

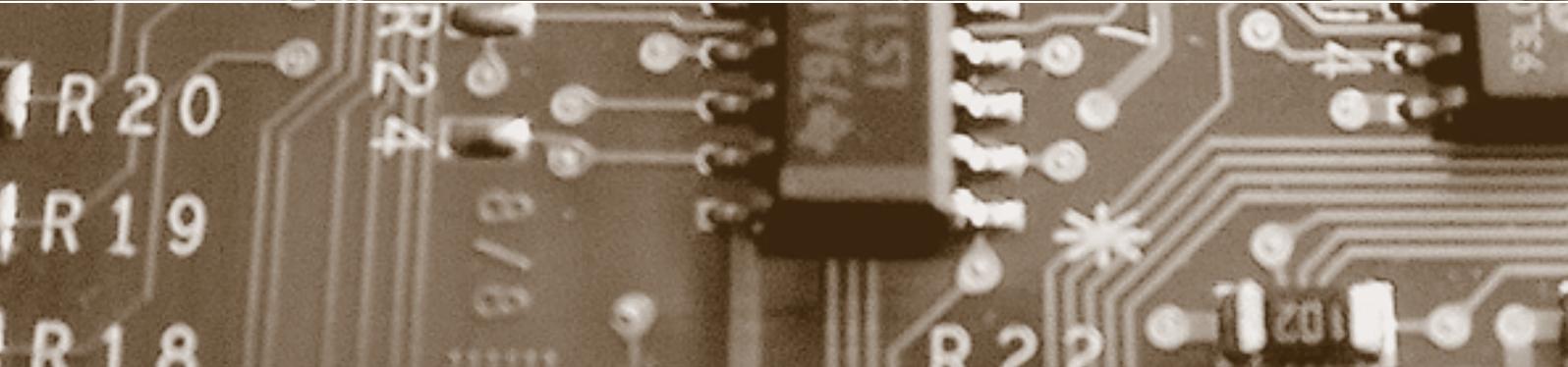
Schwerpunkt:

Sensor-Actor-Netze

fokus: Lagebild für Kritische Infrastrukturen

fokus: Privatsphäre trotz intelligenter Zähler

report: Sicherheit im Cloud Computing



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

fokus

Schwerpunkt:

Sensor-Actor-Netze

auftakt

Prima leben ohne Privatsphäre

Roberto Simanowski Seite 1

Kritikalität von Sensor-Actor-Netzen

von Bernhard M. Hämmerli Seite 4

Lagebild für Kritische Infrastrukturen

von Heiko Borchert/Stefan Brem Seite 6

Schutz der Schweiz vor Cyber-Risiken

von Gérald Vernez Seite 10

Sicherheit im Energienetz der Zukunft

von Sven Garrels Seite 14

PET – ein Konzept harrt der Umsetzung

von Bruno Baeriswyl Seite 18

Privatsphäre trotz Intelligenter Zähler

von Markulf Kohlweiss und Lothar Fritsch Seite 22

Für den Schutz Kritischer Infrastrukturen (SKI) ist der regelmässige Austausch von Informationen zwischen Behörden und Unternehmen unerlässlich. Dieser könnte in einem SKI-relevanten Lagebild gebündelt und aufbereitet werden. Darin können Behörden und Betreiber Informationen zum Schutz Kritischer Infrastrukturen bündeln und die Koordination im Hinblick auf Schutzmassnahmen verbessern.

Lagebild für Kritische Infrastrukturen

Durch den vermehrten Einsatz von ICT und der damit verbundenen erhöhten Anzahl von Schnittstellen im Energienetz entstehen neue Sicherheitsrisiken in Bezug auf Netzverfügbarkeit, Systemintegrität und Datenschutz. Ein Sicherheitskonzept für das intelligente Stromnetz der Zukunft sollte frühzeitig geplant werden.

Sicherheit im Energienetz der Zukunft

Mit «Privacy Enhancing Technology» (PET) sollen neue Anwendungen «datenschutzverträglich» gemacht werden. Die inhärenten Zielkonflikte können nur aufgelöst werden, wenn neben der Technik auch das Datenschutzrecht in die Betrachtung einbezogen wird.

PET – ein Konzept harrt der Umsetzung

Intelligente Zähler versprechen eine bessere Ausnutzung vorhandener Infrastruktur für Netzbetreiber und erhöhte Transparenz für Konsumenten. Kann die Privatsphäre im eigenen Heim bedingungslos geschützt werden, oder folgt auf den gläsernen Mobilfunkkunden nun der gläserne Stromkunde?

