_swissprivacy.law

Aspects réglementaires de l'intelligence artificielle

Frédéric Erard, Dr iur., av., CIPP/E

Livio di Tria, MLaw, CIPP/E, CIPM

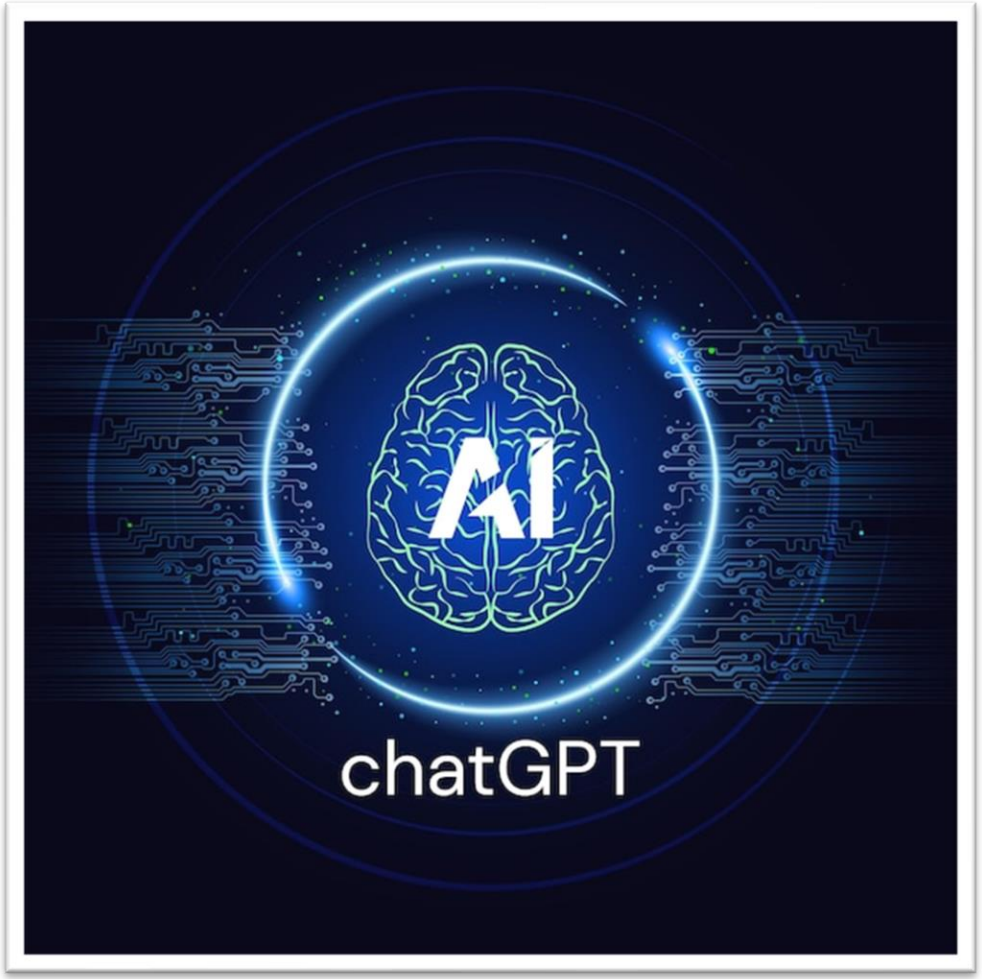
Plan de la présentation

- Introduction
- Pourquoi réglementer?
- Cadre réglementaire et normatif
- Conclusion

Introduction

Évolutions législatives

- Les législateurs s'intéressent à l'IA depuis quelques années déjà
  - Obligations de transparence des décisions individuelles automatisées (art. 21 LPD ; art. 22 RGPD)
  - Règlement européen du 21 avril 2021 sur l'intelligence artificielle (*AI Act*)
- Pour quelles raisons est-il important de légiférer ?
  - Permettre **l'exploitation du potentiel** de l'IA tout en réduisant autant que possible les **risques** pour la société



Nécessité de légiférer

Transparence (Black Box Effet)

- Comment gérer les difficultés liées au manque de transparence ?
- Peut-on prendre des décisions qui ont des effets juridiques si nous ne sommes pas en mesure d'interpréter correctement les résultats ?

