Deutsches Institut für Vertrauen und Sicherheit im Internet

DIVSI magazin

APRIL 2015

Your Net – DIVSI Convention 2015

Eine Lanze für unsere Jugend

Kongress zur Zukunft der digitalen Welt. 500 Teilnehmer zwischen 16 und 24 Jahren treffen sich in Hamburg. Ministerin Manuela Schwesig ist Schirmherrin

Neue Studie vorgelegt

Die digitale Dimension der Grundrechte: Es gibt Anpassungsbedarf

Hochkarätiges Treffen in Berlin

Der „Digitale Kodex" und das Recht auf Vergessenwerden

Inhalt

3 Editorial
Die digitale Welt und der letzte Hort des Analogen

SCHWERPUNKT „INSIDE DIVSI“

4 Eine Lanze für unsere Jugend
Aufräumen mit Vorurteilen, Ideen sammeln, Anregungen geben

5 Anmeldungen jetzt möglich: „Your Net – DIVSI Convention 2015“
Bundesministerin Manuela Schwesig ist Schirmherrin

11 Brauchen wir einen Lösch-Kodex?
Verlieren kleinere Anbieter nach dem Urteil des EuGH ihre wirtschaftliche Grundlage?

14 Ein Pflock, Vollpfosten und der richtige Weg
Info-Veranstaltung im Rahmen des DIVSI-Projekts „Digitaler Kodex“

16 Vertrauen ist gut – (wann) ist Kontrolle besser?
Meeting des Zukunftsforums Öffentliche Sicherheit

19 Schwächstes Glied ist oft der Mensch
Das IKT-Nutzerverhalten hat grundlegenden Einfluss auf Datensicherheit

22 Es gibt Anpassungsbedarf
Die digitale Dimension der Grundrechte – Existenz, Funktion und Grenzen

24 Umparken im Kopf?
Vom blinden Vertrauen zu etwas, dem man eigentlich nicht traut

27 Aktuelle Bücher

Impressum

Herausgeber:
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Matthias Kammer, Direktor
Mittelweg 110B
20149 Hamburg

Chefredaktion:
Jürgen Selonke (V.i.S.d.P.)

Autoren: Matthias Kammer, Dr. Till Kreutzer, Verena Mummert, Carsten J. Pinnow, Dr. Sönke E. Schulz, Dr. Göttrik Wewer

Realisierung:
Lohrengel Mediendesign
Schulterblatt 58
20357 Hamburg

Verbreitete Auflage:
ca. 7.500 Exemplare, Abgabe kostenlos

Titel: BigLike Images – Shutterstock

Haben Sie Fragen oder wünschen weitere Informationen?

Web: www.divsi.de
E-Mail: info@divsi.de

Anfragen DIVSI magazin:
Michael Schneider,
Leitung Kommunikation
Tel.: + 49 40 226 369 895
E-Mail: michael.schneider@divsi.de
E-Mail: presse@divsi.de

Wissenschaftliche Leitung:
Joanna Schmölz
Tel.: + 49 40 226 369 896
E-Mail: wissenschaft@divsi.de

Die digitale Welt und der letzte Hort des Analogen

Lassen Sie mich ausnahmsweise monothematisch sein. Immerhin drehen sich sieben Seiten dieses Magazins um eine Veranstaltung, die DIVSI seit Monaten in Atem hält. Noch roundabout 60 Tage, dann wird Matthias Kammer die „Your Net – DIVSI Convention 2015" eröffnen. Dabei treffen sich junge Menschen zwischen 16 und 24 Jahren zu einem Kongress, bei dem sich alles um Themen der digitalen Welt dreht. Der DIVSI-Direktor bricht denn auch „Eine Lanze für die Jugend" (ab S. 4). Anlass und Ziel für das Meeting lässt sich problemlos mit Aussagen umreißen, die mehr oder weniger prominente Menschen irgendwann von sich gegeben haben sollen.

Johann Wolfgang von Goethe jedenfalls hat schon damals gewusst, warum DIVSI die nachwachsende Generation am Herzen liegt: „Das Schicksal jedes Volkes und jeder Zeit hängt von den Menschen unter 25 Jahren ab." Willy Brandt hätte ihm zugestimmt: „Wir brauchen die Herausforderung der jungen Generation, sonst würden uns die Füße einschlafen."

Gleichzeitig sollte die ältere Generation sich manchmal etwas zurücknehmen und Jüngeren mehr zutrauen. Das erkannte Luc de Clapiers Vauvenargues, ein französischer Philosoph, bereits im 18. Jahrhundert messerscharf: „Die jungen Leute leiden weniger unter ihren Fehlern als unter der Weisheit der Alten."

Wobei sich gelegentlich die Frage stellen lässt: Welche Weisheit? Dies mag ein Zitat belegen, das einer früheren Bundesministerin zugeschrieben wird. Die wurde von ARD-Kinderreportern gebeten, „doch mal ein paar verschiedene Browser, die es gibt", zu nennen. Antwort: „Browser. Was sind'n jetzt noch mal Browser?"

Zugegeben – niemand muss alles wissen. Deshalb gilt auch für sie in Sachen Nichtdurchblick, was der deutsche Maler und Bildhauer Ernst Barlach eigentlich auf junge Menschen gemünzt hat: „Es ist das Vorrecht der Jugend, Fehler zu begehen, denn sie hat genug Zeit, zu korrigieren."

Damit jungen Menschen weniger Fehler auch im Umgang mit den unendlichen Möglichkeiten der digitalen Welt unterlaufen, sollte man vielleicht eine Aussage von Gesche Joost, der Internetbeauftragten unserer Bundesregierung, im Gedächtnis behalten: „Andere europäische Länder investieren viel mehr in digitale Kenntnisse und integrieren das Thema in die Schule. England hat gerade ein neues Fach ‚Computing' eingeführt – in Deutschland herrscht Handyverbot im Klassenraum. Es ist doch absurd, wenn ausgerechnet die Schule der letzte Hort des Analogen und die letzte handyfreie Zone ist! In Deutschland tun viele so, als wäre Internet nur Rumdaddeln. Diese kulturpessimistische Haltung ist fatal."

Auch über Hinweise dieser Art werden die jungen Teilnehmer mit den Experten verschiedener Fachrichtungen beim Kongress sicherlich reden. Auf die Resultate der Diskussionen und Workshops bin ich gespannt. Und neugierig bin ich auf das, was Manuela Schwesig, die Bundesministerin für Familie, Senioren, Frauen und Jugend, ansprechen wird. Sie hat die Schirmherrschaft für „Your Net – DIVSI Convention 2015" übernommen, was die Bedeutung dieser Veranstaltung deutlich unterstreicht.

Jürgen Selonke
Chefredakteur, DIVSI magazin

Anmeldung. Wer dabei sein möchte, der klickt auf www.yournet2015.de

DIVSI CONVENTION 2015
18.–19. JUNI HAMBURG

YourNet

Eine Lanze für unsere Jugend

Aufräumen mit Vorurteilen, Ideen sammeln, Anregungen geben.

Matthias Kammer

DIVSI plant auch 2015 eine Reihe von Veranstaltungen und Veröffentlichungen, die mit Sicherheit bundesweit für Aufmerksamkeit sorgen dürften. Den Auftakt bildete gerade das vierte öffentliche Info-Meeting im Zusammenhang mit dem „Digitalen Kodex" (s. ab Seite 11). Dabei ist das Gesamtbild unserer diversen Aktivitäten in diesem Jahr noch umfassender geworden. Erstmals stellen wir ein Forum speziell für junge Menschen zur Verfügung.

Der bundesweite Kongress zur Zukunft der digitalen Welt wird in Hamburg 500 Teilnehmer zwischen 16 und 24 Jahren versammeln. Die Vorbereitungen laufen bereits seit Monaten.

Warum öffnet sich DIVSI so nachhaltig für die junge Generation? Ich bin überzeugt, dass eine gedeihliche Weiterentwicklung unserer digitalen Zeit zum Nutzen aller generationsübergreifende Initiativen erfordert. Dabei können die Jüngeren durchaus auch von den Älteren lernen – etwa was den sinnvollen Umgang mit dem Internet angeht. Und die reiferen Semester sollten sich von einigen ihrer sorgsam gepflegten Vorurteile befreien.

Uralt-Kritik. Dieser Konflikt ist keine Erfindung unserer Gegenwart. Junge Menschen mussten sich immer für manche ihrer Attitüden Kritik von der Elterngeneration anhören. Daran hat sich im Laufe der Jahrtausende nichts geändert. Dem griechischen Philosophen Sokrates, der 399 v. Chr. starb, wird diese Aussage zugeschrieben: „Die Jugend von heute liebt den Luxus, hat schlechte Manieren und verachtet die Autorität. Die jungen Leute widersprechen ihren Eltern, legen die Beine übereinander und tyrannisieren ihre Lehrer."

Heute würde dieser große Denker des Altertums die heftige Kritik – wenn er denn der Urheber ist – vielleicht noch so ergänzen: „Außerdem spielen sie permanent mit ihren Smartphones rum und hängen pausenlos im Internet ab!" (s. auch Editorial, S. 3). Ist das so? Die Erfindung von mobilen, internetfähigen Geräten hat dazu geführt, dass das Online-Sein besonders für die nachwachsende Generation vollkommen in den Alltag integriert ist. Gemeinsam mit dem SINUS-Institut haben wir in der U25-Studie das Verhalten von Kindern, Jugendlichen und jungen Erwachsenen in der digitalen →

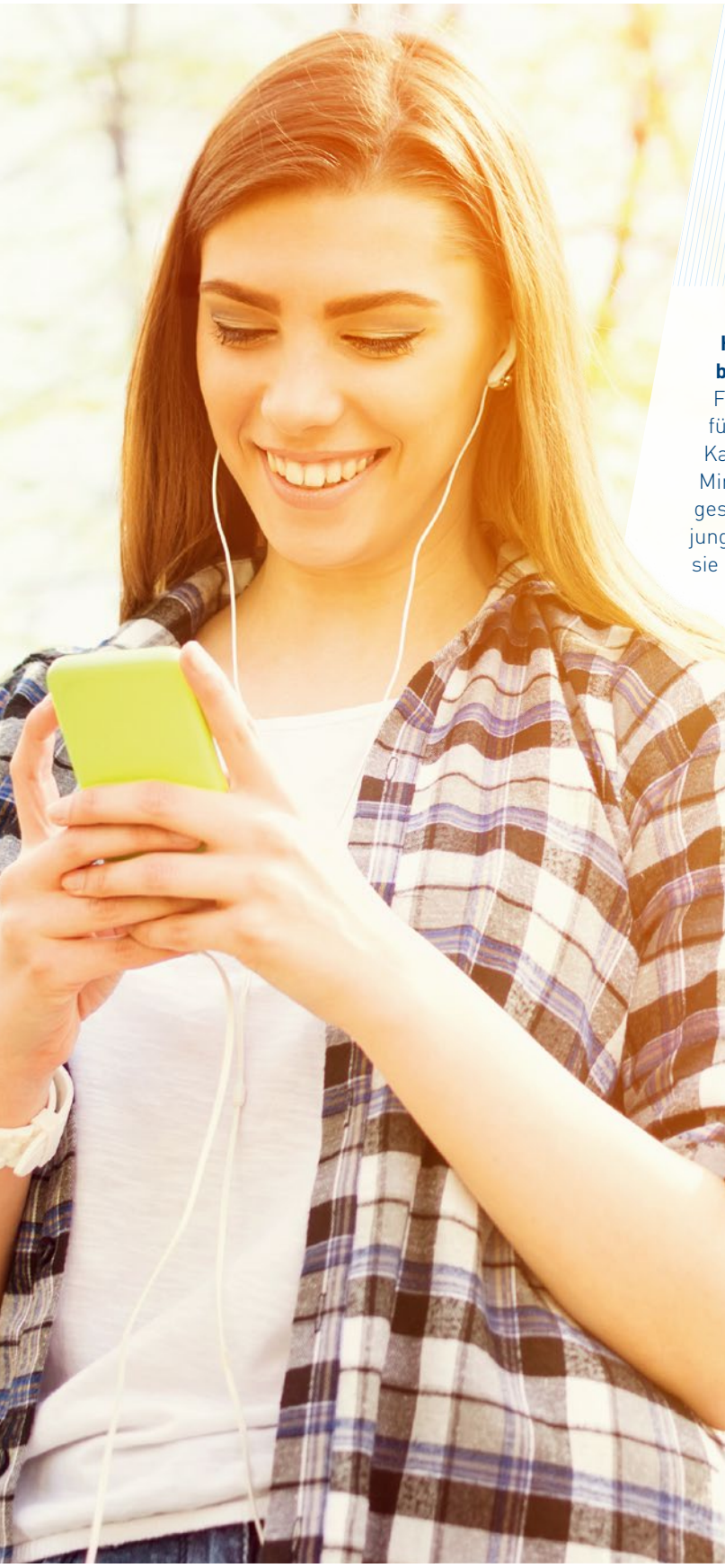
YourNet Experte

Max Schrems

Max Schrems (europe-v-facebook.org), österreichischer Jurist und Bestsellerautor („Kämpf um deine Daten"). Er mischt mit bei der Podiumsdiskussion „Privacy – wie öffentlich möchtest du sein?"

