TECHNISCHE UNIVERSITÄT WIEN
Vienna | Austria

Open Source und Datenschutz

Luis & Thomas

TU Wien & WUK work.space

15. Mai 2025

Was ist Open Source Software (FOSS)

- **Definition**: Quellcode ist öffentlich zugänglich, kann genutzt, verändert und weitergegeben werden.
- **Philosophie**: Zusammenarbeit, Transparenz und Freiheit stehen im Mittelpunkt.
- **Vorteile**: Sicherheit, Anpassbarkeit, keine Lizenzkosten, große Community.
- **Open Source vs. Free Software**: Open Source = praktischer Ansatz, Free Software = ethische/philosophische Grundlage (Stichwort: "Free as in freedom, not as in free beer").
- **Bedeutung für die Gesellschaft**: Digitale Souveränität, Datenschutz, Unabhängigkeit von großen Konzernen.

Die Geschichte von FOSS

- **1950er–1970er**: Software wurde oft frei geteilt, insbesondere in der akademischen Welt.
- **1983**: Richard Stallman startet das GNU-Projekt und begründet die Free Software Foundation (FSF).
- **1991**: Linus Torvalds veröffentlicht den ersten Linux-Kernel.
- **1998**: Der Begriff "Open Source" entsteht als Alternative zu "Free Software".
- **2000er–heute**: Open Source wird Mainstream – von Unternehmen (Google, Microsoft) bis zu Regierungen.

Von UNIX zu GNU: Der Weg zur Open-Source-Bewegung

- **1970er**: UNIX wird an Universitäten verbreitet, BSD (Berkeley Software Distribution) entsteht als modifizierte Version.
- **1980er**: AT&T beginnt, UNIX kommerziell zu lizenzieren, BSD enthält noch proprietären UNIX-Code.
- **1983**: Richard Stallman startet das GNU-Projekt, um ein komplett freies UNIX-ähnliches System zu entwickeln.
- **1990er**: Nach rechtlichen Streitigkeiten wird BSD von proprietären UNIX-Teilen befreit, parallel entwickelt sich GNU weiter.
- **Linux-Kernel (1991)**: GNU fehlte ein Kernel, Linus Torvalds veröffentlicht Linux – GNU/Linux entsteht.

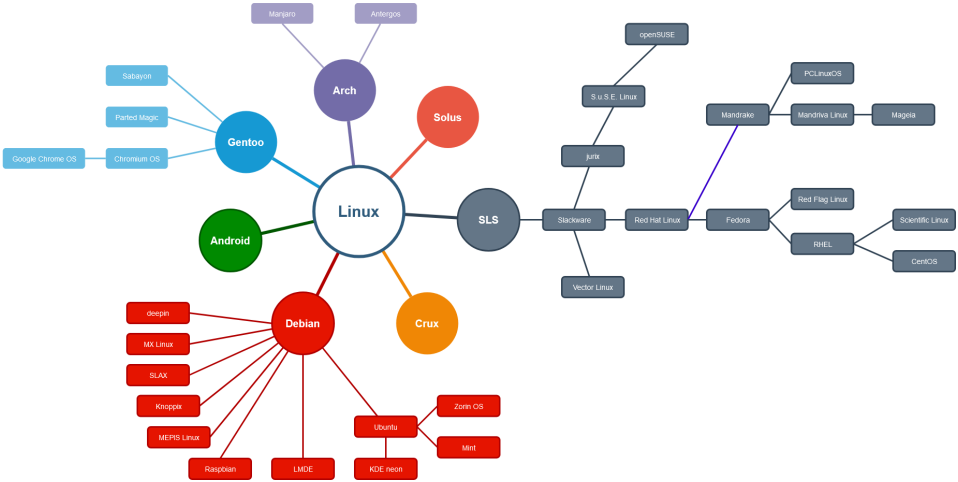
Was ist jetzt GNU?

- **GNU (GNU's Not Unix)**: Ein freies, UNIX-ähnliches Betriebssystem, gestartet von Richard Stallman 1983.
- **Ziel**: Ein komplett freies Software-Ökosystem ohne proprietäre Einschränkungen.
- **Bestandteile**: Compiler (GCC), Editor (Emacs), Shell (Bash), viele UNIX-Tools.
- **GNU Hurd**: Eigentlich als Kernel für GNU gedacht, aber bis heute nicht fertiggestellt.
- **GPL-Lizenz**: Sichert, dass Software frei bleibt (Copyleft-Prinzip).

...und was ist Linux?

- **Linux-Kernel**: 1991 von Linus Torvalds entwickelt, ein freier, monolithischer Betriebssystemkern.
- **Ersatz für GNU Hurd**: Da Hurd nie wirklich fertig wurde, wurde Linux als Kernel für GNU genutzt – so entstand GNU/Linux.
- **Distributionen**: Debian, Ubuntu, Arch, Fedora, openSUSE – unterschiedliche Ansätze und Zielgruppen.
- **Einsatzbereiche**: Server, Embedded Systems, Supercomputer, Smartphones (Android), Desktop.
- **Philosophie**: Open Source, Anpassbarkeit, Stabilität, Sicherheit.

Linux-Stammbaum



GNU, Linux... ja gut, aber was ist BSD?

- **BSD (Berkeley Software Distribution)** – Unix-Derivat, entwickelt ab den 1970er Jahren an der UC Berkeley
- **AT&T vs. BSD** – Rechtsstreit in den 1990ern, führte zur vollständigen freien Veröffentlichung von BSD
- **Lizenz** – BSD-Lizenz erlaubt freie Nutzung, Modifikation und proprietäre Nutzung (weniger restriktiv als GPL)
- **Forks** – FreeBSD, OpenBSD, NetBSD als eigenständige Weiterentwicklungen
- **Einfluss** – TCP/IP-Stack von BSD prägt moderne Netzwerktechnologie
- **macOS & iOS** – Basieren teilweise auf BSD-Komponenten
- **PlayStation 4 & 5** – Betriebssystem "Orbis OS" basiert auf FreeBSD

Die wichtigsten Lizenzen

- **GPL (GNU General Public License)**: Copyleft, Änderungen müssen ebenfalls unter GPL veröffentlicht werden.
- **MIT License**: Sehr permissiv, erlaubt fast alles, solange der ursprüngliche Autor genannt wird.
- **Apache License 2.0**: Ähnlich wie MIT, aber mit Patentklausel zum Schutz vor Patentstreitigkeiten.
- **BSD License (2-/3-Clause)**: Minimalistische Lizenz, erlaubt fast uneingeschränkte Nutzung.
- **Creative Commons (CC)**: Für nicht-softwarebasierte Werke, verschiedene Varianten mit Einschränkungen wie Namensnennung oder nicht-kommerzielle Nutzung.

Vorteile von Open Source in der Forschung

- **Reproduzierbarkeit**: Offen zugänglicher Code sorgt für überprüfbare Ergebnisse.
- **Kosteneffizienz**: Keine teuren Lizenzen, volle Kontrolle über die Tools.
- **Transparenz**: Keine Black-Box-Algorithmen – jeder kann nachprüfen, was passiert.
- **Kollaboration**: Forschungsteams weltweit können gemeinsam weiterentwickeln.
- **Nachhaltigkeit**: Software bleibt nutzbar, auch wenn Unternehmen verschwinden.
- **Anpassbarkeit**: Code kann spezifisch für Forschungsfragen modifiziert werden.

Setzen wir FOSS ein? JA!

- **Python** – Eine weit verbreitete Programmiersprache für Datenanalyse, Automatisierung und wissenschaftliches Rechnen.
- **Octave** – Freie MATLAB-Alternative für numerische Berechnungen.
- **UGENE** – Open-Source-Software für Bioinformatik, Sequenzanalyse und Genomanalysen.
- **OpenChrom** – Freie Software zur Auswertung chromatographischer Daten (z. B. GC/MS, HPLC).
- **Zotero** – Open-Source-Tool zur Verwaltung von Literatur und Quellen.
- **LaTeX** – Ein Schriftsatzsystem für wissenschaftliche Arbeiten – inklusive dieser Präsentation!

Open Source und BigTech

- **Microsoft** – Nutzt und unterstützt Open Source (z. B. Linux auf Azure, WSL, VS Code) und ist größter GitHub-Sponsor.
- **Apple** – Setzt Open-Source-Technologien ein (z. B. WebKit, Swift, Darwin), aber hält viele Teile proprietär.
- **Google** – Entwickelt und fördert Open Source (z. B. Android, Chromium, TensorFlow, Kubernetes), doch sammelt viele Nutzerdaten.
- **Tesla** – Verwendet Linux in seinen Autos, musste Open-Source-Code veröffentlichen, hält aber viele Softwarekomponenten geschlossen.
- **Meta (Facebook)** – Entwickelt Open-Source-Projekte wie React, PyTorch und HHVM, steht aber wegen Datenschutz und Tracking in der Kritik.
- **Red Hat** – Einer der größten Open-Source-Anbieter, entwickelt Linux-Distributionen (z. B. RHEL, Fedora) und verdient mit Support und Dienstleistungen.

