UNIVERSITÉ D'ARTOIS

Journée « Société & IA » @ PFIA 2024
La Rochelle 1 et 2 juillet 2024

CHAIRE IA RESPONSABLE

Le règlement européen sur les systèmes d'IA

Nathalie NEVEJANS
Titulaire de la Chaire « IA Responsable »
Professeure en droit privé
Directrice du DU Responsable de l'éthique de l'IA
Université d'Artois

Introduction générale au Règlement sur l'IA

Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle du 21 avril 2021 (Artificial Intelligence Act)

▪ Objectifs

Le règlement vise à mettre en place un **cadre juridique pour une IA axée sur le facteur humain et digne de confiance**

▪ Valeur juridique

Le Règlement sur l'IA (ci-après « RIA ou AI Act ») a déjà livré sa toute dernière version du 13 juin 2024 qui devrait paraître au Journal officiel le 12 juillet 2024 et entrer en vigueur au 1er août 2024

→ Quand le règlement entrera en vigueur, il sera d'**application obligatoire dans tous les Etats membres de l'UE**, après un certain délai (selon les situations).

▪ Contenu

Le règlement impose des exigences et des obligations relatives à la **mise sur le marché ou en services ou à l'utilisation professionnelle** qui dépendent du **niveau de risques** générés par l'usage du **système d'IA** (voir les précisions après)

▪ A noter

Il s'agit l'un des premiers cadres juridiques stricts obligatoires proposés pour l'IA à l'échelle mondiale.

Est-ce que le RIA concerne la discipline “IA” ?

- Non : il ne concerne que les **usages de l’IA**

- Et **il ne s’applique qu’aux systèmes d’IA**…

… sous réserve de l’IA générative

Qu’est-ce qu’un système d’IA selon le RIA ?

Article 3, § 1 du RIA

« Système d’intelligence artificielle » (système d’IA) :

Il s’agit d’ « **un système automatisé** qui est conçu pour fonctionner à **différents niveaux d'autonomie** et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties **telles que des prédictions, du contenu, des recommandations ou des décisions** qui peuvent influencer les environnements physiques ou virtuels »

Qui sont les personnes protégées contre les risques de l'IA selon le RIA ?

- Les **personnes concernées** sont les personnes physiques ou les groupes de personnes physiques qui utilisent, subissent ou sont soumises à une decision, résultats, etc, provenant d'un système d'IA

- Les risques visés sont les risques en matière de **santé**, de **sécurité** et de **droits fondamentaux**

Qui sont les opérateurs responsables au titre du RIA ?

→ **Les fournisseurs** : acteurs centraux car ils mettent sur le marché européen ou en service des systèmes d'IA, ou encore sur le marché des systèmes et modèles GPAI, qu'ils soient établis ou situés dans l'Union ou dans un pays tiers.

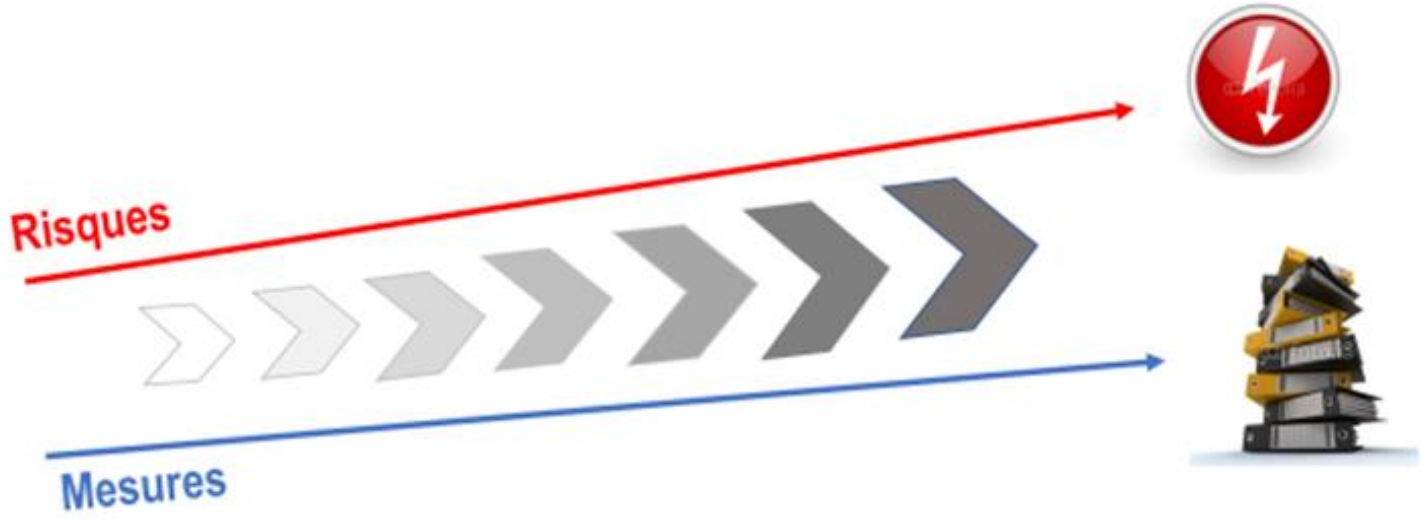
Définition : le fournisseur est « une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit » (Article 3, § 3)

→ **Les déployeurs** : acteurs importants car ce sont les utilisateurs professionnels qui ont leur lieu d'établissement ou sont situés dans l'Union.

Définition : le déployeur est « une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel » (Article 3, § 4)

Quelle est l’approche adoptée par le RIA ?

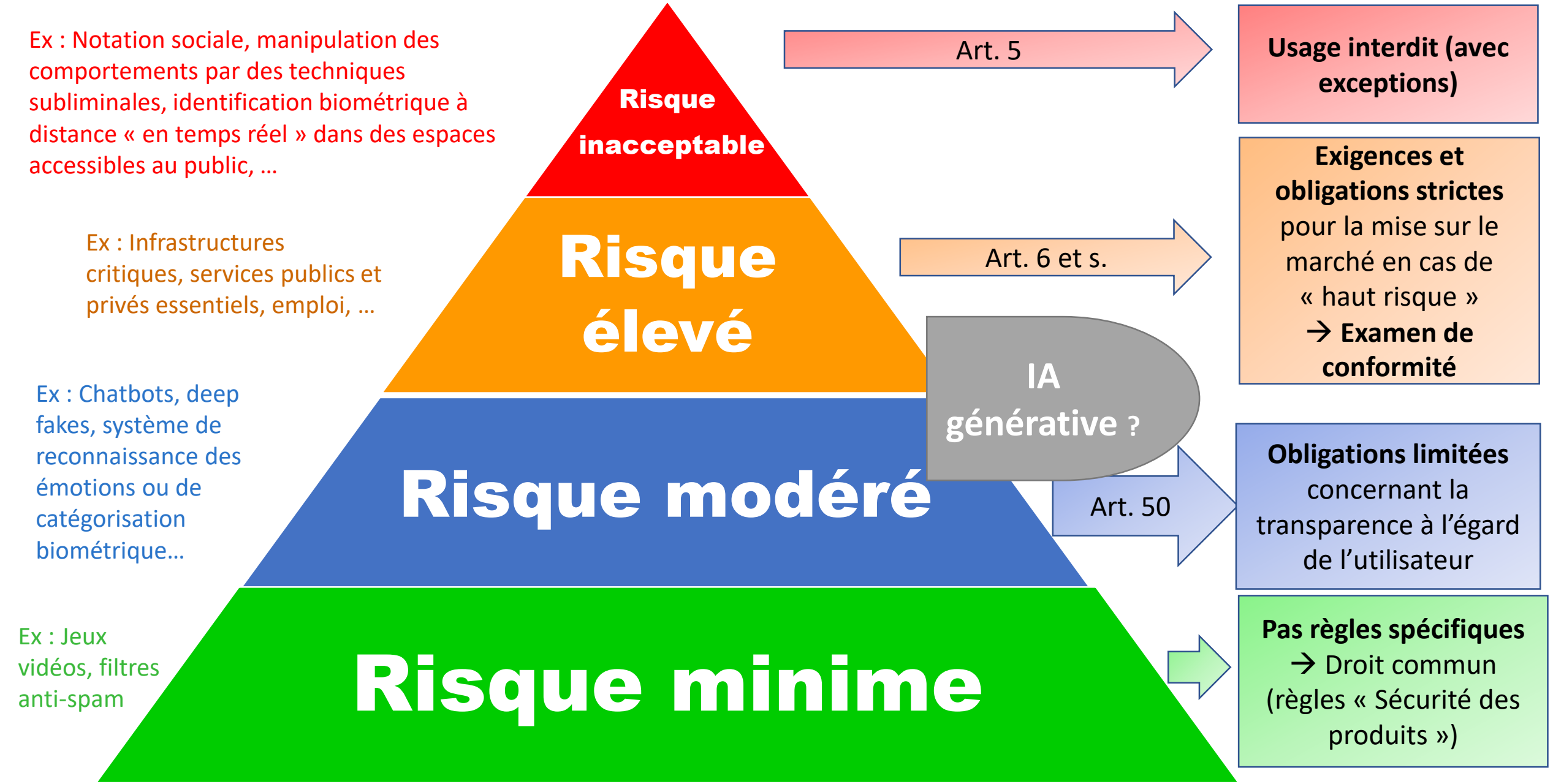
La Commission a choisi d’adopter une **approche fondée sur les risques = Gradation des contraintes légales selon les usages de l’IA**



Approche basée sur les risques

Quelles sont les contraintes imposées par le RIA?