Privatheit ist für fast alle Kinder, Jugendliche und junge Erwachsene ein heißes Thema– insbesondere im Online-Kontext, in dem die meisten einen Großteil ihres Alltags verbringen. Dabei ist ein gewisses Maß an Offenheit bezüglich persönlicher Angaben vor allem in Online-Communitys ein Muss. Risiken werden zwar wahrgenommen, Vertrauensdefizite aber offenbar von der zentralen Bedeutung der Online-Community im Alltag der jungen Menschen und der gewohnheitsmäßigen intensiven Nutzung überlagert.

Always on. Offline sein zu müssen, ist für viele junge Menschen längst eine Notsituation.



Manuela Schwesig

Bundesministerin für Familie, Senioren, Frauen und Jugend

Hohe Anerkennung für „Your Net – DIVSI Convention 2015" bereits im Vorfeld: Manuela Schwesig, die Bundesministerin für Familie, Senioren, Frauen und Jugend, hat die Schirmherrschaft für die Veranstaltung übernommen. DIVSI-Direktor Matthias Kammer: „Über das Engagement und die Unterstützung von Frau Ministerin Schwesig freuen wir uns sehr. Es ist von allgemeinem gesellschaftspolitischem Interesse, zu erkennen, wo der Trend bei jungen Menschen hingeht und welche Erwartungen, welche Ideen sie im Zusammenhang mit dem digitalen Zeitalter haben."

Manuela Schwesig wird die 500 Teilnehmer im Hamburger BeachCenter nicht nur willkommen heißen. Von großem Interesse dürfte für sie auch der Gedankenaustausch im Rahmen der Workshops sein. So, wie die Ministerin bei der Abschlussveranstaltung des YouTube-Wettbewerbs „361 Grad Respekt" unter dem Motto „Was macht dich stark gegen Cybermobbing?" das direkte Gespräch mit den jungen Akteuren gesucht hat.

Dabei würdigte Manuela Schwesig deren Einsatz: „Ich freue mich, mit wie viel Engagement und Kreativität die Jugendlichen mit ihren Videos gegen Cybermobbing Farbe bekennen. Im Internet gibt es viel Ausgrenzung und Beleidigungen, auch Diskriminierung und Hass. Gerade weil sich viele hinter dem Schutz der Anonymität verstecken. Die Jugendlichen setzten ein klares Zeichen: Nein zu Cybermobbing!"

Das Thema Cybermobbing wird auch bei der „Your Net – DIVSI Convention 2015" von Bedeutung sein. Im Workshop „Privat war gestern?!" sollen alle dazu relevanten Fragen angesprochen werden. Manuela Schwesig hat mehrfach darauf hingewiesen, wie wichtig Angebote der Beratung und Aufklärung im Internet sind: „In unserem Zentrum für Kinderschutz im Internet, dem I-KiZ, arbeiten wir daran, den Zugang zu Rat- und Hilfeangeboten zu verbessern. Besonders gut funktioniert Aufklärung aber dann, wenn junge Menschen sie selbst in die Hand nehmen. Denn die Jugendlichen wissen oft am besten, wie sie Gleichaltrige ansprechen können."

Fotos: BigLike Images – Shutterstock, Bundesregierung/Denzel, edition-a

YourNet Expertin

Marina Weisband

Marina Weisband, frühere Politische Geschäftsführerin der Piratenpartei. Sie nimmt teil an der Podiumsdiskussion „Illegal oder legal – Law & Order im Netz“.

Online Musik zu hören, Filme zu schauen und das Hoch- und Herunterladen von Inhalten ist üblich. Dass es sich dabei häufig um rechtliche Grauzonen handelt, ist einem Großteil der 9- bis 24-Jährigen durchaus bewusst. Wo genau liegt die Grenze zwischen Legalität und Illegalität? Wie verändert das Internet die Bedeutung von geistigem Eigentum? Widerspricht das Urheberrecht der Internet-Freiheit oder umgekehrt, in welche Richtung sollte vielleicht eine Angleichung stattfinden? Mit Marina Weisband diskutieren: Prof. Dr. Tobias Keber (siehe Seite 8) und Dr. Florian Drücke (Jurist, Geschäftsführer des Bundesverbandes Musikindustrie e. V.).

→ Welt untersucht. Demnach sind die jungen Leute nicht nur mehr oder weniger den ganzen Tag online – noch härter: Sie empfinden den Zustand, mal offline sein zu müssen, als Notsituation.

Falsche Tendenz. Dennoch – eine pauschale Verdammnis zu ihrem Umgang mit dem Internet wird der jungen Generation keinesfalls gerecht. Auch das belegt die Untersuchung. Ich jedenfalls bin überzeugt, dass die Jugend besser ist als ihr Ruf, auch was das Internet angeht. Und selbst wenn die jungen Menschen in dieser Hinsicht vielleicht manchmal über das Ziel hinausschießen – so what …? Räumen wir also mit Vorurteilen auf.

Bestes Beispiel ist vielleicht der Umgang der jungen Internet-Generation mit dem Begriff „Freund“. Denn dazu hält sich bei uns Älteren beharrlich eine Meinung mit falscher inhaltlicher Tendenz.

Gaming. Da kommt Freude auf. Doch junge Menschen nutzen die Möglichkeiten des Internets weit differenzierter.

Sicherlich wird das Wort „Freund" in Zeiten der sog. sozialen Netzwerke inflationär genutzt. Viele Ältere schütteln darüber den Kopf. Ein Ergebnis der DIVSI-Studie zeigt jedoch: Niemand braucht Bedenken zu haben, dass die jungen Leute leichtfertig damit umgehen, wen sie als „echten Freund" empfinden und nah an sich heranlassen.

Für die Befragten unter 25-jährigen ist es ein wesentlicher Unterschied, einen Freund „nur" zu „adden" oder eine persönliche Freundschaft zu schließen. Populäre Mythen rund um die Unfähigkeit junger Menschen, den Wert von wirklicher Freundschaft zu erkennen, werden dieser Generation nicht gerecht.

Vielmehr differenzieren sie gerade in dieser Hinsicht sehr genau: Facebook-Freunde, Bekannte, echte Freunde. Die Jugendlichen (14– bis 17 Jahre) verfügen im Durchschnitt über 163 Online- →

YourNet Experte

Florian Thalmann

Florian Thalmann, Journalist, der im Mai 2014 einen Selbstversuch unternommen hat: vier Wochen offline! Er ist beim Workshop „Always on – wie möchtest du leben?" dabei.

Mehr als zwei Drittel der Jugendlichen und jungen Erwachsenen sind täglich online. Gleichzeitig ist eine Zukunft ohne Internet für einzelne Milieus durchaus im Bereich des Möglichen, wie die DIVSI U25-Studie gezeigt hat. Dass die Frage, wie ein Leben ohne Internet eigentlich aussehen könnte, für junge Menschen eine Rolle spielt, zeigen zahlreiche Selbstversuche. Frage: Macht das Internet den Einzelnen unabhängiger, oder zwingt es ihn in einen ständigen Bereitschaftsmodus? Wie sieht der „gesunde Mittelweg" aus zwischen Verzicht und Dauerbetrieb?

Fotos: Bastian Bringenberg-marinaslied.de–CC BY 3.0, wavebreakmedia – Shutterstock, privat

YourNet Experten

Tobias Schrödel

Tobias Schrödel, Fachinformatiker, Buchautor („Ich glaube, es hackt!") und vor allem auch Live-Hacker.

Nur 40 Prozent der 14- bis 24-Jährigen sehen die persönlichen Daten im Internet als sicher an. Dennoch glauben 60 Prozent von ihnen, dass ihre persönlichen Daten noch nicht missbraucht wurden. Wie schnell das möglich ist, wird ihnen Schrödel beim Live-Hacking überzeugend demonstrieren. Auf unterhaltsame Weise bringt der IT-Comedian den Zuhörern den wichtigen Bereich Datensicherheit näher. Er erklärt technische Systemlücken und Zusammenhänge für jeden verständlich und lässt dabei auch den Spaß nicht zu kurz kommen.

Dr. med. Bert te Wildt. Er leitet als Oberarzt die Ambulanz der Klinik für Psychosomatik und Psychotherapie des LWL-Universitätsklinikums Bochum. Gabriele Farke, Autorin („Gefangen im Netz") und Website-Betreiberin www.onlinesucht.de). Sie war Bundesvorsitzende des HSO e.V. (Hilfe zur Selbsthilfe für Online-Süchtige).

Sie sind beim Workshop „Wie viel ‚on' ist normal?" dabei. Wo hören Spaß und Entertainment auf, wo fangen Online- und Spielsucht an? (Wie) Muss man die eigene Internet-Nutzung steuern und kontrollieren? Was kann man selbst tun, um sich oder Freunden zu helfen?

Bert te Wildt

Gabriele Farke

Tobias Keber

Prof. Dr. Tobias Keber lehrt an der Stuttgarter Hochschule der Medien (HdM) Medienrecht und Medienpolitik in der digitalen Gesellschaft.

Er leitet den Workshop „Law & Order". Musik und Filme sind massenhaft online zu finden und zu konsumieren – auch ohne notwendigerweise dafür zahlen zu müssen. Die Rechtslage zur Nutzung online verfügbarer Inhalte ist jedoch sehr komplex. Es ist nicht abschließend geklärt, was legal oder illegal und damit potenziell strafbar ist. Fragen also: (Warum) Darf ich streamen, aber nicht downloaden? Welche Strafen drohen für die illegale Nutzung von Online-Gütern?

→ Freundschaften, bezeichnen aber nur elf davon als „wirkliche Freunde". Die jungen Erwachsenen (18 bis 24 Jahre) sind durchschnittlich 175 Online-Freundschaften eingegangen, aber nur neun davon sind enge – wie die ältere Generation formulieren würde – „echte Freunde".

Die Bezeichnung „Freund" ist also zu einem mehrdimensionalen Begriff geworden, mit dessen unterschiedlichen Bedeutungen man sehr sicher und differenziert umgeht. Unverändert macht echte Freundschaft mehr aus als gegenseitig gezeigte Profile in Online-Communitys. Wie seit Urzeiten bedeutet Freundschaft auch für junge Menschen geteilte Interessen, gleiche Werte und verbindende, gemeinsame Erlebnisse im realen Leben.

Verändert hat sich bestenfalls die kommunikative Infrastruktur von Freundschaften, was sich vor allem in

Hilfestellung. Die Möglichkeiten der digitalen Zeit erleichtern in Schule und Job vieles.

neuen Kommunikationsformen äußert. Online-Communitys sind eine selbstverständlich genutzte Austauschform geworden.

Netzwerker. Was den Älteren früher der Beatschuppen war, wird heute ergänzt durch gegenseitige Statusmeldungen und Posts bei Facebook und Co. 74 % der jungen Erwachsenen (18–24 Jahre), 68 % der Jugendlichen (14–17 Jahre) sind mindestens dreimal pro Woche auf Facebook aktiv. Bei den Kindern (9–13 Jahre) sind es bereits 26 %.

Weg also mit dem Vorurteil! Lasst uns als ein Ergebnis der U25-Studie akzeptieren: Facebook-Freunde haben wenig mit dem zu tun, was im Alltag einen Freund ausmacht. Online-Communitys sind Meeting Points für potenzielle Bekanntschaften, aus denen die professionellen Netzwerker – das sind junge Menschen heute – bei Bedarf schöpfen können.

Auch in puncto Privatsphäre ist längst nicht alles so, wie manche Ältere es sich vorstellen. Keinesfalls legt die U25-Generation ihr Intimleben permanent und so freizügig wie nur möglich im Netz offen, so wie dies medial bekannt gewordene spektakuläre Ausnahmen zu signalisieren scheinen. Die Jüngeren assoziieren mit Privatsphäre lediglich anderes als frühere Generationen. Sie halten klassische personenbezogene Daten nicht unbedingt für schützenswert. Dafür jedoch – das gilt jedenfalls für die klare Mehrheit – unbedingt solche Informationen, die ihrer sozialen Reputation schaden könnten.

Privatsphäre bedeutet für Jugendliche und junge Erwachsene vor allem Privatsphäre-Einstellungen in Online-Communitys. Sehr Persönliches oder Intimes gehört für die meisten nicht in die Online-Welt, sondern nach wie vor in ein Vieraugengespräch. Ein gewisses Maß an Offenheit in sozialen Netzwerken wird allerdings als Muss angesehen, wenn man mitspielen will. Für 51 % der Jugendlichen ist der bei Facebook fehl am Platz, der nichts von sich preisgibt. Informationsmanagement – also wem wann zu welchen Inhalten Zugang gewährt wird – ist eine Kernkompetenz, die viele junge Menschen sicher handhaben.

Milieu-Betrachtung. Zeit wird es auch, mit einem fehlerhaften Begriff aufzuräumen. *Die* „Internet-Jugend" gibt es nicht. Zwar sind die 14- bis 24-Jährigen bis auf 2 % sämtlich online. Dieser Status sagt jedoch kaum etwas über ihre Haltung zum und den Umgang mit dem Internet aus. →

Fotos: Jack Frog – Shutterstock, Alexandra Krombholz, Marc-Steffen Unger, privat

Tatort. Das Beach-Center Hamburg ist die Location für „Your Net – DIVSI Convention 2015.

