Vers un droit européen de l'intelligence artificielle

Poullet, Yves

Published in:
Journal de droit européen

Publication date:
2021

Document Version
le PDF de l'éditeur

Analyse

Vers un droit européen de l'intelligence artificielle

Yves Poullet(*)

- **L'intelligence artificielle est censée révolutionner nos économies, nos administrations, nos vies voire notre identité. Elle mobilise nos entreprises ; elle est source d'attentes mais également de craintes de la part des citoyens**
- **L'Union européenne entend encourager son développement tout en rassurant ses citoyens**
- **C'est avec cette double volonté qu'elle a entamé, en particulier depuis l'arrivée de la nouvelle Commission en 2018, des chantiers réglementaires tous azimuts dont nous souhaitons dégager les lignes de force**

Introduction

1. — De l'intelligence artificielle (IA) et des « big data ». — L'IA est sans doute la technologie la plus disruptive que notre société ait produite. La proposition de la Commission européenne de règlement sur l'IA, du 21 avril 2021[1], la définit, en son article 3 (1), comme « un logiciel qui est développé au moyen d'une ou plusieurs des techniques et approches énumérées à l'annexe I et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit ». On note une grande prudence dans la définition de la notion, qui renvoie à une annexe dont le contenu est susceptible d'évolution à travers les modifications que pourra y apporter la Commission. Cette définition renvoie à une pluralité de méthodes et de techniques et souligne l'importance du degré d'autonomie qui sera confié au fonctionnement de la technologie. L'annexe distingue, à cet égard, sous le concept d'IA, les trois types de méthodes suivantes : « (a) approches d'apprentissage automatique, y compris d'apprentissage supervisé, non supervisé et par renforcement, utilisant une grande variété de méthodes, y compris l'apprentissage profond ; (b) approches fondées sur la logique et les connaissances, y compris la représentation des connaissances, la programmation inductive (logique), les bases de connaissances, les moteurs d'inférence et de déduction, le raisonnement (symbolique) et les systèmes experts ; (c) approches statistiques, estimation bayésienne, méthodes de recherche et d'optimisation ».

Cette approche large permet d'inclure dans l'objet de la réflexion les systèmes experts qualifiés d'IA symbolique qui sont pratiqués, par exemple, pour le calcul d'une taxation ou une décision d'octroi de permis de bâtir. Ces systèmes reposent sur la traduction en algorithmes d'un raisonnement logique humain — celui des experts (sous la forme d'un raisonnement causal de forme « si... alors ») — et ne soulèvent pas les mêmes problèmes que ceux posés par l'utilisation des méthodes de *machine learning*. Ces dernières méthodes sont fondées sur les corrélations statistiques entre données, ces corrélations étant, par ailleurs, susceptibles d'évoluer au fur et à mesure des données rentrées. Le système expert est transparent, du moins au regard de celui qui le programme, ce qui est loin d'être le cas du système de *machine learning*, au fonctionnement opaque, du moins en partie[2]. Ces systèmes d'IA dits avancés ou « aggrégationnels » s'appuient sur la conjugaison de données de plus en plus nombreuses, collectées de diverses manières, notamment grâce aux technologies de l'« internet dit des objets »[3] ou par le partage de données entre entreprises et/ou administrations, comme nous l'évoquerons plus loin. Ces « mégadonnées » constituent une condition de l'utilisation d'algorithmes puissants fonctionnant en réseaux de neurones, ce qu'il est coutume d'appeler l'IA dont la discipline de *machine learning* permet à des systèmes d'apprendre par eux-mêmes, en établissant des corrélations entre les données les plus diverses rassemblées au sein des « mégadonnées » et se nourrissant sans cesse des nouvelles données reçues.

2. — Des applications multiples de l'IA et des robots. — De multiples applications de l'IA émergent, certaines sont déjà présentes. Ainsi, certaines applications permettent d'appuyer l'action des entreprises ou des administrations dans divers domaines, dans leurs relations avec les entreprise ou les administrés (par exemple via les *chatbots* ou l'accès à une base de données intelligente en matière d'analyse de réglementation), dans la préparation de leurs décisions voire dans leurs décisions tant au niveau macro (fixation de la stratégie de l'entreprise, décisions d'implantation), qu'au niveau micro pour les décisions individuelles (dans le secteur privé : octroi d'un crédit ou souscription d'une assurance, envoi d'un message publicitaire ciblé en temps réel (*real time bidding*) ; pour le secteur public : octroi d'une aide à une entreprise, détection de suspects...) ou pour des décisions relatives à elle-même (par exemple : engagement de personnel[4] et ce grâce à l'analyse de données collectées à des sources diverses et

(*) 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. Le texte est à jour au 15 septembre 2021. Il n'a pu tenir compte des discussions relatives aux propositions de règlement commentées dans l'article, menées au sein des enceintes du Parlement européen et du Conseil. **(1)** 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, {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}, 21 avril 2021, COM(2021) 206 final, disponible en ligne sur https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN (consulté le 26 mai 2021), en abrégé « Artificial intelligence Act ». **(2)** Sur ces distinctions et l'histoire de l'IA, lire Y. Meneceur, *L'intelligence artificielle en procès*, Bruxelles, Bruylant, 2020, pp. 10 et s. **(3)** En particulier, grâce à ce qu'il est convenu d'appeler « l'Internet des Objets » ou « l'intelligence ambiante ». Une étude récemment publiée prévoit que toute personne « normalement connectée » devrait interagir, en 2025, avec des appareils ou objets connectés toutes les dix-huit secondes, c'est-à-dire 4 800 fois par jour (D. Reinsel, J. Gantz et J. Rydning, *Data Age 2025 : The Evolution of Data to Life-Critical*, avril 2017). **(4)** À cet égard, le système d'IA mis en place par le gouvernement pour le recrutement de son personnel a été jugé anticonstitutionnel (non-conformité aux règles de la protection des données) par la Cour constitutionnelle.

Analyse

en nombre quasi infini ; enfin, d'autres autorisent un meilleur fonctionnement de leur propre gestion (par le support de l'IA à l'automation de tâches et à la facilitation de procédures administratives (par exemple, suivi de dossiers) ou de leur production (lorsqu'il s'agit de gérer des flux d'information en temps réel). On ajoutera que les systèmes d'IA peuvent être « embarqués » dans des machines physiques et, ainsi, simples exemples, aider aux soins de personnes (robots aide-soignant), répondre à la commande vocale de leurs propriétaires (enceintes connectées), remplacer des soldats personnes physiques (voy. les soldats dits autonomes) ou conduire une voiture (véhicules intelligents). Certains robots peuvent prendre des formes humaines (ainsi, le robot Sophia, ambassadrice de charme du Royaume d'Arabie saoudite[5]).

3. — Le fil rouge. — Le droit européen de l'IA est en construction. Les premières bases en sont jetées. La volonté européenne de créer un droit spécifique de l'IA s'explique par la volonté, en particulier de la Commission actuelle, de développer une « troisième voie » de développement du numérique, distincte de celles des deux pôles concurrents : la Chine et les États-Unis. Une troisième voie, que la Commission entend fonder sur l'« Excellence et la Confiance », selon le titre même du Livre blanc de février 2020. Ce sera la première considération du présent article. Une politique de l'IA ne peut se concevoir que si elle est articulée à une stratégie qui favorise la création de mégadonnées ou *big data*, comme nous venons de l'expliquer. En la matière, une politique volontariste est d'autant plus nécessaire que l'Europe ne dispose pas de champion de l'Internet, qu'on songe aux GAFAM américaines ou aux BATX chinoises et qu'il est donc important de favoriser le partage de données tant entre public et privé qu'entre entreprises privées. Un deuxième volet analysera la politique européenne vis-à-vis de ce *new oil* que constitue la donnée. Le troisième volet développe les premiers pas européens dans sa réglementation de l'IA et des robots, en particulier les propositions de règlements d'avril 2021. Ces premiers pas s'inspirent partiellement des travaux de la Commission relatifs à l'éthique de l'IA. Ils laissent dans l'ombre l'articulation de ce texte avec le RGPD et surtout renvoient à des textes complémentaires à venir en matière de responsabilité et de droits d'auteur.