- Quels sont les **différents niveaux de risques visés** ? Dans l'approche par les risques, on trouve le risque inacceptable, le haut risque, le risque modéré, et le risque minime (ou nul).



Pyramide des risques de l'AI Act

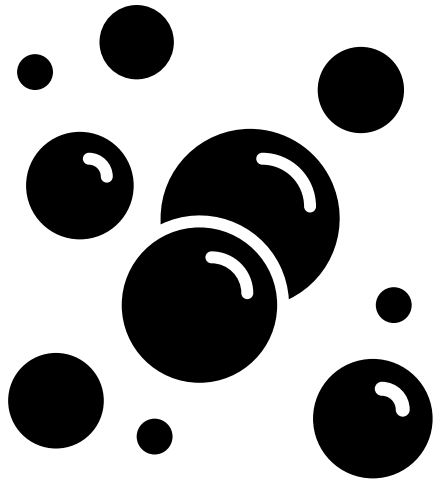
Quels intérêts d'une approche par les risques ?

- L'approche basée sur les risques **permet à l'UE de ne focaliser l'effort de régulation que sur un volume limité de systèmes d'IA dit « à haut risque »** pour la santé, les droits fondamentaux, … dans un effort de maintenir un **équilibre entre la protection des personnes et l'encouragement à l'innovation des entreprises**

Plan de l'intervention

- 1. - Quel est le contexte du règlement sur l'IA ?
- 2. – Quels sont les objectifs de l'Union européenne avec le RIA?
- 3. - Quelles sont les règles juridiques imposées par le RIA?
- 4. – Quelles sont les sanctions administratives imposées par le RIA?

1. - Quel est le contexte du règlement sur l'IA ?



La proposition de règlement sur l'IA du 21 avril 2021 s'inscrit dans le prolongement d'une série d'évolutions de la politique européenne en matière d'IA.

16 février 2017

Résolution du PE

Règles de droit civil sur la robotique

B. « il est d'une importance fondamentale pour le législateur **d'examiner les conséquences et les effets juridiques et éthiques d'une telle révolution, sans pour autant étouffer l'innovation** »

§ 11. « qu'il est **essentiel que l'Union actualise et complète son cadre juridique actuel**, le cas échéant, en se fondant sur des principes éthiques de référence qui puissent refléter la complexité du sujet que constituent la robotique et ses nombreuses implications sociales, médicales et bioéthiques »

§ 13. « le cadre éthique de référence devrait se fonder sur les principes de bienfaisance, de non-malfaisance, d'autonomie et de justice, sur les principes et valeurs consacrés à l'article 2 du traité sur l'Union européenne et par la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée « Charte »), tels que la dignité humaine, l'égalité, la justice et l'équité, la non-discrimination, le consentement éclairé, le respect de la vie privée et de la vie familiale et la protection des données, ainsi que sur d'autres principes et valeurs fondateurs du droit de l'Union, tels que la non-stigmatisation, la transparence, l'autonomie, la responsabilité individuelle et la responsabilité sociale, et sur les pratiques et codes de déontologie existants »

16 février 2017

Résolution du PE

Règles de droit civil sur la robotique

7 décembre 2018

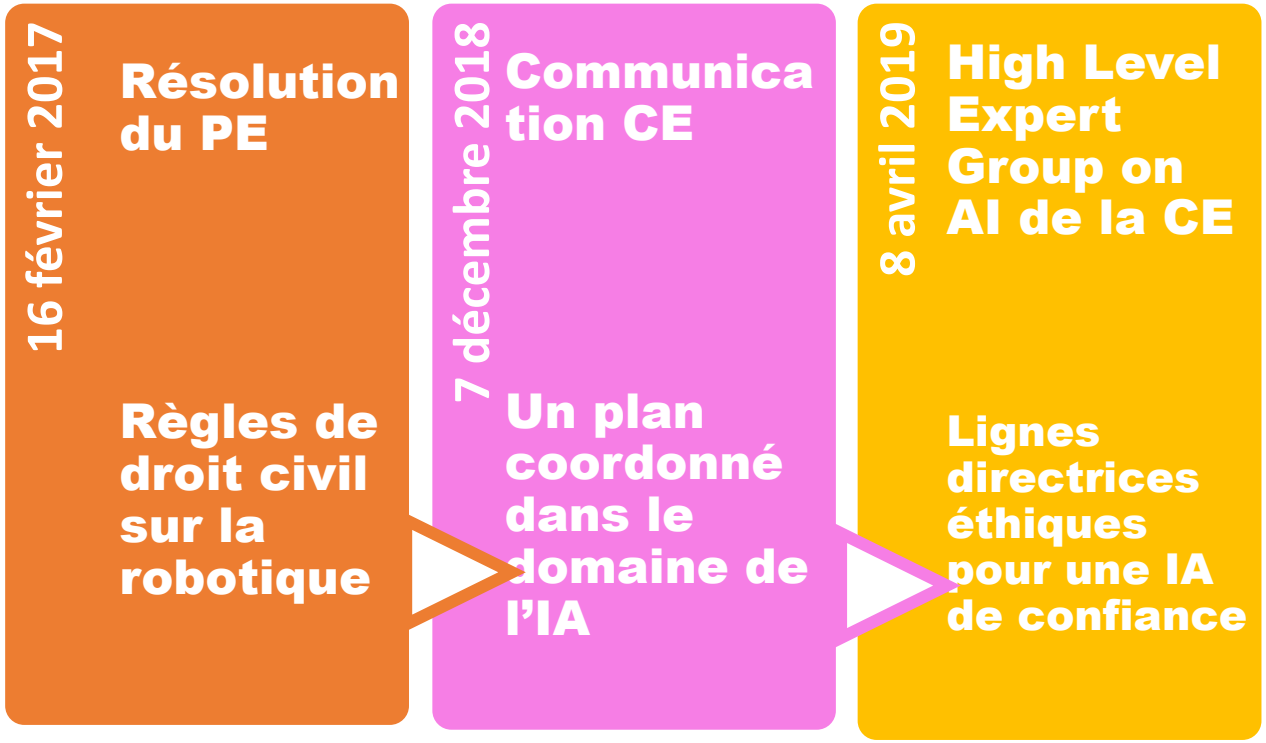
Communication CE

Un plan coordonné dans le domaine de l'IA

Pour la Commission européenne, les défis pour l'Europe sont surtout éthiques ! Elle **fixe des lignes directrices éthiques en IA**.

p. 9 : « *Pour gagner la confiance, qui est nécessaire pour que les sociétés acceptent et utilisent l'IA,* ***la technologie doit être prévisible, responsable et vérifiable, respecter les droits fondamentaux et se conformer à des règles éthiques****. Dans le cas contraire, le recours à l'IA peut donner des résultats non souhaités, comme la création d'une caisse de résonance dans laquelle les personnes ne reçoivent que des informations qui correspondent à leur point de vue ou le renforcement de la discrimination comme dans le cas d'un algorithme devenu raciste en 24 heures après avoir été exposé à du matériel raciste.*

Il est essentiel que les êtres humains comprennent comment l'IA prend ses décisions. L'Europe peut devenir un leader mondial du développement et de l'utilisation de l'IA pour le bien de tous ainsi que de la promotion d'une approche centrée sur le facteur humain et les principes «de la conception respectueuse de l'éthique ».



→ Le respect des principes éthiques permet de garantir la confiance des utilisateurs.

« Une approche digne de confiance est essentielle pour permettre une « compétitivité responsable », **car elle permet à toutes les personnes touchées par les systèmes d'IA de croire que leur conception, leur développement et leur utilisation sont licites, éthiques et solides.** Ces directives ont pour objectif de promouvoir une innovation de l'IA responsable et durable en Europe. Ils cherchent à faire de l'éthique un pilier essentiel du développement d'une approche unique de l'IA, qui **vise à bénéficier, autonomiser et protéger à la fois le développement humain individuel et le bien commun de la société.** Nous pensons que cela permettra à l'Europe de se positionner en tant que leader mondial de l'IA de pointe digne de notre confiance individuelle et collective. **C'est seulement en veillant à la fiabilité que les citoyens européens pourront pleinement profiter des avantages des systèmes d'IA, en sachant que des mesures sont en place pour se protéger des risques potentiels ».**

Quel est le contenu des Lignes directrices éthiques ?

Les 3 éléments clés de la confiance dans l'IA

« **Une IA digne de confiance comporte trois éléments, qui doivent être respectés tout au long du cycle de vie du système**:

1. elle devrait être **licite** et respecter toutes les lois et tous les règlements applicables;
2. elle devrait être **éthique** et garantir le respect des principes et des valeurs éthiques; et
3. elle devrait être **robuste**, tant d'un point de vue technique que social, car même avec de bonnes intentions, les systèmes d'IA peuvent causer des dommages non intentionnels ».

