

KI-Agenten: handeln inzwischen selbständig
Prediction Markets: bepreisen Real-World-Ereignisse
Ergebnis: Daten → strategischer Hebel & neues Risiko

Sicherheit vs Privatsphäre

Daten als Waffe für KI-Agenten und Prediction Markets

Impulsbeitrag von Eric Moser, 17. Februar 2026

KI-Agenten & Prediction Markets – was ist das eigentlich?

KI-Agenten

= KI, die nicht nur antwortet, sondern Aufgaben selbständig plant und ausführt (oft mit Tool-Zugriffen)

Wie funktioniert's?

- Ziel erhalten → Plan erstellen → Tools nutzen (Browser, E-Mail, Dateien, APIs) → Aktion ausführen
- Ergebnis prüfen → Loop (nachjustieren, weiterarbeiten)

Was tun sie typischerweise?

- Infos beschaffen, zusammenfassen, E-Mails schreiben/sendern, Termine buchen, Daten verarbeiten, Workflows automatisieren

Relevanz:

- Produktivität (Delegation)
- Mehr Risiko (zu breite Berechtigungen, „untrusted“ Skills/Plugins, Prompt-Injection, Fehlkonfiguration)



KI-Agenten & Prediction Markets – was ist das eigentlich?

Prediction Markets

= Markt, auf dem “Event-Kontrakte” gehandelt werden (JA/NEIN auf ein Ereignis), ähnlich zu Sportwetten, Preis entspricht grob impliziter Wahrscheinlichkeit.

Wie funktioniert's?

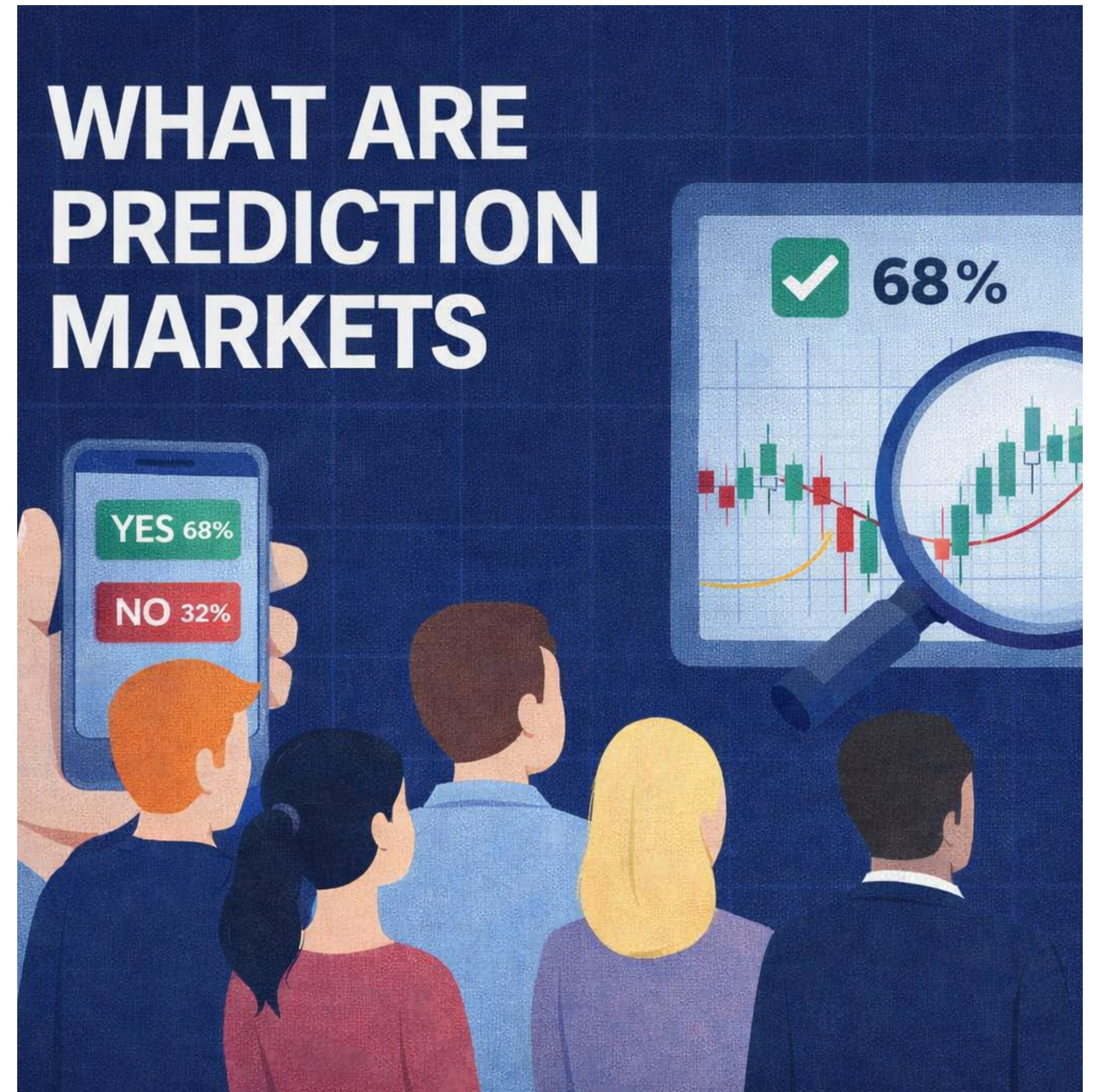
- Frage/Ereignis definieren → Leute handeln JA/NEIN
→ Preis bewegt sich durch Angebot/Nachfrage
- Wenn Outcome feststeht: Abrechnung (Settlement)
→ Gewinne/Verluste

