



**DIGITALE
GESELLSCHAFT
2018**



DIGITALE
GESELLSCHAFT

Jahresbericht
2018

Inhaltsverzeichnis

Tätigkeiten

Meinungs- und Informationsfreiheit	2
Datenschutz und Recht auf Privatsphäre	3
Konsumentenberatung und Konsumentenschutz	12
Workshops und Bildung	13
Dienste	15
Veranstaltungen	16
Öffentlichkeitsarbeit	17

Verein

Organisation	18
Struktur	19
Zahlen	20

Vorwort

2018 war ein aussergewöhnliches Jahr, das speziell durch Volksabstimmungen geprägt war. So betrafen die Abstimmungen zu «No-Billag», Netzsperrern durch das Geldspielgesetz oder die Überwachung von Versicherten auch Anliegen der Digitalen Gesellschaft.

Eine Volksabstimmung zielte zudem direkt auf den Kern der Menschenrechte in der Schweiz: So hatte die «Selbstbestimmungsinitiative» die Kündigung der Europäischen Menschenrechtskonvention zum Ziel. Ohne EMRK wären jedoch beispielsweise Beschwerden gegen die Vorratsdatenspeicherung oder die Kabelaufklärung nicht mehr möglich. Aus diesem Grund engagierten wir uns u. a. im Vorstand von Schutzfaktor M (dem zivilgesellschaftlichen Zusammenschluss von über 100 Menschenrechtsorganisationen) gegen die Initiative.

Daneben hat sich die Digitale Gesellschaft auch 2018 anderweitig und vielfältig für Grund-, Menschen- sowie Konsumentenrechte im Internet eingesetzt. So konnten wir beispielsweise unser Informationsangebot mit dem Winterkongress und der Veranstaltungsreihe KarlDigital deutlich ausbauen.

Mittlerweile zählt der Verein 400 Mitglieder, wobei viele auch aktiv zu den Tätigkeiten in sehr unterschiedlicher Form beitragen. Es freut uns sehr, den dritten Jahresbericht veröffentlichen zu dürfen.

Norbert Bollow (Präsident)

Meinungs- und Informationsfreiheit

Quellenschutz

Das Redaktionsgeheimnis und den Quellenschutz zu gewährleisten, ist im digitalen Zeitalter fast unmöglich geworden. Staatliche und private (Massen-)Überwachung stellen für den kritischen und investigativen Journalismus ein ernsthaftes Problem dar. Diese Situation verschärft sich in der Schweiz mit der Umsetzung des neuen Nachrichtendienstgesetzes (NDG) und des revidierten Überwachungsgesetzes BÜPF nochmals deutlich.

Seminare
am MAZ

Wie in den Jahren zuvor durften wir auch 2018 wieder ein ganztägiges Seminar zum Thema «Quellenschutz in der Praxis» an der Journalistenschule MAZ in Luzern anbieten. Der Kurs ist für 2019 und 2020 bereits wieder ausgeschrieben.

Netzsperrn

Netzsperrn greifen in die Rechte auf Informations- und Wirtschaftsfreiheit ein. Sie bedienen sich derselben technischen Mittel wie es Internetkriminelle tun und stehen damit im Widerspruch zu Entwicklungen, welche die Internetnutzung sicherer machen sollen (wie z. B. DNSSEC, DNS-over-TLS, DNS-over-HTTPS). Gleichzeitig sind Netzsperrn aber bereits mit geringen Kenntnissen leicht zu umgehen.

Geldspiel-
gesetz (BGS)

Mit dem Referendum gegen das Geldspielgesetz ist es gelungen, eine breite Diskussion zu Netzsperrn in der Schweiz zu führen. Leider liessen sie sich im Abstimmungskampf gegen einen übermächtigen Gegner und eine erdrückende Angstkampagne nicht verhindern.

Im Fernmeldegesetz ist es hingegen aus beinahe aussichtsloser Situation zusammen mit der ISOC-CH gelungen, dass der Sperre ein Löschartikel vorangestellt wurde. Dies ist ausserordentlich wichtig, damit das Löschen in den Vordergrund rückt, wenn die vorgesehenen DNS-Sperren durch die absehbaren technischen Entwicklungen kaum noch funktionieren werden.

Fernmelde-
gesetz (FMG)

Dank des Widerstandes gegen das Geldspielgesetz sind Netzsperrungen aus der aktuellen Debatte zum revidierten Urheberrechtsgesetz (URG) verschwunden.

