Big Data – All Data: Wunschtraum von Ländern/Regimes in aller Welt

Steinmüller Workshop 2015 Big Data: Auf dem Weg in die Datendiktatur?
Europäische Akademie für Informationsfreiheit und Datenschutz
Berlin, 27. Mai 2015
Dr. Dieter Klumpp , instkomm e.V., Stuttgart

Programm

10.00	Begrüßung
10.15	Wolfgang Coy: Nachruf auf Klaus Brunnstein
10.30	Wolfgang Coy: Was ist dran an Big Data? Ein Marketingschlagwort aus informatischer Sicht durchleuchtet
11.15	Klaus Lenk: Regulation by Technology – Zu den Folgen datenintensiver gesellschaftlicher Steuerung
12.00	Klaus Fuchs-Kittowski: Zur Ambivalenz der Wirkungen Moderner Informations- und Kommunikationstechnologien
	Mittagspause
14.00	Jochen Rieß: Von der Rasterfahndung zu Big Data
14.45	Jörg Pohle: Big Data und Zweckbindung
15.30	Herbert Burkert: Endlich das Ende der Privatsphäre.
16:15	Dieter Klumpp: Big Data als Wunschtraum von Ländern/Regimes in aller Welt?
	Abschlussdiskussion

Moderation: Hansjürgen Garstka

Teilnehmer

Herbert Burkert
Wolfgang Coy
Alexander Dix
Willi Egloff
Klaus Fuchs-Kittowski
Hansjürgen Garstka
Wolfgang Kilian
Dieter Klumpp
Klaus Lenk
Otto Mallmann
Andrzej Mrozek
Kai Nothdurft
Jörg Pohle
Jochen Rieß
Peter Schaar
Stefan Walz
Henner Wolter

Bebilderung Netzthemen, Spiegel Online, 12.5.2015 (Markus Böhm)

Je intensiver man sich mit **Netzthemen** beschäftigt, desto schwerer lässt es sich übersehen: In kaum einem anderen Fachgebiet begegnen einem medienübergreifend so oft dieselben, **unattraktiven, nichtssagenden Fotos**. Ein Grund für das optische Einerlei ist, dass es in der **Netzwelt meistens um abstrakte Dinge geht – um Daten, um Software, um Codes.**

Ein zweiter, dass die **Bildagenturen wenig Material zu Netzthemen zur Verfügung stellen**. Bei Themen wie Netzwerken oder Internetverbindungen lande man oft bei einem Kabel-Symbolbild, sagt unser Bildredakteur Erik Seemann. Hinzu kommt, dass viele Symbolbilder plump gestellt oder extrem kitschig wirken, etwa zu Hacker-Angriffen.

Die **Bildarmut bei den Digitalthemen** ist ein Problem, gerade **im Online-Journalismus. Bilder entscheiden hier maßgeblich darüber, welche Artikel aufgerufen werden**. Auch in sozialen Netzwerken wie Facebook sind optische Reize wichtig dafür, dass ein **Artikel in der Masse von Inhalten überhaupt wahrgenommen wird.**

Man kann wohl mittlerweile **noch so gute und wichtige NSA- oder BND-Enthüllungsgeschichten schreiben, noch so originelle Plädoyers für oder gegen die Vorratsdatenspeicherung**: Ohne ein Foto, das in den Artikel zieht, ist die **Chance gering, dass der Text überdurchschnittlich oft gelesen wird und nicht nur die übliche Zielgruppe** erreicht.

All Data Sauger

Powerpoint mag keine solche Langtexte, genau wie die Leserschaft

Zur IT-Architektur (2001, vor 11. September):

„Aber mit der Cybercrime Convention, die letzten Monat unterschrieben wurde, hat man offensichtlich überzogen. **Über das Netz wird jetzt eine Saugglocke gestülpt, die *Millionen von Normalbenutzern* die Luft entzieht**, um Tausende von Kriminellen herauszufinden, die sich gegen diese Überwachung mit allen Methoden der Verschlüsselung und der Steganographie schnellstens erfolgreich schützen werden“ .(Klumpp, D., 9. Juli 2001).

