Résumé de haut niveau de la loi sur l'IA

27 février 2024

Dans cet article, nous vous proposons un résumé de haut niveau de la loi sur l'IA, en sélectionnant les parties les plus susceptibles de vous concerner, qui que vous soyez. Le cas échéant, nous fournissons des liens vers le document original afin que vous puissiez toujours vous référer au texte de la loi.

*Pour explorer vous-même le texte intégral de la loi sur l'IA, utilisez notre **Explorateur de la loi sur l'IA**. Si vous souhaitez savoir quelles sont les parties du texte qui vous concernent le plus, vous pouvez également utiliser notre **vérificateur de conformité**.*

Voir en PDF

Résumé en quatre points

La loi sur l'IA classe l'IA en fonction des risques qu'elle présente :

- Les risques inacceptables sont interdits (par exemple, les systèmes de notation sociale et l'IA manipulatrice).
- La majeure partie du texte porte sur les systèmes d'IA à haut risque, qui sont réglementés.
- Une section plus petite traite des systèmes d'IA à risque limité, soumis à des obligations de transparence plus légères : les développeurs et les déployeurs doivent s'assurer que les utilisateurs finaux sont conscients qu'ils interagissent avec l'IA (chatbots et deepfakes).

- Le risque minimal n'est pas réglementé (y compris la majorité des applications d'IA actuellement disponibles sur le marché unique de l'UE, telles que les jeux vidéo et les filtres anti-spam activés par l'IA - au moins en 2021 ; cette situation est en train de changer avec l'IA générative).

La majorité des obligations incombent aux fournisseurs (développeurs) de systèmes d'IA à haut risque.

- Ceux qui ont l'intention de mettre sur le marché ou de mettre en service des systèmes d'IA à haut risque dans l'UE, qu'ils soient basés dans l'UE ou dans un pays tiers.
- Ainsi que les fournisseurs de pays tiers où les résultats du système d'IA à haut risque sont utilisés dans l'UE.

Les utilisateurs sont des personnes physiques ou morales qui déploient un système d'IA à titre professionnel, et non des utilisateurs finaux concernés.

- Les utilisateurs (déployeurs) de systèmes d'IA à haut risque ont certaines obligations, mais moins que les fournisseurs (développeurs).
- Cela s'applique aux utilisateurs situés dans l'UE et aux utilisateurs de pays tiers lorsque les résultats du système d'IA sont utilisés dans l'UE.

IA à usage général (GPAI) :

- Tous les fournisseurs de modèles GPAI doivent fournir une documentation technique, des instructions d'utilisation, se conformer à la directive sur les droits d'auteur et publier un résumé du contenu utilisé pour la formation.
- Les fournisseurs de modèles GPAI sous licence libre et gratuite doivent uniquement respecter les droits d'auteur et publier le résumé des données de formation, à moins qu'ils ne présentent un risque systémique.
- Tous les fournisseurs de modèles GPAI qui présentent un risque systémique - qu'ils soient ouverts ou fermés - doivent également procéder à des évaluations de modèles, à des tests

contradictoires, suivre et signaler les incidents graves et assurer la protection de la cybersécurité.

Systèmes d'IA interdits(titre II, article 5)

Les types de systèmes d'IA suivants sont "interdits" en vertu de la loi sur l'IA.

Systèmes d'IA :

- déployer des **techniques subliminales, manipulatrices ou trompeuses** pour fausser le comportement et entraver la prise de décision éclairée, causant ainsi un préjudice important.
- l'**exploitation des vulnérabilités** liées à l'âge, au handicap ou à la situation socio-économique pour fausser le comportement et causer des dommages importants.
- les **systèmes de catégorisation biométrique** déduisant des attributs sensibles (race, opinions politiques, appartenance syndicale, croyances religieuses ou philosophiques, vie sexuelle ou orientation sexuelle), à l'exception de l'étiquetage ou du filtrage d'ensembles de données biométriques acquis légalement ou lorsque les forces de l'ordre catégorisent des données biométriques.
- la **notation sociale**, c'est-à-dire l'évaluation ou la classification d'individus ou de groupes sur la base de leur comportement social ou de leurs traits personnels, ce qui entraîne un traitement préjudiciable ou défavorable de ces personnes.
- l'**évaluation du risque qu'une personne commette des infractions pénales** sur la seule base d'un profilage ou de traits de personnalité, sauf lorsqu'elle est utilisée pour compléter des évaluations humaines fondées sur des faits objectifs et vérifiables directement liés à l'activité criminelle.
- la **constitution de bases de données de reconnaissance faciale** par l'extraction non ciblée d'images faciales sur l'internet ou d'images de vidéosurveillance.
- la **déduction des émotions sur le lieu de travail ou dans les établissements d'enseignement**, sauf pour des raisons médicales ou

