Vers un droit européen de la société du numérique

Poullet, Yves

Published in:
L'influence du droit européen en droit économique

Publication date:
2022

Document Version
le PDF de l'éditeur

Vers un droit européen de la société du numérique[1]

Yves Poullet

Professeur émérite de la Faculté de droit et co-président du Namur Digital Institute de l'UNamur
Professeur associé à l'UC Lille et Membre de l'Académie Royale de Belgique

1. Nos « carrières », cher Denis, ont débuté ensemble, ta thèse date de 1983, la mienne ne la précède que d'un an. Nos routes ont suivi des chemins certes différents : tu as réussi à cumuler, avec un égal bonheur, d'une part, une activité réputée d'avocat au sein d'un cabinet qui porte ton nom et ton empreinte et, d'autre part, une carrière académique qui te mène bien au-delà des frontières. Toujours, à des moments divers, nos parcours se sont croisés sur des thèmes d'intérêt commun : l'imprévision, la garantie bancaire, la responsabilité, les *blockchains*… Une même passion pour le droit européen et comparé nous unit et elle m'invite à partager cette réflexion, non pour la clore, mais comme base de nouvelles discussions qui mêleront, je le sais, tant le plaisir intellectuel que celui bien plus essentiel encore pour nous deux de l'amitié.

L'arrivée d'une nouvelle Commission européenne s'est traduite par une effervescence de nouveaux textes réglementaires, à l'appui d'une stratégie de plus en plus proactive en vue de tracer une troisième voie pour le développement du numérique. Sans doute, l'intelligence artificielle (en abrégé IA), *buzzword* de l'avènement d'une société du numérique, a été l'occasion pour une intervention qui va bien au-delà de la proposition de règlement sur l'IA.

Il importe de préciser, dans un premier point, cette stratégie qui inspire l'action réglementaire de l'Europe. À l'heure où se multiplient les

1 Il y a 20 ans, soit en 2002, l'auteur publiait un article : « Vers la confiance : Vues de Bruxelles – un droit européen de l'internet », publié dans : *Le droit international de l'Internet*, Actes du colloque organisé à Paris les 19 et 20 novembre 2001, Bruxelles, Academia-Bruylant, pp. 133-176 (texte accessible sur le site du CRIDS de l'Université de Namur). Le lecteur qui voudra bien s'y référer mesurera l'évolution en 20 ans de l'action réglementaire de l'Union européenne.

chantiers réglementaires, le citoyen de cette Europe s'interroge sur les limites de cette intervention des institutions européennes. Les questions de libertés individuelles, de démocratie, d'ouverture de nos administrations, d'économie de la santé, d'encadrement des plateformes, de nouveaux médias… rien n'échappe au régulateur européen.

Mon deuxième point détaillera ces facettes nombreuses de ces chantiers dont certains sont encore ouverts ou simplement envisagés.

Le troisième point met en évidence les caractéristiques particulières des textes relatifs au numérique du droit législatif européen. Les méthodes ont changé. Fini le temps des directives, voilà venu celui des règlements y compris ceux prônant des obligations asymétriques en ce qui concerne certains opérateurs sur le marché du numérique. Dans le même temps, on note la défiance vers l'autoréglementation et le souci d'une corégulation descendante laissant certes une place à la *soft law* mais l'encadrant de nombreuses balises. La constitution et la multiplication d'autorités administratives au niveau national contrôlées ou en tout cas coordonnées au niveau européen sont un second trait. Soucieuses de veiller à la proportionnalité de l'intervention et à l'effectivité des réglementations, on voit poindre une approche par les risques et consacrées des mesures préventives, y compris par la création d'organes de compliance interne, et ce, en complément voire en lieu et place du contrôle *a posteriori*.

Enfin, quelques réflexions abordent la façon dont les textes entendent assurer une véritable souveraineté européenne, n'hésitant pas à étendre l'application de ces textes à des entreprises situées en dehors du territoire de l'Union européenne.

2. Avant d'aborder ces différents points, soulignons que mon propos, pour être complet, aurait dû aborder le rôle, d'une part, de la Cour de justice de l'Union européenne et, d'autre part du Parlement, souvent aiguillon de l'action de la Commission. La multiplication des décisions de la Cour est remarquable par son interprétation osée et innovante des textes réglementaires, renforçant ces derniers. Les résolutions du Parlement européen témoignent de la volonté croissante de cette institution de jouer à plein sa fonction nouvelle d'initiation et d'appui de l'action de la Commission. Les limites de volume imposées aux présentes réflexions constituent la seule justification de notre silence sur leurs initiatives.

Section 1. Les objectifs d'une politique réglementaire européenne de la société du numérique

3. Quelle réponse réglementaire spécifique l'Europe apporte-t-elle aux défis du numérique ? Le numérique ne nous colle-t-il pas, désormais, à la peau, au sens tant figuré que réel et ne guide-t-il pas, pour le meilleur et le pire, tant nos vies que celles des entreprises et des administrations ? Il importe dès lors, et c'est le rôle de l'autorité publique, de tracer la voie des usages d'un outil qui, de plus en plus, constitue l'ossature de notre économie, de notre société, de nos relations et de nous-mêmes. L'introduction mentionnait la volonté européenne de mener une troisième voie. De quoi est-il question ? Sans doute, cette troisième voie était-elle préparée par la précédente Commission européenne et le Parlement d'alors, mais elle est désormais clairement affirmée par le fameux « Livre Blanc sur l'intelligence artificielle » publié par la nouvelle Commission[2] et sa présidente dès leur entrée en fonction. La stratégie y est explicitement énoncée et sa mise en œuvre se réalise depuis, à travers des textes qui se suivent à un rythme accéléré et débordent largement la question de l'intelligence artificielle.

Comme il sera souligné, c'est une politique réglementaire de la donnée, de sa création, de son utilisation, de sa transmission et de ses impacts, que l'Europe entend développer de manière cohérente[3]. Il s'agit bien d'une troisième voie dans la mesure où l'Union européenne entend mener une politique de développement du numérique fondée sur des principes différents de ceux qui expliquent, d'une part, la politique américaine que, sans doute à tort, on résumera par un « tout au marché » et, plus justement, par la volonté de maintenir et de développer le leadership américain et, d'autre part, la politique chinoise marquée – mais sans doute sommes-nous proches de la caricature – par un interventionnisme de l'État et d'une IA au service de l'économie, de la gouvernance sociale par l'État et de la sécurité de ce dernier au détriment des libertés individuelles des citoyens.

2 Voy. le livre Blanc (*White paper on Artificial Intelligence – A European approach to excellence and trust*, COM(2020) 65 final] 8), du 18 février 2020.

3 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, *A European strategy for data*, COM/2020/66 final: « *The European data strategy aims to make the EU a leader in a data-driven society.Creating a single market for data will allow it to flow freely within the EU and cross sectors for the benefit of businesses, researchers and public administrations. People, businesses and organisations should be empowered to make better decisions based on insights from non-personal data, which should be available to all* ».