Zur IT-Architektur (2006, nach 11. September, vor Snowden):

„ NSA has massive database of Americans phone call records *of tens of millions of Americans*, using data provided by AT&T, Verizon and BellSouth, people with direct knowledge of the arrangement told USA TODAY. The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans. This program does not involve the NSA listening to or recording conversations***. But the spy agency is using the data to analyze calling patterns in an effort to detect terrorist activity***, sources said in separate interviews”. (Cauley, Leslie, USA TODAY May 11, 2006)

Zur IT-Architektur (2015, nach Snowden):

„Der Bundesnachrichtendienst ***(BND) soll künftig seinen Datenstaubsauger*** zur strategischen Fernmeldeaufklärung auch gegen Cyber-Gefahren in Stellung bringen können. Dies sieht ein Gesetzentwurf (…) von Bundesinnenminister Thomas de Maizière vor. (…). Bisher darf der BND laut G10-Gesetz 20 Prozent der Leitungskapazität bei internationaler Telekommunikation ***einsaugen und nach vorab genehmigten Begriffen durchsuchen (***…) auf Bereiche beschränkt wie terroristische Anschläge, bewaffnete Angriffe gegen Deutschland, die Verbreitung von Kriegswaffen oder Drogen, Schleuserkriminalität oder Geldwäsche und –fälschung“ . (vgl. heise online, 20. Februar 2015).

Geierfrust: Perzeptionen im *Anderkontext*

Kontext im Mai 2011: So, wie alle Aasgeier gegen die Abschaffung des Todes sind, fürchten alle Datengeier die 100% Datensicherheit

Perzeption (1): Gemeint sind offenbar wir Sicherheitsberater

Perzeption (2): Gemeint sind offenbar wir Hacker

Perzeption (3): Gemeint sind mit „Adlern“ offenbar wir Nachrichtendienstler

Perzeption (4) : Gemeint sind offenbar wir Juristen

Aktuelle Meldungen Februar 2015: Realität heute

NSA-Skandal

NSA/GCHQ unterwandern SIM- und Kreditkarten

Seit Jahren greifen NSA und GCHQ bei den Herstellern von SIM-Karten und Smart Cards die zugehörigen Schlüssel ab. Damit können sie mitlesen und manipulieren. Auch die Rechnungssysteme vieler Mobilfunker sind unterwandert. Mehr... 254

kommt
rz

ird für März
donesien
bald
tphones
Mehr...

Telekom

Phishing-Schutz für Online-Rechnungen

Die Rechnungen per E-Mail von der Telekom erhalten neue Sicherheitsmerkmale, auch zur Bestätigung der Echtheit. Mehr... 83

25 Jahre Photoshop

Umwälzung von Ästhetik und Wahrnehmung

Am 19.02.1990 erschien eine Diskette mit einem Programm, das die Welt verändert sollte. In den vergangenen 25 Jahren wurde Photoshop von der simplen Pixelschubserei zur komplexen Bildbearbeitung. Mehr... 376

30 Jahre SIM-Karten
Schlüsselleser erst jetzt?

25 Jahre Photoshop
Bildmanipulation erst jetzt?

18 Jahre Signatur
Echtheitsprüfung erst jetzt?

29 Jahre Patent 3Druck
Technikfolgen erst 2020?

Das Virtuelle der (nicht vernetzten) Informatisierung

- Bis in die Achtziger war ein *Text noch ein Text*. Wenn er verfälscht wurde, war es eben ein verfälschter Text, im Zweifelsfall konnte man telefonisch nachfragen. Heute ist es ein **virtueller Text**, bei dem nicht einmal der Autor sicher sein kann, ob es wirklich **der von ihm formulierte Wortlaut war**, der auf der anderen Seite ankam – *es kann nichts mehr ausgeschlossen werden*.