de sécurité.

- **Identification biométrique à distance (RBI) "en temps réel" dans les espaces accessibles au public pour les forces de l'ordre**sauf dans les cas suivants
  - la recherche de personnes disparues, de victimes d'enlèvement et de personnes victimes de la traite des êtres humains ou de l'exploitation sexuelle ;
  - la prévention d'une menace grave et imminente pour la vie ou d'un attentat terroriste prévisible ; ou
  - identifier les suspects de crimes graves (meurtre, viol, vol à main armée, trafic de stupéfiants et d'armes illégales, criminalité organisée, crimes contre l'environnement, etc.)

Notes sur l'identification biométrique à distance :

L'utilisation d'un RBI en temps réel basé sur l'IA n'est autorisée que **lorsque la non-utilisation de l'outil causerait un préjudice considérable** et doit tenir compte des droits et libertés des personnes concernées.

Avant le déploiement, la police doit réaliser une **évaluation de l'impact sur les droits fondamentaux** et **enregistrer le système dans la base de données de l'UE**. Toutefois, dans des cas d'urgence dûment justifiés, le déploiement peut commencer sans enregistrement, à condition qu'il soit enregistré ultérieurement sans retard injustifié.

Avant le déploiement, ils doivent également obtenir l'**autorisation d'une autorité judiciaire ou d'une autorité administrative indépendante**[1], bien que, dans des cas d'urgence dûment justifiés, le déploiement puisse commencer sans autorisation, à condition que l'autorisation soit demandée dans les 24 heures. Si l'autorisation est refusée, le déploiement doit cesser immédiatement, en supprimant toutes les données, tous les résultats et toutes les productions.

↲ *[1] Les autorités administratives indépendantes peuvent être soumises à une plus grande influence politique que les autorités judiciaires (Hacker, 2024).*

L'AI Office recrute

La Commission européenne recrute des agents contractuels qui sont des spécialistes des technologies de l'IA afin de gérer les modèles d'IA les plus avancés. Voir ici pour une vue d'ensemble des rôles et des activités de l'Office AI.

Nous partageons cette opportunité car nous sommes convaincus que l'Office de l'IA sera un acteur clé dans la gouvernance des technologies de l'IA dans un avenir proche. Il est essentiel d'attirer des talents de haut niveau dans ce rôle pour réglementer efficacement la technologie de l'IA dans l'UE et pour inspirer des réglementations similaires dans le monde entier.

La date limite de dépôt des candidatures est fixée au 27 mars à 12h00 CET.

Voir le rôle

Systèmes d'IA à haut risque(Titre III)

Certains systèmes d'IA sont considérés comme "à haut risque" en vertu de la loi sur l'IA. Les fournisseurs de ces systèmes seront soumis à des exigences supplémentaires.

Règles de classification des systèmes d'IA à haut risque(article 6)

Les systèmes d'IA à haut risque sont ceux-là :

- utilisé comme composant de sécurité ou comme produit couvert par les lois de l'UE de l'**annexe II** **ET** devant faire l'objet d'une évaluation de la conformité par un tiers en vertu de ces lois de l'annexe II ; **OU**
- ceux qui sont sous **Annexe III** (ci-dessous), sauf si :
  - le système d'IA exécute une tâche procédurale restreinte ;
  - améliore le résultat d'une activité humaine déjà réalisée ;
  - détecte des modèles de prise de décision ou des écarts par rapport à des modèles de prise de décision antérieurs et n'est pas destiné à remplacer ou à influencer l'évaluation humaine effectuée précédemment sans un examen humain approprié ; ou

    - effectue une tâche préparatoire à une évaluation pertinente aux fins des cas d'utilisation énumérés à l'annexe III.