L'Europe entend éliminer les obstacles intra-européens au déploiement de l'IA et, de manière plus générale, du numérique. L'ambition clairement affirmée est de permettre à l'Union européenne « de rivaliser avec les investissements de masse effectués par des pays tiers, notamment les *États-Unis* et la *Chine* »[4].

4. La troisième voie repose sur les deux termes mêmes du titre du Livre Blanc sur l'intelligence artificielle : d'une part, l'Excellence, qui caractérise la qualité des applications et de la recherche qui soutient leur conception et, d'autre part, la Confiance, celle nécessaire à l'acceptabilité sociale des développements novateurs du numérique, peu importe leurs domaines : éducation, santé, mobilité, conduite des affaires publiques, etc. Il s'agit tout à la fois de mettre l'homme au centre des préoccupations du développement du numérique et d'assurer pour les opérateurs un cadre solide qui permette une innovation responsable. Ainsi, « la Commission appelle de ses vœux une société européenne irriguée par des solutions numériques qui soient profondément enracinées dans nos valeurs communes et qui enrichissent la vie de chacun d'entre nous : les citoyens doivent avoir la possibilité de se développer personnellement, de poser des choix en toute liberté et en toute sécurité, de s'engager dans la société, indépendamment de leur âge, de leur sexe ou de leur parcours professionnel. Les entreprises ont besoin d'un cadre qui leur permette de démarrer, de se développer, de mettre en commun et d'utiliser des données, d'innover et d'entrer en concurrence ou de coopérer dans des conditions équitables. Et l'Europe doit avoir le choix de poursuivre la transformation numérique selon ses propres modalités »[5].

---

4 Une faiblesse cependant souvent dénoncée est le niveau des investissements européens. À cet égard, les chiffres cités par le rapport du JRC (M. Craglia (ed.), *Artificial Intelligence : A European perspective*, Luxembourg, Publications Office of the European Union, 2018, https://doi.org/10.2760/11251) : « […] États-Unis, les investissements des GAFAM (secteur privé) et des autorités publiques, de la DARPA (direction de la recherche du ministère de la Défense américain : 7,5 milliards de dollars en 2020) ; Chine, pour un volume de plus de 20 milliards ; Europe (2,5 milliards d'euros pour 2018-2020), suite à la déclaration commune des États membres, en avril 2018 relative à leur coopération en matière d'intelligence artificielle ». À noter les chiffres repris dans le Livre blanc sur l'intelligence artificielle (*op. cit.*, p. 4) : « Toutefois, le montant des investissements consacrés à la recherche et à l'innovation en Europe reste bien inférieur aux investissements publics et privés alloués à ce domaine dans d'autres régions du monde. Quelque 3,2 milliards d'euros ont été investis dans l'IA en Europe en 2016, contre environ 12,1 milliards d'euros en Amérique du Nord et 6,5 milliards d'euros en Asie ».

5 Commission européenne, *Façonner l'avenir numérique de l'Europe*, Communication de la Commission au parlement, au Conseil, au Comité économique et social européen et au Comité des régions, Luxembourg, Office des Publications de l'Union européenne, 2020. p. 2.

Cette politique particulièrement explicite à propos des systèmes IA cherche à concilier le respect des valeurs éthiques européennes sans cacher en même temps que ce respect poursuit une visée économique : c'est-à-dire la création d'un marché européen fort et souverain, en particulier par la création de labels ou certificats européens (voy. *infra*, n° 19). Comme l'a souligné M^me^ Vestager lors de la présentation de la proposition de Règlement « *AI Act* », il s'agit bien de mettre en œuvre par ce texte les principes mêmes d'excellence et de confiance : « En matière d'intelligence artificielle, la confiance n'est pas un luxe mais une nécessité absolue. En adoptant ces règles qui feront date, l'UE prend l'initiative d'élaborer de nouvelles normes mondiales qui garantiront que l'IA soit digne de confiance. En établissant les normes, nous pouvons ouvrir la voie à une technologie éthique dans le monde entier, tout en préservant la compétitivité de l'UE. À l'épreuve du temps et propices à l'innovation, nos règles s'appliqueront lorsque c'est strictement nécessaire : quand la sécurité et les droits fondamentaux des citoyens de l'Union sont en jeu ».

Le but de ce document majeur est, selon la Commissaire, quadruple :

- « veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés soient sûrs et respectent la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union ;
- garantir la sécurité juridique pour faciliter les investissements et l'innovation dans le domaine de l'IA ;
- renforcer la gouvernance et l'application effective de la législation existante en matière de droits fondamentaux et des exigences de sécurité applicables aux systèmes d'IA ;
- faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et dignes de confiance, et empêcher la fragmentation du marché ».

Cette politique ne peut être réalisée sans une parfaite cohérence des actions de tous les pays membres et suppose à la fois la rédaction de textes de plus en plus précis et nombreux mais également de mieux en mieux respectés y compris par les entreprises étrangères, qui offrent des produits ou services numériques sur le « territoire » européen. Elle tient compte de la fusion de trois mondes jusque-là clairement distingués : celui des communications électroniques, celui des médias et celui des services de l'internet.

Section 2. Les thématiques – une multiplication et un élargissement

5. Les thématiques traditionnelles se voient abordées par de nouveaux textes, soit de mise à jour, soit d'élargissement des préoccupations réglementaires. En ce qui concerne les *opérateurs et opérations des services du numérique,* la directive « signature électronique » de 1999 a fait place au Règlement eIDAS n° 910/2014 du 23 juillet 2014 qui entend établir un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques, en instaurant un cadre en matière d'identification électronique et de services de confiance. L'attention accrue à la protection des consommateurs a justifié divers textes consistant en un « *New deal for Consumers* » : la directive n° 2019/2061 du 27 novembre 2019 pour une meilleure application et modernisation des règles en matière de protection des consommateurs et celle du 25 novembre 2020 n° 2020/1828 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs.

On épinglera également la directive n° 2019/770 relative à certains aspects des contrats de fourniture de contenus ou de services numériques. Cette dernière entend harmoniser pleinement les règles régissant la conformité d'un contenu numérique ou d'un service numérique avec le contrat, les recours en cas de défaut de conformité ou de défaut de fourniture et les modalités d'exercice de ces recours, ainsi que la modification d'un contenu numérique ou d'un service numérique.

6. La question de la *protection des libertés individuelles* renvoie à l'adoption du RGPD, en lieu et place de la directive 95/47. La consécration par la Charte des droits fondamentaux de l'Union européenne, adoptée le 12 décembre 2007 permettait une approche européenne plus ferme, d'élargir les droits des personnes concernées en même temps qu'il importait d'aborder de nouvelles problématiques, en particulier le profilage.