1 La « troisième voie » européenne - Entre les « modèles » chinois et américain

4. — De la déclaration d'Ursula van der Leyen à la proposition de règlement sur l'IA. — La volonté exprimée à de nombreuses reprises par les autorités européennes est de fonder le développement des outils et des applications d'IA sur deux valeurs : « Excellence and Trust », selon le titre même du Livre blanc sur l'IA (*White Paper on AI)* de février 2020, document à la base de cette politique qui marque la troisième voie européenne. Lors de l'annonce du « Livre blanc » de l'Union européenne en matière d'IA, la présidente de la Commission soulignait : « Nous voulons que l'application de ces nouvelles technologies soit digne de la confiance de nos citoyens [...] Nous encourageons une approche responsable de l'intelligence artificielle centrée sur l'humain ». L'excellence s'appuie sur le développement d'une recherche scientifique de pointe que l'Union entend financer à côté des financements de chaque état européen. La confiance dans les applications de la technologie de l'intelligence artificielle doit permettre l'acceptation sociale de celles-ci. Cette acceptation est nécessaire pour assurer le développement des applications de l'IA.

5. — L'ambition européenne. — Sans doute, cette troisième voie était-elle préparée par la précédente Commission et le Parlement d'alors[6], mais elle est désormais clairement affirmée par la nouvelle Commission[7] et sa présidente. L'option européenne constitue une stratégie explicitement énoncée et progressivement mise en œuvre à travers des textes qui se suivent à un rythme accéléré. Il s'agit bien d'une troisième voie dans la mesure où l'Union entend mener une politique de développement de l'IA fondée sur des principes différents de ceux qui fondent, d'une part, la politique américaine qu'on résumera par un « tout au marché » ou, plus justement, par la volonté de maintenir et de développer le *leadership* américain[8] et, d'autre part, la politique chinoise marquée — mais sans doute sommes-nous proches de la caricature — par un interventionnisme de l'État et une IA au service de l'économie, de la gouvernance sociale par l'État et de la sécurité de ce dernier (voy., en particulier et de manière emblématique, les applications sécuritaires de reconnaissance faciale)[9].

En appelant à la mise en place d'un marché unique européen de l'IA[10], notamment grâce au principe de reconnaissance mutuelle qui autorise l'utilisation transfrontière des produits intelligents,

(5) « Sophia, activée le 19 avril 2015 à Hong-Kong, en Chine, est une gynoïde saoudienne. Elle a été conçue pour tout apprendre en s'habituant au comportement des êtres humains. Sophia est également capable de répondre aux questions et a été reçue en entrevue à maintes reprises. En octobre 2017, elle obtient la nationalité saoudienne, faisant d'elle le premier andro-gynoïde au monde à recevoir la citoyenneté d'un État. Elle est considérée comme l'un des robots les plus intelligents du monde » (Wikipedia, *v°* Sophia [robot]). **(6)** *Cfr* en particulier la résolution du 12 février 2019 sur une politique industrielle globale sur l'intelligence artificielle et la robotique (dite Résolution Ashley-Fox). **(7)** Le Livre blanc (*White paper on Artificial Intelligence - A European approach to excellence and trust*, [COM(2020) 65 final] 8), de février 2020 exprime cette stratégie. **(8)** À noter, que l'Executive Order 13859 on Maintaining Leadership in Artificial Intelligence, 11 février 2019 (décret présidentiel) adopté par le président Trump qui marque le lancement de l'*American AI Initiative*, la nouvelle stratégie américaine en matière d'intelligence artificielle, donne comme objectif premier à cette dernière le maintien du *leadership* scientifique, technologique, et économique américain en matière de recherche et développement dans le domaine de l'IA. Ce *leadership* passe cependant par une politique de formation des personnes et la promotion de la confiance du public par notamment la protection des libertés civiles, la vie privée et les valeurs américaines. Le récent rapport du National Select Committee on AI publié le 1er mars 2021 et soumis au président des États-Unis et au Congrès pour adoption maintient la même position (https://www.nscai.gov/wp-content/uploads/2021/03/Final_Report_Executive_Summary.pdf). **(9)** Sur la stratégie chinoise en matière d'intelligence artificielle, Jeffrey Ding, *Deciphering China's AI dream*. Centre for Governance of AI, Future of Humanity Institute, University of Oxford, Oxford, accessible à l'adresse suivante : https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf. Elsa B Kania, *China's embrace of AI : Enthusiasm and challenges*, European Council on Foreign Relations (Nov. 6, 2018), https://ecfreu/article/commentary_chinas_embrace_of_ai_enthusiasm_and_challenges/. **(10)** C'était le thème essentiel du Plan cordonné sur l'IA de 2018. Sur cette coordination européenne, lire la « Declaration of Cooperation on Artificial Intelligence », signée par tous les États membres et la Norvège, le 10 avril 2018 (Le texte de la déclaration est accessible sur le site : https://ec.europa.eu/digital-single-market/en/events/digital-day-2018).

Analyse

l'Europe entend éliminer les obstacles intra-européens au déploiement de l'IA. Au-delà, l'ambition clairement affirmée est de permettre à l'Union « de rivaliser avec les investissements de masse effectués par les tiers, notamment les États-Unis et la Chine »[11]. On citera quelques éléments de cette politique économique ambitieuse en faveur du développement des applications de l'IA et de leur utilisation. L'annexe à la Communication : « Fostering a European Approach to Artificial Intelligence », qui contient la mise à jour du plan coordonné de 2018, a été récemment publiée par la Commission le 21 avril 2021[12]. Le plan 2021 note l'objectif de l'Union d'atteindre progressivement un investissement public et privé de 20 milliards par an au cours de la décade 2020-2030 et plaide énergiquement pour une meilleure synergie des instruments de financement au niveau national et européen entre des fonds de pure recherche et des fonds de coopération entre l'industrie et la recherche.

2 Une politique européenne réglementaire en faveur de la constitution de *big data*

6. — Un premier pas - La libre circulation des données à caractère non personnel. — Un premier axe de la politique européenne en faveur de l'IA est de souligner la valeur économique de la donnée. La reconnaissance de la donnée comme un *new oil*[13] commande, en effet, une politique de libre circulation des données. En ce qui concerne le premier point, le règlement (UE) 2018/1807 du Parlement européen et du Conseil, du 14 novembre 2018, complète le cadre applicable au libre flux des données dans l'Union[14] et institue un cinquième principe de libre circulation, celui portant sur les données, qu'elles soient personnelles[15] ou non personnelles. Son objectif principal tient à la stimulation du marché intérieur numérique et à la volonté d'exploiter plus efficacement les potentiels des techniques numériques en réduisant les possibilités pour les États membres d'instaurer ou de maintenir des obligations liées à la localisation des données ainsi qu'en mettant en œuvre un principe d'accès et de portage des données. Le texte de 2018 prône, en particulier, la disponibilité des données et le portage des données pour les utilisateurs professionnels. Pour ce faire, il promeut l'élaboration de codes de conduite par autorégulation[16].

7. — Le partage des données - Une préoccupation essentielle de l'Europe. — Par ailleurs, le partage de données constitue un prérequis absolu pour la création, en Europe, du moins faute de GAFAM ou de BATX, de mégadonnées (ou *Big data)* proprement européennes, condition d'une émergence d'applications IA utilisant des méthodes de *machine learning*. Cette politique d'encouragement au partage des données au sein et au-delà des secteurs[17] y compris entre le public et le privé s'explique certes par l'absence dans l'Union de champions du *big data* que sont les plateformes privées américaines (les GAFAM) et chinoises (les BATX) et donc la nécessité de constituer ces *big data* européennes[18] à partir des lieux de collecte privés ou publics, en créant des mécanismes vertueux de solidarité. Cette politique facilite le développement d'applications d'IA ; elle se justifie, en outre, par son importance tant pour l'économie, pour la société que pour les citoyens[19].

