AI Supply Chain

ai-supply-chain · safety · concept

Source: https://policywindow.org/wiki/ai-supply-chain

Generated 2026-07-09T20:40:39 UTC

Summary

The end-to-end pipeline of inputs, intermediate artefacts, and downstream applications by which an AI system is built and deployed — typically decomposed as training data ’ compute ’ model weights ’ fine-tuning ’ deployment ’ downstream applications.

At a glance

Used by

3 instrument(s)

Related concepts

compute-threshold, training-data-attribution, model-card, model-distillation-risk, data-poisoning

Primary source

NIST AI 600-1 (Jul 2024), 'AI Risk Management Framework: Generative AI Profile' — names 'Value Chain and Component Integration' as a primary risk category.

Details

The AI supply-chain framing treats AI development as an industrial value chain in which each upstream stage constrains what the downstream stage can do, and each stage raises distinct governance questions. Training data raises copyright, consent, and bias questions (NYT v. OpenAI, GEMA v. OpenAI, Andersen v. Stability AI). Compute raises export-control and concentration questions (US BIS rules on advanced GPUs to China, the CHIPS Act, the 2024 EU Chips Act). Model weights raise open-vs-closed governance questions (Meta Llama, Mistral, DeepSeek vs. closed frontier labs). Fine-tuning raises capability-elicitation questions (Qi et al. 2023 'Fine-tuning Aligned LLMs Compromises Safety'). Deployment raises monitoring and incident-reporting questions. Downstream applications raise sectoral-liability questions (medical-device AI, automated decision-making in employment).

Governance treatment is fragmented across the chain. EU AI Act Recital 60 + Art. 25 introduces explicit value-chain obligations: the GPAI provider and the downstream deployer have different obligations, and contracts must allocate them. US EO 14110 §4.2 targeted the compute stage (Defense Production Act reporting for foundation-model training above the threshold). NIST AI RMF GenAI Profile (NIST AI 600-1, 2024) names 'Value Chain and Component Integration' as one of twelve GenAI risk categories. ASEAN AI Guide §3 treats the supply chain as a 'shared responsibility' across actors. The supply-chain framing is increasingly the unit of governance analysis because chokepoints (compute access, training-data legality, weight distribution) determine where policy levers have purchase.

How to cite this article

APA

Policy Window. (n.d.). AI Supply Chain [Wiki article — Concept]. https://policywindow.org/wiki/ai-supply-chain

CHICAGO

Policy Window. n.d.. "AI Supply Chain." Wiki article (Concept). https://policywindow.org/wiki/ai-supply-chain.

HARVARD

Policy Window (n.d.) 'AI Supply Chain', Wiki article — Concept, available at: https://policywindow.org/wiki/ai-supply-chain.

OSCOLA

Policy Window, 'AI Supply Chain' (Wiki article — Concept, n.d.) <https://policywindow.org/wiki/ai-supply-chain> accessed [date].

BIBTEX

```
@misc{policywindow-ai-supply-chain,
title  = {AI Supply Chain},
author = {Policy Window},
year   = {n.d.},
howpublished = {ai-supply-chain — safety},
url    = {https://policywindow.org/wiki/ai-supply-chain},
note   = {Primary source: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf}
}
```