

Citation suggérée : Anaëlle Martin, Les enjeux juridiques et éthiques de l'Artificial Intelligence Act. À propos de la proposition de règlement européen établissant des règles harmonisées concernant l'intelligence artificielle *Blogdroiteeuropéen Working Paper 3/2022*, Mai 2022, Accessible à <https://wp.me/p6OBGR-4uw>

## Les enjeux juridiques et éthiques de l'*Artificial Intelligence Act*. À propos de la proposition de règlement européen établissant des règles harmonisées concernant l'intelligence artificielle

Anaëlle Martin, docteure en droit de l'Université de Strasbourg

### Sommaire :

- I. Le défi d'un cadre législatif de l'intelligence artificielle au niveau de l'Union européenne**
- II. La question insoluble des droits fondamentaux : les limites juridiques de l'approche par les risques**
- III. L'équation complexe d'une *IA made in Europe* : entre protection des principes éthiques et soutien à l'innovation**

## Les enjeux juridiques et éthiques de l'*Artificial Intelligence Act*. À propos de la proposition de règlement européen établissant des règles harmonisées concernant l'intelligence artificielle

<https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52021PC0206>

En raison de son impact croissant sur les entreprises et la société, la transition numérique pose de nouveaux défis à l'Europe. Si l'Union européenne (UE) entend soutenir l'innovation et les compétences numériques, afin de tirer profit du marché unique numérique, elle place le citoyen au cœur de ses préoccupations, en visant à garantir la sécurité, la transparence et la responsabilisation du secteur. Les plateformes numériques, le cloud computing, l'internet des objets et, plus encore, l'intelligence artificielle (IA) font partie des technologies numériques qui suscitent un vif intérêt et appellent une réponse appropriée de l'Union européenne, au regard des risques et des opportunités qui leur sont attachés. C'est dans ce contexte que le 21 avril 2021, la Commission européenne dévoilait son projet de règlement visant à établir des règles

harmonisées concernant l'intelligence artificielle. Un an après la publication de cette proposition législative, force est de constater les nombreuses difficultés auxquelles se heurte l'Union européenne en matière de réglementation des systèmes d'IA. Ces difficultés, d'ordre conceptuel et politique, mettent en évidence la complexité technique du domaine en question. Elles dévoilent aussi les limites du droit — du droit en général et du *droit de l'UE* en particulier — en même temps qu'elles exigent de combiner des approches souples et contraignantes afin de prévenir les risques inhérents aux nouvelles technologies, à l'instar des biais discriminatoires, des erreurs de décision et de l'opacité des algorithmes. Ces risques propres aux systèmes d'IA appellent un régime de responsabilité et des obligations de transparence spécifiques pour faire de l'UE un acteur mondial de premier plan dans le développement d'une IA sûre, fiable et éthique. La présente note ne prétend pas dresser une analyse exhaustive du texte de la proposition, mais propose d'exposer les enjeux normatifs qui se posent à l'UE face à l'urgence d'adopter un cadre réglementaire de l'IA, à la fois éthique et juridique. Le premier défi concerne l'ambition d'établir un cadre législatif de l'IA au niveau de l'UE à l'heure où les stratégies nationales sur la souveraineté numérique se multiplient (I). Le second défi, au cœur de la stratégie européenne visant à promouvoir une IA digne de confiance, a trait à la garantie des droits fondamentaux et impose une approche « par les risques » qui soulève, en termes juridiques, plus d'interrogations qu'elle n'apporte de réponses (II). Enfin, l'équation complexe d'une *IA made in Europe* cherchant à assurer la protection des principes éthiques tout en favorisant un cadre normatif propice à l'innovation, constitue un dernier défi susceptible de cristalliser les débats sur les enjeux attachés à l'*Artificial Intelligence Act* (III).

## I. Le défi d'un cadre législatif de l'IA au niveau de l'UE

L'*Artificial Intelligence Act*, publié le 21 avril 2021 par la Commission européenne, est une proposition de règlement qui s'inscrit dans un cadre législatif européen ayant vocation à s'étoffer dans les prochaines années. L'adaptation de l'Europe à l'ère numérique constitue l'une des six priorités que la Commission européenne s'est fixée pour 2019-2024<sup>1</sup>. Face à l'essor des nouvelles technologies, l'Union européenne souhaite établir un cadre juridique permettant d'offrir de nouvelles opportunités aux entreprises et aux consommateurs, tout en garantissant le respect des droits des citoyens. En plus du *RGPD* relatif à la protection des données à