Was ist GitHub?

- **GitHub** – Die größte Plattform für Open-Source-Software-Entwicklung.
- **2018 von Microsoft übernommen** – Seitdem gemischte Reaktionen aus der Open-Source-Community.
- **Features** – Code-Hosting, Kollaboration, Versionskontrolle mit Git, CI/CD, Codespaces.
- **GitHub Copilot** – KI-gestütztes Coding-Tool, aber umstritten wegen Trainingsdaten aus Open-Source-Code.
- **Alternativen** – GitLab (selbst hostbar), Gitea, Codeberg (FOSS-freundlich, unabhängig).

Hands-on: Open-Source-Projekte

Nehmt euch **10 Minuten** Zeit und überlegt:

- Öffnet **Duck.AI** und fragt gezielt nach Open-Source-Projekten auf **GitHub** zu einem Thema eurer Wahl. Nutzt dazu einen Prompt wie:
  "Finde spannende Open-Source-Projekte zu [Thema] auf GitHub."
- Schaut euch bei den vorgeschlagenen Projekten an:
  - Beschreibung (README)
  - Programmiersprache
  - Lizenz
  - Aktivität (Commits, Issues, Pull Requests)
- Beispiele für bekannte Open-Source-Projekte:
  - **Linux Kernel** (`https://github.com/torvalds/linux`)
  - **Python** (`https://github.com/python/cpython`)
  - **Blender** (`https://github.com/blender/blender`)
  - **OBS Studio** (`https://github.com/obsproject/obs-studio`)
- Welche interessanten Projekte findet ihr?

Open-Source-Anwendungssoftware

- **Open Source im Alltag:**
  - **Firefox** – Datenschutzfreundlicher Webbrowser.
  - **E-Mail:** Thunderbird – Open-Source-E-Mail-Client mit vielen Erweiterungen.
  - **LibreOffice** – Kostenlose Alternative zu Microsoft Office.
  - **VLC** – Mediaplayer für fast alle Formate.
  - **7-Zip** – Dateiarchivierer für `.zip`, `.rar`, `.7z`, etc.
- **Open Source für spezielle Anwendungen:**
  - **Kdenlive** – Videobearbeitung.
  - **GIMP** – Bildbearbeitung (Alternative zu Adobe Photoshop).
  - **Darktable** – Foto-Entwicklung (Alternative zu Adobe Lightroom).
  - **Audacity** – Audio-Editor.
  - **Ardour** – Professionelle DAW für Audio-Produktion.
  - **Blender** – 3D-Modellierung und Animation.
  - **OBS Studio** – Livestreaming und Bildschirmaufnahme.
  - **LibreCAD** – 2D-CAD-Zeichnungen (Alternative zu AutoCAD).

Open Source für Web & Content

Frameworks

- **Bootstrap** – CSS-Framework für responsive Webentwicklung
- **React** – JavaScript-Framework für UI-Komponenten
- **Vue.js** – Fortschrittliches JavaScript-Framework für Web-Apps

Plattformen & CMS

- **WordPress** – Weltweit meistgenutztes Content-Management-System
- **Moodle** – Open-Source-Lernplattform für Bildungseinrichtungen
- **Nextcloud** – Selbstgehostete Cloud-Lösung als Alternative zu Google Drive
- **Joomla!** – Flexibles Open-Source-CMS

Open-Source-Server-Software

- **Apache** – Der Klassiker unter den Webservern. (Bedient etwa 23,04 % der meistbesuchten Websites)
- **Nginx** – Leistungsstarker Webserver und Reverse Proxy. (Bedient etwa 22,01 % der meistbesuchten Websites)
- **Bind** – Einer der meistgenutzten DNS-Server weltweit.
- **OpenVPN / WireGuard** – VPN-Lösungen für sichere Verbindungen.

Open Source in europäischen Verwaltungen (Beispiele)

- **Deutschland:** Entwicklung der *Bundescloud* – eine eigene Cloud-Infrastruktur auf Open-Source-Basis für Bundesbehörden.
  - Einsatz von **Nextcloud** zur sicheren Dateiablage und Kollaboration
  - **Jitsi Meet** für datenschutzfreundliche Videokonferenzen
  - **Moodle**, **Mail-Stacks** und andere Open-Source-Komponenten
- **Frankreich:** *GendBuntu* – eine Ubuntu-basierte Linux-Distribution, speziell für die französische Gendarmerie entwickelt.
- **Niederlande:** Fokus auf *Vendorenunabhängigkeit* – vermehrter Einsatz freier Software in öffentlichen Einrichtungen und digitale Souveränität als Leitprinzip.
- **EU-Kommission:** *Open Source Software Strategy 2020–2023* – Ziel: Förderung von Open Source innerhalb der EU-Institutionen.
- **EU-Initiativen:** Programme wie *EU-FOSSA* (Free and Open Source Software Audit) zur Sicherheitsanalyse und Verbesserung kritischer OSS-Projekte.

Open Source in österreichischen Verwaltungen (Beispiele)

- **Österreichische Bundesverwaltung:**
  - Verwendung von Open-Source-Software zur Steigerung der digitalen Souveränität und Reduzierung von Lizenzkosten.
  - Einsatz von Linux-Servern und Open-Source-Technologien in verschiedenen Ministerien und Behörden.
- **Stadt Wien:**
  - Implementierung von Open-Source-Software in Bereichen wie Bürosoftware (z. B. LibreOffice statt Microsoft Office).
  - Förderung von Open Data-Initiativen (z. B. data.gv.at).
- **Österreichische Justiz:**
  - Einsatz von Linux-Servern und Open-Source-Technologien zur Verwaltung von Justizdaten und Akten.
- **Bundesrechenzentrum (BRZ):**
  - Nutzung von Open-Source-Software in der IT-Infrastruktur für die österreichische Verwaltung und öffentliche Dienste.

Risiken von Open Source Software

- **Supply-Chain-Angriffe**
  - Bösartiger Code kann in beliebte Open-Source-Projekte eingeschleust werden.
  - **Beispiel:** Log4j-Sicherheitslücke – Millionen von Systemen waren betroffen.
  - **Lösung:** Regelmäßige Updates, Code-Review und vertrauenswürdige Quellen nutzen.
- **Unmaintained Software**
  - Manche Open-Source-Projekte werden nicht mehr aktiv gepflegt.
  - Sicherheitslücken bleiben ungepatcht.
  - **Lösung:** Nur gut gepflegte Software mit aktiver Community verwenden.
- **Fake Open Source**
  - Manche Unternehmen labeln ihre Software als "Open Source", schränken aber die Nutzung ein.
  - **Beispiel:** Quellcode ist einsehbar, aber Lizenz verbietet Modifikation oder kommerzielle Nutzung.
  - **Lösung:** Immer die Lizenz genau prüfen (z. B. MIT, GPL, Apache).

Hands-on: Welche Open-Source-Programme nutzt ihr?

Nehmt euch **5 Minuten** Zeit und überlegt:

- Welche Programme nutzt ihr täglich?
- Welche davon sind Open Source?
- Gibt es Alternativen, die Open Source sind?

Diskutiert anschließend eure Ergebnisse!

Open Source als Treiber für KI

Open Source hat viele Bereiche revolutioniert – von Betriebssystemen bis hin zu wissenschaftlicher Software. Doch eine der größten aktuellen Entwicklungen ist Open-Source-KI. Wie verändert sie die Forschung, Unternehmen und unsere digitale Welt?

Open Source in der Künstlichen Intelligenz

- **Transparenz und Reproduzierbarkeit** – Wissenschaftliche Forschung profitiert von offenen Modellen und Algorithmen.
- **Community-getriebene Innovation** – Open-Source-Projekte ermöglichen schnelle Weiterentwicklung durch eine globale Entwicklergemeinschaft.
- **Zugänglichkeit** – Open-Source-KI-Modelle ermöglichen es kleinen Unternehmen, Universitäten und Einzelpersonen, KI-Technologien zu nutzen.
- **Beispiele für Open-Source-KI:**
  - LLaMA (Meta) / DeepSeek (DeepMind) – Sprachmodell-Alternative zu GPT
  - Mistral – Leichtgewichtige und effiziente KI-Modelle
  - Stable Diffusion – Generative KI für Bilder
  - BLIP – Bild-Text-Verständnis
  - GPT-2, DistilBERT – Textverarbeitung
  - Real-ESRGAN – KI-gestützte Bildverbesserung
  - EasyOCR – Optische Zeichenerkennung

Warum veröffentlichen Unternehmen Open-Source-KI?

Open-Source-KI fördert Innovation, aber Unternehmen verfolgen oft auch eigene strategische Ziele.

