CONFRONTATIONS EUROPE

JULIE SCHWARTZ
Collaboratrice senior (Privacy et Cybersécurité) chez Hogan Lovells et enseignante (Protection des données personnelles & Cybersecurité) à l'Université Paris-Saclay

COMMENT RÉGULER L'INTELLIGENCE ARTIFICIELLE DANS L'UNION EUROPÉENNE?

Dans cet article, Julie Schwartz analyse pour Confrontations Europe la proposition de règlement sur l'intelligence artificielle (IA) de la Commission européenne, dressant un état des lieux du texte législatif, actuellement en cours de discussions, et identifiant les interrogations et difficultés qui subsistent.*

1. LE BESOIN D'UNE RÈGLEMENTATION PROTECTRICE ET ADAPTÉE À LA PRATIQUE

Les nombreux débats et communications actuels autour de l'agent conversationnel Chat GPT soulignent parfaitement la nécessité d'avoir une règlementation sur l'Intelligence Artificielle (IA), au niveau européen, qui protège l'utilisateur sans pour autant entraver l'innovation.

Construire une telle réglementation implique de s'interroger. Comment catégoriser les systèmes d'IA ? Quels peuvent être les risques et comment les anticiper ? Quelles doivent être les règles applicables selon les systèmes d'IA ? Sur quelle base et quelle autorité pour protéger, conseiller et sanctionner ?

C'est à ces questions que la proposition de règlement IA du 21 avril 2021 de la Commission européenne tente de répondre et pose les bases d'une future réglementation harmonisée au niveau européen. Ce projet de texte est aujourd'hui encore en cours de discussion et fait l'objet de nombreux échanges au Parlement européen. Si plusieurs avancées notables ont été acquises, des points restent encore en discussion en l'état actuel du texte, avant de poursuivre les discussions avec le Conseil. Prenons un temps d'arrêt pour tenter de comprendre ces principaux points de discussion.

2. LES PRINCIPAUX POINTS DU RÈGLEMENT IA EN L'ÉTAT DE PROJET ACTUEL

2.1 LA CLASSIFICATION DES SYSTÈMES D'IA

Le projet de règlement IA prévoit une catégorisation des systèmes d'IA selon les risques, et décrit notamment les systèmes d'IA interdits ("inacceptables") et les systèmes d'IA à haut risque.

Les **systèmes d'IA interdits** sont ceux représentant une menace pour la sécurité, les moyens de subsistance et les droits des personnes. Ils incluent, à titre d'exemple, les systèmes d'IA pouvant avoir un impact sur les comportements humains (par exemple, un système d'assistance vocale incitant à un comportement dangereux) ou encore les systèmes de notation sociale (dit "social scoring") par les Etats. Des discussions sont en cours pour enrichir cette liste de systèmes d'IA interdits. Par exemple, le Parlement et le Conseil s'entendent pour y ajouter les systèmes de notation sociale par les entreprises privées (réseaux sociaux, fournisseurs d'hébergement en cloud, etc.).

*https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0020.02/DOC_1&format=PDF

Les désaccords demeurent toutefois importants entre le Parlement et le Conseil s'agissant des systèmes d'identification biométrique automatique à distance en temps réel dans des espaces accessibles au public et par les autorités répressives. Si le Conseil souhaite permettre exceptionnellement l'utilisation de ces systèmes à des fins répressives et de manière strictement encadrée, les membres du Parlement semblent avoir trouvé un point d'accord pour interdire un tel usage, compte-tenu des risques trop importants d'abus et de détournements de ces systèmes.

Les **systèmes d'IA à haut risque** sont quant à eux utilisés dans les infrastructures dites "critiques" telles que l'énergie, les transports, l'éducation ou la formation professionnelle (par exemple, la notation d'épreuves d'examen), les composants de sécurité des produits (par exemple, dans le cadre de la chirurgie assistée par robot), l'emploi et les ressources humaines (par exemple, pour le tri de CV lors d'une procédure de recrutement), les services publics et privés essentiels (par exemple, l'évaluation du risque de crédit pour obtenir un prêt), etc. Les discussions en cours sur cette liste soulignent le besoin de la mettre régulièrement à jour pour refléter les risques en pratique et également de la compléter de certains systèmes, tels que les systèmes d'IA utilisés pour déterminer une prime d'assurance, évaluer des traitements médicaux ou encore à des fins de recherche sur la santé, ou de supprimer de la liste sous certaines conditions des systèmes qui ne seraient plus considérés à haut risque selon leurs évolutions.

Les discussions sur la proposition de règlement ont également permis de proposer l'ajout, dans la classification, de **systèmes d'IA à usage général** afin de couvrir les systèmes d'IA qui peuvent être utilisés pour de nombreuses finalités différentes, ainsi que les situations dans lesquelles un système d'IA à usage général est ensuite intégré dans un autre système d'IA qualifiable de système d'IA à haut risque. Cette classification permet de prendre en compte des systèmes d'IA qui se développent sur le marché, tels que "ChatGPT". Des discussions sont actuellement en cours sur les obligations qui s'appliqueraient à ces systèmes d'IA à usage général, incluant éventuellement une partie des obligations des systèmes d'IA à haut risque, et que le Conseil souhaiterait plutôt définir via un acte d'exécution.

2.2 LES OBLIGATIONS APPLICABLES AUX SYSTÈMES D'IA À HAUT RISQUE

Les systèmes d'IA à haut risque font l'objet d'une attention particulière dans la proposition de règlement et des obligations spécifiques leur sont allouées. Ces obligations impliquent notamment de réaliser une analyse de risques afin de les identifier et les limiter autant que possible. Ces systèmes doivent également être construits de telle sorte qu'ils permettent d'assurer la qualité des données et la gouvernance de celles-ci afin de réduire les risques et les effets discriminants, notamment pour les jeux de données d'entraînement, de validation et de tests qui doivent être pertinents, représentatifs, exempts d'erreurs et complets.

