



30-11-
2021

Une législation européenne sur l'intelligence artificielle pour les droits fondamentaux

Déclaration d'organisations de la société civile

Les institutions de l'Union européenne ont franchi une étape importante au niveau mondial avec la proposition d'une législation sur l'intelligence artificielle (LIA). Dans la mesure où les systèmes d'intelligence artificielle (IA) sont de plus en plus utilisés dans tous les domaines de la vie publique, il est essentiel que cette législation prenne en compte les impacts structurels, sociétaux, politiques et économiques de l'utilisation de l'IA, qu'elle soit à l'épreuve du temps et qu'elle donne la priorité à la protection des droits fondamentaux et des valeurs démocratiques.

Nous reconnaissons en particulier que les systèmes d'IA exacerbent les déséquilibres structurels du pouvoir, et que les préjudices se répercutent souvent sur les personnes les plus marginalisées de la société. En tant que telle, cette déclaration collective présente l'appel de 114 organisations de la société civile en faveur d'une législation sur l'intelligence artificielle qui fonde les droits fondamentaux. La déclaration présente des recommandations essentielles pour guider le Parlement européen et le Conseil dans la modification de la proposition de règlement de la commission européenne¹, publiée le 21 avril 2021.

Les organisations soussignées appellent le Conseil de l'Union européenne, le Parlement européen et tous les gouvernements des États membres de l'UE à s'assurer que la future législation sur l'intelligence artificielle atteigne les 9 objectifs suivants :

1. **Une approche cohérente, flexible et à l'épreuve du temps du "risque" des systèmes d'IA**

La forme actuelle de l'approche fondée sur le risque de la LIA est dysfonctionnelle. Elle délimite quatre niveaux de risque : risque inacceptable (titre II), risque élevé (titre III), systèmes présentant un risque de manipulation (titre IV), et tous les autres systèmes d'IA.

Cette approche consistant à désigner ex ante les systèmes d'IA à différentes catégories de risque ne tient pas compte du fait que le niveau de risque dépend également du contexte dans lequel un système est déployé et ne peut être entièrement déterminé à l'avance. En outre, alors que l'IA comprend un mécanisme permettant de mettre à jour la liste des systèmes d'IA à "haut risque", elle ne prévoit aucune possibilité de mise à jour des listes des systèmes "inacceptables" (article 5) et à risque limité (article 52). De plus, bien que l'annexe III puisse être mise à jour pour ajouter de nouveaux systèmes à la liste des systèmes d'IA à haut risque, les systèmes ne

1 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206>

peuvent être ajoutés que dans le cadre des huit rubriques de domaine existantes. Ces rubriques ne peuvent pas actuellement être modifiées dans le cadre de la LIA. Ces aspects rigides du cadre compromettent la pertinence durable de la LIA, et en particulier sa capacité à répondre aux développements futurs et aux risques émergents pour les droits fondamentaux.

Afin de garantir un cadre à l'épreuve du temps, nous recommandons que la LIA soit amendée afin de :