- *Ein Foto war ein Foto*, ein retuschiertes Foto war eben ein retuschiertes Foto. Die russischen Raketen auf Cuba 1962 waren echte Fotos. Heute ist ein Foto ein **virtuelles Foto, das nur mit aufwändiger Daten-Forensik und weiteren kollateralen Informationen als Original bestätigt** werden kann. Das aktuelle Satellitenfoto von schwerem Gerät in der Ukraine ist wahrscheinlich echt, aber man ist nicht mehr sicher – *es kann nichts mehr ausgeschlossen werden.*

- Eine Papier-*Kopie war eben eine Kopie*, wobei sogar Sicherungen eingesetzt wurden, die Kopie vom Original unterscheidbar zu machen. Heute können **nicht nur wenige Spezialisten Kopien herstellen, die besser sind als das Original** – *es kann nichts mehr ausgeschlossen werden.*

Weltweites Internet war nur Zwischenetappe

„2011 war das Internet in **Russland** noch frei. Seither hat es eine Reihe von Gesetzen gegeben: Angefangen von Internetfiltern und deep packet inspection, unter dem Vorwand des Kampfes gegen Kinderpornografie, über Ideen zur Nationalisierung des Internets unter dem Vorwand der NSA-Abhöraffäre bis hin zur Blockade oppositioneller Blogs“ (ZEIT 2014/05/07).

Iran will alle Internetnutzer schon beim Einloggen identifizieren und registrieren, zudem sollen Inhalte stärker gefiltert werden. Irans Telekommunikationsminister Mahmud Waesi im Dezember 2014: "Wir werden die Identität eines jeden Web-Users kennen" (ZEIT Online 2014/12/07).

China verschärfte Anfang Februar 2015 die seit Jahren bestehende Internetzensur. „Wer in China Internetdienste nutzt, soll sich künftig mit seinem Realnamen registrieren müssen, dies gilt für alle 650 Millionen Internet- und Smartphone-Nutzer. Die Internetprovider sind künftig für ‚illegale‘ Inhalte verantwortlich, daher müssen ihre Dienste verbessert und stärker kontrolliert werden.“ (Spiegel 2015/02/05)

Zusammen mit der Blockierung selbst der Virtual Private Networks internationaler Unternehmen markieren diese nationalen Zensierungen bereits den sich rasch verfestigenden Weg zu einer *permanenten* globalen Netzaufteilung. Das weltweite Internet war nur Zwischenetappe.

Globale, regionale und netzkoloniale Cyber-Mächte

Global Players

Staaten, die in vollem Umfang Bauelemente, Netze, Geräte und Softwaresysteme vollkommen autonom erforschen, entwickeln und aufbauen sowie instandhalten/betreiben können

Ohne Zweifel sind die USA führend als Cyber-Supermacht, Russland will seit Juni 2012 erklärtermaßen auf den Stand der USA kommen, China ist bereits autonom.

Regional Actors

Staaten, die aufgrund hoher Wissensressourcen und ihrer nationalen Nachfrage die Chance haben, auch eigene Normen (z.B. für IT-Sicherheit oder Privacy) durchzusetzen. Dazu gehören die zentralen großen EU-Länder, insbesondere im Verbund untereinander.

Cyber-Colonial Dependants

Staaten, die absehbar keine andere Möglichkeit haben, als in voller Abhängigkeit die IT-Systeme der jeweiligen Global Player zu übernehmen.

Cyber-Spionage und „Cyber-Krieg“

Karte: alle Global Player,
viele Regional Actors und
einige Cyber-Colonial Dependants

