

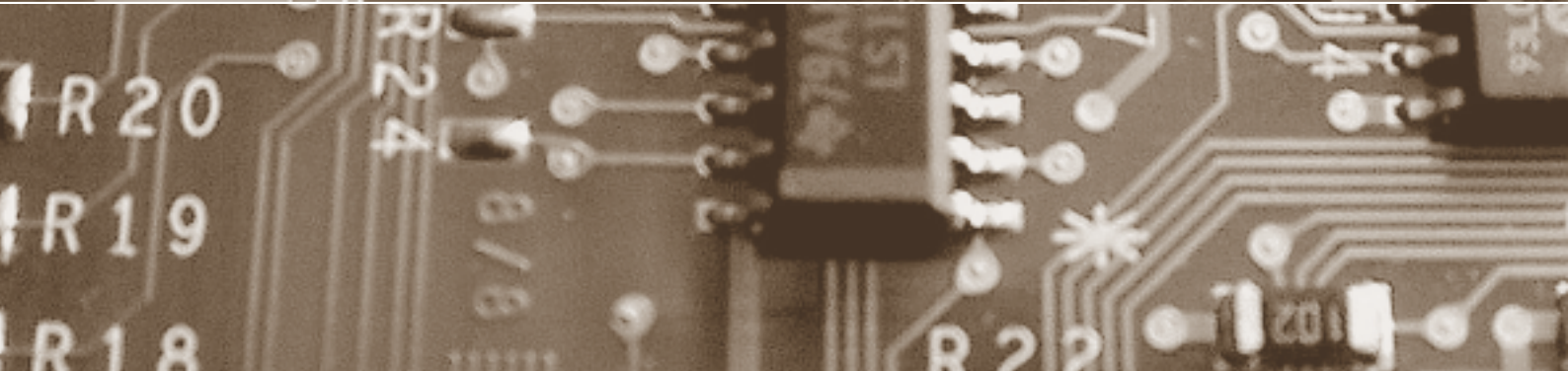
Schwerpunkt:

Mein Ich im Netz

fokus: «Digital Natives» in einer vernetzten Welt

fokus: Wie schütze ich mein virtuelles Ich?

report: Datenschutz in die Prozesse bringen



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

fokus

Schwerpunkt:

Mein Ich im Netz

auftakt

Menschenwürde – ein abwägungsfestes Recht von Jakob Kellenberger

Seite 125

Haben Sie auch schon 345923 Freunde? von Beat Rudin

Seite 128

«Digital Natives» in einer vernetzten Welt von Daniel Süss

Seite 130

Das «persönliche» Internet von Marc Langheinrich und Günter Karjoth

Seite 134

Wie schütze ich mein virtuelles Ich? von Roland Mathys und Lukas Abegg

Seite 140

Verteilte Nutzungskontrolle

von Manuel Hilty, Alexander Pretschner und David Basin

Seite 146

Jugendliche wachsen mit dem Internet auf und nutzen die Chancen, die es bietet. Wie lernen sie, mit den Risiken der virtuellen Welt umzugehen? Der Artikel beleuchtet die Mediennutzung durch Heranwachsende zwischen unbekümmerter Neugierde und gefährlicher Enthemmung.

«Digital Natives» in einer vernetzten Welt

Mit zunehmender Möglichkeit, sich im Internet zu präsentieren, steigt für das virtuelle Ich die Gefahr, in Mitleidenschaft gezogen zu werden: Wie kann man sich wirksam gegen unliebsame Darstellungen über die eigene Person schützen?

Wie schütze ich mein virtuelles Ich?

Die Kontrolle über die Nutzung unserer Daten wird immer wichtiger. Die technische Umsetzung aber ist schwierig, die nötigen Mechanismen sind teilweise erst in Entwicklung. Eine zukunftsgerichtete Kontrolle der Datennutzung könnte zum Enabler für existierende und zukünftige digitale Technologien werden.

Verteilte Nutzungskontrolle

impresum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 13239944, 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

Ständige Mitarbeiter: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 123.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

Anzeigenmarketing: Publimag AG, Europastrasse 30, Postfach, CH-8152 Glattbrugg
Tel. +41 (0)44 809 31 11, Fax +41 (0)44 809 32 22, www.publimag.ch, info@publimag.ch

Druck: Schulthess Druck 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, zs.verlag@schulthess.com

**Transfers of
Personal Data from
EU to USA**

Die EU erlaubt die vorbehaltlose Übermittlung von personenbezogenen Daten nur in Drittländer, die ein angemessenes Schutzniveau gewährleisten. Die Autorin – frühere Chief Privacy Officer von Novartis International – legt die Vorteile der Unterstellung unter das Safe Harbor Framework dar.