- **Marktdominanz & Einfluss** – Firmen wie Meta wollen Standards setzen und sicherstellen, dass ihre Technologie von Entwicklern weltweit genutzt wird.
- **Daten & Feedback sammeln** – Durch Open-Source-Modelle können Unternehmen beobachten, wie ihre KI in der Praxis eingesetzt wird und so indirekt ihre eigenen Modelle verbessern.
- **Kosten sparen** – Externe Entwickler tragen zur Weiterentwicklung bei, ohne dass das Unternehmen alles selbst finanzieren muss.
- **Regulatorischer Druck** – Open-Source kann als Strategie genutzt werden, um sich als transparent zu präsentieren und Kritik an KI-Monopolen zu entschärfen.
- **Konkurrenz zu geschlossenen Systemen** – Meta mit LLaMA gegen OpenAI mit GPT, Mistral gegen Claude usw. $\rightarrow$ Wettbewerb um Entwickler und Marktanteile.
- **Lock-In-Effekte erzeugen** – Unternehmen wollen, dass ihre Infrastruktur genutzt wird (z. B. Meta: LLaMA + PyTorch $\rightarrow$ stärkere Bindung an Meta-Ökosystem).

KI-Sicherheit – Was ist das und warum ist es wichtig?

- **Was ist KI-Sicherheit?**
  - Maßnahmen zum Schutz vor Risiken und Missbrauch von Künstlicher Intelligenz (KI).
  - Sicherer Entwicklungsprozess und verantwortungsvolle Nutzung von KI-Systemen.
- **Warum ist das wichtig?**
  - **Datenschutz:** Schutz sensibler Informationen vor unberechtigtem Zugriff.
  - **Manipulation verhindern:** Schutz vor gezielter Manipulation durch fehlerhafte oder bösartige Trainingsdaten.
  - **Robustheit:** Vermeidung von Fehlverhalten und unvorhergesehenen Ergebnissen.
  - **Verantwortlichkeit:** Transparenz bei Entscheidungen, um Missbrauch und Diskriminierung zu vermeiden.

KI-Sicherheit im Open-Source-Kontext

- **Transparenz:** Offener Quellcode ermöglicht Überprüfung und Verbesserung durch die Community.
- **Vertrauen:** Sicherheit durch "Viele-Augen-Prinzip" – potenzielle Schwachstellen können schneller erkannt werden.
- **Missbrauchspotential:** Offener Zugang kann jedoch auch zu böswilliger Nutzung führen.
- **Abhängigkeiten:** Open-Source-Projekte nutzen oft viele Bibliotheken – Schwachstellen in einer Abhängigkeit können die gesamte KI gefährden.

Best Practices für KI-Sicherheit:

- Regelmäßige Sicherheits-Audits
- Nutzung vertrauenswürdiger Open-Source-Bibliotheken
- Verantwortungsvoller Umgang mit Trainingsdaten
- Dokumentation und Transparenz der Modelle

Hands-on: Erkunde das Open-Source-KI-Projekt!

Aufgabe:

- Öffne das Webinterface des KI-Projekts.
- Teste die verschiedenen Modelle und Funktionen.
- Überlege: Was macht welche KI? Wo könnte man sie einsetzen?

Dauer: 10 Minuten

In meinem ursprünglichen Konzept hättet ihr das alles selber programmieren müssen, aber das ging nicht durch... also klickt einfach ein bisschen herum :P

Open Source und Datenschutz – Ein natürliches Duo?

- Open Source bedeutet Transparenz: Jeder kann den Code überprüfen.
- Proprietäre Software kann versteckte Datensammlungen enthalten.
- Kontrolle über Software und Infrastruktur ist essenziell für Datenschutz.
- Open-Source-Tools bieten Alternativen zu datenhungrigen Big-Tech-Diensten.
- Datenschutz ist Freiheit – und die sollte man nicht kampflos aufgeben.

Open Source schafft Transparenz: Wer den Code einsehen kann, kann überprüfen, ob Daten sicher verarbeitet werden. Doch: Bedeutet Open Source automatisch besseren Datenschutz? Wer prüft den Code tatsächlich?
$\rightarrow$ Datenschutz erfordert mehr als nur quelloffene Software – es geht um Verschlüsselung, Infrastruktur und digitale Selbstbestimmung.

Warum ist Datenschutz wichtig?

- **Daten sind Macht:** Wer Informationen kontrolliert, kontrolliert Menschen.
- **"Ich habe nichts zu verbergen" ist ein Trugschluss:** Datenschutz schützt nicht nur dich, sondern auch andere.
- **Überwachung verändert Verhalten:** Menschen passen ihr Verhalten an, wenn sie beobachtet werden.
- **Personalisierte Manipulation:** Werbung, Meinungsbildung und Wahlbeeinflussung durch gezielte Datenanalyse.
- **Datenunternehmen und Profilerstellung:** Unternehmen und Staaten speichern riesige Datenmengen – oft ohne unser Wissen.

Hands-On: Dein digitaler Fußabdruck

- **Aufgabe:** Finde heraus, welche Standortdaten über dich gespeichert sind!
  - **Google:** `https://www.google.com/maps/timeline`
  - **Apple:** `Einstellungen` → `Datenschutz & Sicherheit` → `Ortungsdienste` → `Systemdienste` → `Wichtige Orte`
- **Fragen zum Nachdenken:**
  - Welche Orte sind gespeichert?
  - Bist du überrascht, was alles getrackt wurde?
  - Wie könnten diese Informationen missbraucht werden?
- **Hinweis:** Falls kein Google-Account oder Apple-Gerät vorhanden ist oder der Verlauf deaktiviert ist, tauscht euch mit anderen aus oder recherchiert, welche Daten sonst noch gespeichert werden.

Arten personenbezogener Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen. Ihr Schutz ist zentral für die Wahrung der Privatsphäre und den Schutz vor Missbrauch.

Diese Daten lassen sich in verschiedene Kategorien unterteilen:

- **Identifizierende Informationen:**
  - Name, Adresse, Geburtsdatum, Telefonnummer.
- **Sensible Daten:**
  - Gesundheit, ethnische Herkunft, sexuelle Orientierung, politische Meinungen.
- **Online-Daten:**
  - IP-Adressen, Cookies, Suchverlauf, Nutzungsverhalten.
- **Finanzielle Informationen:**
  - Bankdaten, Kreditkartennummern.

Cambridge Analytica und Trumps Wahl – Ein Datenschutzskandal

Was ist passiert?

- 2014: Cambridge Analytica sammelt Millionen Facebook-Profile ohne Zustimmung.
- Psychometrische Analysen zur gezielten Wahlwerbung für Trump 2016.
- Microtargeting: Individuelle Botschaften basierend auf Persönlichkeitstests.

Warum war das problematisch?

- Daten wurden ohne Wissen der Nutzer missbraucht.
- Wähler wurden manipuliert, ohne es zu bemerken.
- Datenschutzrechtliche Verstöße und Facebooks Rolle.

Folgen:

- Facebook wurde zu hohen Strafen verurteilt.
- Stärkere Datenschutzregulierungen wie die DSGVO wurden relevanter.
- Bewusstsein für digitale Manipulation und Datenschutz wuchs.

DSGVO – Datenschutz in der EU

- Seit 25. Mai 2018 in Kraft – schützt personenbezogene Daten.
- Ziel: Mehr Kontrolle für Bürger über ihre Daten.

Wichtige Prinzipien:

- **Recht auf Auskunft** – Nutzer können erfahren, welche Daten gespeichert sind.
- **Recht auf Löschung** – Personen können verlangen, dass ihre Daten gelöscht werden ("Recht auf Vergessenwerden").
- **Datenminimierung** – Unternehmen dürfen nur notwendige Daten erheben.
- **Einwilligung** – Datenverarbeitung erfordert eine aktive Zustimmung.
- **Recht auf Datenübertragbarkeit** – Nutzer können ihre Daten in einem gängigen Format anfordern.

Strafen: Verstöße gegen die DSGVO können mit hohen Bußgeldern geahndet werden (bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes).

Datenhandel – Unsere Informationen als Ware

- Daten sind ein Milliardengeschäft: Unternehmen handeln mit Nutzerdaten für gezielte Werbung, Profilbildung und Marktanalysen.
- Große Konzerne (z. B. Google, Meta, Amazon) verdienen durch personalisierte Werbung.
- Datenbroker sammeln und verkaufen Informationen aus verschiedensten Quellen (Webtracking, Kundenkarten, Social Media).
- Konsequenzen: Preisdiskriminierung, Manipulation (z. B. politische Werbung), Datenschutzverletzungen.
- DSGVO schafft strengere Regeln, aber viele Unternehmen umgehen sie oder operieren in Ländern mit schwächeren Gesetzen.

Frage: Haben wir noch Kontrolle über unsere eigenen Daten, oder sind sie längst eine Handelsware?