8. — Les initiatives européennes. — Dans le cadre de cette politique de partage intensifié de données, la Commission a pris diverses initiatives. La principale est certes la proposition de règlement sur la gouvernance européenne des données (*Data Governance Act*). Présentée le 25 novembre 2020[20], elle mérite en particulier notre attention. Comme le note l'exposé des motifs : « L'instrument vise à favoriser la disponibilité de données en vue de leur utilisation, en augmentant la confiance dans les intermédiaires de données et en renforçant les mécanismes de partage de données dans l'ensemble de l'UE ». Quatre objectifs sont visés : « la mise à disposition de données du secteur public en vue d'une réutilisation, lorsque de telles données sont soumises à des droits d'autrui ; le partage de données entre entreprises, contre rémunération sous quelque forme que ce soit ; permettre l'utilisation de données à caractère personnel avec l'aide d'un "intermédiaire de partage de données à caractère personnel », conçu pour aider les personnes physiques à exercer leurs droits au titre du règlement général sur la protection des données (RGPD) ; permettre l'utilisation de données pour des motifs altruistes ».

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

(11) Une faiblesse cependant souvent dénoncée est le niveau des investissements européens. À cet égard, les chiffres cités par le rapport du JRC (Craglia, M. (éd.), *Artificial Intelligence – A European perspective* (2018), Publications Office of the European Union, https://doi.org/10.2760/11251). Aux États-Unis, les investissements des GAFAM (secteur privé) : plus ou moins 14 milliards et des autorités publiques en particulier de la DARPA (direction de la recherche du ministère de la Défense américain) : 7,5 milliards de dollars en 2020 ; en Chine, pour un volume de plus de 20 milliards ; en Europe, ; budget de la recherche et des investissements européens au niveau des seules administrations européennes : 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, également, 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. Quelques 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 » (12) Annex to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence, Brussels, 21.4.2021 COM(2021) 205 final, ANNEX, p. 3. (13) *Cfr* le très intéressant document de l'EPRS : *Is data the new oil ? Competition issues in the digital economy*, PE 646.117 – January 2020, disponible sur le site : https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf. (14) Règlement (UE) 2018/1807, cité note précédente. (15) Il est fait ici référence au RGPD, qui dans un cadre réglementaire protecteur de nos libertés assure la libre circulation des données à caractère personnel. (16) *Cfr* article 6 du règlement (UE) 2018/1807. (17) Ainsi, la Commission encouragera la création de neufs espaces sectoriels communs de données (industrie manufacturière, environnement, mobilité, santé, finances, énergie, agriculture, administration publique, compétences) et intersectoriels. (18) On pourrait s'interroger, au passage, sur l'absence jusqu'ici d'initiatives de l'Union européenne pour stimuler l'émergence d'acteurs du *big data* en Europe, notamment les opérateurs de télécoms qui s'étaient, dans un premier temps, intéressés à ce business — BT, Colt Telecom... — avant de le délaisser. (19) Voy. à cet égard, les développements par la Commission européenne : Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, *Une stratégie européenne pour les données*, Bruxelles, le 19 février 2020, COM(2020) 66 final. (20) 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).

« Open Data »[21] de 2019, qui renforçait 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[22] élargit ces obligations encore sur un point, à savoir ouvrir la réutilisation des données protégées et jusque-là exclues de tout accès. En effet, les données à caractère personnel ou protégés par des droits de propriété intellectuelle étaient jusqu'ici exclues par les directives *PSI* de toute possibilité d'accès et d'exploitation.

Autre versant de la politique européenne vis-à-vis du secteur public, les autorités publiques doivent développer, en interne cette fois, l'utilisation d'outils d'IA au service de l'intérêt général et des citoyens[23]. Ainsi, l'Europe se distingue par une politique qui entend combiner les deux rôles des services publics : pourvoyeurs de données vis-à-vis du secteur privé à travers les directives dites d'« Open Data » ou « Public Sector Information » (en abrégé *PSI*)[24] mais également récepteurs de données cette fois en provenance du privé de manière à nourrir les bases de données informationnelles qui lui permettront de mettre au point de meilleurs services au bénéfice de l'intérêt général. On ajoute que la proposition permet également à des personnes privées, en spécifiant les finalités de ce transfert (exemple : aide des politiques de santé, de l'environnement, de la mobilité, etc.), de mettre à disposition des administrations leurs données. La Commission qualifie d'« altruiste », ce transfert par des particuliers. Afin de sécuriser ces transferts (ne serait-ce que pour assurer la protection des données à caractère personnel), la Commission prévoit l'intervention d'organisations également qualifiées d'altruistes[25], que nous décrirons au paragraphe suivant. L'objectif de ces dispositions reconnaissant l'altruisme des données (« Data for Public Good ») est clairement de permettre au secteur public de disposer de données en nombre suffisant pour lancer des initiatives d'utilisation de l'IA au bénéfice de l'intérêt général[26].

Enfin, en ce qui concerne le secteur privé, la Commission encourage le partage des données au niveau sectoriel comme intersectoriel[27], non seulement en envisageant de mettre sur pied des accords type, pour régler en particulier les questions de propriété intellectuelle, de protection des données, de concurrence et de responsabilité. L'effectivité du règlement proposé reposera sur la création d'un nouveau métier d'intermédiation, contrôlé par des instances nationales : les services de partage des données. Ces prestataires de services de partage de données devront jouer un rôle clé dans l'économie fondée sur les données. Ils facilitent l'agrégation et l'échange de quantités substantielles de données pertinentes[28]. Ces « intermédiaires de données » proposeront, en effet, des services mettant en relation les différents acteurs — les uns, fournisseurs de données, les autres, preneurs de celles-ci — et contribueront à la mise en commun efficace des données ainsi qu'à la facilitation de leur partage. En ce qui concerne le partage des données à caractère personnel, en particulier, ils seront chargés de veiller au respect des dispositions du règlement général de protection des données et assisteront, le cas échéant, les personnes concernées dans l'exercice de leurs droits. Ces intermédiaires de données seront indépendants et neutres, à la fois par rapport aux détenteurs de données et aux utilisateurs de ces données, et leur statut facilitera, on peut l'espérer, l'« émergence de nouveaux écosystèmes fondés sur les données qui soient indépendants de tout acteur jouissant d'une puissance significative sur le marché ». Dernière initiative attendue : alors que l'utilisation du *cloud* par nos entreprises reste à la traîne, le lancement d'un *cloud* européen, garantissant aux utilisateurs la non-surveillance de masse par les autorités policières ou de renseignement, est à noter[29].