**Herausforderungen im
Schulumfeld**

Die Vorsteherin der Bildungsdirektion des Kantons Zürich beleuchtet aktuelle Datenschutzherausforderungen im Schulumfeld und weist auf die Wichtigkeit des sparsamen und sorgfältigen Umgangs mit personenbezogenen Informationen hin.

**Ist Mithören
ein strafbares
Abhören?**

Wenn die Bekannte der übers Handy angerufenen Kollegin der Mitarbeiterin des Zahntechnischen Instituts die verbale Auseinandersetzung mit dem Chef mithört ... nicht der Stoff, aus dem die grossen Spionageromane gemacht sind, aber Gegenstand eines Bundesgerichtsentscheides!

**Nicht nur
Beruhigungspillen!**

Warum sollte Peter Krähenbühl sich für seine Rechte wehren, wenn es Stellen gibt, die das tun? Führen Datenschutzbeauftragte etwa zu einer Schwächung des Datenschutzes? Ein Plädoyer dafür, das Wirken und die Wirkung der Datenschutzbeauftragten zu evaluieren.

report

SAFE HARBOR
Transfers of Personal Data from EU to USA
von Joan Antokol **Seite 150**

SCHULE
Herausforderungen im Schulumfeld
von Regierungsrätin Regine Aepli **Seite 156**

SPS 2007
Datenschutz in die Prozesse bringen
von Simon Hubacher **Seite 158**

FORSCHUNG
MASC: Monitoring and Security of Containers
von Jens Ove Lauf **Seite 160**

RECHTSPRECHUNG
Ist Mithören ein strafbares Abhören?
von Amédéo Wermelinger **Seite 164**

RECHTSPRECHUNG
Einschränkung des Auskunftsrechts
von Amédéo Wermelinger **Seite 165**

TRANSFER
IT-Security und Verantwortung
von Endre Bangerter
und Markus Christen **Seite 166**

forum

ISACA
IT Compliance mit
dem IT-Governance-Modell
von Bruno Wiederkehr **Seite 168**

agenda **Seite 171**

schlussstakt
Nicht nur Beruhigungspillen?
von Beat Rudin **Seite 172**

Cartoon
von Hanspeter Wyss

Wie schütze ich mein virtuelles Ich?

Von den (begrenzten) rechtlichen Möglichkeiten, Daten über die eigene Person im Internet zu kontrollieren



Roland Mathys,
lic. iur. et lic. oec.
publ., LL.M.,
Advokat, WENGER
PLATTNER, Basel
roland.mathys@
wenger-plattner.ch

Die Wege, sich im Internet zu präsentieren, werden immer vielfältiger. Doch kann man sich auch wirksam gegen unliebsame Darstellungen über die eigene Person schützen?

Mit der anhaltenden Verbreitung des Internets werden auch immer mehr Bereiche des täglichen Lebens von der digitalen Welt erfasst. Längst hat das Internet Einzug in unser Privatleben gehalten. Die Wege, seine eigene Person im Internet zu präsentieren, vermehren sich täglich. Von digitalen Leserbriefen (Fast Feedback) auf Online-Zeitungsartikel über Diskussionsforen zu (fast) jedem erdenklichen Thema, Blogs oder Portale und Social Network Sites wie MySpace, Facebook oder YouTube bis hin zur eigenen Website bietet das Internet eine kaum mehr überblickbare Vielzahl von Möglichkeiten, sich in der virtuellen Welt einzubringen.

Informationsverbreitung nicht immer erwünscht

Damit verbunden ist zwangsläufig die Preisgabe von Informationen über sich selbst. Ob in einer Diskussion in einem Forum, beim Onlinestellen der Urlaubsfotos oder beim Registrieren in einer Network Community, immer werden Daten offengelegt, die Rückschlüsse auf und über die eigene Person ermöglichen – und dies nicht wie im persönlichen Gespräch nur flüchtig und gegenüber einzelnen Personen, sondern persistent und für die ganze digitale Welt. Was digital veröffentlicht wird, bleibt originalgetreu festgehalten. Jeder Person mit Zugang zum Internet ist es möglich, diese Informationen einzusehen, auszuwerten oder weiterzuverbreiten. Das Individuum kann folglich gar nicht mehr steuern, wem welche Information in welchem Kontext zukommt.

