IA : les grands axes du futur règlement européen

Inacceptable, élevé, limité ou minime. Ces quatre niveaux de risque caractériseront peut-être bientôt, dans l'UE, les systèmes d'IA. Ils figurent en tout cas dans la proposition de règlement que la Commission européenne a publiée ce 21 avril.

Cette proposition n'arrive pas seule. Bruxelles en a soumis une deuxième. Là aussi en vue d'un règlement, destiné quant à lui à remplacer la directive de 2006 relative aux machines. Avec un objectif : pour poser un cadre à l'intégration sécurisée de l'intelligence artificielle.

Autre initiative : la mise à jour du plan coordonné qui détaille aux États membres les réorientations et les investissements nécessaires pour assurer la cohérence avec la stratégie de l'Union. Par rapport à la version initiale établie en 2018, il y a notamment des changements dans les domaines de la santé et de l'environnement. En toile de fond, la pandémie et le pacte vert pour l'Europe.

L'évaluation des risques inhérents aux systèmes d'IA se ferait sur trois plans : la santé, la sûreté et les droits fondamentaux. Elle tiendrait davantage compte des objectifs de ces systèmes que des fonctions mises en œuvre pour y parvenir.

Conformité : les véhicules autonomes traités à part ?

Le titre II du règlement couvre les cas dits « inacceptables ». On nous les décrit comme ceux qui « constituent une menace évidente pour la sécurité, les moyens de subsistance et les droits des personnes ». Parmi eux, ceux qui exploitent des techniques subliminales et/ou les vulnérabilités de certaines catégories de population. Mais aussi certains cas d'usage de la biométrie « distante » dans les lieux publics (comprendre la reconnaissance faciale).

Le titre III aborde les risques « élevés ». Il distingue les systèmes d'IA autonomes de ceux qui assurent une fonction de sécurité au sein d'un produit.
Pour les premiers, il est question d'établir un nouveau processus de vérification de conformité. Qui, selon les cas, pourra se faire en interne ou nécessitera l'intervention d'un organisme tiers homologué (ce sera systématique pour la biométrie distante).
Pour les seconds, les dispositions du règlement seront intégrées dans les législations sectorielles relatives à la sûreté. On aura donc des vérifications de conformité dans le cadre des processus existants. En tout cas pour les produits qui entrent dans une des catégories que couvre le « nouveau cadre législatif » relatif à la mise de produits sur le marché intérieur. **Pour les autres, dont l'automobile et l'aviation, le règlement ne vaudrait que recommandation…**

Analyse de risque

Parmi les systèmes susceptibles de présenter des risques élevés, il y a, entre autres, ceux :

- Utilisés dans les infrastructures critiques susceptibles de mettre en danger la vie et la

santé des citoyens (par exemple, les transports)
- Qui peuvent influencer l'accès à l'éducation et le parcours professionnel (notation d'examens)
- Employés dans des services privés et publics essentiels (évaluation du risque de crédit)
- Concourant au maintien de l'ordre (vérification de fiabilité des éléments d'une preuve)

Ces systèmes auront à respecter des obligations parmi lesquelles :

- Évaluation et atténuation des risques
- Contrôle des données qui alimentent ces systèmes
- Enregistrement des activités pour garantir une traçabilité
- Documentation technique
- Information claire et adéquate de l'utilisateur
- Contrôle humain
- Sécurité et robustesse à la conception

En cas de risque limité, il y aura uniquement des obligations en matière de transparence, pour trois types de systèmes. Premièrement, ceux qui interagissent avec les humains. Deuxièmement, ceux qui détectent les émotions ou catégorisent en fonction de données biométriques. Troisièmement, ceux qui créent ou manipulent du contenu (*deepfakes*).
Des codes de conduite non contraignants et adoptés sur la base du volontariat pourront intervenir en complément. Même chose avec les systèmes à risque minime (essentiellement les IA des jeux vidéo et des antispams).

Des pénalités au niveau du RGPD

Les systèmes développés exclusivement à des fins militaires échapperaient au règlement. *Idem* pour ceux utilisés dans le cadre de l'entraide judiciaire internationale.

La Commission européenne prévoit aussi la mise en place de « bacs à sable ». En d'autres termes, d'environnements de test dont les fournisseurs des systèmes d'IA auront convenu avec les autorités compétentes et qui leur permettront de tester leur conformité. Bruxelles en appelle à donner un accès prioritaire aux start-up et aux PME, face aux coûts de cette mise en conformité. On nous communique une estimation sur ce point : pour un système d'IA « moyen », il faudrait compter 6000 à 7000 €.

Qu'en est-il des pénalités prévues ? Il appartiendra aux États membres de les fixer, en s'appuyant sur trois plafonds :

- Jusqu'à 30 millions d'euros (ou 6 % du dernier chiffre d'affaires annuel dans le cas d'une société) pour usage d'un système d'IA au risque inacceptable ou non-respect des obligations de gouvernance des données d'entraînement
- Au maximum 20 millions d'euros (ou 4 % du C. A.) dans les autres cas
- Au plus 10 millions d'euros (ou 2 % du C. A.) pour fourniture d'informations « incorrectes, incomplètes ou trompeuses » aux autorités compétentes ou aux organismes de contrôle de conformité

Le texte suit la procédure législative ordinaire. C'est donc désormais au Parlement et aux 27 de s'en emparer. L'entrée en application interviendrait deux ans après le vote pour l'essentiel des dispositions. À l'exception, notamment, de la désignation des autorités compétentes et des organismes de contrôle, qui devrait intervenir sous trois mois.

Photo d'illustration © Parlement européen / CC BY-NC-ND 2.0