- **Introduire des mécanismes de mise à jour robustes et cohérents pour les systèmes d'IA "inacceptables" et à risque limité**, afin que les listes de systèmes relevant de ces catégories de risque puissent être mises à jour au fur et à mesure du développement technologique, en utilisant le même mécanisme de mise à jour actuellement proposé pour ajouter de nouveaux systèmes à haut risque à l'annexe III (voir titre XI). Cela doit permettre de désigner les nouveaux systèmes comme présentant un risque inacceptable et donc classés parmi les pratiques interdites (titre II, art. 5), ou comme présentant un risque limité/un risque de manipulation (titre IV, art. 52) et donc soumis à des obligations de transparence supplémentaires ;
- **Inclure une liste de critères pour les systèmes d'IA "inacceptables" et à risque limité** en vertu des art. 5 et 52 respectivement, afin de faciliter le processus de mise à jour, d'offrir une sécurité juridique aux développeurs d'IA et de promouvoir la confiance en garantissant que les personnes concernées sont protégées contre les applications dangereuses et potentiellement manipulatrices de l'IA ;
- **Veiller à ce que les "domaines" à haut risque (c'est-à-dire les huit rubriques de domaine) énumérés à l'annexe III puissent être mis à jour ou modifiés dans le cadre du mécanisme du titre XI** afin de permettre des modifications du champ d'application des rubriques de domaine existantes et l'inclusion de nouvelles rubriques de domaine dans le champ d'application des systèmes d'IA à haut risque "autonomes" ;
- **Élargir l'annexe III** pour inclure une liste plus complète de systèmes à haut risque, tels que :
 - ↳ Élargir la rubrique de domaine 1 à **tous les systèmes qui utilisent des données physiques, physiologiques, comportementales** ainsi que biométriques, y compris, mais sans s'y limiter, l'identification biométrique, la catégorisation, la détection et la vérification ;
 - ↳ Ajout des utilisations de l'IA aux fins de la réalisation d'analyses prédictives de la migration ;
 - ↳ Ajout de nouvelles rubriques de domaine relatives aux soins de santé et aux assurances.

2. Interdiction de tous les systèmes d'IA présentant un risque inacceptable pour les droits fondamentaux

L'article 5 de la LIA établit le principe selon lequel certaines pratiques d'IA sont incompatibles avec les droits, les libertés et les valeurs de l'UE, et devraient donc être interdites. Cependant, pour que l'IA puisse réellement prévenir et protéger les personnes contre [les déploiements d'IA les plus attentatoires aux droits](#), des amendements essentiels sont nécessaires :

- **Supprimer le seuil élevé pour les systèmes manipulateurs et exploitants de l'Art. 5 (1)(a) et (b)** pour prouver que les systèmes fonctionnent "*d'une manière qui cause ou est susceptible de causer à cette personne ou à une autre personne un préjudice physique ou psychologique*". Le cadre actuel implique à tort que le comportement d'une personne peut être matériellement déformé ou exploité d'une manière qui ne cause pas de préjudice, alors que ces pratiques sont conçues et/ou utilisées pour saper l'essence de notre autonomie, ce qui constitue en soi un préjudice inadmissible ;
- **Étendre le champ d'application de l'art. 5 (1)(b) pour inclure un ensemble complet de vulnérabilités**, plutôt que de le limiter à "l'âge, le handicap physique ou mental". Si un système d'IA exploite les vulnérabilités d'une personne ou d'un groupe sur la base de toute caractéristique sensible ou protégée, y compris, mais sans s'y limiter, l'âge, le genre et l'identité de genre, l'origine raciale ou ethnique, l'état de santé, l'orientation sexuelle,

les caractéristiques sexuelles, le statut social ou économique, le statut de travailleur, le statut de migrant ou le handicap, il est fondamentalement nuisible et doit donc être interdit ;

