Was wir jetzt tun können *(Checkliste)*

Sofort – kleine Hebel, grosse Wirkung

1. **Reduziere deine digitale Spur.**
   Weniger Apps, weniger Sensoren. Lösch alles, was dich ausliest, Maps, Facebook, TikTok. Wenn du's brauchst, nutze es im Browser mit Ad- und Tracker-Blocker.
2. **Handy-Pragmatik statt Dauerüberwachung.**
   Kaufe dir ein einfaches Feature-Phone (das gute alte „Nokia-Prinzip") oder ein Smartphone mit herausnehmbarer Batterie. Nur so kannst du das Gerät wirklich ausschalten. Wenn du dein Smartphone behältst: Flugmodus ist dein Freund, Funk nur an, wenn nötig.
3. **Raus aus dem Google-Apple-Kosmos.**
   Je weniger du über deren Systeme gehst, desto besser. Alternative App-Stores, Web-Apps oder datenschutzfreundliche Android-Versionen sind kein Nerd-Kram, sondern digitale Selbstverteidigung.
4. **Kommunikation sichern.**
   Nutze z.B. Signal für verschlüsselte Chats und Anrufe. Schalte App-Berechtigungen konsequent ab (Mikrofon, Standort, Kontakte). Signal ist kein Garant für Freiheit, aber eines der letzten Werkzeuge, die nicht im Dienst der Kontrolle stehen. (*Bei Threema nach den bekanntgewordenen Vorfällen eher fraglich*.)
5. **Physisch abschirmen.**
   Ein einfacher Faraday-Beutel schützt dein Gerät bei Demos oder Reisen. Akku raus, wenn's wirklich privat sein soll. Bluetooth und WLAN aus, solange du sie nicht brauchst.

Mittelfristig – baue dir Privatsphäre ein

1. **Hardware-Hygiene.**
   Wenn du ein neues Handy kaufst, wähle eines mit herausnehmbarem Akku oder einem offenen System, bei dem du siehst, was im Innern läuft, ohne versteckte Google- oder Apple-Verbindungen.
2. **Je weniger „Smart", desto sicherer.**
   Alte Modelle oder sogenannte Feature-Phones (z. B. Nokia, Punkt, Light Phone) können meist nur telefonieren und SMS schicken und genau das ist ihr Vorteil. Kein Tracking, keine Cloud, keine Überwachung.
3. **Daten offline sichern.**
   Bewahre sensible Daten auf einer externen, verschlüsselten Festplatte. Gib Behörden

und Firmen nur, was zwingend nötig ist. Jede freiwillige Angabe ist ein Geschenk ans System.

4. **E-Mail & Browser absichern.**
   Nutze datenschutzfreundliche Mail-Anbieter und Browser mit integrierten Trackingschutz. Trenne Lebensbereiche: eigene Profile für Arbeit, Privatleben und Behördenkontakte.

Politisch & gemeinschaftlich – der Hebel für echte Veränderung

1. **Aufklären & vernetzen.**
   Organisiert Info-Abende, schreibt Leserbriefe, erklärt Freunden, was hinter digitalen IDs, ESG-Ratings oder Palantir-Verträgen steckt. Wissen ist die stärkste Waffe.
2. **Transparenz einfordern.**
   Stelle Anfragen an Behörden: zur E-ID, zum fedpol, zum NDB, zu IT-Beschaffungen. Fordere Einsicht in Verträge, Datenschutz-Analysen und Folgekosten. Wenn sie Auskünfte verweigern, dokumentiere es.
3. **Lokal handeln.**
   Viele Projekte starten in der Gemeinde. Ein Gespräch mit dem Stadtrat kann mehr bewirken als zehn Petitionen. Wer lokal stoppt, verhindert global.
4. **Zivile Non-Compliance.**
   Sag auch mal Nein. Nutze Barzahlung. Reiche Anträge auf Papier ein. Lass Apps links liegen. Kleine Akte der Verweigerung summieren sich und sie wirken.

Warum das realistisch und optimistisch ist

Weil es funktioniert. Die meisten dieser Schritte kosten kein Geld, nur Bewusstsein. Jede gelöschte App, jedes Offline-Backup, jedes lokale Nein ist ein Schritt zurück in die Eigenverantwortung.

Technologie ist kein Naturgesetz, sie ist ein Werkzeug. Und Werkzeuge gehören in die Hand des Menschen, nicht seiner Verwalter.

Freiheit beginnt nicht im Parlament, sondern im Alltag. Im Umgang mit deinem Handy. Deinen Daten. Deiner Stimme.