<sup>1</sup> Cf. Orientations politiques pour la prochaine commission européenne, 2019-2024, présentée par la candidate à la présidence de la Commission européenne, Mme Ursula von der Leyen, accessible à [https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission\\_fr.pdf](https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_fr.pdf)

caractère personnel<sup>2</sup>, entré en application le 25 mai 2018, d'autres propositions de règlements, publiées entre 2020 et 2022, doivent être mentionnées : le *Digital Market Act* (DMA)<sup>3</sup>, le *Digital Services Act* (DSA)<sup>4</sup>, le *Data Governance Act* (DGA)<sup>5</sup> et le Data Act<sup>6</sup>. Seul l'*Artificial Intelligence Act* retiendra ici notre attention. La publication d'un projet de règlement constitue une étape normative importante dans la mesure où la Commission vise à instaurer un cadre réglementaire contraignant pour certains systèmes d'IA définis par elle. L'abondance des textes produits ces dernières années en matière d'IA ne doit pas occulter le fait que la plupart revêtent une faible valeur juridique puisqu'il s'agit essentiellement de lignes directrices, de résolutions, de recommandations et de communications<sup>7</sup>. Ainsi, le 19 février 2020, la Commission publiait, en même temps qu'elle dévoilait sa stratégie pour les données<sup>8</sup>, son *Livre blanc* sur l'IA<sup>9</sup>, lequel s'appuyait sur un guide rédigé en 2019 par un groupe d'experts européens<sup>10</sup>. La multiplication de cette littérature grise rappelle que si les considérations éthiques sont largement prises en charge par le *soft law*, un cadre juridique plus contraignant s'impose pour encadrer rigoureusement le développement des systèmes d'IA. Puisqu'il s'agit d'établir un cadre harmonisé à l'échelle de l'UE, la Commission est tenue d'identifier la base juridique pertinente tout en s'assurant du respect des principes de subsidiarité et de proportionnalité.

<sup>2</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

<sup>3</sup> Proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act).

<sup>4</sup> Proposal for a regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending directive 2000/31/EC.

<sup>5</sup> Proposal for a regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act).

<sup>6</sup> Proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).

<sup>7</sup> Le Conseil de l'Europe a publié un certain nombre d'instruments juridiques : *Un cadre juridique pour les systèmes d'intelligence artificielle. Étude de faisabilité d'un cadre juridique pour le développement, la conception et l'application de l'intelligence artificielle, basé sur les normes du Conseil de l'Europe sur les droits de l'homme, la démocratie et l'État de droit* DGI (2021)04. *Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme* (8 avril 2020) ; *Déclaration du Comité des Ministres sur les capacités de manipulation des processus algorithmiques* (13 février 2019) ; *Recommandation de l'Assemblée parlementaire du Conseil de l'Europe sur la convergence technologique, l'intelligence artificielle et les droits de l'homme* -Recommandation 2102(2017). S'agissant de l'OCDE et de l'UNESCO : OCDE, *L'intelligence artificielle dans la société*, Éditions OCDE, Paris, [https://doi.org/10.1787/b7f8cd16\\_fr](https://doi.org/10.1787/b7f8cd16_fr) ; Unesco, *Recommendation on the Ethics of Artificial Intelligence* (23 November 2021), <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.

<sup>8</sup> 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. COM(2020) 66 final.

<sup>9</sup> LIVRE BLANC Intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance. COM(2020) 65 final.

<sup>10</sup> European Commission, Directorate-General for Communications Networks, Content and Technology, Lignes directrices en matière d'éthique pour une IA digne de confiance, Publications Office, 2019, <https://data.europa.eu/doi/10.2759/54071>.