Tracking und Personalisierte Werbung

- Webseiten und Apps nutzen Tracker, um Nutzerverhalten zu analysieren (Cookies, Fingerprinting, Pixel).
- Werbenetzwerke (z. B. Google Ads, Meta Ads) erstellen detaillierte Profile für gezielte Werbung.
- Dynamische Preisgestaltung: Nutzer sehen je nach Profil unterschiedliche Preise.
- Psychologische Beeinflussung: Werbung wird so platziert, dass sie maximal effektiv ist.
- Datenschutzprobleme: Nutzer wissen oft nicht, welche Daten gesammelt werden und wie sie verwendet werden.

Frage: Wo liegt die Grenze zwischen Personalisierung und Manipulation?

Dark Patterns – Manipulation durch Design

- **Zwangsregistrierung** – Nutzung einer Website nur mit Account möglich.
- **Versteckte Einwilligungen** – Opt-in riesig, Opt-out winzig.
- **Fake Countdown-Timer** – "Nur noch 5 Minuten!" (bleibt aber immer gleich).
- **Mikro-Transparenz** – Wichtige Optionen tief in den Einstellungen versteckt.
- **Dunkle UX-Farben** – "Ablehnen"-Button unscheinbar grau, "Akzeptieren" leuchtet.
- **Schwerer Ausstieg** – Kündigen kompliziert, Anmelden super einfach.
- **Nudging** – "Du bist der Einzige, der noch keine Freunde eingeladen hat!"

Datenabsaugung durch soziale Netzwerke

- **Totalüberwachung**: WhatsApp, Facebook & Co. sammeln massenhaft Nutzerdaten.
- **Erfasste Daten**:
  - Nachrichten, Kontakte, Standortverläufe
  - Geräte-IDs, App-Nutzung, Online-Aktivitäten
- **Tracking-Methoden**:
  - **Bluetooth-Tracking**: Begegnungen mit anderen Nutzern erfassbar
  - **Geofencing**: Erkennung von Aufenthaltsorten für gezielte Werbung
  - **MAC-Adress-Tracking**: Bewegungsprofile über WLAN-Netze
- **Datenhandel**: Verknüpfung mit anderen Quellen & Verkauf an Werbefirmen.
- **Folgen**: Verhaltensüberwachung, gezielte Manipulation, mögliche Weitergabe an Behörden.

TikTok: Datenschutz & Tracking

- Umfangreiche Datensammlung: Standort, Kontakte, Tastatureingaben, Metadaten.
- Nutzerverhalten wird analysiert, um detaillierte Profile zu erstellen.
- Fingerprinting-Techniken ermöglichen eindeutige Identifikation der Nutzer.
- Zugriff auf die Zwischenablage – mehrfach nachgewiesen.

TikTok: Algorithmus & Einflussnahme

- Hochgradig personalisierte Inhalte – Nutzer werden gezielt gelenkt.
- Manipulationspotenzial: Unterdrückung oder Verstärkung bestimmter Inhalte.
- Förderung von viralen Trends, unabhängig von Wahrheitsgehalt.
- Verstärkung von extremen Meinungen und Radikalisierung möglich.

TikTok: Herkunft & Bedenken

- Gehört zum chinesischen Konzern ByteDance.
- Chinesische Regierung könnte Zugriff auf Nutzerdaten verlangen.
- Sicherheitsbedenken führten zu Verboten/Diskussionen in mehreren Ländern.
- Datenschutzregelungen in der EU stehen im Konflikt mit TikToks Praktiken.

TikTok: Jugendschutz & Suchtfaktor

- Endlos-Scroll-Mechanik sorgt für extrem hohe Verweildauer.
- Suchtpotenzial durch Dopamin-gesteuertes Belohnungssystem.
- Gefährliche Challenges verbreiten sich oft unkontrolliert.
- Minderjährige sind besonders von Datenschutzrisiken betroffen.

Wie der TikTok-Algorithmus extremistisches Verhalten fördert

- **For-You-Page (FYP):** TikTok empfiehlt Videos basierend vor allem auf der Watchtime – selbst ohne Likes zählt, wie lange ein Video angeschaut wird.
- **Echokammer-Effekt:** Inhalte, die bestehende Ansichten bestätigen, werden verstärkt angezeigt.
- **Radikalisierungs-Spirale:** Provokante, emotional aufgeladene Videos erzeugen hohe Watchtime, was zu immer extremeren Inhalten führt.
- **Engagement als Treiber:** Längere Verweildauer signalisiert dem Algorithmus besonderes Interesse, wodurch ähnliche Inhalte öfter empfohlen werden.
- **Kurzvideo-Dopamin-Effekt:** Schnelle, repetitive Inhalte fördern impulsives Konsumverhalten und mindern kritisches Denken.

Fazit: Die algorithmische Optimierung auf maximale Watchtime führt dazu, dass Nutzer in isolierten, extremen Meinungsblasen gefangen werden. Durch kontinuierliche Verstärkung ähnlicher Inhalte werden alternative Perspektiven kaum präsentiert – ein Mechanismus, der die Radikalisierung zusätzlich befeuert.

It's Movie Time!

- **Thema**: Radikalisierung durch soziale Medien – wie Algorithmen unsere Meinungsbildung beeinflussen.
- **Video**: Interview mit Ingrid Brodnig (österreichische Journalistin und Publizistin, Expertin für digitale Themen).
- **Inhalt**: ORF-Sendung "Wien heute" über den Selbstversuch der Satireplattform *Die Tagespresse*:
  - *"Selbstversuch: So radikalisiert TikTok österreichische Teenager"*
  - Wie schnell geraten junge Menschen in extremistische Filterblasen?
- **Achtet auf**:
  - Welche Mechanismen führen zur Radikalisierung?
  - Welche Rolle spielen Algorithmen und Inhalte?
  - Was sagt Ingrid Brodnig zur Verantwortung der Plattformen?

Influencer: Manipulation als Geschäftsmodell

- **Gehirnwäsche durch Algorithmen**: Plattformen pushen extreme Inhalte, weil sie mehr Klicks bringen.
- **Schleichwerbung & Fake-Authentizität**: "Empfohlene" Produkte sind oft nur bezahlte Deals.
- **Perfekte Lügenwelt**: Gefilterte Realität erzeugt Druck und unrealistische Erwartungen.
- **Kaufzwang durch FOMO**: "Nur heute! Nur hier! Nur für dich!" – alles Marketingtricks.
- **Macht & Einfluss**: Einige Influencer verbreiten Desinformationen und Verschwörungstheorien.
- **Alles für die Kohle**: Viele Influencer verkaufen euch alles, solange die Bezahlung stimmt.

Phishing: Gefahr für den Datenschutz

- **Was ist Phishing?**
  - Betrugsmasche, bei der Angreifer sich als vertrauenswürdige Quelle ausgeben.
  - Ziel: Persönliche Daten wie Passwörter, Kreditkarteninformationen oder Logins stehlen.
- **Wie funktioniert Phishing?**
  - Gefälschte E-Mails oder Webseiten (z. B. "Ihr Konto wurde gesperrt – bitte einloggen").
  - Social Engineering: Täuschung durch vermeintlich legitime Nachrichten oder Anrufe.
- **Bezug zum Datenschutz:**
  - Geklaute Daten können für Identitätsdiebstahl oder Überwachung genutzt werden.
  - Besonders gefährlich in sozialen Netzwerken oder schlecht gesicherten Plattformen.
- **Schutzmaßnahmen:**
  - Misstrauen bei unerwarteten Anfragen nach persönlichen Daten.
  - Zwei-Faktor-Authentifizierung (2FA) aktivieren.

Wie können wir uns jetzt schützen?

- **Fact-Checker**: Nutze Plattformen wie *Mimikama* oder *correctiv.org*, um Informationen zu prüfen.
- **Open-Source-Alternativen**: Verwende sicherere Optionen wie *Mastodon* oder *Pixelfed*.
- **Passwort-Management**: Setze Passwort-Manager ein, um deine Konten zu schützen.
- **Datenschutz**: Überprüfe regelmäßig deine Privatsphäre-Einstellungen in sozialen Netzwerken.
- **Bewusster Umgang mit Medien**: Hinterfrage Inhalte und sei dir bewusst, wie Algorithmen dein Verhalten beeinflussen können.
- **Daten sind dauerhaft**: Alles, was einmal im Internet ist, bleibt dort oft für immer – sei dir der Folgen bewusst.

Bilder teilen: Metadaten-Stripping

- **Was sind Metadaten?**
  - Informationen wie **GPS-Koordinaten**, Kameramodell, Erstellungsdatum usw.
  - Können Rückschlüsse auf **Standort** und **Privatsphäre** ermöglichen.
- **Warum Metadaten entfernen?**
  - Schutz der eigenen Privatsphäre.
  - Vermeidung unerwünschter Rückverfolgung.
  - Sicheres Teilen von Bildern im Netz.
- **Wie entfernt man Metadaten?**
  - **Manuell:** Eigenschaften des Bildes prüfen und bearbeiten.
  - **Automatisch:** Viele Messenger (z.B. Signal) entfernen Metadaten beim Teilen.
- **Schutzmaßnahmen:**
  - Nutze Tools wie `ExifTool`, um Metadaten vor dem Teilen zu entfernen.
  - Achte darauf, dass Plattformen wie **Flickr** Metadaten nicht automatisch entfernen, da die Nutzer wissen sollten, was sie tun. Wenn du GPS-Koordinaten oder Kameraeinstellungen nicht teilen möchtest, musst du sie selbst entfernen.