Liste des 7 exigences clés :

- **1 Volonté humaine et surveillance**

Y compris les droits fondamentaux, la volonté humaine et la surveillance de l'humain

- **2 Robustesse technique et sécurité**

Y compris la résilience aux attaques et à la sécurité, le plan de repli et la sécurité générale, la précision, la fiabilité et la reproductibilité

- **3 Confidentialité et gouvernance des données**

Y compris le respect de la vie privée, la qualité et l'intégrité des données et l'accès aux données

- **4 transparence**

Incluant la traçabilité, l'explicabilité et la communication

- **5 Diversité, non-discrimination et équité**

Y compris éviter les biais injustes, l'accessibilité et la conception universelle, et la participation des parties prenantes

- **6 Bien-être sociétal et environnemental**

Durabilité et respect de l'environnement, impact social, société et démocratie

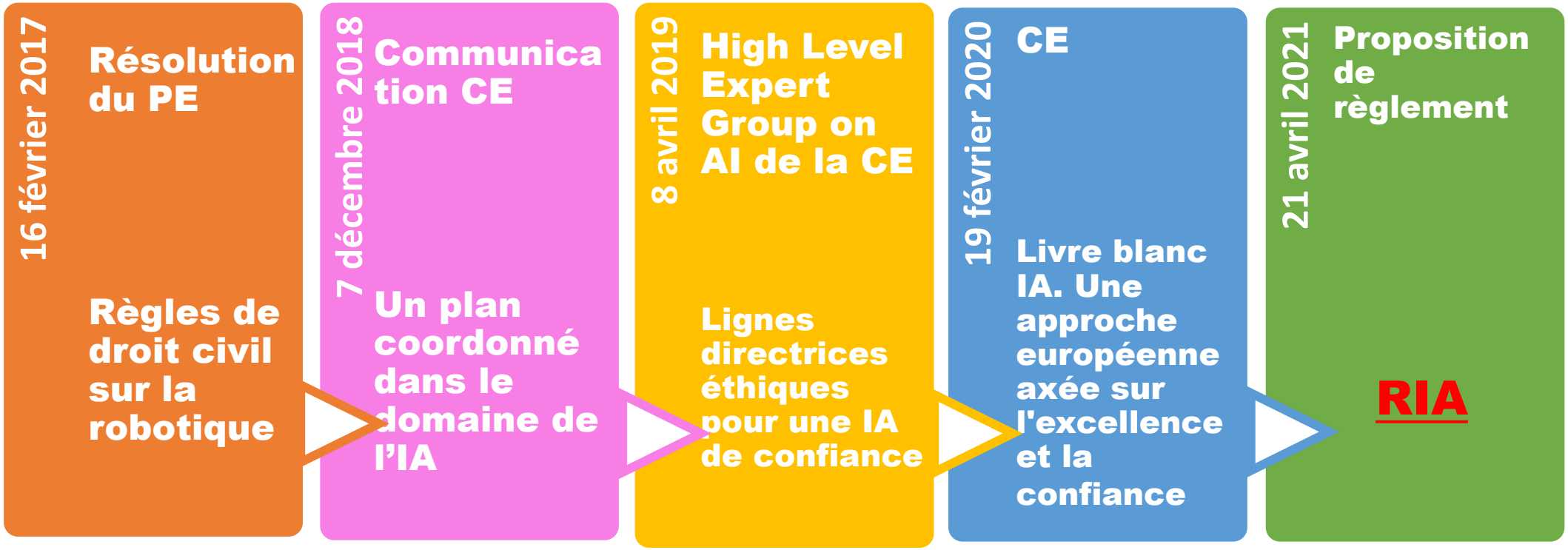
- **7 Rendre compte (responsabilité)**

Y compris la vérifiabilité, la minimisation et le compte rendu des impacts négatifs, les compromis et les réparations.

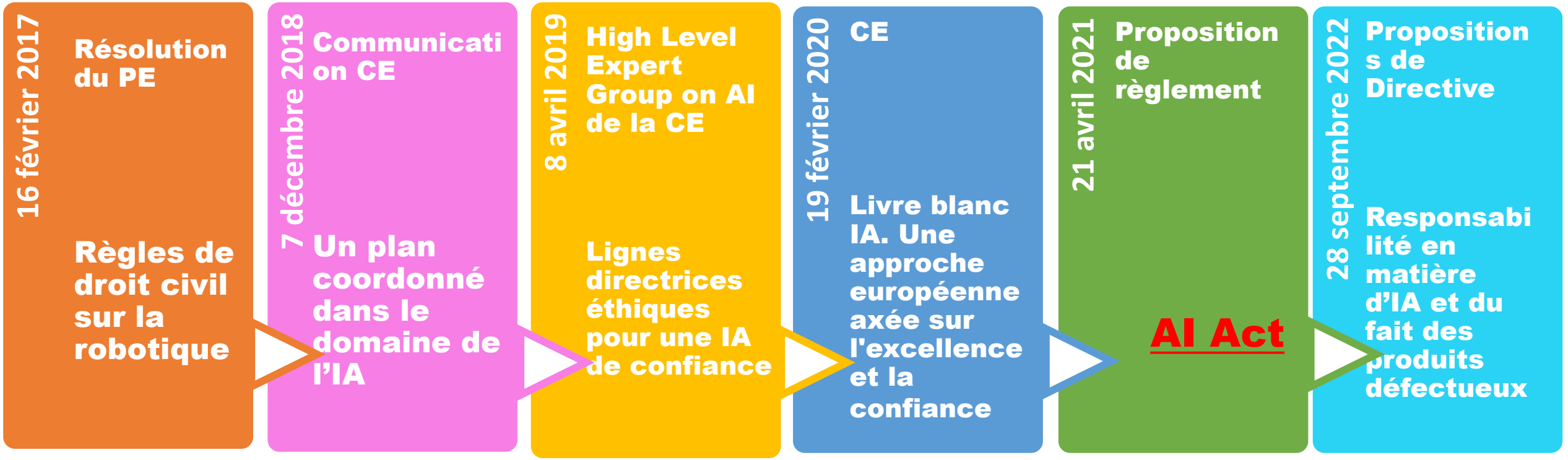
Le Livre blanc **expose les moyens permettant un développement sûr et digne de confiance de l'IA en Europe, respectueux des valeurs et des droits des citoyens européens**.

Il cherche à la fois à **promouvoir l'adoption de l'IA** et à **prendre en considération les risques** associés à certaines utilisations de cette technologie (il initie une approche fondée sur les risques)

Il présente les exigences générales qui constitueront le socle de la future réglementation pour les systèmes d'IA à haut risque.

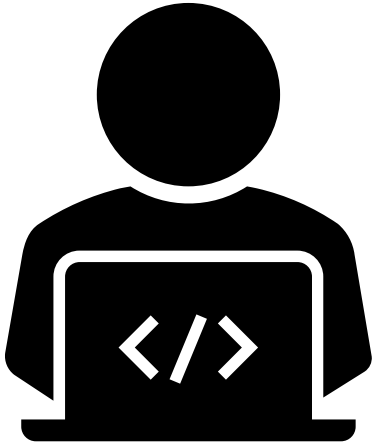


Le règlement sur l'IA concerne uniquement la mise sur le marché et l'utilisation professionnelle des SIA. Elle est englobée dans une politique générale européenne visant à offrir un cadre juridique complet en IA.

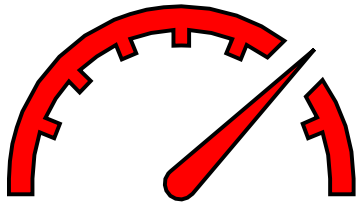


En responsabilité civile, ce sont les premières règles spécifiques aux dommages causés par des systèmes d'IA. Elles couvriront les actions en responsabilité intentées au niveau national pour faute ou omission, quelle que soit la personne ayant commis celle-ci (fournisseurs, développeurs, utilisateurs), qui visent à obtenir réparation pour tout type de dommage couvert par le droit national (vie, santé, biens, vie privée, etc.) et pour tout type de victime (particuliers, entreprises, organisations, etc.).
La directive introduit deux mesures principales: la «présomption de causalité», qui dispensera les victimes de l'obligation d'expliquer en détail comment le dommage a été causé par une faute ou une omission spécifique; et l'accès aux éléments de preuve détenus par les entreprises ou les fournisseurs, lorsque ces derniers utilisent de l'IA à haut risque.

2. – Quels sont les objectifs de l’Union européenne avec le RIA?



Face aux enjeux et aux défis, la Commission a tenté de trouver un équilibre entre :



L’adoption d’exigences minimales pour encadrer les risques et problèmes liés à l’IA

L’établissement d’un cadre suffisamment flexible pour ne pas contraindre ou entraver indûment le développement technologique, ni augmenter de manière disproportionnée les coûts de mise sur le marché

2.1. Les efforts de le RIA en faveur de l'innovation

2.1.1. Une stratégie économique européenne au cœur du RIA

2.1.2 Les mesures mises en place par le RIA en faveur du développement et de l'innovation

2.1.3 L'adoption de mesures complémentaires au RIA

2.1.1. Une stratégie économique européenne au cœur de l'AI Act

Les Etats et les entreprises dans le monde ont investi considérablement dans l'IA.

- Les leaders : Etats-Unis, suivis par la Chine.
- Mais l'UE est une puissance économique non négligeable : marché de près de 500 millions de personnes.

Quelle stratégie de l'UE pour le RIA?

→ La réponse européenne consiste dans l'adoption d'une nouvelle stratégie pour développer une souveraineté reposant sur la règlementation afin de créer un précédent pour la réglementation de l'IA dans le monde entier.

→ Cette politique a d'ailleurs marqué le point de départ d'une surenchère de législations sur l'IA dans le monde (Australie, Canada ou Royaume-Uni).