Digitaler Datenkampf: Cyber-Krieg

- In der Netz-Diskussion wird der **Begriff Cyberkrieg** noch überwiegend im Sinne eines wechselseitigen **geheimdienstlichen „digitalen Datenkampfs“** benutzt, aber auch schon für die heute schon jedem deutlich werdende Automatisierung und Softwaresteuerung von kriegerischen Gefechtsfeldern mit **digitalen „D-Waffen“** (vgl. FIfF 2015).
- Es geht aber zunächst um wirtschaftliche Faktoren vom Datenraub über Computerkriminalität über Sabotage bis hin zu **cyber-terroristischen** Angriffen zum Beispiel auf **Kritische Infrastrukturen**.
- Cyber-Angriffe können von sehr kleinen Gruppen ausgeführt werden **(„Datendschungel-Krieg“)**
- Die **Cyberbedrohung** basiert auf der **durchgängigen architektonischen IT-Unsicherheit** eines in 30 Jahren als Stückwerk entstandenen weltweiten Netzes, das sich einem **ganzheitlichen Re-Design entzieht**.
- Gegen eine totale IT-Unsicherheit hätte zunächst der Beginn für eine Konvention für **gemeinsame Cyber-Verteidigung** nahegelegen.
- Die US-Regierung hat jedoch schon 2010 ein Cyberkommando eingerichtet und auch im Nationalbudget 2015 mit der ausdrücklichen Betonung der eigenen **Cyber-Angriffsmöglichkeit** in der Tat eine weitere Phase des Cyber-Wettrüstens eingeleitet (vgl. Rötzer 2010).

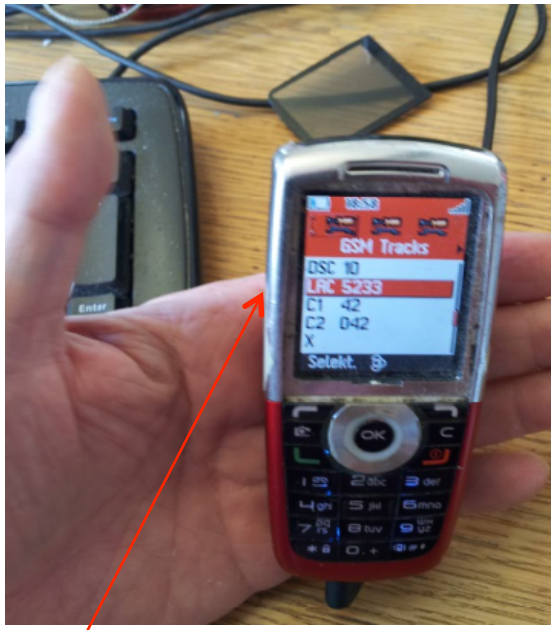
Big Data in lupenreinen Demokratien

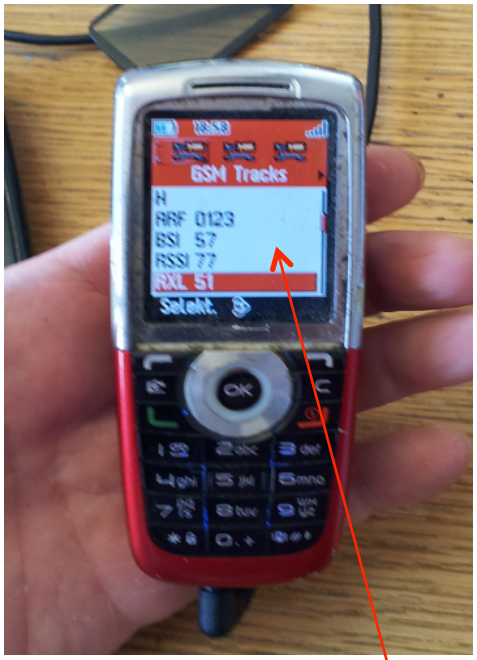
Und wer denkt heute schon daran, dass **in vielen Ländern bereits unzählige „Dissidenten“ 365 Tage im Jahr (auch im chinesischen Jahr) unbemerkt an einer virtuellen Leine von „großen Brüdern“ angehängt sind, und nur an dem Tag ganz überraschend in Probleme kommen, an dem ihnen damit etwas in der „realen“ Welt nachgewiesen werden kann?** Nicht zu vergessen: **Der Zugang zum Internet und der Zugang zum Mobiltelefonnetz können vom gütigen Präsidenten jederzeit und relativ einfach auch völlig abgeschaltet werden, wenn er vermeiden will, dass seine Bürger sich untereinander telekommunikativ verabreden.** (Netzwelt nur für lupenreine Demokratien? in: Klumpp, D., Leitbildkonvergenz in der Netzwelt? Informationsgesellschaft vor der vierten Diskursdekade, edition sigma, Berlin 2010, S. 345).