Hands-On: Vorsicht bei öffentlichen Bildern – Doxxing und Datenschutz

- **Ziel**: Ermitteln der genauen Standortdaten aus öffentlichen Bildern, die GPS-Tags enthalten.
- **Schritt 1 – EXIF-Daten auslesen**:
  - Verwende `ExifTool`, um die GPS-Koordinaten aus den Metadaten eines Bildes zu extrahieren:
- **Schritt 2 – Umrechnung der GPS-Daten in Dezimalgrad**:
  - Um GPS-Koordinaten in Dezimalgrad umzuwandeln, wenn sie im Grad-Minuten-Sekunden-Format vorliegen.
- **Schritt 3 – Bestimmung der genauen Location**:
  - Lade die GPS-Daten in **OpenStreetMap** und bestimme die genaue Adresse.
- **Warnung**:
  - Dies ist ein praktisches Beispiel, wie leicht private Informationen öffentlich zugänglich gemacht werden.
  - **Achtung beim Teilen von Fotos!** GPS-Tags können deine genaue Position preisgeben, ohne dass du es merkst.

Anonyme Anmeldung: Fake E-Mail & Identitätsgeneratoren

- **Fake E-Mail Generatoren**: Tools, die temporäre E-Mail-Adressen erstellen, um sich ohne Angabe persönlicher Daten auf Websites anzumelden.
- **Temporäre Identitäten**: Webseiten, die es ermöglichen, pseudonyme Identitäten zu erstellen, um online anonym zu bleiben und die wahre Identität zu verschleiern.
- **Vorteil**: Diese Dienste bieten Schutz vor Spam, unerwünschter Werbung und Tracking.
- **Beispiele**: `10minutemail.com`, `guerrillamail.com`, `emailfake.org`(für Fake E-Mail) und `fakenamegenerator.com` (für Pseudonyme).

Facebooks Kontrolle über Kommunikation: API-Zugriff wird beendet

- **Facebooks Entscheidung (26.02.2025)**:
  - Beendet den API-Zugriff für Drittanbieter-Clients (z.B. Pidgin mit purple-facebook).
  - **Ziel**: Facebook will die Kontrolle über Kommunikationswege und Nutzerdaten festigen.
  - **Folgen**: U.a keine verschlüsselte Kommunikation via **OTR** mehr möglich, datenschutzfreundliche Nutzung blockiert.
- **Reaktionen der Community**:
  - Open-Source-Entwickler forken das `purple-facebook`-Plugin.
  - Anmeldung über `Pidgin` bleibt vorerst weiterhin möglich.
  - Doch die Situation bleibt fragil: Es ist ein **ständiges Katz-und-Maus-Spiel**.
  - Facebook wird möglicherweise neue Einschränkungen implementieren, was die fortwährende Verfügbarkeit von Drittanbieter-Clients gefährdet.

Die Geschichte von `purple-facebook`: Open-Source-Widerstand gegen Plattformkontrolle

- **Mai 2015: Facebook verändert XMPP**
  - Standard-XMPP-Clients funktionieren nicht mehr mit Facebook.
  - Notwendigkeit für eine Alternative entsteht.
- **Juni – August 2015: Entwicklung von `purple-facebook`**
  - **James Geboski** entwickelt das Plugin im Rahmen des Google Summer of Code (GSoC).
  - Ziel: Facebook-Chat wieder in `Pidgin` nutzbar machen.
- **2016: Dequis** übernimmt das Projekt und verbessert es.
- **Februar 2025: Facebook deaktiviert endgültig die API**
  - `purple-facebook` verliert die Funktionalität.
- **Februar 2025: DMJC forkt das Projekt**
  - Das Projekt wird von `DMJC` weitergeführt, um Facebook-Integration in `Pidgin` wieder zu ermöglichen.

Hands-On: Fake-Account bei Facebook erstellen

- **Ziel**: Untersuchung des Verhaltens von Facebook bei der Erstellung eines Fake-Accounts.
- **Aufgabe**:
  - Erstelle mit Fake-Daten einen Facebook-Account.
  - Beobachte, welche Informationen Facebook abfragt und welche Vorschläge dir gemacht werden.
  - Achte auf Werbeanzeigen und Inhalte, die dir angezeigt werden.
- **Bonus**: Demonstration durch Trainer:
  - Anmeldung bei Facebook über `Pidgin` mit dem `purple-facebook`-Plugin.
  - Nutzung des `OTR`-Plugins für verschlüsselte Kommunikation.
  - Verbindung über `Tor` für maximale Anonymität.

Wie erkenne ich Fake News?

- **Quelle prüfen**: Kommt die Information von einer vertrauenswürdigen Quelle?
- **Fehlende Quellenangabe**: Gibt es keine verlinkten, überprüfbaren Quellen oder Studien?
- **Emotionaler Inhalt**: Wird versucht, eine starke emotionale Reaktion (Angst, Wut) zu erzeugen?
- **Falsche oder manipulierte Bilder**: Achte auf Bildbearbeitung oder alte Bilder, die neu präsentiert werden.
- **Sensationsgier**: Ist die Nachricht zu dramatisch oder extrem, um wahr zu sein?
- **Bestätigungsfehler**: Bestätigt die Nachricht nur deine eigenen Überzeugungen ohne echte Beweise?
- **Faktencheck-Websites**: Nutze Seiten wie APA-Faktencheck, Mimikama oder Correctiv zur Überprüfung.

Mimikama: Faktencheck leicht gemacht

- **Unabhängige Plattform**: Mimikama ist ein gemeinnütziger Verein zur Aufklärung über Falschmeldungen.
- **Gründliche Recherche**: Das Team besteht aus Fachleuten aus verschiedenen Bereichen, die fundierte Analysen liefern.
- **Zugang zu Quellen**: Einige detaillierte Quellen sind für Mitglieder zugänglich, um den laufenden Betrieb zu unterstützen.
- **Frei verfügbare Kurzfassungen**: Zu jedem Faktencheck gibt es eine kompakte, kostenfreie Zusammenfassung.
- **Selbstkostenprinzip**: Mitgliedsbeiträge und Spenden decken die Betriebskosten, ohne kommerzielle Gewinnabsicht.
- **Zielsetzung**: Aufklärung und Schutz vor Desinformation stehen im Vordergrund.

APA-Faktencheck: Verlässliche Quellenprüfung

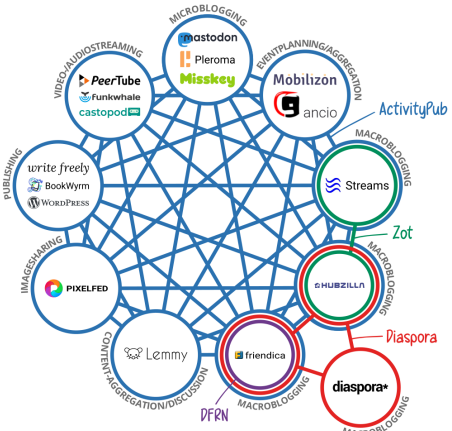
- **Unabhängige Plattform**: Die APA (Austria Presse Agentur) bietet einen Faktencheck-Service zur Überprüfung von Falschmeldungen.
- **Faktenbasierte Recherche**: Alle Artikel basieren auf gründlicher Recherche durch Journalisten und überprüfbaren Quellen.
- **Expertise**: Die APA greift auf ein Netzwerk an erfahrenen Journalisten und Experten zurück, die fundierte Analysen liefern.
- **Transparenz**: Klare Quellenangaben und nachvollziehbare Rechercheprozesse für maximale Transparenz.
- **Nicht kommerziell**: Die APA ist unabhängig und verfolgt keine kommerziellen Interessen bei der Faktenprüfung.

Das Fediverse: Alternativen zu zentralisierten Plattformen

- **Mastodon**: Alternative zu *Twitter* – Mikroblogging mit Fokus auf Datenschutz und Dezentralisierung.
- **Friendica**: Alternative zu *Facebook* – Soziales Netzwerk mit Schwerpunkt auf Privatsphäre und Dezentralisierung.
- **Pixelfed**: Alternative zu *Instagram* – Dezentrales Foto-Sharing ohne Werbung.
- **Lemmy**: Alternative zu *Reddit* – Dezentrale Plattform für Foren und Diskussionen.
- **Loops**: Alternative zu *YouTube Shorts* – Dezentrale Plattform für kurze, kreative Videos.
- PeerTube: Alternative zu *YouTube* – Dezentrales Video-Hosting ohne Werbung und Zensur.
- Funkwhale: Alternative zu *Spotify* – Musikstreaming-Plattform im Fediverse.
- Mobilizon: Alternative zu *Eventbrite* – Dezentrale Event-Planung ohne kommerzielle Interessen.

