Entretien

Institut EGA

Entre protections et pressions, le difficile équilibre de la régulation numérique européenne

Avec Aurélie Banck, professeure associée à l'Université d'Évry Paris-Saclay et spécialisée en droit du numérique.

Propos recueillis par Audrey Crévolin, analyste à l'Institut d'études de géopolitique appliquée.

Institut d'études de géopolitique appliquée

Fondé en 2015, l'Institut d'études de géopolitique appliquée (Iega) est un *think tank* reconnu en France pour son expertise dans l'analyse des relations internationales, des enjeux géopolitiques et des dynamiques diplomatiques contemporaines. Organisme d'intérêt général, l'Iega se consacre à la production d'analyses rigoureuses, à l'information du public, ainsi qu'à la formation et au conseil auprès d'acteurs publics et privés, incluant les milieux économiques, institutionnels et diplomatiques. Animé par une exigence d'indépendance intellectuelle et de rigueur analytique, l'Iega poursuit l'ambition de fédérer la société civile, les décideurs institutionnels et la communauté scientifique autour des grands enjeux géopolitiques.

Face aux réalités du secteur numérique (accroissement exponentiel du volume de données, concurrence féroce sur le marché mondial, dominé notamment par les États-Unis et la Chine, développement rapide de l'intelligence artificielle [IA]), l'Union européenne (UE) a cherché à garantir sa souveraineté numérique et à protéger ses citoyens ainsi que ses entreprises. Cette souveraineté passe notamment par la mise en place de dispositifs de régulation. Après le Règlement général sur la protection des données (RGPD), entré en application en 2018, l'Union européenne s'est dotée d'autres instruments juridiques. Entré en vigueur en 2023, le Digital Services Act (DSA) permet de lutter contre les contenus illicites et préjudiciables, tandis que le Digital Markets Act (DMA), entré en application en 2024, a pour objectif d'encadrer l'activité économique des grandes plateformes numériques. Tous deux sont issus du « paquet législatif relatif aux services numériques » de 2020, qui vise à « protéger les utilisateurs en ligne tout en soutenant l'innovation[1] ». D'autres mesures portent sur le renforcement de la cybersécurité au sein de l'Union européenne, à l'instar des directives NIS[2].

En 2024, l'Union européenne a également adopté une nouvelle législation visant à réglementer l'intelligence artificielle : le règlement sur l'intelligence artificielle (RIA), également appelé IA Act. En s'érigeant en véritable pouvoir normatif mondial, l'Union européenne a imposé sa réglementation numérique au-delà de ses frontières. Ce phénomène a été théorisé sous le nom d'« effet Bruxelles » par Anu Bradford, experte en droit commercial international.

Cet entretien avec Aurélie Banck, professeure associée à l'Université d'Évry Paris-Saclay et spécialisée en droit du numérique, a pour objectif de mettre en lumière les objectifs et les principaux enjeux de la régulation numérique de l'Union européenne, notamment de l'IA Act, tout en analysant la manière dont Bruxelles doit composer avec les diverses pressions exercées par les États-Unis.

© Institut d'études de géopolitique appliquée

Entré en vigueur en 2024, l'IA Act a pour objectif « d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme, en particulier pour le développement, la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle dans l'Union, dans le respect des valeurs de l'Union, de promouvoir l'adoption de l'intelligence artificielle (IA) axée sur l'humain et digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux[3] […] ». L'IA Act (ou règlement européen sur l'intelligence artificielle) s'applique aux fournisseurs et aux déployeurs de systèmes d'intelligence artificielle (SIA), ainsi qu'aux fournisseurs de modèles d'IA à usage général[4]. Les systèmes d'IA sont classés selon les risques qu'ils présentent : pratiques d'IA interdites, systèmes à haut risque, systèmes soumis à une obligation de transparence et autres systèmes. En cas de non-conformité, les sanctions financières peuvent atteindre 35 millions d'euros ou 7 % du chiffre d'affaires annuel mondial réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu. Par ailleurs, un système d'IA non conforme peut être retiré du marché et des injonctions peuvent être prononcées, y compris à titre provisoire, notamment en cas de danger grave et immédiat[5]. Quel regard portez-vous sur l'IA Act ? Selon vous, peut-il constituer un cadre protecteur sans pour autant freiner la compétitivité des entreprises européennes ?

