L’UE s’est-elle tiré une belle balle dans le pied avec sa nouvelle réglementation sur l’IA ?

écrit par Monique B | 9 août 2024

Le projet de loi phare de l'Union européenne sur l'intelligence artificielle, communément appelé « AI Act », est entré en vigueur le jeudi 1er août.

Le projet de loi phare de l'Union européenne sur l'intelligence artificielle, communément appelé « AI Act », est entré en vigueur le jeudi 1er août.

Atlantico : Le 1er août 2024, l'Union européenne a officiellement mis en vigueur sa loi sur l'intelligence artificielle, connue sous le nom d'AI Act. Quel est l'objectif de l'IA Act ? Dans quelle mesure le besoin de régulation est-il nécessaire aujourd'hui ?

Rémi Bourgeot : Les progrès spectaculaires des modèles de langage reposent sur des réseaux de neurones utilisant des milliards de paramètres calculés sur des données de nature peu transparentes. Cela soulève des questions allant du respect de la vie privée à celui du droit d'auteur en passant par de multiples risques sécuritaires liés à leur usage et à leur fonctionnement erratique. Le besoin de réglementation est certain. Cependant, on aurait pu concevoir un texte plus clair et efficace, pour permettre à l'IA européenne de s'imposer sur une scène très compétitive, où la Big Tech américaine mène la danse avec des investissements gigantesques.

L'AI Act, en gestation depuis 2021, a fait face à de nombreux défis. L'explosion de l'IA générative en particulier a bouleversé son approche, fondée sur les

niveaux de risque associés à divers types d'applications. En a résulté un empilement de mesures de contrôle spéciales pour l'IA générative et en retour des exemptions pour l'open source, pour tenter de sauvegarder le potentiel d'innovation européen, dont témoigne notamment le succès des modèles du français Mistral AI.

Bernard Benhamou : Globalement, l'objectif de l'AI Act est d'éviter les dérives en termes de discrimination, de manipulations, de risques pour les personnes, de deepfakes… en soumettant à des obligations spécifiques les IA en fonction de leur niveau de risque.

Mais au-delà de cet objectif, l'esprit de ce texte vise surtout à éviter que nous ne devenions un continent où l'IA et d'autres technologies de surveillance ou d'analyse génétiques, ne soient mises au service du contrôle politique, individuel et social des populations comme c'est le cas en Chine. En allant plus loin, l'AI Act souhaite éviter qu'un système de notation des individus, comme le Crédit social chinois soit mis en place dans l'UE. L'Europe, soucieuse de préserver les libertés individuelles et les droits humains au sens large, souhaite éviter que ces IA ne puissent remettre en cause nos démocraties.

En raison des nombreuses conséquences sociales mais aussi politiques des dérives que peut connaître l'IA, cette régulation est donc primordiale. L'actualité nous le rappelle tous les jours : on voit par exemple de plus en plus de manipulations russes ou chinoises portant sur des désinformations amplifiées par l'IA. Il existe maintenant des systèmes qui permettent, à partir d'une série de « prompts » de quelques pages, de favoriser une personne dans le cadre d'une élection en automatisant la totalité de la campagne de désinformation. Ces systèmes, ces « robots » peuvent ainsi créer des faux comptes par dizaines de millions en l'espace de quelques jours. De tels systèmes de

désinformation entièrement automatisés par l'IA coûtent environ 400 euros par mois. Avec l'IA générative, on est en mesure d'industrialiser les réponses que font les faux comptes aux gens, donnant l'impression de parler à de vraies personnes, alors qu'il s'agit d'une IA qui leur dit ce quoi penser.

Pour vous donner une idée, en moyenne, chaque trimestre, Facebook efface de 1 à 1,5 milliard de faux comptes. Cela montre que les plateformes de réseaux sociaux n'ont aucun intérêt à prévenir en amont l'automatisation de la création de faux compte. Leur intérêt est en effet de faire croître leur audience le plus rapidement possible, pour extraire le plus de données possibles sur les utilisateurs, sans contrainte, en particulier sans exiger un moyen de paiement lors de la création de comptes.

Les pratiques prédatrices des patrons de la Silicon Valley ayant littéralement créé les conditions « idéales » pour qu'un désastre se produise, ce qui a conduit à des scandales comme Cambridge Analytica lors de l'élection présidentielle américaine. Si l'on y prend garde, les IA génératives pourraient avoir des conséquences encore plus graves pour nos sociétés dans les années à l'avenir.

Certains pensent que l'AI Act va décourager les entreprises européennes et renforcer la position des grandes entreprises de la Big Tech. L'Europe peut-elle se tirer une balle dans le pied avec sa nouvelle réglementation sur l'IA ?