Bis heute wird in der Diskussion weitgehend übersehen, dass zeitlich unbegrenzt erfasste große Mengen von Metadaten (z.B. Tracking) real existierendes Big Data sind.

Viele Länder und Regimes werden sich diese Möglichkeiten nie wieder nehmen lassen, auch wenn in den Rechtsstaaten die IT-Architekturen verändert werden sollten.

GSM Tracks (nur für Vorratszwecke)





LAC könnte „Location Area Code“ (Funkzelle) bedeuten, aber LAC 5233 ist keine Postleitzahl, die Nachbarzellen C1 und C2 sind für rein technische Zwecke angegeben (z.B. Trigonometrie).

„BSI 57“ könnte auch als technische Abkürzung „Base Station Ident“ bedeuten, aber auch vieles andere, aber bei Kürzeln weiß man das nie so recht.

Systeme/Algorithmen zuständig für Anfangsverdacht

„Dabei half das berüchtigte XKeyScore-Programm. Es wird so viel spioniert, dass die *menschlichen Kapazitäten* lange nicht mehr ausreichen. Die Systeme suchen nach Stichworten, ***auffälligen*** E-Mails (etwa mit großen Anhängen oder PGP-Verschlüsselung), Verbindungen zu anderen Personen, und so weiter. Daraus werden Scoring-Werte berechnet – je höher der Wert, desto interessanter ist vermutlich die Zielperson *für* ***manuelle*** *Auswertung*. Und noch nicht näher bekannte Menschen wurden so zu neuen Zielen“ (Sokolov, 20. Februar 2015).

Die automatisierte Feststellung von *Auffälligkeiten* beim Big Data Mining determiniert durch Scoring/ Ranking bereits den *Anfangsverdacht,* für den bislang *grundsätzlich und ausschließlich* „manuelle Auswerter“ wie Polizeien und Richter zuständig sind bzw. waren.

In aktiven *Rechtsstaaten* werden auch hierfür durch Schaffung von *Transparenzkontrollen durch unabhängige Institutionen* (z.B. Datenschutz, NGOs) Lösungen *vorgeschlagen*, in Unrechtsstaaten nicht einmal *gesucht*.

FIfF 2015: Kompromissvorschlag zur Verwendung von IP-Adressen
ULD 2015: Notwendigkeit von Personal zur Software-Gestaltung

Änderung für alles Softwaregesteuerte

Eine 'dramatische Änderung für alles Softwaregesteuerte' sieht Andrea Matwyshyn, Microsoft visiting professor at the Center for Information Technology Policy at Princeton University:

"But as more advanced devices use code, the *calculation of that risk is dramatically altered*. **The question of whether legal responsibility needs to be ratcheted up a notch in the software creation process is something we'll need to address in the near future."** (zit. von Chris Morris, Chilling Scenarios That Keep Privacy and Security Experts Up at Night, in: wired.com, May 12, 2015).

Dass **‚in naher Zukunft die Frage der *rechtlichen Verantwortung bei der Software-Erstellung ein Stück hochgeschraubt* werden '** muss, wird von Juristerei und Politik wohl bislang eher **nicht als dramatischer Handlungsbedarf verstanden.**

Weltweiter anonymer Broadcast-Empfang ist Vergangenheit

Schon die physikalischen Eigenschaften von Radiowellen (LW, KW. MW, UKW) **veränderten zwar die Empfangbarkeit von „Auslandssendern“**, aber **alle waren anonym empfangbar**, auch der unilaterale Satelliten-Broadcast.

Diese Funktion des unidirektionalen Broadcast kann das Internetradio oder das Internet-TV **nicht mehr erfüllen**. Denn der gütige und allseits geliebte Regierungschef kann im Internet nicht nur nachprüfen lassen, welches Radio- oder Fernsehprogramm gerade per *Streaming* empfangen wird, er kann sogar auch im Multicast-Modus nachprüfen lassen, **ob in einem Haushalt oder einer Hütte** seine abendliche „Rede an mein Volk“ auch **wirklich eingeschaltet ist bzw. war.**