Pour porter un regard juste sur le RIA, il faut d'abord revenir à sa philosophie. Contrairement au RGPD, qui consacre des droits au bénéfice des personnes concernées, le règlement (UE) 2024/1689 est un texte visant à assurer la sécurité des produits, fondé sur l'article 114 du TFUE. Il encadre la mise sur le marché, la mise en service et l'utilisation de certains systèmes d'IA, selon une approche fondée sur les risques. Cette logique se retrouve dans sa structure : l'annexe I renvoie à des produits déjà réglementés (machines, dispositifs médicaux, véhicules), et le texte impose des obligations que l'on retrouve dans la réglementation des produits, à savoir le marquage CE et la surveillance après commercialisation. La protection des droits fondamentaux est certes un objectif affiché (article 1er), mais elle passe par des obligations imposées aux opérateurs, et non par la création de nouveaux droits subjectifs.



Le montant des sanctions que vous citez correspond en réalité au plafond des sanctions susceptibles d'être prononcées. Comme pour le RGPD, il s'agit d'un pourcentage du chiffre d'affaires annuel mondial. Si ce montant maximal est spectaculaire, il n'en reste pas moins que l'amende requise ou prononcée en cas de violation du RGPD n'atteint jamais nécessairement ce plafond. La même logique est transposable au RIA. Il s'agit ici d'appliquer un principe de proportionnalité : l'amende poursuit un objectif punitif, mais il ne s'agit pas d'entraîner la faillite d'une société. La proposition de la Commission date d'avril 2021, avant l'arrivée des grands modèles de langage auprès du grand public. Elle était construite autour des usages, comme la loi Informatique et Libertés de 1978, et était donc technologiquement neutre. Or, ce sont les textes neutres qui résistent le mieux, parce qu'ils s'adaptent aux évolutions techniques. Le choc provoqué par la démocratisation de ChatGPT a conduit le législateur européen à ajouter un chapitre dédié aux modèles d'IA à usage général (chapitre V). C'est, à mon sens, une inflexion discutable, car le texte ne régule plus seulement les usages de l'IA, mais également une forme de technologie, ce qui fragilise sa cohérence d'ensemble.

Le RIA est par ailleurs moins prescriptif que le RGPD. Il laisse de larges marges d'interprétation aux acteurs et renvoie à de nombreux instruments de droit souple et d'application : lignes directrices de la Commission et du Bureau de l'IA (définition du système d'IA, pratiques interdites, modèles à usage général), code de bonnes pratiques pour les modèles à usage général, normes harmonisées, actes délégués et actes d'exécution.



Un texte qui s'en remet autant à l'interprétation crée de l'incertitude et nuit à la prévisibilité, ce qui est coûteux pour les entreprises, en particulier pour les PME, qui doivent déterminer comment se conformer à ses exigences sans disposer d'un référentiel stabilisé. Ce risque est d'autant plus réel que le calendrier d'application a été remanié par le règlement (UE) 2026/1744, publié en juillet dernier, qui a reporté l'application de certaines dispositions du RIA. Réguler revient à orienter et à contraindre.

L'Union fixe les règles applicables aux produits qu'elle accepte sur son marché, comme elle le fait pour les biens d'équipement ou les denrées alimentaires. Opposer régulation et innovation relève d'un débat simpliste, car une règle claire et proportionnée peut également susciter la confiance, condition de l'adoption de la technologie.