→ Eine konsequente Betrachtung der unterschiedlichen Netzkulturen ist daher notwendig. Die sieben DIVSI U25-Internet-Milieus, gemeinsam mit SINUS entwickelt, machen deutlich, dass die junge Generation in vielen Detailpunkten verantwortungsbewusster handelt, als ihr allgemein unterstellt wird.

Bei aller Unterschiedlichkeit der Milieu-Gruppierungen gibt es ein verbindendes Element der allermeisten U-25-Jährigen – dies ist die generelle Einstellung, wenn man sich einer Grauzone im Netz nähert. Die wesentliche Studienerkenntnis zu diesem Punkt: Erlaubt ist, was alle machen. Vorgenommen werden Risikoabstufungen mit der zentralen Frage: Wie wahrscheinlich ist es, dass ich strafrechtlich belangt werde?

Die meisten jungen Leute sind gegenüber Fragen von Legalität und Illegalität so eingestellt, wie es eine junge Frau im Interview für die Studie unbekümmert formulierte: Selbst „wenn man mal gegen ein Gesetz verstoßen sollte – so schlimm kann das kaum sein, schließlich tun es ja alle".

Kultur der Angst. Hier könnte ein Ansatzpunkt für die ältere Generation gegeben sein: Wir sollten den Jüngeren schon vermitteln, dass eine solche Haltung Risiken birgt. Denn die Logik, „was alle machen, wird schon richtig sein", ist gefährlich und falsch.

Grundsätzlich sollten die Älteren jedoch nicht in den Fehler verfallen, das Internet als „böse" darzustellen, weil vielleicht Unverständnis darüber herrscht, was Kinder, Jugendliche und junge Erwachsene den ganzen Tag über so im Netz machen. Die US-amerikanische Sozialforscherin Danah Boyd sieht die Kritik an der angeblich internethörigen Jugend übrigens ebenfalls als überzogen an. Sie beurteilt die Diskussion als von einer Kultur der Angst geprägt und ist frustriert von dem Denken über die Jugend, dass die Technologie für sie alles viel schlimmer machen müsse.

Ich stimme dem voll zu. Die U25-Generation und wir Älteren sollten versuchen, einen gemeinsamen Konsens zu finden. Die einen sollten vielleicht gelegentlich das Smartphone aus der Hand legen und sich – auch mit den Älteren – einfach nur unterhalten. Und die wiederum sollten nicht allergisch reagieren, wenn die Jüngeren fast permanent ein mobiles Internet-Gerät in der Hand halten.

Solche unterschiedlichen Sichtweisen werden im Rahmen des DIVSI-Jugendkongresses sicher ein Diskussionsthema sein. Ich bin gespannt, wie die Your Net-Teilnehmer diesen Punkt sehen. Und ich bin auch gespannt, welche Anregungen die jungen Menschen uns Älteren insgesamt geben können. Vor allem jedoch bin ich überzeugt, dass nach dem Jugendkongress eine Reihe von Vorurteilen Schnee von gestern sein werden. Und das ist gut so.

Matthias Kammer
ist Direktor des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI).

Your Net Experte

Nico Lumma

Nico Lumma, Co-Vorsitzender von D64, dem Zentrum für digitalen Fortschritt. Er hat sich einen Namen durch Netzkolumnen gemacht und ist beim Workshop „Wem gehört das Internet?" dabei.

Auf das Internet gibt es kein Patent, jeder darf es mitgestalten und sich an seiner Weiterentwicklung beteiligen – so der Grundgedanke. Doch was ist davon geblieben? Funktionieren Konzepte wie Open Source oder auch Wikipedia? Wie sieht das aktuelle Kräfteverhältnis von gemeinschaftlichen bzw. zivilgesellschaftlichen Bestrebungen auf der einen Seite und staatlichen sowie kommerziellen Interessen auf der anderen Seite aus?

Brauchen wir einen Lösch-Kodex?

Nach dem Urteil des EuGH: Bislang mehr als 830.000 Einzelverweise getroffen; 40 Prozent wurden aus den Ergebnislisten entfernt. Aber: Verlieren kleinere Anbieter so ihre wirtschaftliche Grundlage?

Dr. Till Kreutzer

Mit seinem Urteil vom 13. Mai 2014 hat der Europäische Gerichtshof (EuGH) entschieden, dass Google dazu verpflichtet ist, auf Antrag Verweise auf Internet-Seiten aus dem Suchindex zu löschen, auf denen sich persönliche Informationen über den Antragsteller finden. In Reaktion auf das Urteil hat der Suchmaschinenbetreiber ein Formular ins Netz gestellt, das es jedem ermöglicht, einen solchen Löschantrag zu stellen.

Seitdem sind über 230.000 Löschanfragen eingegangen, die mehr als 830.000 Einzelverweise betreffen. Etwa 40 % der beanstandeten URLs wurden aus den Ergebnislisten entfernt. Die Löschungen führen dazu, dass über Namenssuchen bei Google Verbindungen zwischen Personen und Ereignissen nicht mehr hergestellt werden können. Angesichts der erheblichen Bedeutung, die solche Internet-Recherchen heute für die Informationserlangung haben, kann man sagen, dass gewisse Informationen quasi unsichtbar werden, wenn der Verweis hierauf bei Google entfernt wird.

Grundrechtstradition. Das Urteil wurde im Anschluss kontrovers diskutiert. Manch ein Kommentator – vor allem aus politischen Kreisen – sah hierin einen Sieg europäischer Grundrechtstraditionen über einen Internet-Giganten aus den USA. Andere äußerten Bedenken gegen die Entscheidung und ihre Auswirkungen.

In der Tat wirft die Entscheidung viele Fragen auf. Einerseits ist es zu begrüßen, dass Personen eine Möglichkeit gegeben wird, mit einfachen Mitteln persönliche Informationen im Netz mehr oder weniger unauffindbar zu machen. Andererseits können die Löschungen auch erheblich in öffentliche Interessen und Grundrechte eingreifen. Können etwa Politiker ohne Weiteres Verweise auf Skandale tilgen lassen, wird die Wahrnehmung der Geschichte verfälscht.

Pflichten-Druck. Auch ist zu bedenken, dass es wirtschaftliche Auswirkungen auf Verlage oder Blogger haben kann, wenn Links auf werbefinanzierte Inhalte nicht mehr angezeigt werden. Schließlich ist es bedenklich, Suchmaschinenanbietern Pflichten aufzuerlegen, die nur mit erheblichem Aufwand erfüllt werden können. Was für einen Giganten wie Google ärgerlich sein mag, entzieht kleineren Anbietern schnell die wirtschaftliche Grundlage. Unangemessene Prüf- und Löschpflichten drängen kleinere Wettbewerber aus dem Markt und laufen somit dem Ziel zuwider, mehr Wettbewerb bei Suchmaschinen und Aggregatoren zu schaffen.

Im Lichte dieses Spannungsverhältnisses muss nun die Frage beantwortet werden, wie das Urteil des EuGH umzusetzen ist. Das Gericht hat für die Verfahren kaum Regeln aufgestellt. Im Projekt „Braucht Deutschland einen Digitalen →

Ausradiert. Früher war das Löschen einfach. Heute ist es kompliziert.

Fotos: Beach Hamburg, Hayati Kayhan – Shutterstock, privat

→ Kodex" wird daher der Frage nachgegangen, ob es solche Regeln geben sollte, wie sie entstehen, welchen Inhalt sie haben sollten, wie sie wirkmächtig werden und wer an ihrer Entstehung beteiligt werden sollte.

Angesichts der, jedenfalls in manchen Fällen, erheblichen Bedeutung der Löschentscheidungen für öffentliche Interessen sind sich die meisten Kommentatoren einig, dass diese nicht im rechtsfreien Raum ergehen dürfen. Der Umstand, dass Suchmaschinenanbieter wie Google bei grundrechtsrelevanten Fragen als eine Art „Privatgericht" fungieren, ist problematisch genug. Ohne weitere Vorgaben in intransparenten Verfahren getroffene Entscheidungen sind rechtsstaatlich umso fragwürdiger, vor allem, wenn sie nur begrenzt angefochten werden können.

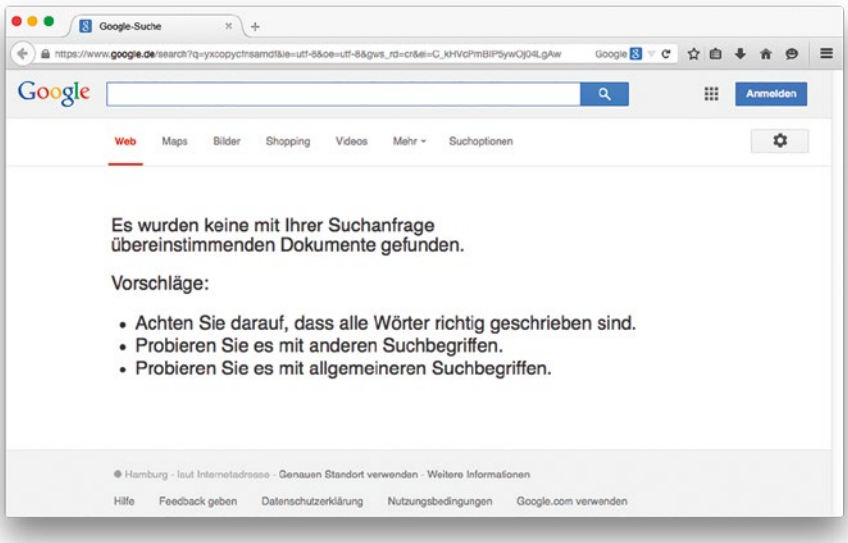
Mindeststandard. Dem könnten Verfahrensregeln entgegenwirken, mit denen rechtsstaatliche Prinzipien sichergestellt werden. Solche könnten einerseits durch Gesetze, andererseits aber auch durch einen Kodex entstehen, der den Suchmaschinenanbietern gewisse Mindeststandards auferlegen würde. Gesetzliche Regeln sind häufig statisch, ihre Einführung dauert lange, und sie sind generell an eine einzige Rechtsordnung gebunden.

Würde nicht die EU solche Regeln aufstellen, sondern die Mitgliedsstaaten, könnten in der Union 28 verschiedene Gesetze entstehen, die jeder Suchmaschinenanbieter einhalten müsste. Google oder Microsoft könnten dies möglicherweise leisten, nicht aber kleinere Anbieter wie Start-ups. Mit anderen Worten: Überkomplexe, territoriale Verfahrensgesetze würden die Marktmacht der großen Anbieter nachhaltig stärken und Wettbewerb verhindern. Eine einheitliche Regelung, die in ganz Europa gilt, wäre daher vorzugswürdig. Eine dementsprechende EU-Verordnung ist jedoch nicht in Sicht, und ihre Verabschiedung würde im Zweifel Jahre dauern.

Vor diesem Hintergrund bietet es sich an, in einem offenen Diskurs einen Verhaltenskodex zum Umgang mit den Löschanfragen auszuhandeln und umzusetzen. Man könnte diesbezüglich von einem „Lösch-Kodex" sprechen.

Der Lösch-Kodex müsste Standards für die Löschverfahren setzen, um die Interessen der Betroffenen zu wahren. Werden solche Regeln im Diskurs ausgehandelt und allgemein anerkannt, wäre zu erwarten, dass die hierauf basierenden Entscheidungen größere Akzeptanz genießen. Allerdings dürfen die Regeln nicht zu großen Aufwand verursachen, und sie müssen flexibel sein. Dies ist notwendig, um unternehmerische Freiheiten zu erhalten und den Effekt zu vermeiden, dass sie von kleinen Anbietern nicht erfüllt werden können.

Verzögerung. In diesem Spannungsverhältnis stellen sich verschiedene Fragen in Bezug auf den Inhalt eines Lösch-Kodex. Beispielsweise in Bezug auf die Beteiligung der potenziell von den Löschverfahren Betroffenen. Da z. B. die Interessen der Publizierenden beeinträchtigt werden, wenn Links nicht mehr gefunden und nicht mehr geklickt wer-



Ergebnislos. Viele Fragen, künftig weniger Antworten.

Löschnutzen. Privat-Peinliches weg – okay. Doch wie ist das mit Verfehlungen etwa von Politikern – auch weg?

den, könnte man erwägen, sie in jedem Fall vor der Entscheidung anzuhören. Ein solcher Prozess wäre indes höchst aufwendig und würde die Verfahren massiv verzögern. Alternativ wäre zu erwägen, den Publizierenden zumindest zu informieren, wenn ein Verweis gelöscht wird. Eine solche Information würde ihm zumindest ermöglichen, gegen die Löschung vorzugehen, vorausgesetzt, er hätte hierfür eine rechtliche Grundlage.