Ne pas « **sacraliser** » l'idée d'une boîte noire

Nécessité de légiférer

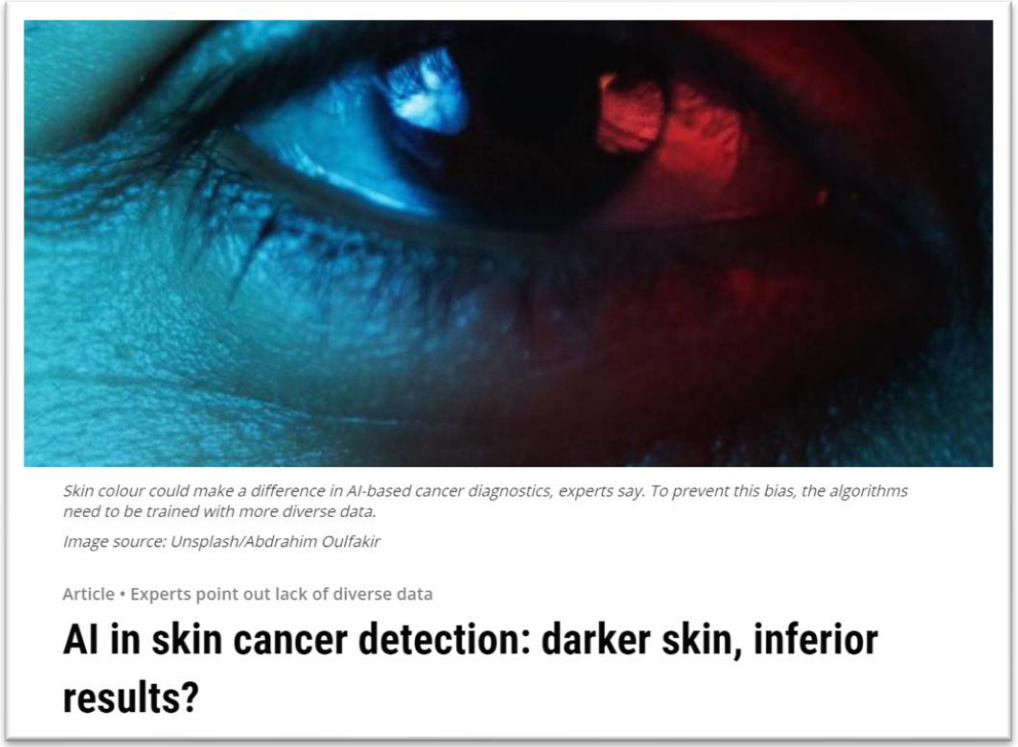
Responsabilité

- Qui est **responsable** en cas de dommage causé par un système d'IA ?
- Comment apporter les **preuves** nécessaires pour établir la responsabilité d'une décision qui conduit à un dommage ?
- Comment **arbitrer** les désaccords entre machine et humain ?

Nécessité de légiférer

Discrimination

- Le choix des données entrées peut induire et renforcer des **biais** dans les résultats
  - Qualité des données ?
  - Nature des données ?
  - Risques d'erreurs ?



Skin colour could make a difference in AI-based cancer diagnostics, experts say. To prevent this bias, the algorithms need to be trained with more diverse data.

Image source: Unsplash/Abdrahim Oulfakir

Article • Experts point out lack of diverse data

AI in skin cancer detection: darker skin, inferior results?

Nécessité de légiférer

Protection des données

- Accès nécessaire à de **larges sets de données** (sensibles ou non)
- Comment concilier les **principes généraux** de la protection des données avec les systèmes d'IA ?
- Comment assurer les **droits** des personnes concernées ?

Intelligence artificielle : la CNIL ouvre une consultation sur la constitution de bases de données d'apprentissage

11 octobre 2023

La CNIL publie ses premières fiches pratiques sur la constitution de bases de données d'apprentissage des systèmes d'intelligence artificielle. Ces fiches doivent aider les professionnels à concilier innovation et respect des droits des personnes. Elles sont soumises à consultation publique jusqu'au 15 décembre 2023.

La loi actuelle sur la protection des données est directement applicable à l'IA

09.11.2023 – En Suisse aussi, l'intelligence artificielle (IA) investit de plus en plus la vie économique et sociale de la population. Dans ce contexte, le PFPDT rappelle que la loi sur la protection des données en vigueur depuis le 1er septembre 2023 est directement applicable aux traitements de données basés sur l'IA.

Nécessité de légiférer

Propriété intellectuelle

- Équilibre à trouver entre la propriété intellectuelle et l'innovation
  - Quelle transparence concernant les données utilisées pour former les systèmes d'IA ?
  - Quelle transparence dans l'utilisation des outils d'IA dans les processus créatifs ?
  - Comment déterminer qui est responsable des systèmes d'IA et de leurs créations (p. ex. développeurs, utilisateurs, propriétaires) ?

The New York Times

The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work

Millions of articles from The New York Times were used to train chatbots that now compete with it, the lawsuit said.

Share full article 1.3K

lawsuit by The New York Times could test the emerging legal contours of generative echnologies. Sasha Maslov for The New York Times

Nécessité de légiférer

Sécurité de l'information

- L'IA offre des capacités avancées de détection des menaces
  - Identification facilitée des comportements anormaux dans les réseaux et les systèmes
  - Réponse rapide aux incidents de sécurité par l'analyse de vastes volumes de données
- Revers de la médaille ?
  - Sophistication et automatisation des attaques informatiques

Nécessité de légiférer

Usage militaire

- Quel cadre légal pour les systèmes d'IA militaires ou de défense ?
- Tendance à l'exclusion
  - Conventions de Genève ?
  - Manuel de Tallin ?