- **Adapter l'art. 5 (1)(c) interdisant le scoring social pour l'étendre à l'ensemble des pratiques de profilage social nuisibles actuellement utilisées dans le contexte européen.** L'interdiction devrait être étendue pour inclure aussi les acteurs privés et un certain nombre de critères problématiques doivent être supprimés, y compris la limitation temporelle "de l'utilisation du profilage social", déplacés, notamment la limitation temporelle " *sur une certaine période* " et les références à la " *fiabilité* " et au " *score unique* " ;
- **Étendre l'art. 5 (1)(d) sur l'interdiction de l'identification biométrique à distance pour qu'elle s'applique à tous les acteurs, et pas seulement aux services de répression pénale, ainsi qu'aux utilisations "en temps réel" et "a posteriori",** qui peuvent être tout aussi dommageables. L'interdiction devrait inclure la mise sur le marché/en service de systèmes RBI dont on peut raisonnablement prévoir qu'ils seront utilisés de manière interdite. Les larges exceptions de l'Art. 5(1)(d), Art. 5(2) et Art. 5(3) portent atteinte aux exigences de nécessité et de proportionnalité de la Charte des droits fondamentaux de l'UE et devraient être supprimées ;
- **Interdire les pratiques suivantes qui présentent un risque inacceptable pour les droits fondamentaux en vertu de l'art. 5 :**
 - ↘ L'utilisation de systèmes de reconnaissance des émotions qui prétendent déduire les émotions et les états mentaux des personnes à partir de données physiques, physiologiques, comportementales, ainsi que biométriques ;
 - ↘ L'utilisation de systèmes de catégorisation biométrique pour suivre, catégoriser et / ou juger les personnes dans les espaces accessibles au public ; ou pour catégoriser les personnes sur la base de catégories spéciales de données personnelles, de caractéristiques protégées, ou d'identité de genre ;
 - ↘ Des systèmes qui reviennent à la physiognomonie de l'IA en utilisant des données sur notre corps pour faire des inférences problématiques sur la personnalité, le caractère, les croyances politiques et religieuses ;
 - ↘ L'utilisation de systèmes d'IA par les autorités de répression pénale et de justice pénale pour faire des prédictions, des profils ou des évaluations de risques dans le but de prévoir les crimes ;
 - ↘ L'utilisation de systèmes d'IA à des fins d'application de la loi sur l'immigration pour établir le profil ou l'évaluation des risques de personnes physiques ou de groupes d'une manière qui restreint le droit de demander l'asile et / ou préjuge de l'équité des procédures de migration.

3. Obligations des utilisateurs de systèmes d'IA à haut risque pour faciliter la responsabilisation des personnes touchées par les systèmes d'IA

La LIA impose principalement des obligations aux "**fournisseurs**" (développeurs) plutôt qu'aux "**utilisateurs**" (« déployeurs ») de l'IA à haut risque. Si une partie du risque posé par les systèmes énumérés à l'annexe III provient de la manière dont ils sont conçus, des risques importants découlent de la manière dont ils sont utilisés. Cela signifie que les fournisseurs ne peuvent pas évaluer de manière exhaustive tout l'impact potentiel d'un système d'IA à haut risque lors de l'évaluation de la conformité, et donc que les utilisateurs doivent également avoir l'obligation de respecter les droits fondamentaux.

Pour remédier à cela, nous recommandons que la LIA soit amendée **pour inclure les obligations explicites suivantes pour les utilisateurs de systèmes d'IA à haut risque :**

- **Inclure l'obligation pour les utilisateurs de systèmes d'IA à haut risque de mener une évaluation d'impact sur les droits fondamentaux (FRIA)** avant de déployer tout système d'IA à haut risque. Pour chaque déploiement proposé, les utilisateurs doivent désigner les catégories d'individus et de groupes susceptibles d'être impactés par le système, évaluer l'impact du système sur les droits fondamentaux, son accessibilité pour les personnes handicapées, et son impact sur l'environnement et l'intérêt public au sens

large ;

- ↳ Les évaluations préliminaires pour les utilisateurs de systèmes d'IA ne présentant pas de risque élevé devraient être encouragées, et un soutien devrait être fourni aux utilisateurs pour déterminer correctement le niveau de risque ;
- **Inclure l'obligation pour les utilisateurs de systèmes d'IA à haut risque de vérifier la conformité du système d'IA avec le présent règlement** avant de mettre le système en service ;
- **Inclure l'obligation pour les utilisateurs de télécharger les informations produites dans le cadre de l'analyse d'impact vers la base de données de l'UE pour les systèmes d'IA autonomes à haut risque** (voir section 4 pour plus de détails).