Zweigleisig. Auch diesbezüglich bestehen derzeit jedoch erhebliche Unsicherheiten. Kann ein Verlag sich rechtlich gegen die Entscheidung des Suchmaschinenanbieters wehren, Verweise auf seine Inhalte aus den Suchergebnissen zu entfernen? Google selbst sieht ein solches Verfahren momentan nicht vor. Die Publizierenden werden über die Löschung offenbar nicht einmal informiert. Ob eine Möglichkeit besteht, vor Gericht zu gehen, ist ebenfalls fraglich. Dafür müsste es einen Anspruch geben, in einer Suchmaschine auf bestimmte Weise gelistet zu werden bzw. aus bestimmten Ergebnislisten nicht entfernt zu werden. Ein solcher Anspruch ist nach geltendem Recht ebenso wenig ersichtlich wie – umso weniger – ein Recht von Vertretern des öffentlichen Interesses, etwa zivilgesellschaftlicher Organisationen, Löschentscheidungen anzufechten.

Um den Interessen der Antragsteller, der Öffentlichkeit, der Suchmaschinenanbieter und der Publizierenden gerecht zu werden, könnte ein zweigleisiger Ansatz verfolgt werden. Zum einen könnten gewisse Mindeststandards und zwingende Abwägungskriterien für die Löschentscheidungen des Suchmaschinenbetreibers ausgehandelt und in einem Lösch-Kodex festgelegt werden. Um diese Verfahren nicht mit rechtsstaatlichen Anhörungs-, Transparenz- und Veröffentlichungspflichten zu überlasten, könnte man eine neue Streitbeilegungsinstanz schaffen, in der die Entscheidungen des Suchmaschinenbetreibers überprüft werden könnten. Zu diesem Zweck könnte eine staatliche Schiedsstelle geschaffen werden, an die sich der Antragsteller – wenn die Löschung abgelehnt wird – oder der Publizierende – wenn sie vorgenommen wird – wenden könnten.

Da eine staatliche Stelle gesetzlichen Regelungen unterworfen wäre, wären rechtsstaatliche Vorgaben auf dieser zweiten Ebene gewährleistet. So könnte man den „demokratischen Druck" auf die Entscheidungen der Suchmaschinenbetreiber verringern und den Betroffenen dennoch die Möglichkeit eröffnen, ihre Interessen durchzusetzen. Ein Schiedsverfahren hätte gegenüber etwaigen Gerichtsverfahren den Vorteil, dass es schneller geht, potenziell günstiger ist und die Schiedsstelle mit Personen von besonderer Sachkenntnis besetzt werden könnte. Die Verfahren in zweiter Instanz wären im Zweifel wesentlich effizienter, als wenn immer der Rechtsweg beschritten werden muss. Der Weg zu den Gerichten wäre so zwar nicht ausgeschlossen, würde aber seltener in Anspruch genommen. Hieran hätten alle Beteiligten ein Interesse.

Projektziel. Im weiteren Verlauf des Projekts „Braucht Deutschland einen Digitalen Kodex" werden diese Fragen mit Experten und Akteuren diskutiert. Am Ende sollte ein Ansatz stehen, der einen sinnvollen Umgang mit dem Recht auf Vergessenwerden gewährleistet und der allen Beteiligten gerecht wird.

Dr. Till Kreutzer
ist Partner beim iRights.Lab sowie Redaktionsleiter von iRights.info.

Fotos: David Jacob, clownbusiness/Julian Rovagnati/wellphoto – Shutterstock

Keynote. Sabine Leutheusser-Schnarrenberger über das Vergessen.

Ein Pflock, Vollpfosten und der richtige Weg

Info-Veranstaltung im Rahmen des DIVSI-Projekts „Digitaler Kodex". Spannende Diskussionen im Berliner Meistersaal.

Jürgen Selonke

Beim 4. öffentlichen Diskussionsabend im Rahmen des DIVSI-Projekts „Braucht Deutschland einen Digitalen Kodex?" prallten unterschiedliche Meinungen zum Google-Urteil des EuGH aufeinander. Direktor Matthias Kammer stellte im Berliner Meistersaal eingangs fest: „Die Grundfrage ist positiv beantwortet – wir brauchen einen solchen Kodex. Unsere Lebensrealität ist längst digital. Wir beschäftigen uns jetzt mit konkreten Fragen wie dem Recht auf Vergessenwerden und versuchen Vorschläge dafür zu entwickeln, wie alle Beteiligten unter Berücksichtigung des Urteils künftig miteinander umgehen sollten."

Kammer weiter: „Der EuGH hat mit dem Urteil einen Pflock eingeschlagen. Anfangs waren alle begeistert. Doch bringt uns das Urteil tatsächlich weiter, was bedeutet es in der Praxis?"

Richtungsweisend. Konstantin Klein, Redaktionsleiter Deutsche Welle, nahm das Bild auf: „Ich habe bei der Lektüre des Urteils allerdings nicht an einen Pflock gedacht. Mir ist eher ein Pfosten eingefallen. In der Ausführung, dass die Richter des EuGH einen Vollpfosten haben!"

Klein wies darauf hin, dass trotz der Entscheidung negative Informationen nicht zu unterdrücken seien: „Sie sind jetzt nur schwerer aufzufinden. Wer versucht, unliebsame Erinnerungen vergessen zu machen, sorgt oft unfreiwillig eher dafür. dass sie erinnert werden. So gesehen kann man sich über das Urteil aufregen, gleichwohl ist es aber nur ein Schritt auf einem ganz langen Weg."

Die frühere Justizministerin Sabine Leutheusser-Schnarrenberger unterstrich in ihrer Keynote, dass man Vergessen weder erlernen oder erzeugen noch verordnen kann. Vergessen sei keine dem individuellen oder kollektiven Willen unterliegende Eigenschaft des Menschen. Eine „Tugend des Vergessens" gibt es nicht. Deshalb gehe nach ihrer Ansicht das Urteil einen „deutlichen Schritt" in die richtige Richtung.

Sabine Leutheusser-Schnarrenberger: „Es hat der millionenfachen Verbreitung privater Informationen, auch wenn sie zutreffend sind, einen begrenzt wirkenden Riegel vorgeschoben. Angesichts der engen Voraussetzungen für einen erfolgreichen Anspruch auf Löschung von Links ist die Einschränkung des Zugangs zu Artikeln und Publikationen angemessen. Sie geraten nicht in Vergessenheit, sie bleiben weiter bestehen, aber das Auffinden verlangt etwas mehr Aufwand. Auch das Erinnern will geübt sein."

Auffindung. Weniger positiv bewertete Dr. Ole Schröder (CDU), Parlamentarischer Staatssekretär im Bundesinnen-

Pflock eingeschlagen. DIVSI-Direktor Matthias Kammer zum Urteil des EuGH.

Annäherung. Katharina Borchert (Spiegel Online) und Dr. Ole Schröder (CDU) bewerteten das Urteil.

Diskussionsrunde. Moderator Prof. Dr. Frank Überall (Mitte) mit Jan Philipp Albrecht (MdEP), Jan Kottmann (Google), Michaela Schröder (Verbraucherzentrale) und Konstantin Klein (Deutsche Welle, v.l.) im Berliner Meistersaal.

ministerium, die Entscheidung: „Ich finde das Urteil schwach. Da wird ein sehr komplexes Problem unterkomplex gelöst. Drittbetroffene wie Verlage oder Blogger werden nicht berücksichtigt. Wir müssen viel stärker die Frage diskutieren, wie weit es auch ein Recht gibt, aufgefunden zu werden."

Abwägung. Auch Katharina Borchert, Geschäftsführerin Spiegel Online, kritisierte: „Das Medienprivileg der Presse wird völlig ausgehebelt. Es geht nur noch um die Ansprüche der Betroffenen, aber nicht um die Ansprüche der Publizierenden und auch nicht um die Informationsansprüche der Öffentlichkeit. So kann das nicht der letzte Stand sein."

Jan Kottmann, Leiter Medienpolitik bei Google, hielt sich bei der Bewertung der Entscheidung bedeckt: „Wir konzentrieren uns darauf, das Urteil umzusetzen, und weniger darauf, zu bewerten, ob uns die Diskussion darüber gefällt."

Jan Philipp Albrecht, Stellvertretender Vorsitzender des Innen- und Justizausschusses des Europäischen Parlaments: „Es wurde sehr viel in das Urteil reininterpretiert, was überhaupt nicht drinsteht." Die Suchmaschinenanbieter forderte er auf, eine „verantwortliche Abwägung" bei Löschanträgen vorzunehmen. Albrecht betonte, dass er die Aufregung darüber nachvollziehen könne, wenn solche Anträge etwa von Menschen mit rechtsradikaler Vergangenheit gestellt würden, die ihr Vorleben tilgen wollten. Hier könne ein massiver Eingriff in die Presse- und Informationsfreiheit vorliegen, wenn solchen Anträgen entsprochen werde.

Der Grünen-Politiker wies ergänzend darauf hin, dass sich der EuGH – wie auch in diesem Urteil – durchaus mit Datenschutzfragen beschäftigen könne. Dies sei ein auf europäischer Ebene gestaltbares Rechtsgebiet. Albrecht: „Nicht zuständig ist der Gerichtshof jedoch für Presse- und Meinungsfreiheit." Deshalb sei eine solche Abwägung auch nicht vorgenommen worden.

Michaela Schröder, Datenschutzexpertin beim Bundesverband der Verbraucherzentrale, bemängelte eine fehlende Aufklärung über das Urteil: „Wir mussten viel Arbeit in dieser Hinsicht leisten. Viele Verbraucher dachten anfangs, sie können jetzt einfach alles mal löschen lassen, was ihnen nicht gefällt."

Schiedsstelle. Dr. Till Kreutzer, Partner iRights.Lab, stellte im Rahmen seiner Ausführungen „Das EuGH-Urteil in a Nutshell" fest: „Die Frage ist nicht, ob das Urteil gut oder schlecht ist, sondern wie sich damit umgehen lässt, ohne die Suchmaschinenbetreiber zu überfordern." Gleichzeitig brachte er auch den unterschiedlich diskutierten Gedanken einer Schiedsstelle ins Gespräch (s. seinen Beitrag ab S. 11).

Die Idee einer solchen Schiedsstelle, die beim Streit um Löschanträge vermittelnd zwischen den Suchmaschinenbetreibern, den Antragstellern und Publizierenden eingreifen könnte, ist umstritten. Grundsätzlich wird über einen Vorschlag diskutiert, eine solche Stelle in die EU-Datenschutzverordnung aufzunehmen, die noch in diesem Jahr kommen soll. In den Regularien könne verankert werden, dass auch die Publizierenden in einem Löschverfahren angehört werden. Derzeit spielt sich das Verfahren ausschließlich zwischen den Suchmaschinenanbietern und jenen Personen ab, von denen die Löschung eines Links beantragt wird.

Vorab-Info. Katharina Borchert unterstützte entsprechende Vorstellungen: „Die Informationsfreiheit der Internetnutzer wird derzeit nicht berücksichtigt." Parlamentarischer Staatssekretär Ulrich Kelber (SPD) sprach sich dafür aus, Schiedsgerichte auf europäischer Ebene zu verankern, und: „Publizierende, deren Link gelöscht werden soll, sollten definitiv vorher informiert werden."

Jan Kottmann (Google) dagegen: „Für die Einrichtung einer Schiedsstelle muss ich noch den Mehrwert erkennen." Verbraucherschützerin Michaela Schröder: „Haben wir dann in jedem EU-Land eine Schiedsstelle? Es wäre besser, die Datenschutzbehörden aufzustocken, als Geld in Schiedsstellen zu investieren." Jan Philipp Albrecht (Grüne): „Schiedsstellen sorgen für zusätzliche Bürokratie, die an dieser Stelle nicht notwendig ist."

Das Projekt „Braucht Deutschland einen Digitalen Kodex?" startete DIVSI 2013 in Zusammenarbeit mit dem unabhängigen Berliner Think Tank iRights.Lab. Seit Herbst 2014 läuft die zweite Phase. Dabei wird anhand der Themenbereiche „Recht auf Vergessenwerden" sowie „Big Data" das Konzept eines Digitalen Kodex in der Praxis ausgelotet. Die nächste öffentliche Veranstaltung zu Big Data ist für den 25. Juni in Stuttgart geplant.

Fotos: Stefan Zeitz

Vertrauen ist gut – (wann) ist Kontrolle besser?

Hochkarätig besetzte Veranstaltung des Zukunftsforums Öffentliche Sicherheit.

Verena Mummert

Während eine Fülle an privaten Daten kommerziellen Unternehmen freiwillig zur Verfügung gestellt wird, würden Integrität und Intentionen staatlicher Institutionen gern infrage gestellt. Dabei bräuchten gerade die Nachrichtendienste Vertrauen, Akzeptanz und auch Kontrolle, wenn sie ihre Aufgaben angemessen erfüllen sollen, sagte Dr. Hans-Georg Maaßen, der Präsident des Bundesamtes für Verfassungsschutz, bei einer Veranstaltung des Zukunftsforums Öffentliche Sicherheit e.V. im Deutschen Bundestag.

Eine „Kultur des Misstrauens" zeige sich schon im Vokabular, mit dem die Arbeit der Dienste bedacht werde: etwa „ausspähen" oder „spionieren". Sicherheit sei aber kein Selbstzweck, sondern diene der Freiheit. Und das Sammeln von Informationen durch die Dienste diene nicht kommerziellen Interessen, sondern der Allgemeinheit. Um die öffentliche Sicherheit gewährleisten zu können, müsse manches vertraulich bleiben. Die Dienste bräuchten und verdienten das Vertrauen, da sie trotz möglicher Unzulänglichkeiten, die dort zutage treten können, wo Menschen arbeiten, unter dem Strich gute Arbeit leisteten.

