Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Legal Status of the AI-Transparency Duties at the Consumer-Facing Interface

Maxim Osovsky

maximosovsky@adam.edu.kg

Adam University https://orcid.org/0009-0004-1594-0940

Ekaterina Krikunova

Luiss University https://orcid.org/0009-0001-8006-7082

Ruth Shonubi

University of Lagos https://orcid.org/0009-0007-3379-4205

Research Article

Keywords: AI transparency, AI disclosure, synthetic content labelling, comparative law, consumer-facing interface, visible compliance, AI governance

Posted Date: September 30th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11168215/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: The authors declare no competing interests.

Abstract

Background

AI regulation now attaches transparency duties to the user interface, including disclosure of AI interaction, labelling of AI-generated content, notices for high-risk AI systems, companion-chatbot safeguards, and publication of governance information. Because these obligations arise across different doctrinal fields and jurisdictions, ordinary legal categories do not compare them well.

Methods

The study is a structured qualitative comparative legal analysis of eleven jurisdictions: the European Union, United States, China, United Kingdom, Canada, Japan, Republic of Korea, Singapore, Australia, Brazil, and the United Arab Emirates. Each jurisdiction was treated as a qualitative case and classified across five predefined visible-transparency variables and by legal status using explicit decision rules. The corpus comprises publicly available statutes, regulations, regulator guidance, governmental policy documents, and official legislative-status records.

Results

The identified duties form a four-level analytical typology: user-facing AI disclosure, synthetic-content labelling, public-facing notices for high-risk or high-impact systems, and externally inspectable organisational or technical transparency. The clearest binding examples in the source corpus appear in the European Union, China, and the Republic of Korea. The United States relies on federal consumer-protection enforcement and state-level statutes. Canada, Brazil, Australia, Singapore, and the United Arab Emirates show different combinations of proposed legislation, soft-law governance, sectoral rules, and data-protection-based duties.

Conclusions

In the eleven jurisdictions studied, AI-transparency regulation shows partial convergence in recurring techniques, especially disclosure, labelling, notice, and public-facing governance information. Developers and operators of cross-border AI services must manage these techniques across jurisdictions with different legal force. The interface provides a useful comparative lens for analysing AI-transparency regulation.

1. Introduction

The emergence of widely available generative AI services has changed the legal significance of the consumer-facing interface. A website or application interface now does more than communicate terms of service, privacy notices, or general product information. In AI-enabled services, the same interface may carry multiple transparency duties that were previously analysed across separate doctrinal categories [1]–[4].

Visible AI transparency comprises duties that make AI-related legal information observable at the consumer-facing interface. It includes disclosure, labelling, high-risk or high-impact notices, and companion-chatbot safeguards. The analysis also covers closely related organisational and technical artefacts when they are publicly available or open to regulatory inspection. These adjacent artefacts remain distinct from the consumer-facing interface itself. The term is an analytical refinement of conventional AI-transparency vocabulary, not an established doctrinal category.

The research question is: **which recurring AI-transparency techniques become visible at the interface across the jurisdictions studied, and how does their legal force differ?** A separate theoretical question asks how the resulting interface-level pattern may be interpreted through the concept of human-machine systems.

This article uses the consumer-facing interface and the adjacent category of externally inspectable transparency as an analytical lens for identifying AI-transparency duties across jurisdictions with different legal instruments, doctrinal categories, and enforcement models.

The article contributes a four-level analytical typology and a coded comparison of eleven jurisdictions as of August 2026. The comparison identifies recurring interface-level techniques despite differences in doctrine and legal force.

A further conceptual premise is that AI-mediated activity is designed human activity organised through human-machine systems. Large language models, chatbots, and generative applications operate within human purposes, institutional roles, business processes, interfaces, and chains of responsibility. Shchedrovitskiy frames the issue in operational terms: once an activity has been given a normative description, some of its functions may be transferred to a machine; if the structure of the operation is known, “what difference does it make who performs it: a machine or a human?” [5].

The relevant legal object is therefore a human-machine configuration in which human intention, machine operation, interface design, organisational workflow, and legal consequences are joined. The term *centaur system* refers here to this heterogeneous allocation of functions across human and machine components [6].

The analysis focuses on duties visible at the interface; the fuller legal construction of human-machine systems lies beyond its scope. Different technical layers distribute functions differently across the system and may therefore require different forms of transparency.

2. Background and literature positioning

This study responds to the classic "Law of the Horse" objection — raised by Easterbrook (1996) as a critique of treating every technology as a separate legal domain and answered by Lessig (1999) — by avoiding the claim that every technology needs a separate legal branch [7]–[8]. The object of regulation is the human-machine system through which AI-mediated activity is organised. The object of this comparative analysis is narrower: the consumer-facing interface as the legally observable surface on which that system performs disclosure, warning, explanation, labelling, visible governance, and attribution.

This approach also avoids a second risk: treating "AI" as a single, uniform object of regulation. In the vocabulary of system-thought-activity methodology, Shchedrovitskiy's account of operationalised activity supports the view that legal analysis should begin from organised human-machine activity rather than from an isolated technical artefact [5]. For AI transparency, this means examining how a model, user, deployer, interface, institutional purpose, and responsibility structure are connected.

AI services are delivered through diverse technical architectures — foundation models, fine-tuned systems, retrieval-augmented pipelines, autonomous agents, embedded models, and API layers — that distribute functions differently across human-machine configurations [16]–[21]. A single service may combine multiple LLMs supplied by different providers, released at different times, and offering different levels of capability, context-window sizes, and suitability for particular tasks. Each model may perform a distinct function, such as generation, retrieval, classification, moderation, speech recognition, or image analysis. The configuration may also include different safety and alignment layers, specialised skills, system and task-specific prompts, and Model Context Protocol (MCP) servers that connect models to external tools, data sources, and actions. The legally relevant system therefore includes not only the individual models but also the organisation that selects and updates them, combines their outputs, allocates tasks among them, configures safety layers, skills, prompts, and external tool access, supplies data and instructions, and presents the resulting service to the user. These differences may call for different transparency requirements. A uniform disclosure can be overbroad for low-risk systems while failing to identify the model, provider, functional layer, or external integration that generates a legally material risk. The interface provides a common point at which those distinctions can become observable.

Wider sociotechnical and accountability scholarship supports this view. Selbst et al. show that algorithmic-fairness analysis fails when technical systems are abstracted from their social settings [9]. Suchman likewise treats machine action as intelligible only within situated human practices [10]–[11]. Bainbridge's "ironies of automation" and Elish's "moral crumple zone" identify a related institutional risk: nominal human involvement may preserve formal responsibility while weakening actual control [12]–[13]. Work on meaningful human control and responsibility gaps reaches the same narrower conclusion: responsibility depends on how functions and control are distributed across the configured system [14]–[21].

Scholarship on algorithmic accountability has shown that formal transparency and real accountability are distinct legal problems. Citron and Pasquale describe the risk of a scored society and the need for procedural safeguards around automated predictions [22]. Kroll et al. develop the idea of accountable algorithms [23].

A related data-protection debate narrows the same problem to explanation, meaningful information, and contestability. Wachter, Mittelstadt and Floridi question whether the GDPR contains a general right to explanation for automated decision-making [24]. Selbst and Powles argue that meaningful information must be connected to the institutional conditions under which affected persons can understand and challenge automated decisions [25]. Edwards and Veale caution that explanation alone may be an inadequate remedy for algorithmic decision-making [26], while Kaminski treats the right to explanation as a structured governance problem rather than a simple disclosure duty [27]. Selbst and Barocas similarly show that intuitive demands for explainability can obscure the social and technical limits of explanation [28].

Broader transparency and opacity scholarship explains why disclosure remains incomplete without institutional accountability. Ananny and Crawford criticise transparency as insufficient without institutional accountability [29]. Burrell identifies distinct sources of opacity in machine-learning systems [30]. Mittelstadt et al. systematise ethical problems associated with algorithmic systems [31].

Algorithmic-regulation literature explains why these duties travel across jurisdictions in uneven ways. Yeung analyses regulation through design in her account of "hypernudging," while Ulbricht and Yeung analyse algorithmic regulation as a maturing regulatory mode [32]–[33]. Interface scholarship adds the next step: disclosure depends on design. Calo analyses digital market manipulation [34]. Susser, Roessler and Nissenbaum connect technological manipulation to autonomy [35]. Gray et al. and Mathur et al. show how dark patterns operate through interface design [36]–[37]. These studies demonstrate that the interface actively shapes how legal information reaches the user. It can inform, obscure, steer, delay, or distort user choice.

Governance and regulatory-diffusion literature supplies the comparative layer. Gasser and Almeida propose a layered model for AI governance [38]. Bradford explains how major regulatory regimes can produce transnational effects [39]–[40]. Veale and Zuiderveen Borgesius analyse the European Commission's 2021 draft AI Act as a proposed risk-based regulatory framework [41].