4. Une transparence publique cohérente et significative

La base de données de l'UE sur les systèmes autonomes d'IA à haut risque (article 60) offre une possibilité prometteuse d'accroître la transparence des systèmes d'IA vis-à-vis des personnes concernées et de la société civile, et pourrait grandement faciliter la recherche d'intérêt public. Cependant, la base de données ne contient actuellement que des informations sur les systèmes à haut risque enregistrés par les fournisseurs, sans informations sur le contexte d'utilisation. Cette lacune compromet l'objectif de la base de données, car elle empêchera le public de savoir où, par qui et dans quel(s) but(s) les systèmes d'IA à haut risque sont réellement utilisés. En outre, la LIA n'impose la notification qu'aux personnes concernées par les systèmes d'IA énumérés à l'Art. 52. Cette approche est incohérente car l'IA n'exige pas une obligation parallèle de notification aux personnes concernées par l'utilisation de systèmes d'IA à haut risque en vertu de l'annexe III.

Afin d'assurer une transparence efficace, nous recommandons de modifier la LIA de la manière suivante :

- **Inclure une obligation pour les utilisateurs d'enregistrer les déploiements de systèmes d'IA à haut risque dans la base de données définie à l'art. 60 avant de les mettre en service**, et d'inclure dans la base de données des informations sur chaque *déploiement* spécifique du système, notamment :
 - ↳ L'identité du fournisseur et de l'utilisateur ; le contexte et l'objectif du déploiement ; la désignation des personnes impactées ; et les résultats de l'évaluation d'impact visée à la section 3 ci-dessus ;
- **Étendre la liste des informations que les fournisseurs de systèmes d'IA à haut risque doivent publier dans la base de données de l'art. 60** pour y inclure les informations visées à l'annexe IV, point 2 b) et point 3, à savoir les spécifications de conception des systèmes d'IA à haut risque (y compris la logique générale, les principaux choix de conception et d'optimisation) ;
- **Veiller à ce que la base de données publique de l'art. 60 soit conviviale, librement accessible** (y compris pour les personnes handicapées) **et exploitable** (y compris par des machines) ;
- **Étendre les obligations de transparence spécifiées à l'art. 52 à tous les systèmes d'IA à haut risque**. Les notifications présentées aux personnes devraient inclure l'information qu'un système d'IA est utilisé, qui est son opérateur, des informations générales sur l'objectif du système, des informations sur le droit de demander une explication, ainsi que - dans le cas des systèmes à haut risque - une référence ou un lien vers l'entrée correspondante dans la base de données de l'UE ;
- **Supprimer les exemptions prévues à l'art. 52 pour les "systèmes d'IA manipulateurs autorisés par la loi à détecter, prévenir, enquêter et poursuivre des infractions pénales"**, car l'utilisation de systèmes d'IA manipulateurs dans des contextes de répression pénale et de justice pénale présente un risque aigu pour les droits fondamentaux.

5. Des droits et des recours significatifs pour les personnes touchées par les systèmes d'IA

Actuellement, la LIA ne confère pas de droits individuels aux personnes touchées par les systèmes d'IA. Elle ne contient pas non plus de dispositions relatives à la réparation individuelle ou collective, ni de mécanisme permettant aux personnes ou à la société civile de participer au processus d'enquête sur les systèmes d'IA à haut risque. En tant que telle, la LIA n'aborde pas pleinement la myriade de préjudices qui découlent de l'opacité, de la complexité, de l'échelle et du déséquilibre de pouvoir dans lesquels les systèmes d'IA sont déployés.

Pour faciliter une réparation significative, nous recommandons :

- **Inclure deux droits individuels dans la LIA comme base pour les recours judiciaires** :
 - ↳ (a) Le droit de ne pas être soumis à des systèmes d'IA qui présentent un risque inacceptable ou qui ne sont pas conformes à la LIA ; et
 - ↳ (b) Le droit de recevoir une explication claire et intelligible, d'une manière accessible aux personnes handicapées, pour les décisions prises avec l'aide de systèmes relevant du champ d'application de la LIA ;
- **Inclure un droit à un recours effectif pour les personnes dont les droits au titre du règlement ont été violés** à la suite de la mise en service d'un système d'IA. Ce recours devrait être accessible tant aux particuliers qu'aux collectivités ;
- **La création d'un mécanisme permettant aux organisations d'intérêt public de déposer une plainte auprès des autorités nationales de surveillance** en cas de violation du règlement ou de systèmes d'IA portant atteinte aux droits fondamentaux ou à l'intérêt public. Cette plainte devrait déclencher une enquête sur le système en question, comme le prévoient les articles 65 et 67. 65 et 67.