Nécessité de légiférer

Stabilité démocratique

- Manipulation de l'opinion publique
- Liberté d'expression

Nécessité de légiférer

Concurrence

- Course aux conditions cadres au niveau international
  - Leadership technologique, compétitivité économique, protection des intérêts nationaux
- Influence sur les normes internationales (*Brussels Effect*)

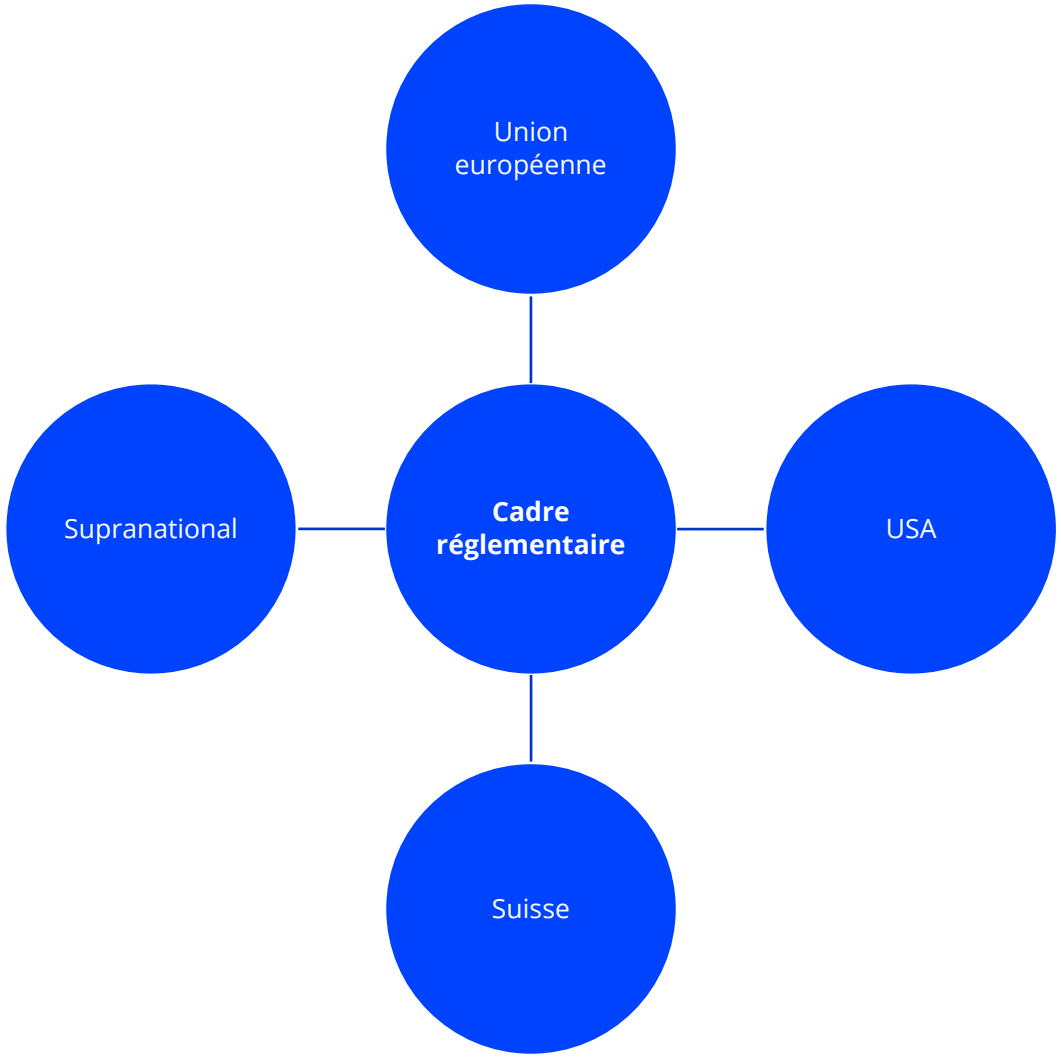
Nécessité de légiférer

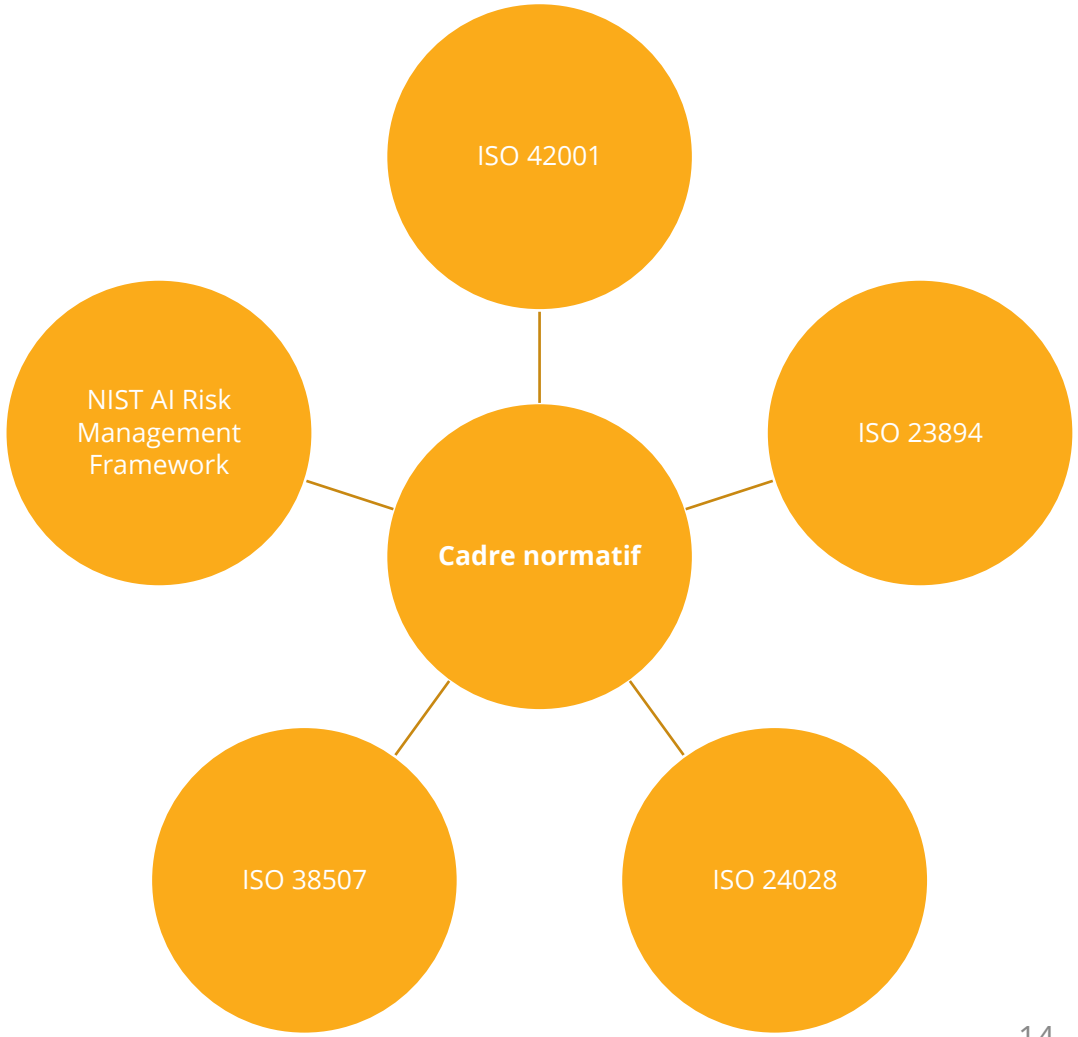
Conclusion intermédiaire

- L'IA suscite des enjeux (juridiques) importants
- Légiférer demeure un **défi complexe** en raison de la **nature transversale** de ces enjeux
- Quelle approche réglementaire ?
  - Réglementation globale vs. sectorielle
  - *Statuo quo (*normes technologiquement neutres)
  - Approche fondée sur le risque ou sur les droits des personnes ?

Cadre réglementaire et normatif

Non exhaustif





Cadre réglementaire

Union européenne

- Train de mesures destinées à **soutenir le déploiement de l'IA** au sein de l'Union européenne
- Règles horizontales relatives aux systèmes d'IA
  - Proposition de Règlement du 21 avril 2021 du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle
    - Législation sur l'intelligence artificielle (***AI Act***)
- Responsabilité liée aux systèmes d'IA
  - Proposition de Directive du 28 septembre 2022 du Parlement européen et du Conseil relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle
    - Directive sur la responsabilité en matière d'IA (***AI Liability Directive***)
- Révision des règles sectorielles et horizontales en matière de sécurité des produits
  - Proposition de Directive du 28 septembre 2022 du Parlement européen et du Conseil relative à la responsabilité du fait des produits défectueux

Cadre réglementaire

AI Act

- Accord **provisoire** sur la législation sur l'intelligence artificielle trouvé le 9 décembre 2023
- Le règlement doit encore être formellement adopté par les organes législatifs européens (objectif : **printemps 2024**)