Daraus können sich unliebsame Situationen ergeben: Der Personalchef stösst auf einem Aus-

gehportal auf Bilder der letzten Zechtour oder auf Details über Gemüts- und Gefühlszustände, ausgeplaudert beim Flirten im Chatroom. Umgekehrt ist denkbar, dass unzufriedene Mitarbeiter in anonymen Blogs über Interna des Arbeitgebers berichten oder den eigenen Chef diffamieren. Schule gemacht haben auch Fälle, in denen Schüler ihre Lehrer bewerten oder mit Schmähsclips verunglimpfen.

Schon diese wenigen Beispiele verdeutlichen die Vielfalt an Erscheinungsformen. Die zugrunde liegende Struktur ist allerdings häufig dieselbe. Allgemein begegnet man meist folgenden Konstellationen:

- Angaben über mich und mein Leben oder Fotos von mir erscheinen *ohne meine Zustimmung* im Internet.
- Ich werde auf Seiten Dritter *angeschwärzt* (z. B. Hate-Sites über mich).

Gesetzliche Grundlagen

Um dagegen rechtlich vorzugehen, bedarf es entsprechender Gesetze. Ein spezifisches Internetgesetz existiert in der Schweiz¹ nicht; vielmehr wird das bestehende Gesetzeswerk mit einzelnen Sondernormen auch auf die internetbezogenen Sachverhalte angewendet. Im Folgenden stehen das Datenschutzrecht², das Urheberrecht³ und das Strafrecht⁴ im Vordergrund:

- Das *Datenschutzrecht* gemäss DSG regelt die Beschaffung, Bearbeitung und Weiterverbreitung von Personendaten. Der Begriff der Personendaten muss dabei weit aufgefasst werden⁵: Erfasst werden alle Daten, die es erlauben, auf eine Person Rückschlüsse zu ziehen. Somit fallen etwa auch E-Mail-Adressen oder Nummern von Skype, ICQ und ähnlichen Kommunikationsdiensten unter das DSG. Wer gegen das DSG verstösst, begeht eine Persönlichkeitsverletzung.

- Das *Urheberrecht* gemäss URG gewährt Schutz für Werke mit individuellem Charakter. In Betracht kommen etwa längere Texte, die mehr als nur Alltägliches beinhalten, oder Fotos, die sich durch eine gewisse Einzigartigkeit auszeichnen⁶.



Lukas Abegg, lic.
iur., juristischer
Mitarbeiter, WEN-
GER PLATTNER,
Basel

■ Das *Strafrecht* gemäss StGB schützt die Persönlichkeit im Internet auf zwei Arten: Einerseits wird auf inhaltlicher Ebene geahndet, wer jemanden beschimpft, verleumdet oder in seiner Ehre verletzt. Andererseits werden auf technischer Ebene das unbefugte Eindringen in ein Datenverarbeitungssystem und die unbefugte Datenbeschaffung sanktioniert.

Dürfen Dritte meine persönlichen Angaben verwenden?

Grundsätzlich kann jedermann über seine eigenen Daten herrschen. In welchen Fällen und unter welchen Voraussetzungen die Datenherrschaft entzogen werden kann, wird im Folgenden für die zuvor erwähnten Rechtsgebiete aufgezeigt.

Datenschutzrecht

Gemäss DSG dürfen Personendaten nur rechtmässig beschafft werden. Deren Bearbeitung muss verhältnismässig sein und nach den Grundsätzen von Treu und Glauben erfolgen. Personendaten werden rechtmässig beschafft, wenn dabei keine Rechtsnorm verletzt wird. Gegen den Grundsatz von Treu und Glauben verstösst etwa, wer Daten heimlich beschafft, ohne hierbei eine Rechtsnorm zu brechen. Daraus wird abgeleitet, dass die Datenbearbeitung *transparent* erfolgen muss. Die Datenbeschaffung muss für die betroffene Person erkennbar sein.

Eine Ausnahme vom Grundsatz der informationellen Selbstbestimmung bildet Art. 12 DSG, wonach keine Persönlichkeitsverletzung vorliegt, wenn die betroffene Person die Daten *allgemein zugänglich* gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Der Gesetzgeber dachte hierbei insbesondere an im Telefonbuch oder ähnlichen Verzeichnissen ersichtliche Personalien⁷, also an Fälle, in denen das Zugänglichmachen die eigentliche Intention bildet. Wenn Angaben über die eigene Person grosszügig nach aussen getragen werden, wenn man sich in der Disco von Fotografen der angesagten Ausgehportale wie tilllate.com ablichten lässt oder wenn man seinen Namen und Adresse auf Websites von Clubs und Vereinen offenlegt, liegt gemäss der Regel von Art. 12 DSG keine Persönlichkeitsverletzung vor, wenn diese Daten in der Folge bearbeitet und weiterverbreitet werden.

