



## Terminologie

**Digital Phenotyping:** Das Analysieren von Online-Spuren (durch Smartphone-, Social Media-, oder „Internet of Things-Nutzung (IoT)), um Aufschluss auf Personen-Merkmale zu erlangen. Möglicherweise wird diese Form der Psychodiagnostik in naher Zukunft so gut sein, dass sie nur unter Verwendung von IoT-Spuren relativ verlässliche Vorhersagen über Vorlieben oder sogar über unseren Gesundheitszustand treffen kann.

**Filterblase:** Social Media Plattformen präsentieren im News-Feed individualisierte Nachrichten. Der Feed wird unter anderem so zusammengestellt, dass Themen, die von einem Nutzer mit einem „Like“ versehen worden sind, eher im eigenen Feed zu finden sind. Falls sich eine Person ausschließlich auf einer Social Media Plattform informiert, besteht die theoretische Gefahr einer einseitigen Sichtweise auf eigentlich pluralistisch diskutierten Themen.

**Internet of Things (IoT):** IoT beschreibt eine Gesellschaft, in der von der Kaffeemaschine bis hin zum Auto alle Gegenstände mit dem Internet verbunden sind.

**Machine Learning:** Üblicherweise präsentiert der Wissenschaftler dem Computer Bilder oder andere Inhalte, die mit einer Kategorie versehen sind. Etwa ein Stapel an Bildern der Männer und einen Stapel an Bildern der Frauen zeigt. Die Maschine lernt aufgrund von Vorgaben selbständig Muster zu erkennen, die typisch für ein Bild mit einem Mann oder mit einer Frau wären. Mit steigenden Trainingseinheiten lernt der Computer noch unklassifiziertes Material selbst zu kategorisieren.

**Psychoinformatics:** Ein interdisziplinäres Forschungsvorhaben, bei welchem Methoden der Informatik in der Psychologie verwendet werden. Genutzt werden Techniken wie Machine Learning, Textmining, aber auch das Nutzen von Apps auf Smartphones, um Verhalten zu studieren.

**Textmining:** Die Analyse-Technik untersucht, welchen emotionalen Gehalt die Nachrichten einer Person in SMS-Nachrichten oder bei Facebook beinhaltet. Dies kann nicht nur Aufschluss über interindividuelle Differenzen in Emotionalität zwischen Personen geben, sondern Aussagen über die Größe des Sprachschatzes, oder Ich-Bezogenheit etc. einer Person machen.

**Microtargeting:** Aufgrund bestimmter Merkmale einer Person wird versucht, eine möglichst passgenau Werbebotschaft an ebendiese zu versenden. Es gibt Hinweise, dass diese Technik bereits zur Wahlmanipulation eingesetzt worden ist.

## Tipps im Umgang mit Daten

**Browser:** Nutzen Sie alternative Web-Browser auf PC und Handy wie beispielsweise Firefox. Hier können Sie individuell und restriktiv das jeweilige Verhalten festlegen.

**Messenger:** Verzichten Sie auf Messenger oder nutzen Sie Alternativen zu WhatsApp und Facebook-Messenger. Diese sind beispielsweise Signa, Threema oder DeltaChat.

**E-Mail Anbieter:** Alternative E-Mail-Anbieter wie Posteo bietet Datenzentren in Deutschland und analysieren nicht die Inhalte der eigenen E-Mails.

**Lesezeichen statt Apps:** Nahezu alle Apps sammeln mehr Daten als sie müssten. Schlagen Sie den Anbietern ein Schnippchen und nutzen Sie Lesezeichen und den Browser. Nahezu alle Webseiten sind für mobile Geräte optimiert.

**Handy-Berechtigungen:** In den Einstellungen können Sie den Apps gezielt Berechtigungen wie die Lokalisierung entziehen. Fragen Sie sich zudem, ob jede App wirklich benötigt wird und löschen Sie ungenutzte mitsamt den hinterlegten Profilen.

**Zugangsschutz:** Verschlüssen PC und Handy. Nutzen Sie einen biometrischen Zugangsschutz oder ein Passwort.

**Kostenlose Angebote:** Nichts ist kostenlos. Hinterfragen Sie Modelle, bei denen Ihnen Dienste kostenlos angeboten werden. Meistens zahlen Sie mit Ihren Daten.

**Öffentliche Netzwerke:** Meiden Sie öffentliche, fremde oder ungesicherte Netzwerke.

**Firewall:** Eine Firewall auf dem Handy unterbindet ungewünschte Verbindungen ins Netz von einzelnen Apps.

**Social Media Plattformen:** Nutzen Sie die Plattformen bewusst oder steigen Sie noch besser auf Alternativen um (Futopolis). Oft sind Plattformen auch einfach nur Zeitfresse. Ein gutes Buch, eine Zeitung oder ein Gespräch stellen oft eine sinnvolle Alternative dar.

**URLs kürzen:** Wenn Sie URLs kürzen möchten, können Sie auf datenschutzkonforme Dienste zurückgreifen, die keine Daten speichern oder Statistiken erheben. Etwa [t1p.de](http://t1p.de)

**Android-Alternativen:** Fortgeschrittene Benutzer können bei Smartphones mit dem Android-Betriebssystem ein alternatives System aufspielen wie etwa LineageOS. Bei Apple bringt das sogenannte „Jailbreaken“ weitreichende Zugriffsmöglichkeiten. Beachten Sie jedoch etwaige Garantieverluste.

**Filmtipp:** ARD-Dokumentation „Facebook außer Kontrolle?“: <http://t1p.de/meineDaten>