→ La règlementation européenne peut aussi être un vecteur d'hégémonie de l'UE en raison de l'« effet Bruxelles »
(= processus de mondialisation qui "se produit lorsqu'un seul État est capable d'externaliser ses lois et réglementations hors de ses frontières par le biais de mécanismes de marché, ce qui entraîne une mondialisation des normes").

C'est déjà le cas avec le RGPD

→ La réglementation comme barrière à l'innovation et au développement des entreprises ? Face à des technologies potentiellement dangereuses pour les personnes, la mise en place d'une règlementation dédiée a toujours été une méthode efficace qui ne nuisait en rien à l'innovation.

2.1.2 Les mesures en faveur de l'innovation

✓ Le bac à sable réglementaire de l'IA

Il s'agit d' « un cadre contrôlé mis en place par une autorité compétente qui offre aux fournisseurs ou fournisseurs potentiels de systèmes d'IA la possibilité de développer, d'entraîner, de valider et de tester, lorsqu'il y a lieu en conditions réelles, un système d'IA innovant, selon un plan du bac à sable pour une durée limitée sous surveillance réglementaire » (article 3, § 55).

→ Chaque Etat membre doit en constituer au moins un.

→ Le fournisseur reste juridiquement responsable des dommages.

✓ Les essais en conditions réelles en dehors des bacs à sable réglementaires

Il s'agit des « essais temporaires d'un système d'IA aux fins de sa destination en conditions réelles en dehors d'un laboratoire ou d'un environnement simulé d'une autre manière, visant à recueillir des données fiables et solides et à évaluer et vérifier la conformité du système d'IA aux exigences du présent règlement » (article 3, § 57).

→ Attention particulière à la protection des sujets des essais en conditions réelles (consentement éclairé)

→ Le fournisseur reste juridiquement responsable des dommages.

✓ Des séries de mesures en faveur des start-ups et PME

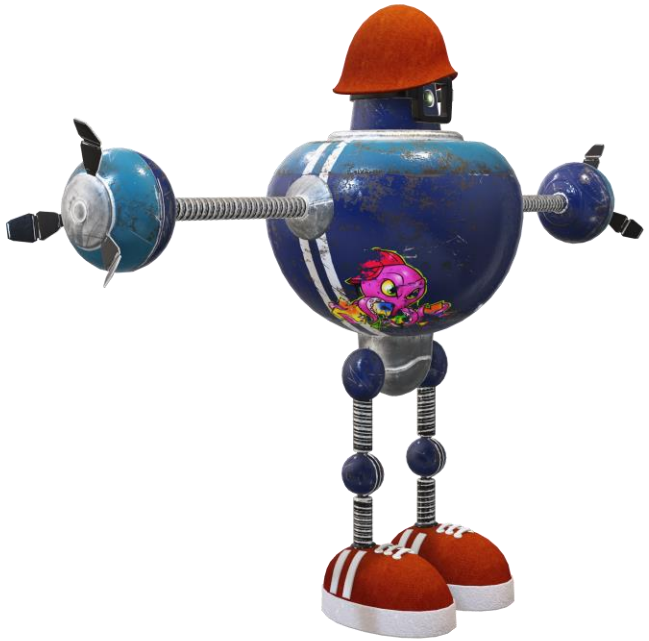
Comme un accès facilité au bac à sable, des obligations plus limitées, des sanctions moins importantes, etc.

2.1.3 L’adoption de mesures complémentaires à l’AI Act

- Différents programmes de **soutiens financiers** de l’UE comme « Horizon Europe » (env. 100 milliards d’euros pour la période 2021-2027), ou « Horizon Europe » et « Europe numérique » (dernièrement, soutien financier d’env. 4 milliards d’euros sur l’IA générative).

- **Accès privilégié aux supercalculateurs** pour les start-ups et PME pour les encourager à développer une IA digne de confiance et respectueuse des valeurs et des règles européennes

2.2. La promotion par le RIA d'une IA axée sur le facteur humain et digne de confiance



2.2.1 Le développement d'une IA digne de confiance par grâce aux dispositions protectrices des personnes

2.2.2 Le développement d'une approche éthique au travers du RIA

2.2.3 Les initiatives législatives complémentaires au RIA pour une IA de confiance

2.2.1 Le développement d'une IA digne de confiance par grâce aux dispositions protectrices des personnes

- Volonté de mettre en place une protection uniforme des personnes dans toute l'UE (→ harmonisation des règles entre tous les Etats membres)

- La protection des droits fondamentaux passe par la Charte des droits fondamentaux obligatoire dans l'UE.

2.2.2 Le développement d'une approche éthique au travers du RIA

L'UE accorde une place importante à une IA éthique qu'elle a évoquée dans différents rapports, résolutions ou livres blancs, ainsi que dans le RIA.

→ Contrairement au droit, l'éthique n'est pas obligatoire.

→ La méthode choisie pour tenir compte de l'éthique est surtout centrée sur les codes de conduite volontaires pour les systèmes d'IA et les modèles d'IA à usage général qui vient donc ajouter une couche d'éthique à des règles obligatoires.

→ Craintes ? Ethics-washing.

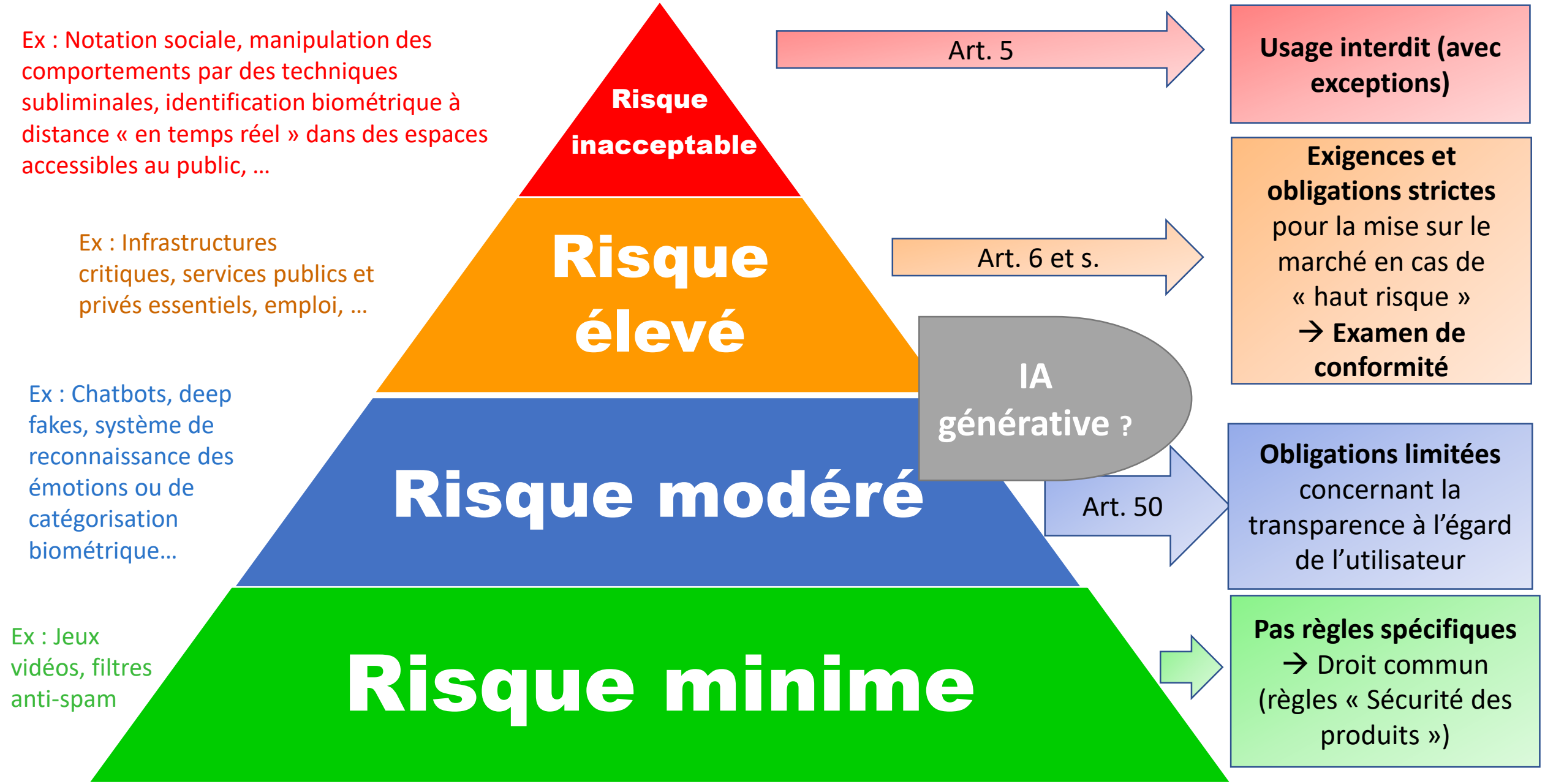
2.2.3 Les initiatives législatives complémentaires au RIA pour une IA de confiance

L'UE a proposé plusieurs initiatives juridiques interdépendantes et complémentaires au RIA.