Urheberrechts-
gesetz (URG)

Datenschutz und Recht auf Privatsphäre

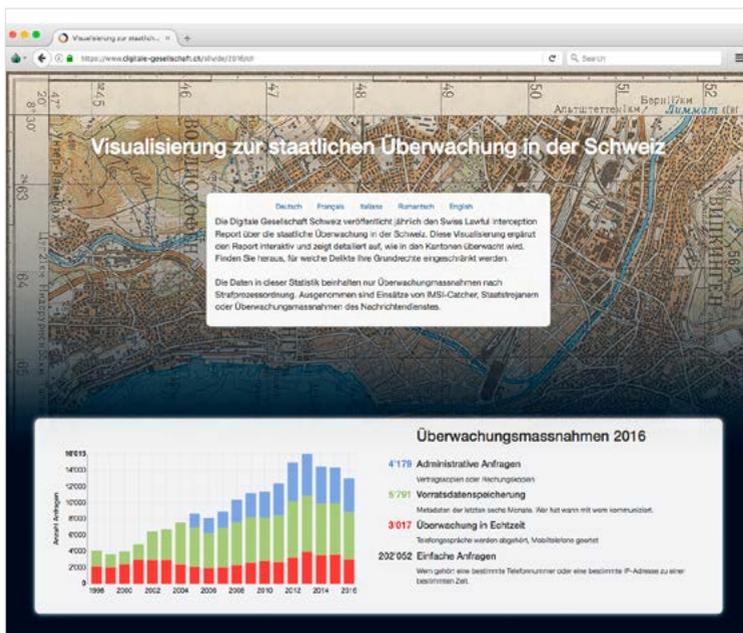
Swiss Lawful Interception Report

Der Swiss Lawful Interception Report wurde 2018 zugunsten eines anderen Projektes zurückgestellt. Die bereits veröffentlichten vier Reports in vier Sprachen sowie die Visualisierung stossen noch immer auf breites Interesse und werden oft zitiert. So können Details zu den Überwachungsmaßnahmen beim Bund und in den Kantonen nachvollzogen werden. Der Vergleich über die Jahre ermöglicht, die Entwicklung der ansonsten wenig transparenten Überwachungstätigkeit zu beurteilen und die wichtige Diskussion über ihre Verhältnismässigkeit öffentlich zu führen.

Überwachung
durch Bund
und Kantone

Aufgrund des Reports wurden wir im April 2018 zu einem ExpertInnen-Interview von der Eidgenössischen Finanzkommission eingeladen, die im Auftrag der Finanzdelegation einen Bericht zur Wirtschaftlichkeit der Fernmeldeüberwachung erstellt.

Viele Entwicklungen im Bereich der digitalen Fernmeldeüberwachung münden in gänzlich neue Fahndungsmethoden, wie der Vorratsdatenspeicherung, dem Antennensuchlauf oder den sogenannten Kopfschaltungen, die überhaupt erst durch den technischen Fortschritt möglich geworden sind. Vergleichbare Fahndungsmöglichkeiten in der «analogen Welt» wären nicht nur gesellschaftlich völlig indiskutabel sondern vor allem auch viel zu aufwändig und teuer zu implementieren. Die Kosten sind daher ein wichtiges begrenzendes Mittel.



Massenüberwachung

Vor 2011 war der Öffentlichkeit in der Schweiz kaum bewusst, dass beispielsweise von sämtlichen Handys bei einem Kommunikationsvorgang der Standort aufgezeichnet wird. Entsprechend galt die erste Kampagne der Digitalen Gesellschaft der Vorratsdatenspeicherung. Inzwischen ist der Begriff in der politischen Debatte präsent. Und entsprechend war es möglich, zumindest die Verdoppelung der Vorratsdatenspeicherung auf 12 Monate im revidierten Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) zu verhindern.

Vorratsdaten-
speicherung

Auch die Debatte um die Kabelaufklärung lässt sich auf eine Medienkampagne der Digitalen Gesellschaft zurückführen: Eine Titelgeschichte in der WOZ, ein offener Brief (zusammen mit Amnesty International und der Stiftung für Konsumentenschutz) sowie ein darauf folgender Hintergrundartikel im Tages-Anzeiger brachte die Massenüberwachung erstmals ins öffentliche Bewusstsein.