La base juridique du projet de règlement est l'article 114 du TFUE relatif aux mesures destinées à assurer le fonctionnement du marché intérieur. La proposition s'inscrit dans le contexte du marché unique numérique en ce qu'elle vise à établir des règles harmonisées pour le développement et l'utilisation de produits et services exploitant les technologies de l'IA. Dans la mesure où certains États membres envisagent de réglementer ce domaine, il existe un risque de fragmentation du marché et de diminution de la sécurité juridique pour les fournisseurs et les utilisateurs des systèmes d'IA. Conformément au principe de subsidiarité, une action normative au niveau de l'UE s'impose pour éviter des législations disparates susceptibles d'entraver la circulation des biens et services intégrant l'IA. Seule une harmonisation européenne est en mesure de protéger la souveraineté numérique<sup>11</sup> de l'Union, *via* un cadre réglementaire solide, et garantir des conditions de concurrence équitables tout en protégeant les droits fondamentaux. Cette proposition qui vise à adopter une approche coordonnée des implications éthiques de l'IA s'appuie sur les craintes suscitées par l'imprévisibilité, la complexité, l'opacité et l'autonomie de certains systèmes d'IA, y compris les risques de résultats biaisés générés par ces derniers. Une réglementation au niveau régional s'impose au regard de la nature même de l'IA, laquelle repose sur de vastes jeux de données et peut, comme le rappelle la Commission, être intégrée à tout produit ou service circulant sur le marché de l'UE. Conformément au principe de proportionnalité, la proposition de la Commission se fonde sur une approche graduée qui n'impose de charges réglementaires que si un système d'IA présente un risque élevé pour les droits fondamentaux et la sécurité. Pour les systèmes d'IA ne présentant pas de tels risques, une simple obligation de transparence, comme la fourniture d'informations aux utilisateurs, est envisageable. S'agissant des systèmes d'IA à haut risque, la Commission propose d'appliquer des exigences accrues en matière de transparence, de qualité, de documentation, de traçabilité, de contrôle humain, d'exactitude et de robustesse. Ces exigences se limitent toutefois au strict nécessaire pour atténuer les risques pour les droits fondamentaux et la sécurité. Le choix de l'instrument juridique — un règlement plutôt qu'une directive — se justifie par la nécessité d'une application uniforme des règles relatives à la définition de l'IA, la classification des systèmes d'IA et l'interdiction des pratiques jugées préjudiciables.

<sup>11</sup> La souveraineté numérique s'inscrit dans un contexte politique international de la gouvernance d'Internet dominé par les États-Unis. A. Blandin-Obernesser, « Les entreprises souveraines de l'Internet : un défi pour le droit en Europe. » dans Droits et souveraineté numérique en Europe, Bruxelles, Bruylant, 95-109. P. Meunier, *Les compétences de l'Union européenne et la souveraineté numérique*, Nice, 2016.

La définition juridique de l'IA présente un enjeu important pour le futur règlement en ce qu'elle détermine son champ d'application. Or, un champ d'application trop large peut se révéler préjudiciable pour l'innovation et le développement de l'IA en Europe. De même, si une définition souple permet de tenir compte de la dynamique inhérente à la matière technologique, un minimum de précision est nécessaire pour garantir la sécurité juridique. La Commission opte, de manière pragmatique, pour l'expression *système d'IA* plutôt qu'*IA*, cette dernière renvoyant davantage à une discipline théorique. Au terme de multiples tâtonnements conceptuels et terminologiques, les systèmes d'IA sont finalement définis, à l'article 3, comme des logiciels développés au moyen de techniques énumérées dans un annexe<sup>12</sup> qui « peuvent, 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 »<sup>13</sup>. Le choix d'une définition relativement large de l'IA ne signifie pas que l'UE entend réguler tous les systèmes d'IA puisque l'article 2 indique que le règlement ne s'applique pas aux systèmes utilisés à des fins militaires. Le caractère flexible des définitions choisies par la Commission<sup>14</sup> permet au futur règlement de s'adapter aux évolutions technologiques tout en s'inscrivant dans la stratégie numérique globale de la Commission. Le projet de règlement prétend ainsi renforcer la contribution de l'UE à la définition de normes mondiales et à la promotion d'une IA qui soit conforme aux intérêts de l'Union.

La poursuite d'une stratégie régionale n'empêche pas les États membres de développer, à leur échelle, une réflexion sur le développement de l'IA prenant la forme d'une stratégie nationale<sup>15</sup>. La transition numérique révèle les dynamiques variées des écosystème technologiques et de

<sup>12</sup> L'annexe I liste 3 catégories de systèmes : les systèmes auto-apprenants (*machine learning*), les systèmes logiques et les systèmes statistiques.

<sup>13</sup> La présente définition diffère sensiblement des précédentes, la Commission ayant proposé, dans une communication de 2018, de définir l'IA comme des systèmes soit purement logiciels, agissant dans le monde virtuel, soit intégrés à des dispositifs matériels : *L'intelligence artificielle pour l'Europe*, COM(2018) 237 final. Cette définition, très éloignée de celle des *data scientists*, fut retravaillée par le groupe d'experts de haut niveau.

<sup>14</sup> L'article 3 définit d'autres notions essentielles relatives aux acteurs de l'IA (fournisseurs, utilisateurs, mandataires, importateurs, distributeurs, importateurs) et aux données (données d'entraînement, de validation, de text, d'entrée, biométriques).