Bernard Benhamou : C'est un discours que l'on entend depuis 25 ans à chaque fois qu'une régulation remet en cause les intérêts des grands acteurs de l'Internet. À chaque moment clé de la régulation technologique, on entend dire que cela va ralentir l'innovation et représenter une perte d'opportunités considérable pour les industriels des technologies et que cela ne pourra *in fine* que favoriser les entreprises chinoises…

Mais la réalité est plus complexe et, surtout, le prix à payer est aussi très élevé pour nos sociétés lorsque l'on ne régule pas suffisamment ou pas assez tôt. Cela a par exemple été le cas aux États-Unis avec l'absence d'une grande loi fédérale de protection des données personnelles. Cette absence a été à l'origine de nombreux scandales et a aussi favorisé des ingérences de pays étrangers. Les dérives de ces plateformes peuvent aussi être toxiques pour nos démocraties. Le Brexit, par exemple, a été largement manipulé par des systèmes d'analyse et l'influence des citoyens britanniques via le microciblage des réseaux sociaux. Ce qui a fait dire à Dominic Cummings, le directeur de la campagne du Brexit : *« Si Victoria Woodcock, la responsable du logiciel [de big data] employé pour la campagne, avait été renversée par un autobus, le Royaume-Uni serait resté dans l'Union européenne…».* Et cela bien sûr sans parler des ingérences russes sur les réseaux sociaux durant cette campagne et qui s'amplifient encore aujourd'hui…

Sur un autre plan, les monopoles qui existent aujourd'hui ralentissent déjà les innovations. À l'opposé, il y a aussi des risques liés une sur-régulation qui serait tatillonne et qui entraverait les entreprises de ce secteur. Mais nous avons déjà vécu le risque de la sous-régulation de ces plateformes qui nous expose à des risques systémiques de perte de confiance et donc de fragilité économique. Le dernier exemple est ce que l'on a appelé la bulle de l'IA. Il y a quelques jours à peine, au début de la semaine, certaines valeurs se sont effondrées, dont Nvidia, qui a perdu 500 milliards de dollars depuis sa plus haute valorisation de l'année. On voit bien que l'excès en l'absence de modèles industriels et économiques solides et durables, reste problématique. Les investisseurs reprochent aujourd'hui à l'IA de produire des innovations intéressantes, mais ils doutent que ces innovations suffisent à leur garantir des profits. Et donc,

fondamentalement, nous sommes dans un état de sous-régulation et de non-responsabilisation des acteurs technologiques. Est-ce que c'est souhaitable pour l'avenir ? Évidemment non.

Rémi Bourgeot : L'AI Act répond à un besoin évident de réglementation et d'encadrement des risques liés à l'IA. Pour autant, sa genèse compliquée a rendu les éléments de l'accord tortueux. L'idée de se positionner en gendarme numérique du monde, en se souciant moins de l'offre technologique du continent, pose en elle-même un risque existentiel à l'économie européenne et à son autonomie compétitive. Surtout, avec sa difficile application aux évolutions techniques futures, l'AI Act risque plutôt de servir les intérêts de la Big Tech, qui a les moyens d'aborder un labyrinthe réglementaire. L'annonce de l'entrée de Mistral dans l'orbite de Microsoft il y a quelques mois semble en fait plutôt le confirmer. L'AI Act arrive dans un contexte complexe et ne facilite pas les choses dans l'ensemble pour les entreprises européennes. Pour autant, il faut constater que le plus grand péril reste celui du déséquilibre de financement par rapport aux entreprises américaines.

Il n'est facile pour aucun État de réglementer une technologie aussi mouvante, que les responsables politiques peinent à appréhender. Le texte européen a beau être d'une rare complexité, on lui reconnaît dans le monde le mérite d'exister. De son côté, l'appareil d'Etat américain a le plus grand mal à se positionner face à l'hyperpuissance de la Silicon Valley et peine à se mettre à la hauteur de l'enjeu technique. Son déséquilibre générationnel, dont la prise de conscience a culminé avec les remous de la candidature Biden, n'y est d'ailleurs pas pour rien.

Comment faire en sorte d'encadrer les évolutions des IA afin qu'elles soient à la fois durables, protectrices des

libertés, sans entraver le développement des acteurs européens ?

