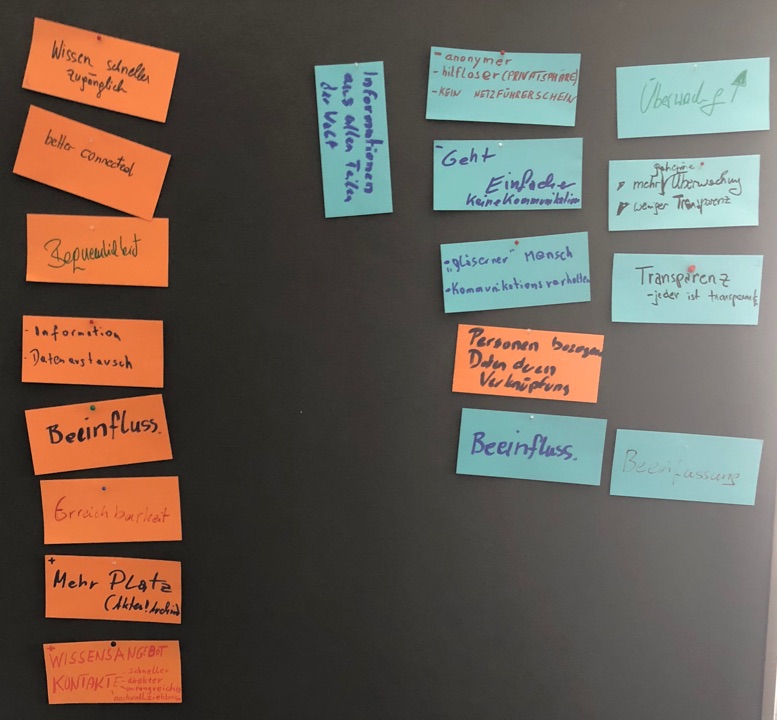
***Kurzbericht zum Workshop***

*Walter Peissl*

# Datenschutz und Demokratie – Wie das Netz unsere Gesellschaft verändert

Der von epicenter.works (<https://epicenter.works/>) gestaltete Workshop zu neuen Technologien und Demokratie beschäftigte sich mit grundlegenden Fragen der Privatsphäre, den Einstellungen dazu und möglichen Folgen bzw. Hinweisen zur digitalen Selbstverteidigung.

Als Einstieg wurde ein Blitzlicht erstellt in dem jede/r der TeilnehmerInnen kurz darstellen sollte, worin Vor- und Nachteile der Vernetzung gesehen werden. Das Bild unten zeigt die Verteilung am Beginn des Workshops. Orange die Vorteile und auf blauen Kärtchen die erwarteten Nachteile.



Danach wurde im ersten Theorieblock einige zentrale Fragen behandelt: Was ist Privacy? Wozu braucht man das und was ist am Argument „Ich habe ja nichts zu verbergen“ dran? Was gefühlte (nicht notwendigerweise reale) Überwachung mit Menschen macht wurde am Beispiel des Panopticons von Jeremy Bentham diskutiert. Weiters wurden einige rechtliche Grundlagen zum Thema Privatsphäre erläutert und auch einige Aspekte der DSGVO vom Vormittag wiederholt.

Dazu zählen die Grundsätze des Datenschutzes:

* Rechtmäßigkeit
* Zweckbindung
* Speicherbegrenzung
* Datenminimierung
* Richtigkeit, Integrität und Vertraulichkeit.

Aus der DSGVO wurde speziell auf die Betroffenenrechte eingegangen:

#### Informationspflicht

#### Auskunftsrecht

#### Recht auf Berichtigung

#### Recht auf Löschung

#### Recht auf Einschränkung der Verarbeitung

#### Recht auf Datenübertragung

#### Widerspruchsrecht

Anhand konkreter Beispiele wie dem „Social Credit System“ in China, dem Gesundheitsprofiling von Versicherungen (auf freiwilliger Basis in Europa und teilweise schon verpflichtend in den USA), sowie konkreter Spuren, die man beim Surfen im Netz hinterlässt wurde ein Bogen von staatlicher, über privater bis zur betrieblichen Überwachung gespannt.

