ASSEMBLÉE NATIONALE

Février 2024

Mission d'information de la commission des Lois

Intelligence artificielle générative et protection des données

Rapporteur :
M. Philippe Pradal

Groupe Horizons

Rapporteur :
M. Stéphane Rambaud

Groupe Rassemblement national

Pourquoi cette mission ?

Si elle est une évidence dans certains domaines depuis de nombreuses années, l'intelligence artificielle générative (IAG) a spectaculairement fait son entrée auprès du grand public par l'intermédiaire des robots conversationnels ou des trucages sur les réseaux sociaux. Conçus pour créer des contenus (sons, images, textes…) à partir de l'exploitation d'immenses quantités de données et de modèles statistiques complexes, ces systèmes peuvent s'adapter à de très nombreux usages, vertueux comme néfastes.

Tandis que l'Europe va se doter d'un nouveau cadre juridique en la matière, la commission des Lois a désigné MM. Philippe Pradal et Stéphane Rambaud pour étudier les évolutions nécessaires pour concilier progrès technologique et protection des citoyens.

Au terme de leurs travaux, nourris par plus de cinquante auditions de tous les acteurs concernés dont de nombreux experts, les rapporteurs mesurent les opportunités immenses qu'offre l'IAG, notamment pour l'action de l'État. Pour en tirer le meilleur, ils estiment urgent de s'assurer que les méthodes d'entrainement et de fonctionnement de ces modèles respectent les données des utilisateurs et n'introduisent pas de biais pouvant menacer, à terme, notre souveraineté. Leur utilisation doit également être sécurisée afin d'éviter tout détournement (arnaques, manipulation de l'information, *etc.*).

Les rapporteurs formulent donc une trentaine de recommandations, qui visent à réguler l'élaboration et l'utilisation des IAG par l'État, les entreprises et les particuliers, tout en veillant à ne pas pénaliser l'innovation, car la France compte parmi les pays les plus avancés dans ce secteur.

Des opportunités et des risques

L'intelligence artificielle générative (IAG) a d'abord été utilisée par les informaticiens pour traiter de grandes masses de données plus efficacement. Avec le progrès des modèles statistiques et le *big data*, ces modèles se sont perfectionnés et leur usage a été simplifié pour les rendre accessible au grand public et les adapter à un très grand nombre de tâches. C'est notamment le cas des modèles de langage (*LLM*) qui permettent de dialoguer en langage humain avec un robot.

Cette innovation présente des opportunités nouvelles en matière de créativité (images, sons), de productivité (bureautique, recherche d'information), de formation (contenus pédagogiques, exercices d'entrainement) et de communication (traduction, synthèse).

Mais elle présente aussi des risques liés à sa conception (utilisation massive de données, biais statistiques) et à son utilisation (tromperie, suppressions d'emplois, manipulation de l'information).

L'*AI Act* : vers une régulation européenne

L'Union européenne s'est dotée d'outils juridiques pour réguler les nouvelles technologies qui sont des références au niveau mondial, par exemple le règlement général sur la protection des données (RGPD).

Mais en l'absence de règlementation spécifique sur l'IA, la concurrence des modèles extra-européens risque de menacer la capacité de l'Europe à faire émerger des modèles conformes à ses principes.

Il apparaît souhaitable que les IAG obéissent à une règlementation commune au niveau mondial, et il est essentiel que le modèle européen puisse s'imposer, en s'appuyant sur l'importance de son marché en matière de nouvelles technologies.

Des outils de régulation nombreux

L'*AI act*, dont la négociation s'est achevée fin 2023 (voir encadré), établit de nouvelles règles de contrôle des systèmes d'intelligence artificielle, selon une échelle de risque.

S'agissant des IAG, il peut s'agir de contrôles *a priori* (qualité des données d'entrainement et du modèle statistique, contrôle des biais, marquage des contenus) ou *a posteriori* (qualité des réponses, hallucinations, traitement des plaintes).

Pour être efficace, ces outils nécessitent un haut niveau de performance technologique, grâce à une coordination entre les États membres pour partager leurs méthodes.

Allier protection et innovation

Une régulation est indispensable pour s'assurer que les IAG soient dignes de confiance. Elle doit s'imposer à l'ensemble des acteurs, y compris extra-européens lorsqu'ils sont accessibles sur le territoire européen ou qu'ils utilisent des données européennes.

Les standards doivent être adaptés à la taille des structures contrôlées, et la règlementation doit associer des règles de droit dur avec des règles de droit souple (*compliance*) visant à prévenir les dérives sans brider l'innovation et les usages.

Le règlement européen sur l'intelligence artificielle (*AI Act*)

Le Parlement européen et Conseil de l'Union européenne sont parvenus, le 9 décembre 2023, à un accord provisoire sur un règlement établissant des règles harmonisées concernant l'intelligence artificielle (*AI Act*). Le texte convenu doit dorénavant être formellement adopté par le Parlement et le Conseil avant d'entrer en vigueur.

Ce nouveau règlement vise à adapter le droit actuel de l'Union européenne aux spécificités de ces technologies, qui utilisent de grandes quantités de données personnelles.

Le degré de régulation sera proportionné au niveau de risque que représente le système, au regard du domaine dans lequel il intervient, de l'ampleur de son utilisation et, s'agissant de l'IAG, de la quantité de données et des capacités de calcul du modèle.

Permettre aux pouvoirs publics de jouer un rôle moteur dans le développement de l'IAG

Les pouvoirs publics sont directement confrontés à l'émergence des modèles d'IAG. Par leurs besoins et leurs pratiques, ils peuvent favoriser une innovation vertueuse.

Peu d'administrations utilisent les IAG à ce jour, malgré les efforts du Gouvernement pour coordonner l'intervention de l'État dans ce domaine.

