

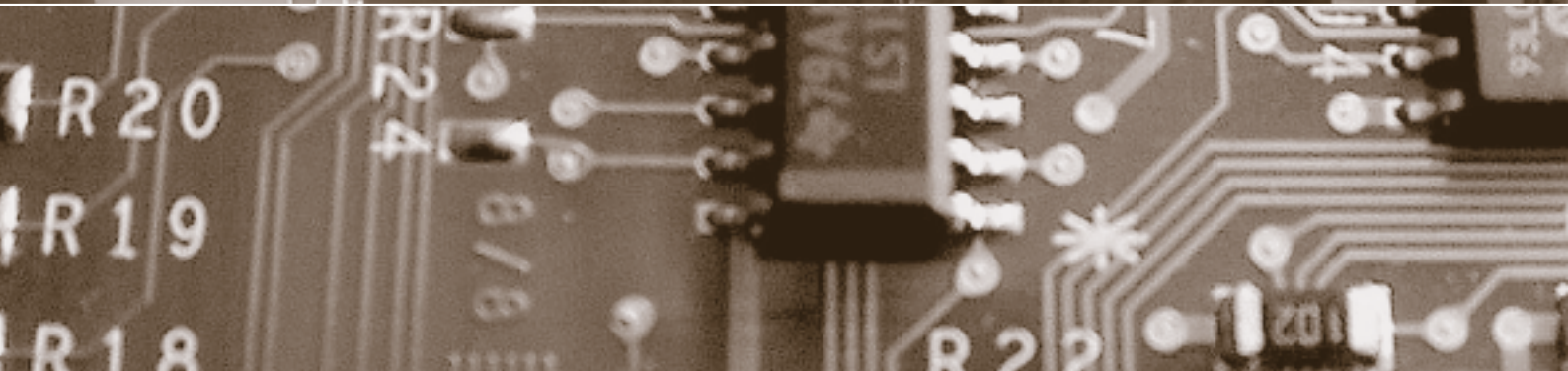
Schwerpunkt:

## Staatsschutz

**fokus:** Kann man aus der «Fichenaffäre» lernen?

**fokus:** Der «nummerierte» Bürger wird vernetzt

**report:** Datendiebstahlsfälle 2008 in Deutschland



Herausgegeben von  
**Bruno Baeriswyl**  
**Beat Rudin**  
**Bernhard M. Hämmerli**  
**Rainer J. Schweizer**  
**Günter Karjoth**

## fokus



### Schwerpunkt: **Staatsschutz**

auftakt

Staatsschutz – ein Hort für  
Wiederholungstäter  
von Roland Stark

**Seite 49**

Staatsschutz unter Kontrolle?  
von Beat Rudin

**Seite 52**

Staatsschutz im Laufe der Zeit  
von Georg Kreis

**Seite 54**

Staatsschutz braucht klare Regelungen  
von Markus H.F. Mohler

**Seite 60**

Der «nummerierte» Bürger wird vernetzt  
von Bruno Baeriswyl

**Seite 64**

Vor zwanzig Jahren kam der «Fichen-  
skandal» ans Licht. Er führte u. a. zum  
Einsatz einer Parlamentarischen Unter-  
suchungskommission. Kann uns die  
Geschichte lehren oder können wir Lehren  
daraus ziehen? Und welche Lektionen  
hätten wir allenfalls aus der Fichenaffäre  
von 1989/1990 ziehen können?

### **Staatsschutz im Laufe der Zeit**

Die föderalistische Teilung von operatio-  
nellen und Kontrollaufgaben gemäss BWIS  
bereitet nach wie vor erhebliche Schwie-  
rigkeiten. Unklare, ja teilweise wider-  
sprüchliche Bestimmungen führen zu  
einem Defizit punkto Föderalismus, Ge-  
währleistung der Rechtsstaatlichkeit  
und Gewaltenteilung.

### **Staatsschutz braucht klare Regelungen**

Die faktisch unbeschränkte Verwendung  
der Sozialversicherungsnummer als univer-  
seller Personenidentifikator schafft hohe  
Risiken für die Grundrechte der Bürger.  
Österreich zeigt, wie ein Personenidentifi-  
kator mit entsprechenden Schutzmass-  
nahmen eingeführt werden kann. In der  
Schweiz weitet sich indessen der un-  
kontrollierte Gebrauch des Personen-  
identifikators aus.