Prior comparative work has addressed AI transparency in particular legal systems and sectors. Recent work on AI-generated-content labelling shows that similar transparency vocabularies can produce different legal-technical infrastructures in China and under Article 50 of the EU AI Act [42]. EU-UK work has reviewed AI-transparency law through a socio-legal lens [43], while sector-specific studies of medical AI and consumer-facing FinTech have examined meaningful transparency, explainability, trust, and disclosure [44]–[45]. Broader comparisons cover regulatory models in the European Union, China, and the United States [46]; a topic-first comparative project maps content-labelling and provenance rules across those three jurisdictions [47]; interface-design scholarship examines how disclosure, explanation, and control choices acquire legal consequences [48]; and practitioner analysis compares the overlapping legal regimes applicable to AI chatbots [49]. Building on this literature, the present study offers a distinct synthesis: it codes five forms of visible AI transparency across eleven jurisdictional regimes, distinguishes their legal status, and uses the consumer-facing interface as a common comparative lens.

3. Methods

3.1 Study design

This article is a structured comparative legal study with five pre-defined visible-transparency variables coded across eleven jurisdictions. It distinguishes enacted law, enforcement practice, proposed legislation, and voluntary standards. The study maps legal design rather than actual interface implementation. A secondary theoretical framework interprets the interface through the concept of human-machine systems; the comparative coding does not test that framework.

Generative AI tools were used for technical drafting support, language editing, organisational assistance, and initial source-discovery support. Every source and legal-status claim was independently checked by the authors against the cited legal or official material. Generative AI was not used as an author or as the final decision-maker for legal-status classification or interpretation. The authors revised the argument and accept responsibility for the final text.

3.2 Unit of comparison

The unit of comparison was the jurisdictional legal and regulatory regime; the interface was the analytical lens through which duties within each regime were selected and compared. Each cited source was reviewed as evidence for whether that regime created or recommended an obligation visible at the interface. The coding records whether each jurisdiction contains binding, proposed, sector-specific, enforcement-based, or recommended transparency duties observable by users, regulators, or counterparties at the interface level.

Tables 1 and 2 and the supplementary CSV file present the resulting jurisdiction-level classifications. The CSV provides one column for each of the five coding variables defined in Section 3.6. These materials are comparative legal summaries. The cited primary and official materials identify the evidentiary basis for each classification.

3.3 Jurisdiction selection

Eleven jurisdictions were selected because they represent major regulatory approaches to AI governance and digital-service regulation: the European Union, United States, China, United Kingdom, Canada, Japan, Republic of Korea, Singapore, Australia, Brazil, and the United Arab Emirates. The selection was based on four criteria: regulatory salience, geographic diversity, relevance to cross-border digital services, and availability of public official sources capable of supporting legal-status verification.

The selection was purposive rather than exhaustive. It was designed to compare prominent horizontal, federal or subnational, data-protection-based, statutory-governance, proposed-law, and soft-law approaches across several regions. This design deliberately increases regulatory diversity and therefore cannot independently demonstrate the global prevalence of fragmentation. The findings establish the presence of recurring techniques within the selected jurisdictions but do not support estimates about their prevalence worldwide.

3.4 Source selection and legal-status verification

The analysis included primary legal instruments, official regulator guidance, governmental policy documents, and official legislative-status records. Academic literature contextualised the analysis but did not serve as primary evidence of legal status. The study preferred official sources to commercial legal summaries. Uncertain instruments were coded as proposed, pending, soft law, or not yet generally applicable rather than as binding law.

The source search ran from June through August 2026, followed by a final verification pass on 27 August 2026. It covered EUR-Lex; United States federal and state legislative and regulator pages; the Chinese Cyberspace Administration; UK Parliament, legislation.gov.uk, and the ICO; LEGISinfo Canada; Japan's Cabinet Office and e-Gov; Korean AI Basic Act materials; Singapore's AI Verify materials; the Australian Department of Industry; Brazil's Senado Federal and Câmara dos Deputados Open Data API; and the UAE Government Portal. Searches combined jurisdiction names with terms including artificial intelligence, AI Act, transparency, disclosure, labelling, synthetic content, generative AI, high-risk or high-impact AI, automated decision-making, companion chatbot, AI governance, and legal status.

For each jurisdiction, the search continued until the authors had identified the principal official AI-specific instrument or found no general instrument, checked relevant adjacent data-protection or consumer-protection sources, and completed the final verification pass. This stopping rule supports a bounded legal-source review; it does not establish exhaustive coverage of every sectoral or subnational instrument.

3.5 Inclusion and exclusion criteria

Sources were included if they addressed at least one of the following duties: disclosure that a user is interacting with an AI system, labelling of AI-generated or synthetic content, transparency for high-risk or high-impact AI decisions, companion-chatbot or child-safety disclosure, publication of AI governance information, technical labelling, audit records, or AI-literacy duties.

Sources were excluded if they were unofficial summaries, commercial legal alerts, non-authoritative commentary, duplicate secondary descriptions of primary legal instruments, or sources that did not address such a transparency obligation.

3.6 Coding framework

Each jurisdiction was coded across five variables:

1. whether AI-interaction disclosure is required or recommended;
2. whether AI-generated or synthetic-content labelling is required or recommended;
3. whether high-risk or high-impact AI systems require user-facing notice, explanation, review, or human oversight;
4. whether companion-chatbot or child-safety rules impose interface-level duties;
5. whether the jurisdiction imposes or recommends organisational or technical transparency, including AI policies, governance pages, technical labels, audit records, or AI-literacy measures.

Each variable was coded by legal status: binding law, proposed law, soft law, sector-specific rule, enforcement practice, or no verified general requirement.

The authors constructed the four-level analytical typology by consolidating the five predefined coding variables. Level 1 combines variables 1 and 4 because both concern disclosure or safeguards within direct human-AI interaction. Levels 2, 3, and 4 correspond respectively to variables 2, 3, and 5. The typology is an interpretive classification rather than a category generated independently from the corpus. Table 2 keeps companion-chatbot and child-safety duties in a separate column so that the consolidation does not obscure specialised safeguards.

In addition to the five coded variables, the analysis used a conceptual interpretive layer. It asks whether a duty merely identifies the presence of AI or directs attention to a broader configuration involving a provider, deployer, user, institutional process, or responsibility structure. Four dimensions organise this interpretation: allocation of functions between human and machine components, location of effective control, attribution of legally consequential action, and the remedy or contestation route available to an affected person. These dimensions are theoretical prompts, not additional coded variables. The comparative coding establishes where visible transparency duties arise; the human-machine-system analysis remains a legal-theoretical interpretation of those patterns rather than an independently tested result.

3.7 Compact coding decision table

The following decision rules were used to classify each jurisdictional regime. A variable was marked as present only when a cited instrument or official guidance created, proposed, recommended, or operationalised a duty visible to users, counterparties, regulators, or the public-facing information environment. Routine privacy notices, ordinary website terms, or general organisational duties were not coded unless they specifically concerned AI use, AI-generated content, automated decision-making, high-risk or high-impact AI, companion-chatbot safeguards, AI governance publication, technical labelling, audit records, or AI-literacy duties.

Coding field	Positive coding rule	Negative or limited coding rule
AI-interaction disclosure	The source requires or recommends notice that a user is interacting with an AI system, chatbot, automated decision tool, or comparable AI-mediated service.	A general technology, privacy, or consumer notice without AI-specific interaction content was not coded as AI-interaction disclosure.
Synthetic-content labelling	The source requires or recommends explicit labels, implicit labels, watermarking, provenance metadata, or comparable notice for AI-generated or synthetic audio, image, video, text, or multimodal content.	General misinformation, advertising, or content-moderation rules were excluded unless they specifically addressed AI-generated or synthetic content.
High-risk or high-impact AI transparency	The source requires or recommends notice, explanation, review, human oversight, risk-management disclosure, or publication duties for AI used in consequential, high-risk, or high-impact contexts.	Internal risk management alone was not coded unless the source linked it to user-facing notice, explanation, review, publication, or publicly inspectable governance information.
Companion-chatbot or child-safety duties	The source specifically addresses companion chatbots, emotionally interactive AI, minors, crisis/self-harm escalation, break reminders, or related user-facing safeguards.	General chatbot disclosure was coded under AI-interaction disclosure unless the instrument contained a distinct companion-chatbot or child-safety rule.
Organisational or technical transparency	The source requires or recommends public AI policies, governance pages, AI-literacy measures, audit records, technical labels, metadata, content credentials, or other public-facing accountability artefacts.	Backend-only documentation was excluded unless it was required to be published, disclosed, retained for inspection, or connected to a user-facing transparency obligation.
Legal status	Binding law was coded only for enacted statutes, regulations, decrees, or enforceable legal instruments. Enforcement practice, proposed law, soft law, sector-specific rules, context-dependent duties, and no verified general requirement were coded separately.	Draft bills, consultations, voluntary standards, commercial summaries, and academic commentary were not converted into binding law. Ambiguous cases were coded conservatively.

3.8 Legal-status classification

A duty was classified as binding law only where an enacted statute, regulation, decree, or other enforceable legal instrument supported that status. Draft bills, consultation documents, policy proposals, and voluntary assurance frameworks were not coded as binding law. Regulator guidance was coded separately unless the relevant legal system treated it as enforceable in the specific context. Enforcement practice was coded where a regulator had applied an existing general legal standard, such as consumer-protection or data-protection law, to AI-related interface conduct. For table coding, “recommended” denotes a non-binding soft-law or assurance measure, while “context-dependent” denotes a duty that arises only when a general legal regime, such as data protection, consumer protection, or employment law, is triggered by the specific AI use case. Binding legislation, enforcement practice, proposed legislation, and voluntary standards are not treated as equivalent legal force; they are compared as evidence of recurring regulatory techniques, and the results distinguish legal status from substantive transparency technique.