A view into the Fediverse

Who talks to whom - and how?



MORE PLATTFORMS AND INFO:
https://en.wikipedia.org/wiki/Fediverse

Vorteile des Fediverse

- **Keine Werbung**: Keine kommerziellen Interessen, keine Anzeigen, die den Inhalt beeinflussen.
- **Kein Tracking**: Nutzer haben die Kontrolle über ihre Daten, keine umfassende Datensammlung durch Dritte.
- **Keine Algorithmen**: Keine Algorithmen, die den Feed kuratieren oder versteckte Inhalte priorisieren – alles ist transparent.
- **Dezentralität**: Jeder kann seinen eigenen Server betreiben und die Plattform nach seinen Wünschen gestalten.
- **Privatsphäre**: Fokus auf Datenschutz und Kontrolle über persönliche Informationen.
- **Weniger Zensur**: Geringere Kontrolle durch zentrale Instanzen, aber dennoch Community-Regeln für verantwortungsbewusstes Verhalten.
- **Plattformübergreifendes Interagieren**: Dank des offenen Protokolls (ActivityPub) können Nutzer auf verschiedenen Plattformen liken, teilen und kommunizieren.

Sichere Kommunikation

- **Signal**: Verschlüsselte Nachrichten-App mit End-to-End-Verschlüsselung, Open Source und kostenlos.
- **Matrix**: Dezentrales Kommunikationsprotokoll für Chat, Sprach- und Videoanrufe mit Ende-zu-Ende-Verschlüsselung. Plattformen wie *Element* nutzen Matrix.
- **Threema**: Sicherer Messenger mit End-to-End-Verschlüsselung, kostenpflichtig, aber ohne die Notwendigkeit einer Telefonnummer.

Signal: Die sichere Kommunikations-App

- **Ende-zu-Ende-Verschlüsselung**: Alle Nachrichten sind sicher verschlüsselt und können nur vom Empfänger gelesen werden.
- **Open Source**: Der Quellcode ist öffentlich einsehbar und wird regelmäßig von der Community überprüft.
- **Keine Werbung**: Signal wird nicht durch Werbung oder Datenverkauf finanziert, was die Privatsphäre schützt.
- **Keine Sammlung von Metadaten**: Signal speichert keine Daten über den Nutzer, wie z.B. Kontakte oder Nachrichteninhalte.
- **Kostenlos**: Signal ist eine kostenlose App, die keine versteckten Kosten oder Premium-Versionen bietet.
- **Multiplattform**: Verfügbar auf iOS, Android und Desktop, ermöglicht sichere Kommunikation auf allen Geräten.
- **Gruppen- und Sprach-/Videoanrufe**: Erlaubt sichere Gruppen-Chats sowie Sprach- und Videoanrufe mit End-to-End-Verschlüsselung.

Signal und der Fall Thomas Schmid

Obwohl Signal als sicherer Messenger gilt, konnten die Ermittler im Fall Thomas Schmid auf seine Signal-Chats zugreifen. Das Problem lag an einem unsicheren Backup.

Wichtige Details:

- Signal-Backups sind lokal verschlüsselt und landen *nicht* in der Cloud.
- Auf iPhones gibt es nur Backups, wenn man ein **komplettes System-Backup** über Time Machine macht.
- Time Machine speichert *alle* Gerätedaten, auch entschlüsselte Signal-Datenbanken, solange das Gerät entsperrt ist. iOS speichert die Signal-Datenbank im RAM entschlüsselt, während die App entsperrt ist. Dies kann bei ungesicherten Backups ein Risiko darstellen.
- Im Fall Schmid war das Backup nicht gut gesichert — Ermittler hatten Zugriff.

Fazit: Wenn ein Gerät entsperrt ist oder Backups unsicher sind, kann selbst die beste Verschlüsselung umgangen werden.

Digital Markets Act (DMA): Warum WhatsApp sich öffnen muss

Was ist der DMA?

- Der Digital Markets Act (DMA) der EU stuft WhatsApp als **Gatekeeper** ein.
- Ziel: Wettbewerb fördern und Lock-in-Effekte verhindern.
- Meta muss **Interoperabilität** mit anderen Messenger-Diensten ermöglichen.

Folgen für WhatsApp:

- Öffnung für externe Messenger wie Signal.
- Mögliche Kompromisse bei Sicherheit und Datenschutz.
- Gefahr von Metadaten-Sammlung durch Meta.

Meta, Fediverse und Signal: Datenschutzrisiken

Problem: Meta könnte durch die Öffnung massive Datenmengen erfassen.

- **Tracking im Fediverse**: Nutzerbewegungen plattformübergreifend analysierbar.
- **Erweiterte Datensammlung**: Metadaten von externen Plattformen nutzbar.
- **Deanonymisierung**: Verknüpfung von Aktivitäten aus verschiedenen Quellen.
- **Gefahr für Ende-zu-Ende-Verschlüsselung**: Druck zur Implementierung von Hintertüren.
- **Kommerzielle Nutzung**: Profilerstellung für gezielte Werbung.

Gegenwehr von Signal und dem Fediverse

Wie reagieren unabhängige Plattformen?

- **Signal**: Droht mit Rückzug aus der EU, falls Datenschutz gefährdet wird.
- **Fediverse**: Admins könnten Meta-Instanzen blockieren.
- **Dezentrale Alternativen**: Förderung unabhängiger Netzwerke.

Mögliche Folgen eines Signal-Rückzugs aus der EU:

- Nicht mehr in App Stores verfügbar, keine Updates mehr.
- Manuelle Installation über APK nötig.
- Mögliche IP-Blockaden $\rightarrow$ VPN erforderlich.
- Nutzer verlieren eine der sichersten Messenger-Optionen.

Schwäche des Fediverse: Eine offene Tür reicht!

Problem: Dezentrale Netzwerke können Meta nicht komplett aussperren.

- **Wenn eine Instanz Meta akzeptiert**, kann Meta über diese das gesamte Fediverse erreichen.
- Öffentliche Posts von Nutzern anderer Instanzen werden abrufbar.
- **Interaktionen (Antworten, Boosts)** von geblockten Instanzen werden trotzdem sichtbar.
- Gefahr der **Metadatenanalyse**: Wer mit wem interagiert, Aktivitätsmuster.
- Mögliche langfristige Strategie von Meta: Erst harmlos starten, dann Nutzerbindung aufbauen.

Lösung? Breite Blockade durch möglichst viele Instanzen – aber keine Garantie!

Wie schütze ich mich beim Surfen?

- **Warum ist Chrome schlecht?**
  - Google sammelt viele Daten über dein Surfverhalten, was deine Privatsphäre gefährdet.
  - Chrome verwendet einen zentralisierten Ansatz, der deine Daten mit Google-Servern verbindet.
  - Zukünftige Änderungen (Manifest V3) könnten Adblocker wie uBlock Origin weniger effektiv machen.
- **Warum lieber Firefox?**
  - Firefox ist Open Source und hat Datenschutz als Kernprinzip.
  - Der Browser bietet erweiterte Datenschutzfunktionen wie Tracking-Schutz und ist nicht von Werbung abhängig.
- **uBlock Origin:**
  - Erweiterung, die Werbung und Tracker blockiert und so deine Privatsphäre schützt.
  - Reduziert die Ladezeiten von Webseiten und verbessert die Sicherheit beim Surfen.

Alternativen zu Google & Bing

- **Ecosia, DuckDuckGo, Startpage:**
  - Alle drei bieten Suchergebnisse ohne das Sammeln persönlicher Daten.
  - **Achtung:** Sie nutzen entweder Bing (Ecosia, DuckDuckGo) oder Google (Startpage) für die Suchergebnisse, sodass trotzdem einige Daten an Microsoft bzw. Google weitergegeben werden.
  - **Vorteil:** Sie schützen vor Tracking und minimieren die Datensammlung im Vergleich zu Google oder Bing.
- **Qwant:**
  - Europäische Suchmaschine, die keine persönlichen Daten speichert und keine Tracker verwendet.
  - Besonders empfehlenswert für Datenschutz und Privatsphäre.

ProtonMail: Sichere E-Mail

- **Ende-zu-Ende-Verschlüsselung:**
  - Alle E-Mails sind standardmäßig verschlüsselt, sodass nur der Empfänger die Nachricht lesen kann.
- **Schweizer Datenschutzgesetze:**
  - ProtonMail unterliegt den strengen Datenschutzbestimmungen der Schweiz, die die Privatsphäre der Nutzer besser schützen als viele andere Länder.
- **Keine Werbung, keine Tracking:**
  - ProtonMail sammelt keine persönlichen Daten und zeigt keine Werbung.
- **Open Source:**
  - Der Code von ProtonMail ist Open Source, was zusätzliche Transparenz bietet und von der Community überprüft werden kann.
- **Kostenlos & Premium-Optionen:**
  - ProtonMail bietet ein kostenloses Konto mit grundlegenden Funktionen sowie kostenpflichtige Pläne mit erweiterten Features.