Il apparait donc urgent d'identifier les usages possibles de l'IAG par les administrations, en consultant et en formant préalablement les agents et les usagers. Il pourrait s'agir, par exemple, d'améliorer l'accès au droit par un robot conversationnel capable de répondre aux questions des administrés.

Le contrôle humain devra rester la norme, mais des gains d'efficacité importants pourraient en résulter au bénéfice des citoyens et des agents.

Protéger les citoyens contre de nouveaux risques

Les pouvoirs publics ont également le devoir de protéger les citoyens contre les risques inhérents aux IAG.

Il s'agit d'abord de protéger les données des utilisateurs, en particulier les données à caractère personnel et celles soumises au droit d'auteur. La mise à disposition d'IAG de confiance, si possible françaises ou européennes, permettra de limiter le risque de biais, d'influence extérieure et d'atteinte aux valeurs républicaines.

Plus largement, il faut protéger les citoyens contre l'utilisation détournée des IAG. La France est souveraine pour adapter son droit pénal aux nouvelles menaces. Plusieurs infractions devraient être reconnues ou spécifiées : les hypertrucages (*deepfakes*), la manipulation de l'information, la définition du faux ou du plagiat…

Il ne doit pas être possible de recourir à une IAG sans en être informé et sans en informer celui qui sera le destinataire final du contenu. Ce principe s'appliquerait utilement lors des campagnes électorales, par exemple.

Enfin, le régime de responsabilité lié aux dommages causés par les IAG semble devoir être réformé. Il ne s'agit pas de créer une responsabilité sans faute des concepteurs, ce qui entraverait l'innovation, mais de compenser l'asymétrie entre les utilisateurs et les fournisseurs d'IAG, notamment dans l'élaboration de la charge de la preuve. Il s'avère effectivement difficile de démontrer l'origine d'un dommage causé par le dysfonctionnement d'une IAG.

Accompagner l'innovation privée en faveur des IAG de confiance

Par leurs besoins et leurs pratiques, les acheteurs publics peuvent favoriser une innovation vertueuse. Les administrations qui utilisent les IAG s'appuient souvent sur des solutions étrangères qu'elles adaptent à leurs besoins.

La France, qui compte parmi les pays les plus avancés en matière d'IAG, doit poursuivre son travail d'accompagnement auprès des *start-ups*. La CNIL, qui pourrait être renommée, apparaît comme la mieux à même d'assurer la mission de réguler les IAG. Elle serait conduite à amplifier ses efforts pour encourager les expérimentations (dans des « bacs à sable ») et sécuriser juridiquement les concepteurs de nouveaux modèles.

Ce travail exige également d'apporter un soutien important, notamment via la commande publique, à la recherche fondamentale et à l'investissement pour réduire la fuite des cerveaux et les coûts de développement des modèles, par exemple en mettant à disposition des calculateurs.

Coordonner les acteurs pour suivre les questions relatives à l'IAG sur le long terme

L'IAG n'en est encore qu'à ses prémices et les usages, tout comme leur régulation, devront s'adapter avec l'évolution des progrès technologiques.

Il apparaît donc nécessaire de spécialiser dès maintenant différents acteurs pour suivre cette thématique sur les moyen et long termes. Il serait utile de désigner un ambassadeur, un organe parlementaire, une administration, une juridiction et un régulateur dédiés à ce suivi.

Le rapport en 10 propositions

1. Spécialiser un ambassadeur, une administration, un organe parlementaire, une juridiction et un régulateur afin de disposer de l'expertise nécessaire au traitement des questions relatives aux IAG (*recommandations n° 1, 17, 32, 33 du rapport*).

2. Adapter le niveau de régulation au caractère systémique des IAG pour contrôler les systèmes d'origine extra-européenne et favoriser l'émergence de nouveaux acteurs (*recommandation n° 4*).

3. Prévoir des mécanismes de contrôle *a priori* et *a posteriori* qui garantissent la protection des données de la population dans l'Union européenne et évitent les biais risquant de porter atteinte aux principes européens (*recommandation n° 5*).

4. Favoriser le partage d'expérience en matière de régulation au niveau de l'Union européenne (*recommandation n° 2*) et favoriser le recours au droit souple pour ne pas pénaliser l'innovation (*recommandation n° 6*).

5. Identifier et coordonner les usages potentiels de l'IAG par les pouvoirs publics (*recommandations n° 12, 15, 18*), en recourant à l'expérimentation (*recommandation n° 21*), et associer et former les agents ainsi que les usagers au développement de l'IAG (*recommandation n° 13*).

6. Encourager le recours des acheteurs publics à des IAG de confiance (*recommandation n° 14*) et internaliser autant que possible le développement de ces systèmes pour en assurer la souveraineté (*recommandation n° 16*).

7. Transformer la CNIL en une Haute Autorité en charge de la protection des données et du contrôle de l'IA (*recommandation n° 9*) et renforcer son rôle d'accompagnement auprès des acteurs économiques pour encourager l'innovation (*recommandation n° 11*).

8. Améliorer la lutte contre les usages détournés de l'IAG par l'étiquetage des contenus (*recommandation n° 19*) et par l'information obligatoire des usagers lorsqu'ils entrent en interaction avec une IAG, notamment dans le cadre des campagnes électorales (*recommandation n° 20*).

9. Adapter la définition de certaines infractions comme le trucage, la contrefaçon ou le plagiat aux possibilités offertes par les IAG (*recommandations n° 23 à 27*).

10. Prévoir un régime de responsabilité spécifique aux concepteurs, aux fournisseurs et aux utilisateurs des IAG (*recommandations n° 29 et 30*) et permettre les actions de groupe dans ce domaine (*recommandation n° 21*).