Cette exigence est particulièrement forte pour l'IA, pour deux raisons :

- L'impact sur les personnes. Les décisions algorithmiques ont des conséquences concrètes en matière de recrutement, d'accès au logement ou au crédit, d'orientation professionnelle ou de justice.
- L'autonomie croissante des systèmes. Les systèmes apprennent et les agents peuvent accomplir seuls des tâches complexes, y compris des actions offensives, comme l'attaque du site Internet Hugging Face par des agents d'IA d'OpenAI.

Exiger que ces systèmes soient sûrs, testés et surveillés après leur mise sur le marché est donc nécessaire, et c'est là le cœur du RIA. Cela peut ralentir le développement ou la commercialisation d'un produit, mais c'est un choix assumé.

La véritable question est celle de l'efficacité : le dispositif permettra-t-il d'éviter les abus, les détournements d'usage et les dérives ? Et quel en sera le coût ?

À ce jour, il est malheureusement trop tôt pour se prononcer sur ce point. La disposition relative à la transparence des contenus générés à l'aide de l'IA est probablement celle du RIA qui, depuis son entrée en application en août 2026, a eu le plus d'impact sur le grand public et a permis une certaine prise de conscience.

Contrairement à l'Union européenne, l'IA semble peu réglementée aux États-Unis. La réglementation américaine de l'IA repose sur plusieurs niveaux : le niveau fédéral, celui des États fédérés et même celui des municipalités. Les États fédérés jouissent d'une grande liberté pour légiférer, ce qui a conduit à la multiplication des lois sur l'IA dans différents domaines : biométrie, IA dans la gestion des ressources humaines, protection de la vie privée, hypertrucage, profilage publicitaire ou encore risques liés aux très grands modèles de langage[6] (LLM).

Cette déréglementation de l'IA s'intensifie sous le gouvernement de Donald Trump. Le 11 décembre 2025, le président américain a signé un décret (Ensuring a National Policy Framework for Artificial Intelligence) visant à centraliser, au niveau fédéral, la régulation de l'IA afin de réduire la marge de manœuvre des États fédérés. Pour rappel, plus de cent lois ont déjà été adoptées dans une trentaine d'États. Ce décret présente les législations des États en matière d'IA, jugées « excessives », comme une entrave à l'innovation, dans la mesure où elles créeraient un paysage réglementaire morcelé et complexifieraient la mise en conformité, en particulier pour les start-up[7].

Ce décret a également pour objectif d'établir un cadre peu contraignant en matière d'IA : « il est de la politique des États-Unis de maintenir et de renforcer sa domination mondiale en matière d'IA au moyen d'un cadre national peu contraignant[8] ». Plus récemment, le 20 mars 2026, la Maison-Blanche a publié une série de propositions législatives, directement issues du décret du 11 décembre 2025, adressées au Congrès dans le but de faire adopter une législation fédérale régissant les questions liées à l'IA. Quels seront les effets et les risques, à l'échelle mondiale, de ce mode de régulation ?

Dire que l'IA est « peu réglementée » aux États-Unis me paraît inexact, comme le montre la question elle-même. C'est la forme de la réglementation qui diffère de l'approche européenne. En Europe, le RIA est considéré comme une réglementation horizontale, c'est-à-dire qu'il s'applique à l'IA et à ses usages de manière globale. Aux États-Unis, la réglementation est sectorielle, fragmentée et organisée à plusieurs niveaux : celui des États fédérés, celui des agences fédérales, etc. Par ailleurs, elle est davantage centrée sur les effets des systèmes d'IA, notamment leurs effets préjudiciables, que sur les conditions de leur mise sur le marché, comme c'est le cas en Europe.

On peut notamment citer la loi californienne SB 53 sur la transparence des modèles de pointe, signée le 29 septembre 2025 et applicable depuis le 1er janvier 2026. À New York, le RAISE Act a été adopté en 2026, avec une entrée en vigueur au 1er janvier 2026. Le Colorado a adopté, en 2024, une loi sur les systèmes à haut risque. Enfin, à New York, une loi municipale impose, depuis janvier 2023, des audits de biais pour les outils automatisés de recrutement.