6. Accessibilité tout au long du cycle de vie de l'IA

La LIA ne prévoit pas d'exigences obligatoires en matière d'accessibilité pour les fournisseurs et les utilisateurs d'IA. La proposition stipule que les fournisseurs de systèmes d'IA ne présentant pas de risque élevé peuvent créer et mettre en œuvre des codes de conduite pouvant inclure des engagements volontaires, notamment en matière d'accessibilité pour les personnes handicapées (Considérant 81, Art 69. (2)).² Il s'agit d'une approche inadéquate du handicap, qui ne respecte pas les obligations énoncées dans la [Convention des Nations unies relative aux droits des personnes handicapées](#) et qui est incompatible avec la législation européenne existante, telle que la [directive](#) européenne sur l'accessibilité. L'absence d'exigences en matière d'accessibilité risque de conduire au développement et à l'utilisation de l'IA avec de nouveaux obstacles pour les personnes handicapées.

Pour garantir l'accessibilité totale des systèmes d'IA, nous recommandons :

- **L'inclusion d'exigences d'accessibilité transversales et intégrées pour les systèmes d'IA, quel que soit le niveau de risque**, y compris pour les informations et les manuels d'instruction liés à l'IA, conformément à la [directive](#) européenne sur l'accessibilité.

7. Durabilité et protection de l'environnement

La LIA manque une occasion cruciale de garantir que le développement et l'utilisation des systèmes d'IA puissent se faire de manière durable et respectueuse des ressources et des limites de notre planète. Comme première étape pour aborder les dimensions environnementales de la durabilité, nous avons besoin de transparence sur le niveau des ressources nécessaires pour développer et exploiter les systèmes d'IA.

Pour y parvenir, nous recommandons :

² Des questions importantes telles que la soutenabilité environnementale, la participation des parties prenantes à la conception et au développement des systèmes d'IA et la diversité des équipes de développement sont également suggérées dans l'IA comme de simples mesures volontaires.

- **L'introduction d'exigences de transparence transversales et publiques sur la consommation de ressources et les impacts des émissions de gaz à effet de serre des systèmes d'IA** - indépendamment du niveau de risque - en ce qui concerne la conception, la gestion des données et la formation, l'application et les infrastructures sous-jacentes (matériel, centres de données, etc.).

8. Des normes améliorées et à l'épreuve du temps pour les systèmes d'IA

La LIA est fortement inspirée de la législation européenne sur la sécurité des produits et, en tant que telle, elle s'appuie sur l'élaboration de normes harmonisées pour faciliter le respect de la législation par les fournisseurs. Cependant, la LIA utilise ces normes techniques pour déléguer les principales décisions politiques et juridiques concernant l'IA aux organismes européens de normalisation (article 3.27, article 40), qui sont des organismes privés opaques largement dominés par les acteurs de l'industrie.

Pour garantir que les décisions politiques et relatives aux droits fondamentaux restent fermement soumises au contrôle démocratique des législateurs européens, nous recommandons de :

