AI *regulation*

Robin Plique

PhD Candidate @Université Paris 1 Panthéon-Sorbonne

AN EU-LAW PERSPECTIVE

2026

— PRÉAMBULE

Four disclaimers, before we begin.

An **EU-law perspective**. I won't address any other legal framework (time constraints). Presentation of the AI Act.

An **extensive focus on definitions and qualifications**. Legal tradition: to operate on reality, we need to first define it.

An **exercise in translation and interdisciplinarity.** Stop me whenever you want to dig in.

Not exhaustive. I've selected the points where the tensions are most visible for researchers. **But a lot of text**.

— PART ONE —

What do we mean by *AI regulation*?

A short history · the 2015 Tech Lash · the EU's "third way" · Article 1 and what it is meant to balance.

“

In 2015, the so-called *Tech Lash* marked a change in tone, as public anxiety about AI's potential adverse impacts grew.

— YEUNG & SMUHA (2025)

— APRIL 2019 – HLEG Ethics Guidelines for Trustworthy AI

7 ethical principles charted out by HLEG – “Trustworthy” AI

(1) Human agency and oversight (incl. need for FRIA)
(2) Technical robustness and safety
(3) Privacy and data governance
(4) Transparency
(5) Diversity, nondiscr° and fairness
(6) Societal and environmental wellbeing
(7) Accountability

Re-evaluate at the end of the lecture what made it into the Act

— A GEOPOLITICAL CONTEXT

EU AI Governance : a "Third way"

— UNITED STATES

Laissez-faire.

MARKET

— CHINA

State-driven.

STATE

— EUROPEAN UNION

A *third* way : a "brand" of AI infused with European values

RIGHTS + MARKET

The *purpose* of AI Regulation in the EU

> Article 1 « *The purpose of this Regulation is to* **improve the functioning of the internal market** *and promote the uptake of* **human-centric and trustworthy artificial intelligence (AI)**, *while ensuring a* **high level of protection of health, safety, fundamental rights enshrined in the Charter** , *including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union* **and supporting innovation** ».

Notice the balancing exercise. Improving functioning of the internal market and protecting fundamental rights. Teleological interpretation.

A staggered entry into force (art. 113)

— PART TWO —

The *scope* of the AI Act

To whom does this regulation apply · where · and at what moment.

How is the application of the Act triggered ?

Article 2.1 – This Regulation applies to:

(a) ***providers*** *placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country ;*

(b) ***deployers*** *of AI systems that have their place of establishment or are located within the Union;*

(c) ***providers*** *and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union .*

Two types of actors - Translating

— ARTICLE 3.3

Provider

*« **provider** » means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge;*

→ Anthropic · OpenAI · Mistral · Google · Meta · Mistral

— ARTICLE 3.4

Deployer

*« **deployer** » means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;*

→ an employer using an applicant-tracking system; bank with a scoring system, etc.

Two types of "actions" (triggers)

— ARTICLE 3.9

Placing on the market

'Placing on the market' means the first making available of an AI system or a general-purpose AI model on the Union market.

→ See: release of ChatGPT in December 2022

— ARTICLE 3.10

Putting into service

'Putting into service': means the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose.

→ What can we think of ?

Three noteworthy exceptions.

Article 2.3. Military AI. *This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.*

Article 2.6. Scientific R&D — the "sole purpose" clause. *This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for* ***the sole purpose*** *of scientific research and development.*

Article 2.10. Non-professional usage. *This Regulation does not apply to obligations of deployers who are natural persons using AI systems in the course of a* ***purely personal non-professional activity.***

— PART THREE —

Definitions of *AI*

Are you and I even talking about the same thing ?

Computer science definitions : lack of consensus ?

— MITCHELL (2019)

*“In a recent report on the current state of AI, a committee of prominent researchers defined the field as “a branch of computer science that studies the properties of intelligence by synthesizing intelligence.” **A bit circular, yes. But the same committee also admitted that it's hard to define the field, and that may be a good thing**: “The lack of a precise, universally accepted definition of AI probably has helped the field to grow, blossom, and advance at an ever-accelerating pace.” Furthermore, the committee notes, “Practitioners, researchers, and developers of AI are instead guided by a rough sense of direction and an imperative to ‘get on with it.’”*

— Mitchell, *Artificial Intelligence, a Guide for Thinking Humans* (2019)

— NARAYANAN & KAPOOR (2024)

*"Artificial intelligence, **AI for short, is an umbrella term for a set of loosely related technologies. ChatGPT has little in common with, say, software that banks use to evaluate loan applicants. Both are referred to as AI, but in all the ways that matter—how they work, what they're used for and by whom, and how they fail—they couldn't be more different.** [...]*

There is no way to answer that question, since there is no consensus about what is and isn't AI.”

— Narayanan and Kapoor, *AI Snake Oil* (2024)

— NARAYANAN & KAPOOR'S HEURISTIC

Is it AI ?

From my understanding of Narayanan and Kapoor

Creative effort / training. Does the task require human creative effort or training? If yes, and the machine can do it — it might be AI.