Le décret que vous mentionnez vise à centraliser, au niveau fédéral, la régulation de l'IA. Il prévoit notamment la contestation judiciaire de certaines lois des États ainsi que l'identification, par le département du Commerce, des lois considérées comme « excessivement contraignantes ». Il s'agit donc de tendre vers un cadre fédéral harmonisé, et non de priver d'effet ou d'annuler les lois déjà adoptées.

Le département de la Justice a effectivement créé l'AI Litigation Task Force le 9 janvier 2026. Le 24 avril 2026, il a annoncé son intervention dans le recours engagé par xAI contre la loi du Colorado relative aux discriminations algorithmiques. Cependant, le décret imposait au département du Commerce de publier une évaluation des lois considérées comme « excessivement contraignantes », ainsi qu'une note de politique générale (Policy Notice). Ces documents n'ont pas été publiés dans leur version définitive. Dès lors, l'ensemble des instruments prévus par ce décret n'ont pas été mis en œuvre.

Face aux initiatives réglementaires de l'UE en matière de numérique et aux sanctions qui en découlent, le gouvernement américain et les grandes entreprises technologiques ont adopté une posture offensive. En matière de sanctions, Bruxelles a infligé, en 2025, une amende de 500 millions d'euros à Apple et de 200 millions d'euros à Meta dans le cadre du DMA, ainsi qu'une amende de 120 millions d'euros à X dans le cadre du DSA.

Cette posture agressive des États-Unis à l'égard de la réglementation numérique européenne et des sanctions qui en découlent s'est accentuée avec le retour au pouvoir de Donald Trump. Elle prend différentes formes : accusations d'atteinte à la liberté d'expression américaine, menaces de sanctions diverses (imposition de nouveaux droits de douane, surtaxes et restrictions visant des entreprises européennes comme Spotify et Mistral AI). En décembre 2025, Thierry Breton, ancien commissaire européen, a été sanctionné pour son implication dans la régulation numérique, en se voyant privé de visa pour les États-Unis. Cette posture offensive se traduit également par un lobbying intensif des grandes entreprises technologiques américaines auprès de l'UE. Selon Corporate Europe Observatory, les grandes plateformes ont augmenté leurs dépenses de lobbying auprès de l'UE de 33,6 % entre 2023 et 2025[9]. Quels leviers l'UE peut-elle activer pour contrer ces pressions exercées par Washington ?

Je pense qu'il faut distinguer les leviers juridiques des leviers politiques ou économiques, ainsi que les objectifs poursuivis en réponse aux actions de l'administration Trump.

D'un point de vue juridique, le premier mode de réponse consiste à recourir au règlement (CE) n° 2271/96, dit « statut de blocage », qui protège les opérateurs européens contre les effets extraterritoriaux des législations de pays tiers énumérées en annexe. Il interdit de se conformer à ces législations (article 5), prive d'effet dans l'Union les décisions juridictionnelles et administratives qui en découlent (article 4) et ouvre une action en réparation des dommages subis (article 6).

La CJUE en a confirmé la portée dans l'arrêt Bank Melli Iran du 21 décembre 2021 (C-124/20), tout en soulignant la nécessité de ménager la liberté d'entreprise. Son efficacité face à la situation actuelle reste toutefois limitée. Il ne s'applique qu'aux actes figurant dans son annexe, qui devrait être modifiée par acte délégué pour couvrir les nouvelles mesures américaines, le cas échéant. Il vise par ailleurs des sanctions économiques, et non des mesures individuelles telles que la privation de visa dont a, par exemple, fait l'objet M. Thierry Breton. Il constitue donc un outil de protection des entreprises plutôt qu'une réponse globale à une mesure de coercition résultant de nouvelles mesures de régulation.