On sait que la directive relative à la protection des données dans le secteur des communications électroniques, dite *e-Privacy*, de 2002, déjà modifiée en 2009, est en cours de révision afin d'être adaptée aux exigences de protection liées aux technologies émergentes de l'internet des objets et aux nouveaux services de communication. Par ailleurs, la question de l'accès par les autorités de polices et judiciaires aux preuves électroniques logées dans le cloud attend l'adoption de la proposition de Règlement **relatif aux injonctions européennes de production et de conservation de preuves électroniques**

en matière pénale[6]. En la matière, la proposition européenne, en forçant l'accès à des serveurs détenus par des compagnies étrangères y compris en territoire étranger, entre en conflit avec les solutions du *Cloud Act* américain de 2018, qui privilégient la loi de l'établissement de l'opérateur des services du *Cloud*, sauf conclusion d'un traité avec le pays étranger.

La *liberté d'expression* et, en particulier, ses dérives liées au contenu violent ou terroriste des messages et à la désinformation, tantôt exacerbées par la pandémie, ont fait l'objet en mai 2021 de « Lignes directrices » publiées par la Commission afin de renforcer le « *Code of Practice on disinformation* » de 2018[7] mais, également, d'une proposition de règlement, soit le « *Digital Services Act* », qui propose un cadre réglementaire pour l'offre de services en ligne[8].

La directive SMA 2018/1808 du 18 novembre 2018 détermine, « compte tenu de l'évolution des pratiques du marché », le socle minimal de règles applicables dans tous les États membres de l'UE aux services audiovisuels y compris les plateformes de produits audiovisuels et les opérateurs de services à la demande. Elle promeut la diversité culturelle et réglemente notamment la publicité, le placement de produits, la protection des mineurs, etc. et fait intervenir dans le champ de la régulation des contenus numériques d'autres autorités à savoir celles compétentes.

On note que cette directive consacre la disparition des frontières jusqu'ici tracées par la réglementation entre services audiovisuels et services numériques, tels les médias sociaux ou les services de partage de vidéos. Elle consacre le principe de transparence des opérateurs de tels services, réglemente les communications commerciales et réclame des mesures nationales appropriées pour protéger la jeunesse, ainsi que pour combattre la violence et la provocation au terrorisme.

---

6 Proposition de Règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale - Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, Bruxelles, 28 février 2019, n° 6946/19.

7 European Commission Guidance on Strengthening the Code of Practice on Disinformation (COM(2021) 262 final).

8 Le 15 décembre 2020, la Commission européenne a présenté sa proposition de règlement visant à réguler le marché unique numérique : le *Digital Service Act*. Cette proposition vise à proposer un cadre harmonisé de règles pour les services en ligne, essentiellement en matière de modération des contenus illicites et transparence du service. Cette proposition distingue les règles suivant diverses catégories d'opérateurs depuis le simple service web jusqu'aux « *very large platforms* ».

La lutte contre la désinformation a fait l'objet d'une « *Guidance for strengthtening the Code of practice on disinformation* » et d'une proposition de règlement de la Commission : le *Digital Service Act*. On ajoute que la lutte contre les messages électroniques terroristes a fait l'objet d'un règlement 2021/784 du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne.

Tous ces textes entendent « améliorer le fonctionnement du marché unique numérique en renforçant la sécurité juridique pour les fournisseurs de services d'hébergement et la confiance des utilisateurs dans l'environnement en ligne, ainsi que les garanties en matière de liberté d'expression, en ce compris la liberté de recevoir et de communiquer des informations et des idées dans une société ouverte et démocratique, et la liberté et le pluralisme des médias ». Ils proposent un contrôle des outils technologiques mis en place pour filtrer les messages à raison de leurs contenus, voire leur audit, obligeant du moins certains opérateurs à mettre en place des organes humains de modération et de médiation et en définitive la possibilité de recours à la justice.

7. Quant à la *propriété intellectuelle*, la même référence à l'évolution technologique justifie l'adoption de la directive 2019/790 sur le droit d'auteur et les droits voisins dans le marché unique numérique en date du 17 avril 2019. La directive « prévoit des règles visant à adapter certaines exceptions et limitations au droit d'auteur et aux droits voisins à l'environnement numérique et transfrontière, ainsi que des mesures destinées à faciliter certaines pratiques d'octroi de licences, notamment, mais pas seulement, en ce qui concerne la diffusion d'œuvres indisponibles dans le commerce et d'autres objets protégés, et la disponibilité en ligne d'œuvres audiovisuelles sur les plateformes de vidéo à la demande, en vue d'assurer un accès plus large aux contenus. Elle contient également des règles destinées à faciliter l'utilisation de contenus qui sont dans le domaine public. Afin de réaliser un marché performant et équitable pour le droit d'auteur, il devrait également exister des règles sur les droits dans les publications, sur l'utilisation des œuvres ou autres objets protégés par les prestataires de services en ligne qui stockent et donnent accès à des contenus téléversés par leurs utilisateurs, sur la transparence des contrats d'auteurs et d'artistes interprètes ou exécutants, et sur la rémunération de ces auteurs et artistes interprètes ou exécutants, de même qu'il devrait exister un mécanisme de révocation des droits que les auteurs et artistes interprètes ou exécutants ont transférés sur une base exclusive ».

8. Au-delà de cette intervention sur des domaines traditionnels, l'Union européenne s'est penchée sur les infrastructures de communication, la

technologie elle-même ou certains de ses produits. En ce qui concerne les infrastructures, à propos de la technologie, la cybersécurité est devenue un enjeu majeur de la politique européenne. Elle fait l'objet d'un Règlement 2019//881 du 17 avril 2019 « relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications »[9]. En ce qui concerne les produits, sans être complet, notons que la voiture intelligente fait l'objet de textes réglementaires.

Ensuite, à la directive sur les dispositifs médicaux a succédé le Règlement 2017/745, que la jurisprudence de la Cour de justice étend désormais aux logiciels de télémédecine et aux applications IA dans le domaine de la santé. Enfin, les technologies de l'IA, applicables en bien des domaines, font l'objet d'une proposition de Règlement de la Commission dite « *AI Act* »[10]. Cette proposition entend encadrer le développement des applications de l'intelligence artificielle, en particulier en distinguant diverses catégories sur base d'une analyse des risques liés à ces applications. Pour les applications dites à haut risque, elle entend instituer à la fois une gouvernance interne et une procédure d'évaluation des risques sur le modèle du Règlement sur les dispositifs médicaux y compris l'évaluation externe par une autorité de supervision, la tenue d'un registre et l'obtention de certificats européens de conformité. À propos des robots qui souvent intègrent des systèmes d'IA, la Commission propose, le même jour que sa proposition relative à l'IA, le remplacement de la directive « Machines » de 2006 par un nouveau **règlement sur les machines et équipements**[11] (robots, imprimantes 3D, tondeuses à gazon…). Ce nouveau règlement sera plus apte à assurer une intégration sûre des systèmes d'IA tout en réduisant les charges administratives et les coûts grâce à des procédures simplifiées.

9. On ajoutera que les textes relatifs à l'IA renvoient à d'autres qui répondent à la stratégie européenne de création d'un marché européen de la donnée et, à la fois, augurent de la possibilité de mise sur pied de « *big data* » européennes, capables de nourrir des systèmes d'IA. Dans le cadre de cette politique de circulation et de partage intensifié de données, la Commission a pris diverses initiatives.