Unklar ist, ob diese Bestimmung auch für *Blogs oder Foren* gilt, für die man sich zuerst anmelden muss, da die allgemeine Zugänglichkeit der Informationen eingeschränkt wird. Zumindest für den Fall, dass sich jemand nur zum Zweck der Beschaffung von Personendaten registriert, kann diese Regel nach hier vertretener Auffassung nicht mehr gelten, da ein solches

Verhalten gegen die Grundsätze des DSG verstösst⁸.

Die Weiterverwendung der Daten ist nur dann unzulässig, wenn *ausdrücklich* darauf hingewiesen wird. Hiervon kann nicht leichthin ausgegangen werden; ein bloss pauschaler Hinweis genügt kaum⁹.

Ungeachtet Art. 12 DSG bleibt die Schranke, dass eine Bearbeitung *verhältnismässig*, d.h. dem Zweck angepasst sein muss und nach Treu und Glauben zu erfolgen hat. Wer also Bilder von einem Ausgehportal beschafft oder Beiträge von allgemein zugänglichen Websites kopiert, darf diese Daten nur insoweit bearbeiten, als sich dies aus den Umständen der allgemeinen Zugänglichmachung ergibt.

Urheberrecht

Das URG schützt Werke der Literatur und Kunst, wenn eine Schöpfung *Werkqualität* erreicht. Dies gilt nicht automatisch für jeden Text oder jede Fotografie: Zufällige Schnappschüsse oder Fotos, die ohne grosses Arrangement aufgenommen wurden, sowie Kurztexte und Äusserun-

Der Personalchef stösst auf einem Ausgehportal auf Bilder der letzten Zechtour oder auf Details über Gefühlszustände, ausgeplaudert beim Flirten im Chatroom.

gen, wie sie meist in Foren oder digitalen Leserbriefen getätigt werden, erreichen die Werkhöhe oft nicht.

Der Urheber eines geschützten Werks hat das ausschliessliche Recht zu bestimmen, ob und wie das Werk verwendet, bearbeitet oder in ein anderes Werk integriert wird¹⁰. Vorliegend versagt der

Kurz & bündig

Mit zunehmender Möglichkeit, sich im Internet zu präsentieren, steigt für das virtuelle Ich die Gefahr, in Mitleidenschaft gezogen zu werden: Unliebsame Kommentare oder Fotos werden von Personen gesehen, die dies besser nicht zu Gesicht bekommen sollten; oder eigene Beiträge tauchen auf Websites auf, mit denen man nicht in Verbindung gebracht werden möchte. Dagegen rechtlich vorzugehen, gestaltet sich schwierig. Einerseits sind die Gesetze oftmals nicht auf die speziellen Umstände ausgerichtet, die eine Rechtsverletzung im Internet mit sich bringt. Andererseits sind die faktischen Möglichkeiten, persönliche Angaben im Internet zu kontrollieren, meist stark eingeschränkt. So tritt nicht selten der Fall ein, dass wohl eine Rechtsverletzung vorliegt, aber eine praktische Handhabe dagegen schlicht fehlt. Was bleibt, sind eine möglichst weitsichtige Prävention und der vorsichtige Umgang mit Angaben zur eigenen Person.

urheberrechtliche Schutz aber häufig deshalb, weil das *Recht am Werk und das Recht am eigenen Namen oder Bild auseinanderfallen*: Wenn der Urheber nicht mit derjenigen Person identisch ist, die in einem Text erwähnt wird oder auf einem Foto abgebildet ist, kann letztere sich nicht mit den Mitteln des Urheberrechts gegen eine unerlaubte Verwendung zur Wehr setzen.

Bei Persönlichkeitsverletzungen mit grenzüberschreitender Dimension und einem Bezug zur Schweiz ist fast immer (auch) schweizerisches Recht anwendbar.

Insgesamt bildet das URG zur Verhinderung von Persönlichkeitsverletzungen somit eine *stumpfe Waffe*.

Strafrecht

Bei den *Ehrverletzungsdelikten* ist die Verwendung persönlicher Angaben jedenfalls dann unzulässig, wenn diese nur zur Beschimpfung oder Herabwürdigung benutzt werden. Wer sich also öffentlich über den Chef beklagen oder seinem Unmut über einen Politiker Luft machen will, darf hierbei die Grenze zur Beschimpfung oder Ehrverletzung nicht überschreiten.