Le règlement (UE) n° 654/2014, modifié par le règlement (UE) 2021/167, est un autre outil qui pourrait être utilisé et qui relève davantage d'une logique offensive. Il permet à l'Union d'adopter des contre-mesures (droits de douane, restrictions à l'importation ou à l'exportation, limitations de l'accès aux marchés publics) lorsqu'un pays tiers adopte des mesures contraires au droit international et fait obstacle au règlement des différends. La réforme de 2021 en a étendu le champ aux services et à certains aspects de la propriété intellectuelle, domaines directement pertinents pour le numérique. Ce texte vise toutefois à faire respecter les droits commerciaux de l'Union. Sa mobilisation suppose donc de qualifier les mesures américaines de contraires au droit international, ce qui n'est pas acquis lorsque la menace brandie consiste en l'imposition de droits de douane ou en une restriction de visa visant un individu.

La réponse juridique doit également être interne, en particulier s'agissant de l'encadrement du lobbying à Bruxelles. Le registre de transparence, régi par l'accord interinstitutionnel de 2021, subordonne les rencontres avec les représentants d'intérêts à leur inscription au registre, mais son caractère contraignant demeure limité.

La proposition de directive de décembre 2023 sur les représentations d'intérêts exercées pour le compte de pays tiers (COM(2023) 637) vise à imposer des obligations de transparence aux acteurs financés ou mandatés par des États tiers. L'enjeu est de renforcer les obligations de déclaration, les règles relatives aux conflits d'intérêts et la traçabilité des échanges avec la Commission. Cette hausse de 33,6 % des dépenses de lobbying relevée par Corporate Europe Observatory dans son rapport montre que l'influence est désormais un enjeu de souveraineté normative.

Sur le plan économique et politique, l'Union européenne est largement importatrice de services numériques américains, ce qui lui offre un levier de négociation : des restrictions d'accès aux marchés publics, une taxation des services numériques, voire une suspension de concessions, pourraient constituer des leviers à activer. Ils sont cependant à double tranchant, car ils créent un risque d'escalade et de représailles, y compris dans d'autres secteurs. Leur mobilisation suppose en outre une unité politique entre les États membres, dont certains privilégient clairement la préservation de la relation transatlantique.



Le cadre commercial convenu en août 2025 illustre cette tension : l'Union a affirmé que sa réglementation numérique n'était pas négociable, mais la pression américaine s'est maintenue.

Le 19 novembre 2025, la Commission européenne a publié deux propositions de règlements afin d'harmoniser et de simplifier le cadre juridique numérique de l'Union européenne, dans le cadre de la réforme dite « Omnibus numérique ». L'une de ces propositions concerne les règles existantes en matière de données, de cybersécurité et de respect de la vie privée. La seconde a pour objectif de modifier la législation sur l'intelligence artificielle. Quels effets ces règlements pourraient-ils avoir sur les droits des personnes situées dans l'Union européenne et sur les entreprises s'ils étaient adoptés ? Quelles sont les raisons qui ont motivé la mise en place de ces ajustements ? S'agit-il uniquement de simplifier le cadre réglementaire pour soutenir la compétitivité de l'Union européenne ou également d'apporter des modifications sous la contrainte des pressions exercées par les États-Unis et les grandes entreprises technologiques américaines ?

S'agissant des textes Omnibus, la Commission européenne a proposé, en novembre dernier, un texte Omnibus sur l'IA (Omnibus on AI) et un texte dit Omnibus numérique (Digital Omnibus), qui vise, comme vous le mentionnez, à rationaliser différentes réglementations relatives aux données, en particulier le RGPD, mais pas uniquement.



Ces deux textes ont connu des évolutions différentes. Dans la mesure où l'Omnibus sur l'IA visait à reporter la date d'entrée en application de certaines dispositions de l'IA Act, qui devaient initialement s'appliquer le 2 août 2026, son calendrier d'examen a été accéléré et le texte a été adopté en juillet 2026. Ce n'est pas encore le cas de l'Omnibus numérique, qui va entrer dans la phase de trilogue. En outre, la portée des modifications présentées par la Commission comme des mesures de simplification, notamment pour les particuliers, est très différente selon les deux textes.

