

Sicherheit vs. Privatsphäre

Daten als Waffe für KI-Agenten und Prediction Markets

Handout – CEC Impulsbeitrag vom 17. Februar 2026 von Eric Moser

Kurzfassung

- Autonome KI-Agenten handeln zunehmend selbständig (Zugriffe, Persistenz, Tools) – das erhöht Nutzen, aber auch Fehlbedienung und Missbrauch.
- Prediction Markets bepreisen Real-World-Ereignisse – Information wird dadurch unmittelbarer monetarisierbar.
- In Kombination wird Datensammlung strategischer: mehr Verknüpfung, mehr Anreiz zur Ausnutzung, mehr Machtasymmetrie.

Was sind KI Agenten und Prediction Markets überhaupt?

KI-Agenten

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

Prediction Markets

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

1) Begriffe: Security vs. Privacy

- Sicherheit (CIA-Triade): Vertraulichkeit (Confidentiality), Integrität (Integrity), Verfügbarkeit (Availability).
- Privatsphäre: Kontrolle und Begrenzung der Verarbeitung personenbezogener Daten (wer weiß was – wann – wozu).
- Konflikt heißt meist Zielkonflikt: höhere Sicherheit kann mehr Datenzugriff bedeuten; mehr Privatsphäre kann Verfügbarkeit/Forensik erschweren.

2) Wo heute Daten gesammelt werden

- Telekom/Internet (ISP): Verkehrs- und Standortdaten (wer/wann/wo/wie lange).
- Bestandsdaten: Name/Adresse/Vertrag, SIM/IMSI, Geräte-IDs.
- Netz-Protokolle: IP-Adresse <-> Anschluss-Zuordnung, Ports, Session-Zeiten.
- Lawful Interception: technische Schnittstellen zur Umsetzung behördlicher Anordnungen (je nach Rechtsgrundlage).
- Vorrats-/IP-Speicherung: Debatten um anlasslose Speicherung von IP+Port über Monate (Ziel: nachträgliche Zuordnung).
- Elektronische Patientenakte (ePA): z.B. Befunde, Arztbriefe, Medikationsliste/-plan, weitere Dokumente.
- Metadaten allgemein: Gerät, Standort, Zeit, Beziehungen/Netzwerk, Nutzungsmuster.
- Biometrie & Identität: Pässe, Grenzsysteme, Identitätsprüfungen.

3) Sicherheits-Rationalität: Warum so viel Datensammlung?

- Betrug/Abuse-Prevention und Aufklärung von Straftaten.
- Patientensicherheit (z.B. bessere Medikationsinfos, Notfallkontext).
- Aber: “Mehr Daten = mehr Sicherheit” ist oft ein Trugschluss – zusätzliche Daten erhöhen auch Angriffsfläche und Profiling-Macht.

4) Warum brauchen wir Privatsphäre überhaupt?

- Autonomie: Entscheidungen ohne unsichtbaren Druck (sozial, ökonomisch, institutionell).
- Würde & Intimität: Schutz sensibler Lebensbereiche (Körper, Beziehungen, Gesundheit).
- Fairness: Schutz vor Diskriminierung, Risiko-Scoring, Preis-/Job-Profilung.
- Sicherheit: weniger Angriffsfläche für Erpressung und Social Engineering.
- Informationelle Selbstbestimmung: Idee, dass Menschen über Preisgabe/Verwendung ihrer Daten mitbestimmen können.

“BIOLOGICAL KNOWLEDGE MULTIPLIED BY COMPUTING POWER MULTIPLIED BY DATA EQUALS THE ABILITY TO HACK HUMANS.”

– YUVAL NOAH HARARI (WEF, DAVOS 2020)

5) Kollisionsbeispiele

- E-Mail-Konto: Anonymität vs. Account-Recovery/Verfügbarkeit (Backup-Codes, Identitätschecks, Wiederherstellung).
- ePA: schnelle Hilfe/Behandlungssicherheit vs. sensibler Missbrauch (Fehlzugriff, Stigma, Erpressung).
- Abwägungsfragen: Welche Bedrohung ist wahrscheinlicher? Wer hat Macht? Wie gut sind Kontrolle und Audit?

6) KI-Agenten: Was ändert sich qualitativ?

- Agenten haben Zugriffe (Files, Shell, Accounts) und können Aktionen ausführen – nicht nur texten.
- Persistenz: sie laufen “nebenbei” und werden über Tools/Skills erweitert.
- Risiken: Prompt-Injection, untrusted Skills/Plugins, Fehlkonfiguration, zu breite Berechtigungen.
- Fallbeispiel Moltbook: Sicherheitsloch machte u.a. private Agent-Nachrichten, Owner-E-Mails und massenhaft Zugangstokens/“Credentials” zugänglich (siehe Reuters-Hinweis unten).

7) Prediction Markets: Kalshi & Polymarket

- Märkte handeln “Event Contracts” auf Real-World-Outcomes (Politik, Wetter, Popkultur, Wirtschaft).
- Risiko: Insider-Information wird direkt monetarisierbar; ab bestimmter Größe entsteht auch Anreiz zur Manipulation.
- Aktueller Hinweis (Feb 2026): Anklage wegen Nutzung klassifizierter Militärintformationen für Polymarket-Wetten (siehe AP-Hinweis unten).

8) These & Leitfragen

Neue Dimension der Verknüpfung und Verarbeitung von Daten durch KI

+ aktive Befähigung von Agenten

+ Prediction Markets (Information wird direkt monetarisierbar)

= neue Risikolage.

- Welche Datensammlung ist schützender Mehrwert – und wo kippt sie in Manipulation/Profiling?
- Welche Mindeststandards brauchen Agenten (Berechtigungen, Secrets, Logging, Updates, Isolation)?
- Welche Märkte/Fragetypen sind “No-Go” (besonders insider-anfällig oder manipulierbar)?
- Welche Governance: Minimierung, Kontrolle, Audit – oder Verbote bestimmter Märkte?

Quellen

- Harari, Y. N. (2020): Davos-Rede, World Economic Forum.
- Reuters (02.02.2026): Bericht zu Moltbook-Sicherheitsloch (Wiz).
- Associated Press (02/2026): Anklage zu Polymarket-Wetten mit klassifizierten Infos.
- BVerfG (1983): Volkszählungsurteil / informationelle Selbstbestimmung.
- BMG: Informationen zur ePA.