3 Pour un cadre réglementaire spécifique à l'IA

9. — Le point de départ - Les risques de l'IA et la réponse « éthique ». — Le Livre blanc de la Commission (voy. *supra* n° 1)

(21) Voy. la 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, *J.O.U.E.* L 172 du 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. **(22)** COM(2020) 767 final. **(23)** Voy., en particulier, le texte : Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions : *EU eGovernment Action Plan 2016-2020 Accelerating the digital transformation of government* (COM(2016) 179 final), 19 avril 2016, disponible en ligne sur https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation (consulté le 26 mai 2021). Voy. aussi la Communication « Artificial Intelligence for Europe » du 25 avril 2018 : « A strategy on AI for Europe » (repris par le Conseil en juin 2018), texte disponible à l'adresse: eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:237:FIN. **(24)** Voy. la 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, *J.O.U.E.* L 172 du 20 juin 2019, disponible en ligne sur https://op.europa.eu/en/publication-detail/-/publication/a6ef4c41-97eb-11e9-9369-01aa75ed71a1/language-fr/format-PDFA2A (consulté le 26 mai 2021). **(25)** Les « organisations altruistes en matière de données reconnues dans l'Union » devraient, selon des exigences dont le respect sera vérifié par l'autorité nationale *ad hoc*, être en mesure de collecter des données pertinentes directement auprès de personnes physiques et morales ou de traiter les données collectées par d'autres et ce moyennant le consentement des personnes concernées. Par organisation altruiste, on entend des entités publiques ou privées servant des fins d'intérêt général « comme les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, l'établissement plus aisé de statistiques officielles ou l'amélioration de la prestation de services publics. Le soutien à la recherche scientifique, et notamment au développement technologique et à la démonstration, à la recherche fondamentale, à la recherche appliquée et à la recherche financée par des fonds privés, devrait également être considéré comme une finalité d'intérêt général ». **(26)** « Le présent règlement vise à contribuer à l'émergence de réserves de données mises à disposition selon le principe de l'altruisme en matière de données, qui soient d'une taille suffisante pour permettre l'analyse des données et l'apprentissage automatique » (Exposé des motifs, n° 35). **(27)** « Sharing and use of privately-held data by other companies (business-to-business - B2B - data-sharing). In spite of the economic potential, data sharing between companies has not taken off at sufficient scale. This is due to a lack of economic incentives (including the fear of losing a competitive edge), lack of trust between economic operators that the data will be used in line with contractual agreements, imbalances in negotiating power, the fear of misappropriation of the data by third parties, and a lack of legal clarity on who can do what with the data (for example for co-created data, in particular IoT data) », 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. **(28)** Ces intermédiaires peuvent ainsi veiller à adapter les données, les enrichir, les convertir à un format standard et interopérable, etc. **(29)** Voy. à ce sujet, les réflexions de la Commission sur le besoin d'une réponse au *Cloud Act* américain, 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. Le « Clarifying Lawful Overseas Use of Data Act », ou « Cloud Act », a été adopté par le Congrès américain le 23 mars 2018. Cette loi autorise, à certaines conditions, le gouvernement américain et ses services spécialisés à accéder à des données à caractère personnel stockées à l'étranger.

Analyse

relatif à l'IA met en évidence que l'acceptabilité sociale de cette technologie, en particulier lorsqu'elle s'appuie sur des systèmes de *machine learning*, nécessite la confiance. Or celle-ci est loin d'être acquise lorsque l'on connaît l'opacité et l'autonomie du fonctionnement des systèmes, en particulier de *deep learning*, lorsque l'on constate les nombreux biais conscients mais surtout inconscients qui peuvent affecter ces systèmes et surtout lorsque l'on attribue à ces systèmes, au motif qu'ils fonctionnent de manière objective et que *data do not lie*, une capacité de prédiction et une compétence de décision. Ces enjeux et risques liés aux applications de l'IA ne concernent pas uniquement les libertés individuelles[30], en particulier la protection des données à caractère personnel. Ils s'étendent à des groupes de personnes : le ciblage négatif des habitants d'un quartier en termes de capacités de crédit ou la détection de caractéristiques de santé communes à des profils génétiques visent, au-delà de leur application à des individus particuliers, des groupes de personnes. Enfin, ces risques peuvent viser la société entière, le fonctionnement des institutions démocratiques, notamment, en accroissant le rôle de certains acteurs privés, disposant d'une meilleure information que les pouvoirs publics, en faussant le jeu des élections comme l'a illustré le cas « Cambridge Analytica », en privant le pouvoir judiciaire de sa compétence par une justice prédictive qui se passe volontiers du jugement humain, etc. Parmi ces risques sociétaux, on ajoute ceux d'atteinte à la justice sociale voire à la protection de l'environnement, lorsque l'on se réfère à la consommation d'énergie que nécessité l'alimentation (IoT et Big Data) et l'utilisation des systèmes d'IA. Cette dimension collective et sociétaire a été soulignée par les divers textes des organisations internationales relatifs à l'éthique de l'IA[31]. Il est ainsi recommandé de mettre en place des règles éthiques intégrant l'idée que l'IA doit être une « technologie centrée sur l'humain », conçue comme un outil qui aide l'humain et qui est contrôlé par lui. On ajoute que le cadre éthique de référence devrait être élaboré dans le respect des droits fondamentaux tels que la dignité, l'autonomie, l'autodétermination, la justice sociale, le respect de l'environnement et d'une démocratie fondée sur l'État de droit. Il implique la responsabilité sociétale de tous les acteurs qui concourent au développement des outils d'IA.

C'est dans ce courant « éthique » que le Livre blanc[32] situe son appel à une technologie « digne de confiance ». Il s'appuie en particulier sur les travaux d'un groupe d'experts de haut niveau (*HLGE on AI*) commandité par la Commission. Ces travaux avaient abouti, en avril 2019, à des recommandations éthiques pour un système d'IA digne de confiance[33] et plus récemment à la publication d'une liste reprenant les critères d'évaluation des sept caractéristiques d'un AI digne de confiance (ALTAI ou *Assessment List for Trustworthy AI*)[34]. À cette impulsion éthique de la Commission et en pleine concertation avec cette dernière, le Parlement européen a entendu répondre par une résolution du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes[35]. On souligne que le texte constituait plus qu'une simple résolution, il contenait, en effet, une proposition de règlement, bref un « prêt-à-signer » pour la Commission et le Conseil. Le texte de la proposition de règlement mis sur la table par la Commission ce 21 avril 2021 nous apparaît plus pragmatique et moins généreux que le texte parlementaire, dans la mesure où il se centre volontiers sur les questions posées par l'IA à nos libertés individuelles, en prêtant moins d'attention aux risques collectifs et de société que pose l'IA[36]. Par ailleurs, le texte de la Commission se montre soucieux des enjeux économiques et d'innovation que représente le développement des applications des méthodes d'IA.

10. — La proposition de règlement du 21 avril 2021. — Le 21 avril 2021, la Commission publiait sa proposition de règlement « instaurant des règles harmonisées en matière d'intelligence artificielle », en abrégé l'« Artificial Intelligence Act »[37]. Il s'agit bien, affirmait Mme Vestager lors de la présentation de la proposition, 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

