



id: SI_005

model: anthropic/claude-haiku-4-5

seeds:

04_risiko: sårbarhet

03_relasjon: avhengighet

05_handling: forhandle

01_perspektiv: juridisk

02_tidhorisont: langsiktig

Instans SI_005

Seeds: juridisk | langsiktig | avhengighet | sårbarhet | forhandle

Analysen

Du står foran en **avhengighetsfelle** som de færreste ser. Systemet du bygger — automatisert innsugning av kilder til en personlig KB — er elegant, men det skaper langvarig avhengighet av dine egne agenter. Hvis du ikke dokumenterer hvordan de velger kilder, blir du låst til deres beslutninger.

Juridisk perspektiv første: OpenRouter-nøkkelen din er et svakt punkt. Hvis du sentraliserer all innsugning gjennom den, hvem eier dataene som genereres? Hvis OpenRouter endrer vilkår eller blir utilgjengelig, krasjer systemet. Du må ha en **lokal fallback-modell** (Llama 2, Mistral lokalt) for kritiske oppgaver. Det er ikke overkill — det er forsikring.

Sårbarhet: Dine 100+ instanser som skal finne kilder — de kan bli dårlige kilder-detektorer. Twitter-algoritmen favoriserer engagement, ikke nøyaktighet. YouTube-anbefalinger er optimalisert for watch-time. Du må bygge inn **eksplisitt**

kvalitetskontroll: Hvem verifiserer før noe kommer inn i KB? En agent som bare aggregere, er en agent som forsterker bias.

Langsiktig: Det du egentlig trenger er ikke en web-side, men en **editorial policy** som agentene følger. Definer: Hvilke kilder teller? Hva er minimum-evidens før noe blir "knowledge"? Dette må være menneske-drevet, ikke agent-drevet.

Forhandling: Hvis du skal skalere dette, må du forhandle med kilder direkte. Kontakt 10-15 relevante X-kontoer og få RSS-feeds eller API-tilgang. Det er manuelt, men det gir deg kontroll og etablerer relasjoner. Agentene blir da kuratorer, ikke jegere.



Konkrete neste steg

1. **Denne uken:** Definer 5 “tier-1”-kilder (mennesker/organisasjoner du absolutt vil følge). Lag en manuell OPML-fil med deres RSS. Test én agent som bare leser disse først — ikke hele Twitter.
2. **Denne måneden:** Bygg lokal fallback med Ollama + Mistral. Ikke for produksjon, men for når OpenRouter faller bort. Tegn arkitektur: Hvor flyter data? Hvem eier det?
3. **Neste kvartal:** Lag editorial workflow hvor du godkjenner nye kilder før agenter bruker dem. En enkel “source approval” step før KB-innsugning. Det er manuelt arbeid, men det gir deg kontroll over avhengigheten du skaper.

Dissens: Du trenger ikke flere agenter. Du trenger færre, bedre kilder og ett human checkpoint.