Vertrauenswerte. Zwar vertraut (nach einer Umfrage aus dem Jahre 2013) eine Mehrheit der Deutschen, nämlich jeweils 58 %, dem Bundesnachrichtendienst und auch dem Verfassungsschutz, aber die Polizei (87 %) und die Bundeswehr (82 %) genießen deutlich höhere Werte als die Nachrichtendienste, auch das Bundeskriminalamt (79 %). Das liege sicher nicht nur daran, dass die einen im Geheimen

Fotos: Zukunftsforum Öffentliche Sicherheit e.V.

Expertenrunde. Um Vertrauen in Politik, Sicherheit und Wirtschaft ging es im Bundestag.

arbeiten müssten, während die anderen meist offen aufträten, sagte BKA-Präsident Holger Münch. Kommunikation und Deeskalation stünden bei der Polizei längst im Vordergrund und würden systematisch trainiert.

Wenn die Polizei nicht an Vertrauen verlieren wolle, dann müsse sie ihre Kompetenz auch in der digitalen Welt beweisen. Das sei leichter gesagt als getan. Einer Studie zufolge würden nur 9 % aller Fälle von Cyberkriminalität überhaupt angezeigt und davon wiederum nur 30 % aufgeklärt. Zum einen erforderten die Flüchtigkeit und die Masse der Daten einen enormen Aufwand bei der Auswertung, zum anderen erschwerten die Möglichkeiten, im Netz Identitäten zu verschleiern und Kommunikation zu verschlüsseln, die Strafverfolgung von Tätern. Nur mit den geeigneten Methoden, entsprechend ausgebildetem Personal und einer intensiven Vernetzung all jener, die für die öffentliche Sicherheit zuständig sind, könne es gelingen, das Vertrauen in die Polizei zu erhalten.

Die Veranstaltung des Zukunftsforums, in der es um die Frage ging, wie es um das Vertrauen in Politik, Sicherheitsorgane und Wirtschaft in Deutschland bestellt ist, war hochkarätig besetzt. Neben dem Präsidenten des Bundesamtes für Verfassungsschutz, dem Präsidenten des Bundeskriminalamtes und dem Kommandeur des Zentrums Informationsarbeit der Bundeswehr schilderten auch zwei Abgeordnete des Deutschen Bundestages ihre ganz persönlichen Erfahrungen im Spannungsfeld zwischen Vertrauen und Kontrolle, Freiheit und Sicherheit.

Transparente Politik. Außerdem erläuterte ein Vertreter des Unternehmens, was Google alles unternimmt, um das Vertrauen seiner Nutzer zu erhalten, und ein Kuratoriumsmitglied des Wittenberg-Zentrums für Globale Ethik, auf welches Leitbild für verantwortliches Handeln man sich in der Wirtschaft verständigt hat. Vertrauen sei der wichtigste Vermögenswert eines Unternehmens. Dieser Wert werde maßgeblich durch das Handeln und die Haltung der Führungspersönlichkeiten bestimmt.

Die Politik war in der deutschen Geschichte noch nie so transparent wie heute, auch noch nie so kontrolliert wie heute, stellte Wolfgang Hellmich (SPD) fest, und dennoch wachse das Misstrauen. Das sei nicht immer leicht zu verstehen. Man müsse zwar intensiv kommunizieren, was man im Parlament mache, und das auch begründen, könne aber nicht immer alles sagen, was man wisse, erklärte das Mitglied des Verteidigungsausschusses. Es gebe sensible Themen, die der Geheimhaltung bedürften, wenn die öffentliche Sicherheit nicht gefährdet werden solle. Das deutlich zu benennen, verspreche durchaus Akzeptanz.

Die Mitglieder des Parlamentarischen Kontrollgremiums, das die Nachrichtendienste kontrolliere, seien alle →

Plädoyer. Dr. Hans-Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz, bat um Vertrauen für die Nachrichtendienste.

Standpunkte. MdB Wolfgang Hellmich und MdB Clemens Binninger (rechts).

> Vertrauen ist der wichtigste Vermögenswert eines Unternehmens.
>
> **Dietmar Kokott**
> **Wittenberg-Zentrum für Globale Ethik**

Ausblick. BKA-Präsident Holger Münch und die polizeiliche Kompetenz in der digitalen Welt.

Politikvertrauen. Dr. Sonja Zmerli machte generelle Zusammenhänge deutlich.

→ mit Kanzlermehrheit gewählt, genössen also im Parlament ein sehr großes Vertrauen, betonte Clemens Binninger (CDU). Aber in den Medien werde immer wieder suggeriert, man werde diesem Vertrauen nicht gerecht, sondern von den Diensten an der Nase herumgeführt. Da man nicht alles sagen könne, was man wisse, sei dem schwer zu begegnen. Die Kontrolle durch das Parlament könne der Exekutive bisweilen lästig sein, böte aber auch die Chance, durch eine unabhängige Bewertung der jeweiligen Vorgänge verloren gegangenes Vertrauen wiederherzustellen.

Das Vertrauen in politische Institutionen wie Parteien, Parlamente und Regierungen sei schon immer geringer gewesen als das Vertrauen in rechtsstaatliche Institutionen wie Polizei, Gerichte oder die Verwaltung, stellte Dr. Sonja Zmerli (Goethe-Universität Frankfurt) fest. Das gelte nicht nur für Deutschland, sondern generell. Man könne vermuten, dass das Vertrauen in den Rechtsstaat gewissermaßen die Grundlage sei für ein darauf aufbauendes Vertrauen in die Demokratie.

Wo die Menschen Polizei und Justiz nicht vertrauen würden, blieben sie auch misstrauisch gegenüber der Politik. Die Unterschiede zwischen West- und Ostdeutschland seien zwar geringer geworden, aber nach wie vor erkennbar. Politisches Vertrauen basiere entweder auf einer Art Tauschgeschäft, wo die Bürger zufrieden mit dem sind, was die Politik liefert, oder aber auf gemeinsamen Werten und Normen und einer gemeinsamen Identität. In dem einen Fall seien es eher strategische Überlegungen bzw. positive Erfahrungen, aus denen Vertrauen resultiert, in dem anderen Fall der Eindruck, derselben moralischen Gemeinschaft anzugehören.

Lohnende Hinweise. Die Veranstaltung hat gezeigt, dass es sich lohnt, intensiver darüber nachzudenken, wie das Vertrauen in Politik, Staat und Wirtschaft gestärkt werden kann. Mehr Transparenz und mehr Kontrolle haben nicht zu mehr Vertrauen geführt, jedenfalls Misstrauen nicht abbauen können. Die Vorträge, die in Berlin gehalten wurden, enthalten Hinweise, wie das besser gelingen könnte. Es könnte hilfreich sein, diesen Hinweisen bei passender Gelegenheit noch etwas genauer nachzugehen.

Verena Mummert
ist seit 2013 Geschäftsführerin des Zukunftsforums Öffentliche Sicherheit e.V.

NEWS

Die Zukunft des Internetrechts

Berlin – Breit gefächerte Sommerkonferenz 2015 von Telemedicus.

Um die Zukunft des Internetrechts geht es bei der Sommerkonferenz 2015 von Telemedicus, einem juristischen Internetprojekt zu Rechtsfragen der Informationsgesellschaft. DIVSI unterstützt diese Veranstaltung, die für den 29./30. August in Berlin vorgesehen ist. Tagungsort ist die Hertie School of Governance.

Zum Motto „Zwei Schritte vorwärts: Die Zukunft des Internetrechts" sagen die Macher: „Wir merken, dass wir in einer Zeit leben, in der sich unsere Lebenswelt zunehmend und rasend schnell

Internetrecht. Neues Aufgabenfeld für Justitia.

technologisiert. Selbst erfahrene Telemedicus-Blogger, die seit Jahren über rechtliche Zukunftsthemen schreiben, sind verblüfft, wie krass diese Entwicklungen sich auswirken können und wie nahe Rechtsfragen mittlerweile an Fragen heranreichen, die bisher als Science-Fiction galten. Selbst fahrende Autos, Virtual Reality, Roboterrecht: All dies beschäftigt nicht mehr nur Schriftsteller, sondern auch Rechtsanwälte, Rechtspolitiker – und bald auch Richter. Wir denken, dass es in dieser Situation Sinn macht, nicht nur einen, sondern zwei Schritte vorauszudenken."

Die Diskussionspalette ist groß. Sie umfasst Themen wie „Robotik und Recht", „Sachenrecht trifft Internetrecht", „Regulierung von und über Standards", „Netzneutralität oder Tendenzfreiheit" oder „Die Zukunft des Urheberrechts".

Schwächstes Glied ist oft der Mensch

Das IKT-Nutzerverhalten hat grundlegenden Einfluss auf Datensicherheit.

Carsten J. Pinnow

Unsere Gesellschaft befindet sich derzeit in einer folgenreichen Umbruchphase – nahezu kein Lebensbereich wird sich der Digitalisierung und Vernetzung entziehen können. Das Internet ist zur Lebensader moderner Gesellschaften geworden, denn beinahe alle Bereiche hängen von dessen einwandfreier Funktion ab.

Hier sind insbesondere die kritischen Infrastrukturen zu nennen, also solche Organisationen und Einrichtungen mit besonderer Bedeutung für das staatliche Gemeinwesen. Ihr Ausfall oder auch nur ihre Beeinträchtigung würden existenzgefährdende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder sonstige negative Auswirkungen größeren Ausmaßes hervorrufen.

Neun Sektoren. Die zunehmende Vernetzung und gegenseitige Abhängigkeit dieser kritischen Infrastrukturen birgt zusätzliche Gefahren und lässt Kaskadeneffekte befürchten. Das Bundesministerium des Innern (BMI) gliedert diese kritischen Infrastrukturen in neun Sektoren (Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung, Medien und Kultur).

Sensible Daten. Einloggen ohne Gefahr – der Fingerabdruck als Schutzinstrument.

Aber auch für private Nutzer, für Unternehmen oder andere Institutionen können Ausfall oder Störung des Internets ebenfalls erhebliche schädliche Auswirkungen haben.

Für Verbraucher ergeben sich aus der Nutzung von Internet-Angeboten eine Reihe von Annehmlichkeiten im Alltag: schnelle Informationsrecherche, Pflege sozialer Kontakte über soziale Netzwerke, Beteiligung an Diskussionen, Online-Banking oder Einkaufen auch außerhalb von Ladenöffnungszeiten.

Die steigende Vernetzung birgt indes Chancen und Risiken gleichermaßen. Dies gilt gerade auch für das sogenannte „Internet der Dinge", also die zunehmende Vernetzung von Geräten, die nicht im klassischen Sinne Personal Computers sind. Dazu gehören solche eingebetteten Geräte, die Menschen unmerklich im Alltag unterstützen („Wearables" etc.).

Zunehmend sind Informations- und Kommunikationssysteme wie Computer und mobile Geräte (Smartphones, Tablets) einer Vielzahl von Gefahren ausgesetzt. Dazu zählen Sicherheitslücken in Betriebssystemen und Anwendungen oder Schadprogramme wie Viren, Würmer und Trojaner. Allerdings darf auch und gerade das Fehlverhalten der Nutzer nicht vergessen werden. Die Gesamtsicherheit eines IKT-Systems ist immer nur so stark wie das schwächste Glied der Sicherheitskette – in den meisten Fällen ist der Mensch dieses schwächste Glied!

Restrisiko. Mit den Regeln für Datensicherheit verhält es sich wie mit den Regeln im Straßenverkehr. Sie sind nur dann nützlich, wenn sie auch konsequent beachtet werden. Das Wissen und die Einhaltung sind der eigenen Sicherheit, aber auch der Sicherheit anderer →

Fotos: Alexey Boldin/Jorg Hackemann – Shutterstock.com, Zukunftsforum Öffentliche Sicherheit e.V.

→ dienlich. In beiden Fällen bleibt aber wie so oft im Leben ein Restrisiko. Während für den Straßenverkehr grundlegende Kenntnisse in Kindergärten, Schulen und Fahrschulen vermittelt werden, ist beim Wissen um die Datensicherheit meist Eigeninitiative gefragt.

Längst sind Auswirkungen der eigenen Versäumnisse nicht mehr nur auf einen selbst beschränkt. Digitale Sorglosigkeit bedroht mitunter auch andere, z.B. durch Bot-Netze und Schäden durch den Diebstahl digitaler Identitäten.

80 bis 90 Prozent der Angriffe auf IT-Systeme sind mit vorhandenen Abwehrmaßnahmen abzuwehren – wenn diese konsequent zum Einsatz kommen.

Michael Hange, BSI-Präsident

Diskrepanz. Spätestens seit der sogenannten „Snowden-Affäre" ist das Themenfeld Datensicherheit/Datenschutz für alle Internet-Nutzer in den Fokus gerückt. Umfragen in der Folge dieser Affäre zeigen die Diskrepanz zwischen subjektiver Wahrnehmung von Sicherheit und den eigenen Kenntnissen sowie dem objektiven Risiko, z.B. Opfer einer „digitalen Straftat" zu werden, bzw. den Fähigkeiten, diese zu verhindern.