(30) La liberté d'expression peut être mise en danger par l'utilisation, en particulier par les plateformes d'information et les réseaux sociaux, de systèmes de recommandation ou de filtrage utilisant l'intelligence artificielle pour repérer certains types de messages et en empêcher parfois illégitimement la diffusion ; la liberté de déplacement peut demain être mise en danger par le contrôle des déplacements liés à l'utilisation de systèmes d'intelligence artificielle dans les voitures autonomes ; le profilage peut amener à exclure certaines personnes pour leurs opinions politiques, religieuses ou. **(31)** En particulier, l'UNESCO (projet de Recommandation sur l'éthique de l'intelligence artificielle en date du 25 juin 2021 proposé à l'AG de novembre) et le Conseil de l'Europe (*Ad Hoc HLGE, Council of Europe, Feasibility study on a legal framework for the creation, development and application of AI based on Council of Europe standards, Dec. 17, 2020*). Un projet de Convention du Conseil de l'Europe sur l'éthique de l'IA est attendu pour la fin de cette année. **(32)** Cette dimension sociétale est encore rappelée par la Communication de la Commission révisant le plan stratégique de développement de l'intelligence artificielle. On note qu'elle est associée avec l'enjeu économique de *leadership* européen sur le marché de cette technologie (« Fostering a European Approach to Artificial Intelligence », EU Commission Communication, 21 avril 2021). **(33)** HLGE (High Level Group of experts on AI). Sur ce groupe et ses travaux, https ://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence) et notamment sa publication des Lignes directrices en matière d'éthique pour une IA digne de confiance (publiés le 8 avril 2019), texte disponible sur le site : Ethics guidelines for trustworthy AI - Publications Office of the EU (europa.eu) - https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. **(34)** Les sept critères dégagés par les *guidelines* sont respectivement : Human Agency and Oversight ; Technical Robustness and Safety ; Privacy and Data Governance ; Transparency ; Diversity, Non-discrimination and Fairness ; Societal and Environmental Well-being ; Accountability. Sur les méthodes d'évaluation et les critères à prendre en compte, voir le site de présentation d'Altai (Assessment List fot Trustworthy AI) : https://futurium.ec.europa.eu/en/european-ai-alliance/pages/altai-assessment-list-trustworthy-artificial-intelligence. **(35)** Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes (2020/2012(INL)) P9 TA (2020) 0275. Cette résolution s'accompagnait de deux autres résolutions, l'une sur la responsabilité des acteurs de l'IA et l'autre sur les questions de droit d'auteur. Nous reviendrons sur ces deux résolutions (*infra*, n° XX) **(36)** Voy. nos remarques sur la nécessité d'élargir aux risques sociétaires et collectifs, l'évaluation des applications de l'intelligence artificielle, Y. Poullet, « Cinq ans après : le RGPD et les défis du profilage à l'heure de l'intelligence artificielle », *Rev. des affaires européennes*, n° spécial : le RGPD, cinq ans après, (sous la direction de C. Castets, 2021/1, pp. 90 et s.). Sur l'analyse de ces trois risques, l'article de A. Mantelero, « Regulating Big Data. The Guidelines of the Council of Europe in the context of the European Data Protection Framework », *CL&SR*, 2019, p. 584. **(37)** Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle, précitée. Pour une critique développée de la proposition, lire l'excellent rapport de N. Smuha, E. Ahmed-Rengers, A. Herkens *e.a.*, « How the EU can achieve Legally Trustworthy AI : A response to the European Commission's proposal for an Artificial intelligence Act », *University of Birmingham Leads Lab report*, disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991.

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 du texte est quadruple : « 1. ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values ; 2. ensure legal certainty to facilitate investment and innovation in AI ; 3. enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems ; 4. facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation ».

La Commission s'explique longuement sur le choix de l'approche réglementaire, elle écarte une approche basée sur l'autorégulation, jugée dangereuse au vu des risques présentés par certains systèmes, et celle sectorielle, là où l'Europe entend mener une politique intersectorielle ; elle ne retient pas non plus l'option réglementaire qui viserait tous les systèmes IA, au vu de l'exigence de proportionnalité de l'intervention réglementaire européenne et adopte donc un instrument normatif directement obligatoire fondé sur une approche basée sur les risques propres à certains systèmes d'IA, laissant les autres systèmes gouvernés par l'autoréglementation. Cet ensemble de règles harmonisées concernant la conception, le développement et l'utilisation de certains systèmes d'IA n'entend pas se substituer mais au contraire s'ajouter, de manière cohérente, à toute une série de réglementations européennes, qu'il s'agisse de textes en matière de protection des consommateurs, de protection des données à caractère personnel, de non-discrimination ou d'égalité des genres.

11. — L'approche basée sur les risques et les conséquences réglementaires envisagées. — La proposition de règlement cherche à établir un compromis entre les exigences légales et éthiques, traduisant les valeurs de l'Union et la nécessité de ne pas contraindre de manière exagérée le développement et l'initiative technologiques voire de la promouvoir[38]. Pour ce faire, le texte adopte une approche réglementaire strictement proportionnée et évolutive. Elle énonce l'interdiction de pratiques illégales de l'IA[39] (article 5) ; elle met en place un système de contrôle et de gestion des systèmes d'IA à haut risque (article 6.2) listées de manière très partielle dans une annexe susceptible de modification par la Commission ; elle soumet à des obligations spécifiques de transparence pour 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.

En ce qui concerne la première catégorie, celle des risques inacceptables « en raison de leur caractère contraire aux valeurs de l'Union européenne », l'article 5 les liste parfois avec un manque de précision et surtout sans souci de l'évolutivité nécessaire de cette liste. Sans les citer tous, on relève les interdictions suivantes :

— « les systèmes d'IA qui exploitent les éventuelles vulnérabilités dues à l'âge ou au handicap physique ou mental d'un groupe de personnes donné[40] pour altérer substantiellement le comportement d'un membre de ce groupe d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers » ;

— « l'utilisation par les pouvoirs publics[41] ou pour leur compte, de systèmes d'IA destinés à évaluer ou à établir un classement de la fiabilité de personnes physiques au cours d'une période donnée en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues ou prédites », dans la mesure où ce *scoring* conduit à un traitement préjudiciable injustifié ou sur la base de données utilisées de manière incompatible avec les finalités de la collecte et du traitement originaire[42] ;

— enfin, « l'utilisation de systèmes d'identification biométrique (en clair les systèmes de reconnaissance faciale) à distance "en temps réel » dans des espaces accessibles au public à des fins répressives[43], sauf si et dans la mesure où cette utilisation est strictement nécessaire[44]... » et a fait l'objet d'une autorisation judiciaire ou administrative par une autorité compétente. Selon l'opinion de l'EDPB (*European Data Protection Board*) et de l'EDPS (*European Data Protection Supervisor*), cette liste aurait dû être élargie à tous les systèmes d'évaluation sociale et à nombre de traitements de données biométriques[45].

Les articles 52 et s. soumettent à des obligations particulières de transparence certains systèmes AI (article 52), ainsi l'obligation d'informer les personnes interagissant avec un système d'IA de la présence d'un robot comme interlocuteur. Même obligation d'information des personnes concernées en cas d'utilisation de systèmes de reconnaissance d'émotions ou de profilage sur la base de données biométriques ou de manipulation d'images, de sons ou de vidéos relatives à des personnes (*deepfakes)*.

(38) Les articles 53 et s. prévoient diverses mesures de soutien à l'innovation, en particulier le développement de certains outils d'IA dans le cadre de « bacs à sable » réglementaires. **(39)** 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...). **(40)** À noter que l'interdiction vise ici un risque collectif propre à un groupe de personnes. Par ailleurs, on s'interroge sur la raison de limiter l'interdiction aux seules IA exploitant les handicaps physiques et mentaux et de subordonner l'interdiction à la nécessité d'un dommage physique ou psychologique prévisible, l'interdiction proposée. Ne peut-on considérer que certains *nudges* exploitant la vulnérabilité de certains groupes en dehors de ceux cités ne devraient pas être également considérés ? À cet égard, le projet de recommandation CM/Rec(2021)... du Comité des ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage du Comité consultatif de la Convention n° 108, article 1.j.) : L'expression « traitements de profilage à risque élevé » peut notamment désigner ... : ii. le profilage qui en raison du public visé, du contexte, de la finalité du traitement en particulier dans une situation de déséquilibre dans le pouvoir d'information, comporte un risque d'affecter ou d'influencer indûment des personnes concernées notamment lorsqu'il s'agit de mineurs ou de personnes vulnérables. **(41)** ... et non par les pouvoirs privés, ainsi une banque qui évaluerait le potentiel de crédit des clients. Notons que nombre de systèmes privés de *social rating* seront considérés comme des systèmes à haut risque (voy. *infra*). **(42)** On retrouve là des principes du RGPD : non utilisation à des fins illégitimes ou incompatibles. **(43)** Les pouvoirs privés peuvent-ils utiliser de tels systèmes ? Il eût été bon que le texte exclut l'utilisation par les pouvoirs privés de tels systèmes dans des « lieux publics ». En ce qui concerne leur utilisation par des pouvoirs privés dans des lieux accessibles au public (par exemple, un parking de grande surface ou un magasin), s'agit-il (*infra*) d'un système à haut risque ou faut-il l'interdire ? **(44)** La suite renvoie aux causes de finalités légitimes acceptées traditionnellement sur base de la directive « Police ». À cet égard, il est intéressant de noter que la détection, la localisation, l'identification ou les poursuites à l'encontre de l'auteur ou du suspect ne sont possibles via ces systèmes de reconnaissance faciale en temps réel dans des lieux accessibles au public que pour des infractions punies par une peine ou une privation de libertés d'au moins trois ans. Dans de tels cas d'admissibilité, le point 3 de l'article 5 demande que l'on tienne compte de certains critères. **(45)** EDPB/EDPS, Joint opinion (/2021 on the proposal for a regulation laying down harmonized rules on Artificial intelligence, 18 juin 2021).