9 On ajoutera le document relatif à la sécurité des réseaux 5G et celui relatif aux voitures connectées.

10 Proposition de Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle et modifiant certains actes législatifs de l'Union COM(2021), Bruxelles, 21 avril 2021, 206 final {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final.

11 Bruxelles, 21 avril 2021, COM(2021 202 final.

La principale est certes la proposition de règlement sur la gouvernance européenne des données (*Data Governance Act*) présentée le 25 novembre 2020[12], qui encourage, grâce à la création de services réglementés dits de partage des données, la mutualisation des données non seulement entre entreprises mais également entre secteurs privé et public, voire entre particuliers et secteur public, en ce qui concerne les « *data for public good* » et ce, dans le cadre d'un « *data altruism* ».

En ce qui concerne le secteur public, l'Europe promeut l'exploitation la plus large possible des données du secteur public par le secteur privé. En la matière, à peine séchée l'encre de la directive « *Open Data* »[13] de 2019, renforçant déjà sensiblement les obligations de mise à disposition des informations détenues par le secteur public, la proposition de règlement sur la gouvernance des données du 25 novembre 2020[14] élargit ces obligations sur un point, à savoir la réutilisation des données protégées et jusque-là exclues de tout accès.

10. Enfin, il faut noter une attention particulière de l'Union européenne à l'encadrement réglementaire de certains opérateurs, en particulier les *very large plateforms* désormais qualifiées de « *gatekeepers* » de la société de l'information. À ce titre, celles-ci génèrent par les systèmes de recommandations et de profilage, des risques dits « systémiques », selon la qualification du projet de DSA, c'est-à-dire qu'elles ont des impacts, outre ceux sur nos libertés individuelles, sur le fonctionnement démocratique de notre société et sur la justice sociale. La part de marché occupée par ces entreprises et leur stratégie de diversification des activités déstructurent profondément le fonctionnement concurrentiel du marché et oblige l'Union européenne à intervenir. C'est l'objet à la fois du Règlement du 20 juin 2019 « promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne »[15] et, plus récemment, de la proposition par

12 Proposition de Règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), Bruxelles, le 25 novembre 2020, COM(2020) 767 final 2020/0340(COD).

13 Voy. directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, *JOUE*, L172, 20 juin 2019, disponible en ligne sur : https://op.europa.eu/en/publication-detail/-/publication/a6ef4c41-97eb-11e9-9369-01aa75ed71a1/language-fr/format-PDFA2A. La proposition a été adoptée moyennant quelques modifications mineures par la Commission de l'industrie, de la recherche et de l'énergie, le 16 juillet 2021.

14 COM(2020) 767 final.

15 Ce règlement oblige les services d'intermédiation en ligne à une plus grande transparence et à une équité dans leurs relations contractuelles avec les entreprises utilisatrices de leurs services et, en particulier, leur *ranking*.

la Commission du *Digital Market Act* qui introduit une réglementation asymétrique des opérateurs des services de l'information[16].

Par ailleurs, on souligne que le Code des communications électroniques depuis sa révision de 2018[17] inclut désormais les fournisseurs de services dits OTT (over-the top communication services), les fournisseurs de services de messagerie instantanée, courriels, appels téléphoniques sur Internet et messages personnels émis par le biais de réseaux sociaux, dans la définition des opérateurs de communications électroniques. Ceux-ci sont donc soumis aux mêmes obligations que les opérateurs « classiques », notamment en matière d'interopérabilité, d'information et de protection des utilisateurs finals, de sécurité publique et de défense nationale voire de financement du service universel, ainsi qu'à des règles spécifiques de protection de la vie privée[18].

Les technologies avancées amènent en effet une fusion des marchés autrefois distincts des opérateurs classiques de communication électronique, d'une part et des plateformes de communication comme *WhatsApp*, d'autre part. Comme le note le considérant n° 7 de la directive, la convergence des secteurs des télécommunications, des médias et des technologies de l'information implique que tous les réseaux et services de communications électroniques devraient être soumis dans la mesure du possible à un même code des communications électroniques européen établi au moyen d'une directive unique.

Section 3. Vers des modes originaux de régulation

11. Que tirer de cette efflorescence de textes européens ? En quoi marquent-ils une évolution des modes de régulation de l'Union européenne ? Plusieurs remarques à cet égard : la première constate la

16 Proposition de Règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), Bruxelles 15 décembre 2020, COM(2020) 842 final. Le *Digital Markets Act* instaure un nouveau modèle de régulation fondé sur un système d'obligations graduées, dit « asymétrique », qui cible de façon adéquate les plus grands acteurs.

17 Directive (UE) 2018/1972 du 11 décembre 2018. Cette directive remplace cinq directives.

18 « *The definition of electronic communications services should therefore contain three types of services which may partly overlap, that is to say internet access services as defined in point (2) of Article 2 of Regulation (EU) 2015/2120 of the European Parliament and of the Council, interpersonal communications services as defined in this Directive, and services consisting wholly or mainly in the conveyance of signals*. » (Considérant n° 15). L'extension de la directive e-Privacy de 2009 à l'ensemble de ces OTT (soit over-the-top communications services) est un des points délicats en discussion lors des négociations en cours relatives à la révision de la directive *e-Privacy* en un nouveau règlement.

multiplication des règlements, là où l'Europe se contentait jusqu'à il y a peu de directives. L'exemple du passage de la directive de 1995 en matière de protection des données qui laissait, selon les termes mêmes de ses considérants, une marge de manœuvre aux États membres, a fait place à un règlement qui impose non seulement des règles communes mais, crée les organes du maintien, voire de l'amplification de cette cohérence.

Sans doute, conserve-t-on au niveau national (autorités de protection des données et de contrôle de l'audiovisuel, organes de surveillance en matière d'IA…) des relais dont les pouvoirs d'enquête et de sanction se voient renforcés mais ces autorités nationales sont forcées de travailler en étroite coopération avec, voire se trouvent contrôlées par, des instances européennes dites de coordination.

Nombre de textes créent ainsi des agences ou des autorités européennes en charge d'assurer la cohérence des actions des autorités nationales et de veiller à une interprétation et application uniformes des textes. Ces autorités s'expriment par voie de « Lignes directrices », de recommandations, d'avis, de rapports et conseillent la Commission dans son œuvre réglementaire. Sans être exhaustif, citons : l'EDPB en matière de protection des données, l'ENISA, en matière de cybersécurité, le Groupe de coordination en matière de dispositifs médicaux, le Comité européen de l'intelligence artificielle, le Groupe des régulateurs européens pour les services de médias audiovisuels (ERGA), le BEREC (Body of European Regulators for Electronic Communications) ou en français, l'ORECE, qui fournit un appui administratif et professionnel à la Commission européenne[19].

