Sebastian und Rainer W. Gerling

Wie realistisch ist ein „Recht auf Vergessenwerden“?

Der Entwurf der Europäischen Datenschutz-Grundverordnung fordert in Artikel 17 ein „Recht auf Vergessenwerden“. Dies ist als organisatorische Regel sicherlich sinnvoll; es stellt sich aber sofort die Frage, inwieweit so etwas auch technisch realisierbar ist. Die existierenden Lösungen und Ansätze werden bewertet und im Licht der Vorgaben der Verordnung beleuchtet.*

1 Rechtliche Vorgaben

Am 25. Januar 2012 hat die EU-Kommissarin Viviane Reding einen Entwurf einer Datenschutz-Grundverordnung[1] vorgestellt. Der Artikel 17 ist dem Anspruch auf Löschen und dem „Recht auf Vergessenwerden“ gewidmet. Während der Löschanspruch sich auf eine verantwortliche Stelle bezieht, ist der Anspruch auf „Vergessenwerden“ weiter gefasst. Die verantwortliche Stelle muss – so zumindest der ursprüngliche Entwurfstext – alle vertretbaren Schritte unternehmen, um auch die Löschung der Daten bei Dritten, an die die Daten übermittelt wurden, sicherzustellen.

Gerade vor dem Hintergrund des Internets mit seinen zahlreichen Playern und der damit verbundenen nahezu ungehemmten Verbreitung und Verfügbarkeit von Daten ist dies eine echte Herausforderung für die speichernde Stelle.

* Vortrag auf dem 4. Forum Verbraucherrechtswissenschaft „Datenschutz als Verbraucherschutz“ veranstaltet von der Forschungsstelle für Verbraucherrecht an der Universität Bayreuth.

1 http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf

Sebastian Gerling, M.Sc.

Administrativer Leiter des „Center for IT-Security, Privacy and Accountability“ (CISPA) und wissenschaftlicher Mitarbeiter am Lehrstuhl für Informationssicherheit und Kryptographie an der Universität des Saarlandes
E-Mail: sgerling@cs.uni-saarland.de

Prof. Dr. Rainer W. Gerling

Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft sowie stellvertretender Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit. Honorarprofessor für IT-Sicherheit an der Hochschule München
E-Mail: gerling@gv.mpg.de

2 Entwicklung

In der Vergangenheit wurden viele Informationen im Laufe der Zeit vergessen. Nur besonders wichtige Ereignisse (der Zeitgeschichte) und zentrale Elemente der Kultur wurden weitererzählt. Mit der Möglichkeit der Aufzeichnung von Informationen, insbesondere durch den Buchdruck, wurde eine längere Speicherung von Informationen möglich.

So ist heute mit dem Erscheinen einer Tageszeitung der gedruckte Inhalt in großer Anzahl verfügbar. Mit dem Zerfall des Papiers tritt ein natürliches Vergessen ein. Nur in speziellen Archiven bleibt die Information auch im Anschluss erhalten. In diesen Archiven sind Informationen zwar verfügbar, allerdings ist auf Grund von eingeschränkten Recherchemöglichkeiten zum Auffinden doch einiger Aufwand durch den Suchenden zu betreiben.

Mit dem Internet werden Informationen von jedem Ort jederzeit für jeden recherchierbar. In der Wahrnehmung vieler Nutzer machen gerade die durch Zugangsmakler (Portale, Suchmaschinen) auffindbaren Informationen das Internet aus.[2]

Ein aktuelles Verfahren vor dem EuGH[3] zeigt eindrucksvoll den aus dieser Entwicklung herrührenden Konflikt zwischen dem „Recht auf Vergessenwerden“ und dem Recht auf Informations- und Meinungsfreiheit. Ein Spanier, dessen Haus im Jahre 1998 zwangsversteigert wurde, will erreichen, dass die amtliche Ankündigung der Zwangsversteigerung nicht mehr an prominenter Stelle unter den Suchergebnissen erscheint. Nach spanischem Recht musste diese Bekanntmachung damals in einer Tageszeitung erfolgen. Mittlerweile ist das Zeitungsarchiv jedoch auch online verfügbar.

3 Technische Möglichkeiten

Eine der ersten technischen Umsetzungen des „Rechts auf Vergessenwerden“ war X-pire![4]. Dieses Tool implementiert eine Soft-

2 Vgl. den Beitrag von R. Bengez zum „Schlüsselkonzept der Suchmaschinen“ in diesem Heft.

3 http://curia.europa.eu/juris/liste.jsf?language=de&num=C-131/12; http://heise.de/-1811505

4 Julian Backes, Michael Backes, Markus Dürmuth, Sebastian Gerling und Stefan Lorenz: X-pire! – A digital expiration date for images in social networks, eprint

warelösung für Fotos, wäre konzeptionell aber auch auf andere Inhalte erweiterbar. Das Konzept von X-pire! geht davon aus, dass die Nutzer kooperativ sind, d.h. die Nutzer halten sich an die Regeln und greifen nicht in das System ein, um es auszuhebeln.