Privatsphäre trotz Intelligenter Zähler

impresum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: 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

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (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, 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 19, Fax +41 (0)44 200 29 08, www.schulthess.com, zs.verlag@schulthess.com

Sicherheit im Cloud Computing

Obwohl in den Medien intensiv über Cloud Computing und entsprechende ökonomische Vorteile berichtet wird, werden die latent vorhandenen Sicherheitsprobleme meist verschwiegen bzw. ignoriert. Muss man den Cloud-Anbietern einfach vertrauen?

E-Learning: Kryptografie und -analyse

Das Open-Source-Projekt CrypTool (CT) hat sich die Aufgabe gestellt, Kryptografie und Kryptoanalyse mit Beispielen und Visualisierungen so darzustellen, dass man ein gutes Verständnis und Awareness für IT-Sicherheit erreicht.

Familie und Arbeitsplatz: heikle Ortung

Location Based Services sind heikel oder unzulässig, wenn sie der Überwachung von Kindern und Arbeitnehmenden dienen. Die gesetzliche Vertretung ist bei älteren Kindern meist nicht befugt, an deren Stelle die Einwilligung zur Datenbearbeitung zu erteilen. Das Arbeitsrecht schränkt die Überwachung von Arbeitnehmenden erheblich ein.

EU: Zu neuen Ufern lockt ein neuer Tag?

Die EU-Kommission hat Entwürfe für eine «Regulation» und eine «Directive» zur Vereinheitlichung des Datenschutzrechts vorgelegt. Mit dem darin enthaltenen «right to be forgotten» und dem Strafenkatalog würde ein bedeutender Schritt in Richtung Harmonisierung des Datenschutzrechts getan. Es ist zu hoffen, dass der Gedanke der Entwürfe in der definitiven Fassung immer noch zu erkennen sein wird.

Aus den Datenschutzbehörden

Wer ist neu zur Datenschutzbeauftragten gewählt worden? Welche Themen haben Datenschutzbehörden im letzten Quartal bearbeitet? Die Unterrubrik berichtet über Personelles und Aktuelles aus der Datenschutzszene.

report



Sicherheit

Sicherheit im Cloud Computing

von Rolf Oppliger

Seite 28

Lernen

E-Learning:

Kryptografie und -analyse

von Bernhard Esslinger/Sibylle Hick Seite 32

Follow-up: Location Based Services

Familie und Arbeitsplatz: heikle Ortung

von Daniel Kettiger

Seite 36

Rechtsentwicklung

EU: Zu neuen Ufern lockt ein neuer Tag?

von Sandra Husi-Stämpfli

Seite 38

Transfer

Private Smartphones im Geschäftsumfeld

von Roland Portmann

Seite 42

forum



privatim

Aus den Datenschutzbehörden

von Sandra Husi-Stämpfli

Seite 44

ISSS

Jahresprogramm ISSS 2012

von Ursula Widmer

Seite 45

ISSS

Wie sicher sind «sichere» IT-Systeme?

von Sonja Hof

Seite 46

agenda

Seite 47

schlussstakt

In der Gratis-Falle

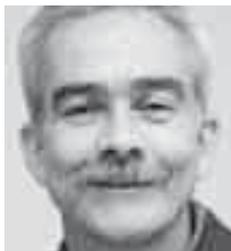
von Bruno Baeriswyl

Seite 48

cartoon

von Reto Fontana

Familie und Arbeitsplatz: heikle Ortung



Daniel Kettiger,
Mag.rer.publ.,
Anwalt und
Berater, Bern
info@kettiger.ch

digma 2011.2 befasste sich mit Location Based Services (LBS)¹. Eine Unterkategorie bilden die *Location-Sharing-Systeme*, deren hauptsächlichster Zweck die Ermittlung, Auswertung und Darstellung der Standortdaten des mobilen Endgeräts ist². Es bestehen weltweit über 90 solche Angebote³. Besonders heikel ist bei solchen Systemen der Persönlichkeitsschutz von Kindern sowie von Arbeitnehmerinnen und Arbeitnehmern⁴. Darauf weist u.a. ein Bericht einer Arbeitsgruppe der EU⁵ hin.

Kinder

Location Sharing Services eignen sich zur *Überwachung der Standorte von Kindern* und werden diesbezüglich beworben⁶. Untersuchungen zeigen auf, dass Eltern gerade darin den hauptsächlichsten Nutzen von Location-Sharing-Systemen sehen⁷. Es stellen sich somit Fragen des *innerfamiliären Persönlichkeitsschutzes*⁸.