Kabelaufklärung

<https://www.woz.ch/-5775>

<https://www.tagesanzeiger.ch/22803449>

Beschwerde gegen die Kabelaufklärung

Am 1. September 2017 ist das Nachrichtendienstgesetz (NDG) in Kraft getreten. Mit der darin vorgesehenen Kabelaufklärung wird das Grundrecht auf Schutz der Privatsphäre schwerwiegend verletzt, das Anwaltsgeheimnis und das Arztgeheimnis werden ausgehöhlt. Die Kabelaufklärung verletzt zudem die Unschuldsvermutung und das Verhältnismässigkeitsprinzip.

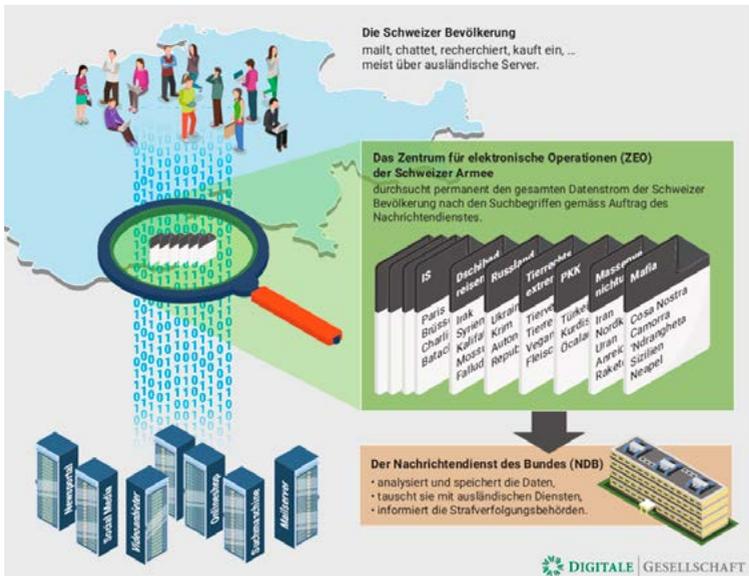
Unschulds-
vermutung und
Verhältnis-
mässigkeit

Die Digitale Gesellschaft gelangte deshalb Ende August 2017 mit einem Gesuch an den Nachrichtendienst des Bundes (NDB), die Kabelaufklärung zu unterlassen. Der Geheimdienst hielt es nicht für notwendig, auf das Gesuch inhaltlich einzutreten. Die Umsetzung des Massnahmengesetzes, so der Geheimdienst, verletzt «offensichtlich keine durch die Verfassung und die EMRK garantierte Grundrechte».

Die Verletzungen der Grundrechte durch die Kabelaufklärung sind im Gesuch detailliert und umfangreich dargelegt. Die Digitale Gesellschaft hat deshalb die Beschwerde gegen die Kabelaufklärung an das Bundesverwaltungsgericht weitergezogen.

Bundesverwaltungsgericht

2018 haben umfangreiche, schriftliche Anhörungen am Bundesverwaltungsgericht stattgefunden. Der Geheimdienst zeichnete dabei ein verharmlösendes Bild der Überwachung; so werde nur



«eine [einzelne] Glasfaser auf der viel Verkehr aus Syrien durchläuft» überwacht. Aus der Betrachtung der Internet-Architektur und des Bedrohungsbilds des NDB ist diese Darstellung jedoch unzulässig, vereinfacht und schlicht irreführend. Abschliessend haben wir ein Sachverständigengutachten gefordert, für dieses sich Edward Snowden zur Verfügung stellen würde. Mit einem Urteil kann 2019 gerechnet werden.

<https://www.digitale-gesellschaft.ch/?p=12268>

Beschwerde gegen die Vorratsdatenspeicherung

Die verdachtsunabhängige Vorratsdatenspeicherung verstösst gegen das Menschenrecht auf Privatsphäre und hat negative Auswirkungen auf die Meinungs- und Versammlungsfreiheit. Entsprechend hat das Bundesverfassungsgericht in Deutschland die Vorratsdatenspeicherung bereits 2010 als unzulässig erklärt. Der Europäische Gerichtshof (EuGH) lehnte die anlasslose und verdachtsunabhängige Massenüberwachung bereits zweimal ab. Jüngst erklärte nun auch der Europäische Gerichtshof für Menschenrechte, was gemäss EuGH gegen die EU-Grundrechtecharta verstosse, sei auch mit der Europäischen Menschenrechtskonvention (EMRK) nicht vereinbar.

