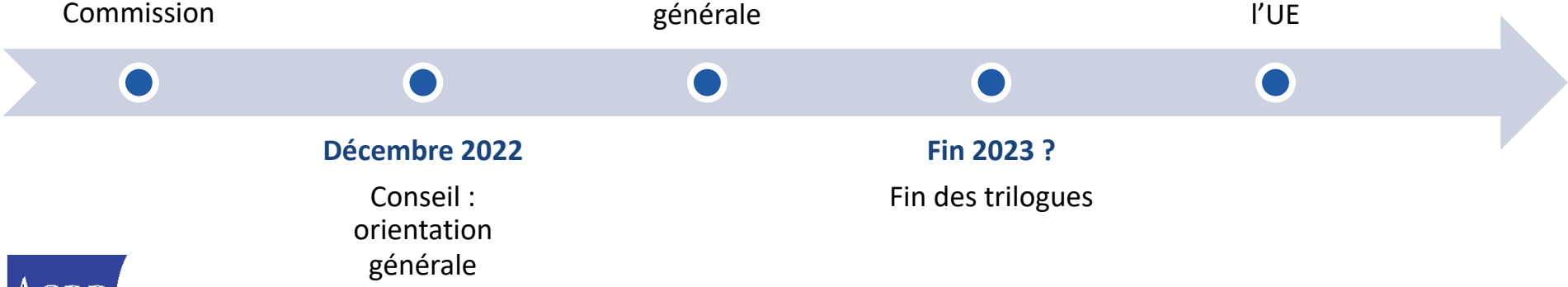
ACPR
BANQUE DE FRANCE

LE RÈGLEMENT EUROPÉEN SUR L'INTELLIGENCE ARTIFICIELLE (*AI ACT*)

JULIEN URI
PÔLE FINTECH-INNOVATION
LUNDIS DE L'IA – 15 MAI 2023

POURQUOI UN RÈGLEMENT EUROPÉEN SUR L'IA ?

- Deux objectifs principaux :
  - Répondre aux risques pour la sécurité, la santé et les droits fondamentaux
  - Créer un marché unique européen de l'IA de confiance
- Rendre applicables certaines règles habituelles du marché intérieur à la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA
- Donner de la sécurité juridique aux opérateurs et accroître la confiance des consommateurs
- Créer des conditions de concurrence équitables pour les acteurs de l'UE et des pays tiers : le règlement s'applique quelle que soit l'origine du fournisseur ou de l'utilisateur du système