### **Der «nummerierte» Bürger wird vernetzt**

## impresum

**digma:** Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: [www.digma.info](http://www.digma.info)

**Herausgeber:** Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

**Redaktion:** Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

**Zustelladresse:** Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel  
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, [redaktion@digma.info](mailto:redaktion@digma.info)

**Erscheinungsplan:** jeweils im März, Juni, September und Dezember

**Abonnementspreise:** Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 99.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

**Anzeigenmarketing:** Publicitas Publimag AG, Mürtchenstrasse 39, Postfach, CH-8010 Zürich  
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, [www.publimag.ch](http://www.publimag.ch), [service.zh@publimag.ch](mailto:service.zh@publimag.ch)

**Herstellung:** Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

**Verlag und Abonnementsverwaltung:** Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich  
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, [www.schulthess.com](http://www.schulthess.com), [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

**Whistleblowing:  
heikle Konflikt-  
felder**

In der globalen Arbeitswelt soll Whistleblowing Wirtschaftsdelinquenz, Korruption und weitere erhebliche Missstände im Unternehmen aufdecken. Dabei werden nachhaltig Kernbereiche des Datenschutzes am Arbeitsplatz berührt. Wie können die Probleme des Whistleblowing annäherungsweise und datenschutzkonform geregelt werden?

**Datendiebstahls-  
fälle 2008 in  
Deutschland**

Eine Meldung über einen Datendiebstahl Deutschland jagt die andere. Wie kam es zu den verschiedenen Fällen? Was waren die Ursachen? Was kann dagegen unternommen werden?

**Vorsorgliche Mass-  
nahmen des EDÖB**

Zum ersten Mal seit Einführung des DSGVO 1992 hatte sich das Bundesverwaltungsgericht mit der Frage zu beschäftigen, ob und inwieweit vorsorgliche Massnahmen bei der Anwendung des DSGVO angebracht sind. Der EDÖB sieht in der Bejahung der Frage eine Stärkung seiner Position gegenüber Datenbearbeitern.

**Verfassungswidrige und  
unnötige  
Regelung**

Immer häufiger erklärt der Bundesgesetzgeber das Bundesdatenschutzgesetz auch anwendbar für kantonale und kommunale öffentliche Organe – entgegen der verfassungsrechtlichen Kompetenzverteilung und ausserdem unnötigerweise. Ein aktuelles Beispiel betrifft die Verordnung über die Videoüberwachung im öffentlichen Verkehr

**report**



**RECHTSETZUNG**

Whistleblowing: heikle Konfliktfelder

von Marie-Theres Tinnefeld

**Seite 68**

**ZWISCHENTAKT**

Lesarten ...

von Frank U. Frey

**Seite 73**

**LESSONS TO LEARN**

Datendiebstahlsfälle 2008 in Deutschland

von Martin Meints

**Seite 74**

**RECHTSDURCHSETZUNG**

Vorsorgliche Massnahmen des EDÖB

von Marc-Frédéric Schäfer

**Seite 78**

**forum**



**PRIVATIM**

Verfassungswidrige und unnötige Regelung

Stellungnahme von privatim

**Seite 82**

**PRIVATIM**

Google Street View

Medienmitteilung von privatim

**Seite 84**

**ISSS**

DRM: the good, the bad and the ugly?

von Giampaolo Trenta

**Seite 86**

**agenda**

**Seite 87**

**schlussakt**

«Deanonymisierung» – das neue alte Rezept

von Beat Rudin

**Seite 88**

**Cartoon**

von Hanspeter Wyss

ISSS

# DRM: the good, the bad and the ugly?



Giampaolo Trenta,  
Vorstandsmitglied  
ISSS, [www.iss.ch](http://www.iss.ch)  
[giampaolo.trenta@iss.ch](mailto:giampaolo.trenta@iss.ch)

Am 17. Juni hat ISSS in den edlen Kulissen des Widder Hotels in Zürich eine ganztägige Konferenz über Digital Rights Management (DRM) mit hochwertigen Beiträgen von Hochschuldozenten, Vertretern aus der Unterhaltungsindustrie, Juristen und Lösungsanbietern organisiert. Die wesentlichen Erkenntnisse aus der Konferenz werden in diesem Artikel kurz zusammengefasst.