- **Limiter explicitement les normes harmonisées établies dans l'art. 40 (pour le titre III, chapitre 2, Exigences relatives à l'IA à haut risque) aux seuls aspects véritablement techniques**, en veillant à ce que le pouvoir général de fixer des normes et d'assurer la surveillance de toutes les questions qui ne sont pas purement techniques, telles que l'atténuation des préjugés (article 10, paragraphe 2, point f)), reste du ressort du processus législatif ;
- **Veiller à ce que les normes répondent aux besoins de tous les membres de la société par une approche de conception universelle**. Par exemple, pour garantir que les systèmes et pratiques de l'IA sont accessibles aux personnes handicapées, les normes harmonisées pour l'IA doivent être compatibles avec les normes pertinentes harmonisées pour la loi européenne sur l'accessibilité, au minimum ;
- **Garantir que les autorités compétentes, telles que les autorités chargées de la protection des données et les organismes de promotion de l'égalité, les organisations de la société civile, les PME et les parties prenantes dans le domaine de l'environnement, de la consommation et de la société, sont représentées et ont la possibilité de participer efficacement aux processus et aux organismes de normalisation et de définition des spécificités de l'IA ;**
- **Veiller à ce que l'harmonisation dans le cadre de l'IA soit sans préjudice des lois nationales existantes ou futures** relatives à la transparence, à l'accès à l'information, à la non-discrimination ou à d'autres droits, afin de garantir que l'harmonisation ne soit pas utilisée à mauvais escient ou étendue au-delà du champ d'application spécifique de la LIA.

9. Une législation sur l'IA vraiment complète qui fonctionne pour tout le monde

Malgré la documentation constante de l'impact négatif disproportionné que les systèmes d'IA peuvent avoir sur les groupes déjà marginalisés (en particulier les femmes*, les personnes racisées, les migrants, les personnes LGBTIQ+, les personnes handicapées, les travailleurs du sexe, les enfants et les jeunes, les personnes âgées et les personnes en difficultés), des changements significatifs sont nécessaires pour garantir que la LIA traite de manière adéquate ces préjudices systématiques.

Pour s'assurer que la LIA fonctionne pour tout le monde, nous recommandons de :

- **Garantir la protection des données et la vie privée des personnes handicapées**. Le règlement général sur la protection des données (RGPD) de l'UE dispose de règles qui s'appliquent avant le traitement des données de catégorie spéciale des personnes qui sont "physiquement ou juridiquement incapables de donner leur consentement" (art.

9(2)(c) du RGPD) qui peuvent être insuffisantes pour protéger les droits de ces personnes dans certains contextes liés à l'utilisation de l'IA :

- ↳ **La législation sur l'IA doit donc garantir que la vie privée et la protection des données de toutes les personnes, incluant celles sous des régimes de décision substitués tels que les tutelles, sont protégées lorsque leurs données sont traitées par des systèmes d'IA.**
- **Supprimer l'exemption pour les systèmes informatiques européens à grande échelle dans l'art. 83.** Les systèmes informatiques à grande échelle existants traitent de grandes quantités de données à un niveau qui présente un risque significatif pour les droits fondamentaux. Aucune justification raisonnable de cette exemption des règles de l'IA n'est prévue dans la législation ou ne peut être donnée :
 - ↳ **Tout système informatique à grande échelle utilisé par l'UE doit donc être inclus dans le champ d'application de la LAI par la suppression de l'exclusion de la section un de l'art. 83.**
- **Doter les organes d'exécution des ressources nécessaires.** Alors que l'art. 59 (4) souligne la nécessité de doter les autorités nationales de "ressources financières et humaines adéquates", selon l'exposé des motifs, la Commission ne prévoit actuellement que 1 à 25 postes équivalents temps plein par État membre pour les autorités nationales de surveillance. C'est clairement insuffisant :
 - ↳ **Les implications financières de l'IA doivent être réévaluées et planifiées de manière à garantir que les organismes de contrôle et les autres organismes concernés disposent des ressources nécessaires pour s'acquitter utilement de leurs tâches au titre de la LAI.**
- Garantir une IA européenne digne de confiance au-delà de l'UE. Contrairement à l'objectif de "façonner des normes et des standards mondiaux pour une IA digne de confiance et cohérente avec les valeurs de l'UE", tel qu'indiqué dans l'exposé des motifs, ses règles ne s'appliquent actuellement pas aux fournisseurs et aux utilisateurs d'IA établis dans l'UE lorsqu'elles affectent des individus dans des pays tiers :
 - ↳ **L'IA devrait garantir que les fournisseurs et utilisateurs d'IA établis dans l'UE dont les résultats affectent des individus en dehors de l'Union européenne sont soumis aux mêmes exigences que ceux dont les résultats affectent des personnes au sein de l'Union, afin d'éviter tout risque de discrimination, de surveillance et d'abus par le biais de technologies développées dans l'UE.**