→ Révision des législations sectorielles sur la sécurité des produits pour les adapter au développement des technologies d'IA (ex : Règlement sur les machines révisé en juin 2023, Règlement sur la sécurité générale des produits révisé en mai 2023)

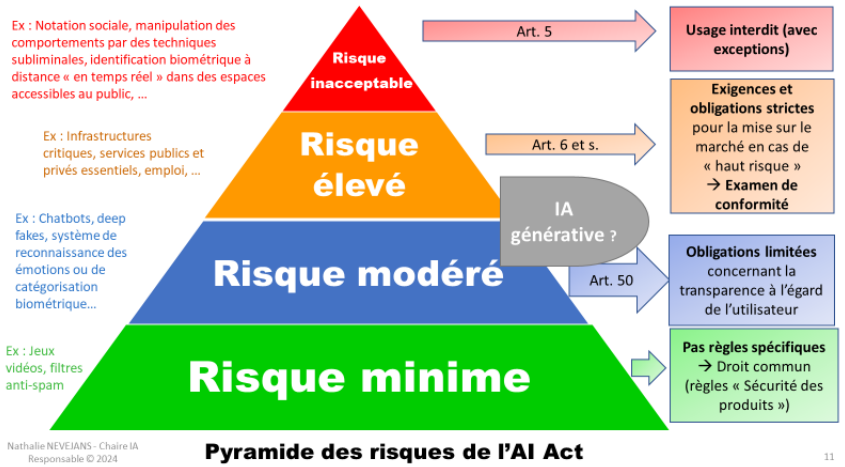
→ Créations ou modifications de directives concernant la responsabilité en cas de dommages causés par les systèmes d'IA (Projet de directive sur un cadre de responsabilité civile et révision de la directive sur les produits défectueux).

3. - Quelles sont les règles juridiques imposées par le RIA?



Pyramide des risques de l'AI Act

3.1 Usages à risque inacceptable



Usages à risque inacceptable

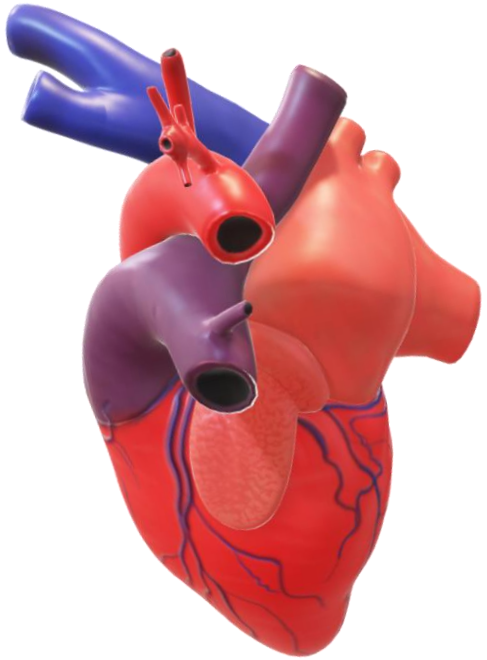
La proposition contient une liste de **systèmes d'IA dont l'utilisation est considérée comme inacceptable car contraire aux valeurs de l'UE**, en raison de violations des droits fondamentaux (article 5).

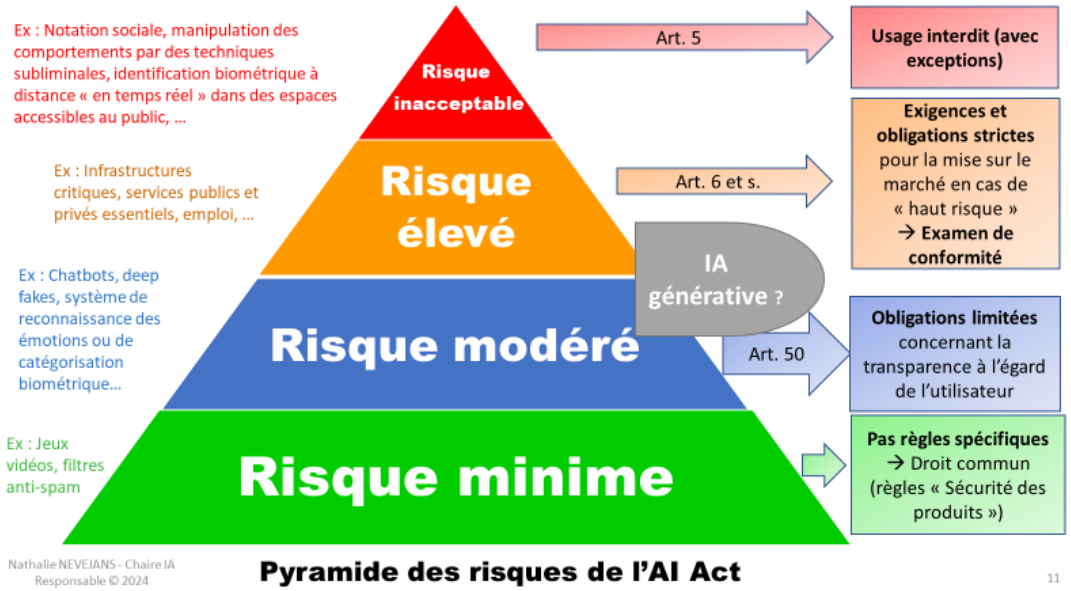
Usages à risque inacceptable

→ **Sont interdits les pratiques suivantes en vertu de l'article 5 :**

- **Techniques subliminales ou de techniques délibérément manipulatrices ou tr**ompeuses pour fausser significativement le comportement d'une personne ou d'un groupe l'amenant à prendre une décision susceptible de causer un préjudice important
- **L'exploitation des vulnérabilités d'une personne** ou d'un groupe en raison de ses caractéristiques spécifiques pour en altérer significativement le comportement l'amenant à prendre une décision susceptible de causer un préjudice important
- La **catégorisation biométrique** des personnes physiques en fonction d'informations sensibles, sauf pour les données biométriques légalement acquises
- La **notation sociale** à des fins publiques ou privées conduisant à un traitement préjudiciable ou défavorable de certaines personnes ou groupes
- Le recours à la **police prédictive** sur le seul fondement du profilage ou des traits de personnalité et de ses caractéristiques, sauf si le système d'IA est utilisé pour soutenir les évaluations humaines fondées sur des faits objectifs et vérifiables liés à la criminalité
- L'exploitation de bases de données de reconnaissance faciale construite grâce à un recours au scraping non ciblé
- Le recours à des **systèmes capables de déduire les émotions d'une personne sur les lieux de trav**ail ou dans les établissements d'enseignement, sauf pour des raisons médicales ou de sécurité .
- L'utilisation par les services répressifs de **l'identification biométrique à distance en temps réel dans des espaces accessibles au public**, sous réserve d'exceptions strictement limitées (comme l'enlèvement)

3.2 Usages à haut risque





Usages à haut risque

3.2.1. Règles de classification d'un système d'IA à haut risque

3.2.2. Parties prenantes, et leurs exigences et obligations

3.2.1 - Règles de classification d'un système à haut risque (article 6)

Article 6
Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque

Soit il remplit les conditions de l'art. 6, § 1, a) et b)

Soit il remplit les conditions de l'art. 6, § 2

Annexe I (extraits)

- Règlement (EU) 2017/745 Dispositifs médicaux
- Règlement Machines 2023/1230 du 14 juin 2023;
- Directive 2009/48/EC Jouets ;
- Règlement (EU) 2016/425 sur les équipements de protection individuelle ;

- le système d'IA est destiné à être utilisé comme composant de sécurité d'un produit couvert par la **législation d'harmonisation de l'Union dont la liste figure à l'annexe I**, ou le système d'IA constitue lui-même un tel produit.

- le produit dont le composant de sécurité visé au point a) est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une **évaluation de conformité par un tiers en vue de la mise sur le marché ou de la mise en service de ce produit** conformément à la législation d'harmonisation de l'Union dont la liste figure à l'annexe I.

Les systèmes d'IA visés à l'annexe III sont considérés comme étant à haut risque

Exception : lorsque la SIA ne présente pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques, y compris en n'ayant pas d'incidence significative sur le résultat de la prise de décision

Annexe III (NB : mises à jour possibles)

1 : Systèmes biométriques et fondés sur la biométrie
2 : gestion et exploitation des infrastructures essentielles (ex : composants de sécurité dans la gestion et le fonctionnement de la fourniture d'eau, de gaz, de chauffage, d'électricité et des infrastructures numériques critiques)
3 : éducation et formation professionnelle
4 : emploi, gestion des salariés et accès au travail indépendant
5 : accès aux services privés essentiels et aux services publics (ex : systèmes d'IA destinés à être utilisés par les autorités publiques ou en leur nom pour évaluer l'éligibilité des personnes physiques aux prestations et services d'aide sociale, les services de santé et services essentiels, qui comprennent sans s'y limiter le logement, l'électricité, le chauffage/refroidissement et l'internet, ainsi que pour octroyer, réduire, révoquer, augmenter ou récupérer ces prestations et services)
6 : application de la loi
7 : gestion des flux migratoires, de l'asile et des contrôles aux frontières
8 : administration de la justice et processus démocratique (ex : systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums)

Usages à haut risque

3.2.2. Parties prenantes, et leurs exigences et obligations

Fournisseurs

Déployeurs (anciennement : utilisateurs)

Fabricants du produit

Importateurs

Distributeurs

Usages à haut risque

Fournisseurs : exigences et obligations

Usages à haut risque

- **Le fournisseur d'un système d'IA est l'acteur central** = il développe (ou pas) et met sur le marché le système d'IA

Il doit respecter les exigences pour la mise sur le marché du système d'IA à haut risque : art. 8 à 15.