Informationelle Privatheit dient dem Schutz von Identität, Gefühlswelt und Menschenwürde; sie ist für das menschliche Dasein existenziell⁹. Es geht u.a. darum, einen autonomen Bereich der Lebens- und Beziehungsgestaltung zu schützen, in dem die einzelne Person ihre Individualität entwickeln, entfalten und erhalten kann. Die von Art. 27 ff. ZGB geschützte Persönlichkeit umfasst mithin die Freiheit der persönlichen Lebensgestaltung sowie die

Möglichkeit jeder Person, ihre sozialen Bindungen (auch Freundschafts- und Intimbeziehungen) autonom zu gestalten¹⁰. Fremdbeobachtung beeinträchtigt beides erheblich¹¹. Die elterliche Sorge schränkt die autonome Lebens- und Beziehungsgestaltung bei unmündigen Kindern und Jugendlichen ein. Das Kind darf u.a. ohne Einwilligung der Eltern die häusliche Gemeinschaft nicht verlassen (Art. 301 Abs. 3 ZGB). Die Eltern bestimmen über den Aufenthalt ihres Kinds und haben somit ein berechtigtes Interesse, diesen zu kennen. Sie müssen sich allerdings bei der Erziehung ihres Kinds vom Kindeswohl leiten lassen (Art. 301 Abs. 1 ZGB) – ihre elterliche Sorge endet dort, wo das Kindeswohl verletzt wird¹². Sie müssen zudem dem Kind die seiner Reife entsprechende Freiheit der Lebensgestaltung gewähren und in wichtigen Angelegenheiten, soweit tunlich, auf die Meinung des Kinds Rücksicht nehmen (Art. 301 Abs. 2 ZGB). Dies gilt auch für die dem Kind ausserhalb des elterlichen Haushalts zu gewährende Bewegungsfreiheit und Kontaktfreiheit ohne Beobachtung.

Bezüglich der für die Abon- nierung bzw. Nutzung eines Location Sharing Services notwendigen *Einwilligung* sind die Eltern grundsätzlich befugt, das Kind zu vertreten (Art. 304 Abs. 1 ZGB), allerdings nur so weit, wie dies im Interesse des Kinds ist¹³, d.h. für dieses aus

objektiver Sicht nutzbringend ist und seinen Interessen nicht zuwiderläuft¹⁴. Weil die Einwilligung zu einer Persönlichkeitsverletzung ein höchstpersönliches Recht ist und hierfür die Urteilsfähigkeit des Kinds unabhängig von dessen Mündigkeit genügt (Art. 19 Abs. 2 ZGB), ist die gesetzliche Vertretung nur so weit zulässig, als das Kind *habituell urteilsunfähig* ist¹⁵. Eine vertretungsweise Einwilligung für urteilsfähige Unmündige oder Entmündigte in eine Persönlichkeitsverletzung ist deshalb unzulässig¹⁶. Entspricht der Reifegrad eines Kinds nicht der Urteilsfähigkeit zur Einwilligung in eine Persönlichkeitsverletzung, aber derjenigen zur Verweigerung des Eingriffs, geht die Verweigerung des Kinds der Einwilligung der gesetzlichen Vertretung i.d.R. vor¹⁷.

Ab 12–14 Jahren sind Kinder zu ihrer notwendigen, altersgemässen, physisch und psychisch gesunden Entwicklung zunehmend auf mehr Freiheit in ihrer Lebensgestaltung und ihrer Beziehungspflege angewiesen¹⁸. Ab diesem Alter dürfen daher die Eltern weder stellvertretend für die Kinder die Einwilligung zur Nutzung eines Location-Sharing-Systems (und damit wohl implizit zum Zugriff auf die Daten der aktuellen Standorte) geben noch das Kind gegen seinen Willen zwingen, ihnen Zugriff auf die Standorte in einem von ihm abonnierten bzw. genutzten Location-Sharing-System zu bewilligen.

Wenn Eltern auf einem Endgerät, das vom Kind genutzt

wird, ohne dessen Einwilligung heimlich Software installieren, erfüllt dies in der Regel den Tatbestand des unbefugten Eindringens in ein Datenverarbeitungssystem (Art. 143^{bis} StGB).

Bei Kindern und Jugendlichen, welche eine Berufslehre oder ein Praktikum absolvieren, kann die Bekanntgabe von Daten über deren Standort während der Arbeitszeit das Fabrikations- und Geschäftsgeheimnis des Lehrbetriebs verletzen.

Arbeitnehmende

Art. 328 OR verpflichtet die Arbeitgeberin bzw. den Arbeitgeber, die Persönlichkeit der Arbeitnehmenden zu achten und zu schützen; dies betrifft auch die Zulässigkeit von

Überwachungsmassnahmen am Arbeitsplatz¹⁹. Zudem regelt Art. 26 ArGV 3 die Überwachung am Arbeitsplatz; Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmenden am Arbeitsplatz überwachen sollen, dürfen nicht eingesetzt werden (Art. 26 Abs. 1 ArGV 3). Aus anderen Gründen erforderliche Überwachungs- oder Kontrollsysteme sind so auszugestalten, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmenden dadurch nicht beeinträchtigt werden (Art. 26 Abs. 2 ArGV 3). Gemäss bundesgerichtlicher Praxis ist der Einsatz von Lokalisierungssystemen zur Überwachung von Aussendienstmitarbeitenden dann zulässig, wenn diese zu

deren Sicherheit oder zu organisatorischen Zwecken (z.B. effizienterer Einsatz) dienen²⁰ und dem Verhältnismässigkeitsgebot entsprechen²¹. Der Einsatz von Lokalisierungssystemen zur Überwachung der Mitarbeitenden ist demgegenüber verboten²². Eine schriftliche Einwilligung der Arbeitnehmenden ist unbeachtlich, wenn der Verdacht besteht, dass diese nicht freiwillig erfolgte²³.