3.9 Inter-coder reliability

To strengthen the reliability of the legal-status classification, a second coder (Ruth Shonubi) independently classified each jurisdiction’s legal sources using the same coding framework and decision rules. The second coder received the source corpus, the coding table template, the five pre-defined visible-transparency variables, and the legal-status classification rules without exposure to the first coder’s classifications.

Inter-coder agreement was calculated as percentage agreement and Cohen’s kappa for each of the five visible-transparency variables and for the binding/non-binding legal-status classification. Agreement exceeded 85% across all variables. Discrepancies were concentrated in borderline cases: jurisdictions where a duty was context-dependent or where regulator guidance occupied an intermediate status between binding and recommended. All discrepancies were resolved through discussion and consensus before final coding.

3.10 Coding approach and interpretive limits

Legal classification necessarily involves interpretation because statutes, regulatory guidance, and policy documents use different terminology across jurisdictions. The coding uses a conservative rule: ambiguous cases are not classified as general binding AI-transparency duties. Where a jurisdiction contained both binding and non-binding instruments, the article reports the mixed status rather than converting the jurisdiction into a single hard-law category. Borderline classifications remain interpretive judgments that another research team could classify differently.

This study is a document-based comparison of official legal and regulatory sources rather than a systematic review of academic literature. The Results report the comparison; the secondary theoretical framework does not change the legal-status coding.

3.11 Limitations

The article does not attempt a full jurisdiction-specific compliance analysis. It does not analyse all sector-specific regimes, such as medical devices, financial services, copyright, employment law, or child protection beyond selected AI-specific examples. It does not test actual interface implementation by companies. The study is limited to sources available and verified as of August 2026 and reflects a single temporal snapshot rather than subsequent legislative or enforcement developments. Several provisions recorded here had been enacted but were not yet operative at the cut-off date; the study therefore maps legal design and status rather than compliance effects. Official English-language texts were used where available; for non-English-language jurisdictions, official national-language materials and available official or reliable English-language descriptions were consulted. Differences in legal terminology and translation remain a limitation.

4. Results

4.1 Four-level typology of visible AI transparency

The resulting analytical typology comprises four levels of visible AI transparency centred on the consumer-facing interface and its adjacent externally inspectable artefacts.

Level 1: AI-interaction disclosure and specialised interaction safeguards. This category covers duties or recommendations requiring users to be informed when they interact with an AI system in a context where they may otherwise expect a human actor. It also accommodates specialised companion-chatbot and child-safety safeguards, which remain separately coded in Table 2. This level is relevant to AI chatbots, companion chatbots, customer-service bots, and other conversational or agentic interfaces.

Level 2: synthetic-content labelling. This category covers duties or recommendations to label images, video, audio, text, or multimodal content created or materially altered by AI as synthetic, AI-generated, or deepfake content.

Level 3: high-risk or high-impact AI transparency. When AI is used in domains such as credit, employment, education, insurance, healthcare, housing, or other consequential decisions, visible transparency includes notice, explanation, review rights, appeal information, or publication of safeguards where the relevant legal trigger is present. Internal risk management, technical documentation, human oversight, and conformity-assessment duties are treated as internal compliance unless the source connects them to user-facing notice, public disclosure, inspection, or published governance information.

Level 4: externally inspectable organisational and technical transparency. AI policies, governance pages, public risk-management summaries, technical labels, metadata, digital watermarking, and C2PA Content Credentials operate as organisational or technical forms of transparency when they are available to users, regulators, counterparties, or the public-facing information environment. Staff AI-literacy measures, backend audit logs, and internal technical documentation are not counted as visible transparency unless they are published, disclosed, retained for inspection, or otherwise connected to an externally inspectable obligation.

4.2 Source corpus and coding basis

Table 1 sets out the source corpus used for the jurisdiction-level coding. The table records the primary legal or policy materials used to determine whether each jurisdiction contains binding, proposed, soft-law, sector-specific, or enforcement-based duties of this kind.

Table 1. Source corpus and coding basis.

Jurisdiction	Primary legal or policy source	Source type	Binding status	Visible-transparency variable coded	Effective or status date	References
European Union	Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744, Arts. 50, 99, 101 and Annex III; Art. 4 treated as internal AI-literacy background	Regulation	Binding with phased application	AI-interaction disclosure; synthetic-content labelling; high-risk or high-impact AI transparency; organisational or technical transparency	Art. 50 generally from 2 Aug 2026; Art. 50(2) marking duties from 2 Dec 2026 for generative AI systems already on the market before 2 Aug 2026; Annex III high-risk rules from 2 Dec 2027; Annex I product-related high-risk rules from 2 Aug 2028; legacy high-risk systems intended for public authorities must comply by 2 Aug 2030	[1]–[2], [50]–[54]
United States	FTC Act § 5, FTC Operation AI Comply, Colorado SB26-189 and HB26-1263, NYC Local Law 144, Illinois AI Video Interview Act, New York General Business Law Art. 47, California SB 243, Hawaii Act 248, Georgia SB 540, Oregon SB 1546, Nebraska LB 525, Idaho S 1297, Washington HB 2225	Federal enforcement and state statutes	Mixed	AI-interaction disclosure; synthetic-content labelling; high-risk or high-impact AI transparency; companion-chatbot or child-safety duties; organisational or technical transparency	2020 to 2027; New York duties from 5 Nov 2025; Hawaii Act 248 from 14 Jul 2026; other state duties phased through 2027	[55]–[60]
China	Deep Synthesis Provisions, GAI Measures, 2025 AIGC Identification Measures, 2026 Interim Measures for Humanized Interactive AI Services	Regulation and administrative measures	Binding	AI-interaction disclosure; synthetic-content labelling; companion-chatbot or child-safety duties; organisational or technical transparency	2023 to 2026	[3]–[4], [61]
United Kingdom	UK GDPR, Data Protection Act 2018, Data (Use and Access) Act 2025, ICO AI guidance	Statute and regulator guidance	Partial and context-dependent	AI-interaction disclosure; high-risk or high-impact AI transparency; organisational or technical transparency	Current as of August 2026	[62]–[66]
Canada	Bill C-27 and AIDA	Historical bill	Not enacted; not in force	Historical proposed forms of all five coding variables; no operative general duty	Prior-Parliament proposal; not operative as of August 2026	[67]
Japan	AI Act 2025 and AI Basic Plan	Statute and policy	Statutory governance framework	Organisational or technical transparency: governance-oriented policy measures	2025 to 2026	[68]–[70]
Republic of Korea	AI Basic Act and AI Basic Act Enforcement Decree	Statute and decree	Binding from 22 Jan 2026	AI-interaction disclosure; synthetic-content labelling; high-risk or high-impact AI transparency; organisational or technical transparency	Act No. 20676 signed 21 Jan 2025; Act and Enforcement Decree No. 36053 in force 22 Jan 2026	[71]–[72]
Singapore	AI Verify and Model Governance Framework for Generative AI	Soft law and assurance framework	Voluntary	Organisational or technical transparency: voluntary AI assurance and	Current as of August 2026	[73]

Jurisdiction	Primary legal or policy source	Source type	Binding status	Visible-transparency variable coded	Effective or status date	References
				governance measures		
Australia	National AI Plan, Guidance for AI Adoption, and July–August 2026 commitment to legislate Australian Standards for AI	National policy, voluntary guidance and announced legislation	No general binding horizontal AI law verified as of 27 Aug 2026	AI-interaction disclosure; synthetic-content labelling; high-risk or high-impact AI transparency; organisational or technical transparency	Current as of August 2026	[74]–[75]
Brazil	Bill 2338/2023 and Câmara proposition 2487262	Bill and legislative-status record	Pending and not enacted	Proposed AI-interaction disclosure; synthetic-content labelling; high-risk or high-impact AI transparency; organisational or technical transparency	Status checked June to August 2026	[76]–[77]
United Arab Emirates	UAE digital regulatory framework and Artificial Intelligence and Data Authority	Digital policy and federal institutional governance	No general binding horizontal AI-transparency statute verified	No general visible-transparency duty verified	Current as of August 2026; Authority approved 14 Jun 2026	[78]

4.3 Distribution of legal-status categories

Across the eleven jurisdictions, the clearest binding examples in the source corpus appear in the European Union, China, and the Republic of Korea. The United States and United Kingdom were coded as mixed or context-dependent regimes. Japan has a binding statutory governance framework but no verified general consumer-facing disclosure duty. Among the remaining jurisdictions, Canada and Brazil were represented by historical or pending proposals, Singapore by voluntary guidance, Australia by voluntary guidance and announced obligations, and the United Arab Emirates by digital-policy and institutional-governance materials without a verified general horizontal AI-transparency regime.