Avec le même souci et de manière à accroître encore l'effectivité des textes réglementaires et assurer leur adaptation rapide aux besoins de

19 « *BEREC aims at fostering the independent, consistent and high-quality regulation of digital markets for the benefit of Europe and its citizens* » (BEREC strategy 2021-2025). La directive (EU) 2018/1972 du 11 décembre 2018 confère un nombre significatif de nouvelles tâches au BEREC « *such as issuing guidelines on several topics, reporting on technical matters, keeping registers, lists or databases and delivering opinions on internal market procedures for draft national measures on market regulation. Overall, the EECC aims to create an internal market for electronic communications within the EU while ensuring a high level of investment, innovation and consumer protection through enhanced competition* ». Les autorités nationales de régulation et la Commission doivent tenir compte au maximum des recommandations, des lignes directrices et des bonnes pratiques adoptées par le BEREC (Considérant n° 21 de la directive sur les services de communications électroniques). Le BEREC s'emploie à garantir que la législation européenne est appliquée de manière uniforme, afin de permettre à l'UE de disposer d'un marché unique des communications électroniques efficace. Il fournit des conseils, sur demande et de sa propre initiative, aux institutions européennes. Il est constitué d'un conseil des régulateurs. Il s'agit d'un organe composé des directeurs (ou de représentants de haut niveau) de chaque autorité de régulation nationale.

l'évolution technologique, les textes confient en outre des pouvoirs à la Commission, soit pour assurer le suivi de l'application des réglementations sous forme notamment de rapports, soit pour prendre des actes délégués en application du texte du règlement. Ainsi, pour reprendre l'exemple du *AI Act* : revoir le champ d'application du Règlement IA, compléter la liste des systèmes à haut risque, etc.

À noter que lorsque la Commission est directement en charge de l'exécution des dispositions d'une compétence européenne (comme, en matière de concurrence, le DMA), la Commission, assistée certes par un Comité consultatif des marchés numériques reprenant des représentants des différents pays membres, peut imposer directement des mesures contraignantes aux entreprises.

12. La **prolifération d'autorités administratives** créées par tous ces textes récents soulève des difficultés lorsqu'il s'agit d'analyser de manière transversale l'impact d'une technologie ou de se prononcer à l'occasion d'un litige qui met en cause les diverses thématiques envisagées séparément dans le cadre réglementaire et par des organes dont la culture et les prérogatives sont différentes. Pour ne prendre que l'exemple[20] de l'utilisation, par les plateformes numériques, de systèmes de recommandations et de profilage des internautes, il s'agit bien là d'un problème touchant à la protection des données, à la liberté d'expression et à la régulation des médias, à la concurrence et à la protection des consommateurs.

Cette nécessité d'une approche transversale ne peut, à notre avis, être rencontrée que par une clarification du rôle et des compétences de chaque catégorie d'autorités administratives mais, surtout, par la création institutionnalisée de lieux de dialogue entre ces différents organes, sans quoi on risque des interventions dans des sens contradictoires, voire une rivalité croissante entre instances.

On relèvera, à l'occasion de la désignation des organes nationaux de supervision proposés en matière d'IA, la revendication des autorités de protection des données d'assurer cette compétence, alors même que les enjeux de protection des données ne constituent qu'une partie des risques à envisager lors de l'évaluation des systèmes d'IA. Sans doute une des premières initiatives de réglementation transversale d'une technologie. Exemple à suivre ?

Enfin, on souligne que la **convergence entre des secteurs autrefois distincts** comme les mondes des télécommunications, de l'audiovisuel

20 Autre exemple, la réglementation des voitures connectées touche à des questions du choix de l'infrastructure (5G ou WiFi), de protection des données, d'interopérabilité, de normes de sécurité.

et des services du commerce électronique oblige désormais, en particulier les plateformes en ligne, à jongler avec des régulations issues de cultures différentes, qui trouvent en ce qui les concerne à s'appliquer de manière cumulative et, on l'espère, cohérente.

13. La volonté de l'Europe d'atteindre ses objectifs explique le « tout au réglementaire » et sa défiance vis-à-vis d'une autorégulation difficilement contrôlable et surtout apanage des puissants. Cette attitude n'est pas en contradiction avec des formes de **corégulation** que dans de précédents textes nous qualifions de descendante, c'est-à-dire que les mécanismes privés de régulations sont certes promus mais sévèrement encadrés par une réglementation qui en fixe les balises, voire contrôlés par les autorités administratives indépendantes mises en place ou par la Commission elle-même[21].

Cette tendance se retrouve dans de nombreux textes et, parfois, de manière explicite, comme dans ces considérants (n° 12 et 14, traduit par l'article 4*bis*) de la directive « services audiovisuels » : « Les États membres devraient, dans le respect de leurs différentes traditions juridiques, reconnaître le rôle que peut jouer une autorégulation efficace en tant que complément aux mécanismes législatifs, judiciaires et administratifs existants, ainsi que l'utilité de sa contribution à la réalisation des objectifs de la directive 2010/13/UE. Toutefois, si l'autorégulation peut constituer une méthode complémentaire pour la mise en œuvre de certaines dispositions de la directive 2010/13/UE, elle ne devrait pas pouvoir se substituer aux obligations qui incombent au législateur national. La corégulation, dans sa forme la plus simple, assure un lien juridique entre l'autorégulation et le législateur national, dans le respect des traditions juridiques des États membres. Dans la corégulation, le rôle de régulateur est partagé entre les parties prenantes et les pouvoirs publics ou les autorités ou organismes de régulation nationaux. Le rôle des autorités publiques compétentes comprend la reconnaissance du dispositif de corégulation, l'audit de ses procédures et son financement. La possibilité d'une intervention de l'État devrait exister, dans le cadre de la corégulation, lorsque les objectifs du système ne sont pas atteints… ». Elle est illustrée par la façon dont, en matière de désinformation, après avoir accepté en 2018 une autorégulation par les acteurs majeurs du marché, outre le lancement de la proposition du DSA déjà étudiée, la Commission publiait le 26 mai 2021 – le titre

21 Pour un exposé plus complet des relations entre la réglementation européenne, l'autorégulation et la « *lex informatica* », voy. Y. Poullet, « Vues de Bruxelles. Modes alternatifs de régulation et libertés dans la société du numérique », in C. Castets-Renard, V. Ndior et L. Rass-Masson (dir.), *Enjeux internationaux des activités numériques*, Bruxelles, Larcier, 2020, pp. 91-137.

est évocateur – les « lignes directrices pour renforcer le Code de conduite relatif à la désinformation »[22].

Sans être complet, on citera, dans le même sens, les articles 40 et s. du RGPD qui, tout en reconnaissant diverses méthodes de régulation privée (les codes de conduite, les labels, les certificats), leur fixent des conditions minimales et prévoient leurs approbations par les APD[23]. L'*AI Act* permet une autorégulation mais uniquement pour les applications IA à faible risque. On note que les autorités européennes insistent sur une participation *multistakeholders* à la rédaction des instruments d'autorégulation[24].