Analyse

Ensuite, dernière catégorie réglementée, elle est vaste. En effet, l'article 6.1, de manière sibylline, ouvre la boîte de Pandore, lorsqu'il renvoie à une vaste liste de réglementations, ainsi en matière d'aviation, de dispositifs médicaux, de véhicules, de finances... soit lorsque « le système d'IA est destiné à être utilisé comme composant de sécurité d'un produit couvert par les actes législatifs d'harmonisation de l'Union énumérés à l'annexe II, ou constitue lui-même un tel produit ». En outre, l'annexe III reprend la liste susceptible d'évolution de huit types de systèmes à haut risque[46] : systèmes biométriques d'identification (reconnaissance faciale, utilisation des empreintes digitales, etc.) systèmes de gestion des infrastructures critiques (trafic routier, infrastructures de transport de gaz, électricité...) ; applications dans le secteur de l'éducation et de la formation (systèmes d'accès et d'évaluation des étudiants) ; applications en matière d'emploi (recrutement, contrôle et évaluation du personnel) ; applications en ce qui concerne l'accès ou la jouissance de services publics (en particulier les systèmes d'assistance) ou de services privés (évaluation de la valeur de crédit) essentiels (prioritisation de l'accès à des systèmes de santé ou de secours) ; systèmes utilisés par les forces de l'ordre (évaluation de la dangerosité des personnes, fiabilité des moyens de preuve, détection des émotions...) ; systèmes utilisés en matière de migration ou de contrôle des frontières ; systèmes d'administration de la justice (recherche et interprétation des faits ou interprétation et application de la loi).

Les fournisseurs (*providers)* de systèmes IA à haut risque se voient imposer de multiples devoirs (article 16)[47]. La proposition impose, pour les systèmes dits à haut-risque, un système de gestion des risques (article 9) qui implique le suivi de bonnes pratiques en matière d'évaluation des systèmes (absence de biais, qualité des données...). L'article 10 mentionne divers devoirs liés à la gouvernance des données, ainsi le *testing* et la validation des choix de *design* et des données prises en compte, l'examen des biais possibles, etc. On ajoute les obligations de documentation technique, par ailleurs détaillée dans son contenu et son format par l'annexe IV de la proposition, (articles 11 et 18), de *loggings* (articles 12 et 20) et surtout de surveillance humaine (*human oversight*)[48]. Le projet mentionne le devoir de coopération avec les autorités nationales compétentes y compris en fournissant l'accès à tous les logs. En particulier, l'article 19 mentionne l'obligation d'une évaluation interne (*self assessment* sans les applications en matière de données biométriques), préventive de la conformité du système aux exigences du règlement ou l'apposition d'un certificat européen de conformité avant toute mise sur le marché[49].

D'autres obligations concernent d'autres acteurs : à côté des fournisseurs de systèmes à haut risque, la proposition identifie les producteurs, les distributeurs, les importateurs les utilisateurs ayant recours à un système à haut risque dans le cadre de leurs activités professionnelles (ainsi, une banque utilisant un système de *credit rating*) et ce, suivant leur rôle précis lors des diverses étapes qui mènent de la conception à l'exploitation du système IA. Ce point est important dans la mesure où, à la différence du RGPD, concentré sur les seuls acteurs — responsable de traitement et sous-traitants, d'une part, et personnes concernées, d'autre part —, la proposition de règlement prend pleinement en compte la diversité des acteurs qui constituent la chaîne d'intervenants, depuis la conception du système d'IA jusqu'à son suivi, même si la qualification de certains intervenants risque de poser difficulté[50] et que les systèmes IA résultent souvent d'une collaboration entre une entreprise informatique et un ou des utilisateurs futurs.

Enfin, l'article 30 oblige les États membres à créer une autorité dite de notification (*notifying body)*. Chaque État membre désigne ou établit une autorité « chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle ». On note que coiffent ces autorités de notification, des autorités de supervision, « établies ou désignées par chaque État membre aux fins d'assurer l'application et la mise en œuvre du présent règlement y compris le pouvoir de sanctionner le non-respect des prescrits. Les autorités nationales compétentes sont organisées de manière à garantir l'objectivité et l'impartialité de leurs activités et de leurs tâches ». C'est à propos de ces autorités de supervision que l'EDPB, dans son avis commun avec l'EDPS[51], souhaitait que leurs tâches soient confiées aux autorités de protection des données : « The designation of data protection authorities (DPAs) as the national supervisory authorities would ensure a more harmonized regulatory approach, and contribute to the consistent interpretation of data processing provisions and avoid contradictions in its enforcement among Member States. Consequently, the EDPB and the EDPS consider that data protection authorities should be designated as national supervisory authorities pursuant to Article 59 of the Proposal ». Cette position peut s'expliquer si on se limite à la considération des seuls

(46) On s'étonnera de la liste qui mélange des critères différents, tantôt basés sur le type de données (exemple : données biométriques d'identification), tantôt fondés sur le secteur en cause (exemple : le secteur financier), tantôt sur la finalité (recrutement de personnel, accès à des services publics ou privés essentiels), tantôt par une combinaison de plusieurs critères (exemple : dans le secteur éducatif, l'évaluation des étudiants). L'utilisation de tels critères rend la lecture et l'interprétation du texte difficile et peut poser problème. Ainsi, un système expert (IA symbolique) traditionnel qui traduirait en algorithmes les règles de délibération est un système à haut risque, alors que les systèmes d'IA de contrôle des agriculteurs fondés sur la géomatique à des fins de contrôle ne le seraient pas. Par ailleurs, ne fallait-il pas considérer que les méthodes d'AI ne présentent pas le même niveau de risque. Ainsi, un système expert qui traduit un raisonnement humain transparent apparaît moins dangereux qu'une application utilisant des méthodes de *machine learning* dont le fonctionnement est peu transparent et évolue en fonction des données qu'elle rencontre. **(47)** Article 16 du projet de règlement. **(48)** Article 14.1 : « La conception et le développement des systèmes d'IA à haut risque permettent, notamment au moyen d'interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant la période d'utilisation du système d'IA ». On notera le flou d'une telle disposition. **(49)** Les annexes VI et VII définissent la procédure soit légère et purement interne si le fournisseur (*provider*) s'appuie sur des systèmes se référant à des standards harmonisés, soit plus lourde et dans ce cas externe auprès d'un organe de notification (autorité de contrôle) si tel n'est pas le cas. Cette évaluation est interne au fournisseur, ce qui peut faire craindre un certain laxisme dans l'interprétation des exigences du futur règlement, sous réserve certes du contrôle par l'autorité nationale de supervision évoquée dans le paragraphe suivant. On ajoute que l'absence d'évaluation ou de certificat ou leur mauvaise réalisation sont lourdement sanctionnées. **(50)** La notion de fournisseur est définie par l'article 3 point (2) comme suit : « fournisseur », une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit ; » ; celle d'utilisateur au point (4) : « utilisateur », toute personne physique ou morale, autorité publique, agence ou autre organisme utilisant sous sa propre autorité un système d'IA... ». Considérera-t-on que la banque qui achète « clé sur porte » à une entreprise spécialisée en IA est fournisseur ou utilisateur ? *Quid* d'une administration ou d'un hôpital, qui « outsourcent » la gestion de 'leur' système IA ? Par ailleurs, il n'est pas fait mention des fournisseurs des éléments du système : par exemple une base de données ou un algorithme. **(51)** Opinion déjà citée (note 52)

risques d'atteinte à nos libertés individuelles, elle s'avère plus critiquable si on considère également les autres risques collectifs et sociétaux liés aux applications de l'IA. À cet égard, on note que les lignes directrices de la Commission consultative de la Convention n° 108 du Conseil de l'Europe en matière de mégadonnées, en même temps qu'elle estime que sa compétence se limite à la protection des données, prend soin de souligner les risques majeurs sociétaires et collectifs des *big data* et de l'intelligence artificielle et prône la création de commissions d'éthique en charge d'une approche globale des risques. Enfin, et ici la critique de certains[52] est acerbe, rien n'est prévu en ce qui concerne la possibilité pour les citoyens ou pour des groupes de citoyens (*class action*) de se plaindre des dommages subis suite à la mise en place d'un système d'IA.