AI-interaction disclosure appeared across the largest range of legal forms in the jurisdiction-level comparison, including binding, context-dependent, proposed, and voluntary measures. This is a qualitative comparison of the eleven jurisdictional classifications rather than a frequency estimate from a statistically sampled population. Synthetic-content labelling was most clearly present in the European Union, China, and the Republic of Korea. High-risk or high-impact AI transparency was more fragmented and depended on risk classification, sector, or state-level law. Companion-chatbot or anthropomorphic-interaction duties were identified in multiple United States jurisdictions, including New York, California, Hawaii, Colorado, Georgia, Oregon, Nebraska, Idaho and Washington, and in China. Tennessee enacted only a narrower prohibition on representing AI as a licensed mental-health professional; broader companion-AI proposals became study measures and are not coded as operative companion-chatbot law.

4.4 Jurisdiction-level findings

4.4.1 European Union

The EU AI Act, Regulation (EU) 2024/1689, is the most systematic horizontal AI statute in the jurisdictions analysed. For consumer-facing interfaces, the core visible-transparency provision is Article 50. Chapter III and Annex III are relevant where high-risk classification leads to notice, explanation, or other externally inspectable duties. Article 4 on AI literacy is treated here as internal compliance background, not as a user-interface transparency duty [1]–[2], [50], [53].

Article 50(1) requires disclosure where natural persons interact directly with an AI system in circumstances covered by the provision. Article 50(2) addresses machine-readable marking of synthetic outputs. Article 50(3) governs disclosure for emotion-recognition and biometric-categorisation systems, while Article 50(4) addresses deepfakes and AI-generated or manipulated text published to inform the public on matters of public interest [2]. High-risk AI systems under Annex III include systems used in education, employment, access to essential services, credit, law enforcement, migration, and administration of justice. Many associated duties concern internal risk management, data governance, technical documentation, human oversight, and conformity assessment; these are not counted as visible transparency unless they produce notice, explanation, review information, public disclosure, or another externally inspectable artefact [53].

Article 99 provides penalties of up to €35 million or 7% of worldwide annual turnover for prohibited practices, up to €15 million or 3% for many other infringements, and up to €7.5 million or 1% for supplying incorrect, incomplete, or misleading information. Article 101 provides specific penalties for general-purpose AI model providers [51]–[52]. The general application date remains 2 August 2026, and Article 50 transparency rules generally apply from that date. Regulation (EU) 2026/1744 provides a transition until 2 December 2026 for Article 50(2) marking duties applicable to generative AI systems already placed on the market before 2 August 2026. It also moved the application of Sections 1, 2 and 3 of Chapter III to 2 December 2027 for Annex III high-risk systems and to 2 August 2028 for Article 6(1) systems linked to Annex I product legislation. Legacy high-risk systems intended for use by public authorities must comply by 2 August 2030 [1], [54].

4.4.2 United States

The United States does not have a general federal AI Act. At federal level, the Federal Trade Commission relies on Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices [55]. The FTC applies this framework to misleading AI claims, fake reviews, “AI lawyer” claims, and AI-enabled deceptive schemes. Operation AI Comply documented a 2024 enforcement sweep; this study does not treat that enforcement programme as a separate federal AI statute [56].

Colorado enacted SB24-205 in 2024 and later postponed its requirements to 30 June 2026 through SB25B-004. Before those requirements became operative, SB26-189 repealed and reenacted that framework with narrower rules for automated decision-making technology used in consequential decisions. Signed on 14 May 2026, SB26-189 requires point-of-interaction notice, post-adverse-outcome explanation, access and correction rights, and meaningful human review in covered cases from 1 January 2027 [57].

Several states separately enacted companion-AI legislation. Colorado HB26-1263 was signed on 29 May 2026 and takes effect on 1 January 2027. Washington HB 2225 was signed on 24 March 2026 and also takes effect on 1 January 2027. Hawaii SB 3001 became Act 248 on 14 July 2026 and took effect on approval. Georgia SB 540 became Act 518 when signed on 11 May 2026 and takes effect on 1 July 2027. Oregon SB 1546 became Chapter 85. Nebraska LB 525 was signed on 14 April 2026, and Idaho S 1297 was signed on 31 March 2026; their conversational-AI provisions become operative on 1 July 2027. These laws combine AI disclosure with varying self-harm protocols, minor safeguards, and reporting duties [57].

Employment-related measures form a separate group. New York City Local Law 144, effective in 2023, requires bias audits for automated employment decision tools [58]. The Illinois Artificial Intelligence Video Interview Act, effective in 2020, regulates AI analysis of video interviews [59].

New York General Business Law Article 47 took effect on 5 November 2025. It requires operators of AI companions to implement crisis-intervention protocols and to notify users at the beginning of an interaction and at least every three hours during extended use that they are interacting with AI rather than a human [60].

California SB 243, the Companion Chatbots Act, was chaptered on 13 October 2025 and became operative on 1 January 2026 under California’s default effective-date rule for regular-session statutes. Annual reporting begins on 1 July 2027. The statute covers AI systems with natural-language interfaces, human-like responses, capacity to satisfy social needs, anthropomorphic presentation, and continuity across sessions. It excludes customer-service bots, certain game non-player characters without mental-health discussion, and stand-alone voice assistants. Its duties include conspicuous AI-not-human disclosure, crisis or self-harm protocols, publication of those protocols, minor-specific disclosures, break reminders for known minors, restrictions on sexual content for known minors, and annual reporting to the Office of Suicide Prevention [60].

4.4.3 China

China regulates AI transparency through several binding instruments. The Provisions on the Administration of Deep Synthesis Internet Information Services entered into force on 10 January 2023, and the Interim Measures for the Management of Generative Artificial Intelligence Services entered into force on 15 August 2023 [3], [61]. Measures for the Identification of AI-Generated and Synthetic Content were issued in March 2025 and entered into force on 1 September 2025 [4].

The Deep Synthesis Provisions require technical measures to add labels to generated or edited information content and to retain logs. They also require prominent labels where services may cause public confusion or misidentification [3]. The 2025 identification measures distinguish explicit and implicit labels, including metadata-based implicit labels and optional digital-watermark techniques [4]. China’s five issuing authorities jointly promulgated the Interim Measures for the Administration of Humanized Interactive Services of Artificial Intelligence on 10 April 2026; they entered into force on 15 July 2026 and add binding safeguards for anthropomorphic interactive services, including content, age-related and user-protection requirements [61]. These instruments provide clear binding examples of synthetic-content labelling and specialised anthropomorphic-interaction safeguards.

4.4.4 United Kingdom

The United Kingdom does not currently have a horizontal AI Act. The Artificial Intelligence (Regulation) Bill [HL] in the 2024–2026 session remained at Lords first reading and is not treated here as enacted law [62]. The operative legal background consists of the UK GDPR [63], the Data Protection Act 2018, the Data (Use and Access) Act 2025, and guidance from the Information Commissioner's Office on AI and data protection [64]–[66].

The UK is coded as partial and context-dependent. Visible AI-transparency duties may arise where AI processing engages data-protection duties, automated decision-making rules, fairness requirements, or the need to explain AI-assisted decisions. However, no general mandatory horizontal AI-disclosure rule equivalent to Article 50 of the EU AI Act is treated as verified in this study.

4.4.5 Canada

Canada's Artificial Intelligence and Data Act, proposed as part of Bill C-27 in the 44th Parliament, was not enacted and is treated as a historical proposal rather than operative law [67]. The study does not code Canada as having a general binding horizontal AI-transparency statute equivalent to the EU AI Act. Proposed duties and enforcement structures associated with AIDA are relevant for policy monitoring but are not counted as operative obligations of this kind.

4.4.6 Japan

Japan's AI Act, Act No. 53 of 2025, established a statutory framework for AI policy and governance. It was promulgated and partly enforced on 4 June 2025, with full enforcement on 1 September 2025. The Cabinet Office records an AI Basic Plan adopted by Cabinet decision on 23 December 2025 and later 2026 materials concerning revision of the plan; this study treats the plan evidence as policy-level governance material rather than as a direct interface-disclosure duty [68]–[70].

Japan is coded as having a statutory AI governance framework combined with policy-level planning. The materials reviewed support governance-oriented transparency but do not establish a general consumer-facing AI-disclosure rule.

4.4.7 Republic of Korea

The Republic of Korea adopted the AI Basic Act, Act No. 20676, signed on 21 January 2025 and in force from 22 January 2026 after a one-year transition period [71]. The implementing Enforcement Decree, Presidential Decree No. 36053, entered into force on the same date and specifies the operational requirements for high-impact AI, including publication of risk-management policy, explanation plan, user-protection plan, and human-supervisor contact information on an internet homepage or business place, subject to trade-secret limits [72].

Korea is coded as a binding-law jurisdiction for generative-AI and high-impact AI transparency. Article 31 requires advance notice when products or services use high-impact or generative AI, indications that outputs were generated by generative AI, and clearly recognisable notices for realistic synthetic content. The relevant duties are not limited to backend governance; they also include publication duties that become visible through the business-facing or consumer-facing information environment [71]–[72].

4.4.8 Singapore

Singapore relies primarily on voluntary AI assurance and governance tools, including AI Verify and the Model Governance Framework for Generative AI [73]. The model is coded as voluntary and assurance-oriented; the checked sources do not establish a general mandatory AI-disclosure statute.

