Für Fortgeschrittene:

6. OpenSource Betriebssysteme

Über 99 % aller Smartphones weltweit haben entweder ein **Android oder iOS** Betriebssystem, gehören also entweder zum Ökosystem von Google oder Apple. Doch es ist auch möglich, ein Smartphone ohne die beiden Big-Tech-Konzerne zu nutzen. Dein Android-Handy kannst du zum Beispiel auf **/e/ OS, Calyx, Lineage oder Graphene** betreiben. Schau doch mal nach, mit welchem System dein aktuelles Handymodell kompatibel ist.

Für PCs empfiehlt sich die Nutzung von **Linux** oder Linux-Versionen wie **Ubuntu**. Das klingt zu kompliziert? In vielen Städten gibt es auch Linux-Install-Parties, bei denen dir erfahrene Menschen helfen können.

Deine Ideen & Notizen:

Was ist dabei zu beachten?

Diese Tipps sind ein super erster Schritt, um sich tiefer mit dem Thema Datenschutz und -gerechtigkeit zu beschäftigen. Wichtig ist es, zu verstehen, dass es primär Ansätze auf **individueller Ebene** sind. Jedoch sollte es natürlich **keine individuelle Verantwortung** sein, die gesellschaftlichen Risiken, die von Datenaggregation und Machtasymmetrien ausgehen, zu bewältigen.

Nicht alle Menschen haben die Kapazitäten und Ressourcen, um sich technisch vor Datenüberwachung, Vorhersagen und Diskriminierung zu schützen. Trotzdem verdienen sie natürlich den **gleichen Schutz in ihren Grundrechten!** Daher braucht es Veränderungen auf allen Ebenen!

Wir empfehlen, diese Schritte als Einladung zu nutzen, um einen **besseren Einblick** zu bekommen, wie unsere digitale Welt aufgebaut ist und funktioniert.

ein Projekt von

DATA ETHICS OUTREACH LAB

AG Ethik und kritische Theorien der Künstlichen Intelligenz

Universität Osnabrück

https://ikw.uni-osnabrueck.de/forschung/ethik_der_ki/deol.html

TIPPS FÜR kollektiven & macht-kritischen DATENSCHUTZ

1. App-Berechtigungen checken

Bevor du eine neue App installierst, lies dir durch, worauf sie **Zugriff** verlangt. Brauch sie wirklich Zugang zu deinen Kontakten, deinem Standort oder Mikrophon? Kommen dir die Berechtigungen merkwürdig vor, suche nach alternativen Apps.

Besonders empfehlenswert sind Open-Source Apps, die du zum Beispiel im **F-Droid Store** finden kannst.

2. Unique Identifier vermeiden

Um Online-Shops oder andere Dienste zu nutzen, müssen wir uns eigentlich immer mit einer E-Mail-Adresse registrieren. Da jede E-Mail-Adresse nur einmal existiert, ist sie ein „unique identifier". Dadurch können Daten von **verschiedenen Quellen** später besonders leicht zusammengeführt werden und so noch mehr Wissen generieren. Es wäre z.B. möglich, Informationen aus deinem LinkedIn Profil mit deiner Bestellung bei einem Online-Sexshop zu verknüpfen.

Einige Mailanbieter bieten es an, **Aliase** zu erstellen. Das sind E-Mail-Adressen, die zwar eine andere Adresse haben, aber deren E-Mails am Ende trotzdem bei dir im Postfach landen.

Mit **Plus-Adressen** lassen sich ganz einfach für jeden Online-Shop/Dienst eine eigene E-Mail-Adresse verwenden, z.B.:
meineemail+onlineshop@mail.de

3. Keine Telefonnummer angeben

Ein weiterer Unique Identifier sind **Telefonnummern**. Eine neue E-Mail-Adresse ist schnell erstellt, aber eine neue Telefonnummer zu bekommen, kostet Zeit, Geld und verlangt sogar die Vorlage eines Ausweisdokuments. Kein Wunder also, dass Telefonnummern zur Registrierung bei Online-Diensten immer mehr Anwendung finden.

Überprüfe daher: Ist es überhaupt **notwendig, eine Telefonnummer anzugeben?** Ist irgendwo ein Button zum Überspringen oder Schließen eines Pop-Ups oder ist das Feld keine Pflichtangabe?

Geht es ohne Telefonnummer tatsächlich nicht weiter, kannst du dich fragen, ob dieser Online-Dienst dich tatsächlich telefonisch erreichen sollte/muss. Falls nicht, kannst du stattdessen auch eine **Fantasie- Nummer** angeben.

4. Browser richtig einstellen

Zunächst ist die Wahl des Browsers entscheidend: **Firefox** ist freie, non-profit Software und ist daher unbedingt Chrome, Edge oder Safari vorzuziehen!

Außerdem solltest du in deinen Browsereinstellungen auf jeden Fall **Drittanbieter-Cookies deaktivieren**, da diese genutzt werden können, um dich über verschiedene Seiten und Sessions zu tracken.

Empfohlen wird die Nutzung von Browser Add-ons wie **Cookie Auto Delete** (löscht Cookies automatisch beim Schließen des Tabs), **uBlock origin** (blockiert Werbung und Tracker) und **ClearURL** (entfernt Tracking-Parameter aus URLS).

5. Firefox Container

Beim Surfen ist es normalerweise möglich, dass du **zwischen** den **verschiedenen Aktivitäten und Tabs getrackt** wirst. Firefox Container, oder auch „Tab-Umgebungen" genannt, verhindern das.

Falls du also doch einmal einen Tracking-intensiven Service wie Google nutzen möchtest, empfiehlt es sich, dies in einem Container durchzuführen, so dass deine wertvollen Informationen über andere Aktivitäten geschützt bleiben.