12. — Et les robots. — Une autre proposition de règlement dit « machines et équipements »[53], publiée le même jour par la Commission, remplacerait la directive de 2006 « machines », qui définissait des exigences en matière de santé et de sécurité dans le secteur des machines. La proposition garantit que les machines de nouvelle génération intégrant des logiciels en particulier d'IA comme, par exemple, les robots de ligne de production, les imprimantes 3D, les drones et les robots aide-soignant, offrent, au regard des nouveaux risques créés[54], toute la sécurité requise aux utilisateurs et aux consommateurs et encouragera l'innovation. Alors que le règlement sur l'IA traitera des risques liés à la sécurité que présentent les systèmes d'IA, le nouveau règlement sur les machines garantira une intégration sûre des systèmes d'IA dans les machines et les responsabilités liées au fonctionnement de ces produits d'intégration[55]. En particulier, le règlement exige pour les machines et équipements à haut risque définis à l'annexe du règlement, de suivre une procédure d'évaluation de conformité. Les critères d'appréciation des risques sont fixés dans le texte du règlement (article 5). Le texte (articles 6 et s.) impose aux producteurs, importateurs, distributeurs une série d'obligations en matière de documentation, de tests, etc. Enfin, la proposition impose (articles 24 et s.) aux États membres de désigner un organe de notification qui peut s'appuyer ou non sur un organe externe d'accréditation[56]. On ajoute qu'en cas de défaillance d'un produit ou de crainte raisonnablement suffisante de non-respect par un produit des requis en matière de sécurité ou de santé, l'autorité de surveillance peut exiger des mesures correctives (articles 36.3 et 41.1).

13. — En marge de la proposition de règlement, la question de la responsabilité[57]. — La question de la responsabilité du fait de l'utilisation de l'IA est sans doute l'une des questions les plus complexes à résoudre. Les hypothèses peuvent être nombreuses. Tantôt le dommage est physique : la voiture intelligente utilisée par l'administration heurte un piéton ou un drone pique sur une maison ; tantôt le dommage est financier : le système d'IA d'aide à la décision refuse à une personne, pourtant légitime demanderesse, un avantage fiscal voire moral ou une personne est suspectée à tort de fraude sociale et son nom circule dans la presse. Sous réserve des systèmes de responsabilité mis en place par des législations particulières comme celle en matière de protection des données, qu'en est-il de manière générale ? La discussion est vive et d'aucuns regretteront qu'elle n'ait point fait l'objet d'une proposition de règlement, émise le même jour que celle relative à l'IA.

Pour l'approcher, nous nous baserons sur une récente résolution du Parlement européen du 20 octobre 2020, complétée par une proposition de règlement adressée au Conseil et à la Commission, qui aborde la question de la responsabilité civile pour les systèmes d'IA[58]. Pour faire bref, le Parlement répond à une interrogation qu'il s'était posée en 2017[59] (résolution relative aux règles de droit civil applicables aux robots) qui suggérait d'octroyer une personnalité juridique aux robots et ce sur base du rapport en date de novembre 2019 d'un groupe d'experts européens sur la responsabilité civile de l'IA[60].

Tenir la plume en la matière n'est pas simple : créer la confiance des utilisateurs ou personnes affectées par l'IA sans pour autant alourdir démesurément les charges et la responsabilité des entreprises qui s'y lancent au point de les décourager. L'approche par les risques est également ici proposée. La proposition parlementaire repose sur la distinction entre systèmes à haut risque et les autres. Une liste de systèmes à haut risque devrait être proposée. Si l'approche est semblable, il n'est pas évident que les listes, celle en matière de responsabilité, celle en matière de gouvernance de l'IA (*supra*, n° 11), voire celle développée par l'article 36 du RGPD qui soumet à un *Privacy Impact Assessment* les systèmes présentant des risques élevés en matière de protection des données soient les mêmes au regard des objectifs différents poursuivis par les trois textes.

Pour ces systèmes dits à haut risque, tout en souhaitant une évolution de la directive 85/374/CE de 1985 sur la responsabilité du fait des produits dont les conditions réglementaires sont peu rencontrées dans le cadre de « produits » d'IA, le Parlement (article 4 de la proposition de règlement) envisage une responsabilité stricte sans faute pour les opérateurs de tels systèmes : « L'opérateur d'un système d'IA à haut risque est objectivement responsable de tout préjudice ou de tout dommage causé par une activité, un dispositif ou un procédé physique ou virtuel piloté par

(52) Voy. à la fois les critiques de N. Smuha *et alii* dans le rapport de l'université de Birmingham, cité *supra* note 44 et celles de l'EDPB et EDPS dans leur opinion conjointe déjà citée. **(53)** *Proposal for a regulation of the European Parliament and of the Council on machinery products*, Bruxelles, 21 avril 2021 COM(2021) 202 final 2021/0105 (COD). **(54)** Voy. l'*Explanatory Memorandum*, n° 11, p. 16. **(55)** Sur ce point, la proposition s'appuie sur l'excellent rapport de la Commission au Parlement européen, au Conseil et au Comité économique et social européen, Rapport du 19 février 2020 sur les conséquences de l'intelligence artificielle, de l'internet des objets et de la robotique sur la sécurité et la responsabilité, COM/2020/64 final, *disponible à l'adresse* https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implicationsai-internet-things-and-robotics-0_en et la résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle (2020/2014(INL)). **(56)** Article 25.3. **(57)** Les réflexions qui suivent constituent un résumé des réflexions développées dans le rapport CRIDS/Nadi, remis à la Région wallonne sur l'IA et les services publics, Y. Poullet, N. Bontridder et L. Gerard, *Intelligence artificielle et autorités publiques wallonnes - L'impact des technologies d'intelligence artificielle sur le gouvernement et l'administration numérique en Wallonie*, Rapport remis à l'AdN, en mai 2021, pp. 164 et s., à paraître. **(58)** Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission sur un régime de responsabilité civile pour l'intelligence artificielle (2020/2014(INL)). **(59)** Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)), disponible en ligne sur https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_FR.html (consulté le 2 juin 2021). **(60)** Rapport du groupe d'experts sur la responsabilité et les nouvelles technologies, section « nouvelles technologies », du 21 novembre 2019 sur la responsabilité en matière d'intelligence artificielle et d'autres technologies numériques émergentes (*Liability for Artificial Intelligence and other emerging digital technologies*).

Analyse

un système d'IA ». Pour les autres systèmes, un régime de responsabilité basée sur la faute présumée selon l'article 8 de la proposition[61] serait retenu. L'article 8.1. décrit ce régime comme suit : « L'opérateur d'un système d'IA qui n'est pas défini comme un système d'IA à haut risque au sens de l'article 3, point c), et de l'article 4, paragraphe 2, et qui ne figure donc pas dans l'annexe du présent règlement, est soumis au régime de la responsabilité pour faute en cas de préjudice ou dommage causé par une activité, un dispositif ou un procédé physique ou virtuel piloté par le système ». Nous ajoutons que la proposition de règlement du Parlement prévoit, comme celle de la Commission dans le cadre de l'AI Act, l'existence de certificats de conformité européens délivrés par des organismes accrédités. En l'occurrence, ils permettront aux opérateurs de faire la preuve de leur diligence et donc de renverser la présomption de faute. La proposition introduit l'idée d'une assurance, obligatoire pour les systèmes à haut risque et volontaire pour les autres[62].

