM ist selbst in einem kleineren unternehmensinternen Umfeld sowohl auf technischer als auch auf rechtlicher Seite komplex. Notwendige Regelungen zur Implementierung und Überwachung der Eigentumsrechte stoßen in Social Media Diensten auf dieselben Probleme wie eine staatliche Regulierung im Internet allgemein. Darüber hinaus besteht ein weiteres Problem konzeptioneller Natur. Damit ein weltweites DRM funktionieren kann, muss dieses wissen, wer, was, wann und mit welcher Information macht. Dies bedeutet jedoch die Schaffung perfekter technischer Überwachung zum Schutz der Privatsphäre. [Ma08, 14; HMoJ] Die Einführung von Eigentumsrechten an persönlicher Information unter Verwendung technischer Mechanismen des DRM, unterstützt von gesetzlichen Regelungen, kann somit, insbesondere vor dem Hintergrund der dadurch entstehenden Möglichkeiten der perfekten technischen Überwachung, nicht als Lösung zur Verbesserung des Schutzes personenbezogener Daten in Social Media-Diensten empfohlen werden.

4 Verfallsdatum für personenbezogene Information

Ein Kernproblem für die Problematik des Schutzes der Privatsphäre in Social Media-Diensten stellt die beschriebene Besonderheit des Internets dar, nichts zu vergessen. Der folgende Vorschlag setzt an dieser Kernproblematik für private Daten an. Durch die Einführung eines Verfallsdatums soll Social Media-Diensten ein „Vergessen“ beigebracht werden, um so möglichen negativen Auswirkungen der Preisgabe privater Information entgegen zu wirken.

4.1 Grundidee

Vergessen ist ein elementarer Prozess der menschlichen Gesellschaft. Erst der Unterschied zwischen der Gewohnheit, dass unwichtige Informationen mit der Zeit in Vergessenheit geraten, und der Tatsache, dass dies in Social Media-Diensten heute nicht mehr der Fall ist, führt größten Teils zu den beschriebenen Problemen mit personenbezogenen Daten in diesen Diensten. Würden Daten, wie aus der analogen Welt gewohnt, im Zeitverlauf vergessen und damit gelöscht werden, würden viele Probleme mit privaten Daten im Internet gar nicht erst entstehen. [Pl08; Sc08, 40].

Der aus dieser Grundidee enstandene „Privacy by Design“-Ansatz [SPC09, 34ff.] beinhaltet dementsprechend die Entwicklung eines Verfallsdatums für digitale Information. Dabei soll zu jeder veröffentlichen Information ein Verfallsdatum angegeben werden können. [Ma07, 19] Entscheidender Unterschied zu anderen Ansätzen des Datenschutzes ist dabei, dass nicht der unmittelbare Schutz persönlicher Informationen im Vordergrund steht, sondern die Frage nach der Kontrolle über diese Informationen. Die Eingabe des Verfallsdatum soll dem Konzept nach dem Nutzer obliegen. [Ma01, 7; Pa08, 3; Re08, 63] Die Nutzer sollen durch das Verfallsdatum eine bewusste Wahlmöglichkeit darüber haben, wie lange sie eine Information aufbewahren wollen. Das Verfallsdatum soll somit keinen Zwang zur Löschung von Information, ähnlich einer externen Zensur, darstellen, sondern die explizite Wahlmöglichkeit des Nutzers darüber, was mit seiner personenbezogenen Information geschieht, in den Vordergrund stellen. Dabei soll es auch möglich sein, für Informationen, die einem Nutzer wichtig genug erscheinen, diese unbegrenzt aufzubewahren. [Mü07b; Pa08; Pl08]

