Protokoll der Frühjahrstagung 2019
Imperiale Lebensweise, die Realitäten in Brasilien und Perspektiven der Solidarität
www.kooperation-brasilien.org

Titel: Praxisworkshop: Freiheit in autoritären Zeiten - Datenschutz und Tools zur sicheren Kommunikation in Journalismus und NGOs

Datum: 30.03.2019
Uhrzeit: 9:30 Uhr

Podium/Input: Jens Gutsche und Jonas Vollmer

Moderation: Jan Erler zur Einführung

Protokoll: Viktoria Wölfl

Kurze Einführung in den Tag mit Jan Erler inklusive organisatorischer Informationen.

Peter Zorn sagt etwas zur Stellungnahme, die später in der Mitgliederversammlung besprochen werden soll. Daher sollte sie vorher jedes Mitglied durchgelesen haben. Wenn man sich einig wird, wird das in der MV beschlossen bzw. Änderungen werden auch besprochen und sind noch möglich einzubringen.

Vorstellung der Arbeitsgruppen:

1) Imperiale Lebensweise mit Bettina Köhler: Bestandsaufnahme zu gestern, was ergeben sich für Fragen und wo würde es Sinn man in die Tiefe zu gehen, nach Bedarf in der Runde. Verbindung mit konkreten Erfahrungen, Verknüpfung mit Brasilien
2) Selbstbestimmt Digital e.V.: wie kann man sensibel mit Daten umgehen, gerade in diesen Zeiten umso wichtiger. Kurzer Überblick, erste Schritte wie man Kommunikation sicher gestalten kann. Live Schaltung mit dem Zivilrechtler Danilo Daneda aus Rio.

*Arbeitsgruppe 2 mit Selbstbestimmt Digital e.V. (*ca 20 Teilnehmer*innen):

Jonas erklärt zum Einstieg die drei Basics zur Grundlage:

1) sei dein eigener Chairman/women: eigener Lernfortschritt und Zeit, aber auch Rücksicht
2) ich bin pünktlich, da auch ein Live-Schaltung mit Danilo Daneda geplant ist
3) ich lasse mich überraschen

Danach kurze Vorstellungsrunde, bunt gemischt, sehr viele Teilnehmer*innen aus diversen Organisationen, aber auch vereinzelt Student*innen.

Ziel ist ein **Digitales Empowerment** zum kritischen mitgestalten, wie kann man sich zu netzpolitischen Themen äußern kann, neue technische Entwicklungen, sowie neue Datenschutzgrundverordnung, aber auch die Frage wie Social Media Tools auf Wahlen Einfluss nehmen und was man hier tun kann, soll besprochen werden.

Kurze Vorstellung der Referenten Jonas Vollmer und Jens Gutsche, sowie der eigene Brasilien Hintergrund.

Thematischer Einstieg mit einem **Szenario über die Schließung einer NGO in Brasilien**. Dazu gibt es drei Fragen, die wir mit unserem Sitznachbarn besprechen sollen: 1) Welches Gefühl löst die Geschichte bei und aus? 2) Welche Erfahrungen haben wir schon selbst mit ähnlichen Geschichten gemacht? 3) Welche Fragen ergeben sich für uns aus dieser Situation?

Antworten: Wut, Angst, Traurigkeit, Machtlosigkeit -> Wie kann man mit diesem Szenario in der Realität umgehen, welche Handlungsmöglichkeiten gibt es, auch hier für uns in Deutschland? Link zur Rechtsfrage? Kriminalisierung? Welche Kommunikation?

➔ Welche Berührungen haben wir im Alltag mit Datenschutz und Sicherheit? Und was will ich heute mitnehmen?

Der Klassiker, wenn es um Datenschutz geht: **„Ich habe doch nichts zu verbergen".** Aber wenn man alle Apps durchschaut die man benutzt, denkt man meist schnell ganz anders darüber. Aber nicht nur der digitale Raum, sondern auch der analoge Raum und die vernetzte Umwelt birgt hier Gefahren, die man mitdenken sollte!

Privatsphäre Modell in dieser Reihenfolge: allein, intim, Familie, Wohnung, echte Freunde, Gesellschaft/Staat/Wirtschaft

Privatheit ist politisch, denn ohne Privatheit gibt es keine Demokratie (persönliche Autonomie, emotionaler Ausgleich, Selbstevaluation, geschützte Kommunikation – um zu verhindern manipuliert und dominiert zu werden -> es geht in Richtung Überwachungsstaat und das ist sehr bedenklich!