Privatsphäre,
Meinungs- und Ver-
sammlungsfreiheit

Für das Bundesgericht hingegen heiligt der Zweck die Mittel: Der Gesetzgeber in der Schweiz habe sich für ein System einer allgemeinen und umfassenden Vorratsdatenspeicherung entschieden. Würde die Vorratsdatenspeicherung in der Schweiz entsprechend eingeschränkt, könne diese Massenüberwachung in der heutigen Form nicht mehr stattfinden.

Bundesgericht

Europäischer
Gerichtshof
für Menschen-
rechte (EGMR)

Entsprechend hat das Bundesgericht unsere Beschwerde im März 2018 gegen die anlasslose und verdachtsunabhängige Vorratsdatenspeicherung (erwartungsgemäss) nur teilweise gutgeheissen. Da die Schweiz kein Verfassungsgericht kennt, haben wir die Beschwerde im Herbst an den Europäischen Gerichtshof für Menschenrechte (EGMR) in Strassburg weitergezogen.

<https://www.digitale-gesellschaft.ch/?p=12369>

Datenschutz

Mangelnde)
Durchsetzbarkeit

Das geltende Datenschutzgesetz trat bereits 1992 in Kraft. Die Digitale Gesellschaft begrüsst die aktuelle Revision und ist mit der Stossrichtung des Bundesrats einverstanden. Wir sehen allerdings noch Schwächen, insbesondere beim Auskunftsrecht, im Bereich der Durchsetzbarkeit und mit Blick auf die neue Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU).

Ende 2017 waren wir in die Staatspolitische Kommission des Nationalrats eingeladen und konnten unsere Vorschläge, insbesondere jene zur Verbesserung der Durchsetzbarkeit, konkret einbringen. 2018 wurde dann die Revision des Datenschutzgesetzes in zwei Etappen beschlossen. Die erste Etappe zur Anpassung des Rechts zur Schengener Zusammenarbeit im Strafrechtsbereich ist mittlerweile verabschiedet. Nun wird in der Staatspolitischen Kommission der dritte Entwurf für ein neues Datenschutzgesetz debattiert. Mit dem neuen Gesetz wird sich weisen, ob der Datenschutz zukünftig auch tatsächlich durchgesetzt werden kann.

E-Voting

Demokratische Entscheidungen haben eine sehr hohe Akzeptanz, weil sich grosse Teile der Bevölkerung an der Entscheidung beteiligen können und das Entscheidungsverfahren nachvollziehbar ist. Nur so werden kontroverse und sehr knappe Entscheidungen auch von den VerliererInnen akzeptiert. Vollständig verifizierbare E-Voting-Systeme (so sie denn erfolgreich aus den Konzepten entwickelt werden können) bedingen jedoch umfangreiche technische und organisatorische Massnahmen. Die Verifikation setzt insbesondere weitreichendes Fachwissen – speziell auch bei den abstimmenden Personen – voraus.

Das deutsche Bundesverfassungsgericht hat 2009 die weitere Verwendung von Wahlcomputern verboten, da «der Wähler ohne nähere computertechnische Kenntnisse selbst nachvollziehen können muss, ob seine abgegebene Stimme als Grundlage für die Auszählung oder jedenfalls als Grundlage einer späteren Nachzählung unverfälscht erfasst worden ist».

Nachvollziehbarkeit nicht gegeben

Nun sind aber die Abläufe beim E-Voting nochmals deutlich komplexer als die Verwendung von Wahlcomputern. IT-Sicherheit und Nachvollziehbarkeit der Wahl schliessen sich daher bereits in der Theorie aus.

Bereits seit 2013 arbeiten wir kontinuierlich an diesem momentan sehr aktuellen Thema. So waren wir an verschiedenen kantonalen Vorstössen und Anhörungen beteiligt. Diese haben dazu beigetragen, dass die E-Voting-Systeme der ersten Generation verboten wurden und das sogenannte Consortium

aufgelöst wurde. Im Herbst 2018 hat nun auch der Kanton Genf die System-Entwicklung aufgegeben. Aktuell übrig geblieben ist das vom spanischen Hersteller Scytel stammende und von der Schweizer Post vertriebene System. Das Jahr 2019 dürfte ein entscheidendes Jahr für E-Voting in der Schweiz werden.