Il doit respecter les obligations de mise sur le marché du système d'IA à haut risque : art. 16 à 21.

Usages à haut risque

Quelles sont les exigences essentielles pour le fournisseur (articles 8 à 15) ?

- Mettre en place un **système de gestion des risques** tout au long du cycle de vie du SIA à haut risque (art. 9)
- S'agissant des **données et de la gouvernance des données**, si les SIA à haut risque utilisent des techniques impliquant l'apprentissage de modèles à l'aide de données, ils doivent être développés sur la base d'ensembles de données d'apprentissage, de validation et d'essai qui satisfont aux critères de qualité, notamment pour détecter les biais éventuels et les éventuelles erreurs. Si le développement des systèmes d'IA ne recoure pas à l'apprentissage du modèle, les exigences de qualité ne concernent alors que les ensembles de données d'essai. Il existe une exception autorisant le traitement des données personnelles sensibles en vue de détecter les biais (art. 10)
- Etablir avant la mise sur le marché ou en service une **documentation technique** et la tenir à jour dans le but de démontrer que le SIA à haut risque satisfait aux exigences et fournir aux autorités les informations nécessaires pour évaluer la conformité du système d'IA à ces exigences. Il contient, au minimum, la liste des informations à renseigner au titre de l'annexe IV sur la documentation technique (art. 11)
- Tenir des **registres** qui permettent techniquement l'enregistrement automatique d'un certain nombre d'événements pertinents pendant toute la durée de vie du système (art. 12)
- Des obligations relative à la **transparence** (notamment le problème des biais injustes) et les informations à livrer aux déployeurs (art. 13)
- Mettre en place des mesures de **contrôle h**umain (**art. 14)**
- **Mesures en matière de** précision, robustesse et cybersécurité (art. 15).

Usages à haut risque

Quelles sont les <u>obligations</u> du fournisseur pour mettre sur le marché des systèmes d'IA à haut risque (articles 16 à 22) ?

- **Procédure d'évaluation de la conformité**, qui devra être recommencée en cas de modification substantielle des systèmes ou de leur finalité
- **Déclaration UE de conformité** pour garantir un niveau élevé de fiabilité de leur système et apposer le marquage CE qui permettra à leur système de circuler librement dans le marché intérieur
- **Système de gestion de la qualité** afin de garantir qu'il respecte les exigences
- Conserver non seulement toute la **documentation** (documentation technique, documentation relative au système de gestion de la qualité, etc.), mais aussi le cas échéant les journaux générés automatiquement par le système d'IA.
- En cas de non-conformité ou de risque de non-conformité au Règlement, les fournisseurs doivent prendre immédiatement des **mesures correctives nécessaires** pour mettre leur système en conformité, le retirer, le mettre hors service ou le rappeler, selon les cas, et informer les opérateurs concernés.
- Coopérer avec les autorités nationales compétentes

Usages à haut risque

Déployeur (anciennement Utilisateurs) : obligations

Usages à haut risque

- **Le déployeur** = il utilise le SIA dans une activité à caractère professionnel

Il doit respecter des obligations propres au déployeur (art. 26).

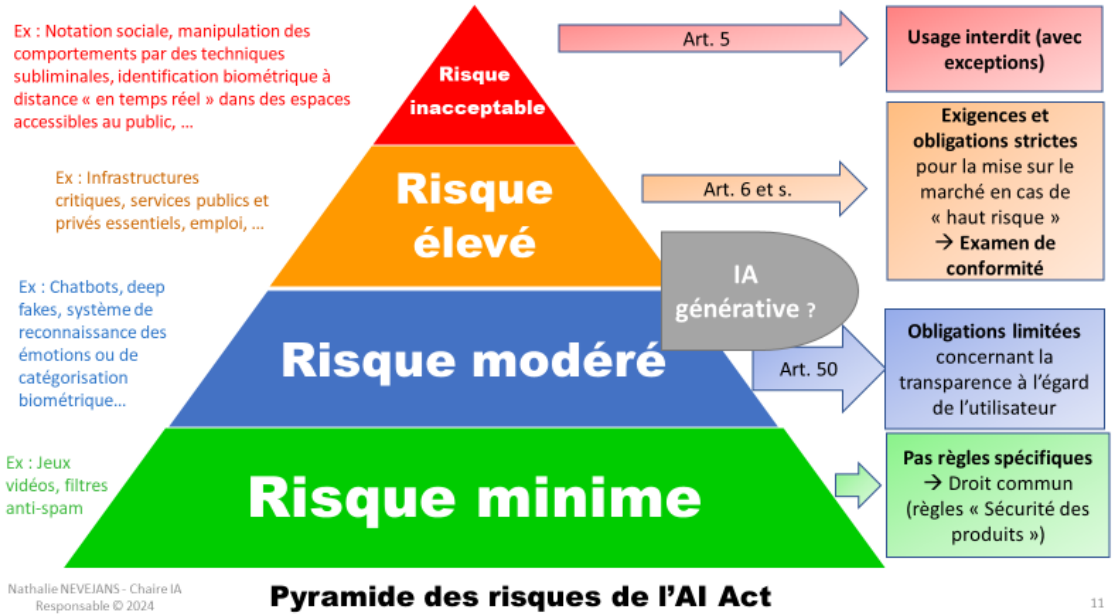
Usages à haut risque

Quelles sont les obligations propres pour l'utilisation du SIA à haut risque des déployeurs (art. 26) ?

- Prendre les **mesures techniques et organisationnelles** appropriées pour s'assurer qu'ils utilisent les systèmes d'IA à haut risque conformément aux instructions d'utilisation.
- Veiller à ce que les personnes chargées de mettre en œuvre la **surveillance humaine** disposent des compétences nécessaires, spécialement un niveau adéquat de connaissance de l'IA, une formation et une autorité leur permettant de s'acquitter correctement de ces tâches.
- Veiller à la **pertinence et la représentativité** au regard de la finalité du système d'IA des données d'entrée si elles se trouvent sous leur contrôle.
- Surveiller le **fonctionnement du système d'IA** sur la base de la notice d'utilisation et, le cas échéant, informent les fournisseurs
- Assurer la **tenue des journaux générés automatiquement** par le système d'IA à haut risque si ces journaux se trouvent sous leur contrôle.
- **Informations de diverses personnes** en cas de risque ou d'incident grave.
- **Conserver les journaux générés automatiquement** qu'ils ont sous leur contrôle pendant un délai,
- Avant de mettre en service ou d'utiliser un SIA à haut risque sur le lieu de travail, les déployeurs/**employeurs informent les représentants des travailleurs et les travailleurs concernés** qu'ils seront soumis à l'utilisation du système d'IA à haut risque, etc.

+ **Obligation de réaliser une analyse d'impact sur les droits fondamentaux** préalablement à la mise en service d'un système d'IA à haut risque pour les déployeurs qui sont des organismes de droit public ou des entités privées fournissant des services publics pour les déployeurs relevant de certains points de l'Annexe III.

3.3 Usages à risque modéré



Usages à risque modéré

Au fil du temps, cette catégorie est devenue complexe avec l'apparition de l'IA générative. On a donc :

- Des obligations de transparence spécifiques pour les fournisseurs et les déployeurs de certains systèmes d'IA et GPAI
- Des règles applicables aux seuls modèles GPAI

Usages à risque modéré

3.3.1 Des obligations de transparence spécifiques (consistant en une information spécifique) pour certains systèmes d'IA et GPAI : article 50

Quatre domaines soumis à l'obligation spécifique de transparence

Une précision avant de développer.
Nous avons déjà défini les SIA, mais par encore les systèmes GPAI. Selon l'art. 3, 66), le système d'IA à usage général est « un système d'IA qui est fondé sur un modèle d'IA à usage général et qui a la capacité de répondre à diverses finalités, tant pour une utilisation directe que pour une intégration dans d'autres systèmes d'IA ».

Usages à risque modéré

1. Les fournisseurs veillent à ce que les **systèmes d'IA destinés à interagir directement avec des personnes physiques** soient **conçus et développés de manière à ce que les personnes physiques concernées soient informées qu'elles interagissent avec un système d'IA, sauf si cela ressort clairement du point de vue d'une personne physique normalement informée et raisonnablement attentive et avisée**, compte tenu des circonstances et du contexte d'utilisation.
2. Les fournisseurs de systèmes d'IA, **y compris de systèmes d'IA à usage général**, qui **génèrent des contenus de synthèse de type audio, image, vidéo ou texte**, veillent à ce que les **sorties des systèmes d'IA soient marquées dans un format lisible par machine et identifiables comme ayant été générées ou manipulées par une IA**. Les fournisseurs veillent à ce que leurs solutions techniques soient aussi efficaces, interopérables, solides et fiables que la technologie le permet, compte tenu des spécificités et des limites des différents types de contenus, des coûts de mise en œuvre et de l'état de la technique généralement reconnu, comme cela peut ressortir des normes techniques pertinentes. |…]
3. Les déployeurs d'un **système de reconnaissance des émotions ou d'un système de catégorisation biométrique informent les personnes physiques qui y sont exposées du fonctionnement du système** et traitent les données à caractère personnel conformément au règlement (UE) 2016/679, au règlement (UE) 2018/1725 et à la directive (UE) 2016/680, selon le cas.[…]
4. Les déployeurs d'un **système d'IA qui génère ou manipule des images ou des contenus audio ou vidéo** constituant un hypertrucage indiquent que **les contenus ont été générés ou manipulés par une IA**. […] Lorsque le contenu fait partie d'une **oeuvre ou d'un programme manifestement artistique, créatif, satirique, fictif ou analogue, les obligations de transparence énoncées au présent paragraphe se limitent à la divulgation de l'existence de tels contenus générés ou manipulés d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'oeuvre**.
Les déployeurs d'un système d'IA qui génère ou manipule des textes publiés dans le but d'informer le public sur des questions d'intérêt public indiquent que le texte a été généré ou manipulé par une IA […]

Usages à risque modéré

3.3.1 Des obligations de transparence spécifiques (consistant en une information spécifique) pour certains systèmes d'IA et GPAI : article 50

<u>Attention</u> :

- Si le système d'IA visé dans l'un des 4 cas est à haut risque, on applique aussi les règles sur le haut risque + celles de l'article 50

- Sinon, s'il n'est pas à haut risque, on applique seulement l'article 50
  → Ce sera un vrai système à risque modéré.