➔ Um was geht es im **Datenschutz**? Sicherheit, Auskunft, Transparenz. Es geht aber nicht um Technik

Unterschied zwischen Datenschutz und Datensicherheit. 1) Datenschutz ist Privatsphäre (Handynummer, Gehalt, Geburtstag) 2) Datensicherheit ist IT-Sicherheit (Hacking, Firewall, Passwörter etc.)

<u>Aber beides ist miteinander verbunden, denn oft gibt es ohne Technik, also Datensicherheit, keinen Datenschutz.</u>

- Datenschutz durch Technikgestaltung
- Datenschutzfreundliche Voreinstellungen
- Neue Rechte als Verbraucher

Schutz gegen den Staat benötigt sehr viel Gedanken und Zeit und ist nicht von heute auf morgen möglich. Im Allgemeinen geht es aber vor allem darum nicht einfach irgendetwas zu machen, weil es alle machen, sondern selbstreflektiert darüber nachzudenken!

➔ Wissen praktischen anwenden: **Messenger**

Whatsapp ist weltweit und im Besondern auch in Brasilien der meistgenutzte Messenger. Die App ist im Allgemeinen aber kein Mittel zur sicheren Kommunikation, da sie die Daten an unsichere Drittländer weitgeben!

Sichere Messenger wären beispielsweise Open-Source und/oder End-to-end Verschlüsselt!

Szenario mit drei Menschen in Sao Paulo, die prüfen wollen welcher Messenger für ihre Bedürfnisse am besten geeignet wäre. Die Seite www.securemessagingapps.com informiert über diverse Messaging-Apps und ihre Vorteile/Nachteile.

Kriterien im Szenario: Finanzierung, ID-Vergabe, Transparency Report, End-to-end Verschlüsselung, von der App gesammelte Kundendaten, Daten auf dem Server des Anbieters verschlüsselt

Wir vergleichen drei Apps: Whatsapp, Signal und Threema. Das Ergebnis ist nicht ganz klar, wobei Whatsapp natürlich ganz durchfällt. Signal und Threema halten mehr oder minder die Waage, wobei der Vorteil bei Signal sicher die Open-Source Struktur ist.

Fabian kritisiert, dass Threema eben nicht Open-Source ist und dadurch auf externe Zertifizierungen angewiesen sind, die aber nicht immer die beste Lösung sind wie man am aktuelle Beispiel von Brumadinho und TÜV-Süd sehen kann!

Weitere Frage die aufgeworfen wird: Kann man der Seite www.securemessagingapps.com vertrauen? Wichtigkeit die Quellen zu prüfen wird unterstrichen. Die Referenten vertrauen aber auf die Seite, da diese schon durch mehrere eigene Datenschutzbeauftragte abgesichert wurden.

PAUSE 11:15 Uhr bis 11:30 Uhr

➔ **Live-Schaltung nach Rio de Janeiro:**

Nach der Pause ist **das Interview mit Danilo Daneda via appear.in** (Alternative zu Skype) geplant, das allerdings durch die schlechte Internetverbindung nach kurzer Zeit unterbrochen werden muss.

Danilo Daneda ist Anwalt und Datenschutzexperte und informiert uns über die Durchsetzung eines neuen Datenschutz-Gesetzes in Brasilien, das letztes Jahr im August in Kraft getreten ist und dem Präsidenten viel Macht gibt, was massive Auswirkungen hat -> **Marco Civil**

➔ **Sichere Kommunikation via E-Mail:**

Vorab: Vorsicht vor allem bei Öffnen von Anhängen. Man muss dem Absender vertrauen! Aber auch bei Absender und Links ist Vorsicht geboten: Oft wird versucht an Nutzerdaten zu gelangen.

Wie kann ich meine E-Mail verschlüsseln? –> mit zwei Schlüsseln: einen Schlüssel habe ich selbst (privat) und einem öffentlichen Schlüssel: Klartext –> Schlüssel -> Geheimtext -> privater Schlüssel

➔ **Open-Source Alternativen zur Datenspeicherung?** Beispielsweise Nextcloud

Welche Anforderungen habe ich an eine Cloud?