Einer gemeinsamen Studie der Messe „INTERNET WORLD" und Fittkau & Maaß Consulting zufolge bezeichnet sich gut jeder zweite Internet-Nutzer als sicherheitsbewusst. Fast ein Drittel bewertet den eigenen Kenntnisstand als gut oder sehr gut, nur 3 % stufen ihren Kenntnisstand als gering ein.

Sicherheit ist Bürgern wichtig, jedoch ist kaum jemand bereit, dafür zu zahlen. Hier ist also ein Kulturwandel dringend notwendig! BSI-Präsident Michael Hange betonte im Rahmen der „it-sa 2014", dass 80 bis 90 % der Angriffe auf IT-Systeme mit den vorhandenen Abwehrmaßnahmen abzuwehren seien – diese müssten jedoch auch konsequent zum Einsatz kommen.

Vom BSI wird für Bürger ein Basisschutz empfohlen. Dazu gehören regelmäßige Updates, der Einsatz von Antiviren-/Antischadsoftware, die Nutzung einer Personal Firewall, regelmäßige Back-ups der eigenen Daten, die Abschaltung unnötiger Dienste, möglichst die Verwendung verschlüsselter Internet-Verbindungen (https://), die Nutzung nicht privilegierter Nutzerkonten, die Deinstallation nicht genutzter Programme sowie auch sichere Passwörter.

Browser-Plugin. Ferner sollten Standardkonfigurationen von Betriebssystem und Geräten unbedingt einem Sicherheitscheck unterzogen werden. Viel zu häufig sind Standardkonten mit Standardpasswörtern vorhanden. Häufig ist sogar ein Zugang ohne Passwort möglich. Für die tägliche Arbeit sollten dem Nutzer grundsätzlich so wenig Rechte wie möglich und so viel wie nötig eingeräumt werden!

Browser-Plugins (Erweiterungen) für Multimedia-Inhalte (Adobe Flash etc.) sollten aus Sicherheitsgründen nicht

NEWS

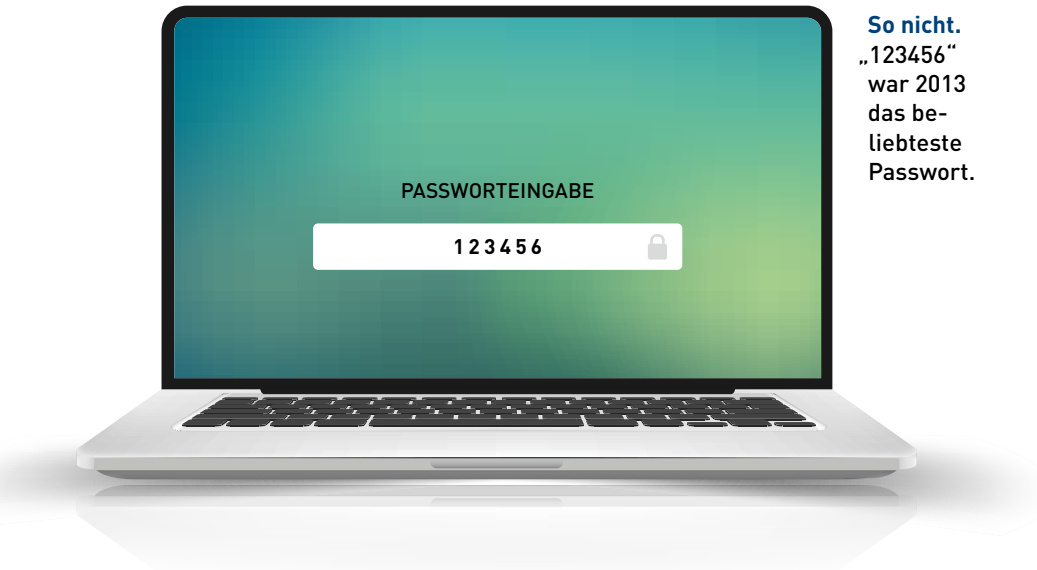
Google gegen StartPage und Duck Duck Go

Hamburg/Erfurt – Suchmaschinen als studentisches Forschungsprojekt.

Mit einer gezielten Projektunterstützung durch DIVSI arbeiten Studenten der Uni Erfurt in der Forschungsgruppe „Zufallstreffer" daran, Erkenntnisse darüber zu gewinnen, welchen Einfluss die personalisierten und stark auf Relevanz ausgerichteten Suchergebnisse bei Google auf den Wissenshorizont der Suchmaschinennutzer haben. Rund 83 % der deutschen Bevölkerung nutzen mindestens einmal wöchentlich eine Suchmaschine.

Teamarbeit. Unterstützung von DIVSI für das Projekt der Erfurter Studenten.

Die Studie soll darüber hinaus klären, ob die voranschreitende Optimierung der Effizienz von Suchmaschinen normativ sinnvoll für den Nutzer ist oder ob nicht offenere Algorithmen, die mehr Vielfalt und auch Zufallstreffer zulassen, eine umfassendere Perspektive über gesellschaftlich relevante Themen bieten können. Hierfür wollen die Studenten die personalisierende Suchmaschine Google mit den nicht personalisierenden Suchmaschinen StartPage und Duck Duck Go vergleichen. Das Forschungsvorhaben läuft im Rahmen einer Bachelorarbeit.



So nicht. „123456" war 2013 das beliebteste Passwort.

automatisch aktiviert werden. Moderne Internet-Browser gestatten es, diese von Fall zu Fall einzuschalten. In letzter Zeit sind immer wieder Sicherheitslücken in diesen Erweiterungen aufgetaucht, die zum Schaden des Anwenders genutzt wurden, bevor vom Hersteller ein Patch (Zero-Day-Exploit) zur Schließung der Lücke zur Verfügung gestellt wurde.

Riesenschaden. Entscheidend ist es, zu verhindern, dass Geräte (PCs, Router, mobile Geräte) zu fremdgesteuerten Bestandteilen eines sogenannten Bot-Netzes werden, das z.B. zu DDoS-Angriffen (Lahmlegen von IKT-Systemen) missbraucht werden kann. Gerade in diesem Bereich hat sich bereits seit Längerem eine regelrechte Schattenwirtschaft etabliert, in der Bot-Netze gekauft, aber auch verkauft werden können.

Solche Attacken sollen Experten zufolge für unter 50 US-Dollar pro Tag zu kaufen sein. Betroffenen, z.B. Online-Händlern, die auf diesen Vertriebsweg angewiesen sind, entstehen nach einer Schätzung der Kaspersky Labs Schäden von 50.000 US-Dollar je Stunde. Haupteinfallswege für Schadsoftware, die den eigenen Rechner zum Teil eines Bot-Netzes werden lassen, sind verseuchte E-Mails und USB-Sticks. Ein gesundes Misstrauen ist ein guter Wegbegleiter für die eigene Sicherheit und damit auch für die Sicherheit anderer!

Schlüsselfaktor. Der Befall durch Malware geschieht bei E-Mails hauptsächlich durch das Klicken auf eingebettete Links oder das Öffnen von Dateianhängen und bei USB-Sticks dadurch, dass Programme automatisch nach Einstecken des Speichersticks zur Ausführung gebracht werden.

E-Mails, die eine Kontenüberprüfung verlangen, große Erbschaften versprechen oder angeblich noch nie gesehene Bilder von Stars zeigen, sollten gelöscht und keinesfalls geöffnet werden. Bei USB-Sticks aus unbekannter Quelle ist ohnehin Vorsicht geboten!

Das Nutzerverhalten ist ein Schlüsselfaktor für ein akzeptables Datensicherheitsniveau insgesamt; daher ist eine ausreichende Sensibilisierung der Anwender dringend notwendig. Sicherheitsfunktionalitäten von IKT-Systemen müssen so bereitgestellt werden, dass Nutzer sie anwenden können und wollen.

Verantwortung in der Digitalen Welt ist von Nutzern, Unternehmen und dem Staat gleichermaßen zu übernehmen!

Carsten J. Pinnow
studierte Elektrotechnik. Er leitet eine Firma für Technologieberatung und ist stellv. Leiter des Arbeitskreises Sicherheit im VDI Bezirksverein Berlin-Brandenburg.

NEWS

Macht, Verantwortung und die digitale Welt

Hamburg – Symposium in der Bucerius Law School.

Um „Neue Macht und Verantwortungsstrukturen in der digitalen Welt" geht es bei einem zweitägigen Symposium, zu dem DIVSI gemeinsam mit der Hamburger Bucerius Law School und dem Lorenz-von-Stein-Institut) einlädt. Termin ist der 7./8. Mai in Hamburg (Jungiusstraße 6). Nach der Eröffnung des Symposiums (Beginn 15.00 Uhr) durch Hamburgs Ersten Bürgermeister Olaf Scholz wird der EU-Abgeordnete und Datenschutzexperte Jan Philipp Albrecht den Stand der Diskussion um die EU-Datenschutzverordnung aufzeigen.

Ehrengast. Olaf Scholz eröffnet das Symposium.

Am Freitag (8.5.) sollen nach der Begrüßung durch DIVSI-Direktor Matthias Kammer (9.00 Uhr) verschiedene Aspekte von Macht und Regulierung, Verantwortung und Teilhabe im digitalen Kontext aus rechtswissenschaftlicher Sicht beleuchtet werden.

Interessenten an dem Symposium können sich ab sofort unter http://bit.do/Bucerius anmelden. Sie erhalten dann von dort das vollständige Programm und den Anmeldelink zugemailt.

Foto: BSI, LiquidLayout – Shutterstock, SPD, Universität Erfurt

Es gibt Anpassungsbedarf

Die digitale Dimension der Grundrechte – Existenz, Funktion und Grenzen.

Dr. Sönke E. Schulz

Eine am Lorenz-von-Stein-Institut durchgeführte Analyse im Rahmen eines vom DIVSI geförderten Projektes konnte die Existenz einer digitalen Dimension der Grundrechte zeigen. Die Etablierung einer (neuen) Kategorie der digitalen Dimension fügt sich in die Grundrechtsdogmatik ein. Sie ist nicht dem Vorwurf ausgesetzt, man habe dies in der Vergangenheit für vergleichbare Entwicklungen nicht getan. Mit dem Internet steht nämlich erstmals eine gesellschaftliche Errungenschaft bereit, die in der Lage ist, nahezu das gesamte menschliche – und grundrechtlich erfasste – Verhalten abzubilden.

Infrastrukturschutz. Neben aktiven Handlungsweisen, von denen exemplarisch nur Online-Predigt und Online-Seelsorge im Rahmen von Art. 4 Abs. 1 GG, reine Online-Versammlungen und -Vereinigungen sowie die Nutzung des Internets im Kontext klassischer Demonstrationen oder Vereine und ihr Schutz über Art. 8 und Art. 9 GG genannt werden sollen, bietet der Grundrechtskatalog den ergänzend notwendigen Infrastrukturschutz. Digitale Grundrechte sind auf digitale Infrastrukturen angewiesen – das Fernmeldegeheimnis sowie das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme stellen Vertraulichkeit und Sicherheit her. Die Verfügbarkeit für jedermann ist im Rahmen einer E-Daseinsvorsorge ebenfalls staatliche Aufgabe.

Digitale Infrastrukturen übernehmen zunehmend die Rolle klassischer Infrastrukturen, sodass die Erweiterung des Grundrechtsschutzes konsequent ist. So wie in der Vergangenheit Art. 13 GG (Schutz der Wohnung) eine räumliche Rückzugsmöglichkeit sicherte, bedarf es digitaler Rückzugsräume. Viele analoge wie auch digitale Grundrechte weisen eine räumliche Dimension auf. Für analoge Handlungsweisen steht – trotz Privatisierungstendenzen – offensichtlich hinreichend öffentlicher Raum zur Verfügung. Im Internet bewegen sich die Grundrechtsträger aber immer auf „privatem Grund". Nur solange ausreichend (nichtkommerzialisierte) Ausweichmöglichkeiten existieren, dürften staatliche Maßnahmen nicht gefordert sein.

Persönlichkeitsrecht. Komplettiert wird der Grundrechtsschutz durch die Absicherung passiver Komponenten, nämlich ein Online-Persönlichkeitsrecht. Je mehr sich persönlichkeitsrelevantes Handeln im Internet manifestiert, desto mehr entsteht eine Kategorie der Online-Persönlichkeit, die eng mit der analogen Persönlichkeit verbunden ist, aufgrund der anderweitigen Entstehungsvoraussetzungen und Bedrohungen aber eines eigenständigen Grundrechtsschutzes bedarf. Die Entwicklung steht hier erst am Anfang: Die Bewertung der Rolle von Suchmaschinen, die digitale Persönlichkeiten für Dritte sichtbar werden lassen, ist Gegenstand der Rechtsprechung.

Gibt es eine digitale Dimension der Grundrechte, und „ist das tauglich für das digitale Zeitalter"?