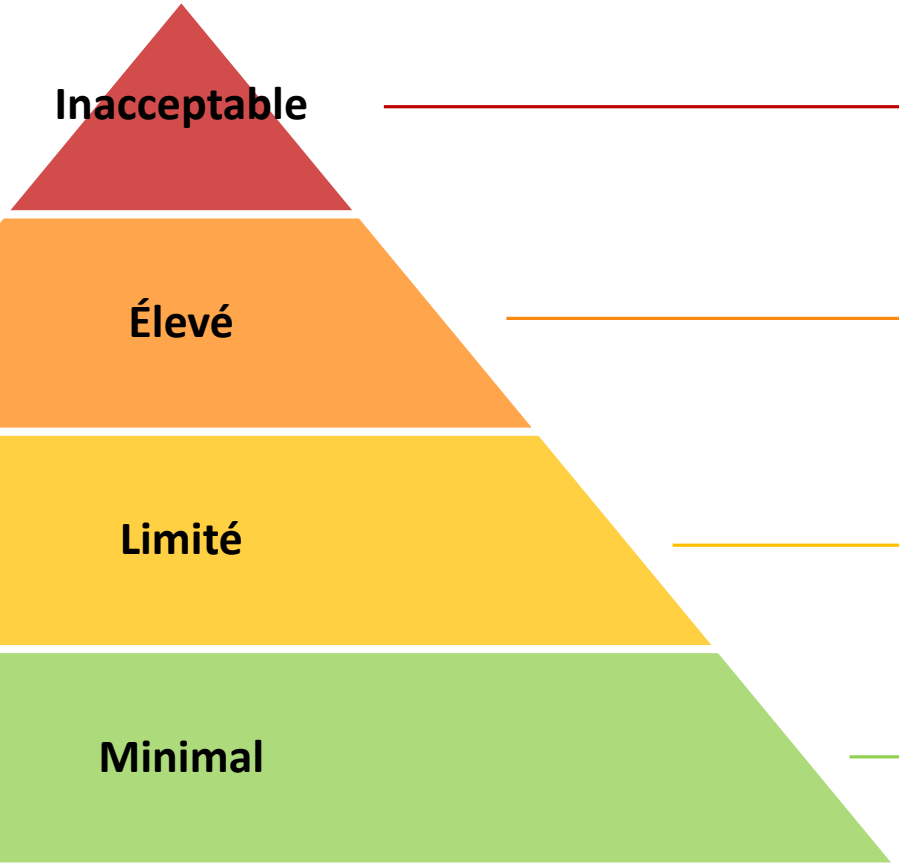


ACPR
BANQUE DE FRANCE

LA (DIFFICILE) DÉFINITION DE L'IA

- La définition initialement adoptée par la Commission a été jugée trop large (elle comprenait notamment toutes les approches statistiques)
- Dans la dernière version du texte du Conseil (OG), l'IA désigne :
  - les systèmes utilisant le *machine learning* ou des « *logic and knowledge based approaches* » (systèmes experts),
  - fonctionnant avec un certain degré d'autonomie,
  - produisant des résultats tels que des contenus (IA générative), des prévisions, des recommandations ou des decisions
  - qui influencent l'environnement avec lequel le système d'IA interagit.
- Toutefois, le contenu exact de cette définition reste flou : la Commission est ainsi chargée de définir plus précisément le contenu du *machine learning* et des *logic and knowledge based approaches* (par acte délégué)

QUATRE NIVEAUX DE RISQUE POUR LES SYSTÈMES D'IA



Manipulation par des techniques subliminales ; notation sociale ; identification biométrique en temps réel (avec exceptions)		**Interdiction**
Infrastructures critiques, services publics et privés essentiels etc.		**Conformité**
Chatbots, *deep fakes*, reconnaissance d'émotion, reconnaissance biométrique		**Transparence**
Autres systèmes (ex : jeux vidéo, détection automatique de spam etc.)		**Aucune obligation**

ACPR
BANQUE DE FRANCE

LE PÉRIMÈTRE DES SYSTÈMES À HAUT RISQUE

- **Deux types de systèmes potentiellement « à haut risque »** (Art 6) **:**
  - Produits / composants de sécurité faisant l'objet d'une évaluation de conformité *ex ante* par un tiers, conformément aux règles sectorielles de l'Union européenne (Annexe II)
  - Systèmes servant une série de **cas d'usage spécifiques, énumérés à l'Annexe III**

- **Annexe III** : liste de cas d'usage établie en fonction de l'**objectif** visé par les systèmes d'IA, au sein de 8 domaines considérés comme sensibles.

  Pour le secteur financier :

  - Domaine 5 : « *Accès et droit aux services privés essentiels et aux services publics et prestations sociales essentiels* »

    (b) Systèmes d'IA destinés à l'évaluation de la solvabilité des personnes physiques ou à l'établissement de leur note de crédit*

    d) Systèmes d'IA à des fins d'évaluation et de tarification pour les personnes physiques en matière d'assurance vie et d'assurance maladie (*ajouté par le Conseil*)*

    **à l'exception des systèmes d'IA mis en service par des PME pour leur propre usage*

  - Le cas d'usage de l'**identification biométrique** peut concerner indirectement le secteur financier

ACPR
BANQUE DE FRANCE

HAUT RISQUE : OBLIGATIONS APPLICABLES AUX SYSTÈMES

Obligations des systèmes d'IA

Établir et mettre en œuvre un processus itératif de **gestion des risques**

Utiliser des **données** d'entraînement, de validation et de test de **haute qualité.**
Mettre en œuvre des procédures de **gouvernance des données.**

Établir la **documentation technique** prévue et concevoir le système avec des fonctions **d'enregistrement automatique** => **traçabilité et auditabilité**.

Assurer un degré approprié de **transparence et d'interprétabilité** du système par sa conception et fournir des informations aux utilisateurs sur la manière de l'utiliser.

Permettre une **surveillance humaine** visant à minimiser les risques résiduels (mesures intégrées dans le système et/ou à mettre en œuvre par les utilisateurs)

Garantir la **robustesse, l'exactitude et la cyber-sécurité** tout au long du cycle de vie.

Prise en compte de **l'objectif** du système et de **l'état de l'art** reconnu pour assurer la conformité.
Les **normes techniques harmonisées** élaborées par les **autorités européennes de standardisation** (ESOs) aideront à démontrer la conformité du système.