On ajoute que ce même souci de mettre la régulation privée en accord avec les exigences de la réglementation s'exprime également par rapport à un autre mode de régulation : la technologie dont le fonctionnement impose ce que nombre d'auteurs ont appelé la *lex informatica* ou *electronica*. Il importe que dès la conception, le *design* des outils technologiques et de leurs applications soit conforme à la règle de droit. Nombre de textes européens réclament des concepteurs ou utilisateurs cette conformité: ainsi, pour ne reprendre que quelques exemples, le RGPD met en avant le principe du « *privacy by design* » (art. 25) ; la directive 2019/790 sur le droit d'auteur insiste pour que les systèmes de contrôle utilisés pour lutter contre les copies illicites respectent les exceptions légales au droit d'auteur (art. 17(7)) ; la proposition DSA (art. 28) exige la vérification des systèmes de recommandation et nous reviendrons amplement sur la proposition d'*AI Act* qui, au-delà du « *privacy by design* » du RGPD, prône un « *ethical values by design* »[25].

14. Une autre caractéristique semble poindre dans les textes les plus récents de l'Union européenne, à savoir une **réglementation**

22 « *The Guidance aims at evolving the existing Code of Practice towards a co-regulatory instrument foreseen under the Digital Services Act (DSA), offering an early opportunity to design appropriate measures to address systemic risks related to disinformation stemming from the functioning and use made of the platforms' services in view of the anticipated DSA risk assessment and mitigation framework* ».

23 Sur ce point, la politique suivie par les APD, « *Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement (UE) 2016/679* », 4 juin 2019.

24 Parmi de nombreux exemples, on citera l'injonction reprise p. 2 des « Guidance for strengthening the code of Practice on disinformation » : « *Online platforms and all other players of the online advertising ecosystem should thus take responsibility and work together to defund disinformation* » (voy., part., la création par les *Guidances de l'European Digital Media Observatory*, qui inclut des chercheurs, des représentants des « *fast-checkers* » et autres « *relevant stakeholders* »).

25 Au-delà du respect de la loi, on citera la déclaration de mai 2019 de la Commission européenne qui fait suite aux recommandations du groupe d'experts « *AI applications should not only be consistent with the Law but also adhere to ethical principles* ».

asymétrique tantôt des acteurs, tantôt des applications opérées, ou produits ou services offerts par ceux-ci et ce, en fonction des risques (*risk-based approach*) liés à ces applications, produits ou services. Dans les deux cas, l'asymétrie réglementaire se justifie par le principe de proportionnalité, affirmé par l'article 5(4) du Traité sur l'Union européenne qui dispose que celle-ci ne doit pas, dans l'exercice de ses compétences, faire plus que ce qui est nécessaire pour atteindre ses objectifs. Détaillons ces deux points.

15. Certains textes réglementaires européens imposent à des catégories d'acteurs des obligations plus lourdes. À d'autres, ils accordent le bénéfice d'exceptions de manière à faciliter leur développement. Le deuxième chapitre (*supra,* n° 10) pointait déjà certaines dispositions imposées aux plateformes de communication et d'information, ainsi le traitement égalitaire et transparent des utilisateurs professionnels par ces intermédiaires nécessaires. De même, le DSA assujettit les « *very large platforms* » (c'est-à-dire celles ayant une clientèle égale ou supérieure à 10 % de la population européenne) à des obligations en matière de contrôle des contenus et d'audit des systèmes de recommandations. En matière de protection des données, le RGPD l'impose aux autorités publiques, mais aussi aux entreprises traitant des données sensibles ou une large partie de la population.

À l'autre bout, on note la volonté, de manière à garantir l'innovation, de protéger les organismes de recherche et les start-up voire les PME. Ainsi, l'article 3 de la directive de 2019 sur le droit d'auteur prévoit pour les organismes de recherche scientifique le droit exceptionnel d'effectuer des fouilles de données, nonobstant le droit d'auteur ou les droits sui generis des titulaires de droit. On retrouve le même souci dans les textes relatifs à l'accès aux données publiques et au partage des données. De même, l'*AI Act* prévoit en son article 55 la possibilité de mesures nationales « en faveur des petits fournisseurs et utilisateurs ».

On sait que le Règlement européen de 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne se justifie pleinement par cette volonté de protection des PME[26] et que les services d'intermédiation envisagés dans le cadre de la

26 « Les services d'intermédiation en ligne peuvent être déterminants pour le succès commercial des entreprises qui y font appel pour entrer en contact avec les consommateurs. Pour tirer pleinement parti de l'économie des plateformes en ligne, il importe donc que les entreprises puissent se fier aux services d'intermédiation en ligne avec lesquels elles nouent une relation commerciale. Cela a son importance, principalement parce que l'intermédiation croissante des transactions par le biais de services d'intermédiation en ligne, conséquence d'importants effets de réseau indirects fondés sur les données, conduit à une dépendance accrue de ces entreprises utilisatrices, en particulier des micro-, petites et moyennes entreprises (ci-après dénommées « PME »), à l'égard de ces services pour entrer en contact avec les consommateurs » (Considérant n° 2).

proposition du *Governance Data Act* ont pour mission d'assister en particulier les PME afin de les faire bénéficier des avantages liés au partage des données.

Enfin, l'article 17(6) de la directive de 2019 sur le droit d'auteur exonère de certaines obligations de vigilance les « nouveaux fournisseurs de services de partage de contenus en ligne dont les services ont été mis à la disposition du public dans l'Union depuis moins de trois ans et qui ont un chiffre d'affaires annuel inférieur à 10 millions d'euros calculés conformément à la recommandation 2003/361/CE de la Commission (qui définit les PME) »[27].

16. L'approche par les risques conduit à créer des obligations nouvelles lorsque certains critères proposés par la réglementation indiquent que des risques supérieurs sont présents. Cette approche est déjà pratiquée mais, de manière très limitée, dans les dispositions du RGPD : l'article 35 réserve l'obligation d'analyse d'impact aux seuls traitements présentant un « risque élevé » pour les droits et libertés des personnes physiques. La notion de « risque élevé » reste imprécise. Le règlement sur les dispositifs médicaux distingue de même différentes classes de produits et services selon la finalité de leur utilisation et les risques liés à la santé et à la sécurité et soumet les classes de produits à « haut risque » à des procédures d'évaluation de la conformité aux exigences de la régulation.

La même idée parcourt *l'AI ACT*. La proposition énonce l'interdiction de pratiques illégales de l'intelligence artificielle[28] (art. 5) ; elle met en place un système de contrôle et de gestion des systèmes d'IA à hauts risques (art. 6.2) listés dans une annexe susceptible de modification par la Commission ; elle soumet à des obligations spécifiques pour défaut de transparence certaines applications cachées « en particulier lorsque des dialogueurs ou des trucages vidéo ultra-réalistes sont utilisés » et, enfin, abandonne à l'autoréglementation du marché les autres applications présentant un risque minime. *L'AI Act* ou plutôt les travaux du *High Level*

27 À noter à l'alinéa 2 du même article, l'adjonction d'un second critère nuançant l'application du premier : « Lorsque le nombre moyen de visiteurs uniques par mois de tels fournisseurs de services dépasse les 5 millions, calculé sur la base de l'année civile précédente, ils sont également tenus de démontrer qu'ils ont fourni leurs meilleurs efforts pour éviter d'autres téléversements des œuvres et autres objets protégés faisant l'objet de la notification pour lesquels les titulaires de droits ont fourni les informations pertinentes et nécessaires ».

