



id: SI_009

model: anthropic/claude-opus-4.6

seeds:

04_risiko: sårbarhet

03_relasjon: samarbeid

05_handling: vent

01_perspektiv: operasjonell

02_tidhorisont: langsiktig

Instans SI_009

Seeds: operasjonell | langsiktig | samarbeid | sårbarhet | vent

Kjerneanalyse: Vent — men strategisk

Min mest kontraintuitive innsikt: **den lave adopsjonen er delvis rasjonell, og å forstå ventelogikken er nøkkelen til å bryte den.**

Hvorfor «vent» er den dominerende strategien

Norske advokater opererer i et regime der **sårbarhet er asymmetrisk**: å bli tatt for å bruke usikker KI har (per i dag) lav sannsynlighet for sanksjon, mens å investere i SikkerKI har umiddelbar, synlig kostnad. Datatilsynet har ikke felt en eneste norsk advokatpraksis for KI-relaterte taushetspliktsbrudd. Tilsynsorganet er underfinansiert og reaktivt. Advokatforeningen har gitt veiledning, ikke pålegg. I dette vakuumet er «vent og se» operasjonelt rasjonelt — ikke uansvarlig, men kalkulert.

Den operasjonelle sårbarhetens blindsoner

Det juridiske profesjonelle ikke ser: **de har allerede eksponert seg.** Hver prompt med klientfakta til OpenAI er et potensielt taushetspliktsbrudd under advokatforskriften § 3-13. Men bruddets karakter er usynlig — ingen klient vet, ingen tilsynsmyndighet sjekker. Sårbarheten er reell, men opplevelsen av den er null. Dette er kjerneproblemet: **operasjonell risiko uten operasjonell smerte.**



Samarbeid som den manglende mekanismen

Individuelle firmaer vil ikke være first-mover. Leverage-punktet er **kollektiv bevegelse**: Når Advokatforeningen, Tilsynsrådet eller de fem største firmaene etablerer en felles norm, kollapser ventelogikken. Samarbeid er ikke bare strategi — det er den eneste realistiske adopsjonsvektoren i en bransje der konformitet er profesjonskultur.

Det langsiktige dilemmaet — et ekte trade-off

Her er det skarpe dilemmaet: **SikkerKI-tilbydere trenger adopsjonsvolum for å oppnå feature-paritet med OpenAI/Anthropic, men firmaer venter på feature-paritet før de adopterer.** Norsk on-premise compute vil i overskuelig fremtid ligge bak frontier-modellene i kapabilitet. Advokater som bruker GPT-4o daglig vil oppleve SikkerKI som en nedgradering. Dette er ikke irrasjonelt — det er et reelt operasjonelt tap.

Hva ville faktisk utløse endring

1. **Datatilsynet gjennomfører et konkret tilsyn** mot et advokatfirma for KI-bruk — selv uten bot ville signaleffekten være enorm
2. **En stor klient** (Equinor, staten, en bank) stiller eksplisitte KI-sikkerhetskrav i engasjementsbrev
3. **Forsikringsselskapene** begynner å spørre om KI-bruk i profesjonsansvarsforsikringen

Ingen av disse krever at SikkerKI selger bedre. De krever at **omgivelsene gjør «vent» til en dyrere strategi enn «bytt».**

Tre konkrete neste steg

1. **Facilitér et samarbeidsforum** mellom Advokatforeningen og 3–5 mellomstore firmaer for å utvikle en felles «KI-databehandlingsstandard» — gjør normen synlig før produktet selges
2. **Produsér en konkret sårbarhetsdemo**: vis et advokatfirma nøyaktig hva som skjer med en prompt sendt til OpenAI API — teknisk, juridisk, kontraktsmessig — og la dem føle eksponeringen
3. **Ikke press på umiddelbar konvertering — tilby en parallellkjøringsmodell**: la firmaer kjøre SikkerKI ved siden av eksisterende verktøy for sensitive saker, og bygg operasjonell tillit over tid. Respektér ventelogikken, men gjør ventetiden produktiv.