Usages à risque modéré

3.3.2 Les règles applicables aux modèles GPAI

Définition du modèle d'IA à usage général (modèle GPAI) : « un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché » (art. 2, 63))

Après une période confuse concernant les désaccords en matière d'IA générative, un compromis a été trouvé sur les modèles d'IA à usage général (« GPAI ») sous la forme d'une approche à 2 niveaux.

Niveau 1 : des obligations identiques les fournisseurs de tous les modèles GPAI

Article 53
Obligations incombant aux fournisseurs de modèles d'IA à usage général

1. Les fournisseurs de modèles d'IA à usage général:

a) élaborent et tiennent à jour la **documentation technique du modèle**, y compris son processus d'entraînement et d'essai et les résultats de son évaluation, qui contient, au minimum, les informations énoncées à l'annexe XI aux fins de la fournir, sur demande, au Bureau de l'IA et aux autorités nationales compétentes;

b) élaborent, tiennent à jour et mettent à disposition **des informations et de la documentation à l'intention des fournisseurs de systèmes d'IA qui envisagent d'intégrer le modèle d'IA à usage général dans leurs systèmes d'IA**. Sans préjudice de la nécessité d'observer et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national, ces informations et cette documentation:

i) permettent aux fournisseurs de systèmes d'IA d'avoir une bonne compréhension des capacités et des limites du modèle d'IA à usage général et de se conformer aux obligations qui leur incombent en vertu du présent règlement; et

ii) contiennent, au minimum, les éléments énoncés à l'annexe XII;

c**) mettent en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteu**r et droits voisins, et notamment à identifier et à respecter, y compris au moyen de technologies de pointe, une réservation de droits exprimée conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790;

d) élaborent et mettent **à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle** d'IA à usage général, conformément à un modèle fourni par le Bureau de l'IA.

2. **Les obligations énoncées au paragraphe 1, points a) et b), ne s'appliquent pas aux fournisseurs de modèles d'IA qui sont publiés dans le cadre d'une licence libre et ouverte** permettant de consulter, d'utiliser, de modifier et de distribuer le modèle, et dont les paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics. Cette exception ne s'applique pas aux modèles d'IA à usage général présentant un risque systémique.

[…]

Niveau 2 : des obligations supplémentaires pour les modèles GPAI présentant des risques systémiques

Article 51 Classification de modèles d'IA à usage général en tant que modèles d'IA à usage général présentant un risque systémique

1. Un modèle d'IA à usage général est classé comme modèle d'IA à usage général présentant un risque systémique s'il remplit l'une des conditions suivantes:

a) il dispose de capacités à fort impact évaluées sur la base de méthodologies et d'outils techniques appropriés, y compris des indicateurs et des critères de référence;

b) sur la base d'une décision de la Commission, d'office ou à la suite d'une alerte qualifiée du groupe scientifique, il possède des capacités ou un impact équivalents à ceux énoncés au point a), compte tenu des critères définis à l'annexe XIII.

2. Un modèle d'IA à usage général est présumé avoir des capacités à fort impact conformément au paragraphe 1, point a), lorsque la quantité cumulée de calcul utilisée pour son entraînement mesurée en opérations en virgule flottante est supérieure à 10^{25}.

[…]

Article 55
Obligations incombant aux fournisseurs
de modèles d'IA à usage général présentant un risque systémique

1. Outre les obligations énumérées à l'article 53**, les fournisseurs de modèles d'IA à usage général présentant un risque systémique:**

a) effectuent une évaluation des modèles sur la base de protocoles et d'outils normalisés reflétant l'état de la technique, y compris en réalisant et en documentant des essais contradictoires des modèles en vue d'identifier et d'atténuer le risque systémique;

b) évaluent et atténuent les risques systémiques éventuels au niveau de l'Union, y compris leurs origines, qui peuvent découler du développement, de la mise sur le marché ou de l'utilisation de modèles d'IA à usage général présentant un risque systémique;

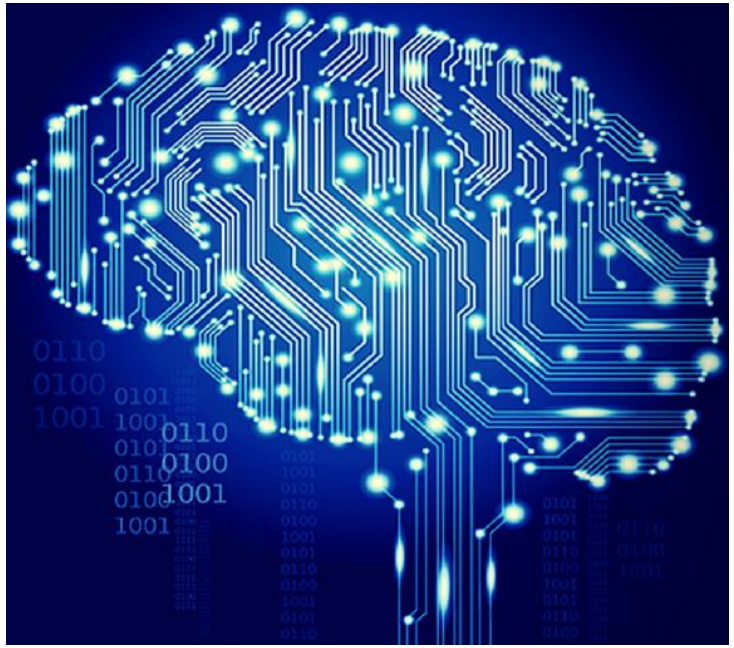
c) suivent, documentent et communiquent sans retard injustifié au Bureau de l'IA et, le cas échéant, aux autorités nationales compétentes les informations pertinentes concernant les incidents graves ainsi que les éventuelles mesures correctives pour y remédier;

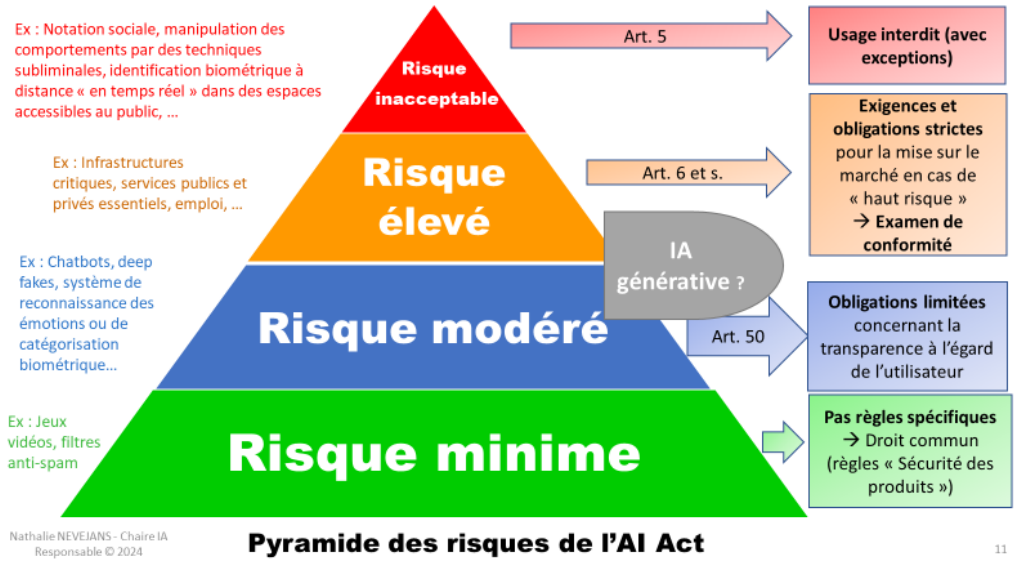
d) garantissent un niveau approprié de protection en matière de cybersécurité pour le modèle d'IA à usage général présentant un risque systémique et l'infrastructure physique du modèle.