28 Ainsi, les systèmes de manipulation par messages subliminaux, l'exploitation des vulnérabilités, l'utilisation par le secteur public de systèmes de « *social ranking* » entraînant de potentielles discriminations entre personnes ou groupes, de systèmes biométriques fonctionnant en temps réel et à distance, placés dans des endroits publics (par exemple, des systèmes de reconnaissance faciale).

Group of experts on AI sur l'éthique de l'IA[29], auxquels se réfère constamment cette proposition, élargit les risques à prendre en considération lors de l'évaluation des applications de l'IA. Ainsi, à côté des risques encourus par nos libertés individuelles, s'ajoute la nécessité de prendre en considération les risques dits collectifs propres à un groupe déterminé ou non de personnes, les risques d'atteinte à la justice sociale et, au-delà, les risques sociétaux, comme ceux encourus par l'environnement, la démocratie, le respect de l'État de droit. Cet élargissement trouve un écho dans la définition de « risques systémiques » liés au fonctionnement des systèmes de notation et de recommandation et à leur utilisation par les « *very large platforms* »[30]. On sait que les premiers travaux sur la responsabilité des systèmes d'IA[31] retiennent la même idée de différencier les responsabilités des « producteurs » ou utilisateurs professionnels de système d'IA selon la gravité des dommages que l'utilisation des systèmes peut causer.

17. L'approche par les risques induit une autre conséquence : elle justifie pleinement le passage d'une rédaction légale classique – fondée sur la définition de contenus comportementaux à respecter et, en cas de non-respect, sur la répression ou la sanction *a posteriori* des infractions à la réglementation – à une **approche *a priori* fondée sur l'obligation d'évaluation des risques,** soit la mise sur pied d'une procédure en la matière et du contrôle du respect de cette procédure. L'approche préventive fondée sur les risques semble être une caractéristique des textes réglementaires européens récents. L'exemple déjà cité du « *Privacy Impact*

29 HLGE (*High Level Group of experts*) on AI, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, 8 avril 2019, n° 67, texte disponible sur le site : Ethics guidelines for trustworthy AI – Publications Office of the EU (europa.eu).

30 Le considérant n° 57 du DSA décrit ces fameux risques. Le premier concerne l'ampleur de la diffusion de contenus illicites permis par les plateformes en ligne occupant une place importante sur le marché. Le deuxième concerne « l'incidence du service sur l'exercice des droits fondamentaux, tels que protégés par la Charte des droits fondamentaux, y compris la liberté d'expression et d'information, le droit à la vie privée, le droit à la non-discrimination et les droits de l'enfant. De tels risques peuvent découler, par exemple, de la conception des systèmes algorithmiques utilisés par la très grande plateforme en ligne ou de l'usage abusif de ses services par la soumission de notifications abusives ou d'autres méthodes visant à empêcher la liberté d'expression ou à entraver la concurrence ». Le troisième risque vise l'utilisation des mécanismes mis en place par la plateforme, comme le système de recommandations, afin de manipuler autrui lors d'élections, diffuser des messages intentionnellement erronés qui mettent en danger la santé publique, la démocratie, etc.

31 Rapport du groupe d'experts sur la responsabilité et les nouvelles technologies, section « nouvelles technologies », du 21 novembre 2019 et sur la responsabilité en matière d'intelligence artificielle et d'autres technologies numériques émergentes : *Liability for Artificial Intelligence and other emerging digital technologies*. La Commission européenne semble vouloir reprendre les idées de cette proposition de règlement à travers une modification profonde de la directive de 1985 sur la responsabilité du fait des produits défectueux.

Assessment », introduit par le RGPD, déplace ainsi le champ d'intervention de la réglementation vers une démarche préventive d'écartement des risques par la nécessité de mise sur pied d'une procédure d'évaluation dès la conception du traitement. La même idée traverse les autres règlements cités au paragraphe précédent. En particulier, la proposition *d'AI Act* développe à loisir cette procédure, définissant ses étapes, son contenu, insistant sur la participation de tous les acteurs intéressés, etc. On louera cette manière de faire, certes plus lourde administrativement et qui ne peut être justifiée que dans les cas de risques importants.

18. Le chapitre 1 soulignait in fine le souci de l'Union de veiller à **l'effectivité de la réglementation**, c'est-à-dire à garantir son respect. Les paragraphes précédents ont déjà illustré la façon dont l'Union entendait répondre à ce souci notamment par la mise au pas de l'autorégulation, par la traduction par la technologie des prescrits réglementaires, par le rôle des autorités administratives, sans omettre la surveillance régulière par la Commission européenne. Un point doit être ajouté : l'imposition de mécanismes de *compliance* interne. Le RGPD impose (art. 37 et s.) l'obligation pour certaines entreprises de nommer un délégué à la protection des données, jouissant d'un statut lui assurant une certaine protection et disposant de nombreuses compétences et missions afin de veiller au respect du RGPD. D'autres textes ont, depuis, rejoint cette idée. Ainsi, la proposition dite DSA oblige, d'une part, les plateformes à instituer des systèmes internes de traitement des réclamations, chargées de veiller à la légalité des décisions prises automatiquement ou non par la plateforme et, d'autre part, les très larges plateformes à désigner un ou plusieurs responsables de la conformité au Règlement[32]. L'article 15 du Règlement de 2017 sur les dispositifs médicaux prévoit que « les fabricants disposent au sein de leur organisation d'au moins une personne chargée de veiller au respect de la réglementation possédant l'expertise requise dans le domaine des dispositifs médicaux ».

19. Enfin, on évoquera la détermination européenne **à exercer pleinement sa souveraineté** dans l'espace numérique. Cette souveraineté implique, d'une part, l'extension des règles européennes à des entreprises situées hors Europe mais également, d'autre part, la présence sur le marché européen de produits ou services conformes à ces réglementations. Première facette de cette souveraineté, c'est-à-dire de la « maîtrise de notre

32 Article 32.2 : « Les très grandes plateformes en ligne désignent uniquement comme responsables de la conformité des personnes qui disposent des qualifications professionnelles, des connaissances, de l'expérience et des aptitudes nécessaires pour mener à bien les tâches visées au paragraphe… ».