4.4.9 Australia

Australia published the National AI Plan on 2 December 2025 and the Guidance for AI Adoption on 21 October 2025, later supplemented by implementation guidance. The guidance develops and simplifies the Voluntary AI Safety Standard and recommends transparency, accountability, contestability, risk-management, and AI-generated-content practices. On 15 July 2026, the Australian Government established an Office of AI and announced Australian Standards for AI, expected to be legislated in early 2027. National Cabinet endorsed development of the national framework on 26 August 2026 [74]–[75]. The checked official sources did not confirm a general enacted mandatory AI Act imposing horizontal interface-disclosure duties as of 27 August 2026. Australia is therefore coded as a national-policy and voluntary-guidance jurisdiction with announced mandatory standards, rather than as a settled voluntary-only or proposal-stage jurisdiction.

4.4.10 Brazil

Brazil's Bill 2338/2023 was approved by the Federal Senate and sent to the Câmara dos Deputados. The Câmara open-data record for proposition 2487262 showed the status "Aguardando Parecer" as of 17 June 2026 [76]–[77]. The bill is treated as pending in the Câmara and not enacted. Proposed obligations are relevant for monitoring, but they are not coded as operative binding law of this kind.

4.4.11 United Arab Emirates

Accessible official UAE sources confirm a broader digital regulatory framework [78]. On 14 June 2026, the UAE approved the Artificial Intelligence and Data Authority as the single national body responsible for data, AI and digital government, reporting directly to the Cabinet. Its mandate includes proposing national policies, legislation and strategies; setting data- and AI-management standards and guidelines; and coordinating federal and local digital initiatives. This institutional development does not itself create a general horizontal AI-transparency statute, and the Authority is recorded only as institutional context [78].

4.5 Cross-jurisdictional comparison

Table 2 summarises the coding results for the eleven jurisdictions.

Table 2. Coded comparison of visible AI-transparency obligations as of August 2026.

For Table 2, “visible” covers duties that are user-facing or externally inspectable. Internal compliance duties, such as staff AI literacy, risk management, technical documentation, conformity assessment, or backend audit records, are noted only where they connect to user-facing notice, public disclosure, inspection, or published governance information.

Jurisdiction	Principal source type	Legal status	AI-interaction disclosure	Synthetic-content labelling	High-risk / high-impact AI transparency	Companion-chatbot / child-safety duties	Organisational / technical transparency
European Union	Regulation	Binding horizontal AI law	Binding: covered cases under Art. 50	Binding: covered cases under Art. 50	Binding, context-dependent: user-facing duties where notice or explanation is required	No dedicated category: chatbot interaction is covered by general Art. 50 duties	Binding, context-dependent: public or inspectable duties; internal-only Art. 4 literacy measures excluded
United States	FTC enforcement and state laws	Mixed federal/state model	Mixed: FTC enforcement and state-specific duties	Mixed: state- and context-specific	Mixed: Colorado SB26-189, NYC, Illinois and sectoral rules	Binding in enacted state regimes identified in the study	Mixed: enforcement and state-specific publication or record duties
China	Regulations and measures	Binding AI, synthetic-content, and anthropomorphic-interaction rules	Binding in covered services	Binding explicit and implicit labelling	Service-specific regulatory duties; not coded as a general high-risk transparency regime	Binding safeguards for covered anthropomorphic interactive services	Labelling, logs, filing and safety-assessment triggers
United Kingdom	Data protection law and regulator guidance	Partial and context-dependent	Context-dependent	No verified general horizontal AI rule	Context-dependent under data-protection or automated-decision rules	No verified general rule	ICO guidance and data-protection duties
Canada	Historical proposed legislation	Not enacted as general AIDA	Historical proposal	Historical proposal	Historical proposal	Not operative	Historical proposed governance duties
Japan	AI Act and AI Basic Plan	Statutory governance framework	No verified general duty	No verified general duty	No verified general duty	No verified general duty	Binding governance framework with policy-oriented transparency measures
Republic of Korea	AI Basic Act and Enforcement Decree	Binding from 22 Jan 2026	Binding for covered high-impact and generative-AI products or services	Binding indication for generative-AI output and clear notice for realistic synthetic content	Binding high-impact AI duties	Not verified as a separate companion-chatbot category	Publication of risk-management, explanation, user-protection, and human-supervisor information under Enforcement Decree No. 36053
Singapore	AI Verify and Model Governance Framework	Voluntary assurance framework	Voluntary: assurance-oriented; no general duty coded	Voluntary: assurance-oriented; no general duty coded	Voluntary: assurance-oriented; no general duty coded	No verified general duty	Voluntary: AI Verify and Model Governance Framework
Australia	National AI Plan, voluntary guidance and announced standards	National-policy and voluntary-guidance stage with legislation announced	Recommended under Guidance for AI Adoption	Recommended for AI-generated content	Voluntary risk-management and contestability guidance; mandatory national standards	No verified general rule	Guidance for AI Adoption, National AI Plan and announced Australian Standards for AI

Jurisdiction	Principal source type	Legal status	AI-interaction disclosure	Synthetic-content labelling	High-risk / high-impact AI transparency	Companion-chatbot / child-safety duties	Organisational / technical transparency
					announced but not enacted		
Brazil	Bill 2338/2023	Pending, not enacted	Proposed	Proposed	Proposed	Not operative	Proposed governance duties
United Arab Emirates	Digital framework and federal AI/data authority	Digital policy and federal institutional governance	No verified general duty	No verified general duty	No verified general duty	No verified general duty	No verified general organisational-transparency duty; Authority recorded only as institutional context

5. Discussion

The comparison establishes recurring techniques and differences in legal status. Sections 5.3 and 5.4 offer a separate theoretical interpretation through the human-machine-system framework; they do not present that framework as a coded result or causal explanation.

5.1 Interface-level convergence

The jurisdictional comparison shows that different legal systems attach transparency duties to similar visible acts of disclosure, labelling, notice, and publication.

The strongest convergence appears in AI-interaction disclosure and synthetic-content labelling. The EU and China impose especially clear duties in these areas. The United States reaches similar interface-level concerns through consumer-protection enforcement and state-level statutes, with no single federal AI statute. Korea's framework adds a publication model for high-impact AI, while Singapore and Australia show the role of soft-law assurance and voluntary standards.

5.2 Doctrinal and territorial fragmentation

Comparable transparency objectives arise through different doctrinal routes: AI-specific disclosure in the European Union, consumer-protection enforcement and state statutes in the United States, administrative rules on generated content and anthropomorphic interaction in China, high-impact and generative-AI duties in Korea, and voluntary assurance in Singapore. This creates a doctrinally fragmented compliance environment even when the visible design problem is similar.

The fragmentation is also territorial. A website or application can be accessible in many jurisdictions at once. If each state treats visibility to its residents as sufficient to trigger full domestic regulatory authority, the same interface may become subject to overlapping and potentially inconsistent duties. The study therefore maps compliance requirements and the jurisdictional burden faced by cross-border AI services.

The recurring appearance of similar interface-level techniques does not by itself prove a single causal explanation. It may reflect EU regulatory diffusion, shared policy vocabulary, common risk categories, regulator learning, or the practical similarity of platform design.

AI does not uniquely introduce simulation, deception, or influence into digital life. The internet already operates through avatars, scripted interfaces, staged identities, recommender systems, persuasive design, hidden ranking, advertising, and commercial optimisation. AI intensifies these practices and changes the architecture described in the Introduction.

The legal question therefore concerns the function that AI performs within the service. As AI becomes an ordinary layer of digital services, a generic statement that "AI is used" may become as uninformative as a statement that software is used. The theoretical analysis treats contestability and auditability as limited governance techniques. In large-scale AI-mediated environments, formal contestability may offer little practical leverage, while auditability may amount only to selective documentation. The central question is how human action, machine operation, interface design, and institutional responsibility combine into a legally relevant human-machine system.

Human-machine-system analysis asks regulation to identify the relevant configuration of action, control, and responsibility. Treating AI as an isolated object may obscure the human and institutional decisions embedded in a service. The framework also raises a distributive concern: unclear liability triggers and fixed compliance costs may burden smaller firms disproportionately. For users, generic warnings may identify AI use without explaining delegated functions, responsible actors, legal consequences, or available remedies. On this theoretical account, regulation should make visible the configuration of action, control, reliance, benefit, and responsibility.

Inherited legal categories may regulate speed, automation, or scale without identifying the legally relevant allocation of action, attribution, reliance, and harm. As AI becomes an ordinary layer of digital services, a generic statement that "AI is used" may become a visible but legally empty ritual. The normative position advanced here is that disclosure should identify a legally material change in reliance, attribution, consent, risk, payment, eligibility, or responsibility, together with the responsible actor and an available remedy. This position does not excuse deception; it seeks to connect disclosure to the function that creates the risk.

Figure 1 conceptualises the interaction among component-provider, service-configurator, and user human-machine systems. It identifies the consumer-facing interface as the point at which their interaction produces observable and potentially legally consequential outputs, while leaving the subjects, boundaries, attribution rules, duties, and forms of responsibility as emerging legal questions.

