



id: SI_001

model: google/gemma-4-26b-a4b-it

seeds:

04_risiko: sårbarhet

03_relasjon: makt

05_handling: implementer

01_perspektiv: strategisk

02_tidhorisont: langsiktig

Instans SI_001

Seeds: strategisk | langsiktig | makt | sårbarhet | implementer

Diagnose: Den asymmetriske risiko-paradokset

Motstanden er ikke teknologisk uvitenhet, men en **strategisk feilberegning av sårbarhet**. Juridiske profesjonelle opererer i et system der mikro-effektivitet (å få svar fra ChatGPT nå) trumfer makro-eksponering (potensiell taushetsbrudd om to år).

1. Gapet: Bevissthet vs. makt Gapet ligger i at risikoen er abstrakt og kollektiv, mens gevinsten er konkret og individuell. Bruken av åpne LLM-er er en “skjult subsidie” til de store teknologigigantene; advokaten bytter bort klientens data-suverenitet mot personlig tidsbesparelse. De vet om risikoen, men de har ikke følt maktforskyvningen ennå.

2. Tillit og teknisk determinisme De stoler ikke på “blind compute” fordi de ikke forstår kontrollmekanismer. For en jurist er “sikkerhet” ikke en teknisk spesifikasjon, men et juridisk ansvarsfraskrivelses-dokument. De krever ikke bare teknisk isolasjon, men en garanti som kan fremlegges i en disiplinærsak.

3. Drivere: Skiftet fra “valgfritt” til “tvingende” Adopsjon skjer ikke via opplysning, men via **eksternt press på maktstrukturer**:

- **Klient-mandater:** Når de største klientene (Equinor, Statnett, store banker) krever revisjon av KI-verktøy i tjenesteleverandør-avtaler.
- **Forsikrings-eksperimentet:** Når ansvarsforsikringen (f.eks. via Advokatforeningen/gjensidige ordninger) ekskluderer datalekkasjer som skyldes “uautorisert bruk av tredjeparts LLM-er”.



4. Sosiale barrierer og “The Race to the Bottom” Det eksisterer en frykt for å tape konkurransekraft ved å implementere “tunge” løsninger. Hvis konkurrenten bruker en usikker, men lynrask modell, føles SikkerKI som en strategisk brems.

Skarpe dilemmaer

- **Hastighet vs. Vern:** Er det etisk forsvarlig å nekte en junioradvokat et effektivt verktøy for å beskytte data, hvis det gjør at firmaet taper anbud på pris?
- **Kontroll vs. Kapasitet:** On-premise gir kontroll, men ofrer de nyeste modellene som krever enorme GPU-ressurser?

Implementerbare angrepsvinkler

1. **Flytt fokus fra “Sikkerhet” til “Forsikringsbarhet”:** Ikke selg datavern; selg eliminering av profesjonsansvar.
2. **Angrip klient-leddet:** Ikke selg til advokaten, selg til klientens innkjøpsavdeling som et “Compliance-sertifikat” for deres eksterne juridiske bistand.

Neste steg:

- Utvikle et “Risk Exposure Matrix”-verktøy som kvantifiserer økonomisk risiko ved bruk av åpne LLM-er mot norske advokatregler.
- Sikre partnerskap med forsikringsaktører for å definere “standard for forsvarlig KI-bruk”.