## Anwendung von DRM

DRM behandelte in diesem Kontext zwei Anwendungsmöglichkeiten, nämlich den Schutz der Urheberrechte aus Sicht der Unternehmensindustrie sowie den Schutz unternehmensinterner Information gegen Durchsickern nach Aussen als Teil einer umfassenden Data-Leakage-Prevention-Lösung (DLP).

## Grundlagen von DRM

Technische und architektonische Gemeinsamkeiten in den oben erwähnten Anwendungsbereichen wurden aufgrund eines Referenzmodells aufgezeichnet. Inhalt und Bestimmungen über den autorisierten Umgang mit dem Inhalt werden durch DRM mit Hilfe der Kryptografie zusammengeschnitten. Der Zugang zum verschlüsselten Inhalt erfolgt dann durch eine vertrauenswürdige Komponente, welche die für die Entschlüsselung erforderlichen Schlüssel von einem Lizenzserver bezieht und die mit dem Inhalt assoziierte Bestimmung auf dem System des Anwenders

durchsetzt. Natürlich kann dieser Ansatz niemals eine 100%-Sicherheit garantieren, denn die vertrauenswürdige Komponente kann auf dem Anwendersystem beobachtet, attackiert, disassembliert und allenfalls teilemuliert werden, was eine Aufhebung des Schutzes ermöglicht.

## DRM in der Unterhaltungsindustrie

DRM wurde am Beispiel der Musikindustrie zuerst als tot erklärt. Das Gleiche sollte demnächst der Filmindustrie passieren, wenn keine neuen Business-Modelle entwickelt werden. Es hatte sich nämlich gezeigt, dass Konsumenten nicht bereit sind, für einschränkende oder gar destabilisierende Mechanismen zu bezahlen. Ehrliche und zahlende Konsumenten würden bei der legitimen Verwendung legal erworbener Musikstücke oder Computerspiele behindert, während illegale Kopien uneingeschränkt und über die Grenzen verschiedener Produkte und Hersteller hinaus verwendet werden können. Die neue Tendenz ist, Inhalte unentgeltlich und ohne Kopierschutz zur Verfügung zu stellen, wobei die Finanzierung aus anderen Quellen gesichert werden sollte. Beispiele sind Datenvolumenverrechnung bei Telekom-Gesellschaften, Werbung, etc. Dies bedeutet, dass in der Tat DRM nicht unbedingt tot ist, sondern dass es anders verwendet wird. Mit der Bezeichnung «DRM-frei» ist oft nur der fehlende Kopierschutz gemeint, nicht aber die Möglichkeit, den

Umgang der Konsumenten mit den Inhalten zu überwachen, zu protokollieren und auszuwerten. Marketing-Aspekte und die Profilierung der Konsumenten rücken immer mehr in den Vordergrund und werden voraussichtlich Bestandteil neuer Geschäftsmodelle.

## DRM im Unternehmen

Innerhalb von Unternehmen haben DRM-Technologien noch nicht Fuss fassen können. Die Verwendung von DRM zur Unterstützung von DLP-Produkten ist noch relativ unreif. Zudem sind bei einer allfälligen Verwendung von DRM noch eine ganze Reihe technischer und organisatorischer Fragen zu beantworten. Insbesondere die Datenklassifizierung sowie starke Bedenken bezüglich der Langzeitzugänglichkeit von DRM-geschützten Informationen über die Grenzen von Produkten und Technologien hinaus sprachen bis heute gegen den breiten Einsatz von DRM-Systemen im Unternehmen. So ist es heute unschwer möglich, DLP-Systeme auf dem Markt zu finden, welche ohne DRM-Komponente auskommen. Natürlich können aber solche Lösungen mit dem direkten Zugang auf die ungesicherte Information über allfällig vorhandene DLP-freie Systeme ausgehebelt werden.