Machine learning. Was the behaviour directly specified in code, or did it emerge indirectly — from examples, from search ? (Second-wave AI *vs* GOFAI)

Autonomy. Does the system operate with some degree of flexibility and adaptability to the environment ?

“

AI is whatever hasn't been done yet.

Do we even care ?

NARAYANAN AND KAPOOR, *AI SNAKE OIL* (2024)

— ARTICLE 3(1) · KEY DEFINITION

The key legal definition: “AI System”

> *Article 3(1) – 'AI system' means* ***a machine-based system*** *that is* **designed to operate with varying levels of autonomy** *and that* **may exhibit adaptiveness after deployment**, *and that, for explicit or implicit objectives,* **infers, from the input it receives, how to generate outputs** *such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.*

Breaking it down: four conditions (*glose*)

(i) A machine-based system.

(ii) Designed to operate with varying levels of autonomy.

(iii) That *may* exhibit adaptiveness.

(iv) That, for explicit or implicit objectives, **infers**, ***from the input it receives, how to generate outputs such as*** predictions, content, recommendations or decisions that can influence physical or virtual environments.

“

The legislator has visibly preferred to take the risk of creating *a category that is too broad*, rather than one that is too narrow — because the narrowing can still happen downstream.

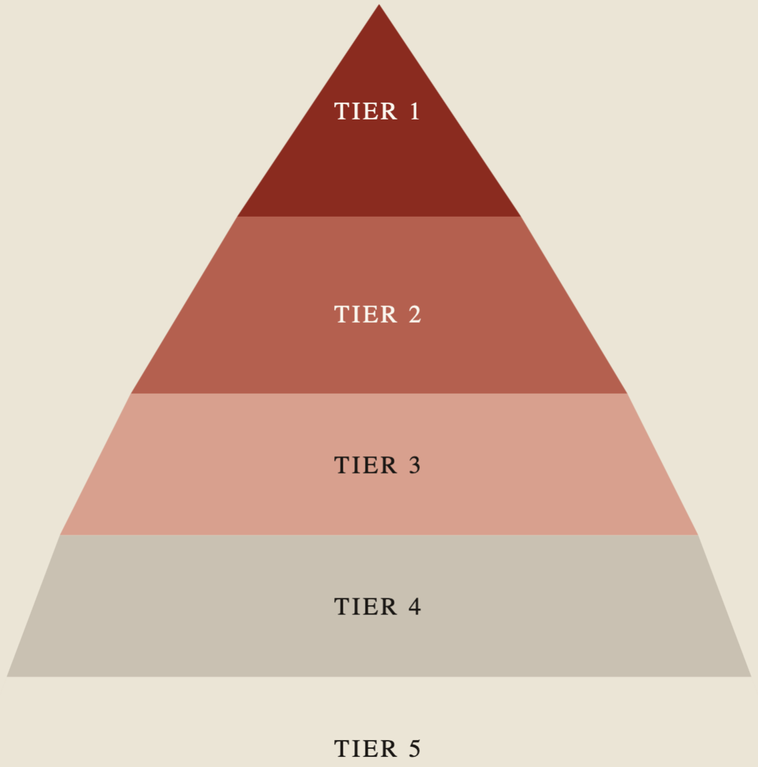
— NETTER (2024)

— PART FOUR —

The legal *obligations*

A risk-based approach

The pyramid of risks.



TIER 1 · ARTICLE 5

Unacceptable risk. Prohibited practices

Prohibited practices. Red lines.

TIER 2 · ARTS. 6–27 · ANNEX III

High-risk systems. Core compliance regime

Risk management system.

TIER 3 · ARTS. 51–55

GPAI models

Technical documentation and transparency, Intellectual property management provisions.

TIER 4 · ARTICLE 50

Limited-risk

Transparency obligations only.

TIER 5

Low / minimal risk

Unregulated. Residual category.

— TIER ONE · ARTICLE 5

Prohibited *practices*

Not subject to mitigation, not subject to conformity assessment. Prohibited.

Seven red lines.

(1) Using AI to manipulate human behavior in order to circumvent a person’s free will.

(2) Using AI to exploit the vulnerability of natural persons in light of their age, disability, or their social or economic situation.

.

(3) Social scoring

(4) Criminal risk assessments/predictions of natural persons without human involvement

(5) Emotion recognition in workplaces and educational institutions.

(6) Untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases

.

(7) Biometric categorisation inferring political opinion, religion, sexual orientation, race — "phrenological/physiognomic AI".

AI manipulation

(1) Using AI to **manipulate human behavior** in order to circumvent a person's free will.