- Les systèmes d'IA sont toujours considérés comme présentant un risque élevé s'ils établissent des profils de personnes, c'est-à-dire un traitement automatisé de données personnelles
  pour évaluer divers aspects de la vie d'une personne, tels que ses performances professionnelles, sa situation économique, sa santé, ses préférences, ses intérêts, sa fiabilité, son comportement, sa localisation ou ses déplacements.
- Les fournisseurs qui estiment que leur système d'IA, qui ne répond pas aux exigences de l'**annexe III**, n'est pas à haut risque, doivent documenter cette évaluation
  avant de le mettre sur le marché ou de le mettre en service.

Exigences applicables aux fournisseurs de systèmes d'IA à haut risque (article 8-25)

Les fournisseurs d'IA à haut risque doivent :

- Mettre en place un **système de gestion des risques** tout au long du cycle de vie du système d'IA à haut risque ;
- Assurer la **gouvernance des données**, en veillant à ce que les ensembles de données de formation, de validation et de test soient pertinents, suffisamment représentatifs et, dans la mesure du possible, exempts d'erreurs et complets conformément à l'objectif visé.
- Établir une **documentation technique** pour démontrer la conformité et fournir aux autorités les informations nécessaires à l'évaluation de cette conformité.
- Concevoir leur système d'IA à haut risque pour qu'il **enregistre** automatiquement les événements pertinents pour l'identification des risques au niveau national et les modifications substantielles tout au long du cycle de vie du système.
- Fournir des **instructions d'utilisation** aux utilisateurs en aval pour leur permettre de se conformer à la réglementation.

- Concevoir leur système d'IA à haut risque pour permettre aux déployeurs de mettre en place une **surveillance humaine**.
- Concevoir leur système d'IA à haut risque pour atteindre les niveaux appropriés de **précision, de robustesse et de cybersécurité**.
- Mettre en place un **système de gestion de la qualité** pour garantir la conformité.

Cas d'utilisation de l'annexe III
Biométrie non interdite : Systèmes d'identification biométrique à distance, à l'exclusion de la vérification biométrique qui confirme qu'une personne est bien celle qu'elle prétend être. Systèmes de catégorisation biométrique déduisant des attributs ou des caractéristiques sensibles ou protégés. Systèmes de reconnaissance des émotions.
Infrastructures critiques : Composants de sécurité dans la gestion et l'exploitation des infrastructures numériques critiques, du trafic routier et de l'approvisionnement en eau, en gaz, en chauffage et en électricité.
Éducation et formation professionnelle : Systèmes d'IA déterminant l'accès, l'admission ou l'affectation aux établissements d'enseignement et de formation professionnelle à tous les niveaux. Évaluer les résultats de l'apprentissage, y compris ceux utilisés pour orienter le processus d'apprentissage de l'étudiant. Évaluer le niveau d'éducation approprié pour un individu. Contrôler et détecter les comportements interdits des étudiants pendant les tests.
L'emploi, la gestion des travailleurs et l'accès à l'auto-emploi : Systèmes d'IA utilisés pour le recrutement ou la sélection, en particulier les offres d'emploi ciblées, l'analyse et le filtrage des candidatures, et l'évaluation des candidats. Promotion et résiliation de contrats, attribution de tâches en fonction de traits de personnalité ou de caractéristiques et de comportements, suivi et évaluation des performances.
L'accès aux services publics et privés essentiels et la jouissance de ceux-ci : Les systèmes d'IA utilisés par les autorités publiques pour