Ja, sagen wir Rechtsstaats-Gewohnte, „aber er kann nur feststellen, welches Gerät welche Sendung empfängt, aber das lässt keine Rückschlüsse auf die natürliche Person zu“. Es ist für uns Rechtsstaatler nur schwer vorstellbar, dass etwas, was bei uns zu einer Verfahrenseinstellung vor Gericht führen würde, in vielen **Ländern zum außergerichtlichen Verschwinden ganzer Familien samt ihrer Nachbarn ausarten** könnte (…)

Mobilfunk und Internet sind interaktiv, nicht anonym

Was mithilfe des „Internet“ und anderer Daten-Netze, ja, sogar mit der „einfachen“ Mobiltelefonie in diktatorischen Schurkenstaaten mit den Nutzern geschehen könnte?

Welcher Nutzer in diesen Ländern weiß denn schon, dass **eine einzige Silent SMS über Mobiltelefon oder eine Mail mit 140 Zeichen an Twitter.com seine exakte Lokalisierung** samt anschließender Festnahme ermöglicht?

Lupenreine Lokalisierung durch Funkzellenabfrage mit unkalkulierbaren Folgen ist auch die Überprüfung, wer etwa eine „Dissidentin“ trotz **ausgeschaltetem** Mobiltelefon in ihrem Hausarrest besucht hat.

Wer die in einem solchen Land gesperrten oder **verbotenen Netzadressen auch nur anklickt, also nur zu erreichen *versucht*** oder sie gar über Umwege tatsächlich aufsucht, riskiert seine Existenz.

Die einzige Personengruppe, die auf personalisierte Mobiltelefonie und Internetnutzung weitestgehend verzichtet, sind **weltweit Banden-Bosse und Top-Terroristen.**

Wunschtraum autoritärer Staaten/Regimes ist bereits erfüllt

Ob eine Regierung es zulässt, dass die Bürger im Netz frei diskutieren dürfen, ist **für autoritäre Staaten und Diktaturen eine Sache der Abwägung**. In einer Harvard-Studie über China wurde analysiert, wann und wie genau in den dortigen sozialen Netzwerken Zensur ausgeübt wird. Das Ergebnis: Kritik an sich wird nicht automatisch geblockt. Erst ab dem Moment, in dem es um "collective action" geht, also wenn eine Masse zum Handeln aufgefordert wird, **setzt die Totalzensur** ein - und zwar unabhängig davon, ob die einzelnen Wortmeldungen positiv oder negativ ausfallen.

Syrien gilt seit Jahrzehnten als Land, das sehr genau kontrolliert, was die eigene Bevölkerung mitbekommen darf und was nicht. In Pressefreiheit-Rankings bekam das Land zu dieser Zeit 83 von 100 Punkten, wobei 100 für Unfreiheit steht. Gohdes vermutete hinter dem Schritt, das Internet für alle zu öffnen, politisches Kalkül (Anita Gohdes hat ihre Forschung im Rahmen des Hackerkongresses 31c3 am 5.1.2015 präsentiert).

Equipment und Software weltweit für Regimes verfügbar

IT-Sicherheitsexperte Magnus Harlander im F.A.Z.-Gespräch 24.10.2013

Wie hört man Handys ab, wie geht das technisch genau vor sich?
Bei einem Standard-Handy ist das Abhören absolut kein Problem. Prinzipiell gibt es mindestens zwei Möglichkeiten. Einmal über einen sogenannten IMSI-Catcher: Der „Gegner“ täuscht gewissermaßen eine Basisstation des Mobilfunkproviders für den Abgehörten vor, bei dem sich das Handy anmeldet, und von der aus er alle Kommunikation überwachen kann, SMSe genauso wie Gespräche, indem das Handymikrofon eingeschaltet wird. So einen **IMSI-Catcher kann man sich für 50.000 Euro kaufen oder, in einer erheblich einfacheren Version, mit einem Bausatz für zwei- bis dreihundert Euro selbst zusammenbasteln.** Die zweite Möglichkeit ist, dass der Gegner, beispielsweise die NSA, der abzuhörenden Person SMSe oder MMSe schickt, **mit oder ohne Anhang, die auch unsichtbar sein, also im Hintergrund bleiben** können. So kann das Handy manipuliert und zum Beispiel **zusätzliche Software** installiert werden.