Die Tatbestände des unbefugten Eindringens in ein Datenverarbeitungssystem und der unbefugten Datenbeschaffung setzen voraus, dass die betroffenen Daten gegen den unbefugten Zugriff *besonders gesichert* sind, was bei den hier besprochenen Fällen meist nicht zutreffen dürfte. Beispielsweise stellt eine Pflicht zur Registrierung in einem Forum oder Blog noch keinen solchen Zugriffsschutz dar. Die unbefugte Datenbeschaffung verlangt zudem eine Absicht, sich mit den beschafften Daten an einem fremden Vermögen zu *bereichern*, woran es bei blossen Persönlichkeitsverletzungen meist fehlen dürfte.

Das StGB stellt überdies das *unbefugte Beschaffen von Personendaten* explizit unter Strafe¹¹. Vorausgesetzt wird hierbei, dass die Personendaten nicht frei, d.h. nur mit Berechtigung zugänglich sind¹², was etwa auf den Privatbereich von Social Network Sites wie MySpace zutreffen dürfte. Geschützt werden aber nur besonders schützenswerte Personendaten und Persönlichkeitsprofile gemäss Art. 3 lit. c und d DSGVO.

Wie gehe ich bei einer Verletzung vor?

Liegt in materieller Hinsicht eine Persönlichkeitsverletzung vor, stellt sich die oft viel problematischere Anschlussfrage, wie dagegen am besten vorzugehen ist.

Wo und nach welchem Recht kann vorgegangen werden?

Für *Zivilsachen* bestimmt im schweizerischen Binnenverhältnis das Gerichtsstandsgesetz¹³, dass Verletzungen des Persönlichkeits- und Datenschutzrechts am Sitz oder Wohnsitz des Schädigers oder des Geschädigten einzuklagen sind. Im internationalen Verhältnis sehen das Lugano-Übereinkommen¹⁴ und das IPR-Gesetz¹⁵ unter anderem einen spezifischen Gerichtsstand am Ort vor, an dem das schädigende Ereignis eingetreten ist. Da eine Persönlichkeitsverletzung primär im näheren eigenen Umfeld des Geschädigten wahrgenommen wird, steht einem Betroffenen aus der Schweiz fast immer auch ein schweizerischer Gerichtsstand offen.

Das *anwendbare Recht* bestimmt sich bei einem Vorfall mit internationalem Bezug nach dem IPRG. Hierbei findet nach Wahl des Geschädigten das Recht desjenigen Staates Anwendung, in dem der Schädiger seinen gewöhnlichen Aufenthalt oder der Geschädigte seinen Wohnsitz hat oder wo der Erfolg der Persönlichkeitsverletzung eintrat. In den beiden letzteren Fällen wird jedoch verlangt, dass der Schädiger mit dem Eintritt des Erfolges der Persönlichkeitsverletzung in diesem Staat rechnen musste¹⁶. Wer etwas im Internet veröffentlicht oder aus dem Internet herunterlädt, muss wegen der Ubiquität des Internets grundsätzlich damit rechnen, dass dies auch auf der ganzen Welt einen Erfolg zeitigen kann. Somit ist bei Persönlichkeitsverletzungen mit grenzüberschreitender Dimension und einem Bezug zur Schweiz fast immer (auch) schweizerisches Recht anwendbar.

In *strafrechtlichen Belangen* ist ein Gerichtsstand in der Schweiz gegeben und schweizerisches Strafrecht anwendbar, wenn die Einspeisung des strafbaren Inhalts in der Schweiz stattfand oder wenn der Täter damit rechnen musste, dass besagter Inhalt in der Schweiz abgerufen wird.

Wie kann vorgegangen werden?

Zunächst empfiehlt sich, den *direkten Kontakt zum Schädiger* zu suchen, insbesondere wenn keine eigentliche kriminelle Energie hinter der Verwendung persönlicher Daten steckt. So wird z. B. ein Betreiber von Ausgehportalen, auf denen Fotos der letzten Party aufgeschaltet sind, kaum etwas gegen die Löschung gewisser Bilder einzuwenden haben.

Wenn illegale oder rufschädigende Inhalte auf Websites abrufbar sind, sollte versucht werden, vorweg vom *Provider* eine Löschung zu verlangen¹⁷. Viele Provider verbieten in ihren Nutzungsbedingungen die Aufschaltung rechtswidriger Inhalte, weshalb sie an deren Löschung interes-

siert sind. Faktisch eingreifen kann aber nur derjenige Provider, der auch Kontrolle über den Inhalt der entsprechenden Website hat, d.h. primär der Host Provider. In der Praxis dürfte es an dem für diesen Lösungsansatz erforderlichen einvernehmlichen und kooperativen Handeln aller Beteiligten häufig fehlen: Denn ein Provider mit Sitz etwa in China oder Russland wird allein schon aus sprachlichen Gründen kaum auf ein solches Begehren reagieren. Ausserdem bleibt die Gefahr bestehen, dass der Schädiger den Provider wechselt und mit seinen Machenschaften von vorne beginnt.