Cadre réglementaire

AI Act – Approche fondée sur les risques

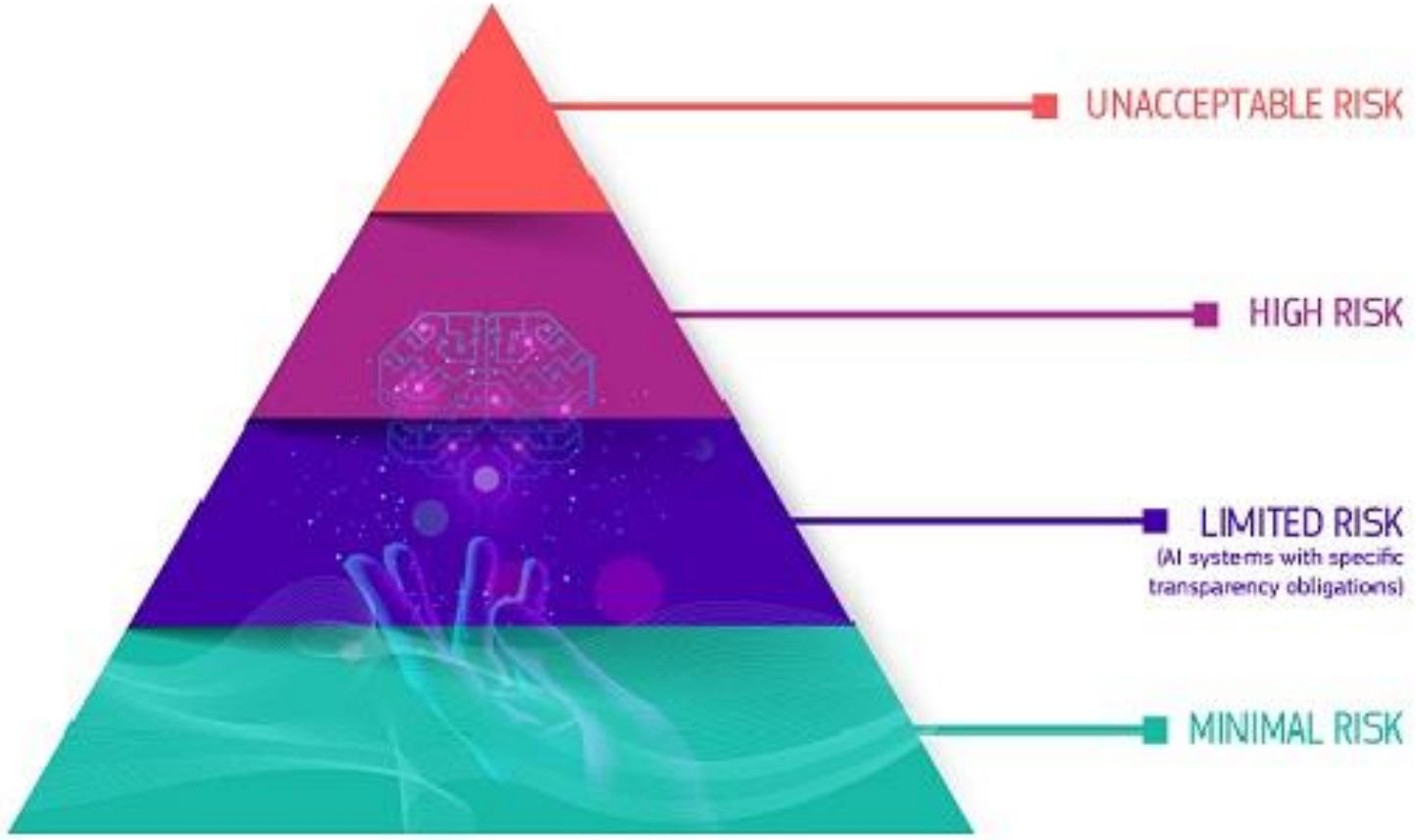


Image: Commission Européenne, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Cadre réglementaire

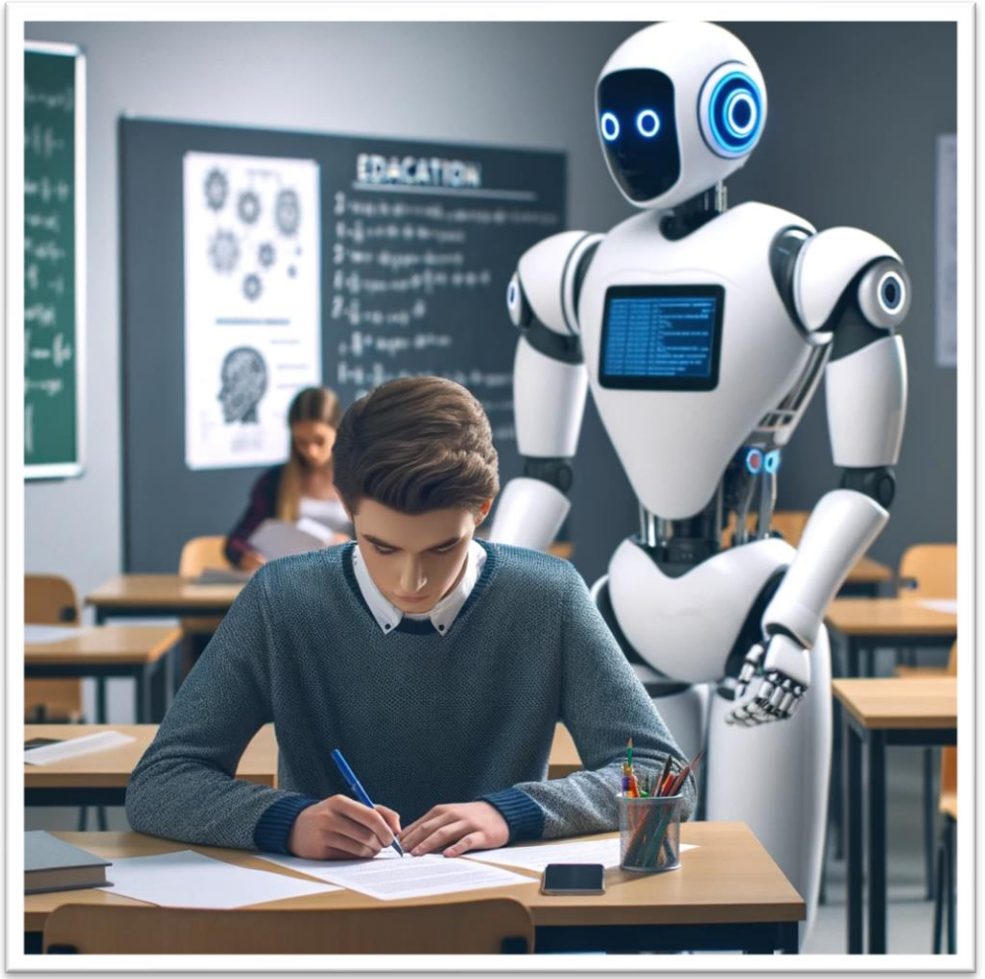
AI Act – Pratiques interdites (risques inacceptables)