Russland und China: Nichtangriffspakt im Internet

Moskau drängt parallel nicht erst seit dem Ukraine-Konflikt darauf, die Rolle der USA bei der **Internetverwaltung** einzuschränken und das Netz stärker zu kontrollieren. Das Pentagon hat seinerseits im April eine neue Strategie der USA für die Kriegsführung im Internet präsentiert. Als die aktivsten und **gefährlichsten Länder im Bereich Internetattacken** nennt der Report China, Russland, den Iran und Nordkorea. (Stefan Krempl, Heise 13.5.2015)

Western sanctions against Russia over the crisis in Ukraine have caused Russian officials to re-evaluate areas of **critical dependency** on Europe and the U.S., and increasingly turn to the east. Russian lawmakers have also campaigned for **tighter control over the Internet** following the revelations by (...) Edward Snowden.

President Vladimir Putin, meanwhile, has called for **moving key online infrastructure into Russia** from overseas, complaining publicly last year **that the Internet began as "a CIA project."** (Russia and China Pledge Not to Hack Each Other, Olga Razumovskaya, Blog Wall Street Journal, 8.5.2013)

Yandex: Privacy Browser – künftiger Exportschlager?

Der russische Suchmaschinenbetreiber Yandex.ru hat die Betaversion seines Browsers für Windows und Mac OS X veröffentlicht. Der **Yandex-Browser erleichtert anonymes Surfen** und **schützt die Privatsphäre** seiner Nutzer, versprechen die Macher. Außerdem sollen **keine "statistischen Daten"** zu den Aktivitäten im Browser erfasst werden.

Mit einem Klick lässt sich auf Wunsch ein **"Stealth Mode"** aktivieren. Der Browser **blockiert dann Tracking-Pixel, Analyse-Tools und Cookies von Drittanbietern**. Wer keine "Likes" verteilen will, kann zudem die Widgets der sozialen Netzwerke blockieren. Vertrauenswürdige Websites lassen sich auf eine Whitelist setzen. Zudem kann **der Nutzer in den Einstellungen festlegen**, welche Inhalte der Browser ausfiltern soll, und welche passieren dürfen. (22.05.2015)

Schon **2005 wünschten** einige ältere Moskauer Verwaltungsmitarbeiter (in perfektem Englisch) auch **für das einfache ganze Volk preislich adäquate Mobiltelefone.** Für die Bemerkung „ja, es ist in einer Demokratie gut zu wissen, wo die Bürger sind“, gab es Schulterklopfen (You ‘ve got it, man!),

btw: ein nicht öffentlich-rechtlicher Browser ohne Gebühren und ohne Werbeeinnahmen?

Türkische Regierung will kostenlosen Internetzugang einführen

Obgleich die türkische Regierung in stetem Kampf gegen das Internet und die sozialen Netzwerke ist, die Zensur zunimmt und die freie Meinungsäußerung immer eingeschränkter wird, will das Entwicklungsministerium nach seiner Strategie für die Informationsgesellschaft 2015-2018 die digitale Kluft schließen und den Bürger und Familien mit geringem Einkommen einen **kostenlosen Internetzugang** zur Verfügung stellen.

Nach der Website Engelli Web haben die türkischen Behörden den Zugriff auf 67.683 Adressen gesperrt. Das **kostenlose Internet für die Armen** könnte auch eine Möglichkeit sein, ein **noch besser staatlich reguliertes Internet** einzuführen. Mit dem kostenlosen Internet soll auch die Internet-Infrastruktur **modernisiert** werden. Neubauten müssen einen Internetzugang ermöglichen.

Es gibt in der Türkei mit einer Bevölkerung von **80 Millionen Menschen fast 70 Millionen Handys.** Bis zum Ende des Jahres sollen 4G-Mobilfunknetze verfügbar sein. Innerhalb der nächsten sechs Jahre sollen nach dem Verkehrs- und Kommunikationsminister mindestens 90 Prozent auf 4G-Netze zugreifen können. (Florian Rötzer,Telepolis*10.03.2015)*

Macht das Transparenzgebot Schule?

