

Supplementary Material B

Replication codebook for Human in the Log

Tyche Institute

17 June 2026

Purpose

This codebook defines the public-evidence fields used for the article “Human in the Log: Public Evidence Chains for Public-Sector AI Oversight.” It is intended to make the case-synthesis method reproducible without publishing internal working paths or overclaiming from heterogeneous source records.

Unit of Analysis

The coding unit is a public evidence function, not an “AI incident.” A single case can therefore support several coded functions, and a single coded function can remain narrow even when the underlying controversy is large.

Example: Robodebt is coded for assumptions, notice, review paths, publication of business rules or algorithms, and repair architecture. It is not coded as a machine-learning case unless a source independently supports that technical claim.

Source Classes

Surface	Article-facing use	Denominator
LIMEN	Boundary cases with legal, regulator, audit, civil-society, media, and security source routes.	LIMEN public atlas rows only; not a global prevalence denominator.
GAIA	Public-agent and public-system visibility rows.	Validated global record rows and structured facts; not harm findings.
PALLAS-adjacent layers	Country-route and source-context anchors.	Route and context support; not full legal review.
Public-sector bundles	Source-preserved case studies, timelines, and evidence trails.	Selected case bundles; not all public-sector AI systems.
Register/procurement bridges	Visibility chains across registers, procurement, vendor, and public-service records.	Disclosure and procurement traces; not deployment or compliance proof.

Surface	Article-facing use	Denominator
Standards-to-evidence bridges	Mappings from legal or governance duties to evidence carriers.	Normative mapping; not evidence of field compliance.

Core Fields

Field	Description	Required for article use
case_id	Stable internal or public row identifier.	Yes for deposit.
case_label	Short public name used in prose or matrix.	Yes.
jurisdiction	Country, region, court, regulator, or authority.	Yes.
region	Regional grouping used only for navigation.	Yes for supplement.
system_family	Generative AI, scoring, data matching, biometric, chatbot, routing, source-code eligibility, or other.	Yes.
authority_or_source_type	Court, regulator, audit, commission, official service page, procurement notice, vendor page, media, civil society, or CVE/security.	Yes.
evidence_tier	T3, T2, media/civil-society, CVE/security, GAIA visibility, register/procurement, or standards bridge.	Yes.
posture_finality	Final, appeal-pending, interim, guidance, audit, inquiry, visibility-only, or unknown.	Yes.
date_or_range	Decision, publication, audit, procurement, or service-publication date.	Yes when available.
source_surface	Observatory, article ledger, public-agent visibility row, or source-preserved bundle from which the row was harvested.	Yes.
source_row_ids	Original row IDs, aliases, or source-bundle IDs preserved for duplicate control.	Yes.
duplicate_cluster_id	Cluster identifier for related but non-identical rows, such as Clearview national decisions or Dutch tax-administration rows.	Yes.
duplicate_relation	Whether the row is canonical, a cluster member, an alias route, or a visibility row.	Yes.

Field	Description	Required for article use
source_url_or_neutral_citation	Stable public link, neutral legal citation, or source-route note.	Yes for public deposit; source-route gaps must be flagged.
source_access_date	Date on which the public source route was last checked for the article package.	Yes for public URLs.
source_language	Original source language.	Yes for non-English rows.
translation_gate	Whether legal-sensitive or quote-heavy use requires human translation review.	Yes for non-English rows.
evidence_function	Sequence, notice, transparency layer, human capacity, public visibility, retention, repair, rights response, or professional verification.	Yes.
record_part	Entry point, input/output, human view, human act, reasons, contest path, or retention and repair.	Yes.
strongest_supportable_claim	Strongest claim the source posture can support.	Yes.
excluded_claim	Claim the row must not be used to support.	Yes.
privacy_or_sealing_note	Anonymization, sealed material, sensitive data, or privileged-material constraint.	Yes where applicable.
article_use	Main text, supplementary matrix, excluded, or source-discovery only.	Yes.
public_source_status	Whether the public URL is present, inherited from the article ledger, source-limited, or not preserved in the export.	Yes.

Evidence-Tier Rules

T3 rows can support what a court, regulator, audit body, royal commission, or equivalent public authority recorded, held, ordered, settled, or reviewed. They do not support prevalence, technical efficacy, or cross-sector legality unless the source itself makes that claim.

T2 rows can support procedural posture, allegations, interim measures, appeal-pending issues, regulator-process steps, and issue spotting. They do not support final liability or settled fact claims.

Media and civil-society rows can support public visibility, controversy, investigation routes, and source discovery. They do not substitute for legal findings.

CVE and security rows can support public vulnerability, affected-version, notice, and fix-visibility claims. They do not support realized harm or exploitation unless separately evidenced.

GAIA visibility rows can show that a system, service, or agent is publicly described through official, provider, audit, or independent records. They do not prove harm, safety, deployment completeness, legality, or effective oversight.

Register and procurement rows can show disclosure or buyer-side visibility. They do not prove operational deployment, procurement completeness, or legal compliance.

Inclusion Rules

A row may enter the main article only if it supports one of the article’s evidence functions and has a source posture compatible with the claim made in prose.

A row may enter Supplementary Material A if it broadens geography, technology class, legal posture, or evidence function and can be described without stronger legal or factual claims than the source supports.

A row remains excluded or source-discovery-only if it lacks a public source route, has unresolved identity or date conflicts, requires legal interpretation not yet reviewed, or cannot be assigned a clear evidence function.

Review Gates

1. Source identity: title, authority, date, jurisdiction, docket, and URL are checked against the public record where possible.
2. Posture: finality, appeal status, interim status, audit status, or visibility-only status is recorded before prose use.
3. Claim ceiling: strongest supportable claim and excluded claim are coded together.
4. Non-English sources: legal-sensitive claims remain caveated until human translation or local-law review supports stronger use.
5. Privacy and confidentiality: anonymization in official sources is preserved; prompts, case files, and personal data are not reproduced unless legally and ethically appropriate.
6. Duplicate control: source row ID, country, case name, authority, date, and URL or neutral citation are checked for false merges before rows are counted or compared. Related records are assigned a `duplicate_cluster_id` rather than collapsed into one row when the legal posture or source function differs.

Public Package Contents

The public article package includes:

- the article-facing matrix from Supplementary Material A;
- this codebook;
- a machine-readable 315-row case table with the core fields above as Supplementary Material C;
- stable public-source URLs or neutral legal citations;
- source-access dates where URLs are unstable;
- source-rights notes for any local copies or screenshots;
- language and translation-gate flags;
- claim-ceiling and excluded-claim fields;
- duplicate/cluster fields showing which aliases or related records were kept separate;
- a short changelog for corrections after peer review, if the public repository is updated.

The public package should not include internal-only vault paths, copyrighted full-text copies unless redistribution is permitted, private personal data, sealed records, privileged material, or confidential prompts.