- Liste des pratiques d'IA interdites car elles créent un **risque inacceptable**
- Exemples
  - Reconnaissance des émotions sur le lieu de travail et dans les établissements d'enseignement
  - Scoring social basé sur le comportement social
  - Systèmes d'identification biométrique à distance « en temps réel » dans les espaces publics à des fins répressives, avec un certain nombre d'exceptions soumises à autorisation judiciaire (très débattu lors des dernières discussions politiques)

Cadre réglementaire

AI Act – Systèmes d'IA entraînant des risques élevés

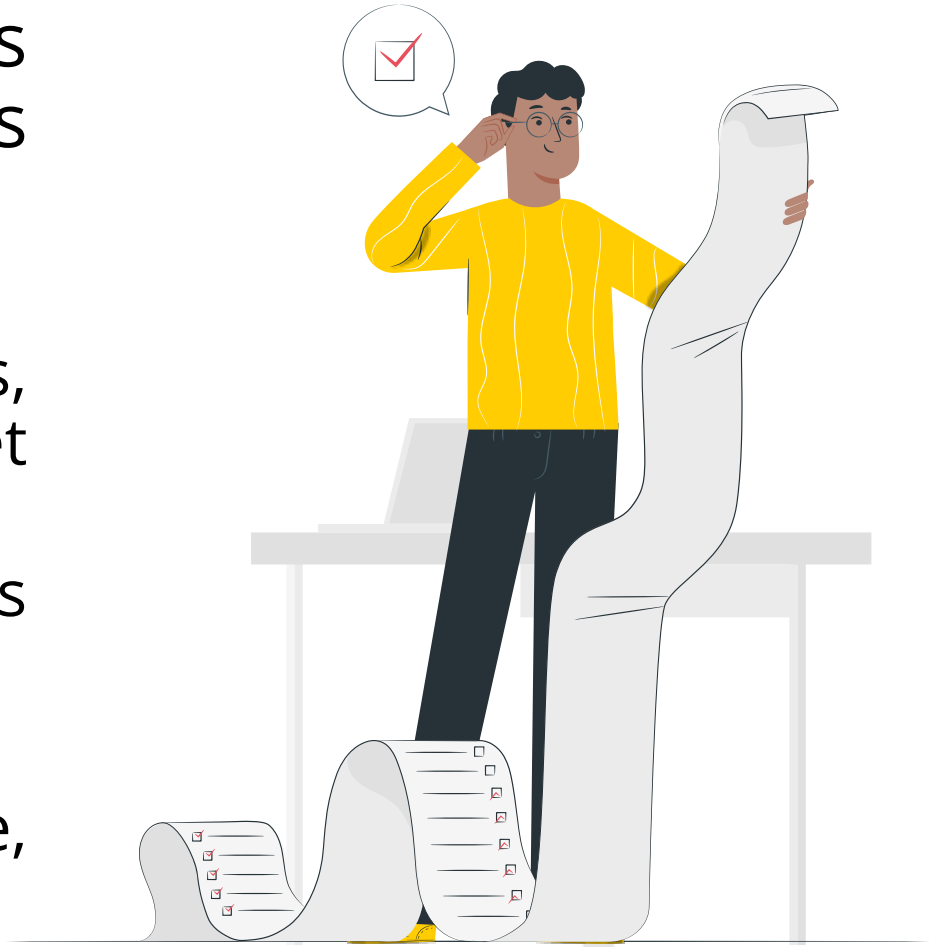
- Les systèmes d'IA qui entraînent des **risques élevés** pour la santé, la sécurité ou les droits fondamentaux, à savoir :
  - Systèmes d'IA qui constituent des produits faisant l'objet d'une évaluation indépendante (ex.: grand nombre de dispositifs médicaux)
  - Autres systèmes d'IA qui menacent entre autres les droits fondamentaux (ex.: évaluation des étudiants, accès à des programmes d'études, recrutement, licenciement, centrales d'appels d'urgence)