X-pire! zeigt hier die Grenze des technisch Möglichen für reine Softwarelösungen auf. Es ist nicht möglich, bei den heutigen Betriebssystemen eine Softwarelösung zu implementieren, die den rechtmäßigen Käufer und Nutzer von Eingriffen in das System abhält, die vom Softwarehersteller unerwünscht sind. Die gesamte Kritik an dem System X-pire! geht von einem Nutzer aus, der sich nicht an die legitimen Nutzungsregeln hält[5]. Allerdings weisen die Autoren von X-Pire! selbst auf diese technische Grenze hin und das angenommene kooperative Nutzerverhalten ist in der angewandten IT-Sicherheit eine durchaus gängige Annahme. Selbst das bekannte Common Criteria „Controlled Access Protection Profile" geht davon aus: „Authorized users … are expected to act in a cooperating manner in a benign environment."[6]

Unterstellt man dem Nutzer unkooperatives Verhalten, so bleibt nur eine hardwarebasierte Lösung. Dass auch dies nicht einfach ist, zeigen Spielekonsolen (z.B. PS3[7], Xbox[8] oder Wii U[9]) sowie Betriebssysteme wie iOS[10], deren Hersteller erheblichen (bisher oft vergeblichen) Aufwand treiben, ein auch gegen Angriffe durch den legitimen Nutzer (der sein System anders nutzen möchte, als vom Hersteller vorgesehen, z.B. Starten von Linux auf einer PS3-Spielkonsole) abgesichertes System zu bauen.

Da es beim „Recht auf Vergessenwerden" in der Regel „nur" um die Anzeige von Dateien mit Texten, Bildern, Videos und Tönen geht, ist der Prüfungsaufwand geringer, da die Implementierung des Anzeigemoduls in der Regel weitaus weniger komplex ist als die eines komplettes Betriebssystems. Es macht aber trotzdem Sinn, sich auf das alte Konzept des Reference Monitor[11] zu besinnen und die Hardware nach diesem Konzept zu entwerfen. Er stellt die Kontrolle und Durchsetzung von Zugriffsrechten sicher[12]:

- Subjekte können nicht direkt, sondern ausschließlich durch den Referenzmonitor auf Objekte zugreifen (complete mediation).
- Der Referenzmonitor selbst, seine Konfiguration und seine Daten müssen vor Manipulation geschützt sein (tamperproof).
- Der Referenzmonitor muss klein genug sein, dass er verifiziert und getestet werden kann (verifiable).
- Die Implementierung des Referenzmonitors muss fehlerfrei sein (correctness).

Zusätzlich sollte die Hardware sehr nahe an dem Ausgabe- bzw. Anzeigegerät sein. Der Vorschlag von Stephan Lukas für das System „P3 – Picture and Privacy Protection"[13] geht auch in diese Richtung.

Die kleinste Realisierung eines hardwarebasierten Referenzmonitors wäre ein spezieller Chip. Dieser Chip müsste in alle Endgeräte (Monitore, Fernseher usw.) eingebaut werden und einen Kopierschutzkanal (ähnlich High-bandwidth Digital Content Protection (HDCP)[14] für die Inhalte aufbauen. In das Design und vor allem die Verifikation des Chips müsste erheblicher Aufwand gesteckt werden, da eine fehlerfreie Implementierung unabdingbar ist.

4 Konsequenzen

Jede technische Lösung, die ein „Recht auf Vergessenwerden" implementiert, kann auch zur Kontrolle von anderen Inhalten genutzt werden. Ob ein Foto, ein Video aus Datenschutzgründen technisch eingesperrt wird oder ob die Verbreitung aus anderen Gründen kontrolliert wird, ist egal: Konzeptionell handelt es sich um ein „Digitales Rechtemanagement" (DRM).

Aus diesem Grunde liefert eine technische Implementierung des „Rechts auf Vergessenwerden" der Content-Industrie oder weniger demokratischen Herrschern und Regimen immer auch das Werkzeug zur Kontrolle ihrer Inhalte. Im Grunde ist es ein klassisches janusköpfiges „Dual-Use-Tool", bei dem technisch nicht zwischen datenschutzrechtlicher und anderer Verwendung unterschieden werden kann.

5 Fazit

Es ist technisch möglich durch geeignete Hardware die technische Infrastruktur zu schaffen, um ein „Recht auf Vergessenwerden" umzusetzen. Ob dies in einer Art und Weise geschaffen werden kann, die dem Nutzer einen leichten Umgang damit ermöglicht, ist eine andere Frage. Auch wenn z.B. Facebook einige Möglichkeiten für Privacy-Einstellungen bietet: Nicht jeder Nutzer beherrscht diese. Eine Technik, die die Nutzer nicht beherrschen, kann aber per definitionem nicht sicher sein.

Es muss auch klar sein, dass jedweder Inhalte von Beginn an für das Vergessen markiert werden muss. Eine nachträgliche Ergänzung dieses Attributs ist nicht möglich.

Für die Durchsetzung der nötigen Infrastruktur scheint der Datenschutz nicht das geeignete Mittel zu sein. Hierzu wäre die Content-Industrie oder die Legislative sicherlich eher in der Lage. Ob der Datenschutz mit der Forderung nach dem „Recht auf Vergessenwerden" eine Infrastruktur fordern soll, die das ultimative digitale Rechtemanagement implementiert und damit anderen Playern (Content-Industrie, Staaten) die Rechtfertigung und die technische Voraussetzung hierfür liefert, sollte ergebnissoffen diskutiert werden. Nicht, dass wir am Ende mit Goethe sagen müssen „Die ich rief, die Geister, werd' ich nun nicht los."[15]

arXiv:1112.2649 (2011) http://arxiv.org/abs/1112.2649.

5 Siehe z.B. http://heise.de/-1180381.

6 http://www.niap-ccevs.org/pp/pp_os_ca_v1.d.pdf, am 5.3.2013 archiviert

7 http://heise.de/-1736203

8 http://heise.de/-1332614

9 http://heise.de/-1752416

10 http://heise.de/-1797221

11 http://csrc.nist.gov/publications/history/ande72.pdf

12 In Anlehnung an : http://ix.cs.uoregon.edu/~butler/teaching/10F/cis607/papers/jaeger-refmon.pdf.

13 http://heise.de/-1569814

14 http://www.digital-cp.com/

15 Johann Wolfgang von Goethe, Der Zauberlehrling, 1797.