14. — La diversité des intervenants et la répartition de leurs responsabilités. — Par ailleurs, comme la proposition de règlement sur l'IA de la Commission, la proposition parlementaire insiste sur la responsabilité des différents intervenants de la *supply chain* exigée par le montage des applications de l'IA. Ici, la proposition distingue les opérateurs en amont et en aval. « Le Règlement précise que l'opérateur frontal désigne « toute personne physique ou morale qui exerce un certain contrôle sur un risque associé à l'exploitation et au fonctionnement du système d'IA et tire profit de son exploitation »[63] et l'opérateur en amont, « toute personne physique ou morale qui, de manière continue, définit les caractéristiques de la technologie et fournit des données ainsi qu'un service de soutien en amont essentiel et exerce donc également un certain contrôle sur le risque lié à l'exploitation et au fonctionnement du système d'IA ». Eu égard à la multiplicité des acteurs nécessaires à la mise sur pied d'un système d'IA (fournisseur[s]) de données, concepteur d'algorithmes, service de *testing*, de paramétrage ou d'intégration de systèmes dans le contexte particulier d'une entreprise, déployeurs, opérateurs finaux, utilisateurs finaux du produit ou service et des rôles plus ou moins importants que chaque acteur peut jouer dans cette chaîne d'acteurs, la proposition de règlement propose des règles de répartition ou non-répartition de responsabilité entre ces acteurs. Ainsi, l'article 11 évoque la responsabilité solidaire de certains acteurs, lorsque plusieurs d'entre eux peuvent être qualifiés d'opérateurs : « S'il y a plus d'un opérateur pour un système d'IA, ils sont conjointement et solidairement responsables ». L'exemple de la fourniture de profils par des plateformes à des entreprises ayant défini leur cible de clientèle est un bon exemple de co-responsabilité. Dans le cas où l'administration est l'opérateur frontal, on pourrait de même imaginer qu'un fournisseur de données, dans la mesure où il participe par le choix des données transmises et la fourniture de l'algorithme adéquat aux besoins de l'administration, soit reconnu comme responsable solidaire. Dans les hypothèses où l'on ne peut conclure à la solidarité entre les opérateurs, la règle sera celle de proportionnalité : entre les opérateurs, la répartition suit le degré de contrôle exercé sur le risque lié à l'IA. Enfin, la proposition retient l'idée déjà émise par le Groupe d'experts[64] d'utiliser les *logs* du système pour apporter la preuve tantôt de la faute de la personne lésée, tantôt de celle de l'opérateur. L'article 10.2 souligne : « Un opérateur tenu responsable peut utiliser les données produites par le système d'IA pour prouver une faute concurrente de la part de la personne lésée, conformément au règlement (UE) 2016/679 et aux autres actes législatifs applicables en matière de protection des données. La personne lésée peut également utiliser ces données comme moyens de preuve ou d'éclaircissement dans l'action en responsabilité ». Nous ajoutons que la proposition introduit l'idée d'une assurance, obligatoire pour les systèmes à haut risque et volontaire pour les autres.

Conclusions

15. — L'Europe entend prendre place sur le marché global du numérique, dominé de la tête et des épaules par les géants chinois et américains. Pour ce faire, elle met à son service l'outil réglementaire. Il s'agit d'abord de permettre un réel marché européen de la donnée et de stimuler des *big data*, tant dans le secteur public que privé, en décloisonnant les frontières entre privé et public, en *sensibilisant* les citoyens au *public good* et en appelant au partage de données. Nul ne songera à critiquer cette approche courageuse mais sans doute impliquant un changement de culture tant au sein d'une administration peu interconnectée et souvent encore cloisonnée, qu'au sein des entreprises jalouses de leurs données et craignant les compétiteurs. Cette politique d'ouverture des données est nécessaire pour réussir le développement d'une IA dont on entend qu'elle doit être excellente et mériter la confiance des citoyens. Pour ce faire, là également, l'Union européenne entend développer un cadre légal encore à ses balbutiements par une approche préventive des hauts risques en imposant une procédure à la fois d'évaluation et de gestion des risques et une politique de certificats qui garantit le développement d'un marché souverain des systèmes d'IA. Certains reprocheront les exigences de ce cadre légal tant dans son contenu que par la lourdeur administrative qu'il met en place. Ce cadre remet l'état au centre du jeu. L'autorégulation par le secteur a vécu. Il s'ajoute, encore que les frontières sont mal placées[65], à celui déjà lourd des législations de protection des données dont l'objet plus étroit n'est pas exactement le même que celui envisagé par la réglementation de l'IA. On ne peut résoudre les questions de manipulation génétique ou de justice sociale soulevées par certaines applications d'intelligence sociale avec les seuls concepts et prescrits d'une législation qui a pour seul objectif la protection des libertés. Il y a là des conflits potentiels entre les autorités de pro-

(61) Cette présomption de faute peut être renversée de diverses manières comme le précise le considérant 18, « La diligence qui peut être attendue de la part d'un opérateur doit être proportionnée [...]. Il convient de présumer que l'opérateur a fait preuve de la diligence qui peut raisonnablement être attendue de lui dans la sélection d'un système d'IA approprié si l'opérateur a sélectionné un système d'IA qui a été certifié au titre d'un système semblable au système de certification volontaire envisagé par la Commission. Il convient de présumer que l'opérateur a fait preuve de la diligence qui peut raisonnablement être attendue de lui durant l'exploitation du système d'IA si l'opérateur peut prouver qu'il a effectivement et régulièrement contrôlé le système d'IA durant l'exploitation et qu'il a notifié au fabricant les irrégularités potentielles au cours de l'exploitation [...] ». Dans ce dernier cas, l'obligation de diligence est considérée comme remplie, lorsque l'opérateur dispose d'un certificat de conformité. **(62)** Les considérants s'étendent longuement sur le besoin d'assurance appropriée aux risques particuliers liés à l'IA. Voy. le considérant 22. En complément, est suggérée la création d'un fonds d'indemnisation. **(63)** Article 3, e), du règlement proposé par la résolution. **(64)** L'idée était défendue par le groupe d'experts qui souhaitait rendre obligatoire la mise à disposition d'un produit disposant d'une boîte noire. **(65)** Sur ce thème, les observations très critiques de N. Smuha, E. Ahmed-Rengers et A. Herkens *e.a.*, *How the EU can achieve Legally Trustworthy AI : A response to the European Commission's proposal for an Artificial intelligence Act*, University of Birmingham Leads Lab Report, disponible à l'adresse : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991.

tection des données et celles envisagées par le règlement IA à résoudre et des territoires de compétence à délimiter en même temps que leur solution nécessite leur dialogue.

Faut-il regretter ces choix européens ? La confiance citoyenne dans une IA au service du bien commun et de l'humain mérite à notre avis de tracer cette « troisième voie ». Sans doute, l'invocation de principes éthico-juridiques ne suffit pas : l'effectivité de la mise en œuvre de ces principes suppose que les entreprises soient convaincues de l'intérêt, y compris dans leur chef, de cette évaluation de conformité aux principes ; l'approche basée sur les risques qui fonde la limitation de l'utilisation de l'outil réglementaire et de règles dérogatoires au droit commun de la responsabilité aux systèmes à hauts risques apparaît sage même si toutes les interrogations relatives à l'étendue et aux critères de ce qu'il faut appeler un « haut risque » ne semblent pas closes. Allons, le pari européen est loin d'être gagné mais il vaut la peine d'essayer de le relever !