4.2 Umsetzung

Staatliche Regulierung hat bei der Implementierung eines Verfallsdatums lediglich dessen Verwendung zu ermöglichen und die spätere Ausübung durch den Nutzer zu eröffnen. Die Betreiber von Social Media-Diensten, also ggf. auch Unternehmen, die solche Dienste intern einsetzen, müssten daher durch entsprechende Rahmenbedingungen dazu verpflichtet werden, das Verfallsdatum in ihre Anwendungen zu integrieren. Dabei sollte erreicht werden, dass die Standardeinstellung von dem bis jetzt gültigen „unbegrenztes Aufbewahren“ von Information auf „Löschen nach einem definierten Zeitpunkt“ verändert wird. In der Umsetzung könnte dies im Rahmen eines Dialogfeldes, in welches ein Verfallsdatum einzutragen ist realisiert werden. Nach Eintritt des Verfallsdatums soll die zugehörige Information dann automatisch aus dem Social Media-Dienst gelöscht werden. [Ra07; Pa08; Mü07b] Eine implementierte Nachrichtenfunktion könnte den Nutzer beispielsweise vorab per E-Mail über eine Löschung informieren. Dies bietet die Chance, darauf zu reagieren, falls sich die Bedeutung einer Information im Zeitablauf verändert hat, weshalb es sinnvoll sein kann, sie noch länger zu speichern.

4.3 Intention

Die vorrangige Intention der Implementierung eines Verfallsdatums ist nicht die Schaffung einer perfekten technischen Lösung [Pl08; Pa08, 2], sondern die fortwährende aktive Einbindung des Nutzers. [Ka10b, 104] Dies soll Nutzer hinsichtlich der bestehenden Gefahren für den Datenschutz sensibilisieren. [Ma07, 20 ff.; Ma08, 15] Dadurch sollen die Gefahren, die durch einen unbeschwerten Umgang mit persönlichen Daten in Social Media-Diensten entstehen können, nachhaltig minimiert werden. [Pa08, 4; We08; Pl08]

4.4 Vorteile des Verfallsdatums

Auf technischer Seite ist eine Implementierung des Verfallsdatums beispielsweise in Metadaten sehr leicht realisierbar, da diese bereits in jedem Bereich der digitalen Welt vorhanden sind und von allen modernen Betriebs-, Datenbank- und Dateisystemen verstanden werden. Die Angabe zum Verfallsdatum wäre so neben den bereits zahlreichen vorhandenen Datenkategorien in Metadaten nur eine weitere Datenkategorie. Eine umfangreiche Umstellung bestehender Systeme zur Integration des Verfallsdatums ist daher nicht erforderlich. [Pl08; Ma07]

Auf rechtlicher Seite ist es bedeutend einfacher, die Implementierung und Befolgung eines Verfallsdatums zu gewährleisten als die Durchsetzung umfassender Privatsphärenschutzgesetze. Es gibt heute bereits viele Standards im Bereich Software, die von den Unternehmen und Nutzern befolgt werden. Die Implementierung eines Verfallsdatums wäre nur ein weiterer zu befolgender Standard. Durch die Kombination von Recht mit Technik und die aktive Einbindung der Nutzer ist die Überwachung der Befolgung dieser Regelung zum Verfallsdatum zusätzlich kostengünstiger, als sie bei einer rein rechtlichen Regelung möglich wäre. [Pl08; Ma07, 21; Ma08, 15]

Auf gesellschaftlicher Seite ist die Regelung zum Verfallsdatum für jeden Nutzer leicht verständlich und instinktiv anwendbar und bringt nicht die beschriebenen Verständnisprobleme herkömmlicher Regelungen mit sich [Ma07, 22].

4.5 Kritik

Der Ansatz des Verfallsdatums beinhaltet naturgemäß noch konzeptionelle Schwächen, die es im Rahmen zukünftiger Forschung (siehe Kapitel 6) auszugleichen gilt. Einige Kritikpunkte sollen hier im stichwortartig genannt werden [Ka10a, 106f.]:

- staatliche Regulierung ist nicht vollkommen verzichtbar [Ma07, 19; Ra07],
- eine bis hierhin ggf. vorhandene Hemmschwelle, etwas in Social Media-Diensten zu veröffentlichen, wird weiter abgesenkt [Ha08],
- Metadaten eignen sich aufgrund der einfachen Manipulierbarkeit und Umgehbarkeit nur eingeschränkt zur technischen Umsetzung des Verfallsdatums,
- Einmal veröffentlichte Informationen können leicht durch Dritte kopiert und erneut eingestellt werden. (z.B. mittels einer Bildschirmkopie) [Ha08; Pö07],
- fremdgenerierte Informationen können mittels eines Verfallsdatums ebenfalls nicht kontrolliert werden,
- Informationen die rechtlich geschäftsrelevante Daten enthalten sind von einem Verfallsdatum auszunehmen.