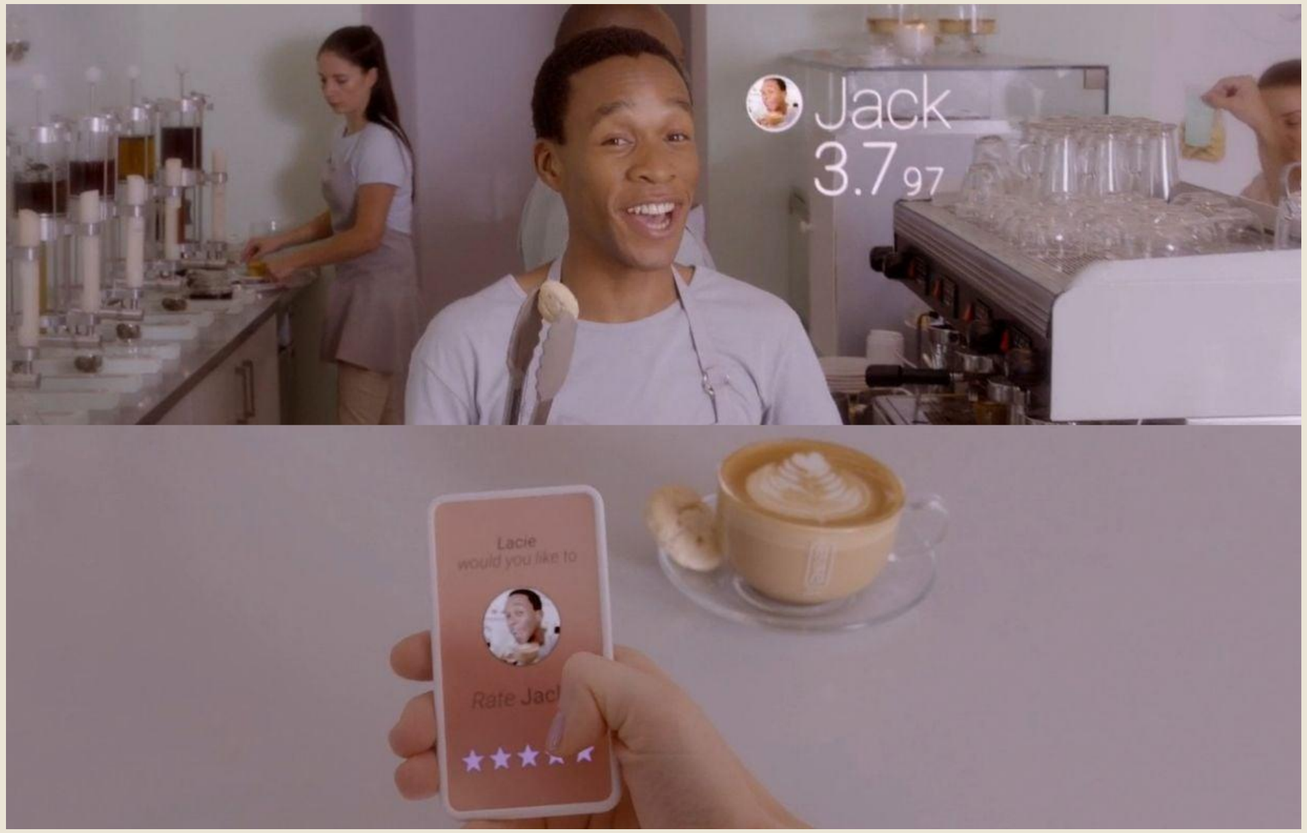
(2) to **exploit the vulnerability** of natural persons in light of their ***age***, disability, or their ***social*** or economic situation.

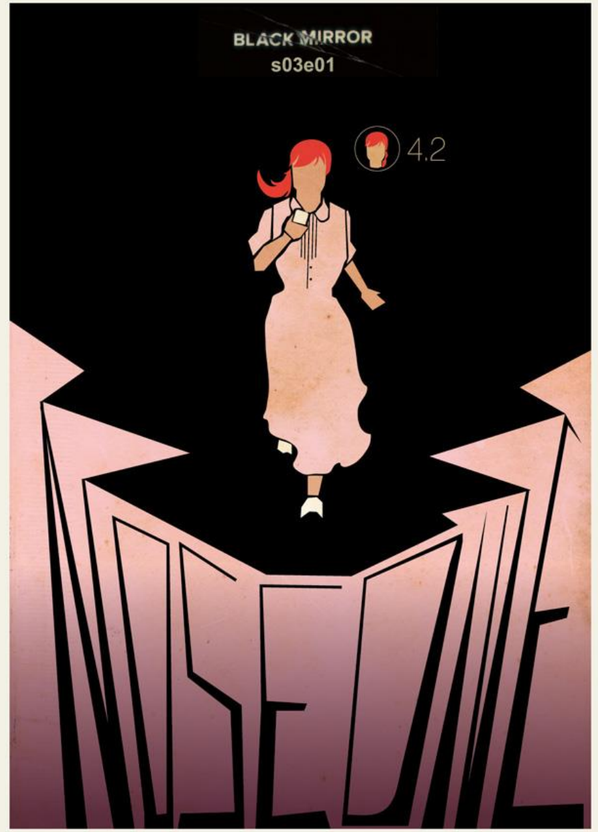
*the placing on the market, the putting into service or the use of an AI system that **deploys subliminal techniques beyond a person's consciousness** or **purposefully manipulative or deceptive techniques**, with the **objective**, or the **effect** of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;*

exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm

Social scoring

(3) **Evaluation or classification** of natural persons or groups of persons





— CAS PRATIQUE

Social scoring — the "Black Mirror" clause

— ARTICLE 5(1)(C) · TEXT

(c) the placing on the market, the putting into service or the use of AI systems for the ***evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics****, with the social score leading* ***to either or both*** *of the following:*

(i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts; ***that are unrelated to the contexts*** *in which the data was originally generated or collected;*

(ii) detrimental or unfavourable treatment of certain natural persons or groups of persons ***that is unjustified or disproportionate*** *to their social behaviour or its gravity.*

— REAL CASES

Netherlands — *Toeslagenaffaire* (2013–2019)

Child-benefit fraud algorithm; thousands of families, disproportionately of immigrant background, wrongly accused. Government fell, 2021.