Im zweiten Teil wurde eine Vertiefung eines von zwei Themen angeboten:

* Thema 1: Staatliche Überwachung, aktuelle gesetzliche Initiativen und
* Thema 2: Digitale Selbstverteidigung

Die TeilnehmerInnen entschieden sich mit großer Mehrheit für Thema 2.

In diesem Block ging es darum die Sensibilität für Spuren im Netz und ihre mögliche Vermeidung zu heben. Wichtigste Aussage war, dass zu vielen der gut funktionierenden und teilweise ja auch hilfreichen Anwendungen privatsphärenfreundliche Alternativen bestehen.

Als Beispiele wurden der Browser Firefox (<https://www.mozilla.org/de/firefox/new/>) und einige dazu passende Add-ons vorgestellt: Privacy Badger (<https://addons.mozilla.org/de/firefox/addon/privacy-badger17/>) blockt unsichtbare Tracking Software, die das Surfverhalten aufzeichnen soll, Ghostery (<https://www.ghostery.com/de/>) ist eine Software, die den Anwender beim Surfen auf versteckte Dienste hinweist, die im Hintergrund private Daten an Seitenbetreiber übermitteln, und diese auf Wunsch blockiert. Werbungsfrei ist man durch uBlock origin (<https://addons.mozilla.org/de/firefox/addon/ublock-origin/>). Https-everywhere (<https://www.eff.org/de/https-everywhere> ) stellt, dort wo verfügbar, immer auf die sichere verschlüsselte Kommunikation mit dem Webserver um.

Besonderes Augenmerk sollte auf Suchmaschinen gelegt werden, den Google, der Platzhirsch, weiß mehr über die UserInnen, als die oft selbst über sich. Eine Alternative ist Startpage (<https://www.startpage.com/>) eine Suchmaschine, die in Google sucht, sich aber zwischen Google und die UserInnen schaltet und die Suchverläufe nicht aufzeichnet.

Wer ganz sicher gehen möchte, nicht verfolgt werden zu können, muss allerdings geringe Einbußen bei Leistungsfähigkeit und Schnelligkeit in Kauf nehmen. Bei der Verwendung des Browsers Tor (<https://www.torproject.org/>) kommt das so genannte Onion-Routing zur Anwendung, was den Weg von der nachfragenden NutzerIn zur angesteuerten Website in Form von Zwiebelschalen über mehrere Schichten (Server) weiterleitet und so nicht zurück verfolgbar macht.

Zur Kommunikation am Smartphone kann man statt Whatsapp z.B. Signal (<https://signal.org/>) verwenden, für Einmal e-mails (um sich zB bei einem Newsletter anzumelden) gibt es mehrere Services. Hier lag die Empfehlung klar auf: spamgourmet (<https://www.spamgourmet.com/index.pl>)

In der Diskussion wurde vor allem ein Thema sehr prominent diskutiert. Aus Berichten von Betroffenen wurde nämlich deutlich, dass sich Netzwerkeffekte (was viele nutzen, kann man kaum umgehen bzw. neue Markteintritte sind extrem schwer) auch zu starkem sozialen Druck führen können. Wer etwa seinem Kind die Nutzung von Whatsapp verbietet, weil es zB. die Adressen aus dem gesamten Adressbuch des jeweiligen Smartphones runterlädt und ev. mit Facebook (dem Eigentümer von Whatsapp) teilt, läuft Gefahr, dass das Kind in der Schule, in der Peer-Group, ausgeschlossen und von (sozial) wichtigen Informationen abgeschnitten wird. Hier wurde darauf hingewiesen, dass es allein wahrscheinlich schwer sein dürfte sich gegen alle anderen zu stellen, dass aber Unterstützung durch ExpertInnen (etwa von epicenter.works ) und die Vorstellung von Alternativen (zB.: Signal) hilfreich sein könnten.

Insgesamt war der Workshop sehr hilfreich um zur bewussten, datensparsamen und privatsphärenfreundlichen Nutzung des Internet beizutragen. Die vorgestellten Instrumente haben deutlich gemacht, dass ein hilfloses Ausliefern an die Datenkraken nicht notwendig ist und mit ein wenig Wissen viele Datenspuren vermieden werden können.

Details zu den Instrumenten finden sich auch unter:

<https://epicenter.works/crypto>