Sicheres Passwortmanagement

Eigenschaften eines sicheren Passworts:

- Mindestens 16 Zeichen, besser 20+.
- Mischung aus Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen.
- Kein Bezug zu persönlichen Daten.
- Keine Wörterbuch-Passwörter (z.B. "Passwort").

Sicheres Passwortmanagement:

- Jedes Konto sollte ein eigenes Passwort haben.
- Passwortmanager nutzen: Keepass (offline, Open Source) oder Firefox Lockwise.
- Zwei-Faktor-Authentifizierung (2FA) aktivieren, wo möglich.

Beispiel für ein sicheres Passwort: `A9b$4x!F2pLqW8zR6tUv`


Strong password
Using it for multiple sites

Passwortstärke - Beispielrechnung

Ein sicheres Passwort:
Länge: 22 Zeichen, Zeichensatz: 94 Zeichen (Groß-/Kleinbuchstaben, Ziffern, Sonderzeichen)
Kombinationen:

$$94^{22} \approx 2{,}56 \cdot 10^{43}$$

Zeit zum Knacken (Brute-Force):
Ryzen 5700G: 3,7 GHz $\times$ 8 Kerne = 29,6 Milliarden Versuche/Sekunde

$$\text{Benötigte Zeit} \approx \frac{2{,}56 \cdot 10^{43}}{2{,}96 \cdot 10^{10}} \approx 8{,}66 \cdot 10^{33} \text{ Sekunden}$$

Das entspricht etwa $2{,}75 \cdot 10^{26}$ Jahren — deutlich mehr als das Alter des Universums!

Exponentielle Explosion — Warum lange Passwörter sicher sind

Exponentielle Explosion:
Ein Begriff, der beschreibt, wie schnell die Anzahl der Möglichkeiten bei zunehmender Komplexität wächst.
Beispiel:
Passwort mit 6 Zeichen (Zeichensatz: 94 Zeichen):

$$94^6 = 689{,}869{,}781{,}056$$

Passwort mit 22 Zeichen:

$$94^{22} \approx 2{,}56 \cdot 10^{43}$$

Kombinatorische Explosion:
Bereits kleine Erhöhungen der Passwortlänge führen zu enormen Zuwächsen an möglichen Kombinationen.
Fazit: Das exponentielle Wachstum macht es extrem aufwendig, komplexe Passwörter zu knacken!

Passwortsicherheit überprüfen

- **CheckDeinPasswort.de**: Hier kannst du dein Passwort auf Sicherheitslücken prüfen. Der Service zeigt dir, wie stark dein Passwort ist und gibt dir Tipps, wie du es sicherer machen kannst, indem du z.B. stärkere Kombinationen verwendest. Besuche die Seite unter: checkdeinpasswort.de
- **Have I Been Pwned?**: Mit diesem Tool kannst du überprüfen, ob deine E-Mail-Adresse oder dein Passwort in einer bekannten Datenpanne veröffentlicht wurde. So erfährst du, ob deine Anmeldedaten in einem Leck auftauchen und kannst entsprechende Maßnahmen ergreifen. Besuche die Seite unter: haveibeenpwned.com

Hands-On: Passwortchecker vs. Realität

- **Ziel**: Überprüfung, ob Online-Passwort-Checker realistische Aussagen treffen.
- **Theorie vs. Praxis**:
  - Online-Tools wie `checkdeinpasswort.de` berechnen oft nur theoretische Werte.
  - Tatsächliche Passwortsicherheit hängt stark von der Implementierung ab.
- **Experiment:**
  - Wie sicher sind verschiedene Passworttypen wirklich?
  - PDF-Passwörter unter realen Bedingungen testen mit John the Ripper.
- **Challenge:**
  - In einer `zip`-Datei steckt ein lustiges Meme, das sich über die Kommentarsektion bei der Distowahl lustig macht.
  - **Was müsst ihr machen?**
    - Ihr müsst `duck.ai` das Problem schildern.
    - Das Programm, das ihr braucht, ist noch nicht installiert – also müsst ihr es selbst via `apt` nachinstallieren!

Einführung in die Laufwerksverschlüsselung

- **Was ist Laufwerksverschlüsselung?**
  - Prozess, bei dem Daten auf einem Laufwerk (Festplatte, USB-Stick) verschlüsselt werden.
  - Nur autorisierte Benutzer mit dem korrekten Passwort oder Schlüssel haben Zugriff.
- **Warum ist das wichtig?**
  - Schutz vor unbefugtem Zugriff bei Verlust oder Diebstahl.
  - Schutz sensibler Daten (z.B. persönliche Dateien, Projekte, Fotos).
  - Absicherung bei Mehrbenutzersystemen.
- **Einsatzgebiete:**
  - Private Daten auf Laptops und PCs.
  - Externe Festplatten oder USB-Sticks.
  - Verschlüsselte Container für spezielle Dateien (z.B. Backups).

Was ist VeraCrypt?

- Open-Source-Software zur Verschlüsselung ganzer Laufwerke oder Container.
- Plattformunabhängig: Verfügbar für Windows, Linux und macOS.
- **Vorteile:**
  - Kostenlos und quelloffen, dadurch überprüfbar.
  - Unterstützt AES, Serpent, Twofish und deren Kombinationen.
  - Unterstützung für versteckte Container für zusätzliche Sicherheit.
  - Keine bekannten Backdoors.
- **Nachteile:**
  - Datenverlust bei Vergessen des Passworts.
  - Keine offizielle mobile Version (z.B. Android, iOS).

Grundlegende Konzepte der Verschlüsselung

- **Symmetrische Verschlüsselung:** Ein Passwort für Ver- und Entschlüsselung (VeraCrypt nutzt dies).
- **Hash-Funktionen:** VeraCrypt nutzt SHA-512 oder Whirlpool für Hashing, um Passwörter sicher zu speichern.
- **Schlüssellänge:** AES-256 bietet eine Schlüssellänge von 256 Bit, was als sicher gilt.
- **PBKDF2:** Passwort wird mehrfach gehasht, um Brute-Force-Angriffe zu erschweren.
- **Salting:** Einzigartiger Wert wird zu Passwörtern hinzugefügt, um Rainbow-Table-Angriffe zu verhindern.

Hands-On: Versteckte Partition auf USB-Stick

- **Ziel**: Erstellung einer versteckten, verschlüsselten Partition auf einem USB-Stick.
- **Tool**: VeraCrypt – Open-Source-Software zur Verschlüsselung.
- **Schritte**:
  - USB-Stick in zwei Partitionen aufteilen:
    - **Kleine Partition** (ca. 256 MB): Verschlüsselt und versteckt mit VeraCrypt.
    - **Restliche Partition**: Normale Nutzung ohne Verschlüsselung.
  - Versteckte Partition enthält eine KeePass-Datenbank und wichtige Dokumente.

- **F-Droid:** Open-Source App-Store für Android, bietet datenschutzfreundliche Alternativen.
- **NewPipe:** Open-Source YouTube-Client ohne Werbung und Tracking.
- **K-9 Mail:** Sichere und datenschutzfreundliche E-Mail-App für Android.
- **LineageOS:** Android-Betriebssystem, datenschutzfreundlich und ohne Google-Dienste.
- **GrapheneOS:** Android-basierte, datenschutzorientierte ROM mit verstärkter Sicherheit und Privatsphäre.

Apps und Berechtigungen:

- Zugriffsrechte kritisch prüfen (Standort, Kamera, Mikrofon).
- Deinstallation unnötiger Apps.

Warum Apple keine echte Alternative ist

- **Geschlossenes Ökosystem**: Apple erlaubt nur Apps aus dem eigenen App Store.
- **Kein echtes Open Source**: iOS ist proprietär, und der Code kann nicht überprüft werden.
- **Vendor Lock-in**: Nutzer werden in die Apple-Infrastruktur gezwungen (iCloud, Safari, Apple Mail etc.).
- **Tracking & Werbung**: Trotz Datenschutz-Versprechen sammelt Apple Daten für personalisierte Werbung.
- **Keine unabhängigen App-Stores**: F-Droid, NewPipe und andere datenschutzfreundliche Apps sind nicht erlaubt.