Alternativ kann über die Meldestellen für Internetkriminalität und andere Bundesbehörden vorgegangen werden:

- Die nationale *Koordinationsstelle zur Bekämpfung der Internetkriminalität* (KOBIK)¹⁸ bildet zentrale Anlaufstelle für Personen, die verdächtige Internetinhalte melden möchten. Die Meldungen werden nach einer ersten Prüfung und Datensicherung den zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet.

- Die *Melde- und Analysestelle Informationssicherung* (MELANI)¹⁹ bietet vor allem technische Hilfe bei Fragen über Informations- und Datensicherheit sowie ausführliche Informationen zu möglichen Gefahren im Zusammenhang mit dem Internet. Die bei MELANI eingehenden Meldungen werden nicht an andere Behörden weitergeleitet. Stattdessen erhält die meldende Person professionelle Beratung, wie sie gegen den gemeldeten Verstoss vorgehen und sich zukünftig davor schützen kann.

- Der *Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte* (EDÖB)²⁰ überwacht in erster Linie Behörden und Private, die Datensammlungen anlegen. Für das betroffene Individuum stellt der EDÖB lediglich eine Vielzahl von Informationen wie Musterbriefe und Informationsbegehren zur Verfügung. Die Untersuchung und Verfolgung möglicher Persönlichkeitsverletzungen zählen nicht zu seinen Kernaufgaben.

Stösst man beim Betreiber einer Website oder bei dessen Provider auf taube Ohren und bringt auch ein Vorgehen über die erwähnten Bundesbehörden keinen Erfolg, muss auf *gerichtliche Hilfe* zurückgegriffen werden:

- *Zivilrechtlich* sieht das DSG die Möglichkeit vor, gerichtlich insbesondere die Berichtigung falscher Angaben sowie die Löschung oder Sperrung von Daten zu beantragen, damit diese nicht mehr an Dritte weitergegeben werden können²¹. Das Verfahren ermöglicht den Erlass vorsorglicher Massnahmen, die auf eine schnelle vorläufige Anspruchsdurchsetzung abzielen.

- Bei den *strafrechtlichen* Massnahmen muss unterschieden werden, ob ein Delikt nur auf Antrag oder von Amtes wegen verfolgt wird: Straftatbestände wie Beschimpfung, Verleumdung, Ehrverletzung, unbefugtes Eindringen in ein Datenverarbeitungssystem und der spezielle Datenschutzstrafatbestand bilden Antragsdelikte. Der Strafantrag muss bei der zuständigen Behörde deponiert werden. Wo genau und in welcher Form das zu geschehen hat, bestimmt sich nach der anwendbaren kantonalen Strafprozessordnung, wobei die Anforderungen an die Begründung des Strafantrags unterschiedlich hoch sind. Die unbefugte Datenbeschaffung hingegen ist ein Officialdelikt und wird auf Hinweis von Amtes wegen verfolgt.

Gegen wen soll vorgegangen werden?

Grundsätzlich ist derjenige für eine Widerrechtlichkeit verantwortlich, der diese kausal verursacht hat. Konkret heisst dies, dass primär

Zunächst empfiehlt sich, den direkten Kontakt zum Schädiger zu suchen, insbesondere wenn keine eigentliche kriminelle Energie hinter der Verwendung persönlicher Daten steckt.

gegen denjenigen vorgegangen werden muss, der einen ehrverletzenden oder beschimpfenden Beitrag verfasst oder widerrechtlich Personendaten beschafft, bearbeitet oder weitergegeben hat. In der Praxis stellt dies oft ein Problem dar: Längst nicht jede Website verfügt über ein Impressum, und anonyme oder pseudonyme Einträge in öffentlichen Foren können fast nie identifiziert werden.

Es wurde und wird daher breit diskutiert, ob nicht auch die *Provider* einer gewissen Verant-

Literatur

- MAURER-LAMBROU URS/VOGT NEDIM PETER (Hrsg.), Basler Kommentar zum Schweizerischen Datenschutzgesetz, 2. Auflage, Basel 2006 (zitiert: BSK-DSG-AUTOR).
- NIGGLI MARCEL A./WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar zum Strafgesetzbuch II, Basel 2007 (zitiert: BSK-StGB-AUTOR).
- ROSENTHAL DAVID, Internet-Provider-Haftung – ein Sonderfall?, in: Jung Peter (Hrsg.), Aktuelle Entwicklungen im Haftungsrecht, Bern/Zürich/Basel/Genf 2007, 150 ff.