Elektronische Identität (E-ID)

Hoheitliche
Aufgabe

Bereits 2017 haben wir uns in einer Stellungnahme kritisch zur geplanten Einführung einer staatlichen elektronischen Identität geäußert, die von Privaten herausgegeben werden soll. Auch wir sehen den Bedarf einer benutzbaren und vertrauenswürdigen elektronischen Identität (wie auch Unterschrift). Dies ist vom Bund jedoch in seiner hoheitlichen Aufgabe zügig an die Hand zu nehmen. Das Ausweisgesetz kann hierzu als Grundlage dienen. Eine E-ID muss den BürgerInnen dienen. Zudem muss das Recht auf Privatsphäre – gerade im Internet – gestärkt und nicht noch weiter ausgehöhlt werden.

Im November 2018 waren wir schliesslich in die Rechtskommission des Nationalrats eingeladen, um unsere Kritik zu präsentieren und über unsere Vorschläge zu diskutieren.

Freedomvote.ch

Smartspider

Freedomvote.ch ist ein Wahlhilfetooll und Smartspider für netzpolitische Fragen. Es ist bei den National- und Ständeratswahlen 2015 erstmals zum Einsatz gekommen.

Auch auf kantonaler und kommunaler Ebene sind die Abgeordneten vermehrt mit Themen der Digitalisierung konfrontiert. Zu den Erneuerungswahlen 2018 im Kanton Bern und in der Stadt Zürich stand daher ein aktuelles Freedomvote zur Verfügung. Es konnte die Kandidierenden für netzpolitische Anliegen sensibilisieren und den Wählenden als Orientierung dienen.

Die Digitale Gesellschaft hat bei der Auswahl und Gestaltung der Fragen mitgearbeitet.

Replay-TV

Früher mussten die KonsumentInnen in der Schweiz Fernsehsendungen selbst aufnehmen. Danach konnten sie zu einem beliebigen späteren Zeitpunkt die Aufnahmen abspielen, aber auch vor- und zurückspulen. Dafür wurden ursprünglich Videokassetten verwendet, später folgten digitale Datenträger. Es handelt sich hierbei um rechtlich unbestrittene Privatkopien zum Eigengebrauch, die kollektiv entschädigt werden.

Recht auf
Privatkopie

Beim Internet-TV ersetzt das Replay-TV das frühere Aufnehmen und Spulen daheim. Das Aufnehmen und Spulen erfolgt effizient und nachhaltig direkt bei den Internet-TV-Anbietern. Für das Replay-TV werden die Fernsehsender von Swisscom, Sunrise, UPC und anderen Internet-TV-Anbietern ebenfalls kollektiv entschädigt. Die KonsumentInnen bezahlen – direkt oder indirekt – mit ihren Abonnementsgebühren für Replay-TV.

In einer Nacht- und Nebelaktion drohte im Nationalrat dieses Recht faktisch abgeschafft zu werden. Gemeinsam mit anderen Organisationen konnte dies verhindert werden.

Konsumentenberatung und Konsumentenschutz

Netzneutralität

Alle grossen Mobilfunkanbieter in der Schweiz bieten (oder boten) Abos an, welche die Netzneutralität verletzen. Indem gewisse Dienste nicht zum Datenverbrauch gezählt werden, wähnt sich die Kundschaft zwar im Vorteil, tatsächlich findet jedoch eine Diskriminierung aller anderen Dienstanbieter statt.

Grosse Internetzugangsanbieter versuchen zudem einen zweiseitigen Markt bei der Interconnection zu etablieren. Nicht nur der Internet-Abonnent, sondern auch die Inthalteanbieter oder andere Provider sollen zur Kasse gebeten werden. Dies ist ein klarer Nachteil für kleinere Unternehmen, den Innovationsstandort und die KonsumentInnen, deren Einfluss abnimmt.

Transparenz
unzureichend

Der Bundesrat hingegen sieht keine Diskriminierung und hält im überarbeiteten Fernmeldegesetz eine Transparenzpflicht bei beispielsweise Zero-Rating-Angeboten für ausreichend.