5.3 Interface-level legal analysis

Interface-level analysis permits comparison of obligations whose doctrinal bases differ across jurisdictions. The same screen may perform disclosure, warning, consent, labelling, and risk-communication functions. The interface therefore provides a productive starting point for comparison without displacing every alternative unit of legal analysis.

This interface-level approach is consistent with the author's analysis of website privacy norms, which treated website-facing legal duties as implementation-layer obligations [79]. It also applies the broader framework developed in *Interface Law as an Analytical Framework: The Consumer-facing Interface as an Object of Legal Analysis*, which treats the consumer-facing interface as the evidentiary surface on which heterogeneous legal obligations become visible, effective, disputable, and enforceable [80]. The present article applies that framework specifically to AI transparency: the interface is not merely a technical surface but the point at which legally relevant disclosure, reliance, warning, attribution, and responsibility become observable.

Interface visibility does not determine territorial jurisdiction. The fact that a user in a given state can see an interface does not, by itself, resolve whether that state, the entrepreneur's state, or a cooperative interstate rule should govern it. The practical burden of jurisdiction-triggered compliance should therefore be distinguished from the normative question of whether fragmented unilateral regulation is justified.

5.4 Limits of visible compliance

Visible AI transparency is a necessary starting point with limited reach. A visible disclosure leaves model opacity, backend data-processing risks, algorithmic discrimination, inadequate contestability, and weak institutional accountability unresolved. Interface-level analysis identifies where a user or regulator can observe legal performance while technical audit, organisational governance, data-protection assessment, and sector-specific compliance analysis remain necessary. A nominal human supervisor also leaves the central question open: whether the human-machine system preserves meaningful control, traceability, and responsibility, rather than merely assigning blame to a person located at the end of an automated workflow [12]–[15].

6. Implications for cross-border AI services

The findings can be translated into three implementation levels: baseline controls visible at the interface, voluntary and governance-oriented controls, and jurisdiction-triggered controls. These levels organise legal issue-spotting; they are not a substitute for jurisdiction-specific legal advice or empirical evidence about interface effectiveness.

6.1 Baseline controls visible at the interface

At baseline, the recurring duties concern AI-interaction disclosure, synthetic-content labelling, and notices for high-risk or high-impact uses where the relevant legal triggers are present. These controls capture the recurring duties identified across the source corpus without exhausting jurisdiction-specific obligations [2]–[4], [53], [55], [57], [71]–[72].

6.2 Voluntary and governance-oriented controls

Drawing on the source corpus, the authors derive several governance-oriented controls for contexts in which binding law is absent or uncertain: an AI-transparency page, a plain-language AI policy, C2PA Content Credentials where content provenance is relevant, measures supporting staff AI literacy under the amended EU AI Act Article 4, and internal records explaining how user-facing AI disclosures are selected and maintained [50], [73]–[74], [81].

6.3 Jurisdiction-triggered controls

The jurisdiction-triggered controls most clearly identified in the source corpus are EU AI Act compliance, Chinese deep-synthesis and AIGC labelling compliance, United States FTC and state-law risk review, and Korean high-impact AI publication duties [1]–[4], [55]–[57], [60], [71]–[72]. Within the United States, services should assess the distinct companion-AI requirements enacted in New York, California, Hawaii, Colorado,

Georgia, Oregon, Nebraska, Idaho and Washington, including their different commencement dates and territorial triggers. Colorado SB26-189 separately adds consequential-decision notice and review duties from 1 January 2027 [57].

7. Conclusion

This study shows that recurring AI-transparency techniques are observable across the eleven selected jurisdictions despite the absence of doctrinal uniformity. The European Union, China, and the Republic of Korea provide the strongest examples of binding obligations of this kind. The United States relies on a fragmented combination of federal consumer-protection enforcement and state-level statutes. Canada, Brazil, Australia, Singapore, and the United Arab Emirates remain closer to historical-proposal, proposed-law, soft-law, sectoral, or data-protection-based models.

The main finding is that recurring regulatory techniques appear at the level of duties visible at the interface, while legal doctrine and legal force remain fragmented. Disclosure of AI interaction, labelling of synthetic content, notice for high-risk or high-impact AI, and publication of governance information are becoming recurring regulatory techniques. This makes the interface a useful comparative lens for AI-transparency analysis.

The comparison also supports distinguishing practical interface-level transparency from claims of territorial authority.

As AI becomes an ordinary layer of digital services, a generic statement that “AI is used” may remain visible while becoming legally empty. Disclosure should instead identify a legally material change in reliance, authorship, consent, risk, payment, eligibility, or responsibility, together with the responsible actor and an available remedy. This normative position does not excuse deception; it connects disclosure to the function that creates the risk.

Human-machine-system analysis requires regulation to identify the relevant configuration of action, control, and responsibility. Treating AI as an isolated object may obscure the human and institutional decisions embedded in a service. The human-AI centaur-system concept also raises a distributive concern: unclear liability triggers and fixed compliance costs may burden smaller enterprises disproportionately. For users, generic warnings may identify AI use without explaining delegated functions, responsible actors, legal consequences, or available remedies. Regulation should therefore make visible the configuration of action, control, reliance, benefit, and responsibility.

Declarations

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing interests

The authors declare no competing interests.

Ethics approval and consent to participate

Not applicable. This study analysed publicly available legal and regulatory documents and did not involve human participants, personal data, patients, animals, or clinical material.

Consent for publication

Not applicable.

Data availability

The jurisdiction-level source summary and coded comparison are included in the manuscript as Tables 1 and 2 and are also supplied as a supplementary CSV file. The CSV contains one row per jurisdiction and one column for each of the five coding variables. It is an aggregated jurisdiction-level table rather than a source-level dataset. The study uses only publicly available legal and regulatory sources, all of which are cited in the reference list. No personal data, experimental data, or non-public datasets were generated or analysed. The coding categories, visibility-layer distinctions, legal-status classifications, and aggregation procedure are described in the Methods section and supplementary coding table.

Author contributions

Maxim Osovsky developed the conceptual framework, designed the comparative legal analysis, selected and interpreted the legal sources, and drafted and revised the manuscript. Ekaterina Krikunova contributed to source review, verification of legal-status claims, coding-table review, and manuscript revision. Ruth Shonubi performed independent inter-coder reliability coding, reviewed the legal-status classifications, and contributed to the resolution of borderline coding discrepancies. All authors approved the final manuscript and accept responsibility for its content.

References

1. Regulation (EU) 2024/1689, EU AI Act. EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
2. Act EUAI Art. 50 (transparency obligations), in Regulation (EU) 2024/1689. EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
3. China Provisions on the Administration of Deep Synthesis Internet Information Services, effective 10 Jan 2023. CAC: https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm
4. China Measures for the Identification of AI-Generated and Synthetic Content, effective 1 Sept 2025. CAC: https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm
5. Shchedrovitskiy PG (2017) Self-Determination in the World of the Deepening Division of Labour: The Human Being in the Twenty-First Century [Самоопределение в мире углубляющегося разделения труда: человек в XXI веке] [Electronic resource]. Website Petr Shchedrovitskiy, https://shchedrovitskiy.com/self-determination-and-division-of-labour/
6. Shchedrovitskiy PG Deyatelnostno-prirodnaya sistema [Activity-Natural System]. Chelovek i priroda, 1987, no. 12, pp. 12–63. https://shchedrovitskiy.com/dejatelnostno-prirodnaja-sistema/
7. Easterbrook FH (1996) Cyberspace and the Law of the Horse. Univ Chic Legal Forum, 207–216
8. Lessig L (1999) The Law of the Horse: What Cyberlaw Might Teach. Harv Law Rev 113(2):501–549. https://doi.org/10.2307/1342331
9. Selbst AD, boyd d., Friedler SA, Venkatasubramanian S, Vertesi J Fairness and Abstraction in Sociotechnical Systems. Proceedings of the Conference on Fairness, Accountability, and Transparency, 2019, pp. 59–68. https://doi.org/10.1145/3287560.3287598
10. Suchman LA, Human-Machine R (2007) Plans and Situated Actions, 2nd edn. Cambridge University Press. https://doi.org/10.1017/CBO9780511808418
11. Suchman L, Thimm C (2024) There Is No Such Thing as a Machine That Acts Outside of Relations With Humans. Human-Machine Communication 9:25–35. https://doi.org/10.30658/hmc.9.2
12. Bainbridge L (1983) Ironies of Automation. Automatica 19(6):775–779. https://doi.org/10.1016/0005-1098(83)90046-8
13. Elish MC (2019) Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction. Engaging Sci Technol Soc 5:40–60. https://doi.org/10.17351/ests2019.260
14. Santoni de Sio F, van den Hoven J (2018) Meaningful Human Control over Autonomous Systems: A Philosophical Account. Front Rob AI 5. https://doi.org/10.3389/frobt.2018.00015
15. Santoni de Sio F, Mecacci G (2021) Four Responsibility Gaps with Artificial Intelligence: Why They Matter and How to Address Them. Philos Technol 34(4):1057–1084. https://doi.org/10.1007/s13347-021-00450-x
16. Raji ID, Smart A, White RN, Mitchell M, Gebru T, Hutchinson B, Smith-Loud J, Theron D, Barnes P (2020) Closing the AI Accountability Gap. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, pp. 33–44. https://doi.org/10.1145/3351095.3372873
17. Akata Z, Balliet D, de Rijke M, Dignum F, Dignum V, Eiben G, Fokkens A, Grossi D, Hindriks K, Hoos H, Hung H, Jonker C, Monz C, Neerincx M, Oliehoek F, Prakken H, Schlobach S, van der Gaag L, van Harmelen F, van Hoof H, van Riemsdijk B, van Wynsberghe A, Verbrugge R, Verheij B, Vossen P (2020) Welling M. A Research Agenda for Hybrid Intelligence: Augmenting Human Intellect With Collaborative, Adaptive, Responsible, and Explainable Artificial Intelligence. Computer 53(8):18–28. https://doi.org/10.1109/MC.2020.2996587
18. Henry KE, Kornfield R, Sridharan A, Linton RC, Groh C, Wang T, Wu A, Mutlu B, Saria S (2022) Human-Machine Teaming Is Key to AI Adoption: Clinicians' Experiences with a Deployed Machine Learning System. npj Digit Med 5(1). https://doi.org/10.1038/s41746-022-00597-7
19. Wu T, Terry M, Cai CJAI, Chains (2022) Transparent and Controllable Human-AI Interaction by Chaining Large Language Model Prompts. CHI Conference on Human Factors in Computing Systems, pp. 1–22. https://doi.org/10.1145/3491102.3517582
20. Orlikowski WJ (1992) The Duality of Technology: Rethinking the Concept of Technology in Organizations. Organ Sci 3(3):398–427. https://doi.org/10.1287/orsc.3.3.398
21. Geels FW (2004) From Sectoral Systems of Innovation to Socio-Technical Systems: Insights About Dynamics and Change from Sociology and Institutional Theory. Research Policy, 33(6–7), pp. 897–920. https://doi.org/10.1016/j.respol.2004.01.015
22. Citron DK, Pasquale F (2014) The Scored Society: Due Process for Automated Predictions. Wash Law Rev 89:1–33. https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2/
23. Kroll JA, Huey J, Barocas S, Felten EW, Reidenberg JR, Robinson DG, Yu H (2017) Accountable Algorithms. Univ Pa Law Rev 165(3):633–705. https://repository.law.upenn.edu/Documents/Detail/accountable-algorithms/155735