wortung unterstehen sollen. Die EU erliess im Jahre 2000 die E-Commerce-Richtlinie²², die unter anderem die Verantwortlichkeit der Internet Service Provider regelt. Dabei unterscheidet die Richtlinie nach den verschiedenen Arten von Providern: Wer bloss Zugang zum Internet verschafft (Access Provider), haftet nicht. Wer hin-

desgesetz über den elektronischen Geschäftsverkehr einzuführen, scheiterten an den kontroversen Kritiken in der Vernehmlassung, was den Bundesrat im Jahre 2005 dazu bewog, von der Ausarbeitung eines E-Commerce-Gesetzes abzusehen²³. Somit bleiben lediglich die vorhandenen Rechtsgrundlagen. Ein höchstrichterliches Urteil steht in dieser Frage noch aus. Die Lehrmeinungen gehen überwiegend dahin, dass den Access Provider in aller Regel keine Haftung trifft, während ein Host Provider für rechtswidrige Inhalte, von denen er Kenntnis erlangt, einstehen soll²⁴.

Es wurde und wird daher breit diskutiert, ob nicht auch die Provider einer gewissen Verantwortung unterstehen sollen.

gegen auch Dienstleistungen anbietet (z. B. Proxy Provider) oder gar Websites Dritter auf seinen Servern betreibt (Host Provider), kann rechtlich belangt werden. Host und Proxy Provider müssen rechtswidrige Inhalte, von denen sie Kenntnis haben oder auf die sie aufmerksam gemacht werden, umgehend entfernen oder sperren.

In der Schweiz existiert kein der Richtlinie entsprechendes Gesetz. Bemühungen, ein Bun-

Durchsetzbarkeit als Achillesferse

Selbst wenn eine Persönlichkeitsverletzung gerichtlich festgestellt wird, bleibt die Frage, ob dieses Unrecht wieder gutzumachen ist. Im einfachsten Fall, in dem auf einer Website mit Server und Provider in der Schweiz ein Urheber mit bekannten Personalien etwas Unzulässiges verbreitet hat, lassen sich die Gesetze wohl durchsetzen. Was gilt jedoch, wenn der Server in China steht, der Provider von der Südsee aus

Fussnoten

- ¹ Auf Ausführungen zum ausländischen Recht muss aus Platzgründen verzichtet werden.
- ² Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1). Auf die per 1. Januar 2008 in Kraft tretende DSG-Revision (AS 2007 4983) ist in diesem Beitrag nicht einzugehen.
- ³ Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG, SR 231.1).
- ⁴ Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB, SR 311.0).
- ⁵ BSK-DSG-BELSER, Art. 3 N 3.
- ⁶ Vgl. dazu BGE 130 III 168 («Bob Marley») und 130 III 714 («Wachmann Meili»).
- ⁷ AB 1990 S 142 f.
- ⁸ Vgl. BSK-DSG-RAMPINI, Art. 12 N 13.
- ⁹ BSK-DSG-RAMPINI, Art. 12 N 14.
- ¹⁰ Art. 10 f. URG.
- ¹¹ Art. 179^{novies} StGB.
- ¹² BSK-StGB-VON INS/WYDER, Art. 179^{novies} N 16.
- ¹³ Bundesgesetz vom 24. März 2000 über den Gerichtsstand in Zivilsachen (Gerichtsstandsgesetz, GestG, SR 272).
- ¹⁴ Übereinkommen vom 16. September 1988 über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen (mit Prot. und Erkl.) (Lugano-Übereinkommen, LugÜ, SR 0.275.11).
- ¹⁵ Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht (IPRG, SR 291).
- ¹⁶ Art. 139 Abs. 1 IPRG.
- ¹⁷ Der Name des Betreibers einer Website oder eines Providers kann meist über Dienste wie <www.whois.org> oder <www.nic.com> ausfindig gemacht werden.
- ¹⁸ Vgl. <http://www.kobik.ch>.
- ¹⁹ Vgl. <http://www.melani.admin.ch>.
- ²⁰ Vgl. <http://www.edoeb.admin.ch>.
- ²¹ Art. 15 DSG.
- ²² Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (E-Commerce-Richtlinie).
- ²³ Pressemitteilung des Bundesamtes für Justiz vom 9. November 2005, abrufbar unter: <http://www.admin.ch/cp/d/4371cd9a_1@fwsrvg.html>.
- ²⁴ Vgl. zum Ganzen ROSENTHAL, Rz. 101 ff.
- ²⁵ Ein solcher Anspruch kann etwa aus dem Berichtigungsrecht (Art. 5 DSG) abgeleitet werden.
- ²⁶ Vgl. <www.myonid.de>.
- ²⁷ Vgl. <www.naymz.com>.

operiert und der Urheber der Persönlichkeitsverletzung unbekannt ist? Hier stösst das Recht an seine *Grenzen*. Um die Löschung von Daten auf einem Server im Ausland zu veranlassen, muss mit der ausländischen Behörde zusammengearbeitet werden, was viel Zeit beanspruchen kann. Damit fällt der Sinn einer Klage dahin.