France — CNAF fraud scoring

Allocations familiales risk-scoring algorithm using variables close to proxies for socioeconomic vulnerability (single parent, low income, fraud being presupposed rather than using AI to target non-recourse)

China — Experimental social credit scoring (SCS)

Punishment-reward system based on social behaviour (payment of debts ; playing video games). Issue. Reliability of informations re: this subject.

— CAS PRATIQUE

Predicting crime ?

— ARTICLE 5(1)(D) · TEXT

Article 5(D) *the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;*

— REAL CASES

COMPAS

Software used by courts in the US to predict risk of another crime (receidive)

Rationales for prohibition (*selected*) ?

Intervention vs prediction

Target-construct mismatch

Limiss to prediction

***Source**: Wang, Kapoor, Barocas and Narayanan, 2023 [https://predictive-optimization.cs.princeton.edu/]*

— CAS PRATIQUE

AI and Phrenology / Physiognomy

Enter pseudoscience

— ARTICLE 5(1)(G AND F) · TEXT

Article 5(1)(g). *AI systems used to* ***infer emotions of a natural person in the areas of workplace and education institutions****, except where the use of the AI system is intended to be put in place or into the market for* ***medical or safety reasons****;*

Article 5 (1)(f). *The placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation ;*

— REAL CASES

Hiring systems

See Stark and Hudson (2022) - Physiognomic Artificial Intelligence

Emotion recognition systems

See Lisa Feldman Barrett et al. (2017) How Emotions are Made: the Secret Life of the Brain (2017);

What consequences ?

> Non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to EUR **35 000 000** or, if the offender is an undertaking, **up to 7 % of its total worldwide annual turnover for the preceding financial year**, whichever is higher.”

— TIER TWO · ARTICLE 6 AND FOLLOWING

High-risk *AI Systems*

Subject to a conformity assessment

— TIER TWO · TWO GATEWAYS

Two types of high-risk systems

— ARTICLE 6(1)

Safety component of a regulated product

Toys, machinery, lifts, aviation, cars, medical devices — if an AI system is a safety component of a product already covered by Union product-safety legislation, it is high-risk.

— ARTICLE 6(2) · ANNEX III

Stand-alone high-risk systems

Exhaustively listed in Annex III — *eight domains* : biometrics · critical infrastructure · education · employment · essential services · law enforcement · migration & borders · justice and democracy.

The six families of high-risk obligation.

Notice — almost all are about technical functionality, not directly about safeguarding the rights they claim to protect.

01 Risk management system Art. 9	02 Data & data governance Art. 10	03 Technical documentation & logging Arts. 11–12
04 Transparency to deployers Art. 13	05 Human oversight Art. 14	06 Accuracy, robustness, cybersecurity Art. 15

Any "residual risk" must be judged *acceptable*.

Article 9(5). Acceptable by whom? — By the provider. This is the meta-regulatory turn.

Consequences ?

> *Non-compliance with any of the following provisions related to operators or notified bodies, other than those laid down in Articles 5, shall be subject to administrative fines of up to* **EUR 15 000 000** *or, if the offender is an undertaking,* **up to 3 % of its total worldwide annual turnover** *for the preceding financial year, whichever is higher.*

Article 9(5). Acceptable by whom? — By the provider*. This is the meta-regulatory turn.*

— PART FIVE —

Specifics — LLM *regulation*

What is an LLM in the language of the AI Act ? What obligations ? IP ?

What is an LLM for the purposes of the AI Act ?

(63) ***'general-purpose AI model'*** *means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale,* ***that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications****, except AI models that are used for research, development or prototyping activities before they are placed on the market ;*

(64) ***'high-impact capabilities'*** *means capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models ;*

(65) ***'systemic risk'*** *means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain ;*

(66) ***'general-purpose AI system'*** *means* ***an AI system which is based on a general-purpose AI model*** *and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems ;*

— QUALIFICATIONS, TRANSLATED

Model, system — why the distinction?

— GPAI **MODEL**

The foundation: the LLM.

GPT-5, Claude Opus, Gemini, Mistral Large, Llama. Obligations sit on the model provider: documentation, copyright, training summaries.

e.g. Anthropic · OpenAI · Google DeepMind · Mistral

— GPAI **SYSTEM**

The chatbot/UI on top.

ChatGPT, Claude.ai, the API endpoint exposed to users. System-level obligations: transparency, watermarking, disclosure. High-risk overlay when deployed in a high-risk context.

e.g. ChatGPT · Claude.ai · Copilot

Primary obligations for GPAI model providers.