## Legale Aspekte

Der Schutz der Urheberrechte wird in unterschiedlichen Ländern oft unterschiedlich ausgelegt. In der Schweiz

ist es (ausser bei Software) möglich, private Kopien urheberrechtlich geschützter Werke anzufertigen. Die Meinung ist, dass die Abgeltung für Privatkopien durch die Leerträgerabgaben erfolgt. Das Umgehungsverbot des Kopierschutzes gilt im privaten Bereich nicht. Es ist erlaubt, Lösungen zur Umgehung des Kopierschutzes zu erwerben und zu besitzen, wenn diese nicht für Erwerbszwecke verwendet werden. Solche Lösungen dürfen aber keinesfalls angeboten oder ausgebreitet werden. Das Gleiche gilt auch für das Zur-Verfügung-Stellen urheberrechtlich geschützter Werke ausserhalb des Kreises von Freunden und Familie. Dies gilt auch, wenn es ohne aktives Zutun erfolgt, wie es zum Bei-

spiel im Rahmen der Verwendung von Peer-to-Peer-Netzwerken wie Kazaa der Fall ist.

#### **Die Zukunft von DRM**

Bei der Frage, ob DRM-Systeme in Zukunft auf offener Basis entwickelt werden sollten, waren sich die Experten uneinig. Es hatte sich nämlich gezeigt, dass dominierende Anbieter Lösungen diktieren können. Zudem, so behaupten andere Experten, hätten im Bereich DRM proprietäre Lösungen sicherheitstechnische Vorteile gegenüber offenen Lösungen.

#### **Fazit**

Die Verwendung von DRM-Technologien ist sehr umstritten und erzeugt einige Emotionen.

Es ist jedoch klar, dass Information einen Wert hat. Diejenigen, die sich angestrengt haben und diesen Wert geschaffen haben, sollten die Früchte ihrer Anstrengungen ernten können. Auf der anderen Seite darf DRM nicht dazu Anlass geben, die ehrlichen Konsumenten mehrmals zum Kauf des gleichen Inhalts zu zwingen.

Unternehmen, welche DRM-Technologien für den Schutz interner Informationen bereits heute verwenden möchten, sind gut beraten, das Vorhaben äusserst vorsichtig abzuwägen und besonders sorgfältig zu planen. ■

## agenda

### **14. Symposium on Privacy and Security**

Stiftung für Datenschutz und Informationssicherheit

Internet mit neuen Dimensionen. Cloud Computing – Suchtechnologien – Sicherheit – Daten- und Geheimnisschutz – Recht auf Vergessen

9. September 2009, ETH Zürich, Zürich

<http://www.privacy-security.ch>

<<http://www.privacy-security.ch>>

### **SecurityConference'09**

ISPIN AG

10. September 2009, Zürich

<http://www.securityconference.ch>

### **Security-Zone 2009**

Plattform für Informationssicherheit

23./24. September 2009, Zürich

<http://www.security-zone.info>

### **Informatik 2009**

Im Fokus das Leben

39. Jahrestagung der Gesellschaft für Informatik

28. September bis 2. Oktober 2009, Lübeck/D

<http://www.informatik2009.de/>

### **ISSE 2009**

Information Security Solutions Europe

6.–8. Oktober 2009, Den Haag/NL

<http://www.isse.eu.com>

### **31th International Conference of Data Protection and Privacy Commissioners**

Privacy: Today is Tomorrow

4.–6. November 2009, Madrid/E

<http://www.privacyconference2009.org>

### **12. Berner Tagung für Informationssicherheit**

ICT Risk Management: Aufwand und Nutzen  
ISSS

26. November 2009, Bern

<http://www.isss.ch/veranstaltungen/2009/>

12-berner-tagung/

## Nächste Nummer

Die nächste Ausgabe von digma erscheint im September 2009 und widmet sich schwerpunktmässig dem Thema «**Einwilligung**»

## Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)  
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name \_\_\_\_\_ Vorname \_\_\_\_\_

Firma \_\_\_\_\_

Strasse \_\_\_\_\_

PLZ \_\_\_\_\_ Ort \_\_\_\_\_ Land \_\_\_\_\_

Datum \_\_\_\_\_ Unterschrift \_\_\_\_\_

### Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich

Telefon +41 44 200 29 19

Telefax +41 44 200 29 18

E-Mail: [zs.verlag@schulthess.com](mailto:zs.verlag@schulthess.com)

Homepage: [www.schulthess.com](http://www.schulthess.com)

Schulthess 