Cas d'utilisation de l'annexe III
évaluer l'éligibilité aux prestations et services, y compris leur attribution, leur réduction, leur révocation ou leur recouvrement. L'évaluation de la solvabilité, sauf en cas de détection d'une fraude financière. L'évaluation et la classification des appels d'urgence, y compris l'établissement de priorités pour la police, les pompiers, l'aide médicale et les services de triage des patients urgents. L'évaluation des risques et la tarification en matière d'assurance maladie et d'assurance vie.
Application de la loi : Systèmes d'IA utilisés pour évaluer le risque qu'une personne soit victime d'un crime. Polygraphes. Évaluation de la fiabilité des preuves dans le cadre d'enquêtes ou de poursuites pénales. Évaluation du risque de délinquance ou de récidive d'une personne, qui ne repose pas uniquement sur le profilage ou l'évaluation des traits de personnalité ou du comportement criminel antérieur. Le profilage au cours de détections, d'enquêtes ou de poursuites pénales.
Gestion des migrations, de l'asile et des contrôles aux frontières : Polygraphes. Évaluation des migrations irrégulières ou des risques sanitaires. Examen des demandes d'asile, de visa et de permis de séjour, ainsi que des plaintes liées à l'éligibilité. Détection, reconnaissance ou identification d'individus, à l'exception de la vérification des documents de voyage.
Administration de la justice et processus démocratiques : Systèmes d'IA utilisés pour la recherche et l'interprétation des faits et l'application de la loi à des faits concrets ou utilisés dans le cadre d'un règlement extrajudiciaire des litiges. Influencer les résultats des élections et des référendums ou le comportement des électeurs, à l'exclusion des résultats qui n'interagissent pas directement avec les personnes, tels que les outils utilisés pour organiser, optimiser et structurer les campagnes politiques.

IA à usage général (GPAI)

On entend par **modèle GPAI** un modèle d'IA, y compris lorsqu'il est entraîné à l'aide d'une grande quantité de données en utilisant l'autosupervision à grande échelle, qui fait preuve d'une grande généralité et qui est capable d'exécuter avec compétence un large éventail de tâches distinctes, quelle que soit 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. Cela ne couvre pas les modèles d'IA qui sont utilisés avant leur mise sur le marché pour des activités de recherche, de développement et de prototypage.

Système GPAI: un système d'IA basé sur un modèle d'IA à usage général, capable de répondre à des besoins variés, tant pour une utilisation directe que pour une intégration dans d'autres systèmes d'IA.

Les systèmes GPAI peuvent être utilisés comme des systèmes d'IA à haut risque ou y être intégrés. Les fournisseurs de systèmes GPAI doivent coopérer avec les fournisseurs de systèmes d'IA à haut risque pour permettre à ces derniers de se mettre en conformité.

Tous les fournisseurs de modèles GPAI doivent

- Rédiger la **documentation technique**, y compris le processus de formation et d'essai et les résultats de l'évaluation.
- Élaborer des **informations et de la documentation à fournir aux fournisseurs en aval** qui ont l'intention d'intégrer le modèle GPAI dans leur propre système d'IA, afin que ces derniers en comprennent les capacités et les limites et soient en mesure de s'y conformer.
- Établir une politique de **respect de la directive sur le droit d'auteur**.
- Publier un **résumé suffisamment détaillé du contenu utilisé pour la formation du** modèle GPAI.

Les **modèles GPAI à licence libre et ouverte** - dont les paramètres, y compris les poids, l'architecture du modèle et l'utilisation du modèle sont accessibles au public, ce qui permet l'accès, l'utilisation, la modification et la distribution du modèle - ne doivent respecter que les deux dernières obligations ci-dessus, à moins que le modèle GPAI à licence libre et ouverte ne soit systémique.

Les **modèles GPAI présentent des risques systémiques lorsque la quantité cumulée de calcul utilisée pour la formation est supérieure**

à 10^{25} opérations en virgule flottante (FLOP). Les fournisseurs doivent notifier à la Commission si leur modèle répond à ce critère dans un délai de deux semaines. Le fournisseur peut présenter des arguments selon lesquels, bien que répondant aux critères, son modèle ne présente pas de risques systémiques. La Commission peut décider d'elle-même, ou par le biais d'une alerte qualifiée du groupe scientifique d'experts indépendants, qu'un modèle a des capacités d'impact élevées, ce qui le rend systémique.