5 Schlussfolgerungen

Bei der Untersuchung verschiedener alternativer Lösungsansätze zur Verbesserung des Schutzes der Privatsphäre in Social Media-Diensten wird deutlich, dass insbesondere Lösungen, welche den Schutz der Privatsphäre stärker in die Hände der Nutzer legen, erfolgversprechend sind. Die Lösungsansätze der digitalen Enthaltsamkeit und der perfekten Kontextualisierung können allerdings nur eingeschränkt zu einer Verbesserung des Schutzes der Privatsphäre beitragen. Als richtungsweisender Ansatz kann die Idee der Einführung von Eigentumsrechten an personenbezogenen Daten bewertet werden. Die Verknüpfung mit Fragestellungen des Digital Rights Management erschweren jedoch einen sinnvollen Einsatz. Der Ansatz der Einführung eines Verfallsdatums für Informationen will die Kontrolle über persönliche Daten ebenfalls stärker in die Hände der Nutzer legen. Die primäre Absicht des Verfallsdatums ist dabei, die Nutzer für das Problem des mangelnden Schutzes der Privatsphäre in Social Media-Diensten zu sensibilisieren. Ein entscheidender Vorteil gegenüber der Idee der Eigentumsrechte ist, dass das Verfallsdatum wesentlich spezieller und in der Anwendung sowohl auf technischer Ebene als auch auf der Nutzerebene unkomplizierter ist. Ein Verfallsdatum ist für den Nutzer durch die Nachbildung des natürlichen Vergessensprozesses des menschlichen Gedächtnisses instinktiv verständlich und anwendbar. Allerdings bestehen auf technischer Seite Hürden bzgl. der leichten Manipulierbarkeit der zur Implementierung des Verfallsdatums vorgeschlagenen Metadaten. Zu erforschende Verbesserungsvorschläge können dazu beitragen, diese Probleme zu verringern.

Im Hinblick auf die weitere Entwicklung des Einsatzes von Social Media-Diensten in Unternehmen wird sich die Gefährdung der Privatsphäre des Nutzers in Zukunft weiter verstärken. Der Trend in Richtung mobiler Dienste steigert die Intensität und Dauer deren Nutzung weiter. Dieser Trend wird durch das steigende Nutzenpotenzial aufgrund immer neuer Anwendungsmöglichkeiten verstärkt. Mit zunehmender Nutzung steigt aber auch die Menge personenbezogener Daten, die preisgegeben werden, weiter an. Damit steigt auch das Potential für den Missbrauch dieser Daten. Weiterhin lassen Schlagworte wie Semantic Web und Ubiquitous Computing erahnen, dass der Schutz der Privatsphäre in Zukunft vor weiteren Herausforderungen stehen wird.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

6 Ausblick

Zukünftig sind Forschungsergebnisse aus dem seitens der DFG geförderten Projekt "Young Scholars Network on Privacy and Web 2.0" (http://gepris.dfg.de/gepris/OCTOPUS/?module=gepris&task=showDetail&id=161857057) zu erwarten. Erste softwaretechnische Ansätze zur Realisierung eines Verfallsdatums für Daten im Internet, wie sie beispielsweise an der Universität Saarbrücken entwickelt wurden, liefern Ansatzpunkte für weitere Forschungsvorhaben. Die im April 2011 seitens des Bundesministeriums des Inneren gestartete Webseite www.vergessen-im-internet.de fordert die Nutzer im Rahmen von Innovationswettbewerben zur Teilnahme auf und motiviert die Weiterentwicklung der Forschungsfrage. Ziel dieser Initiative ist eine möglichst breite Diskussion in Gesellschaft und Wissenschaft über die Chancen und Risiken anzustoßen, die mit der Verfügbarkeit von Daten im Internet verbunden sind. Die dort formulierte Erkenntnis das die Bandbreite möglicher Ideen noch nicht ausgeschöpft ist, bestätigt die Ergebnisse des hier vorliegenden Forschungsbeitrags.