Cadre réglementaire

AI Act – Systèmes d'IA entraînant des risques élevés

- Exemples **d'exigences** pour les systèmes d'IA entraînant des risques élevés
  - Evaluation de la conformité
  - Données d'entraînement: pertinentes, représentatives, exemptes d'erreurs et complètes
  - Analyse d'impact sur les droits fondamentaux
  - Contrôle du système par des humains
  - Exigences en matière d'exactitude, robustesse et cybersécurité



Cadre réglementaire

AI Act – Systèmes d'IA entraînant des risques limités ou minimaux

- Obligation de transparence pour certains systèmes d'IA (ex.: systèmes qui interagissent avec des personnes ou qui génèrent des *deep fakes*)

- Encouragement au développement et à l'application de codes de conduits pour l'utilisation de système d'IA qui ne présentent pas de « hauts risques »

Cadre réglementaire

AI Act – Systèmes d'IA à usage général

Ajout récent d'une couche réglementaire supplémentaire

- Dispositions spécifiques pour les **systèmes d'intelligence artificielle à usage général** (y compris larges modèles d'IA générative comme ChatGPT ou Bard), c'est-à-dire les modèles développés avec une grande quantité de données en utilisant l'auto-supervision à grande échelle et capable d'effectuer un large éventail de tâches
  - Obligations de transparence, information aux utilisateurs de tels systèmes
- Obligations particulières pour les **systèmes ayant un impact « systémique »** (catégorisés avec un seuil de puissance de calcul à définir précisément), p. ex.:
  - Evaluations des modèles, reporting d'incidents graves mécanismes d'atténuations des risques, cybersécurité, rapport d'efficience énergétique

Cadre réglementaire

USA (aperçu)

- *Algorithmic Accountability Act* (2023)
  - Transparence, évaluations d'impact, formation et sensibilisation
- *AI Foundation Model Transparency Act* (2023)
  - Établissement de normes de transparence pour le déploiement de modèles de fondation (*Foundation Model)* par certaines autorités américaines, transparence sur les données d'entraînement et les mécanismes d'entraînement du modèle
- *Executive Order on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence* (2023)
  - Normes pour la sûreté et la sécurité de l'IA, protection de la vie privée des Américains, faire progresser l'équité et les droits civils, défense des consommateurs et des travailleurs, promotion de l'innovation et la concurrence

Cadre réglementaire

Suisse – Des stratégies

- Le Conseil fédéral a fait de l'IA une thématique centrale de sa stratégie 2018-2022 «Suisse numérique» et a créé un **groupe interdépartemental** «Intelligence artificielle» (IDAG-KI)
  - Défis de l'intelligence artificielle – Rapport du groupe de travail interdépartemental «Intelligence artificielle» au Conseil fédéral (décembre 2019)
  - Intelligence artificielle – Lignes directrices pour la Confédération (novembre 2020)
  - Réseau de compétences en intelligence artificielle (*Competence Network for Artificial Intelligence – CNAI*)
- Le Conseil fédéral a l'ambition de positionner la Suisse au niveau international dans le domaine de l'IA
  - DFAE, Intelligence artificielle et réglementation internationale – Rapport à l'attention du Conseil fédéral (avril 2022)
- Il n'existe toutefois actuellement **aucun cadre réglementaire** en matière d'IA
  - Lois technologiquement neutres (LPD, règles générales de responsabilité, LDA, LPTh, etc.)

ETH zürich ETH AI Center

About Us Research Industry & Entrepreneurship Education Art and Critical Thinking

Homepage > News & Events > ... > 2024 > 01 > Launch of a Risk Exploration and Mitigation Network for Generative AI

Launch of a Risk Exploration and Mitigation Network for Generative AI

The Swiss Call for Trust & Transparency has today launched a Pilot Gen AI Redteaming Network. The network unites all stakeholders - tech companies and public research institutions alike - to work collectively on disclosing, replicating, and mitigating the most urgent safety issues of generative AI systems. As of mid January 2024, 12 major tech companies have committed to joining forces with the network, thereby significantly advancing AI safety.

16.01.2024 by Helga Rietz-Pankoke

Cadre réglementaire

Suisse – Un cadre à fabriquer

- Volonté de créer un cadre réglementaire en matière d'IA annoncée le 22 novembre 2023
  - Le DETEC est chargé de présenter d'ici **fin 2024** les approches réglementaires possibles
  - Compatibilité avec l'*IA Act* et la Convention du Conseil de l'Europe sur l'intelligence artificielle
- Questions…
  - Approche générale ou sectorielle ?
  - Compétences de la Confédération ?

Cadre réglementaire

Suisse – Un cadre à fabriquer (et vite!)