ACPR
BANQUE DE FRANCE

SYSTÈMES À HAUT RISQUE : OBLIGATIONS DES OPÉRATEURS

Obligations des fournisseurs

- Établir et mettre en œuvre un système de **gestion de la qualité**
- Élaborer et tenir à jour la **documentation technique**
- Procéder à l'**évaluation de la conformité** et éventuellement à la réévaluation du système
- Enregistrer le système d'IA autonome dans la base de données de l'UE, signer la déclaration de conformité et apposer le marquage « CE »
- Effectuer un **suivi du système** après sa mise sur le marché
- Signaler les **incidents graves** et les dysfonctionnements entraînant une violation des droits fondamentaux
- **Collaborer** avec les autorités de surveillance du marché

Obligations des utilisateurs

- Utiliser le système d'IA à haut risque **conformément au mode d'emploi**
- Assurer une **supervision humaine** et surveiller les opérations pour déceler les risques éventuels
- **Conserver les journaux** du système (*logs*)
- Signaler tout **incident grave** au fournisseur ou au distributeur
- Appliquer les autres obligations légales (ex : RGPD)
- **Collaborer** avec les autorités de surveillance du marché

ACPR
BANQUE DE FRANCE

LE CAS DES SYSTÈMES GÉNÉRALISTES

- **Systèmes d'IA généralistes** = ceux qui peuvent être utilisés dans une multiplicité de contextes
- Les **fournisseurs** de systèmes d'IA à usage général qui peuvent être utilisés comme systèmes à haut risque (ou comme composants de systèmes à haut risque) devront respecter des exigences **proches de celles des systèmes à haut risque** (Conseil)
- **Mécanisme de transfert de responsabilité** du fournisseur vers l'utilisateur lorsque ce dernier utilise un système d'IA généraliste dans un domaine à haut risque (ou modifie le système pour qu'il devienne à haut risque). Le fournisseur initial doit cependant fournir la documentation technique et collaborer avec le « nouveau » fournisseur (Parlement)
- **« Modèles de fondation »** (basés sur une grande quantité de données et pouvant être utilisés pour diverses tâches) : obligations spécifiques (Parlement)
- Exigences supplémentaires de transparence pour les **systèmes d'IA générative**, notamment quant à l'utilisation de données protégées par la législation sur le droit d'auteur pour l'entraînement des modèles (Parlement)

L'ARCHITECTURE DE SUPERVISION DES SYSTÈMES D'IA

- **Avant** mise sur le marché / mise en service des systèmes d'IA :
  - Les **autorités notifiantes**, désignées par chaque État membre, supervisent le **processus de certification** des systèmes d'IA, et surveillent en particulier l'activité des organismes notifiés
  - Les **organismes notifiés** sont des certificateurs désignés par les autorités notifiantes (et/ou d'autres textes de l'Union, par exemple les règlementations industrielles)
- **Après** mise sur le marché / mise en service : contrôle par les **autorités nationales de surveillance du marché**
- Le règlement établit un **Comité européen de l'IA** :
  - Composé d'un représentant par État membre
  - Il conseille et assiste la Commission et les États membres pour la mise en œuvre du règlement ; il édicte des règles de niveau III ; il peut assister les autorités de surveillance du marché
- Possibilité de créer des **bacs à sable règlementaires** donnée aux autorités nationales compétentes (autorités notifiantes ou autorités de surveillance du marché) pour le développement de systèmes d'IA

ACPR
BANQUE DE FRANCE

QUELLE ARTICULATION ENTRE LES RÉGLEMENTATIONS SECTORIELLES ET LES RÈGLES HORIZONTALES ? LE CAS DU SECTEUR FINANCIER

- Dans le règlement IA, les établissements financiers **régulés par le droit de l'Union** sont soumis à un régime particulier :
  - Les **autorités nationales de supervision financière** seront vraisemblablement les autorités de surveillance du marché dans le secteur financier
  - **Intégration** de certaines des obligations des fournisseurs et des utilisateurs dans les processus existants de **contrôle interne** des établissements financiers
  - **Présomption de conformité** pour certaines dispositions

- Mais **l'articulation** entre les règles sur l'IA et le contrôle sectoriel n'est **pas explicitement prévue** par le règlement
  - ➢ A notamment pour but de donner une plus grande flexibilité aux autorités de supervision financière sur la manière d'intégrer (le cas échéant) les nouvelles missions à leurs procédures existantes

ACPR
BANQUE DE FRANCE

EN CONCLUSION PROVISOIRE

- Il manque encore des briques dans le dispositif déployé par le règlement IA :
  - Contenu exact de certaines des obligations prévues par le règlement => **standards européens** à élaborer
  - Application du règlement au secteur financier et audit des systèmes d'IA par les autorités de surveillance du marché => des **orientations** des **autorités européennes de supervision** (ESAs) pourraient préciser les choses
- Le secteur financier va devoir se doter des moyens techniques pour évaluer la conformité (*ex ante*) de ses systèmes d'IA, au moins pour certains cas d'usage
- L'autorité de contrôle devra élaborer des techniques d'audit appropriées pour vérifier la conformité (*ex post*) des systèmes utilisés par le secteur financier

ACPR
BANQUE DE FRANCE