Die Analyse konnte zeigen, dass sich nicht nur zahlreiche (persönlichkeitsrelevante) Handlungsweisen ins Internet verlagern und unter Rückgriff auf informationstechnische Systeme vollziehen, sondern auch, dass diese Aktivitäten den gleichen Schutz beanspruchen wie analoge Verhaltensweisen – wie der klassische Grundrechtsgebrauch. Gleichwohl ist der zweite Teil der Frage nicht zwingend ebenfalls positiv zu beantworten. Das Grundgesetz ist als Antwort auf eine bestimmte historische Situation konzipiert worden. Daher steht die klassische Abwehrdimension im Vordergrund. Diese ist es aber nicht, die Antworten auf die Fehlentwicklungen im Internet geben kann. Es sind vielmehr staatliche Schutzpflichten und die (mittelbare) Drittwirkung der Grundrechte, die es zu aktivieren gilt. Die Beeinträchtigung durch private Dritte (oder andere Staaten) wird bei den digitalen Grundrechten zur Regel.

Welchen Mehrwert bietet vor diesem Hintergrund die Rückführung digitaler Handlungsweisen auf die grundrechtlichen Schutzbereiche? Es dürfte weniger die unmittelbare Wirkung sein, die gegenüber staatlichen Maßnahmen geltend gemacht werden kann und einen rechtfertigenden Grund verlangt. Stattdessen kann die Vergewisserung darüber, dass digitale Handlungsweisen grundrechtlichen Schutz genießen, aktuellen Debatten neue Impulse geben.

Neue Zeiten. Passt unser Grundgesetz in die digitale Gegenwart?

Herausforderung. Technische wie gesellschaftliche Innovationen stellen sich immer auch als Herausforderung für eine Rechtsordnung dar. Vor allem Gesetzgebung und Verwaltung sind zur Bewältigung berufen – auch wenn die Rechtsprechung mangels konkreter gesetzlicher Vorgaben derzeit eine Vorreiterrolle einnimmt und durch zur Entscheidung gebrachte Sachverhalte gezwungen ist, sachgerechte Lösungen unter Rückgriff auf eine Auslegung eines nicht für

Foto: r.nagy – Shutterstock

das Internet gemachten Rechts zu entwickeln. Ein solcher Zwang besteht für die Gesetzgebung nicht – gleichwohl dürfte es kaum mehr möglich sein, sich dieser gesellschaftlichen Herausforderung nicht anzunehmen. Gerade weil die unmittelbare abwehrrechtliche Komponente der Grundrechte keine zeitgemäße Antwort auf die drohende Beeinträchtigung auch elementarer Grundrechte im digitalen Raum gibt, ist es die Verpflichtung der Gesetzgebung, eine grundrechtsadäquate Ordnung unter Privaten herzustellen.

Leitplanken. Hier setzt die digitale Dimension der Grundrechte an. Sie kann „Leitplanken" definieren. Der Gesetzgeber ist berufen, durch Recht einen schonenden Ausgleich zwischen kollidierenden Rechtspositionen zu formulieren. Auch die (mittelbare) Drittwirkung, konstruiert über Einbruchstellen im einfachen Recht, stellt eine Form des Ausgleichs dar. In einem tripolaren Verhältnis kommt dem Staat die Rolle eines „Moderators" zu, der allen Rechten zu optimaler Durchsetzung verhelfen muss.

Selbstbestimmung. Der Blick auf die grundrechtlichen Schutzbereiche und konkrete Konfliktfälle – sowie deren Bewältigung durch die Rechtsprechung – hilft dabei, tatsächlich einen solchen Ausgleich anzustreben, während in der öffentlichen Debatte oder auf Grundlage geltenden Rechts ohne Rückbesinnung auf die grundrechtlichen Positionen oft die Überbetonung der einen oder anderen Position droht. Dies zeigen die Debatten zum Datenschutz, wo zum Teil vernachlässigt wird, dass neben dem Recht auf informationelle Selbstbestimmung auch Unternehmen (selbst „amerikanische Großkonzerne") Träger von Grundrechten sind. Die Einräumung eines grundsätzlichen Vorrangs durch Gesetzgebung oder Rechtsprechung ist im Verhältnis von Grundrechtsträgern und ihren Rechtspositionen untereinander kritisch zu bewerten. Bei aller Zuversicht, dass der Gesetzgeber den Schutz der Grundrechte vor privaten Beeinträchtigungen sichert, bleibt gleichwohl die begrenzte Steuerungskraft eines Nationalstaats im Hinblick auf globale Sachverhalte das wohl dringlichste Problem in diesem Zusammenhang.

Anpassungsbedarf. Abschließend sei darauf hingewiesen, dass unter der grundrechtlichen Perspektive – trotz eines fast lückenlosen Schutzes digitaler Handlungsweisen – Anpassungsbedarf auszumachen ist. Exemplarisch ist insofern die Einordnung der verschiedenen Kommunikationsvorgänge im Internet.

Die Erfassung – sowohl der Individual- als auch der Massenkommunikation – lediglich über die „Auffanggrundrechte" der Rundfunkfreiheit und des Fernmeldegeheimnisses erscheint der Bedeutung des Internets nicht angemessen. und dogmatisch fragwürdig. Grundrechtlicher Schutz soll allgemein verständlich sein – warum die reine Online-Zeitung nicht „Presse", sondern Rundfunk ist und wieso eine E-Mail oder ein Online-Speicher dem Fernmeldegeheimnis unterliegen sollen, ist nicht auf den ersten Blick überzeugend. Klärungsbedürftig erscheint zudem die Abgrenzung von laufender Kommunikation und abgeschlossenen Kommunikationsvorgängen sowie zwischen dem Schutz des Gegenstands der Kommunikation (bspw. personenbezogenen Daten) und dem Schutz des Kommunikationsvorgangs und von Kommunikationsinfrastrukturen.

Dr. Sönke E. Schulz
ist Berater bei der ÖPP Deutschland AG, Berlin, und freier Mitarbeiter am Lorenz-von-Stein-Institut

Umparken im Kopf?

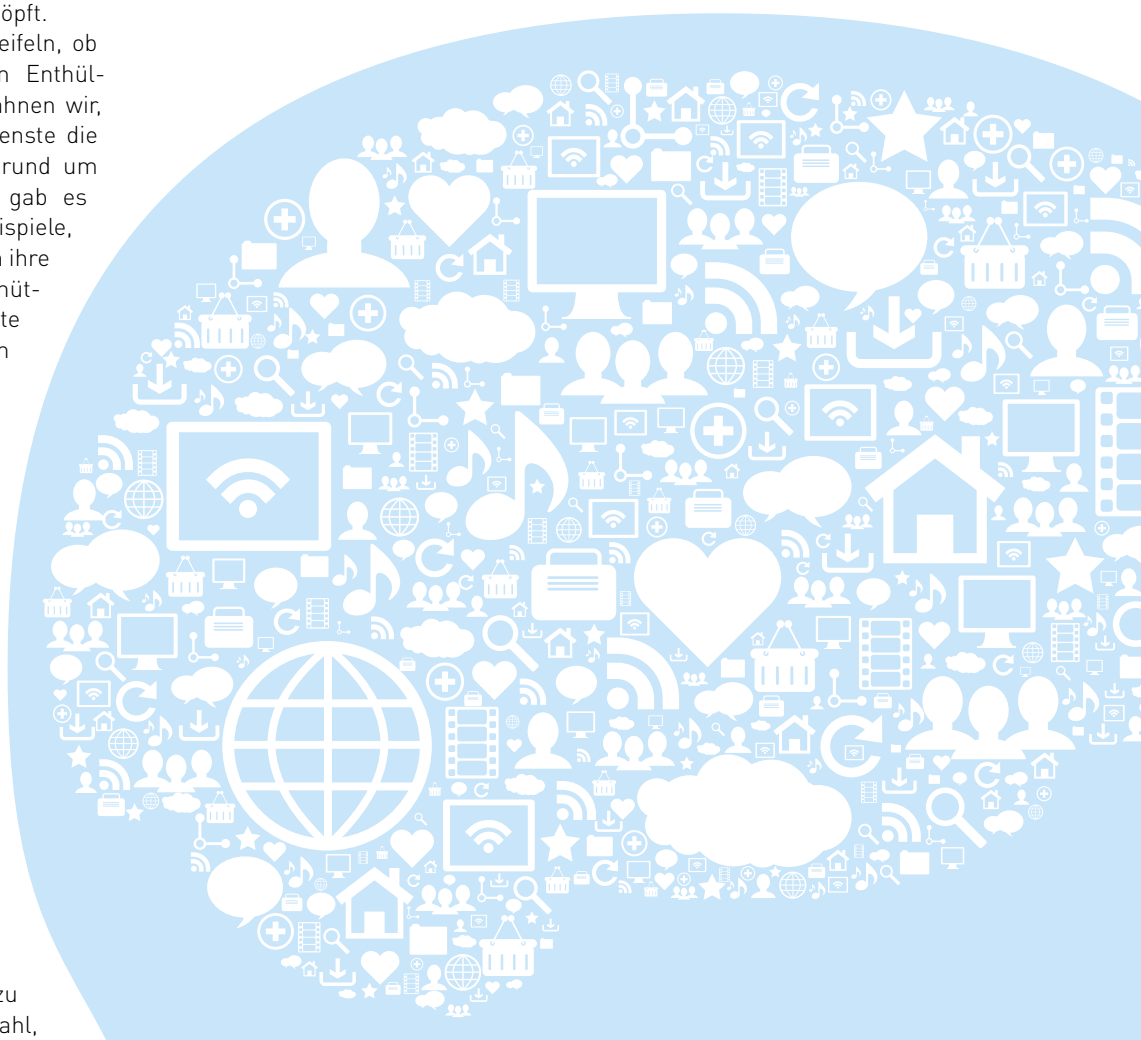
Vom blinden Vertrauen zu etwas, dem man eigentlich nicht traut.

Dr. Göttrik Wewer

Vertrauen, so heißt es allenthalben, ist der Schlüssel für die digitale Wirtschaft. Wenn die Menschen sich im Internet nicht sicher fühlen und den Angeboten nicht trauen, die ihnen dort gemacht werden, dann werden sie diese nicht nutzen, so schön das technisch auch alles funktionieren mag. Und dann werden weder die Potenziale von E-Commerce noch die von E-Government richtig ausgeschöpft.

Inzwischen lässt sich bezweifeln, ob diese These stimmt. Seit den Enthüllungen von Edward Snowden ahnen wir, in welchem Ausmaß Geheimdienste die elektronische Kommunikation rund um den Globus ausspähen. 2014 gab es zudem wiederum etliche Beispiele, dass selbst große Unternehmen ihre Daten nicht vor Hackern schützen konnten. Wenn Unbekannte Nacktbilder von Prominenten veröffentlichen, die sie sich aus der Cloud besorgt haben, mag man darüber vielleicht noch lächeln, aber bei Wirtschaftsspionage und Massenüberwachung hört der Spaß schnell auf.

Milliardenschaden. Bei der Organisierten Kriminalität wirke das Internet wie ein „Brandbeschleuniger", sagte Innenminister Thomas de Maizière bei der Herbsttagung des Bundeskriminalamtes. Mussten Kriminelle früher Menschen, Häuser oder Banken überfallen, um sich deren Eigentum anzueignen – mit allen Risiken, gestört oder erkannt zu werden – , so lassen sich Diebstahl, Bedrohung und Erpressung heute auch vom heimischen Computer aus bewerkstelligen. Schätzungen zufolge beläuft sich der Schaden, den Hacker in der Wirtschaft anrichten, weltweit auf 300 Milliarden Euro.



Sicherheit? Nur in die Köpfe lässt sich noch nicht sehen. Bei unseren Daten im Netz ist das anders. Da bleibt nichts verborgen.

Schöne neue Welt? Geld für Spiele-Apps wird ausgegeben, für mehr Sicherheit nicht.

Sicher ist nichts. Ob die Datenbestände von Sony Pictures, das den Film „The Interview" produziert hatte, von Nordkorea aus angegriffen, geknackt und teilweise ins Netz gestellt worden sind oder ob sich Mitarbeiter, die entlassen worden waren, an ihrem alten Arbeitgeber gerächt haben, ist unklar, kann dem gewöhnlichen Nutzer aber auch egal sein. Die Botschaft, die von allen diesen Vorfällen ausgeht, lautet: Nichts ist im Internet wirklich sicher. Wenn selbst Unternehmen wie Sony oder Microsoft ihre Daten letztlich nicht schützen können, wie soll das dem Einzelnen an seinem Laptop gelingen? Wenn selbst Mitglieder von Anonymus, die ihre Identität sorgfältig abzuschirmen versuchen, von Sicherheitsdiensten aufgespürt werden konnten, wie kann da der normale User glauben, er könne sich ernsthaft verbergen? Gängige Verschlüsselungen sollen längst geknackt worden sein.

Führt das alles dazu, dass die Menschen vorsichtiger werden? Dass sie das Internet weniger nutzen und genau überlegen, wozu sie es wirklich brauchen? Dass sie ihre Daten, wenn sie denn ins Netz gehen, regelmäßig verschlüsseln, um wenigstens einen gewissen Schutz zu haben, auch wenn es keine absolute Sicherheit gibt? Ändern also derartige Vorfälle irgendetwas am Verhalten der Menschen? Mitnichten!