Verfahrensdauer und -kosten bilden weitere Hürden gerichtlicher Verfahren. Zwar kann zivilrechtlich eine vorsorgliche Massnahme beantragt werden, die einstweilig einen Text sperrt oder ein Foto löscht und in der Regel auch innert nützlicher Frist ausgesprochen wird. Allerdings muss nach Erlass der Massnahme eine ordentliche Klage eingereicht und ein ordentlicher Prozess geführt werden, was mit Unkosten in Form von Gerichtskostenvorschüssen und Anwaltshonoraren verbunden ist. Verfahren, die mittels Anzeige (z. B. über KOBİK oder eine kantonale Strafbehörde) eingeleitet werden, sind weniger kostenintensiv, da hier meist auf Staatskosten ermittelt wird.

Wird ein gerichtliches Verfahren angestrengt, sollte nicht nur der Schädiger verpflichtet werden, seine Website anzupassen, da die fragliche Website mit hoher Wahrscheinlichkeit auch auf Proxy-Servern oder in Cache-Speichern in der ursprünglichen Fassung abgerufen werden kann. Das Verfahren würde seinen Zweck nicht erfüllen, wenn lediglich der Urheber einer Persönlichkeitsverletzung verpflichtet wird, diese zu beseitigen, während die bisherige Website bei Suchmaschinen wie Google oder Yahoo abrufbar bleibt. Es wird daher empfohlen, zusätzlich zumindest die *grösseren Suchdienste* in die Pflicht zu nehmen und die umgehende Aktualisierung der entsprechenden Seiten zu verlangen²⁵.

Prävention als Rettungsanker?

Wer den Schutz seiner Persönlichkeit erst nachträglich verlangt, ist dem Risiko ausgesetzt, diesen nicht zu erhalten. Damit steigt die Bedeutung der Prävention im Persönlichkeitsschutz: Wer seine persönlichen Angaben überall und bei jeder Gelegenheit im Internet verbreitet, läuft Gefahr, dass sein Name auf unliebsamen Websites auftaucht oder Bilder von ihm in unpässlicher Lage erscheinen. Sind Informationen einmal im Web eingespeist, können sie tausendfach kopiert und weitergegeben werden. Fotos oder Aussagen in Foren, die einmal von einer Website heruntergeladen wurden und in einem Mailverteiler gelandet sind, können nie mehr gänzlich aus der virtuellen Welt entfernt werden. Das Motto *«Trau, Schau, Wem»* geniesst beim Umgang mit persönlichen Angaben höchste Priorität. Vor jeder Datenbekanntgabe sollte man sich etwa folgende Fragen stellen: Sind meine Angaben wirklich

erforderlich? Ist der Bearbeiter vertrauenswürdig? Werden eine sichere Bearbeitung und die Nichtweitergabe an Dritte garantiert?

Eine andere Möglichkeit der Prävention im Stile von *«Angriff ist die beste Verteidigung»* bieten seit jüngerer Zeit Onlinedienste wie myON-ID²⁶ oder Naymz²⁷. Diese gewähren eine Plattform, sich selbst im Internet zu präsentieren. Sie ermöglichen, Links zu Websites, auf denen man erwähnt oder abgebildet ist, zu sammeln und zu kommentieren. Die verschiedenen Tags, die eine Suchmaschine als Treffer liefert, lassen sich sortieren und kanalisieren. Auf diesem Weg kann ein eigentliches Reputationsmanagement mit dem Ziel betrieben werden, dass das selbst erstellte Profil bei den gängigen Suchmaschinen

Aussagen in Foren, die einmal von einer Website heruntergeladen wurden und in einem Mailverteiler gelandet sind, können nie mehr gänzlich aus der virtuellen Welt entfernt werden.

als erster Eintrag erscheint. Damit stossen informationssuchende Personen wie beispielsweise Personalchefs von Anfang an auf die *«richtigen»* und begrüssenswerten Einträge. Aber auch dies kann nicht verhindern, dass ein Personalchef nach weiteren Einträgen und Angaben sucht. ■

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

Homepage: www.schulthess.com

Schulthess 