Als Folge des zweiten Weltkriegs sind **staatliche Nachrichtendienste** in Deutschland und Japan **an gesetzliche Grundlagen gebunden** und sind damit auch gegenüber dem Parlament berichtspflichtig.

In Frankreich galt noch 1999 sogar unter Datenschützern der Grundsatz „Ils sont secrets, que l ‘on pourrait faire?“, dies wird aus praktischen Gründen in vielen Ländern mit Hinweis auf die **volle Akzeptanz des UN-Zivilpakts** gepflegt, auch wenn das "Recht auf Privatheit im digitalen Zeitalter" der UN-Generalversammlung nicht völkerrechtlich bindend ist.

Im angelsächsischen Recht waren Gesetze wie z.B. der Patriot Act erforderlich, um eventuell notwendige Gesetzesübertretungen zu legitimieren. Die **NSA reform bill** ist aktuell in den USA im Senat abgelehnt. EFF sagt: “Section 215 of the Patriot Act has been wrongly interpreted in secret by the government for years”.

US-Regierung lässt NSA-Überwachungsbefugnisse auslaufen: Das Weiße Haus hat die Genehmigung zur Sammlung von Verbindungs- und Standortdaten durch die NSA nicht verlängern lassen **(**26.05.2015 19:16, wird sicher zeitnah erneuert).

Fefes Blog 22 MAI 2015: Doch noch das Resignieren lernen?

- Hier kommt gerade ein Linktipp herein, bei dem der Kommentar mir wichtiger ist als der Link selbst. Der Link geht zu dieser **Story, dass die HUK-Coburg ihre Tarife an das Fahrverhalten anpassen will.** Das hat der CCC jahrelang als **Horrorszenario** an die Wand gemalt, langfristig mit Gesundheitsdaten, kurzfristig mit Fahrverhalten. Insofern: Scheiße, dass wir bei sowas immer Recht haben.

- Schön **langsam habe ich keine Lust mehr im IT Sektor zu arbeiten**, wenn ich solche Meldungen lese. Ich trage zwar keine direkte Schuld daran, dass sowas implementiert wird, bin jedoch eines der **kleinen Rädchen, die dafür verantwortlich sind, dass die Infrastruktur läuft,** die derartige Sachen ermöglicht!

- (Wenn) ich derartige Meldungen lese und dann die **Veränderungen der letzten Zeit in die Zukunft interpoliere, dann hoffe ich, dass ich einer der Pessimisten bin!** Schade eigentlich...ich war halt immer derjenige, der der Meinung war, dass der technische Fortschritt UNS zugute kommt!

Schritt von Big Data zu All Data

Schon **Big Data** macht Ergebnisse von Algorithmenkombinationen für Menschen praktisch unkontrollierbar, bei **All Data** ist Maschinen-Totalitarismus möglich. Wo kann man “nicht resignieren”?

http://futureoflife.org
In January, the British-American computer scientist Stuart Russell drafted and became the first signatory of an open letter calling for researchers to look beyond the goal of merely making artificial intelligence more powerful. “We recommend expanded research aimed at ensuring that increasingly capable AI systems are robust and beneficial,” the letter states. “Our AI systems must do what we want them to do.”

Future of Life: Artificial Intelligence Kontrollforschung : “(...) we cannot predict what we might achieve when this intelligence is magnified by the tools AI may provide, but the eradication of war, disease, and poverty would be high on anyone's list. However, like any powerful technology, AI has also raised new concerns, such as ***humans being replaced*** on the job market and ***perhaps altogether”*** (FLI 2015).

Der Cyberlehrling: Code! Code manche Strecke …

Walle! Walle
Manche Strecke,
Daß, zum Zwecke,
Wasser fließe,
Und mit reichem, vollem Schwalle
Zu dem Bade sich ergieße.

http://www.textlog.de/18471.html

Code! Code
Manche Strecke,
Dass, zum Zwecke,
Software fließe,
Und mit digitalem, vollem Schwalle
Zu Big Data sich ergieße.