Une documentation technique détaillée doit également être établie et un enregistrement des évènements afin de garantir la traçabilité de toute action et du fonctionnement du système d'IA est obligatoire. Des solutions techniques doivent enfin assurer un niveau approprié d'exactitude, de robustesse et de cybersécurité du système, tout au long du cycle de vie du système d'IA. Les derniers ajustements envisagés sur le texte clarifient ces obligations en termes de documentation et qualité des données pour les rendre moins contraignantes et techniquement plus praticables.

Le système d'IA à haut risque doit également être suffisamment transparent pour que l'utilisateur puisse l'utiliser et en interpréter les résultats de manière appropriée. Enfin, un contrôle humain demeure indispensable afin de limiter les risques.

Les modifications envisagées au texte ajoutent également de nouvelles obligations pour renforcer la transparence, par exemple l'obligation pour certaines entités publiques utilisatrices d'un système d'IA à haut risque de s'enregistrer dans une base de données de l'Union européenne. Des débats sont encore en cours sur les critères qui seront applicables pour définir les acteurs soumis à cette obligation.

3. LES PRINCIPAUX ENJEUX

Le texte de la proposition de règlement IA en l'état actuel soulève plusieurs interrogations et discussions. Par exemple, **l'analyse de risques** exigée pour les systèmes d'IA à haut risque peut être assimilée à l'analyse d'impact relative à la protection des données personnelles ("AIPD") ou "Privacy Impact Assessment" (PIA) de l'article 35 du Règlement Général sur la Protection des Données (RGPD). En pratique, il apparaît encore difficile d'identifier si ces deux analyses de risques, répondant à des obligations réglementaires différentes, seront concomitantes ou bien si elles devront être réalisées distinctement.

La qualification des acteurs est également l'un des enjeux de la proposition de règlement et notamment du fait de la terminologie utilisée. Est qualifiée de **fournisseur** la personne physique ou morale qui développe ou fait développer un système d'IA. L'**utilisateur** est la personne physique ou morale qui utilise le système d'IA sous sa propre autorité. L'**importateur** est la personne physique ou morale qui met sur le marché ou met en service un système d'IA, tandis que le **distributeur** est celui qui met le système d'IA à disposition sur le marché de l'UE (UE) sans altérer ses propriétés. Il est précisé que les termes "**mise sur le marché**" désignent la première mise à disposition du système d'IA sur le marché européen, "**mise en service**" signifie la fourniture du système d'IA pour sa première utilisation sur le marché européen et "**mise à disposition sur le marché**" fait référence à toute distribution ou utilisation sur le marché européen (à l'issue semble-t-il de sa première mise sur le marché ou mise en service).

Au-delà de la compréhension des termes utilisés, l'attribution des qualifications relèvera en pratique d'un travail ardu, qui sera d'autant plus nécessaire que les qualifications seront incluses dans les contrats et détermineront les obligations de chaque acteur concerné. Les risques de contentieux et requalification devront donc être anticipés.

Au niveau national, la **gouvernance** est également un enjeu important car la proposition de règlement IA impose de désigner une autorité nationale pour les sujets d'IA. Si, en Espagne, une autorité spécifique a d'ores et déjà été créée pour gérer ces sujets, en France, l'autorité de protection des données personnelles, la CNIL, déjà très présente sur ces sujets et réflexions depuis plusieurs années, semble s'imposer comme l'autorité qui prendra en charge cette responsabilité. Le Conseil d'Etat s'est d'ailleurs prononcé à ce sujet et encourage à faire évoluer et renforcer les pouvoirs et rôles de la CNIL pour qu'elle devienne l'autorité de contrôle française pour la régulation des systèmes d'IA. La CNIL s'est clairement positionnée en créant en début d'année un service de l'intelligence artificielle. Les discussions au Parlement ont permis de renforcer la gouvernance avec la création d'un "**bureau de l'IA**" qui devrait être le coordinateur de l'ensemble des autorités.

L'autorité nationale désignée pour réguler les systèmes d'IA sera également celle en charge de prononcer les **sanctions**, le cas échéant. En l'état d'actuel du texte, les montants maximums peuvent s'élever jusqu'à 30 millions d'euros ou 6% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Les parlementaires envisagent de prévoir des plafonds plus proportionnés selon les manquements et adaptés pour les plus petites entreprises.

4. LA SUITE

La proposition de règlement fait à ce jour encore l'objet de discussions au Parlement sur des sujets importants tels que la définition de l'IA elle-même ou encore la classification des différents types de systèmes d'IA à usage général.

Les prochaines étapes de discussion incluront les négociations entre la Commission européenne, le Parlement européen et le Conseil européen dans le cadre des trilogues. Une version finalisée ne semble donc pas pouvoir être envisagée avant plusieurs mois.

Le texte sera ensuite applicable deux ans après son entrée en vigueur, afin de permettre aux acteurs concernés de se mettre en conformité. En tant que règlement européen, il sera d'application directe dans tous les pays membres de l'Union européenne et ne nécessite donc pas de loi nationale de transposition, ce qui accélère et facilite une application harmonisée par chaque État membre.

L'entrée en vigueur du règlement IA sera également à mettre en perspective avec la proposition de directive en matière de responsabilité civile extracontractuelle dans le domaine de l'IA du 28 septembre 2022 qui impactera les règles de responsabilité applicables aux systèmes d'IA. Celle-ci nécessitera, en revanche, des lois nationales de transposition, pouvant ainsi créer certaines disparités entre les États membres.