destin sur les réseaux informatiques »[33], la confiance et les valeurs de l'Union européenne, que traduisent les textes réglementaires, ne peuvent être garanties et respectées que dans la mesure où, dans un marché numérique global, les services et produits recourant à l'intelligence artificielle et déployés sur le territoire européen sont effectivement conformes aux requis des règlements européens. C'est, sur base de ce postulat, que notamment le RGPD (art. 3) et le règlement proposé en matière d'IA ou en matière de services numériques n'hésitent pas à étendre leur champ d'application à des entreprises situées en dehors de l'Union européenne lorsque le traitement, l'application IA ou le service numérique vise une clientèle située dans l'Union européenne ou lorsque l'application ou le produit sont destinés au marché ou à des résidents européens[34]. Cet élargissement du champ d'application *ratione loci* des textes européens traduit bien la volonté européenne d'utiliser l'outil réglementaire pour garantir la protection des personnes résidentes en Europe et, dès lors, leur confiance en l'outil de l'IA qui y est développé ou utilisé. Au-delà, il s'agit d'une tentative d'exporter le modèle réglementaire européen, dans la mesure où la pénétration dans l'espace européen par des entreprises sises hors Europe les oblige à obéir aux règles qui y prévalent et les invite à se prévaloir de la valeur ajoutée de ces règles vis-à-vis de l'ensemble de leurs marchés. La même idée de souveraineté se traduit dans le projet d'« *e-evidence Act* », qui autorise les autorités policières et judiciaires à exiger d'entreprises

33 Sur la souveraineté numérique, lire entre autres, l'excellente contribution de A. T. Norodom, « Être ou ne pas être souverain, en droit, à l'ère numérique », in C. Castets-Renard, V. Ndior et L. Rass-Masson (dir.), *Enjeux internationaux des activités numériques*, op. cit., pp. 21 et s.

34 L'argument est noté dans nombre de règlements et de propositions de règlements, tels le RGPD, les propositions relatives à l'IA, le DSA… Parmi tous ces textes, citons simplement : « Les services d'intermédiation en ligne et les moteurs de recherche ayant une dimension mondiale, le présent règlement devrait s'appliquer aux fournisseurs de tels services, qu'ils soient établis dans un État membre ou en dehors de l'Union, pour autant que deux conditions cumulatives soient remplies. La première est que les entreprises utilisatrices ou les utilisateurs de sites internet d'entreprise devraient être établis dans l'Union. La seconde est que les entreprises utilisatrices ou les utilisateurs de sites internet d'entreprise devraient proposer, grâce à la fourniture de ces services, leurs biens ou services à des consommateurs situés dans l'Union au moins pour une partie de la transaction. Afin de déterminer si des entreprises utilisatrices ou des utilisateurs de sites internet d'entreprise proposent des biens ou services à des consommateurs situés dans l'Union, il est nécessaire de déterminer s'il est patent que les entreprises utilisatrices ou les utilisateurs de sites internet d'entreprise orientent leurs activités vers des consommateurs situés dans un ou plusieurs États membres » (Exposé des motifs, pt 9 du Règlement du Parlement européen et du Conseil promouvant l'équité et la transparence pour les entreprises utilisatrices des services d'intermédiation en ligne, adopté le 14 juin 2019 (*JOUE*, L186, 11 juillet 2019, pp. 57-79).

sises hors Europe des données conservées au-delà du territoire européen lorsqu'il s'agit de lutter contre certaines infractions graves.

20. L'exigence de souveraineté suppose également, seconde facette de la souveraineté de l'Union sur l'espace numérique, la **promotion de produits ou de services conformes aux exigences européennes**. Indirectement, la mesure entend favoriser le développement d'une industrie des produits et services du numérique. Nombre de textes mettent ainsi en place des certificats européens qui permettent, aux entreprises qui les utilisent, d'être présumées satisfaire aux requis réglementaires et, aux citoyens, de disposer d'un label de qualité rassurant. Le RGPD prévoit cette possibilité dans le contexte de la corégulation. Un *EU Trust Mark* est mis en place pour les opérateurs de service de confiance de certification, dans le cadre du Règlement eIDAS. Le Règlement en matière de cybersécurité de 2019 met en place un système de certification volontaire auprès de l'ENISA des produits, services ou procédures relatifs à leur sécurité dans le cadre de schémas de certification adoptés par la Commission[35]. Les règlements sur les dispositifs médicaux et sur l'IA représentent une avancée en la matière dans la mesure où, y compris pour les importateurs étrangers, elles prescrivent, du moins pour les systèmes ou dispositifs présentant un risque supérieur, cette obligation de se faire certifier en interne voire, exceptionnellement, par un organisme de notification agréé, organisent le contrôle de la qualité de la certification par un organisme de supervision et, enfin, organisent un registre européen de tels certificats. On le conçoit, ces systèmes de certification constituent un enjeu majeur pour la création d'un marché européen de produits et services conformes aux exigences réglementaires et la promotion d'acteurs européens sur ce marché, avec l'espoir que ces certificats puissent être également une plus-value sur les marchés à l'exportation.

35 Voy. les articles 46 et s. du Règlement du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications. Article 46 : « 1 Le cadre européen de certification de cybersécurité est établi afin d'améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l'Union et en permettant de disposer, au niveau de l'Union, d'une approche harmonisée en ce qui concerne les schémas européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les produits TIC, services TIC et processus TIC. 2. Le cadre européen de certification de cybersécurité prévoit un mécanisme visant à établir des schémas européens de certification de cybersécurité et à attester que les produits TIC, services TIC et processus TIC qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services qui sont offerts par ces produits, services et processus ou accessibles par leur intermédiaire tout au long de leur cycle de vie ».

Section 4. Conclusion

21. Cher Denis, nombre de tes écrits mettent en avant cette omniprésence de la réglementation européenne. Les quelques réflexions qui précèdent témoignent de la vérité de ton point de vue. L'effacement des frontières due à la création d'un espace universel du numérique ne signifie pas le laissez-passer dont rêvent les superpuissances du Net. L'Union européenne entend non réinstaller les barrières ou du moins les filtres dont certaines puissances comme la Chine ou la Russie entourent leurs espaces nationaux mais au moins soumettre l'impact sur la vie des citoyens et notre société européenne des citoyens européens à un certain nombre de précautions qui, nous l'avons vu, vont bien au-delà du seul souci de la protection des données et des libertés individuelles pour s'étendre à la protection de nos sociétés démocratiques européennes et des valeurs de justice sociale. Au nom de ces valeurs, elle affirme, voire impose – certains diront de manière impérialiste – ses choix réglementaires. Ce faisant, l'Union européenne quitte la culture défensive qui a souvent été la sienne ; elle met une sourdine elle met une sourdine au principe de subsidiarité et refuse la profusion de textes nationaux dont l'impact eut été insuffisant pour combattre les dangers d'un espace qui sans cela aurait obéi à la loi du plus fort ou du pays « le moins disant ». Le pari de l'« excellence et de la confiance » ne peut être réussi qu'ensemble. L'Union adopte des textes sans doute loin des approches traditionnelles ; multiplie les courroies qui, entre la loi et la pratique, assurent le respect de la première ; force certaines cultures, celle de la propriété en encourageant le partage des données, celle d'une administration jalouse de ses secrets et de ses données, celle propre aux autorités administratives jalouses de leurs compétences traditionnelles et de leurs prérogatives.

La réglementation de l'Union de notre société du numérique ouvre de vastes chantiers pour nous juristes et, sans doute, de nouvelles manières de faire. Je sais que sur ces nouveaux chantiers, j'aurai le plaisir de te retrouver, mon cher Denis, et je m'en réjouis.