Der Einsatz von Lokalisierungssystemen zur Überwachung von Mitarbeitenden im öffentlichen Dienst bedarf zudem einer Grundlage in einem Rechtserlass, in der Regel auf Gesetzesstufe (Art. 5 Abs. 1 i.V.m. Art. 36 Abs. 1 BV). ■

Fussnoten

- ¹ Vgl. insb. MARTIN WERNER, Datenschutz in ortsbezogenen Diensten, *digma* 2011, 54 ff.
- ² Vgl. DANIEL KETTIGER, Rechtliche Rahmenbedingungen für Location-Sharing-Systeme in der Schweiz, *Jusletter* vom 9. August 2010, Rz. 4 ff.
- ³ Vgl. JACINE Y. TSAI ET AL., Location-Sharing Technologies: Privacy Risks and Controls, *CyLab*, Carnegie Mellon University, 22 f. (Appendix); WERNER (Fn. 1), 54.
- ⁴ Vgl. KETTIGER (Fn. 2), Rz. 44 ff. und Rz. 50 f.
- ⁵ Vgl. Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, 811/11/EN, WP 185, 16. Mai 2011, 14 ff.
- ⁶ NZZ vom 24.10.2011, 50.
- ⁷ Vgl. TSAI ET AL. (Fn. 3), 16 und 18.
- ⁸ Vgl. REGINA E. AEBI-MÜLLER, Personenbezogene Information im System des zivilrechtlichen Persönlichkeitsschutzes, Bern 2005, Rz. 665 i.V.m. Rz. 740.
- ⁹ Vgl. AEBI-MÜLLER (Fn. 8), Rz. 650.
- ¹⁰ Vgl. AEBI-MÜLLER (Fn. 8), Rz. 665.
- ¹¹ Vgl. AEBI-MÜLLER (Fn. 8), Rz. 652 und 654.
- ¹² Vgl. RAPHAËL HAAS, Die Einwilligung in eine Persönlichkeitsverletzung nach Art. 28 Abs. 2 ZGB, Zürich 2007, 116.
- ¹³ Vgl. AEBI-MÜLLER (Fn. 8), Rz. 235; HAAS (Fn. 12), 116; Opinion 13/2011 (Fn. 5), 15.
- ¹⁴ Vgl. AEBI-MÜLLER (Fn. 8), Rz. 240.
- ¹⁵ Vgl. AEBI-MÜLLER (Fn. 8), Rz. 239; HAAS (Fn. 12), 114 f.
- ¹⁶ Vgl. HAAS (Fn. 12), 104.
- ¹⁷ Vgl. HAAS (Fn. 12), 115.
- ¹⁸ Vgl. Opinion 13/2011 (Fn. 5), 15.
- ¹⁹ Vgl. ROLF A. TOBLER ET AL., Arbeitsrecht, Kommentierte Gesetzesausgabe, Lausanne 2006, Art. 328 OR, Rz. 1.8.
- ²⁰ Vgl. BGE 130 II 425, E. 4; KURT PÄRLI, Datenschutz durch Selbstregulierung, *digma* 2011, 66; AMÉDÉO WERMELINGER, GPS-Überwachung von Mitarbeitenden, *digma* 2005, 96 ff; Opinion 13/2011 (Fn. 5), 14.
- ²¹ Vgl. BGE 130 II 425, E. 4.4 und 5.2 ff.; Opinion 13/2011 (Fn. 5), 14.
- ²² Vgl. BGE 130 II 425, E. 4.4.
- ²³ Vgl. Opinion 13/2011 (Fn. 5), 14.

Kurz & bündig

Location Based Services sind hinsichtlich des Persönlichkeitsschutzes von Kindern und Arbeitnehmenden heikel oder unzulässig, wenn sie zu deren Überwachung dienen. Die gesetzliche Vertretung ist bei älteren Kindern meist nicht befugt, an deren Stelle die Einwilligung zur Datenbearbeitung zu erteilen. Das Arbeitsrecht schränkt die Überwachung von Arbeitnehmenden erheblich ein.

Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (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

Homepage: www.schulthess.com

Schulthess 