Rédigé par : European Digital Rights (EDRi), Access Now, Panoptikon Foundation, epicenter.works, AlgorithmWatch, European Disability Forum (EDF), Bits of Freedom, Fair Trials, PICUM, et ANEC (European consumer voice in standardisation).

Signé par :

1. European Digital Rights (EDRi) (*European*)
2. Access Now (*International*)
3. The App Drivers and Couriers Union (ADCU) (*United Kingdom*)
4. Algorights (*Spain*)
5. AlgorithmWatch (*European*)
6. All Out (*International*)
7. Amnesty International (*International*)
8. ARTICLE 19 (*International*)
9. Asociación Salud y Familia (*Spain*)
10. Aspiration (*United States*)
11. Association for action against violence and trafficking in human beings - Open Gate / La Strada Macedonia (*North Macedonia*)
12. Association for Juridical Studies on Immigration (ASGI) (*Italy*)
13. Association for Monitoring Equal Rights (*Turkey*)

14. Association of citizens for promotion and protection of cultural and spiritual values - Le-gis Skopje (*North Macedonia*)
15. Associazione Certi Diritti (*Italy*)
16. Associazione Luca Coscioni (*Italy*)
17. Baobab Experience (*Italy*)
18. Belgian Disability Forum asbl (BDF) (*Belgium*)
19. Big Brother Watch (*United Kingdom*)
20. Bits of Freedom (*The Netherlands*)
21. Border Violence Monitoring Network (*European*)
22. Campagna LasciateCIEntrare (*Italy*)
23. Center for AI and Digital Policy (CAIDP) (*International*)
24. Chaos Computer Club (CCC) (*Germany*)
25. Chaos Computer Club Lëtzebuerg (*Luxembourg*)
26. CILD – Italian Coalition for Civil Liberties and Rights (*Italy*)
27. Controle Alt Delete (*The Netherlands*)
28. DataForGoodBCN (*Spain*)
29. DATAWO (*Greece*)
30. D3 - Defesa dos Direitos Digitais (*Portugal*)
31. D64 - Zentrum für digitalen Fortschritt (Center for Digital Progress) (*Germany*)
32. DataEthics.eu (*European*)
33. Digital Defenders Partnership (*International*)
34. Digitalcourage (*Germany*)
35. Digitale Freiheit e.V. (*Germany*)
36. Digitale Gesellschaft (*Germany*)
37. Digitale Gesellschaft (Schweiz) (*Switzerland*)
38. DIMMONS Digital Commons Research Group (*Spain*)
39. Disabled Peoples Organisations (*Denmark*)
40. DonesTech (*Spain*)
41. Državljan D / Citizen D (*Slovenia*)
42. Each One Teach One e.V. (*Germany*)
43. Elektronisk Forpost Norge (EFN) (*Norway*)
44. epicenter.works (*Austria*)
45. Equinox Initiative for Racial Justice (*European*)
46. Eticas Foundation (*Spain*)
47. Eumans (*European*)
48. European Anti-Poverty Network (*European*)
49. European Center for Not-for-Profit Law Stichting (*International*)
50. European Civic Forum (*European*)
51. European Disability Forum (EDF) (*European*)
52. European Network Against Racism (ENAR) (*European*)
53. European Network on Religion and Belief (*European*)
54. European Network on Statelessness (*European*)
55. European Sex Workers' Rights Alliance (*European*)
56. European Youth Forum (*European*)
57. Fair Trials (*European*)
58. FAIRWORK Belgium (*Belgium*)
59. FIDH (International Federation for Human rights) (*International*)
60. Fundación Secretariado Gitano (*Spain*)
61. Future of Life Institute (*International*)
62. GHETT'UP (*France*)
63. Greek Forum of Migrants (*Greece*)
64. Greek Forum of Refugees (*European*)
65. Health Action International (*The Netherlands*)
66. Helsinki Foundation for Human Rights (*Poland*)
67. Hermes Center (*Italy*)
68. Hivos (*International*)
69. Homo Digitalis (*Greece*)