- Verschlüsselt der Anbieter meine Daten auf seinem Server?
- Macht der Anbieter Updates von seiner Software?
- Quellcode offen?
- Finderlohn für Fehler?
- Ist das Geschäftsmodell offen erkennbar?
- Gibt es Sicherheitshinweise zu Lücken?

Open Source Software? Heißt, dass jede Textzeile offen zugänglich ist, jeder damit arbeiten kann und so auch jeder überprüfen kann. Jeder kann die Software umschreiben! Dadurch gibt es keine Lizenzgebühren, und Tausende Beteiligte, die mit hoher Wahrscheinlichkeit kritisch überprüfen!

Nextcloud versucht die Nutzer zu stärken, sie stellen die Kernsoftware zur Verfügung -> Open Source

Danach ist eine Gruppenübung mit Nextcloud angedacht, das funktioniert aber nur die Server-Überlastung nicht ganz und Jens stellt Nextcloud einfach selbst vor: Kalender, Kontakte aber auch gemeinsame Dokumentenbearbeitung ist dort möglich. Die Software ist grundsätzlich kostenlos, die Infrastruktur dahinter kostet aber! Jens zahlt dafür circa 2Euro im Monat.

Generell muss aus unseren Köpfen heraus, dass das Internet gratis ist, denn sonst bezahlen wir mit unseren Daten!

- ➔ Alternatives und kooperatives Arbeit ist vor allem auch die die Open-Source Plattformen Etherpad und rise-up Pad möglich. Dort können mehrere Personen gleichzeitig arbeiten und die Daten werden nach 70 Tagen vernichtet.
- ➔ Kurze Diskussion über Proton-Mail: ist grundsätzlich sehr sicher, aber natürlich nur, wenn beide Parteien es nutzen.
- ➔ Idee sich am Nachmittag nochmal kurz zusammenzusetzen, um weitere Themen besprechen zu können (Zeit ist einfach zu knapp)

- ➔ **Was nehmen wir mit?**

Es ist kompliziert. Der Workshop gab uns konkrete Anregungen und Anhaltspunkte, es ist aber noch zu wenig um wirklich anfangen zu können.

Wenn man sich wirklich absichern möchte, braucht das sehr viel Zeit! (vor allem gegen den Staat)

Dennoch: die Anregung das Thema Datensicherheit mit dem Partner/ der Partnerin durchzusprechen und dann weitergehen zu können. Denn es ist wichtig darüber zu kommunizieren, viel zu oft wird es vermieden, da auch die Wissensbestände zum Thema sehr unterschiedlich sind. Doch nur über Austausch kann Veränderung passieren.

WICHTIG: **Privatheit ist ein Grundbaustein von Demokratie** und genau deswegen ist auch das Thema rund um Datenschutz und Sicherheit so unglaublich wichtig!

MITTAGSPAUSE 12:45 Uhr bis 13:30 Uhr/15 Uhr

Von 13:30 Uhr bis 14 Uhr gibt es noch einen kurzen Einschub zu den Themen Backups und Passwörter für Interessierte:

Datensparsamkeit und Datenhygiene sind sehr wichtig: was brauche ich wirklich? -> Unnötige Online-Konten unbedingt löschen!

Gut wäre es so lokal wie möglich zu bleiben. Dennoch: die ganze Welt muss sich an die europäische Datenschutzgrundverordnung halten!

- ➔ **Backup-Empfehlung**: 1 Original und 2 Kopien auf unterschiedlichen externen Datenträgern und dann im besten Fall wöchentliche Updates, aber immer mit der Frage im Hintergrund: Wie viel Verlust an Arbeit kann in mir leisten? -> Empfehlenswert ist auch eine Datensicherung via Nextcloud!

➔ Sicheres **Passwort-Management**: 12 Zeichen, Groß und Klein, Sonderzeichen und Zahlen

Jonas hat selbst ein kleines Buch, in dem er alle seine Passwörter verwaltet, sonst kann man das Ganze auch digital über einen Passowort-Manager (Kee-Pass) probieren!

Wichtig ist vor allem auch, die Passwörter einmal jährlich zu wechseln -> inklusive Datenhygiene

Auf der Seite www.haveibeenpwned.com kann man herausfinden, ob man schon einmal gehackt wurde!

PAUSE 14 Uhr bis 15 Uhr