Literaturverzeichnis

[Ad03] Adamowsky, N.: Totale Vernetzung - totale Verstrickung? In: Politik und Zeitgeschichte 42 (2003), S. 3-5.

[Ba08] Bannasch, B.: Arbeitskreis "Techniken der Ausspähung - bedrohte Privatheit: 'Der gläserne Mensch' - was wir von uns preisgeben". 2008. https://www.edvgt.de/media/Tagung08/Praesentationen/PrDa2Bannasch.pdf. Abruf am 2009-04-28.

[Bi08] Bielefeldt, H.: "Ich hab nichts zu verbergen" - ein gedankenloser Spruch. 2008. http://www.datenschutz.fu-berlin.de/dahlem/ressourcen/datenschutzfachtagung-2008/dana-1-2008-datenschutz-bielefeldt.pdf. Abruf am 2009-05-03.

[Bo03] Bohn, J.; Coroama, V.; Langheinrich, M.; Mattern F.; Rohs M.: Allgegenwart und Verschwinden des Computers - Leben in einer Welt smarter Alltagsdinge. 2003. http://www.vs.inf.ethz.ch/res/papers/bohn_allgegenwart_privat_2003.pdf. Abruf am 2009-05-27.

[Fu09] Fuchs, M.: Außer Kontrolle: Digitale Daten - Wie könne wir unser Daten in Zukunft schützen. 2009-01-23. http://www.3sat.de/mediathek/frameless.php?url=/neues/sendungen/magazin/130305/index.html. Abruf am 2009-05-21.

[Ha08] Hahn, F.: Zur KeyNote “Nützliches Vergessen” auf der re:publica. 2008-04-02. http://blog.synaxon.de/index.php/2008/04/02/zur-keynote-%e2%80%9cnutzliches-vergessen%e2%80%9d-auf-der-republica/. Abruf am 2009-06-04.

[HKP08] Henkel, T.; Küch, O.; Poller, A.: Privatsphärenschutz in Soziale-Netzwerke-Plattformen. 2008. http://www.sit.fraunhofer.de/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf. Abruf am 2009-05-02.

[HKW08] Hass, B. H.; Kilian, T.; Walsh, G.: Grundlagen des Web 2.0. In: Hass, B. H.; Kilian, T.; Walsh, G. (Hrsg.): Web 2.0 - Neue Perspektiven für Marketing und Medien. Springer, Berlin, Heidelberg, 2008, S. 4–19.

[HMoJ] Hansen, M.; Möller, J.: Digital Rights Management zwischen Sicherheit und informationeller Selbstbestimmung. https://www.datenschutzzentrum.de/vortraege/050510_hansen-moeller_bsi.htm. Abruf am 2009-07-13.

[Ka10a] Karla, J.: Can Web 2.0 ever forget?. In: Business & Information Systems Engineering (2010) 2, 105-107

[Ka10b] Karla, J.: Privacy Concerns with Social Software in the Workplace - A Discussion of Concepts to make Enterprise 2.0 Services forget. In: International Journal of Business Research (2010) 5, 101-109

[KÖG08] Kleimann, B.; Özkilic, M.; Göcks, M.: Studieren im Web 2.0. 2008-11. https://hisbus.his.de/hisbus/docs/hisbus21.pdf. Abruf am 2009-06-25.