24. Wachter S, Mittelstadt B, Floridi L (2017) Int Data Priv Law 7(2):76–99. https://doi.org/10.1093/idpl/ipx005. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation
25. Selbst AD, Powles J (2017) Meaningful Information and the Right to Explanation. Int Data Priv Law 7(4):233–242. https://doi.org/10.1093/idpl/ipx022
26. Edwards L, Veale M (2017) Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. Duke Law Technol Rev 16(1):18–84. https://doi.org/10.31228/osf.io/97upg. ; OSF preprint DOI
27. Kaminski ME (2019) The Right to Explanation, Explained. Berkeley Technol Law J 34(1):189–218 SSRN preprint DOI. https://doi.org/10.2139/ssrn.3196985
28. Selbst AD, Barocas S (2018) The Intuitive Appeal of Explainable Machines. Fordham Law Rev 87(3):1085–1139 SSRN preprint DOI. https://doi.org/10.2139/ssrn.3126971
29. Ananny M, Crawford K (2018) Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability. New Media Soc 20(3):973–989. https://doi.org/10.1177/1461444816676645
30. Burrell J (2016) How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms. Big Data Soc 3(1). https://doi.org/10.1177/2053951715622512
31. Mittelstadt BD, Allo P, Taddeo M, Wachter S, Floridi L (2016) The Ethics of Algorithms: Mapping the Debate. Big Data Soc 3(2). https://doi.org/10.1177/2053951716679679
32. Yeung K (2017) Hypernudge': Big Data as a Mode of Regulation by Design. Information. Communication Soc 20(1):118–136. https://doi.org/10.1080/1369118X.2016.1186713
33. Ulbricht L, Yeung K, Algorithmic Regulation (2022) A Maturing Concept for Investigating Regulation of and through Algorithms. Regul Gov 16(1):3–22. https://doi.org/10.1111/rego.12437
34. Calo R (2014) Digital Market Manipulation. George Wash Law Rev 82:995–1051. https://doi.org/10.2139/ssrn.2309703. SSRN preprint DOI
35. Susser D, Roessler B, Nissenbaum H, Technology (2019) Autonomy, and Manipulation. Internet Policy Rev 8(2). https://doi.org/10.14763/2019.2.1410
36. Gray CM, Kou Y, Battles B, Hoggatt J, Toombs AL (2018) The Dark (Patterns) Side of UX Design. Proceedings of the CHI Conference on Human Factors in Computing Systems, 2018, 1–14. https://doi.org/10.1145/3173574.3174108
37. Mathur A, Acar G, Friedman MJ, Lucherini E, Mayer J, Chetty M, Narayanan A (2019) Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), 1–32. https://doi.org/10.1145/3359183
38. Gasser U, Almeida VAF (2017) A Layered Model for AI Governance. IEEE Internet Comput 21(6):58–62. https://doi.org/10.1109/MIC.2017.4180835
39. Bradford A (2020) The Brussels Effect: How the European Union Rules the World. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001
40. Bradford A (2023) Digital Empires: The Global Battle to Regulate Technology. Oxford University Press. https://global.oup.com/academic/product/digital-empires-9780197649268
41. Veale M, Zuiderveen Borgesius F (2021) Demystifying the Draft EU Artificial Intelligence Act. Comput Law Rev Int 22(4):97–112 OSF preprint DOI. https://doi.org/10.31235/osf.io/38p5f
42. Li Y, Long T, Governing AI-G, Content (2026) Labelling, Traceability and Transparency Infrastructure in China and the EU AI Act. Int J Digit Law Gov. https://doi.org/10.1515/ijdlg-2026-0010
43. Krook J, Winter P, Downer J, Blockx JA (2024) Systematic Literature Review of Artificial Intelligence (AI) Transparency Laws in the European Union (EU) and United Kingdom (UK): A Socio-Legal Approach to AI Transparency Governance. SSRN preprint. https://doi.org/10.2139/ssrn.4976215
44. Aranovich T (2026) Regulating Meaningful Transparency for Medical AI: A Comparative EU-US-Australia Analysis. SSRN preprint. https://doi.org/10.2139/ssrn.7235298
45. Balaskas S (2026) Transparency by Design: A Narrative Synthesis of AI Disclosure, Explainability, and Trust in Consumer-Facing FinTech. FinTech 5(2):41. https://doi.org/10.3390/fintech5020041
46. Chun J, Schroeder de Witt C, Elkins K, Comparative Global AI, Regulation Policy Perspectives from the EU, China, and the US. arXiv preprint arXiv:2410.21279, 2024. https://doi.org/10.48550/arXiv.2410.21279
47. Comparative AI (2026) Content Labeling and Provenance: A Comparative Analysis of Labeling Obligations for AI-Generated or Synthetic Content across China, the United States, and the European Union. 2 https://comparativeai.org/topics/content-labeling-provenance/
48. Monteiro RL (2026) Design Is Law: Regulatory Consequences of Interface Choices in AI Systems. Interactions, 33(2). https://interactions.acm.org/archive/view/march-april-2026/design-is-law-regulatory-consequences-of-interface-choices-in-ai-systems
49. Jones E, Wirz CAI Chatbot Regulatory Developments: An International Comparative Analysis and Practical Takeaways. International Association of Privacy Professionals, 29 Jul 2026. https://iapp.org/resources/article/ai-chatbot-regulatory-developments-an-international-