En ce qui concerne l'Omnibus sur l'IA, il s'agit essentiellement de modifications techniques, à l'exception d'un changement portant sur l'utilisation de données dites sensibles au sens du RGPD pour entraîner des modèles d'IA. Le RGPD prévoit des conditions de traitement assez strictes pour les données dites particulières ou sensibles, dont le traitement est interdit, sauf exceptions.

La modification du RIA adoptée en juillet dernier vise à prévoir une exception permettant l'utilisation de ces données à des fins d'entraînement des modèles d'IA. Dès lors, au-delà de ce changement et du report du calendrier d'application des obligations, ces modifications n'auront pas d'impact direct. Les exigences de fond sont conservées, mais elles s'appliqueront plus tard. Pendant cette période, les personnes exposées à des systèmes à haut risque (recrutement, crédit, éducation) bénéficient cependant d'une protection moindre que celle initialement prévue.

Pour les entreprises, le report de l'entrée en application est bien entendu salué, notamment parce que l'ensemble des textes d'interprétation n'a pas encore été adopté (cf. *supra*).

En ce qui concerne l'Omnibus numérique, la portée des modifications est différente.

Dans sa version initiale, la Commission européenne proposait notamment de modifier la définition de la notion de données à caractère personnel afin d'en réduire la portée. De nombreux lobbyistes ont saisi cette occasion pour aller encore plus loin, et l'on a pu voir circuler des propositions visant à réduire la notion de données à caractère personnel à celle de données nominatives, ce qui équivaudrait à revenir à la définition applicable en France en 1978.

Ce texte propose également de rationaliser les dispositions applicables en matière de protection des données non personnelles, en particulier en fusionnant le Data Governance Act dans le Data Act, ce qui constitue une amélioration en matière de lisibilité de la réglementation.

Dès lors, si ces modifications sont officiellement présentées comme des mesures techniques destinées à répondre à de réelles difficultés d'application, certaines vont au-delà et pourraient entraîner une réduction substantielle du niveau de protection des données des personnes en Europe.

Il est évident que le marché numérique européen et les conditions d'accès à ce marché, dont fait partie la réglementation, sont devenus une monnaie d'échange dans les négociations avec l'administration Trump. Pour autant, je ne pense pas que la régulation du numérique doive servir de monnaie d'échange car, au-delà des aspects économiques, elle traduit également des valeurs et un modèle social. Les élections de mi-mandat aux États-Unis pourraient cependant rebattre les cartes.

RÉFÉRENCES

[1] « Paquet législatif relatif aux services numériques », consilium.europa.eu, 26 octobre 2022, https://www.consilium.europa.eu/fr/policies/digital-services-package/

[2] La directive « Sécurité des réseaux et de l'information » (dite « directive NIS », de son nom anglais Network and Information System Security) poursuit un objectif majeur : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne (UE). Elle a été adoptée le 6 juillet 2016. La directive NIS 2, adoptée en 2022 et qui s'appuie sur les acquis de NIS 1, élargit ses objectifs et son périmètre d'application afin d'apporter une protection renforcée. Source : Cyber.gouv.fr.

[3] « Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) », Journal officiel de l'Union européenne, eur-lex.europa.eu, 17 juillet 2024, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1689

[4] *Ibid*., article 2, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202401689

[5] « EU AI Act : comprendre le premier cadre réglementaire sur l'intelligence artificielle », deloitte.com, 23 juin 2025, https://www.deloitte.com/fr/fr/our-thinking/explore/tech/EU-AI-Act.html

[6] Winston MAXWELL, « La régulation de l'intelligence artificielle aux États-Unis », Action publique. Recherches et pratiques, 2024/4, n° 23, p. 39.

[7] « Ensuring a National Policy Framework for Artificial Intelligence », Executive Order, whitehouse.gov, 11 décembre 2025, https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/

[8] *Ibid*., section 2.

[9] « Big Tech lobby budgets hit record levels », corporateeurope.org, 29 octobre 2025, https://corporateeurope.org/en/2025/10/big-tech-lobby-budgets-hit-record-levels