Anonymes Surfen: Tor

- **Was ist Tor?**
  - Tor (The Onion Router) ist ein Open-Source-Netzwerk, das für anonymes Surfen entwickelt wurde.
  - Es verschlüsselt deine Internetverbindung und leitet sie über mehrere zufällige Knotenpunkte weltweit.
  - Ziel: Deine Identität und Aktivität im Internet zu verschleiern, sodass niemand (einschließlich Internetanbieter oder Websites) dich zurückverfolgen kann.
- **Vorteile von Tor:**
  - Schutz vor Zensur und Überwachung.
  - Bietet Anonymität, besonders für Journalisten, Aktivisten und Menschen in autoritären Staaten.
  - Ermöglicht Zugang zu gesperrten Webseiten ("Great Firewall" in China).
- **Wie funktioniert Tor?**
  - Deine Verbindung wird durch mehrere Knoten (Relays) im Tor-Netzwerk weitergeleitet, wobei jeder Knoten nur einen Teil der Verbindung kennt.
  - Diese Verschlüsselung macht es für Dritte nahezu unmöglich, die Verbindung bis zu ihrem Ursprung zurückzuverfolgen.

Clear Web, Deep Web und Dark Web

- **Clear Web:**
  - Das "normale" Web, das von Suchmaschinen indexiert wird.
  - Öffentlich zugängliche Webseiten wie Google, Wikipedia, Nachrichtenportale.
  - Jeder kann diese Inhalte durchsuchen und darauf zugreifen.
- **Deep Web:**
  - Der Teil des Webs, der nicht von Suchmaschinen indexiert wird.
  - Beinhaltet private Datenbanken, E-Mail-Konten und andere nicht öffentlich zugängliche Informationen.
  - Der Zugriff erfolgt in der Regel über Passwörter oder spezielle Berechtigungen.
- **Dark Web:**
  - Ein Teil des Deep Webs, der absichtlich verborgen ist und Anonymität bietet.
  - Meist über das Tor-Netzwerk zugänglich, um die Privatsphäre zu schützen.
  - Wird von Personen genutzt, die Anonymität benötigen, z.B. in Ländern mit Zensur oder für den sicheren Austausch von Informationen.

Das Dark Web und sichere Kommunikation

- **Warum das Dark Web?**
  - Bietet Schutz vor Zensur und Überwachung, besonders für Whistleblower.
  - Anonymität bei der Weitergabe von Informationen, z.B. über das Tor-Netzwerk.
- **Beispiel: SecureDrop**
  - Plattform für den sicheren Austausch von Informationen zwischen Whistleblowern und Journalisten.
  - Über Tor erreichbar, schützt vor Verfolgung.
- **Bedeutung für die Gesellschaft:**
  - Whistleblower decken Missstände auf und spielen eine wichtige Rolle bei der Aufklärung von Korruption und Verbrechen.
  - Sie helfen, gesellschaftliche Missstände zu beseitigen und Verantwortliche zur Rechenschaft zu ziehen.
  - Ohne Whistleblower könnten viele Skandale, wie die Massenüberwachung durch die NSA oder Kriegsverbrechen, unentdeckt bleiben.

Das Dark Web – Mythen vs. Realität

- **"Das Darkweb ist ein gefährlicher Ort voller Geheimnisse."**
  Realität: 99% der Onion-Links funktionieren nicht oder führen zu gesperrten Seiten.
- **"Es gibt geheime, unzensierte Märkte."**
  Realität: Von den funktionierenden Seiten sind etwa 99% Scams oder betrügerische Angebote.
- **"Das Darkweb ist der geheime Handel für alles, was illegal ist."**
  Realität: Die verbleibenden 1% der Seiten verlangen meist Bitcoins als einzige Zahlungsmethode.
- **Zusammengefasst:** Das Darkweb ist weit weniger mystisch und viel mehr ein Labyrinth voller toter Links und Betrüger.

Hands-On: Umgehen von Geoblocking und Verbesserung der Privatsphäre

- **Ziel**: Vergleich von Methoden, um auf gesperrte Inhalte zuzugreifen und gleichzeitig die Anonymität sowie den Datenschutz zu wahren.
- **Test-Websites**:
  - `de.rt.com` (Russia Today)
  - `kinox.to` (Streamingseite)
  - `serienstream.to` (Streamingseite)
- **Methoden**:
  - **1. Normaler Browser**: Überprüfung der allgemeinen Zugänglichkeit und der möglichen Geoblocking-Maßnahmen.
  - **2. Tor-Browser**: Testen der Anonymität und der Umgehung von Geoblocking.
  - **3. Browser mit geändertem DNS-Server**: Nutzung alternativer DNS-Dienste (z.B. 1.1.1.1 oder 8.8.8.8) zur Umgehung von Zensurmaßnahmen und Verbesserung des Datenschutzes.

Sexting — Was ist das?

- **Was ist Sexting?**
  - Austausch intimer oder erotischer Bilder oder Nachrichten, meist über digitale Medien.
- **Risiken:**
  - Verlust der Kontrolle: Bilder können weitergeleitet oder veröffentlicht werden.
  - Mobbing und Erpressung: Ungewollte Verbreitung kann zu psychischem Druck führen.
  - Rufschädigung: Negative Auswirkungen auf soziale und berufliche Beziehungen.
- **Tipps:**
  - Keine intimen Bilder teilen, die später bereut werden könnten.
  - Klare Kommunikation in Beziehungen: Respekt vor Privatsphäre und Einwilligung.
  - Unterstützung suchen bei Missbrauch (Beratungsstellen, Polizei).

Sexting — Rechtliche Aspekte

- **Gesetzlicher Schutz:** § 207a StGB schützt Minderjährige vor Missbrauch und Ausbeutung durch pornografische Inhalte.
- **Minderjährige unter 14 Jahren:** Strafmündigkeit liegt nicht vor, jedoch können Eltern oder Erziehungsberechtigte einschreiten.
- **Minderjährige ab 14 Jahren:**
  - Erstellung und Verbreitung expliziter Bilder ist strafbar, wenn ohne Einwilligung oder gegen den Willen der betroffenen Person.
  - Ausnahme: Freiwillige Erstellung und privater Austausch zwischen Gleichaltrigen (15-18 Jahre) ist meist straffrei.
- **Strafrechtliche Konsequenzen:**
  - Verbreitung ohne Zustimmung: Verletzung der Persönlichkeitsrechte.
  - Erpressung mit intimen Bildern: Straftatbestand der Nötigung oder Erpressung.

Was tun bei unangemessenen Anfragen (z.B. "Sexting")?

- **1. Nicht antworten:** Keine Reaktion auf die Anfrage zeigen. Sich nicht auf die Unterhaltung einlassen.
- **2. Screenshot machen:** Einen Screenshot der Anfrage anfertigen, auf dem folgende Informationen sichtbar sind:
  - URL der Seite oder der Nachricht
  - Benutzername der anfragenden Person
  - Datum und Uhrzeit der Anfrage
- **3. Melden:** Die Anfrage an die entsprechenden Stellen weiterleiten:
  - **Rat auf Draht (147):** Telefonische Beratung für Kinder und Jugendliche. Anonym und rund um die Uhr erreichbar. Weitere Informationen unter `https://www.rataufdraht.at/`.
  - **Meldestelle gegen Kinder- und Jugendpornografie (Saferinternet.at):** Möglichkeit zur Meldung von Online-Inhalten, die gegen das Gesetz verstoßen. Besuche `https://www.saferinternet.at/` für mehr Informationen.
  - **Polizei:** Bei strafrechtlich relevanten Vorfällen kann die lokale Polizeidienststelle kontaktiert werden. Notrufnummer: 133.

Was ist ein VPN?

- VPN steht für **Virtual Private Network**.
- Erstellt eine **verschlüsselte Verbindung** zwischen deinem Gerät und einem Server im Internet.
- Deine **IP-Adresse** wird maskiert, wodurch du scheinbar von einem anderen Standort surfst.
- Bietet **Sicherheits-** und **Datenschutzvorteile**.

Wofür braucht man ein VPN?

- Erhöhung der **Anonymität** im Internet.
- Umgehen von **Geoblocking** (z.B. bei Streaming-Diensten).
- Schutz vor **Tracking** durch Websites, Werbetreibende und Dritte.
- Sicherer Zugriff auf das Internet in **öffentlichen WLANs**.
- Schutz vor **Man-in-the-Middle-Angriffen**.

Hilft ein VPN beim Datenschutz?

- Schützt vor Ausspähung in **unsicheren Netzwerken**.
- Verhindert **IP-basiertes Tracking**.
- Aber: VPN-Anbieter kann **Zugriff auf deine Daten** haben.
- Ein **vertrauenswürdiger Anbieter** ist entscheidend!

Vor- und Nachteile eines VPNs

Vorteile:

- **Erhöhte Anonymität** und Datenschutz.
- Zugriff auf **gesperrte Inhalte** (z.B. länderspezifische Inhalte).
- Schutz vor **Datenklau** und Überwachung.

Nachteile:

- Vertrauen in den **VPN-Anbieter** nötig.
- Kann die **Internetgeschwindigkeit** verlangsamen.
- Schützt nicht vor allen **Tracking-Methoden** (z.B. Cookies).
- In einigen Ländern sind VPNs **eingeschränkt** oder verboten.