RTS INFO | SPORT | CULTURE | PLAY RTS | AUDIO | TV | PROGRAMME TV | MÉTÉO | LA RTS | PLUS — RECHERCHER

L'INFO

INFO • TV • RADIO • FÉDÉRALES • ISRAËL-HAMAS • UKRAINE • SUISSE • MONDE • ENVIRONNEMENT • ECO • PLUS

Sciences-Tech. Modifié le 12 novembre 2023 à 05:21

La Suisse a besoin d'une réglementation sur l'intelligence artificielle, estime Albert Rösti

Pour Albert Rösti, la Suisse a besoin d'une réglementation sur l'IA / Le Journal horaire / 20 sec. / le 12 novembre 2023

La Suisse a besoin d'une réglementation dans le domaine de l'intelligence artificielle (IA), estime le conseiller fédéral Albert Rösti dans un entretien diffusé dimanche par la NZZ am Sonntag. Il préconise également la mise en place d'une instance de recours.

Son département, le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), va présenter un état des lieux au Conseil fédéral d'ici à la mi-2024 précise Albert Rösti. Mais il est important de ne pas entraver l'innovation dans le domaine de l'IA, relève le Bernois.

Intelligence artificielle: le Conseil fédéral examine les approches réglementaires

Berne, 22.11.2023 - Le Conseil fédéral souhaite permettre l'exploitation du potentiel de l'intelligence artificielle tout en réduisant autant que possible les risques pour la société. C'est pourquoi, dans sa séance du 22 novembre 2023, il a chargé le DETEC d'élaborer un aperçu des approches réglementaires possibles. Cet aperçu devrait être disponible fin 2024.

Cadre réglementaire

Suisse – Une activité parlementaire intense

- Postulat 23.3201 – Situation juridique de l'IA. Clarifier les incertitudes et encourager l'innovation.
- Motion 23.3807 – Reprise de la réglementation européenne en matière d'IA.
- Motion 23.3806 – Obligation de déclarer les recours à l'IA et aux systèmes de décisions automatisées.
- Motion 23.3849 – Un centre ou un réseau de compétences pour l'IA en Suisse.
- Interpellation 23.3930 – IA. Quel cadre pour en tirer le meilleur et en éviter les dérives ?
- Interpellation 23.4255 – Augmentation frénétique du volume de données. Faut-il intervenir en matière de gestion du volume de données et de consommation énergétique ?
- Interpellation 23.4133 – La protection légale contre la discrimination est-elle suffisante quand il est question de discrimination algorithmique ?

Cadre réglementaire

Et au niveau supranational ?

- Le Comité sur l'IA du Conseil de l'Europe a pour tâche d'élaborer un cadre juridique adéquat sur le **développement, la conception et l'application de l'IA**, qui se fonde sur les normes du Conseil de l'Europe en matière de droits de l'homme, de démocratie et d'État de droit et est propice à l'innovation
  - Instrument juridique contraignant à caractère transversal qui inclut notamment des **principes généraux communs**, ainsi que des instruments additionnels contraignants ou non contraignants afin de relever les défis liés à l'application de l'IA dans des secteurs spécifiques
- Projet de convention-cadre sur l'IA, les droits de l'homme, la démocratie et l'État de droit
  - Dernière version de travail connue datée du 8 janvier 2024

Cadre normatif

Aperçu en bref

- **ISO 42001:2023 (IA – Système de management)**
  - Spécifie les exigences relatives à l'établissement, à la mise en œuvre, au maintien et à l'amélioration continue d'un système de management de l'IA au sein des organisations
- **ISO 38507:2022 (Gouvernance des TIC – Implications de gouvernance de l'utilisation par des organisations de l'IA)**
  - Fournit des orientations aux membres de l'organe de direction d'une organisation pour permettre et régir l'utilisation de l'IA, afin d'en garantir une utilisation efficace, efficiente et acceptable au sein de l'organisation
- **ISO 23894:2023 (IA – Recommandations relatives au management du risques)**
  - Procure des recommandations relatives à la manière dont les organismes qui développent, produisent, déploient ou utilisent des produits, systèmes et services faisant appel à l'IA peuvent gérer le risque spécifiquement lié à l'IA
- **ISO 23028:2020 (IA – Examen d'ensemble de la fiabilité en matière d'IA)**
  - Passe en revue les sujets liés à la fiabilité des systèmes d'IA (p. ex. approches visant à établir la confiance dans les systèmes d'IA, menaces et risques typiques associés aux systèmes d'IA)
- **NIST *AI Risk Management Framework (*Cadre de gestion des risques de l'IA)**
  - Vise à améliorer la capacité à intégrité des considérations de fiabilité dans la conception, le développement, l'utilisation et l'évaluation des produits, services et systèmes d'IA

Conclusion

Quelle suite ?

- Les choses bougent (vite)
- La question principale est de déterminer la façon de réglementer l'IA
- Enjeux stratégiques et protection des droit fondamentaux

_swissprivacy.law