Gesetzes-
entwurf

Die Digitale Gesellschaft hat bereits 2016 zu diesem wichtigen Thema eine umfangreiche Stellungnahme veröffentlicht. Für die Debatte im Parlament haben wir darauf aufbauend einen Gesetzesentwurf ausgearbeitet. Im November 2017 waren wir dann von der Kommission für Verkehr und Fernmeldewesen (KVF-N) zu einer Anhörung eingeladen.

2018 ist es in einer gemeinsamen Anstrengung mit Exponenten der Eidgenössischen Jugendsession gelungen, eine Verpflichtung für Netzneutralität in das Gesetz zu hieven. Das ist ein toller Erfolg. 2019 gilt es die vom Ständerat hinzugefügte Ausnahme für Spezialdienste nach europäischem Modell möglichst einzugrenzen.

<https://www.digitale-gesellschaft.ch/?p=12655>

Workshops und Bildung

Die Digitale Gesellschaft hat sich 2018 vermehrt für die Vermittlung der technischen Grundlagen für einen verantwortungsvollen Umgang mit digitalen Werkzeugen engagiert. Im Fokus standen verschiedene Gruppen: JournalistInnen, SchülerInnen und die breite Bevölkerung ohne spezifische Vorkenntnisse.

Journalist-
Innen und
Allgemeinheit

Kurse

Unsere Workshops zur digitalen Selbstverteidigung wurden 2018 an der Journalistenschule MAZ, für Amnesty International (in deutsch und französisch), an der Primarschule und am Winterkongress im Zentrum Karl der Grosse in Zürich durchgeführt. Die Standardmodule umfassen:

- Computer-Grundschutz
- Sicherheit von Messenger
- Spurenarm und anonym surfen
- E-Mails verschlüsseln mit GnuPG

<https://www.digitale-gesellschaft.ch/slides/master.html>

Ratgeber

Bereits 2017 haben wir zusammen mit der WOZ und dem CCC Schweiz einen Digital-Ratgeber herausgebracht. Dieser beschäftigt sich mit dem Thema Datenschutz und bietet eine Vielzahl konkreter Anregungen, wie die Privatsphäre im Internet geschützt werden kann. Nachdem die ersten 22 000 Exemplare bereits nach kurzer Zeit vergriffen waren, haben wir 2018 eine Neuauflage gedruckt. Für 2019 ist ein ergänzendes Online-Portal und eine Übersetzung ins Französische geplant.



<https://www.digitale-gesellschaft.ch/digital-ratgeber.pdf>

Dienste

Das «Tor Project» und die darauf aufbauenden Dienste bieten unbeobachtete, sichere und zensurresistente Kommunikation. Tor ist eines der wenigen Hilfsmittel, die wirkungsvoll vor Massenüberwachung schützen. Dies ist wichtig für die eigene informationelle Selbstbestimmung und unersetzlich für die politische Auseinandersetzung in repressiven Staaten.

2018 konnten wir zwei neue Tor-Server in Kooperation mit der Stiftung SWITCH in Betrieb nehmen. Die leistungsfähigen Server sind in Zürich direkt an das Backbone des Schweizer bzw. europäischen Forschungsnetzes angebunden.

Tor-Exit-Node

Die Digitale Gesellschaft betreibt damit aktuell 15 Exit-Nodes auf fünf Servern und gehört weltweit zu den drei grössten Betreiberinnen von Exit-Nodes.

Veranstaltungen

Winterkongress

Im Februar 2018 konnten wir unseren ersten Winterkongress im Zentrum Karl der Grosse in Zürich durchführen. Den Teilnehmenden standen über 25 Vorträge und Workshops in vier parallelen Tracks zur Auswahl. Diese deckten die Bereiche «Digitale Selbstverteidigung», «Ethik, Wissenschaft & Gesellschaft», «Recht & Politik» sowie «Netzwerke, Security, Hard- & Software» ab.

Im Februar 2019 steht die zweite Auflage an, und es gibt bereits Pläne fürs Jahr 2020.

<https://digitale-gesellschaft.ch/kongress/>

KarlDigital

Ebenfalls gemeinsam mit dem Zentrum Karl der Grosse lancierten wir im November 2018 die neue Veranstaltungsreihe KarlDigital. Den Auftakt bildete das Thema «Digitale Demokratie». Das Konzept sieht einen Vortrag mit Diskussion, eine Pause mit Suppe und anschliessend drei parallele Workshops vor. Für 2019 sind fünf Veranstaltungen geplant.