2. Les fournisseurs de modèles d'IA à usage général présentant un risque systémique peuvent s'appuyer sur des **codes de bonne pratique** au sens de l'article 56 pour démontrer qu'ils respectent les obligations énoncées au paragraphe 1 du présent article, jusqu'à la publication d'une norme harmonisée. Les fournisseurs qui respectent une norme européenne harmonisée sont présumés se conformer aux obligations énoncées au paragraphe 1 du présent article. Les fournisseurs de modèles d'IA à usage général présentant un risque systémique qui n'observent pas un code de bonne pratique approuvé démontrent qu'ils disposent d'autres moyens appropriés de mise en conformité et les soumettent à l'approbation de la Commission.

3. Toute information ou documentation obtenue en vertu du présent article, y compris les secrets d'affaires, est traitée dans le respect des obligations de confidentialité énoncées à l'article 78.

Usages à risque minime ou nul





Usages à risque minime ou nul

Ex : Jeux vidéos, filtres anti-spam reposant sur l'IA

- **Pas de règles au titre de l'AI Act. On applique donc les autres directives, comme la directive sécurité des produits.** Les fournisseurs sont encouragés à appliquer, sur la base du volontariat, des codes de conduite facultatifs.

4. – Quelles sont les sanctions en cas de non-conformité au RIA ?

Quelles sont les sanctions en cas de non-conformité au RIA ?

PÉNALITÉS DE NON-CONFORMITÉ POUR LES SYSTÈMES D'IA INTERDITS (ARTICLE 5)

- 1 août-2025 (période de grâce de 6 mois)
- L'amende peut s'élever jusqu'à 35 millions d'euros ou pour les entreprises jusqu'à 7 % du chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent

PÉNALITÉ DE NON-CONFORMITÉ POUR LES SYSTÈMES À HAUT RISQUE

- Inscrits à l'annexe III : 1er août 2026 (pas de période de grâce)
- Inscrits à l'annexe I : 1er août 2027 (pas de période de grâce).
- L'amende peut s'élever jusqu'à 15 millions d'euros ou pour les entreprises 3 % du chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent

PÉNALITÉ DE NON-CONFORMITÉ POUR LES MODÈLES D'IA À USAGE GÉNÉRAL

- 1er août 2026 (période de grâce de 1 an).
- Jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial total en l'absence de risque systémique
- Jusqu'à 40 millions d'euros ou 8% du chiffre d'affaires annuel mondial total en cas de risque systémique

PÉNALITÉ POUR NON-COOPÉRATION AVEC LES AUTORITÉS

- L'amende peut aller jusqu'à 7,5 millions d'euros ou pour les entreprises 1 % du chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent

→Pour chacune de ces infractions, c'est le seuil le plus faible des deux montants qui est retenu pour les PME et le plus élevé des deux pour les autres entreprises.

→Le montant de l'amende est fixé dans chaque cas individuel en fonction des circonstances pertinentes de la situation spécifique, comme par exemple la nature, la gravité et la durée de l'infraction, la taille ou le chiffre d'affaire de l'entreprise, l'existence d'autres condamnations ou encore la coopération avec les autorités.

Conclusion

Quelles sont les principales échéances pour la ise en œuvre du RIA ?

ENTRÉE EN VIGUEUR

Signé le 13 juin, publication au Journal officiel de l'UE le 12 juillet 2024, entrée en vigueur le 1er août 2024.

Source : Peter Ide-Kostic, Introduction to the «AI Act», 3e conference Science Europe, 28 juin 2024

INTERDICTION DES PRATIQUES D'IA

L'interdiction de certaines pratiques d'IA de l'article 5 entrera en vigueur le 1er février 2025.

CONFORMITÉ DES SYSTÈMES D'IA À HAUT RISQUE

- 1er août 2026 pour les cas directs (annexe III)
- 1er août 2027 pour la législation sectorielle (annexe I)
- fin 2030 pour les systèmes spécifiques utilisés pour soutenir l'application de la législation dans les États membres et les agences de l'UE
- 1er août 2030 pour les systèmes utilisés par les autorités publiques.

CONFORMITÉ DES MODÈLES D'IA À USAGE GÉNÉRAL (GPAI)

- Les nouveaux modèles GPAI mis sur le marché après le 1er août 2025 doivent être mis en conformité immédiatement,
- Les modèles GPAI existants (mis sur le marché avant le 1er août 2025) auront jusqu'au 1er août 2027 pour se mettre en conformité.
- Un projet de code de pratiques et de lignes directrices visant à faciliter la mise en conformité devrait être prêt au cours du deuxième trimestre 2025.

CONFORMITÉ DES SYSTÈMES D'IA HAUT RISQUE

- 1er août 2026 pour les cas directs (annexe III)
- 1er août 2027 pour la législation sectorielle (annexe I)
- Fin 2030 pour les systèmes spécifiques utilisés pour soutenir l'application de la législation dans les États membres et les agences de l'UE
- 1er août 2030 pour les systèmes utilisés par les autorités publiques.

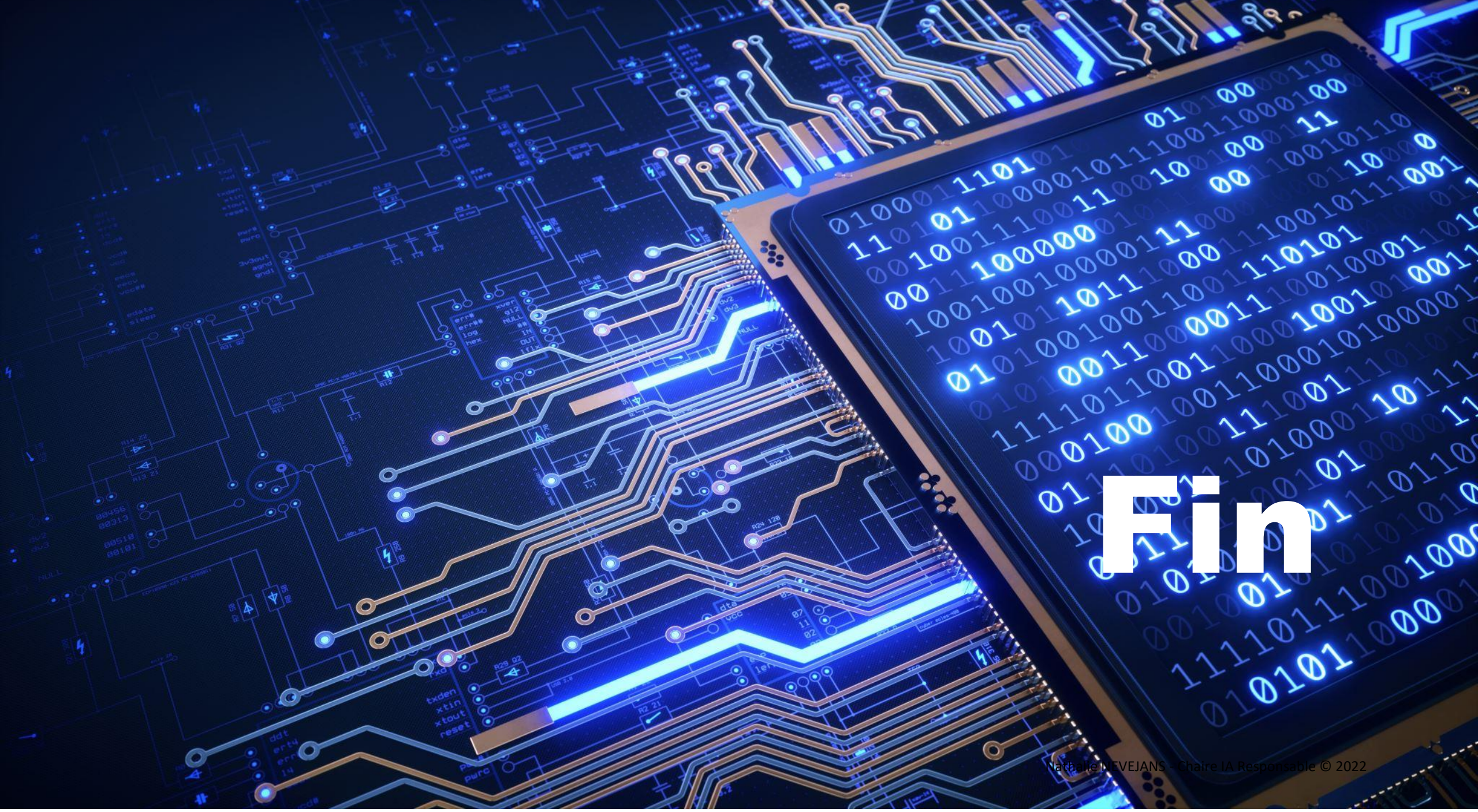
Pour finir, les entreprises européennes doivent-elles se réjouir de l'adoption prochaine de le RIA?

le RIA est la solution et non le problème : ce texte constitue une **clé pour la confiance des citoyens européens**.

Sans texte légal pour réguler l'IA : ce serait (au mieux) l'empire de la *soft law*.

→ Cela laisserait le champ libre aux pays hors UE de développer une IA non éthique, sans aucune mesure protectrice des citoyens européens.

Les chercheurs et la R&D ne sont pas impactés directement.



Prix 2019 Francis Durieux de l'Académie des sciences morales et politiques (France)

Nathalie NEVEJANS, TRAITÉ DE DROIT ET D'ÉTHIQUE DE LA ROBOTIQUE CIVILE,

LEH édition, 2017, *1232 pages.*

Merci d'avoir écouté. Des questions ?

CHAIRE IA RESPONSABLE

UNIVERSITÉ D'ARTOIS