Draw up and maintain technical documentation covering training, testing, and evaluation. Idea : help regulator + providers downstream.

Comply with EU copyright law — in particular, respect Article 4(3) DSM opt-outs (see below).

Publish a sufficiently detailed summary of the content used for training, before placing the model on the market.

— ARTICLE 51(2) · THE SYSTEMIC-RISK PRESUMPTION

10^{25} floating-point operations

MODELS TRAINED ABOVE THIS THRESHOLD ARE PRESUMED TO POSE SYSTEMIC RISK — TRIGGERING TRIGGERING EVALUATIONS, ADVERSARIAL TESTING, INCIDENT REPORTING, CYBERSECURITY. ALL SELF-ALL SELF-ASSESSED.

Secondary obligations for GPAI model providers with *systemic risks*

Cf. definition of systemic risk - those that pose systemic risk due to their high impact capabilities are subject to additional obligations:

Conduct model evaluations, incl. adversarial testing.

Assessing and mitigating systemic risks

Report on serious incidents

Ensure an adequate level of cybersecurity

Transparency obligations: three cases.

(1) General **transparency** of "HCI"

> *Providers shall ensure that AI systems intended to interact directly with natural persons are* ***designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use****.*

Transparency obligations: three cases.

(2) The (technical) watermarking clause

> *Providers of AI systems,* ***including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated****. Providers shall ensure their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards.* ***This obligation shall not apply to the extent the AI systems perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof,*** *or where authorised by law to detect, prevent, investigate or prosecute criminal offences.*

Is this currently respected ? But consider implementation timeline
Question about predicates (back to grammar) ; is this just a technical requirement ?
Is this even technically feasible ? (I do not know)

Transparency obligations: three cases.

(3) Deepfakes – is this enough ?

> ***Deployers of an AI system that generates or manipulates image, audio*** *or* ***video*** *content* ***constituting a deep fake, shall disclose that the content has been artificially generated or manipulated****. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offence. Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work. Deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated. [...]*

Transparency obligations: three cases.

(3 cont'd) Manipulation of the public

> ***Deployers of an AI system that generates or manipulates image**, **audio** or **video** content **constituting a deep fake**, **shall disclose that the content has been artificially generated or manipulated**. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offence. Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work. **Deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated**. […]*

— PART SIX —

LLMs and *intellectual property*.

Three questions · who can own an AI system · who owns the output · is training infringement?

Three questions about AI and IP.

(1) Can you protect an AI system you are developing with intellectual property ?

(2) Who, if anyone, *owns* the output ?

(3) Is training on copyrighted content infringement ?

(1) Protecting the system : Patent law ?

Under patent law: algorithms usually excluded from protection because “pure abstract methods”

But patentability may arise if demonstrated a connection to a material object in the “real” world.

Conditions for patentability — The application must be (1) Novel (2) Inventive (3) Industrially applicable

(1) Protecting the system : Copyright ?

— (I) CONCRETE EXPRESSIONS

Graphical interface for instance (see C-393/09, BSA case); object and source code of the computer program but not the mere algorithm (too abstract).

— (II) ORIGINALITY

“an intellectual creation of the author reflecting his personality and expressing his free and creative choices” **In practice: low threshold for originality.**

Painer, C-145/10 ; Art. L. 112-1 / L. 112-2 CPI · Cass. Ass. Plén. 7 mars 1986 · Paris, 8 déc. 2023, n° 21/19696. n° 21/19696.

Example under French Law :

Article L. 112-1 of the French Intellectual Property Code: The provisions of this Code shall protect the rights of authors in all works of the mind, whatever their kind, form of expression, merit or purpose.

Article L. 112-2 of the French Intellectual Property Code: The following, in particular, shall be considered works of the mind within the meaning of this Code [...] Software, including the preparatory design material.

“

Copyright law requires the work at issue to show *authorship* ; the personal stamp of the author. The author is considered to be a physical person, especially in the civil law tradition, where copyright protection is viewed as a natural right, granted to the author to protect emanations of their personality

IN SUM – VANHERPE, 2025, P. 216

(2) Who owns the output ? – Three hypotheses

— ANTHROPIC · CLAUDE

The AI itself ? Impossible

Legal personality needed to be vested rights.

ASSIGN-TO-USER

— OPENAI · CHATGPT

The AI system Provider ? Unlikely

Substantial contribution to the output as they programmed the system

ASSIGN-TO-USER

— YOU & ME?

The AI user/coder ? Probably

The user/coder, by contractual assignment from the provider.

NO CLAIM

(2) Who owns the output — per the T&Cs

Contractual assignation of rights.

— ANTHROPIC · CLAUDE

User retains inputs.

Anthropic hereby assigns to Customer its right, title and interest (if any) in and to Outputs. Enterprise tier: “Anthropic may not train models on Customer Content from Services.”

ASSIGN-TO-USER

— OPENAI · CHATGPT

Ownership of content.

As between you and OpenAI, and to the extent permitted by applicable law, you (a) retain your ownership rights in Input and (b) own the Output. We hereby assign to you all our right, title, and interest, if any, in and to Output. Free tier may be used for model improvement — opt-out available.

ASSIGN-TO-USER

— GOOGLE · GEMINI

"Google does not claim ownership of generated content."

As between you and Google, Generated Output is owned by the user/customer. Google does not assert any ownership rights in new intellectual property created in the Generated Output. Free-tier conversations used for training by default; Workspace & Enterprise data are not.

NO CLAIM

(3) Is training infringement ? Two possibilities

— ARTICLE 3 DSM

Scientific research TDM

1. Member States shall provide for an exception to the rights provided for in Article 5(a) and Article 7(1) of Directive 96/9/EC, Article 2 of Directive 2001/29/EC, and Article 15(1) of this Directive for reproductions and extractions made by *research organisations and cultural heritage institutions* in order to carry out, for the purposes of scientific research, text and data mining of works or other subject matter to which they have lawful access.

— ARTICLE 4 DSM

General / commercial TDM

1. Member States shall provide for an exception or limitation … for reproductions and extractions of *lawfully accessible* works and other subject matter for the purposes of text and data mining.

3. The exception or limitation provided for in **paragraph 1 shall apply on condition that the use of works and other subject matter referred to in that paragraph has not been *expressly reserved* by their rightholders in an appropriate manner, such as machine-readable means in the case of content made publicly available online.**

Article 53(1)(c) AI Act presupposes Article 4(3) DSM applies to LLM training. Paired with Article 53(1)(d) — the training-content summary — this could become a significant disclosure regime. If the template bites.

(3) Is training infringement ? Implicit AI Act wording

> Article 53(1)(c)(d) AI Act — *GPAI Model providers shall:*
>
> **(c)** *put in place a policy to comply with Union law on copyright and related rights,* ***and in particular to identify and comply with****, including through state-of-the-art technologies,* ***a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790****;*
>
> **(d)** *draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office.*

— CAS PRATIQUE

(3) Is training infringement ? Litigations

— REAL CASES

Germany — *GEMA v. OpenAI* (2025)

Munich Regional Tribunal – GEMA v. OpenAI (OpenAI lost)

Reproduction of famous song lyrics in output by ChatGPT – infringement of copyright by reproducing the work and communicating it to the public

France — SNE, SGDL, et SNAC c. Meta (2025) - Pending

TJ Paris, 3e chambre (IP)

Allegations : Meta infringing copyright to train its model LLAMA + "economic parasitism" (art. 1240 Civil Code).

(3) Is training infringement ? AI Act provisions

> Article 53(1)(c)(d) AI Act — *GPAI Model providers shall:*
>
> **(c)** *put in place a policy to comply with Union law on copyright and related rights,* ***and in particular to identify and comply with****, including through state-of-the-art technologies,* ***a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790****;*
>
> **(d)** *draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office.*

— PART SEVEN —

Monitoring and Enforcement of the AI Act

Enforcement · meta-regulation · technical standardisation · the question of political capture.

THE THESIS.

AI regulation in Europe is *product* regulation — not a rights-based regime.

Like toys, lifts, medical devices. A compliance machine built on the "New Legislative Framework" — not like the GDPR.

Enforcement of the Act - une *usine à gaz*.

The AI Act's enforcement architecture, schematised. Overlapping competences at Union and Member State level.

A "product" regulation – New Legislative Framework

(1) Member states must designate a "MSA" (market surveillance authority).

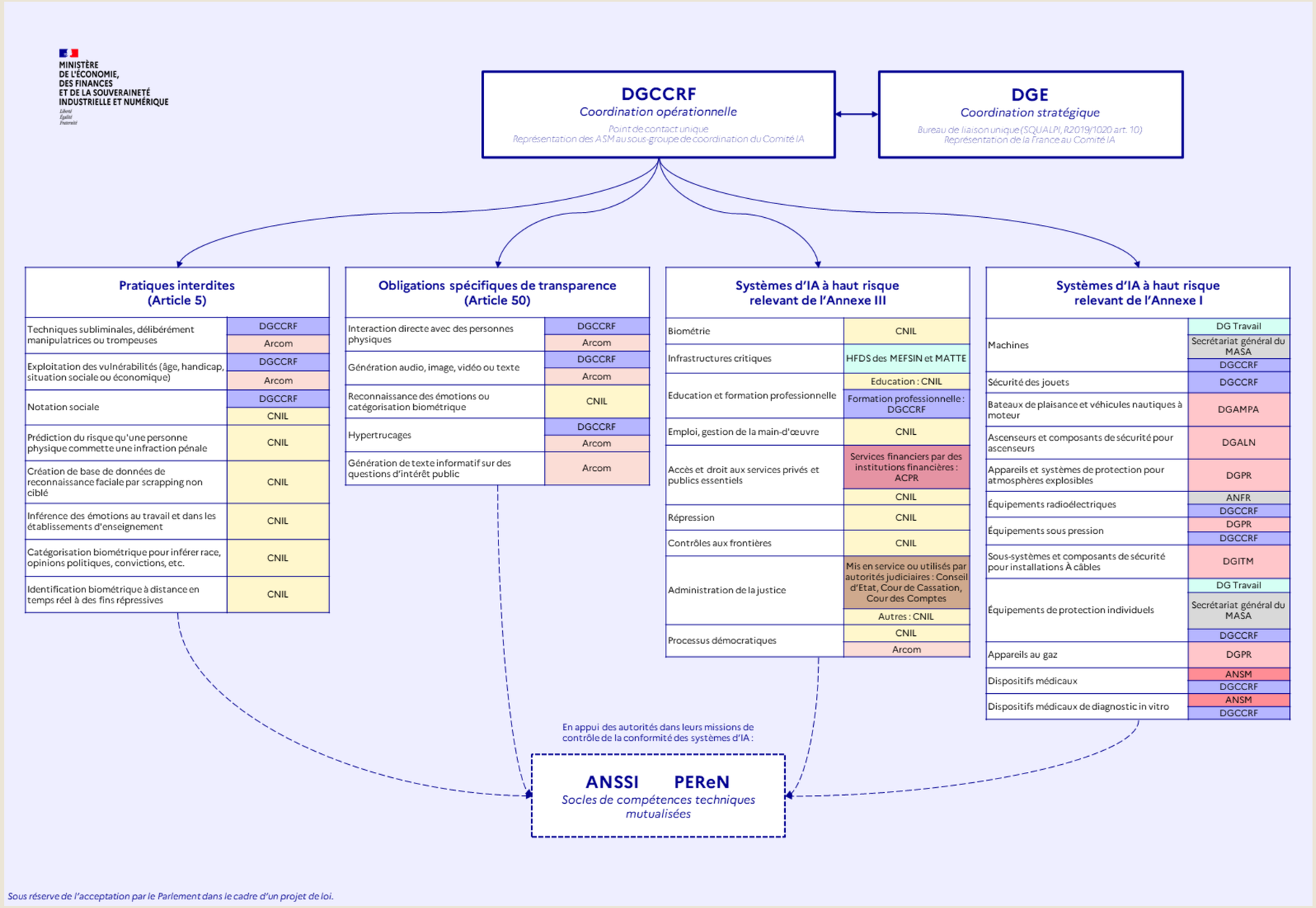
(2) AI providers to self-assess their conformity and affix CE marking (art. 43, art. 48).

(3) A mere “surveillance role”

(4) Issues with NLF.

(1) Market surveillance authority designation

> Article 70 - *Each Member State shall establish or designate as national competent authorities* [...] *at least* ***one market surveillance authority*** *for the purposes of this Regulation. Those national competent authorities shall exercise their powers* ***independently, impartially and without bias*** *so as to* ***safeguard the objectivity of their activities and tasks****, and to ensure the application and implementation of this Regulation. The members of those authorities shall refrain from any action incompatible with their duties. Provided that those principles are observed, such activities and tasks may be performed by one or more designated authorities, in accordance with the organisational needs of the Member State.*


MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE
Liberté
Égalité
Fraternité
DGCCRF
Coordination opérationnelle
Point de contact unique
Représentation des ASM au sous-groupe de coordination du Comité IA
DGE
Coordination stratégique
Bureau de liaison unique (SQUALPI, R2019/1020 art. 10)
Représentation de la France au Comité IA
Pratiques interdites (Article 5)
Techniques subliminales, délibérément manipulatrices ou trompeuses
DGCCRF
Arcom
Exploitation des vulnérabilités (âge, handicap, situation sociale ou économique)
DGCCRF
Arcom
Notation sociale
DGCCRF
CNIL
Prédiction du risque qu'une personne physique commette une infraction pénale
CNIL
Création de base de données de reconnaissance faciale par scrapping non ciblé
CNIL
Inférence des émotions au travail et dans les établissements d'enseignement
CNIL
Catégorisation biométrique pour inférer race, opinions politiques, convictions, etc.
CNIL
Identification biométrique à distance en temps réel à des fins répressives
CNIL
Obligations spécifiques de transparence (Article 50)
Interaction directe avec des personnes physiques
DGCCRF
Arcom
Génération audio, image, vidéo ou texte
DGCCRF
Arcom
Reconnaissance des émotions ou catégorisation biométrique
CNIL
Hypertrucages
DGCCRF
Arcom
Génération de texte informatif sur des questions d'intérêt public
Arcom
Systèmes d'IA à haut risque relevant de l'Annexe III
Biométrie
CNIL
Infrastructures critiques
HFDS des MEFSIN et MATTE
Education et formation professionnelle
Education : CNIL
Formation professionnelle : DGCCRF
Emploi, gestion de la main-d'œuvre
CNIL
Accès et droit aux services privés et publics essentiels
Services financiers par des institutions financières : ACPR
CNIL
Répression
CNIL
Contrôles aux frontières
CNIL
Administration de la justice
Mis en service ou utilisés par autorités judiciaires : Conseil d'Etat, Cour de Cassation, Cour des Comptes
Autres : CNIL
Processus démocratiques
CNIL
Arcom
Systèmes d'IA à haut risque relevant de l'Annexe I
Machines
DG Travail
Secrétariat général du MASA
DGCCRF
Sécurité des jouets
DGCCRF
Bateaux de plaisance et véhicules nautiques à moteur
DGAMPA
Ascenseurs et composants de sécurité pour ascenseurs
DGALN
Appareils et systèmes de protection pour atmosphères explosibles
DGPR
Équipements radioélectriques
ANFR
DGCCRF
Équipements sous pression
DGPR
DGCCRF
Sous-systèmes et composants de sécurité pour installations À câbles
DGITM
Équipements de protection individuels
DG Travail
Secrétariat général du MASA
DGCCRF
Appareils au gaz
DGPR
Dispositifs médicaux
ANSM
DGCCRF
Dispositifs médicaux de diagnostic in vitro
ANSM
DGCCRF
En appui des autorités dans leurs missions de contrôle de la conformité des systèmes d'IA :
ANSSI PEReN
Socles de compétences techniques mutualisées
Sous réserve de l'acceptation par le Parlement dans le cadre d'un projet de loi.

— THE HIGH-RISK PROVIDER'S CHOICE

(2) Three options to demonstrate conformity.

Remember high-risk AI models ? They have to assess their conformity to the requirements of the AI Act in case they get controlled.

— DOOR 1

Self-assess conformity to reqt's

The provider self-assesses his conformity – risky choice given legal uncertainty and hefty fines risked.

LIABILITY RISK

— DOOR 2

Notified body assessment

Contract an accredited private third-party assessor. Mandatory only for certain biometric systems. In any case : costly (paid service).

PRIVATE · PAID

— DOOR 3

Follow the harmonised standard

Obtain the Article 41 *presumption of conformity* . *De facto*, everyone will do this. Private standard drafted by ESO CEN-CENELEC.

DE FACTO LAW

“

The AI Act's regulatory framework delegates many crucial functions — and thus considerable discretionary power — to the very actors *whom the regime purports to regulate* .

— YEUNG & SMUHA (2025)

— THE QUIET REALITY OF ENFORCEMENT

The overwhelming majority of high-risk providers will *self-assess*.

Sign the declaration. Affix the CE mark. Notify the public register. No pre-market approval. Permissive, not precautionary.

(3) Market surveillance – little remedies for affected people

Recall the goal of the Regulation : Article 1 « *The purpose of this Regulation is to* **improve the functioning of the internal market** *and promote the uptake of* **human-centric and trustworthy artificial intelligence (AI)**, *while ensuring a* **high level of protection of health, safety, fundamental rights enshrined in the Charter** , *including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union* **and supporting innovation** ».

Very meager rights for affected individuals : Article 85 - *Without prejudice to other administrative or judicial remedies, any natural or legal person having grounds to consider that there has been an infringement of the provisions of this Regulation may submit complaints to the relevant market surveillance authority.*

In accordance with Regulation (EU) 2019/1020, such complaints shall be taken into account for the purpose of conducting market surveillance activities, and shall be handled in line with the dedicated procedures established therefor by the market surveillance authorities.

(4) Critique of the NLF regime

(a) Ineffective (see Larson and Jordan (2018) International Review of Administrative Sciences, 85(4), 763–79).
(b) Dangerous (see PIP scandal).
(c) Testing of documentation rather than the product.
(d) Standardization : a political act, *not* a technical one.

“

Even when technical standards for software are useful, they are *ripe for regulatory capture* .

— JOANNA BRYSON · QUOTED IN YEUNG & SMUHA

Selected references

P. DEWITTE, « AI Meets the GDPR: Navigating the Impact of Data Protection on AI Systems », *in* Nathalie A. SMUHA (dir.), *AI Meets the GDPR*, Cambridge University Press, coll. Cambridge Law Handbooks, 2025.

N.A. SMUHA, K. YEUNG, « The European Union's AI Act: Beyond Motherhood and Apple Pie? », *in* Nathalie A. SMUHA (dir.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge University Press, coll. Cambridge Law Handbooks, 2025.

J. VANHERPE, « Artificial Intelligence and Intellectual Property Law », *in* Nathalie A. SMUHA (dir.), The Cambridge Handbook of the Law, Ethics and Policy of Artificial IntelligenceCambridge University Press, coll. Cambridge Law Handbooks, 2025

E. NETTER, « Définir l'intelligence artificielle, un défi impossible ? La première pièce du puzzle », *RDSS. Revue de droit sanitaire et social*, *Sirey ; Dalloz* , 2024, n°5, p. 747.

A. NARAYANAN, S. KAPOOR, *AI snake oil: what artificial intelligence can do, what it can't, and how to tell the difference*, Princeton, Etats-Unis d'Amérique, Princeton University Press, 2024.

A. WANG et al., « Against Predictive Optimization: On the Legitimacy of Decision-Making Algorithms that Optimize Predictive Accuracy », SSRN Scholarly Paper, 4 oct. 2022, en ligne sur : https://papers.ssrn.com/abstract=4238015.

M. MITCHELL, *Artificial intelligence: a guide for thinking humans*, United Kingdom, Pelican, 2019

L. STARK, J. HUTSON, « Physiognomic Artificial Intelligence », SSRN Scholarly Paper, 20 sept. 2021, en ligne sur : https://papers.ssrn.com/abstract=3927300.