Rémi Bourgeot : Les évolutions très rapides de l'IA auraient tendance à nécessiter une réglementation flexible, adaptative même. L'approche reposant sur des centaines de pages de considérations autoréférentielles, inscrites dans le marbre législatif, court le risque d'une rapide obsolescence. Au-delà d'un système d'exemptions prévues par l'AI Act, une certaine flexibilité est rendue d'autant plus nécessaire par le rôle de plus en plus central de l'open source dans l'IA, opportunité dont s'emparent les startups européennes. La plupart se réapproprient certains grands modèles de langage développés par les géants du secteur alors que certains développent désormais aussi leurs propres modèles sous-jacents.

L'Europe affiche un retard préoccupant, face aux géants américains, mais aussi face à la Chine. Cela n'était pas une fatalité. Les réseaux de neurones ont bénéficié, ces dernières décennies, du travail acharné de visionnaires européens, qu'ils soient restés sur le continent ou partis aux États-Unis, à une époque où d'autres types de modèles dominaient la scène de l'IA. Malgré la crise éducative, l'Europe et la France notamment gardent des poches d'excellence qu'il convient d'encourager au profit d'une IA différente. Le sous-entendu selon laquelle l'Europe s'épanouirait dans un rôle de régulateur mondial, dans une dépendance généralisée vis-à-vis des États-Unis et de la Chine en matière d'électronique, d'IA et de semi-conducteurs, n'est pas viable sur le plan économique et stratégique. On a vu un début important de correction avec des mesures de soutien et l'annonce d'exemptions réglementaires mais le chantier reste de taille.

Bernard Benhamou : Par définition, les opportunités perdues ne se manifestent pas directement pour les utilisateurs. En

effet, lorsqu'un grand acteur industriel est désavantagé par une régulation, il le fera savoir très fortement. Mais les petites sociétés qui ne pourront pas se créer ou se développer à cause d'une régulation trop contraignante, elles, ne se feront pas entendre.

Il y a des segments entiers de l'industrie qui auraient pu se développer en Europe et pas seulement aux États-Unis ou en Chine mais qui n'ont pu le faire en raison de régulations inadaptées en particulier dans le domaine de l'antitrust. Quand on ajoute à cela une incompréhension de la part des autorités européennes sur ce que sont les monopoles aujourd'hui et leur refus de créer des grands européens par crainte d'augmenter les prix pour les consommateurs, on se retrouve avec des monopoles extra-européens, surtout américains et chinois, qui écrasent les industries européennes. Comme le disait Thierry Breton, le temps n'est plus à la naïveté, mais à une réponse volontariste avec la mise en place d'une véritable politique industrielle pour les technologies en Europe.

Il faudra négocier cette bascule pour reconstruire une industrie européenne des technologies et établir des limites non pas de protectionnisme, mais de rééquilibrage concurrentiel. Ainsi, nous avons favorisé les Chinois de manière absurde sur les panneaux solaires, en subventionnant les industries chinoises au détriment des industries européennes. Cela ne doit pas se reproduire pour le secteur stratégique de l'IA.

L'application du texte peut-elle rencontrer des difficultés ?

Bernard Benhamou : L'application de ce texte sera très complexe à mettre en place. Il faut avoir des instances à l'intérieur de la Commission européenne, mais aussi à l'extérieur, pour effectuer des audits des systèmes. Il faut pour cela développer auprès des acteurs publics européens

des savoir-faire complexes. Par définition, ces instances sont censées valider les différents niveaux de risque et les étudier dans la durée. Elles sont, en gros, les chevilles ouvrières du texte. Le texte est là, mais ce sont les gens chargés de l'appliquer qui en assureront l'efficacité. Le risque est de ne pas développer suffisamment les moyens pour ceux qui devront appliquer la loi. Dans ce cas, on aurait un beau texte sans portée effective…

Y a-t-il des angles morts encore dans le projet ?

Bernard Benhamou : Certains ont soulevé des points techniques sur la limite entre technologies et usages, mais l'approche du texte est généralement saluée comme novatrice, y compris par les Américains. Toutes les grandes régions du monde suivent de près ce que nous faisons, car elles savent qu'elles devront s'en inspirer. C'était le cas pour le RGPD il y a quelques années, et ce sera le cas pour l'AI Act. En somme, la vraie difficulté réside dans la nécessité de faire évoluer ce texte. Si le texte est trop général, il n'aura pas de portée effective. S'il est trop spécifique, il deviendra facilement contournable. Il y a donc une obligation d'évolution du texte, avec des instances qui suivent et analysent le paysage pour adapter l'application de la loi au fur et à mesure. C'est là que résident à la fois la complexité et la difficulté.

https://atlantico.fr/article/decryptage/lue-sest-elle-tiree-une-belle-balle-dans-le-pied-avec-sa-nouvelle-reglementation-sur-lia-intelligence-artificielle-ia-act-regulation-europe-remi-bourgeot-bernard-benhamou