[La04] Langheinrich, M.: Die Privatsphäre im Ubiquitous Computing – Datenschutz-aspekte der RFID-Technologie. 2004. http://www.vs.inf.ethz.ch/publ/papers/langhein2004rfid.pdf. Abruf am 2009-05-26.

[Le01] Lessig, L.: Code und andere Gesetze des Cyberspace. Berlin-Verlag, Berlin, 2001.

[Li08] Linder, E.: Das Netz vergisst nichts. In: technische Fachzeitschrift der vereinigten Fachverlage (2008).

[Ma01] Mayer-Schönberger, V.: Information und Recht - Vom Datenschutz bis zum Urheberrecht; praxisbezogene Perspektiven für Österreich, Deutschland und die Schweiz. Springer, Wien, 2001.

[Ma07] Mayer-Schönberger, V.: Useful voide: The art of Forgetting in the Age of Ubiquitous Computing. 2007. http://www.vmsweb.net/attachments/pdf/Useful _Void.pdf. Abruf am 2009-07-25.

[Ma08] Mayer-Schönberger, V.: Nützliches Vergessen. In: Reiter, M.; Wittmann-Tiwald, M. (Hrsg.): Goodbye Privacy - Grundrechte in der digitalen Welt. Linde, Wien, 2008, S. 9-15.

[Mü02] Mülder, W.: Webbasiertes Personalmanagement. In: Information Management & Consulting (2002) 1, S. 61-66.

[Mü07a] Mülder, W.: Die Chancen von IT 2.0 nutzen. In: Personalwirtschaft - Sonderheft 7 (2007) 7, S. 8-10.

[Mü07b] Müller, C.: Daten mit Verfallsdatum. 2007-12-11. http://www.telemedicus. info/article/565-Daten-mit-Verfallsdatum.html. Abruf am 2011-04-20.

[Os07] Osl, M.: Safer Web 2.0: Datenschutz Anwenderstrategien im Web 2.0. 2007. http://netzwertig.com/2007/04/15/zn-safer-web-20-datenschutz-anwenderstrategien-im-web/. Abruf am 2009-04-27.

[Pa08] Pauli, R.: Vergessen muss wieder einfacher werden! - Viktor Mayer-Schönberger. 2008. http://www.wienerzeitung.at/print.aspx?TabID=4664&Alias=wzo&cob=375083&currentpage=0&ModID=15309. Abruf am 2009-04-28.

[Pl08] Pluta, W.: Interview: "Daten brauchen ein Verfallsdatum". 2008-04-02. http://www.golem.de/0804/58721.html. Abruf am 2011-04-20.

[Pö07] Pötzel, N. F.: Anarchie im Netz - Einfallstor in die Privatsphäre. In: Spiegel (26.06.2007), S. 52-58.

[Ra07] Raguse, M.: Verfallsdatum für Daten im Internet - Regulierung gefordert. 2007-12-07. http://www.datenschutz.de/news/detail/?nid=2382. Abruf am 2009-06-05.

[Re08] Reischl, G.: Die Google-Falle - Die unkontrollierte Weltmacht im Internet. Ueberreuter, Wien, 2008.

[Sc08] Schoen, A.: Brennpunkt Privatsphäre: Persönliche Infos im Web ausradieren. In: Chip 7 (2008), S. 40-41.

[SPC09] Sterbik-Lamina, J.; Peissl, W.; Cas, J.: Privatsphäre 2.0 Beeinträchtigung der Privatsphäre in Österreich. 2009. http://epud.oeaw.ac.at/ita/ita-projektberichte/d2-2a53.pdf. Abruf am 2009-04-27.

[We08] Weigert, M.: Datenschutz im Web 2.0 - Ein Umdenken ist notwendig. 2008. http://netzwertig.com/2008/05/28/datenschutz-im-web-20-warum-ein-umdenken-notwendig-ist/. Abruf am 2009-05-02.

[Ze09] Zeger, H. G.: Paralleluniversum Web 2.0 - Wie Online-Netzwerke unsere Gesellschaft verändern. 1. Aufl., Kremayr & Scheriau, Wien, 2009.