Outre les quatre obligations susmentionnées, les fournisseurs de modèles GPAI présentant un risque systémique doivent également

- Effectuer des **évaluations de modèles**, y compris mener et documenter des **tests contradictoires** afin d'identifier et d'atténuer le risque systémique.
- **Évaluer et atténuer les risques systémiques éventuels**, y compris leurs sources.
- **Repérer, documenter et signaler les incidents graves** et les éventuelles mesures correctives à l'Office AI et aux autorités nationales compétentes dans les meilleurs délais.
- Assurer un niveau adéquat de **protection de la cybersécurité**.

Tous les fournisseurs de modèles GPAI peuvent prouver qu'ils respectent leurs obligations en adhérant volontairement à un code de bonnes pratiques jusqu'à la publication de normes européennes harmonisées, dont le respect entraînera une présomption de conformité. Les fournisseurs qui n'adhèrent pas à des codes de pratique doivent démontrer qu'ils disposent d'**autres moyens adéquats pour se conformer à** leurs obligations, afin d'obtenir l'approbation de la Commission.

Codes de pratique

- Tiendra compte des approches internationales.
- Elle couvrira, sans nécessairement s'y limiter, les obligations susmentionnées, en particulier les informations pertinentes à inclure dans la documentation technique destinée aux autorités et aux fournisseurs en aval, l'identification du type et de la nature des risques systémiques et de leurs sources, ainsi que les modalités de

gestion des risques, en tenant compte des défis spécifiques que pose la gestion des risques en raison de la manière dont ils peuvent émerger et se matérialiser tout au long de la chaîne de valeur.
- L'office AI peut inviter les fournisseurs de modèles GPAI et les autorités nationales compétentes à participer à l'élaboration des codes, tandis que la société civile, l'industrie, le monde universitaire, les fournisseurs en aval et les experts indépendants peuvent soutenir le processus.

Gouvernance

Comment la loi sur l'IA sera-t-elle mise en œuvre ?

- L'Office AI sera créé, au sein de la Commission, pour contrôler la mise en œuvre effective et la conformité des fournisseurs de modèles GPAI.
- Les fournisseurs en aval peuvent déposer une plainte auprès de l'Office AI concernant l'infraction commise par les fournisseurs en amont.
- L'Office AI peut procéder à des évaluations du modèle GPAI pour :
  - évaluer la conformité lorsque les informations recueillies dans le cadre de ses pouvoirs de demande d'informations sont insuffisantes.
  - Enquêter sur les risques systémiques, notamment à la suite d'un rapport qualifié du groupe scientifique d'experts indépendants.

Calendrier

> Voir ce billet pour une vue d'ensemble du calendrier de mise en œuvre.

Après l'entrée en vigueur, la loi sur l'IA s'appliquera :

- 6 mois pour les systèmes d'IA interdits.

- 12 mois pour le GPAI.
- 24 mois pour les systèmes d'IA à haut risque relevant de l'**annexe III**.
- 36 mois pour les systèmes d'IA à haut risque relevant de l'**annexe II**.

Les codes de pratique doivent être prêts 9 mois après l'entrée en vigueur.

Cet article a été publié le 27 février 2024.

Articles connexes

L'AI Office recrute

22 mars 2024

La Commission européenne recrute des agents contractuels spécialisés dans les technologies de l'IA pour gérer les modèles d'IA les plus avancés. La date limite de candidature est fixée au 27 mars à 12h00 CET (formulaire de candidature). Rôle Il s'agit d'une opportunité de travailler au sein d'une équipe...

Le bureau de l'IA : Qu'est-ce que c'est et comment cela fonctionne-t-il ?

21 mars 2024

Dans cet aperçu, nous proposons un résumé des éléments clés de l'Office de l'IA pertinents pour ceux qui s'intéressent à la gouvernance de l'IA. Nous avons souligné les responsabilités de l'Office de l'IA, son rôle au sein de la Commission européenne, sa relation avec le Conseil de l'IA, ses...

Mise en œuvre de la loi sur l'IA : Calendrier et prochaines étapes

28 février 2024

Dans cet article, nous présentons les dates clés de la mise en œuvre de la loi sur l'IA. Nous dressons également la liste des actes de droit dérivé que la Commission pourrait ajouter pour compléter la loi sur l'IA, ainsi que des lignes directrices qu'elle pourrait publier pour soutenir les efforts de mise en conformité. Les...