Always on. Die Deutschen gehen nicht weniger ins Internet als vor den Enthüllungen von Snowden, sondern immer mehr sind „always on". Und obwohl das besonders unsicher ist, gehen immer mehr heute mobil ins Internet, also von ihrem Smartphone, Tablet oder Laptop aus. Nach Erhebungen der Initiative D 21 haben 2014 über die Hälfte der Deutschen (54 Prozent) das Internet unterwegs genutzt, ein Anstieg von 14 Prozent gegenüber dem Vorjahr. Zugleich waren aber 70 Prozent der Nutzer der Ansicht, dass das mobile Internet das Risiko birgt, dass sich jemand illegal Zugriff auf persönliche Daten verschafft.

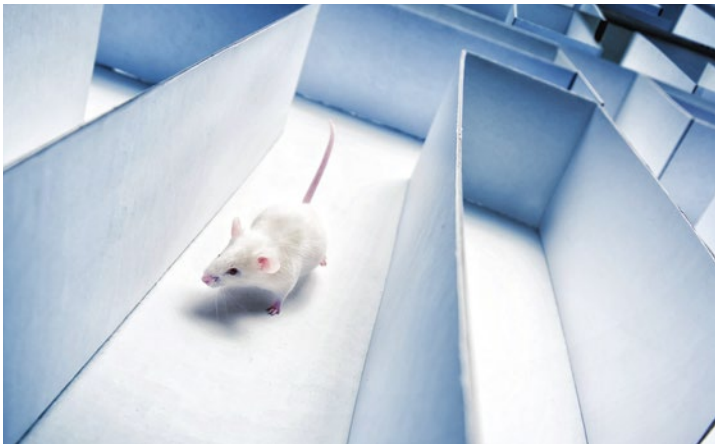
Weder die Risiken, die sie sehen, noch das, was wir von Edward Snowden wissen, noch die Datenverluste bekannter Unternehmen haben dazu geführt, dass die Menschen das Internet weniger nutzen oder ihr Verhalten ändern. All das hat sie auch nicht dazu bewogen, ihre Daten wenigstens ein bisschen besser zu schützen, auch wenn klar ist, dass es keinen absoluten Schutz geben kann. Aber man könnte es Angreifern immerhin etwas schwerer machen. Technische Lösungen gibt es durchaus, aber nur wenige sind bereit, für eine höhere Sicherheit ein paar Euro monatlich auszugeben. Dann lieber für eine schöne neue App, mit der man Musik hören kann.

Misstrauen. Das wirft die Frage auf, ob Vertrauen wirklich der entscheidende Schlüssel für die digitale Wirtschaft ist. Schon vor einigen Jahren hat eine BITKOM-Studie gezeigt, dass es um das Vertrauen in die Sicherheit sozialer Netzwerke insgesamt eher schlecht bestellt ist: Bei allen abgefragten Netzwerken gab jeweils mindestens die Hälfte der Nutzer an, der Plattform eher nicht oder gar nicht zu vertrauen. Dem Marktführer Facebook misstrauten 62 Prozent, Google plus 64 Prozent und Twitter sogar 70 Prozent. Noch weniger vertrauten der Online-Community Netlog (85 Prozent) (siehe DIVSI-Magazin 1/2012, S. 20).

Facebook macht täglich rund 1.000 Tests, ohne dass die Nutzer wissen, was da getestet wird, wozu es getestet wird und welche Ergebnisse dabei herauskommen. Dabei nutzt die Firma nicht →

Foto: cifotart/Syda Productions – Shutterstock

Laborratte.
Ist der Internet-Nutzer mittlerweile zum Versuchstier der großen Player abgesunken?



→ nur die Datenbestände, die ihre Nutzer aufgebaut haben, sondern sie manipuliert auch Daten, um herauszufinden, wie die Nutzer darauf reagieren. Wir seien längst, ohne das zu wollen und ohne dem zugestimmt zu haben, zu „Laborratten von Facebook" geworden, schreibt Harald Staun.

Sättigung. Früher hätte man vermutet, dass solche Versuche, unser Verhalten zu beeinflussen, zu Misstrauen und womöglich dazu führen würden, das Labor schleunigst zu verlassen. Das ist nicht der Fall: Obwohl viele der Plattform misstrauen, nutzen sie Facebook. Das Netzwerk wächst zwar nicht mehr so schnell wie in den ersten zehn Jahren, aber das scheint eher auf Sättigungseffekte zurückzuführen zu sein. Es wächst zwar nicht mehr rasant, aber es schrumpft auch nicht. Und der Grund für das verlangsamte Wachstum ist auch nicht mangelndes Vertrauen. Das fehlte – wie gesagt – schon immer.

Wer Vertrauen als den Schlüssel für die digitale Wirtschaft ansieht, der muss darüber nachdenken, wie er Vertrauen stärken kann. Strategisch geht es um eine entsprechende Reputation, die sich Firmen erarbeiten und täglich verteidigen und erneuern müssen. Zu den Werkzeugen, die man dafür einsetzen kann, zählen nicht nur IT-Sicherheit und Transparenz, Sicherheitsplanung und Reaktionsfähigkeit, sondern auch Penetrationstests, Hack Days, Zertifikate durch unabhängige Dritte und Ähnliches mehr. Vertrauen stellt sich nicht von allein ein, Vertrauen will gemanagt werden.

Wenn aber die meisten das Internet nutzen, obwohl sie nicht glauben, dass ihre Daten dort sicher sind, sie den Angeboten häufig misstrauen, müssen wir womöglich umdenken. Dann ist es vielleicht aufschlussreicher, besser zu verstehen, warum das so ist, als nach Strategien und Instrumenten zu suchen, das Vertrauen zu steigern. Das eine schließt das andere im Übrigen nicht aus.

In den USA oder in Großbritannien ist die Aufregung darüber, dass die kommerziellen Datensammler Profile anlegen, um uns maßgeschneiderte Werbung zukommen zu lassen, und dass die Geheimdienste alles sammeln, was sie im Netz kriegen können, weitaus geringer als in Deutschland. Dass Daten im Internet nicht wirklich geschützt werden können, sieht man dort (und anderswo) viel gelassener. 51 Prozent der Amerikaner finden auch die „verschärften Methoden" gerechtfertigt, mit denen die CIA Gefangene traktiert hat, um an Informationen zu kommen, und nur 29 Prozent sehen das anders, wie eine Umfrage des Pew Research Center kürzlich erbracht hat. 20 Prozent hatten dazu keine Meinung. Zweifel daran, dass das die richtige Entscheidung war, hatten 43 Prozent der Amerikaner nicht etwa daran, solche Methoden einzusetzen, sondern daran, den Bericht des Senats darüber zu veröffentlichen. 42 Prozent fanden das allerdings richtig.

Zielrichtung. Die diversen DIVSI Studien haben gezeigt, dass es den einen Nutzer, der für alle anderen steht, nicht gibt. Das mahnt zur Vorsicht, wenn man Antworten auf die Frage sucht, warum viele das Internet und bestimmte Angebote darin nutzen, obwohl sie ihnen nicht vertrauen. Stichworte dazu lauten:

- Abstraktheit der Gefährdungslage: Was technisch alles möglich ist, durchschauen nur die wenigsten.
- Geringschätzung des Risikos: Was soll mir schon passieren?
- Bequemlichkeit der Nutzung: Auf die einfachen, mobilen Möglichkeiten der Kommunikation möchte kaum noch jemand verzichten.
- Kostenloskultur des Internets: Wenn man etwas unentgeltlich nutzen kann, dann muss man manches halt in Kauf nehmen.
- Gruppendruck in Beruf und Freizeit: Wer nicht online ist, ist außen vor!
- Betroffenheit als Ausnahmefall: Echte Schäden an Leib, Leben oder Portemonnaie haben bisher nur wenige erlitten.
- Fatalismus als Ausrede: Wirklich schützen kann man sich sowieso nicht!

Diese Liste ist sicherlich nicht vollständig. Aber sie deutet doch die Richtung an, in der man suchen muss, um Antworten auf die Frage zu finden, warum Vertrauen in der virtuellen Welt vielen offenbar weniger wichtig erscheint als in der realen Welt. Dass Daten, die auf Plattformen im Internet mit anderen geteilt werden, Rückwirkungen haben auf das richtige Leben, scheint nicht allen bewusst zu sein. Wenn wir besser verstehen, warum viele dem Internet nahezu blind vertrauen, obwohl sie ihm doch eigentlich nicht vertrauen, finden wir vielleicht auch den geeigneten Schlüssel, um Wirtschaft, Staat und Demokratie im 21. Jahrhundert zu stärken.

Dr. Göttrik Wewer
ist Vice President E-Government bei der Deutsche Post Consult GmbH.

Foto: cifotart/Fer Gregory – Shutterstock

Aktuelle Bücher

Es ist kompliziert

Das Leben der Teenager in sozialen Netzwerken

Danah Boyd

Welche Auswirkungen haben Online-Plattformen wie Facebook auf Jugendliche? Danah Boyd hat über Jahre hinweg Jugendliche mit unterschiedlichstem sozialem und ethnischem Background zu ihren Online-Tätigkeiten befragt und diese untersucht. Dabei deckt sie einige der typischen Vorurteile und Mythen über den Gebrauch sozialer Netzwerke bei jungen Leuten auf und macht deutlich, dass der Versuch von Eltern und Gesellschaft, Jugendliche vor den Gefahren des Internets schützen zu wollen, nicht immer sinnvoll ist.

Redline, ISBN: 978-3-86881-555-9; 24,99 €

Think New!

22 Erfolgsstrategien im digitalen Business

Christian Hoffmeister, Yorck von Borcke

Nur wenigen gelingt es, den Erfolg von Apple, Google und Co. nachzubilden. Was machen die Großen richtig? Die Autoren haben Erfolgsprinzipien ermittelt, die vor allem unter den veränderten Rahmenbedingungen durch die Digitalisierung und das Internet große Bedeutung haben.

Hanser Verlag, ISBN: 978-3-446-44228-3; 39,99 €

Open Government, Staat und Demokratie

Aufsätze zu Transparenz, Partizipation und Kollaboration

Göttrik Wewer

Der Autor untersucht alle Bauteile von Open Government kritisch: das Paradigma der Offenheit, dem sich alles unterordnen soll, die Säulen Transparenz, Partizipation und Kollaboration, aber auch die technischen und ideologischen Fundamente, auf denen das Modell ruht.

Edition Sigma, ISBN: 978-3-8360-3600-9; 24,90 €

Finger weg von unseren Daten!

Wie wir entmündigt und ausgenommen werden

Jan Philipp Albrecht

Durch die nahezu unbegrenzten Möglichkeiten der Datenverarbeitung werden wir zum gläsernen Menschen, ausgebeutet und entmündigt. EU-Datenschutzexperte Jan Philipp Albrecht klärt auf über die Missstände beim Datenschutz, was die Politik tun muss und wie wir uns schützen können.

Knaur TB, ISBN: 978-3-426-78687-1; 7,00 €

Die digitale Dimension der Grundrechte

Das Grundgesetz im digitalen Zeitalter

Dr. Christian Hoffmann, Dr. Anika D. Luch, Dr. Sönke E. Schulz, Kim Corinna Borcher

Ist das Grundgesetz ins digitale Zeitalter übertragbar (s. auch „Es gibt Anpassungsbedarf", S. 22)? Die Analyse konnte u.a. zeigen, dass die zahlreichen ins Internet verlagerten Handlungsweisen den gleichen Schutz beanspruchen wie analoge Verhaltensweisen.

Nomos Verlag, ISBN: 978-3-8487-2027-9; 57 €

DIVSI Veröffentlichungen

Studien

Milieu-Studie zu Vertrauen und Sicherheit im Internet, 2012
Meinungsführer-Studie: Wer gestaltet das Internet?, 2012
Entscheider-Studie zu Vertrauen und Sicherheit im Internet, 2013
Freiheit versus Regulierung im Internet, 2013
U25-Studie – Kinder, Jugendliche und junge Erwachsene in der digitalen Welt, 2014
DIVSI Studie zu Bereichen und Formen der Beteiligung im Internet, 2014
Braucht Deutschland einen Digitalen Kodex? – Verantwortung, Plattformen und soziale Normen im Internet, 2014
DIVSI Studie – Wissenswertes über den Umgang mit Smartphones, 2014
DIVSI Studie – Daten: Ware und Währung, 2014

Reden

Roman Herzog: Internet und Menschenwürde, 2013
Olaf Scholz: Braucht das Internet Vertrauen?, 2013

Diskussionsbeiträge

Dominic Völz, Timm Christian Janda: Thesen zur Netzpolitik – Ein Überblick, 2013
Christina Heckersbruch, Ayten Öksüz, Nicolai Walter, Jörg Becker, Guido Hertel: Vertrauen und Risiko in einer digitalen Welt, 2013
Göttrik Wewer: Digitale Agenda 2013 – 2017 – Netzpolitik im neuen Deutschen Bundestag, 2013
Miriam Meckel, Christian Fieseler, Jan Gerlach: Der Diskurs zur Netzneutralität, 2013
Timm Christian Janda, Dominic Völz: Netzpolitik in Deutschland – Wahlprogramme, Koalitionsvereinbarung, Regierungserklärung, 2014
Manuel Schubert: Vertrauensmessung in der digitalen Welt – Überblick und Aussicht, 2014

DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet