L'Europe comme architecte d'un "AI Rulebook" complet

May 1, 2025 • 43 min read

Gouvernance des données | Gouvernance de l'IA | Avantage concurrentiel réglementaire

L'Union européenne n'a pas créé une seule loi sur l'IA. Elle a plutôt mis en place un ensemble cohérent de textes qui forment un AI rulebook.

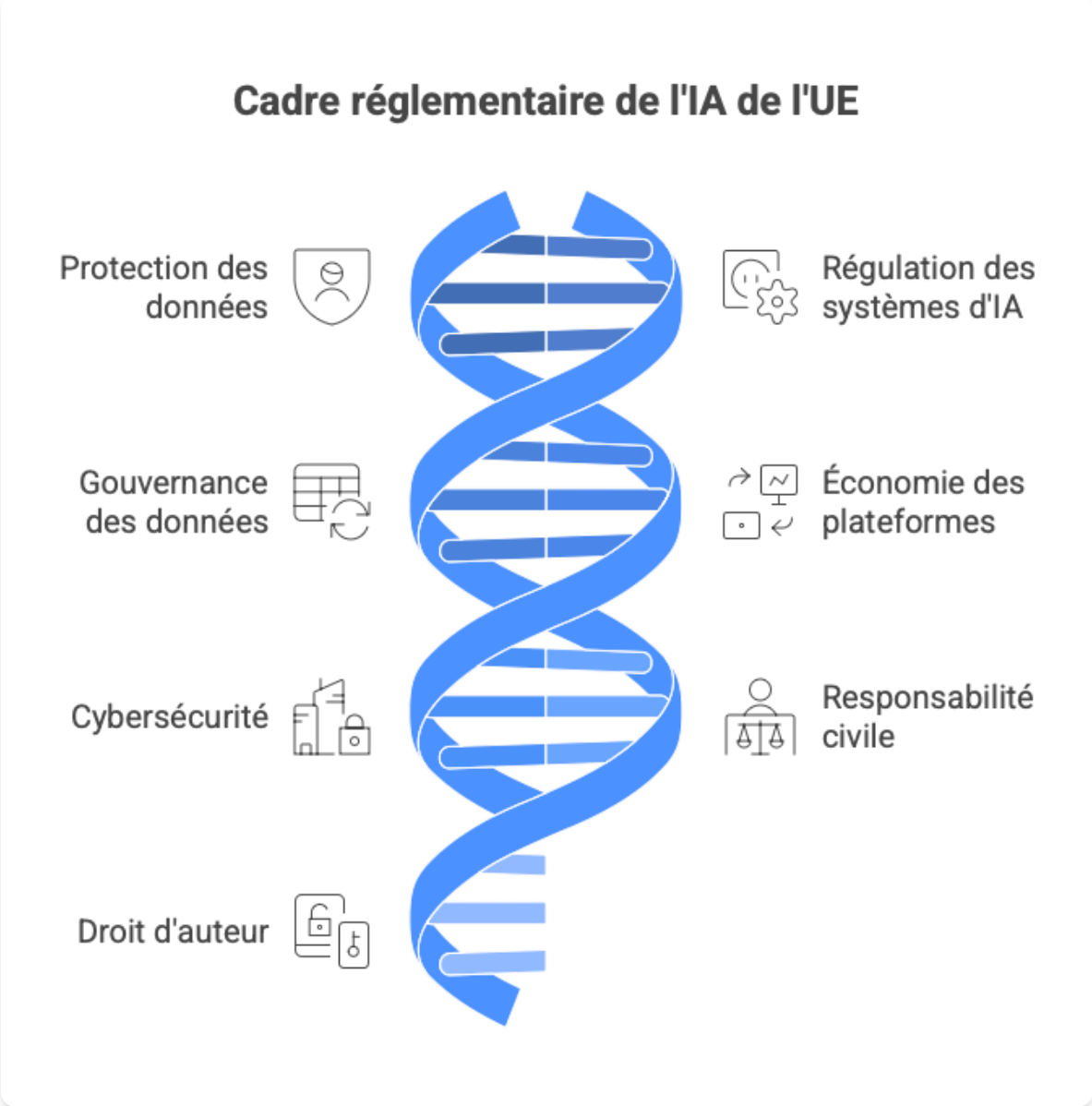
Ceux ci regroupent:

- **Protection des personnes et de leurs données** : RGPD, DPIA, Directive police et justice (LED).
- **Régulation des systèmes d'IA** : AI Act (systèmes d'IA, modèles de base, fondations, usages interdits ou à haut risque).
- **Gouvernance et circulation des données** : Data Act, Data Governance Act, espaces de données sectoriels (EHDS en santé, etc.).
- **Plateformes & économie des écosystèmes** : DSA (services numériques) et DMA (gatekeepers et interopérabilité).
- **Cybersécurité & sécurité produit** : CRA (Cyber Resilience Act), NIS2 et DORA pour la finance.
- **Responsabilité civile** : nouvelle directive relative à la responsabilité du fait des produits (PLD 2024/2853).
- **Droit d'auteur & Text and Data Mining (TDM)** : Directive 2019/790 et exceptions de TDM pour l'entraînement des modèles.
- Notons que le projet de **directive sur la responsabilité de l'IA (AI Liability Directive)** a finalement été abandonné en 2025, la Commission

considérant que le couple AI Act + PLD + droit national fournit déjà une base robuste.

Ainsi, ce rulebook exige des organisations qu'elles transforment la complexité réglementaire en un avantage concurrentiel tangible, indispensable pour rester compétitives en IA, plutôt que de la considérer simplement comme un facteur de coût.

> *Vu d'un autre continent, ils disent : "Votre AI Rulebook, c'est compliqué !"*
> *Je leur réponds : "C'est notre avantage : on a déjà les règles, pas vous !"*



Ce document présente de façon simplifiée les principaux arguments généralement avancés par une partie des experts européens en faveur des réglementations encadrant l'IA.

Opportunités offertes par la réglementation IA européenne

La réglementation IA renforce la confiance et une adoption accrue avec des systèmes d'IA conformes perçus comme plus sûrs et fiables et des utilisateurs (entreprises, citoyens, administrations) moins réticents à adopter des solutions IA. Elle donne un avantage compétitif pour les entreprises européennes grace à un cadre clair permettant aux entreprises de développer des produits dès le départ conformes, sans risque juridique majeur : l'IA "made in Europe" devient un label de qualité et de conformité, comparable à celui du RGPD. Elle ouvre de nouveau marchés et métier (exper en conformité IA, auditeur, specialiste en gouvernance...). C'est aussi un gage de sécurité juridique et prévisibilité pour les investisseurs (les règles sont claires, harmonisées et applicables dans tous les États membres). Ce constat n'est pas nouveau, il est partagé par de nombreux experts tels que Sandra Wachter (Wikipédia), Mariarosaria Taddeo (Wikipédia), Andréa Bertolini (TheRecursive.com) ou encore Lilian Edwards (adalovelaceinstitute.org, adalovelaceinstitute.org)

Quelque exemples pertinents

- Le rapport Organisation for Economic Co-operation and Development (OECD) intitulé *"Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses"* montre que la réglementation peut être mobilisée comme un levier pour encourager l'innovation et non seulement pour la contenir. (OECD)
- L'article "How regulation and standards be a driver of innovation?" (sur LinkedIn) affirme explicitement que les **règlementations et les normes peuvent être un moteur d'innovation**. (LinkedIn)
- Le rapport Ada Lovelace Institute *"Regulate to innovate"* (2021) pose que la réglementation peut fournir des règles claires et un environnement sûr, ce qui permet d'embrasser des technologies comme l'IA "sur des bases bénéfiques pour les personnes et la société". (adalovelaceinstitute.org)
- Une étude sur les standards et l'innovation montre que la relation entre réglementation/standards et dépenses R&D est **positive** dans certains contextes. (ScienceDirect)

- L’hypothèse dite de Hypothèse de Porter (Porter hypothesis) affirme que des réglementations environnementales strictes peuvent stimuler l’innovation et la compétitivité. (Wikipédia)
- “Regulation and regulators need to … help to create an environment that is encouraging of innovation, for example by levelling the playing field through standards, or giving clarity that enables investment cases” (dans un rapport du gouvernement britannique sur les innovations technologiques). (Gouvernement du Royaume-Uni)
- “We find that restrictiveness can have both a negative and positive relationship with innovation output depending on … regulatory uncertainty.” (étude M. Park, 2025) (pubsonline.informs.org)
- “How regulation can boost the EU innovation?” (article de l’European Federation of Pharmaceutical Industries and Associations – EFPIA) : explique comment une réglementation bien conçue dans le secteur pharmaceutique peut accélérer l’innovation. (EFPIA)

Ce qu’on peut en retirer

Quand bien même le lien réglementation / innovation n’est pas automatique : il dépend de comment la réglementation est conçue (clarté, prévisibilité, normes, soutien à l’innovation) plutôt que d’être simplement plus stricte. Une réglementation bien conçue peut réduire l’incertitude juridique, créer un terrain de jeu clair, encourager les investissements et soutenir la confiance des utilisateurs, ce qui stimule l’innovation. Et cela s’applique très bien au cas de l’IA : un cadre réglementaire clair comme AI Act peut être vu comme une opportunité pour les entreprises qui s’y préparent tôt et créent des offres conformes, innovantes, et exportables.

Un dernier coup de marteau pour enfoncer le clou des opportunité de l'AI RuleBook : les enseignements des secteurs régulés pour la gouvernance de l’IA en Europe

L’adoption de l’AI Act par l’Union européenne s’inscrit dans une tradition de régulation qui a façonné d’autres industries fortement technologiques, telles que l’aéronautique, l’automobile ou la santé. Plusieurs experts et institutions soulignent que ces secteurs offrent des enseignements directs sur les dangers d’une approche laxiste ainsi que sur les opportunités qu’ouvre une

régulation anticipée. Les cas du **Boeing 737 MAX** et du **scandale Volkswagen Dieselgate** sont particulièrement mobilisés dans les débats européens pour illustrer les conséquences d'une absence d'encadrement adéquat, d'un contournement de normes ou d'un déficit de supervision.

L'aviation civile est souvent considérée comme la référence mondiale en matière de régulation orientée sécurité : certification stricte, enquêtes systématiques, normes internationales (ICAO, FAA, EASA). Ce modèle est explicitement cité par des experts de la régulation de l'IA comme un exemple de gouvernance efficace. Ici le crash du Boeing 737 MAX(2018–2019) est un cas d'école illustrant de ce qui peut arriver lorsque la supervision d'un logiciel critique est insuffisante, les processus de certification sont affaiblis et qu'un fabricant contourne certaines étapes pour accélérer la mise sur le marché. Pour l'IA cela signifie que les obligations d'évaluation, de documentation technique, de gestion des risques et de qualité des données sont moins une contrainte qu'un **socle de confiance**, nécessaire à l'adoption de systèmes à haut risque (mobilité autonome, santé, infrastructures critiques).

Dans l'automobile, le scandale Volkswagen / Dieselgate est régulièrement cité pour illustrer les risques liés à un système logiciel conçu pour détecter les conditions de test afin de modifier son comportement — un mécanisme qui présente une analogie directe avec les systèmes d'IA pouvant adapter dynamiquement leur fonctionnement. Ce scandale sert donc de cas d'avertissement : ne pas intégrer les exigences réglementaires dans la conception d'un système logiciel conduit non seulement à des sanctions, mais aussi à une perte durable de confiance et de compétitivité.

> *CTO de Volwagen : "Grâce à l'IA Act, nous garantissons désormais une transparence totale : fini les erreurs du Dieselgate. D'ailleurs, nos émissions sont tellement propres que même les vaches cherchent à nous imiter. Si vous sentez du méthane, rassurez-vous : ce n'est plus nos moteurs... juste la ferme d'à côté."*

Ces exemples ne sont pas de simples métaphores : ils sont utilisés dans la littérature scientifique, les rapports de policy-making et l'analyse juridique pour défendre l'idée que la régulation de l'IA n'est pas une barrière à

l’innovation mais une condition nécessaire pour son adoption sûre, généralisée et durable.

RGPD & DPIA : le duo qui vous rappelle que "respecter la vie privée", ce n'est pas optionnel

Le RGPD (Règlement Général sur la Protection des Données) demeure le pivot dès qu'un système d'IA traite des données personnelles. Points critiques pour les projets IA :

- **Licéité du traitement** : il faut rattacher tout cas d'usage de l'IA à une **base légale** (contrat, obligation légale, intérêt légitime, consentement, etc.).
- **Finalité et minimisation** : L'IA qui collecte toutes les données sans but précis pose problème. Il faut des finalités claires et des données limitées.
- **Profilage & décisions automatisées** : une personne a le droit de ne pas être soumise à une décision **uniquement automatisée** produisant des effets juridiques ou similaires importants, sauf exceptions encadrées, avec obligation de prévoir :
  - intervention humaine,
  - explications compréhensibles,
  - possibilité de contester la décision. (RGPD)

  > *Flashé par un radar automatique, Eric a aussitôt réclamé son droit au RGPD à " une intervention humaine " — le policier a donc dû lui expliquer en personne que, oui, 56 km/h, c'est toujours 56 km/h. Rassuré, Eric a alors exercé son droit de contestation... avant d'admettre que le radar et l'humain étaient d'accord à l'unanimité.*
- **Transparence et information** : Plus une IA est opaque, plus il faut expliquer son traitement et ses conséquences.

Quant à la DPIA (Data Protection Impact Assessment), elle impose une analyse d'impact en cas de risque élevé pour les droits et libertés. Les traitements IA typiques y tombent presque "par design"; que ce soit le *scoring* (clients, employés, étudiants...) à grande échelle, l'utilisation de

données sensibles (santé, biométrie, orientation, etc.), la surveillance (analyse vidéo, capteurs, IoT...) ou encore les décisions automatisées produisant des effets significatifs. (RGPD)

... et cela peut coûter cher ...

> *H&M a stocké et exploité les données sensibles des employés (maladies, absences, événements privés, etc.) sur de larges effectifs dans son centre de service. (Herbert Smith Freehills). Cela a été jugé **excessif** et non conforme au RGPD, qui exige notamment que les données soient collectées pour des finalités précises, pertinentes et limitées. Résultat : l'autorité allemande de protection des données de Hambourg a infligé une amende colossal de 35,3 millions d'euros. (EDPB)*

Nous ne sommes pas dénués d'informations ; les autorités (comme la CNIL) ont publié des **guides "DPIA"**, où les traitements par IA apparaissent souvent (notamment en RH, en scoring, en géolocalisation massive, etc.). (cnil.fr)

Concrètement, pour une organisation, cela implique de :

- **Cartographier les cas d'usage de l'IA** concernant des données personnelles (entraînement, inférence, monitoring).
- **Segmenter** :
  - "low risk / low data" (ex. détection de spams sur emails pro peu sensibles),
  - "high risk" (profilage RH, scoring de crédit, tri des candidatures, etc.).
- **Industrialisez les DPIA** : élaborez des modèles de DPIA préremplis pour certains cas d'IA, et mettez en place une revue croisée entre le Data Protection Officer (DPO), le juridique, les experts data/IA et le métier.
- Mettre en place un **registre des traitements basés sur l'IA**, en cohérence avec le registre RGPD classique.

Sous cette apparente lourdeur, une application rigoureuse du RGPD devient un véritable atout de valeur, elle permet de:

- Concevoir des produits d'IA "**privacy by design**", réutilisables dans des secteurs très réglementés (santé, finance, secteur public).
- Intégrer la protection de la vie privée et les contraintes de profilage dans les **features** : explication de la décision, contrôle utilisateur, paramétrage du niveau de personnalisation.
- Vendre des services autour du DPIA IA (audit, templates, coaching des équipes produit) et des briques technologiques (pseudonymisation, anonymisation, données synthétiques, gestion des préférences).

AI Act : parce que "structurer, classifier et gouverner l'IA", ce n'est plus une recommandation - c'est la règle.

L'**AI Act** est une approche **par niveau de risque** : (Stratégie numérique de l'UE)

- **Pratiques interdites** (risque inacceptable) : manipulation subliminale, social scoring par les pouvoirs publics sur des critères sensibles, certains usages de la reconnaissance biométrique à distance, etc.
- **Systèmes à haut risque** : IA utilisée dans l'éducation, l'emploi, le crédit, l'accès à des services essentiels, les dispositifs médicaux, les infrastructures critiques, la justice et l'application de la loi.
- **Risque limité** : obligation de transparence (chatbots, deepfakes, systèmes d'IA génératifs qui produisent du contenu).
- **Risque minimal** : filtres de spam, IA embarquée peu sensible, etc., avec très peu d'obligations.

Pour les systèmes à haut risque, il faut appliquer un véritable système de management de la qualité en IA : gestion des risques sur l'ensemble du cycle de vie, exigences de qualité des données, documentation technique précise, journalisation automatique, supervision humaine, gouvernance claire, robustesse, résilience et cybersécurité.

Pour les entreprises, l'AI Act requiert un véritable changement culturel. Il faut faire un inventaire de tous les systèmes d'IA, pas seulement des projets de data science, mais aussi des moteurs de recommandation, de l'IA embarquée dans des produits, des assistants virtuels, des scoring internes, etc.

> *...bref, un vrai ménage de printemps numérique - fini l'IA de garage bricolée dans la cave de l'entreprise par un vieux barbu qu'on ne sort jamais !*

À l'instar du RGPD, la maîtrise de l'AI Act crée de la valeur : produits d'IA adaptés aux secteurs réglementés, services d'accompagnement des clients (audit de conformité, *AI governance as a service*) et outils logiciels (registre d'IA, documentation automatisée, monitoring des risques, red teaming, simulation). La contrainte imposée demande de renforcer la robustesse dans un cadre établi et finalement de renforcer la confiance client.

Data Act, Data Governance Act & espaces de données : l'oxygène de l'IA

Les données sont le nerf de la guerre en IA. Le **Data Act** vise à clarifier "qui peut faire quoi avec quelles données", en particulier pour les **données générées par des objets connectés et les services associés**. (Stratégie numérique de l'UE)

Ainsi **les utilisateurs** (consommateurs comme entreprises) doivent pouvoir accéder aux données générées par leurs machines, équipements, véhicules, etc., et les partager avec des tiers (y compris des fournisseurs de services d'IA), **les contrats B2B** ne peuvent plus contenir des clauses abusives empêchant le partage de données ou captant toute la valeur côté du fabricant et **les fournisseurs** de services cloud doivent permettre un changement de fournisseur (cloud switching) avec moins de frictions techniques et financières.

Ce texte est fondamental pour l'ensemble des cas d'usage de l'IA dans l'industrie, l'énergie, la mobilité, l'agriculture de précision et d'autres secteurs.

Quant au *Data Governance Act* il participe à l'intermédiation & au *data altruism*.

Le premier est un cadre pour les **intermédiaires de données** (data intermediaries) neutres et réglementés, facilitant le partage de données entre acteurs tout en respectant le RGPD, les secrets d'affaires, la cybersécurité. Le second (*data altruism*) est un ensemble de mécanismes permettant à des citoyens ou des organisations de mettre des données à disposition pour des projets d'intérêt général (recherche, innovation, politiques publiques). (Eur-Lex)

Pour finir les espaces données sectoriels régissant les données par secteur, par exemple L'*European Health Data Space (EHDS)* constitue un cadre sécurisé pour l'échange de données de santé électroniques entre États membres, professionnels de santé, patients, chercheurs et innovateurs. Dans ce dernier exemple e droit d'accès des patients à leurs données est renforcé, cela permet a **réutilisation secondaire des données de santé** pour la recherche, l'innovation et l'IA en santé et cela créé un marché unique des services et produits numériques de santé. (Public Health) Des "health data access bodies" géreront l'accès à ces données pour des projets de R&D, avec des obligations rigoureuses en matière de sécurité et de gouvernance.

Les opportunités de valorisation pour les acteurs de l'IA et du numérique sont déjà établies:

- Utiliser le Data Act pour bâtir des offres **data- & AI-driven** à partir des données d'équipements ou d'objets connectés de tiers (maintenance prédictive, optimisation énergétique, optimisation agricole, etc.).
- Se positionner comme **opérateur d'intermédiation** (data intermediary) ou comme fournisseur de briques technologiques nécessaires aux espaces de données sectoriels : data clean rooms, catalogues, outils de pseudonymisation, etc.
- Proposer des services de **gouvernance des données** compatibles avec DGA / EHDS à des écosystèmes (clusters industriels, hôpitaux, villes, etc.).

Cybersécurité & sécurité des produits : CRA, NIS2, DORA

Le **Cyber Resilience Act (CRA)** impose des exigences de cybersécurité à tous les **produits comportant des éléments numériques** : logiciels, matériel, objets connectés, produits d'IA embarqués. Il impose notamment : (Stratégie numérique de l'UE). Pour les organisations, cela implique une **cybersécurité by design et by default**, une analyse des risques de cybersécurité sur le cycle de vie du produit, la mise à disposition de mises à jour de sécurité pendant une durée définie, des obligations de notification de vulnérabilités et incidents, une évaluation de conformité et, dans de nombreux cas, un **marquage CE**.

Quant aux produits intégrant de l'IA, il est nécessaire de traiter à la fois les risques de cybersécurité classiques et ceux propres à l'IA (poisoning, model stealing, injection de prompts, etc.).

Pour ce qui est de la directive **Network and Information Security 2 (NIS2)** étend les obligations de cybersécurité à 18 secteurs critiques (énergie, santé, transport, administration publique, etc.) avec : (Stratégie numérique de l'UE)

- des exigences de **gestion du risque**,
- des obligations de **reporting d'incidents**,
- et une responsabilité accrue des organes de direction.

Pour finir, dans la finance, Le **Digital Operational Resilience Act (DORA)** est la norme spécifique pour la **résilience opérationnelle numérique** (cyber-incidents, résilience ICT, gestion des tiers cloud/IT). (Eur-Lex)

Ici aussi il y a des opportunités et les marchés évoluent clairement dans ce sens avec le positionnement de l'IA comme une **brique de cybersécurité** (détection d'anomalies, détection de fraudes, SOC augmenté), la Création d'**outils de test et de durcissement** de modèles d'IA (adversarial testing, red teaming IA, détection des attaques de prompt injection pour les LLM, etc.), commercialisables dans le cadre du CRA/NIS2/DORA ou encore la vente

d'offres de **"Secure AI Lifecycle"** (audits, accompagnement, certifications, gestion des vulnérabilités en IA).

DSA / DMA : plateformes, algorithmes & écosystèmes

Le **Digital Services Act** encadre les services intermédiaires (hébergeurs, plateformes, VLOPs / VLOSE). Plusieurs obligations impactent directement les systèmes d'IA : (Eur-Lex)

- Transparence sur les système de recommandation (explication des principaux paramètres qui déterminent pourquoi tel contenu est recommandé, obligation de proposer au moins un mode de recommandation **non basé sur le profilage**)
- Évaluation et atténuation des **risques systémiques** liés aux très grandes plateformes (désinformation, polarisation, atteinte aux droits fondamentaux).
- Accès des autorités et de certains chercheurs à des données pour l'audit des algorithmes.

Pour les fournisseurs d'algorithmes de recommandation ou de modération, cela crée une demande accrue de solutions explicables, contrôlables et auditables.

Le DSA va de pair avec le **Digital Markets Act (DMA)** qui impose aux "gatekeepers" (grands acteurs de plateformes) un ensemble d'obligations visant à rendre les marchés plus contestables : (Digital Markets Act (DMA))

- l'interdiction du **self-preferencing** dans les résultats de recherche ou recommandations,
- la limitations à la combinaison de données personnelles entre différents services sans consentement,
- des exigences d'**interopérabilité** (messagerie, périphériques, app stores, etc.),
- un accès plus ouvert à certaines fonctionnalités de la plateforme pour des services tiers.

Encore une fois les contraintes imposées aux uns ouvrent des opportunités de marché pour les autres, par exemple le développement des **"control layers"** au-dessus de recommandations existantes (paramétrage de feed, filtres, dashboards de transparence), ou la fourniture des outils de conformité (audit des biais, explications des classements, suivi des risques systémiques) aux plateformes.

PLD & responsabilité : quand l'IA cause un dommage

La **nouvelle directive Product Liability Directive (PLD)** modernise radicalement la responsabilité produit pour l'ère numérique (Eur-Lex). Elle impacte la notion de **"produit"** est étendue et couvre désormais les logiciels, les fichiers numériques, les systèmes d'IA, y compris ceux évoluant par apprentissage. Elle élargit le champ des **défendeurs** aux fabricants, importateurs, distributeurs, opérateurs de marketplaces, représentants de fabricants hors de l'UE. La **présomptions de défaut et de causalité** est mis en action dans certains cas (par exemple, quand la complexité technique rend quasi impossible pour la victime de prouver le lien exact entre le système d'IA et le dommage) Pour finir, cette récente directive éxtend les **dommages indemnisables** (préjudice psychologique significatif, perte de données, dommages apparus bien après la mise sur le marché). Les États membres doivent transposer la directive d'ici la fin 2026.

> ⚠ *Avec la nouvelle PLD, si ton IA cause un dommage, c'est simple : on présume que c'est sa faute... un peu comme quand un vase casse à la maison, on accuse toujours le matou, même s'il dormait.*

Plusieurs opportunités de marchés s'ouvrent par exemple:

- Investir dans des **capacités de traçabilité et de preuve** (journaux d'événements, versioning des modèles, documentation des datasets et de leur gouvernance, enregistrement des changements de configuration et de modèles).
- Proposer aux clients des produits IA accompagnés de **services de conformité et d'assurance** (support en cas d'incident, fourniture de "dossiers de preuve" pour les litiges)

En résumé, les organisations qui peuvent démontrer avoir pris toutes les mesures raisonnables pour limiter les risques seront mieux préparées.

Droit d'auteur & Text and Data Mining(TDM) : sécuriser l'entraînement des modèles

La directive sur le droit d'auteur dans le marché unique numérique introduit deux exceptions TDM clés pour l'IA : (Eur-Lex)

- exception obligatoire au text and data mining à des fins de **recherche scientifique** par des organismes de recherche et des institutions patrimoniales, dès lors qu'ils ont un accès légal aux œuvres.
- exception plus large, couvrant aussi des usages **commerciaux**, mais avec la possibilité pour les titulaires de droits de **s'opposer explicitement** via des moyens techniques (par exemple, des balises dans les métadonnées ou des fichiers robots.txt).

Cela impact naturalement l'entraînement de modèles d'IA sur l'utilisation des contenus protégés sans respecter les opt-out ou sans licence expose à des litiges, quand aux modèles fondations (GPAI) déjà visés par l'AI Act devront démontrer le respect de ce cadre, notamment par la mise en documentation des sources d'entraînement (Investopedia).

Sur ces contraintes, certains marchés s'ouvrent par exemple:

- se positionner comme **acteur "propriété intellectuelle friendly"**,
- développer des **corpus sous licence claire**, des "safe datasets" pour l'entraînement,
- proposer des **outils de gestion de droits TDM** (gestion des opt-out, traçabilité des sources, génération automatique des rapports de conformité).

Synthèse stratégique : risques & surtout opportunités pour l'industrie IA

La matrice des risques : de la non-conformité au blocage de marché

Risque réglementaire	Risque business
- RGPD + AI Act + PLD créent un triangle où une défaillance sur un point (données, gouvernance de l'IA, sécurité du produit) peut entraîner des amendes, des interdictions et des litiges coûteux. - DSA/DMA ajoutent un risque réputationnel et financier si vos services prennent une dimension « plateforme ». - CRA/NIS2/DORA exposent directement le board sur la cybersécurité.	- Allongement du time-to-market pour les solutions high-risk. - Augmentation du coût de développement (documentation, évaluation, audits). - Possible impossibilité de lancer certaines fonctionnalités sur le marché européen (ex. certains usages biométriques).

Cependant, la bonne approche stratégique consiste à considérer que la régulation constitue une barrière à l'entrée, mais elle peut être utilisée comme un levier stratégique plutôt que perçue uniquement comme une contrainte.

> *En France et certainement en Europe, la phobie administrative est monnaie courante; elle atteint les plus hauts sommets de l'état. Aahhh, s'il y avait des médecins pour cette pathologie au combien incapacitante ! Quoi qu'il en soit ne pas se soigner coûte cher ...*

Opportunité 1 : faire de la conformité un avantage concurrentiel

La conformité IA peut devenir **un véritable argument de vente**, au même titre que la performance technique. Les acteurs capables d'adopter un positionnement clair de "**Trusted AI provider**" pourront se différencier dans un marché très compétitif. Concrètement, cela signifie être :

- **IA Act-ready**,
- **RGPD & DSA-ready**,
- **PLD & CRA-ready**.

Au-delà de la simple conformité, ces réglementations ouvrent la voie à une véritable **prime de confiance** : la possibilité de pratiquer un prix plus élevé,

justifié par un **risque réduit**, de meilleures **assurances**, et une **réutilisabilité** facilitée des produits dans des environnements fortement réglementés.

Dans un paysage où il existera des dizaines de solutions LLM ou IA génératives techniquement similaires, la différence se jouera ailleurs : la capacité à fournir **une documentation complète, des DPIA solides, un registre IA Act à jour, des preuves PLD, des tests de robustesse, des garanties de sécurité, etc.** C'est ce niveau d'exigence qui fera la différence pour les **grands comptes européens**, de plus en plus sensibles aux risques réglementaires et à la gouvernance de l'IA.

Bien que l'idée de "prime de confiance" est séduisante, elle n'est pas automatique. Dans de nombreux secteurs, les clients ne sont pas encore prêts à payer significativement plus cher pour une solution estampillée ""I Act-ready" ou "PLD-ready", surtout sur les segments PME. En pratique, une partie des coûts de conformité (juridiques, organisationnels, documentaires) pèse donc sur les marges pendant plusieurs années, avant que le marché ne reconnaisse pleinement cette différenciation. Cette réalité doit être intégrée dans les business cases : toutes les entreprises n'ont pas la surface financière nécessaire pour absorber 2 à 3 ans de surcoûts avant que la prime de confiance ne se matérialise réellement.

Opportunité 2 : monétiser l'outillage et les services de gouvernance IA

La stack IA peut être conçue non seulement comme un ensemble d'outils techniques internes, mais comme une véritable **plateforme de gouvernance et de conformité**. En structurant votre environnement MLOps, ModelOps ou LLMOps autour des exigences du RGPD, de l'AI Act ou encore de la directive PLD, vous créez des briques réutilisables qui prennent rapidement la forme d'un produit exportable.

Concrètement, cela implique d'intégrer dans vos outils internes des capacités telles que le registre des systèmes IA attendu par l'AI Act, la conduite automatisée des DPIA et AI Impact Assessments, l'évaluation continue des risques (biais, éthique, sécurité), ou encore le test et le monitoring dynamique des modèles pour détecter drift, variations de fairness ou pertes de

performance. À mesure que ces modules se renforcent, ils permettent également de générer automatiquement une grande partie de la documentation réglementaire, notamment les dossiers de conformité AI Act et PLD.

Une fois ces fondations solides, la valeur ne se limite plus à l'usage interne. La plateforme peut alors être **commercialisée** comme produit ou service (SaaS), ou encore servir de socle à des offres de conseil structurées, par exemple sous la forme d'un "AI Compliance Accelerator". Cette logique ouvre la voie à de nouvelles lignes de revenus autour de la **Compliance as a Service / Platform**, et attire potentiellement des clients situés hors d'Europe mais souhaitant accéder au marché européen en toute conformité.

> *Quand OpenAI lance son "Enterprise Compliance API" pour gouverner les GPTs d'entreprise (SecurityWeek), on peut presque imaginer Amazon Web Services en train de dire : "Super – maintenant on peut vendre Cloud + Audit + Platitude de conformité en un seul package !" (aws.amazon.com)*

Opportunité 3 : exploiter le choc de la donnée (Data Act / DGA / data spaces)

Le *Data Act* et le *Data Gouvernance Act* vont multiplier les occasions pour des acteurs IA de créer de la valeur sur des **données tierces**, jusqu'ici verrouillées : (Stratégie numérique de l'UE)

Par exemple dans l'industrie, l'énergie, la mobilité, l'agriculture les organisation pourront récupérer les flux de données d'équipements pour faire de maintenance prédictive, de l'optimisation énergétique, del' optimisation de l'usage (leasing, pay-per-use). Ou encore dans la santé ou il sera possible d'exploiter l'EHDS et les data spaces nationaux/sectoriels pour développer des modèles d'aide au diagnostic, faire du monitoring populationnel, construire des essais cliniques augmentés par l'IA.

Les acteurs capables d'assurer l'orchestration de données multi-acteurs (nettoyage, alignement sémantique, sécurité, conformité) pourront proposer non seulement des modèles, mais également des écosystèmes d'IA complets.

Opportunité 4 : verticaliser des suites "IA de confiance par secteur"

Chaque secteur a désormais son "mix réglementaire" en matière d'IA. C'est une formidable opportunité de bâtir des **suites verticales** :

- Dans la santé en combinant *Medical Devices Regulation(MDR)|In Vitro Diagnostic Regulation*(IVDR) + AI Act high-risk + EHDS + RGPD. (Public Health)
- Dans la finance en combinant DORA + RGPD + AI Act + réglementations sectorielles (anti-blanchiment, *Markets in Financial Instruments Directive(MIFID)*, etc.). (Eur-Lex)
- Dans l'industrie en combinant Data Act + CRA + AI Act + réglementations de sécurité des machines. (Stratégie numérique de l'UE)
- Ou encore dans le secteur public & sécurité en combinant AI Act (restrictions biométriques & police), *Law Enforcement Directive(LED)*, NIS2. (Eur-Lex)

Opportunité 5 : co-construire les standards – devenir "voix du marché"

Les textes européens renvoient souvent à des **normes techniques, lignes directrices et codes de conduite** encore en cours de construction. En participant à ces travaux (normalisation, associations sectorielles, groupes de travail avec les autorités, projets pilotes ou sandboxes), il est possible de :

- influencer le **niveau d'exigence**,
- inscrire dans les pratiques standard ce qui est aligné avec ton offre,
- te positionner comme une référence dans ton secteur.

Feuille de route opérationnelle : de la régulation à la valorisation

Voici une proposition de feuille de route en quatre étapes, à adapter en fonction des spécificités de chaque organisation.

1 - Cartographier, classifier, prioriser

Objectif : savoir précisément où l'IA se trouve déjà chez toi et sous quelles contraintes elle se heurte.

1. **Cartographie des systèmes IA** :
   - recenser tous les usages d'IA (de "Excel + macro" à "LLM dans le CRM"),
   - inclure les IA intégrées à des produits et les services externalisés (SaaS, API).
2. **Classification régulatoire** :
   - IA avec / sans données personnelles (RGPD),
   - niveau de risque AI Act (inacceptable / high-risk / limited / minimal),
   - exposition PLD (produit mis sur le marché vs outil interne),
   - exposition sectorielle (santé, finance, énergie, etc.).
3. **Priorisation** - focus sur les systèmes :
   - high-risk AI Act,
   - exposés aux clients finaux (produits vendus),
   - fortement sensibles RGPD (scoring, RH, etc.),
   - critiques business (gros revenus ou gros risques).

Livrables :

- un **registre des systèmes IA** (gouvernance centrale),
- une **carte des risques d'IA** par ligne de business.

2 – Construire le "AI & Data Governance Framework"

Objectif : transformer les obligations réglementaires en un **processus standard**.

1. Politiques globales :

- **politique des données** : collecte, qualité, partage (Data Act), TDM, anonymisation, durée de conservation.
- **politique IA** : critères d'acceptabilité, revue éthique, exigences de robustesse, explicabilité, supervision humaine.
- **politique cybersécurité & produit** : alignement sur CRA/NIS2/DORA pour les solutions d'IA.

2. Rituels de gouvernance :
   - comités de revue IA (AI review board) pour les projets à risque,
   - processus standard de DPIA et AI impact assessment,
   - politique de gestion de crise de l'IA (incident, biais, incident cyber lié à l'IA).
3. Modèles de documentation :
   - fiches type de système d'IA,
   - templates de DPIA,
   - trames de dossiers de conformité AI Act/PLD.

Livrables :

- un **AI & Data Governance Handbook**,
- des **processus intégrés** dans les cycles de projet (gates IA obligatoires avant la mise en prod).

3 – Industrialiser la conformité dans la stack technologique

Objectif : éviter que chaque projet d'IA ne réinvente sa propre conformité.

1. Plateforme IA centralisée (MLOps / LLMOps) intégrant :
   - versioning des modèles et des datasets,
   - journaux d'événements (logs) pour PLD & AI Act,
   - tests automatisés (performance, fairness, robustness),
   - dashboards de monitoring continu.
2. Modules "compliance by design" :

- capture automatique de métadonnées pour la documentation AI Act,
- génération assistée des sections de DPIA/AI Impact Assessment,
- connecteurs vers les registres IA,
- outils de gestion des droits d'accès aux données (RGPD, Data Act, DGA).
- intégration des exigences sectorielles (EHDS, DORA ...)

Livrables :

- une **plateforme IA** qui fait gagner du temps à chaque projet,
- une "**usine à preuves**" pour les audits, les clients et les autorités.

4 – Construire et packager des offres "IA de confiance"

Objectif : transformer l'investissement réglementaire en chiffre d'affaires.

- **Produits** : modules IA packagés (recommandation, scoring, détection d'anomalies, chatbots, etc.) contenant une documentation AI Act, un guide DPIA-type, des fiches de risques, des éléments de traçabilité PLD, un engagement contractuel sur certains indicateurs (robustesse, support incident).
- **Services** : fournir un diagnostic IA & data governance chez les clients, un accompagnement AI Act (classification des systèmes, dossiers de conformité), un outillage (licensing de ta plateforme MLOps/LLMOps), une formation des équipes (juridique, IT, métiers) à l'AI Rulebook.
- **Positionnement** : branding sur la **confiance**, la **durabilité** des solutions, la capacité à être "future proof" vis-à-vis des évolutions réglementaires.

... et les petites entreprises dans tout ça !

Pour les **ETI** (voire les **PME**) qui souhaitent tirer parti de cet *AI Rulebook*, viser le même niveau de sophistication qu'un grand groupe serait contre-productif : le risque est d'investir plus en conformité qu'en innovation réelle. Une stratégie pragmatique consiste à **réduire volontairement le périmètre**, à **choisir des cas d'usage maîtrisables**, et à **s'appuyer au maximum sur des solutions packagées**.

> *Pour une ETI qui veut copier la gouvernance IA d'un grand groupe, c'est un peu comme une grenouille qui veut être aussi grosse qu'un bœuf : à la fin, elle n'a plus de souffle… et toujours pas d'IA en production.*

Une gouvernance « light » mais robuste pour ETI/PME

Elles peuvent aller vers une IA responsable sans lourdeur administrative en se dotant de quelques briques essentielles :

- un **registre simplifié** des systèmes d'IA (3–5 lignes suffisent : finalité, données utilisées, risque IA Act, présence de données personnelles, exposition client),
- des **templates prêts-à-l'emploi** (DPIA, AI Impact Assessment) réutilisables,
- un **mini-comité IA** (même 2 personnes : IT/DSI + DG ou responsable métier) avec quelques critères de stop/go (risque RGPD, risque IA Act, risque réputationnel),
- un choix assumé : **privilégier les systèmes low-risk ou limited-risk** (automatisation interne, copilotes métier, classification documentaire, recommandation non contraignante, chatbots internes).

La **mutualisation** devient clé : plateformes SaaS certifiées, offres MLOps prêtes-à-l'usage intégrant déjà l'audit et la traçabilité, accompagnement ponctuel par des cabinets spécialisés plutôt qu'un modèle full-internalisation.

L'objectif n'est pas la conformité parfaite mais **le bon équilibre** entre :

- maîtrise du risque réglementaire (intégré au Go-To-Market),
- création de valeur business,
- capacité réelle à maintenir cette gouvernance dans la durée.

Et les TPE alors ? La grande zone grise du marché

Les **TPE** (0 à 10 salariés), qui représentent plus de **95 % du tissu économique**, se retrouvent face à une situation paradoxale : elles sont **fortement exposées aux outils d'IA** (car elles les utilisent via des SaaS, CRM, emailings, e-commerce, compta, etc.) mais **peu équipées pour absorber la charge réglementaire**.

Aujourd’hui, les TPE disposent essentiellement de :

- **Solutions SaaS IA déjà conformes** (Ex : Microsoft Copilot, Google Workspace, HubSpot, Notion, Shopify, etc.). Ces outils portent la charge principale de conformité (cyber, PLD, AI Act, RGPD). La TPE doit surtout **bien paramétrer**, et **maîtriser ce qu’elle envoie** à ces outils.
- **Guides et ressources publiques** (CNIL, Commission Européenne, Bpifrance, FranceNum) mais souvent trop généraux ou trop techniques pour un dirigeant seul.
- **Aides ponctuelles** (diagnostics subventionnés, formations) mais pas encore d’outillage opérationnel standardisé.

Il manque tout de même beaucoup de facilitateurs

- un *guichet unique IA* pour TPE,
- des *modèles ultra-simplifiés* (1 page) d’analyse de risque,
- des *outils d’auto-audit* faciles à suivre,
- une *certification basique* de conformité pour les PME/TPE productrices d’outils d’IA (aujourd’hui trop complexe).

Dans ce contexte, ce que les TPE peuvent réellement faire, sans structure juridique dédiée, sans DPO(*Data Protection Officer*) interne, et avec peu de temps, une TPE peut viser un "**socle minimal de conformité IA**" en limitant les usages à faible risque (copilotes de mails / documents, automatisation administrative, aide à la vente ou au marketing, analyse de documents internes, chatbots non décisionnels), en vérifiant l'usage des données personnelles, en s'assurant que la machine ne décide pas à la place d'un opérateur et en verifiant l'impact sur le client. Elles peuvent aussi s'appuyer sur des solutions clé-en-main (utiliser des SaaS pour la documentation IA Act, les logs, la transparence, les clauses contractuelles robustes), faire du MLOps "léger" et externaliser ponctuellement le juridique et le technique.

Les TPE sont donc exposées à plusieurs risques : ceux de conformité indirecte (par ex l'utilisation données dans un secteur réglementé), les risques

contractuels (partage de données involontaire), risque de dépendance technologique et les risque réputationnel.

> *Le risque réputationnel, c'est quand ton IA plante et que ta TPE devient la "star locale" … celle dont tout le monde parle à la boulangerie parce qu'elle a envoyé un devis signé "Bisous, votre licorne à paillettes magiques"*

Dès lors les impacts sur le TPE sont concret

Impact positif (si bien maîtrisé) :

- automatisation massive des tâches non productives,
- augmentation de la réactivité commerciale,
- réduction du temps administratif,
- augmentation de la qualité documentaire et communication,
- soutien aux dirigeants souvent isolés.

Impact négatif (si mal maîtrisé) :

- non-conformité RGPD ou IA Act sans le vouloir,
- dérives d'usage par les salariés,
- décisions automatisées non vérifiées,
- perte de données ou mauvaises pratiques de sécurité.

Dans ce cadre un soutien public devient essentiel, pour les TPE, la régulation a un poids **disproportionné** par rapport à leurs capacités internes.

Un modèle efficace pourrait s'appuyer sur :

- **des kits réglementaires prêts à l'emploi** (1 page pour IA Act, 1 page pour RGPD, 1 page pour cybersécurité),
- **un diagnostic IA subventionné et rapide** (2 h),
- **des référentiels sectoriels simplifiés** (commerce, artisanat, services),
- **des outils publics ou européens « compliance-as-a-service »** (registre IA pré-formaté, modèle d'analyse de risque automatique, générateur de clauses contractuelles IA, checklists contextualisées)

De tels dispositifs existent dans certains pays nordiques ; la France/UE pourrait s'en inspirer pour éviter une fracture numérique et réglementaire.

Zoom très opérationnel par secteur

Santé & medtech

Réglementation clé : MDR & IVDR, AI Act (systèmes high-risk), RGPD & EHDS, éventuellement Data Act / DGA. (Public Health)

Contraintes spécifiques IA :

- De nombreux logiciels d'IA (diagnostic, tri de patients, guidage thérapeutique) sont des **dispositifs médicaux** ; ils doivent donc :
  - être classés selon MDR,
  - passer par évaluation de conformité,
  - disposer d'un système de gestion de la qualité, d'un suivi post-market, etc.
- L'AI Act vient compléter MDR/IVDR en couvrant les risques pour les droits fondamentaux (biais, discriminations, manque de supervision humaine). (Public Health)
- Données de santé = données particulièrement sensibles du RGPD (base légale solide, sécurité renforcée, DPIA quasi systématique).
- EHDS : possibilité d'accéder à des données de santé secondaires, mais avec un processus d'autorisation, de pseudonymisation et de restrictions d'usage. (Public Health)

Opportunités IA :

- Solutions d'aide au diagnostic, de triage, d'optimisation des parcours des patients, de planification des ressources hospitalières, déjà **AI Act + MDR ready**.
- Plateformes permettant aux hôpitaux / réseaux de santé de :
  - exploiter les données EHDS,

    - développer des modèles internes dans un cadre fiable (pseudonymisation, gouvernance).
- Outils de monitoring des performances et des biais des algos cliniques (suivi post-market en continu).

Finance, banque, assurance

Réglementation clé : RGPD, AI Act, DORA, réglementation prudentielle (EBA, ESMA, EIOPA), AML/CFT, DSA/DMA pour les plateformes de trading ou de services. (Eur-Lex)

Contraintes spécifiques IA :

- L'IA est utilisée dans des domaines hautement sensibles : scoring de crédit, lutte anti-fraude, tarification, trading.
- DORA impose une gouvernance stricte des risques ICT, incluant les algos critiques, avec :
    - tests de résilience,
    - reporting d'incidents,
    - Gestion des prestataires (cloud, fournisseurs d'IA). (Eur-Lex)
- RGPD + AI Act : profilage à fort impact + high-risk (accès à des services financiers essentiels).
- Pression forte des superviseurs pour des modèles **explicables** et non discriminatoires.

Opportunités IA :

- Proposer des moteurs de scoring **explicables et contrôlables**, avec :
    - logs,
    - simulation de décisions,
    - module d'audit des biais,
    - documentation prête pour les régulateurs.
- Offres de **"regtech IA"** : détection de fraudes, analyse des comportements de marché.

- Plateformes de **modélisation de risques** intégrant DORA & AI Act, vendues aux banques et assureurs.

Industrie, énergie, logistique

Réglementations clés : Data Act, AI Act, CRA, NIS2, réglementations de sécurité des machines, environnement. (Stratégie numérique de l'UE)

Contraintes spécifiques IA :

- Importante utilisation d'IA pour :
  - la maintenance prédictive,
  - l'optimisation de procédés,
  - la robotique,
  - La sécurité au travail.
- Les produits intelligents (machines, robots, véhicules) sont des "produits avec des éléments numériques" soumis au CRA (sécurité & cyber), à la sécurité machine, etc. (Stratégie numérique de l'UE)
- Les données machine/IoT sont au cœur du Data Act, qui oblige à :
  - ouvrir l'accès aux utilisateurs,
  - Parfois partager avec des tiers. (Stratégie numérique de l'UE)

Opportunités IA :

- Construire des services IA utilisant les données récupérées grâce au Data Act :
  - "Optimization as a Service" pour les usines,
  - jumeaux numériques,
  - services de conseil énergétique.
- Packager des produits industriels **"CRA-ready"** :
  - architecture sécurisée,
  - mises à jour régulières,
  - monitoring des vulnérabilités IA.

- Développer des plateformes de **data sharing sectorielles** (manufacturing, énergie, supply chain) pour faciliter la mutualisation et bâtir des modèles d'IA plus robustes.

Secteur public, smart cities, sécurité & justice

Réglementation clé : AI Act (usages par les autorités publiques), RGPD, Directive 2016/680 (LED) pour les autorités répressives, NIS2 pour certains opérateurs publics critiques. (Eur-Lex)

Contraintes spécifiques IA :

- L'AI Act encadre strictement :
  - les systèmes utilisés pour l'évaluation de risque de fraude,
  - la gestion des aides sociales,
  - la police prédictive,
  - la reconnaissance biométrique à distance, avec de fortes restrictions et interdictions. (Reuters)
- La LED impose un régime spécial aux données traitées par les autorités répressives (police, justice).
- NIS2 s'applique à de nombreuses entités publiques considérées comme essentielles ou importantes (santé, transport, énergie, services publics numériques). (Stratégie numérique de l'UE)

Opportunités IA :

- Solutions IA pour :
  - l'optimisation des services publics (gestion de flux, smart city, gestion des demandes citoyens),
  - l'analyse documentaire (dossiers, jurisprudence, réglementation),
  - la lutte contre la fraude, mais avec des mécanismes de supervision humaine robustes.
- Outils de **gouvernance IA pour le secteur public** :
  - registres publics des algorithmes,

- tableaux de bord de transparence,
- dispositifs de participation citoyenne à la conception et au contrôle des algos.

Bibliographie indicative (réglementation & ressources clés)

Textes européens principaux :

- **RGPD** : Règlement (UE) 2016/679.
- **Directive (UE) 2016/680** (LED) – protection des données dans le domaine pénal. (Eur-Lex)
- **AI Act** : Règlement (UE) .../2024 relatif à l'intelligence artificielle – texte consolidé et commenté sur le site "AI Act Explorer". (Stratégie numérique de l'UE)
- **Data Act** : Règlement (UE) 2023/... sur les données, fiches explicatives de la Commission. (Stratégie numérique de l'UE)
- **Data Governance Act (DGA)** : Règlement (UE) 2022/868 relatif à la gouvernance des données. (Eur-Lex)
- **Digital Services Act (DSA)** : Règlement (UE) 2022/2065 relatif aux services numériques. (Eur-Lex)
- **Digital Markets Act (DMA)** : Règlement (UE) 2022/1925 relatif aux marchés contestables et équitables dans le secteur numérique. (Digital Markets Act (DMA))
- **Cyber Resilience Act (CRA)** : Règlement (UE) 2024/2847 relatif aux exigences de cybersécurité pour les produits comportant des éléments numériques. (Stratégie numérique de l'UE)
- **NIS2** : Directive (UE) 2022/2555 relative aux mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'Union. (Stratégie numérique de l'UE)
- **DORA** : Règlement (UE) 2022/2554 relatif à la résilience opérationnelle numérique du secteur financier. (Eur-Lex)

- **PLD** : Directive (UE) 2024/2853 relative à la responsabilité du fait des produits, modernisée pour les produits numériques et l'IA. (Eur-Lex)
- **Directive (UE) 2019/790** sur le droit d'auteur dans le marché unique numérique, articles 3 et 4 (exceptions TDM). (Eur-Lex)
- **EHDS** : Règlement de l'Espace européen des données de santé (EHDS) et pages officielles sur l'IA en santé. (Public Health)
- **Medical Devices Regulation(MDR) / In Vitro Diagnostic Regulation(IVDR)** et documents récents de la MDCG sur l'IA embarquée dans les dispositifs médicaux. (Public Health)

Guidelines & soft law :

- EDPB – *Guidelines on Automated individual decision-making and Profiling* (article 22 RGPD). (EDPB)
- CNIL – ressources sur les DPIA et l'IA (guidelines, référentiels sectoriels). (cnil.fr)
- Commission & agences (EBA, ESMA, EIOPA) – documents sur l'IA et le machine learning dans la finance, ainsi que sur la mise en œuvre de DORA. (EIOPA)
- Notes de la Commission sur l'application de l'AI Act à certains usages (employeurs, sites web, forces de l'ordre). (Reuters)

Analyses & commentaires récents :

- Commentaires sur le CRA et ses implications pour les produits numériques. (bclplaw.com)
- Analyses de la réforme du PLD et de son impact sur l'IA et les smart products. (Bird & Bird)
- Articles académiques et think tanks sur les risques systémiques liés au DSA et leurs recoupements avec l'AI Act. (Observatoire DSA)

Annexe stratégique – Une idée en passant : un outil de pilotage interne : le "Risk–Value Score (RVS)"

La prise de décision sur les projets d'IA en contexte réglementaire nécessite une grille de lecture qui articule clairement la valeur créée, les coûts de conformité, l'exposition résiduelle au risque.

Pour faciliter cet arbitrage, nous proposons un indicateur interne simple : le **Risk–Value Score (RVS)**.

1. Objectif du RVS

Le RVS n'a pas vocation à être un ratio financier formel. Il s'agit d'un **outil de pilotage**, permettant au COMEX et aux équipes métiers de comparer les projets d'IA selon un référentiel homogène, intégrant explicitement les contraintes du cadre réglementaire européen.

En d'autres termes, c'est un **score d'aide à la décision**, pas un modèle de valorisation.

2. Définition du RVS

Le RVS suit une logique simple :

$$\mathbf{RVS} = \frac{\text{Valeur estimée du projet}}{\text{Coûts de conformité} + \text{Exposition au risque résiduel}}$$

Il permet d'évaluer non pas la "rentabilité brute", mais la **capacité d'un projet d'IA à créer de la valeur dans un environnement réglementé**.

3. Les composants du RVS

3.1. Valeur estimée (V)

Valeur économique sur 3–5 ans, incluant :

- gains directs (revenus, efficacité, nouveaux services),
- économies de coûts,
- réduction d'un risque existant (fraude, erreurs, incidents),
- coûts d'implémentation du projet IA.

L'objectif est d'obtenir une estimation **cohérente et comparable**, même approximative.

3.2. Coûts de conformité (C^c)

Coûts liés aux exigences du règlement européen :

- classification RGPD / AI Act,
- DPIA / AI Impact Assessment,
- documentation & registres IA,
- obligations PLD,
- cybersécurité (CRA / NIS2 / DORA),
- audits et contrôles réguliers.

Il s'agit d'un **coût complet** (initial + maintien).

3.3. Risque résiduel (R^r)

Score qualitatif converti en coût équivalent, basé sur 4 dimensions :

1. Risque réglementaire (sanctions, non-conformité)
2. Risque de blocage de marché (interdiction, retrait)
3. Risque réputationnel
4. Risque opérationnel ou cyber

Chaque dimension est notée **1 à 5**, pondérée selon le secteur. Le score agrégé est ensuite converti en "coût équivalent" selon un facteur interne.

Important : Ce coût n'est pas une estimation financière stricte ; il sert à **rendre visible le risque dans le calcul**, en cohérence avec la culture risk-management de l'organisation.

4. Interprétation du RVS

Le RVS ne donne pas une vérité mathématique : il fournit une **lecture synthétique** du rapport valeur / exposition.

Lecture indicative :

- **RVS > 3** : projet attractif dans un cadre réglementé.
- **1,5 < RVS < 3** : projet à arbitrer (re-scope, sandbox, approche progressive).

- **RVS < 1,5** : projet créant peu de valeur au regard des risques & coûts de conformité.

L'intérêt du RVS est d'éviter que des projets "performants techniquement" masquent un **mauvais profil régulatoire**, et inversement.

5. Usage recommandé du RVS

Le RVS doit être utilisé comme :

- un **outil de priorisation** au moment de la planification,
- un support de dialogue entre métiers, juridique, risque, IT et data,
- un mécanisme de **mise en cohérence des projets IA** avec la stratégie de conformité.

Il **ne remplace pas** :

- un business case détaillé,
- une évaluation financière,
- un avis juridique,
- ni une analyse de risques complète.

C'est un **score transversal**, conçu pour rendre la discussion plus structurée et plus transparente.

Pour les PME et ETI, le RVS est particulièrement utile : il rend explicite le fait que certains projets IA techniquement attractifs mais très exposés (high-risk AI Act, données sensibles, forte responsabilité produit) obtiennent un score faible, car les coûts de conformité et le risque résiduel écrasent la valeur créée. Cela permet d'assumer des arbitrages lucides : renoncer à certains projets, ou les décaler dans le temps, n'est pas un échec – c'est une gestion responsable du capital et du risque.

6. Pourquoi intégrer cet outil ?

Parce que l'IA réglementée crée une nouvelle équation stratégique :

> *"Un projet IA n'est pas seulement un gain business : c'est un gain business **dans un contexte réglementé**."*

Le RVS rend cette réalité **mesurable, comparable et actionnable**, sans prétendre à une précision artificielle.

Eric Blaudez - AI Architect | Responsible AI · AI Act · AI Governance | Bringing R&D AI to Production (TRL 3→6) | EU & Sovereign Programs

L'Europe comme architecte d'un "AI Rulebook" complet