Was passiert?

- “Wissen/Erwartungen bündeln” (Crowd-Signal) – oft schneller als Umfragen, aber abhängig von Liquidität/Regeln

Relevanz:

- Information wird direkt monetarisierbar
- Ab bestimmter Größe: Anreiz für Insider-Nutzung oder sogar Manipulation (wenn jemand Einfluss auf das Ereignis hat)



Agenda

- Die IT Schutzziele Sicherheit & Privatsphäre
- Wo Daten heute gesammelt werden – für unsere “Sicherheit”
- Die Bedeutung von Privatsphäre
- KI Agenten: OpenClaw
- Prediction Markets: Kalshi & Polymarket
- Das neue Ausmaß der Verwertungs- & Verknüpfungsmöglichkeiten von Daten
+ anschließende Diskussion

Sicherheit

- Security (CIA): Vertraulichkeit, Integrität, Verfügbarkeit

Privatsphäre (Privacy)

- Kontrolle/Begrenzung personenbezogener Verarbeitung

Wo Daten für notwendige Sicherheit gesammelt werden

- Telekom/ISP: Verkehrs- & Standortdaten (wer/wann/wo/wie lange)
 - Vorrats-/IP-Speicherung: (Debatte)
IP+Port anlasslos für Monate
- Netz-Protokolle: IP-Adresse↔Anschluss, Ports, Session-Zeiten
- Bestandsdaten: Name/Adresse/Vertrag, SIM/IMSI, Geräte-IDs, Metadaten allgemein
- Lawful Interception: technische Schnittstellen für Behördenzugriffe
- ePA: Befunde, Arztbriefe, Medikationsliste/-plan, weitere Dokumente
- Biometrie & Identität: Pässe, Grenzsysteme
- ...

Sicherheits-Rationalität

Warum die Datensammelei?

- Für Betrug/Abuse-Prevention & Aufklärung Verbrechen
- Für Patientensicherheit & Medikationsinfos (bei ePA)
- “Mehr Daten = mehr Sicherheit” ist oft ein Trugschluss
- Welche Datensammlung dient unserem Schutz – und welche dient am Ende Manipulation oder Profiling?

