



id: SI\_003

model: mistralai/mistral-large-2512

seeds:

04\_risiko: sårbarhet

03\_relasjon: makt

05\_handling: utforsk

01\_perspektiv: strategisk

02\_tidhorisont: kortsiktig

## Instans SI\_003

### Analyse: Adopsjonsbarrierer for SikkerKI i norsk juridisk sektor

**Strategisk blindspot:** Juridiske profesjonelle opererer i et **kortsiktig maktparadigme** – de prioriterer umiddelbar effektivitet (ChatGPT nå) over langsiktig risikokontroll (SikkerKI senere). Dette er ikke uvitenhet, men en **bevisst maktutøvelse**: De velger å ignorere sårbarheten fordi konsekvensene (Datatilsynet, klientkrav) fremstår som teoretiske eller fjerne. **Sårbarheten** blir dermed en strategisk ressurs – de utnytter den asymmetriske informasjonen (klienten vet ikke at data lekker) til å opprettholde konkurransefortrinn.

### Psykologisk motstand:

1. **Tillitens paradoks:** De stoler mer på usikre løsninger (ChatGPT) fordi de kjenner risikoen der – den er abstrakt, mens SikkerKIs “blind compute” fremstår som en ukjent sårbarhet. “Hva om on-premise-løsningen likevel lekker?” er en frykt som ikke lar seg falsifisere.
2. **Sosial norm som brems:** Bransjen har en **kollektiv blindhet** – ingen vil være first-mover fordi det bryter med den uuttalte normen om “risikofri nonchalance”. Å adoptere SikkerKI blir en strategisk svakhet: “Hvorfor bruke penger på noe konkurrentene ikke gjør?”

**Regulatorisk illusjon:** Datatilsynet er en **papirtiger** i juridisk sektor. Advokater tolker GDPR gjennom sin profesjonelle makt – de antar at taushetsplikten overstyrer personvernlovgivning (“Vi er advokater, vi vet hva vi gjør”). **Sårbarheten** her er at Datatilsynet mangler konkrete eksempler på sanksjoner mot juridiske aktører – dermed blir regulatorisk press en teoretisk trussel, ikke en drivkraft.

### Leverage-punkter (hvor makten kan utfordres):

1. **Klientdrevet press:** Når store klienter (f.eks. statlige etater, forsikringsselskaper) eksplisitt krever SikkerKI i kontrakter, vil advokatfirmaer



bytte umiddelbart – ikke av etikk, men av **økonomisk makt**. (Eksempel: DNBS krav til leverandører om ISO 27001.)

2. **Forsikringskrav:** Når profesjonsansvarsforsikringer nekter å dekke datalekkasjer fra usikre KI-verktøy, blir sårbarheten plutselig kostnadsberegnet. (Eksempel: Hvordan cyberforsikring endret adferd i finanssektoren.)
3. **Brudd på kollektiv blindhet:** En høystatusaktør (f.eks. BAHR, Thommessen) som offentlig adopterer SikkerKI vil skape en **normkollaps** – konkurrenter må følge for å unngå å fremstå som uansvarlige.

### Konkrete neste steg:

1. **Pilot med en motvillig klient:** Identifiser et advokatfirma som bruker ChatGPT på klientsensitive saker, og få klienten til å kreve SikkerKI som betingelse for videre samarbeid. Dokumenter prosessen som case.
2. **Forsikringshack:** Samarbeid med forsikringsselskaper (f.eks. Gjensidige, If) for å utforme et tillegg til profesjonsansvarsforsikringen som eksplisitt utelukker dekning for datalekkasjer fra usikre KI-verktøy.
3. **Normbryterkampanje:** Få en kontroversiell aktør (f.eks. en “legal tech”-advokat) til å offentlig erklære at de kun bruker SikkerKI – og utfordre bransjen til å følge etter. Målet er å gjøre sikkerhet til en statusmarkør, ikke en byrde.

**Dissens:** Adopsjonsbarrieren handler ikke om teknologi eller pris, men om **makt og sårbarhetens strategiske verdi**. Løsningen ligger ikke i å overbevise advokater om at SikkerKI er trygt, men i å endre maktbalansen slik at det blir farligere å ikke bytte.