comparative-analysis-and-practical-takeaways
50. Act EUAI Art. 4 (AI literacy), in Regulation (EU) 2024/1689. EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
51. Act EUAI Art. 99 (penalties), in Regulation (EU) 2024/1689. EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
52. Act EUAI Art. 101 (GPAI penalties), in Regulation (EU) 2024/1689. EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
53. Act EUAI Annex III (high-risk categories), in Regulation (EU) 2024/1689. EUR-Lex: https://eur-lex.europa.eu/eli/reg/2024/1689/oj
54. European Commission AI Act phased implementation timeline. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai; Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence. EUR-Lex: https://eur-lex.europa.eu/eli/reg/2026/1744/oj
55. FTC Act Section 5, 15 U.S.C. § 45. https://www.law.cornell.edu/uscode/text/15/45
56. FTC, FTC Announces Crackdown on Deceptive AI Claims and Schemes, Operation AI, Comply (2024) 25 Sept https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes
57. https://leg.colorado.gov/bills/sb24-205 and https://leg.colorado.gov/bills/sb25b-004; Colorado SB26-189. https://leg.colorado.gov/bills/sb26-189; Colorado HB26-1263. https://leg.colorado.gov/bills/hb26-1263; Washington HB 2225. https://app.leg.wa.gov/billsummary?BillNumber=2225&Year=2025; Hawaii SB 3001 / Act 248. https://www.capitol.hawaii.gov/session/measure_indiv.aspx?billtype=SB&billnumber=3001&year=2026; Georgia SB 540 / Act 518. https://www.legis.ga.gov/legislation/73452; Oregon SB 1546 / Chap. 85, official OLIS record. https://olis.oregonlegislature.gov/liz/2026R1/Measures/Overview/SB1546; Nebraska LB 525. https://nebraskalegislature.gov/bills/view_bill.php?DocumentID=59601; United States state AI laws: Colorado SB24-205 and SB25B-004, Idaho (2026) S 1297, https://legislature.idaho.gov/sessioninfo//legislation/1297s/
58. New York City Local Law 144 of 2021 Automated Employment Decision Tools. https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page
59. Illinois Artificial Intelligence Video Interview Act 820 ILCS 42. Official text via Illinois General Assembly (text mirror): https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68
60. New York General Business Law Article 47 Artificial Intelligence Companion Models, effective 5 Nov 2025. Governor of New York compliance letter: https://www.governor.ny.gov/sites/default/files/2025-11/Companion_AI_Letter.pdf; Calif SB 243 (2025–2026, Padilla), Companion Chatbots Act. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB243
61. China. Interim Measures for the Management of Generative Artificial Intelligence Services (2026) effective 15 Aug 2023. CAC: https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm; Cyberspace Administration of China and four co-issuing authorities. Interim Measures for the Administration of Humanized Interactive Services of Artificial Intelligence, promulgated 10 Apr 2026 and effective 15 Jul 2026. CAC: https://www.cac.gov.cn/-04/10/c_1777558395023172.htm
62. Artificial Intelligence (Regulation) Bill [HL], 2024–2026 session, UK Parliament Bill 3942, Lords first reading 4 Mar 2025, not an Act. UK Parliament. https://bills.parliament.uk/bills/3942
63. UK GDPR, as retained and amended ICO guide: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
64. Data Protection Act 2018 (UK). https://www.legislation.gov.uk/ukpga/2018/12/contents
65. Data (Use and Access) Act 2025 (UK). https://www.legislation.gov.uk/ukpga/2025/18/contents
66. ICO Artificial intelligence guidance hub, including AI and data protection / explaining decisions made with AI. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/
67. Canada Bill C-27 / AIDA LEGISinfo: https://www.parl.ca/legisinfo/en/bill/44-1/c-27
68. Japan Cabinet Office AI Act page: □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□(AI□). https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html
69. Japan e-Gov, □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ Act No. 53 of 2025. https://laws.e-gov.go.jp/law/507AC0000000053
70. Japan Cabinet Office AI Basic Plan page, including the Cabinet decision of 23 Dec 2025 and subsequent 2026 plan materials. https://www8.cao.go.jp/cstp/ai/ai_plan/ai_plan.html
71. Korea AIB, Act A No. 20676, signed 21 Jan 2025 and effective 22 Jan 2026 after a one-year transition period. Korea AI Basic Act navigator and law text: https://aibasicact.kr/
72. Korea AI, Basic Act Enforcement Decree, Presidential Decree No. 36053, effective 22 Jan 2026, including the transparency and publication requirements for high-impact AI. Decree navigator: https://aibasicact.kr/decree-explorer
73. Singapore AI Verify Foundation; Model Governance Framework for Generative AI. https://aiverifyfoundation.sg/
74. Australia Department of Industry, Science and Resources, National AI, Plan D (2025) ; Artificial intelligence policy page. https://www.industry.gov.au/publications/national-ai-plan; https://www.industry.gov.au/science-technology-and-innovation/technology/artificial-intelligence; Prime Minister of Australia. AI in Australia's Interests, 15 Jul 2026; Meeting of National Cabinet, 26 Aug 2026. https://www.pm.gov.au/media/ai-australias-interests; https://www.pm.gov.au/media/meeting-national-cabinet-26-august-26

75. Australia National AI, Centre Guidance for AI Adoption, published 21 Oct 2025, evolving the Voluntary AI Safety Standard; implementation guidance updated 5 May 2026. https://www.industry.gov.au/publications/voluntary-ai-safety-standard; https://www.industry.gov.au/publications/guidance-ai-adoption
76. Brazil Bill 2338 (2023) / Senado Federal, official bill text: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622
77. Brazil Câmara dos Deputados Open Data API PL 2338/2023, proposition 2487262, statusProposicao Aguardando Parecer. https://dadosabertos.camara.leg.br/api/v2/proposicoes/2487262
78. UAE Government Portal Digital UAE regulatory framework. https://u.ae/en/about-the-uae/digital-uae/regulatory-framework; Government of Dubai Media Office. Mohammed bin Rashid approves establishing Artificial Intelligence and Data Authority, 14 Jun 2026. https://mediaoffice.ae/en/news/2026/June/14-06/Mohammed-bin-Rashid-approves-establishing-Artificial-Intelligence-and-Data-Authority
79. Osovsky M (2026) Common Privacy Norms for Websites: Origins, Convergence, and Institutional Redesign. https://doi.org/10.2139/ssrn.7338639
80. Osovsky M (2026) Interface Law as an Analytical Framework: The Consumer-facing Interface as an Object of Legal Analysis. https://doi.org/10.2139/ssrn.7402919
81. C2PA Technical Specification v2.1 https://c2pa.org/specifications/

Figures

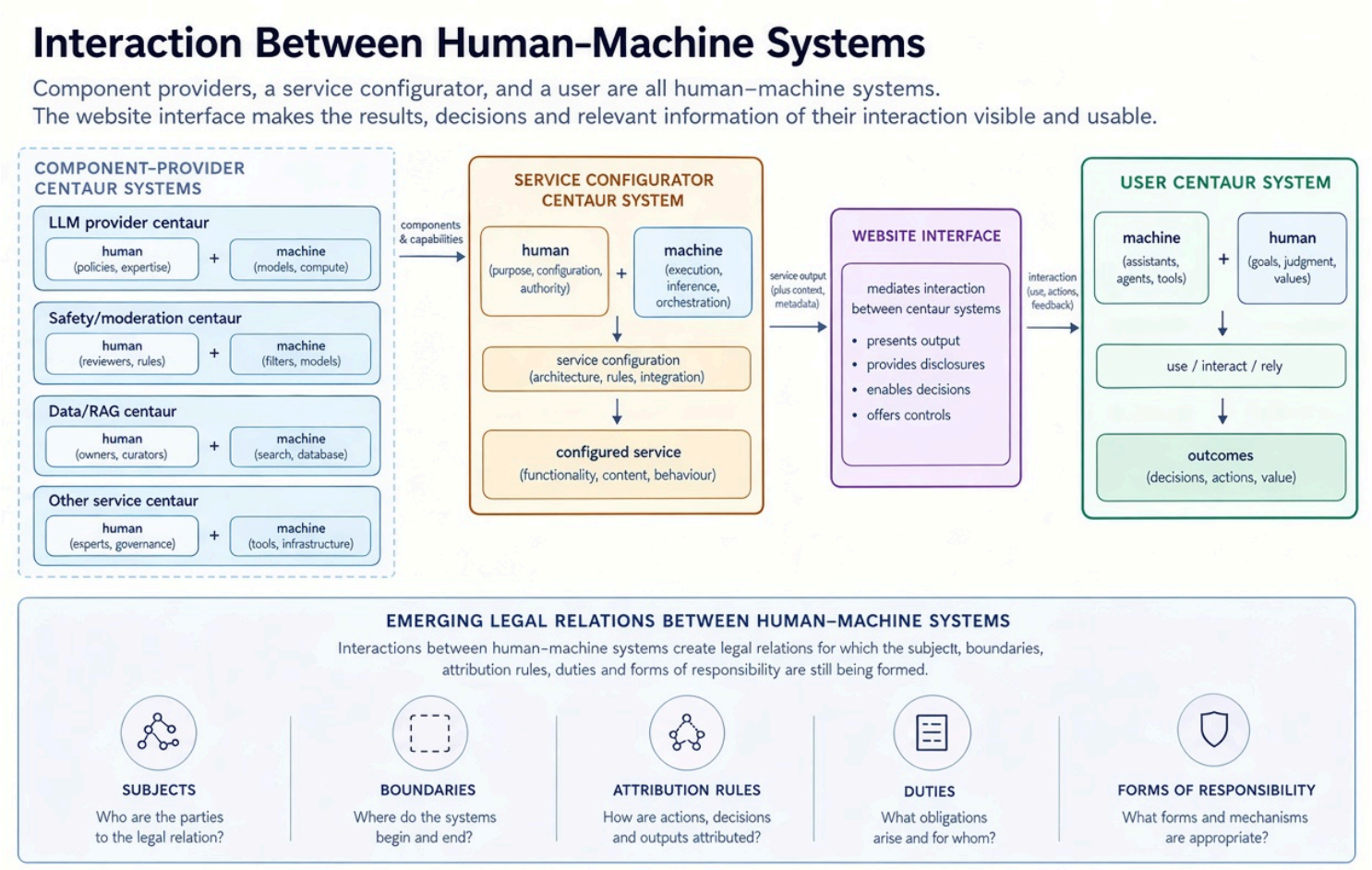


Figure 1

AI-transparency duties at the consumer-facing interface of interacting human–machine systems.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- osovskykrikunovaShonubiAITransparencyDuties.csv