Warum brauchen wir Privatsphäre überhaupt?

Privatsphäre durch Datenschutz

- Informationelle Selbstbestimmung (BVerfG-Urteil zur Volkszählung 1983)
- Schützt Autonomie (Entscheidungen ohne Druck)
- Würde & Intimität: Schutz des Inneren (Körper, Beziehungen, Gesundheit)
- Fairness: Schutz vor Diskriminierung & Preis-/Job-Profiling
- Sicherheit: Weniger Angriffsfläche (Erpressung, Social Engineering)
- Y. N. Harari:
“Hackable Humans” → Daten + Rechenpower = Manipulationspotenzial

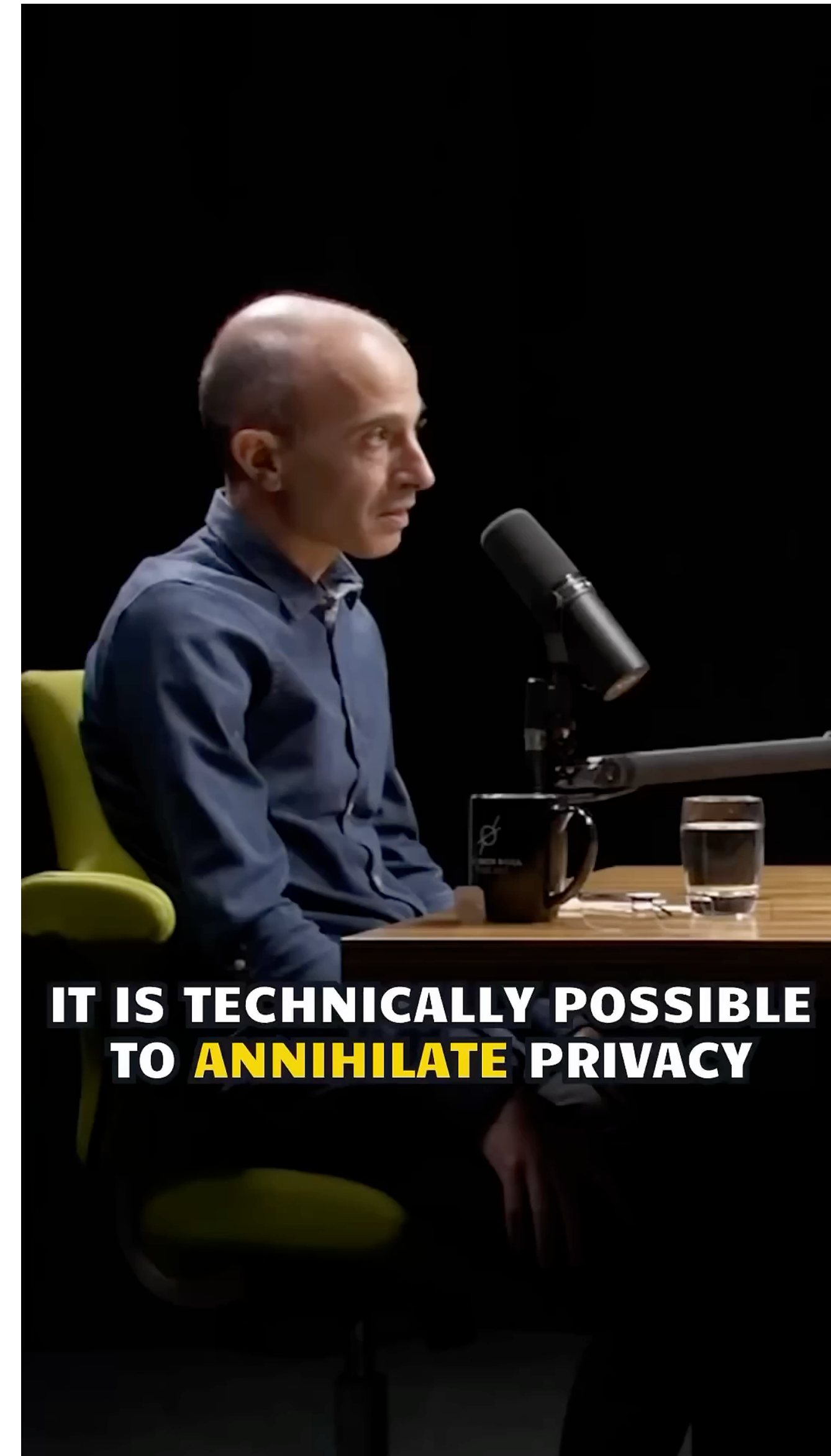
Kollisionsbeispiele Sicherheit / Privatsphäre