70. Human Rights Association (*Turkey*)
71. Human Rights House Zagreb (*Croatia*)
72. HumanRights360 (*Greece / European*)
73. Human Rights Watch (*International*)
74. ILGA-Europe - The European Region of the International Lesbian, Gay, Bisexual, Trans and Intersex Association (*European*)
75. Implementation Team of the Decade of People of African Descent (*Spain*)
76. info.nodes (*Italy*)
77. Interferencias (*Spain*)
78. International Commission of Jurists (NJCM) - Dutch Section (*The Netherlands*)
79. Irish Council for Civil Liberties (ICCL) (*Ireland*)
80. IT-Pol Denmark (*Denmark*)
81. JustX (*European*)
82. JustPeace Labs (*International*)
83. KOK - German NGO Network against Trafficking in Human Beings (*Germany*)
84. Lafede.cat – organitzacions per a la justícia global (*Spain*)
85. Ligue des droits de l'Homme (LDH) (*France*)
86. Ligue des droits humains (*Belgium*)
87. Maruf Foundation (*The Netherlands*)
88. Mediterranea Saving Humans Aps (*Italy / International*)
89. Melitea (*European*)
90. Mnemonic (*Germany / International*)
91. Moje PańUstwo Foundation (*Poland*)
92. Montreal AI Ethics Institute (*Canada*)
93. Movement of Asylum Seekers in Ireland (MASI) (*Ireland*)
94. Movimento SOS Racismo (*European*)
95. Network Democratie (*The Netherlands*)
96. NOVACT (*Spain / International*)
97. OMEP - Oraganisation Mondiale pour l'Education Prescolaire / World Organization for Early Childhood Education (*International*)
98. Open Knowledge Foundation (*International*)
99. Open Society European Policy Institute (OSEPI) (*International*)
100. OpenMedia (*International*)
101. Panoptikon Foundation (*Poland*)
102. The Platform for International Cooperation on Undocumented Migrants (PICUM) (*International*)
103. Privacy International (*International*)
104. Privacy Network (*Italy*)
105. Racism and Technology Center (*The Netherlands*)
106. Ranking Digital Rights (*International*)
107. Refugee Law Lab, York University (*International*)
108. Refugees in danger (*Denmark*)
109. Science for Democracy (*European*)
110. SHARE Foundation (*Serbia*)
111. SOLIDAR & SOLIDAR Foundation (*European*)
112. Statewatch (*European*)
113. Stop Wapenhandel (*The Netherlands*)
114. StraLi (*European*)
115. SUPERRR Lab (*Germany*)
116. Symbiosis-School of Political Studies in Greece, Council of Europe Network (*Greece*)
117. Taylor Bennett Foundation (*United Kingdom*)
118. UNI Europa (*European*)
119. Universidad y Ciencia Somosindicalistas (*Spain*)
120. Vrijschrift.org (*The Netherlands*)
121. WeMove Europe (*European*)
122. Worker Info Exchange (*International*)
123. Xnet (*Spain*)

Soutiens :

1. Coalition des villes pour les droits numériques (européenne)

* Cette déclaration présente l'accord de base entre les organisations de la société civile signataires sur la proposition de la législation de l'UE sur l'intelligence artificielle.

Cependant, certains des signataires ont des positions qui sont en certains endroits plus spécifiques et plus étendues que celles décrites ici.