Öffentlichkeitsarbeit

Veranstaltungen und Podien

Zunehmend werden wir als fachkompetente und kritische Stimme an Veranstaltungen und Podien eingeladen. Im vergangenen Jahr war der Verein beispielsweise an der «Connecta» der Schweizer Post und am 35. Chaos Communication Congress in Leipzig vertreten.

<https://www.digitale-gesellschaft.ch/?p=12819>

Medien

In über hundert Artikeln fanden die Aktivitäten der Digitalen Gesellschaft im Jahr 2018 Erwähnung. Wir sind als ExpertInnen zu verschiedenen Themen in «10vor10», der «Republik» oder der «WOZ» zu Wort gekommen.



<https://www.digitale-gesellschaft.ch/uber-uns/medien-echo/>

Organisation

Vorstand

Norbert Bollow (Präsident)
Hartwig Thomas (Kassier)
Simon Gantenbein
Viktor Györfy
Christoph Laszlo
Reto Schneider
Lorenz Schori
Aline Trede

Revisionstelle

Christine Lent
Hans-Peter Oeri

Geschäftsstelle

Erik Schönenberger

Medienstelle

Martin Steiger

Rechtsform

Gemeinnütziger Verein nach Schweizer Recht

Struktur

Breiter, ehrenamtlicher Vorstand

Zuständig für

- Zielvorgaben, Strategie & Verantwortlichkeiten
- Finanzierung, Finanzen & Personal

Breit abgestützte und aktive Mitgliederbasis

- Setzen inhaltlicher Themenschwerpunkte
- Regelmässige Treffen und Absprachen
- Frühjahres- und Herbsttreffen
- Mitgliederversammlung



Geschäftsleitung

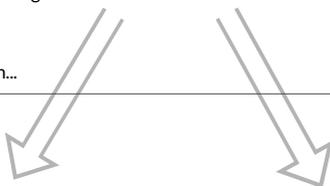
- Teilzeitstelle
- Aufgaben:
 - Redaktion
 - Community Management
 - Koordination & Administration

Strategie, Organisation...

& Administration

Inhalte, Themen...

& Service



Thematische Arbeitsgruppen

- Arbeitsbereiche mit zugeordneten Personen
- Dossiers & Materialien
- Kommunikation
- Vorträge & Präsentationen
- Vorratsdatenspeicherung
- Kabelaufklärung
- Netzsperrern
- Netzneutralität
- E-Voting
- Datenschutz
- Urheberrecht
- Elektronische Identität (E-ID)
- *Online-Portal & Redaktion*
 - *Swiss Lawful Interception Report*
 - *Merkblatt/Hausordnung Public-WLAN*
- *Dienste & Tools*
 - *Messenger-Vergleich*
 - *Tor-Server*
 - *DNS-Server*
 - *Anonip*
- *Workshops zur Digitalen Selbstverteidigung*
- *Ratgeber & Artikel*
- *Winterkongress*
- *KarlDigital*

Stand: Januar 2019

Zahlen

Die Digitale Gesellschaft 2018

400 Mitglieder, davon 70 aktive Mitglieder
14 Organisationen

Einnahmen

CHF

Mitgliederbeiträge	28 400.-
Spenden	25 250.-
Zweckgebundene Spenden	44 450.-
Bildung, Veranstaltungen, Dienstleistungen	10 050.-

Ausgaben

Personalkosten	42 650.-
Beschwerden Massenüberwachung	16 600.-
Dienste und Kampagnen	3 100.-
Bildung, Veranstaltungen, Dienstleistungen	5 000.-
Administration und Betrieb	4 800.-

Gewinn

Total	36 000.-
-------	----------

Kapital

Total	112 000.-
davon nicht zweckgebunden	79 750.-

(Provisorische Zahlen per 18.1.2019)

Vielen Dank für die Unterstützung:

- Stiftung SWITCH
- Nine Internet Solutions AG
- Ticketpark GmbH
- WOZ Die Wochenzeitung
- Zentrum Karl der Grosse

Impressum

Digitale Gesellschaft
4000 Basel
Schweiz

office@digitale-gesellschaft.ch
7EC7 496F 10AF D8D5 04B0
0B9C 202C 8998 CCEB FB34

www.digitale-gesellschaft.ch

Postkonto: 61-177451-1
PostFinance AG, 3030 Bern
CH15 0900 0000 6117 7451 1
POFICHBEXXX

Januar 2019