- E-Mail-Konto: Anonymität vs. Account-Recovery/Verfügbarkeit
- ePA: schnelle Hilfe vs. sensibler Missbrauch
- Abwägung: Welche Bedrohung ist wahrscheinlicher? Wer hat Macht?

Prof. Yuval Noah Harari

Historian, philosopher and international bestseller

"The biggest political question of our era is: who controls the data?"



KI-Agenten: Was ändert sich qualitativ?

- Agenten haben Zugriffe (Files, Shell, Accounts)
- Persistenz (laufen “nebenbei”)
- Risiko: Prompt-Injection, Skills/Plugins, Fehlkonfiguration
- Entwickeln Eigendynamik durch Plattformen wie Moltbook
- Schlussendlich unberechenbar

Und jetzt

...

Prediction Markets: Kalshi & Polymarket

- Märkte handeln “Event Contracts” auf Real-World-Outcomes
- Breite Themen: Politik, Wetter, Popkultur, Wirtschaft
- Risiko: Insider-Infos & Anreiz zur Manipulation
- Feb. 2026: Personen sollen klassifizierte Militärinfos genutzt haben, um auf Polymarket zu wetten

 Polymarket

Search polymarkets...

[How it works](#)

[Trending](#) [Breaking](#) [New](#) | [Politics](#) [Sports](#) [Crypto](#) [Finance](#) [Geopolitics](#) [Earnings](#) [Tech](#) [Culture](#) [World](#)

Taylor Swift predictions & odds · 5 polymarkets

[All](#) [Sports](#) [Music](#) [Celebrities](#) [NFL](#) [Taylor Swift](#) [Culture](#) [Travis Kelce](#)



Taylor Swift · Culture

Taylor Swift x Travis Kelce get married by...?

\$131K Vol. \$2.9K Liq. 3

62% >
June 30



Taylor Swift · Music

Taylor Swift pregnant in 2025?

\$2M Vol. \$5.9K Liq. 88 Ends in 11 months

33% >
December 31, 2026



Taylor Swift · Sports

Will Travis Kelce retire before next season?

\$5.9K Vol. \$942 Liq. 1 Ends in 7 months

11% >

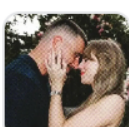


Taylor Swift · Music

Taylor Swift pregnant before marriage?

\$166K Vol. \$16.7K Liq. 19 Ends in 7 months

9% >



Taylor Swift · Music

Who will attend Taylor Swift and Travis Kelce's wedding?

\$208K Vol. \$19.2K Liq. 18 Ends in 11 months

80% >
Jack Antonoff

Meine These:

**Neue Dimension der Verknüpfung & Verarbeitung von Daten durch KI
+ tiefe aktive Befähigung von KI-Agenten
+ Prediction Markets: Information wird direkt monetarisierbar
= **

Leitfragen: Minimierung? Kontrolle? Audit? Verbote bestimmter Märkte?

Diskussionsrunde

Thema A — “Agenten-Hygiene” Guidelines

Thema B — Kreativ werden: Was kann noch alles durch Prediction Markets wettbar werden?

Thema C — “Privacy vs Security” an euren eigenen Beispielen

+ freie und eigene Vorschläge