<sup>15</sup> En 2018, la France s'est dotée d'une stratégie pour l'IA visant à en faire une nation leader. La stratégie poursuit 3 objectifs : renforcer l'attractivité des talents et investissement, diffuser l'IA et la donnée dans l'économie, promouvoir un modèle éthique. Accessible en ligne: <https://www.intelligence-artificielle.gouv.fr/fr>. Fin 2018, l'Allemagne dévoilait également sa stratégie *AI made in Germany*. Accessible en ligne (disponible en anglais et en français): <https://www.ki-strategie-deutschland.de/home.html>. Dotée d'un excellent réseau de recherche, l'Allemagne entend consolider ses atouts en aidant ses entreprises à exploiter le fort potentiel technologique qui découle de la recherche.

possibles divergences entre les États membres de l'UE. La France qui cherche à promouvoir la *French Tech* espère tirer profit de la présidence du Conseil de l'UE, au premier semestre 2022, pour faire émerger des champions européens — parmi lesquels des start-ups françaises — face aux géants technologiques. En tant que technologie hautement politique, l'IA présente un enjeu de souveraineté nationale et internationale. Dans une communication d'avril 2018<sup>16</sup>, la Commission affirmait que tous les ingrédients sont réunis pour que l'UE joue un rôle prédominant dans la révolution de l'IA sur la base de ses propres valeurs. Estimant que les économies les plus développées ont adopté des approches de l'IA qui reflètent leurs systèmes politique, économique, culturel et social, la Commission soulignait la nécessité pour les Européens d'unir leur force afin que l'Europe fasse partie de la transformation numérique. Le contexte international compétitif oblige l'UE à agir à son niveau dans la mesure où les États-Unis et la Chine, mais aussi la Russie, le Canada et le Japon, ont adopté des stratégies visant à en faire des leaders mondiaux<sup>17</sup>. L'urgence à agir est d'autant plus grande que l'Europe accuse un retard en matière d'investissements privés, à l'heure où les entreprises extra-européennes investissent massivement et exploitent de grandes quantités de données. Pour autant, la question du renforcement de la compétitivité et la base industrielle de l'Europe dans le domaine de l'IA est largement éclipsée, dans le débat public, par celle des droits fondamentaux tant les risques en la matière sont grands. La menace qui pèse sur ces derniers contraint l'UE à adopter une approche juridique prudente même si la méthode « par les risques » ne suffit pas à dissiper toutes les craintes qui entourent l'IA.

## **II. La question insoluble des droits fondamentaux : les limites juridiques de l'approche fondée sur les risques**

Le RGPD a révolutionné la manière dont les données personnelles sont collectées et traitées afin d'assurer la protection des personnes physiques. Le considérant 51 rappelle que les données à caractère personnel qui sont « sensibles du point de vue des libertés et des droits fondamentaux méritent une protection spécifique, car le contexte dans lequel elles sont traitées pourrait engendrer des risques importants pour ces libertés et droits ». Ces données dites

---

<sup>16</sup> Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions. L'intelligence artificielle pour l'Europe {SWD(2018) 137 final}

<sup>17</sup> Néanmoins, ces stratégies sont souvent plus économiques et politiques que juridiques. Voir par exemple la stratégie russe sur l'IA, notamment le titre III consacré aux principes fondamentaux dans le développement et l'utilisation des technologies de l'IA (droits fondamentaux, sécurité, transparence) (accessible en ligne) : <https://cset.georgetown.edu/article/thoughts-on-russias-ai-strategy/>.

sensibles sont celles qui révèlent, par exemple, l'origine ethnique de la personne. Pour assurer un traitement équitable, le responsable du traitement doit sécuriser ces données d'une manière qui tienne compte des risques susceptibles de peser sur les droits de la personne concernée et prévienne d'éventuels effets discriminatoires à son encontre. L'approche adoptée par l'UE est détaillée aux articles 32 (pseudonymisation des données) et 35 (analyse d'impact) du RGPD. Pour autant, les dangers liés à l'opacité des algorithmes comme les biais discriminatoires et les erreurs de décision n'ont pas été suffisamment pris en compte, le RGPD ayant privilégié la seule protection juridique des données personnelles. Ces risques éthiques sont habituellement pris en charge par le *soft law* (chartes, recommandations, résolutions).

Le projet de règlement sur l'IA entend combler les lacunes juridiques en la matière pour contraindre les développeurs à satisfaire à certaines exigences. Afin d'assurer un niveau élevé de protection des droits fondamentaux, le texte de la Commission vise à établir des règles communes pour tous les systèmes d'IA dits *à haut risque* en exigeant un certain degré de transparence. Ces règles devraient respecter la Charte des droits fondamentaux afin de garantir que les systèmes d'IA ne deviennent pas une source de discrimination. Pour cela, les systèmes d'IA à haut risque devraient contenir des informations et des instructions précises relatives aux potentiels risques de discrimination. Le respect des droits et libertés, dont la non-discrimination, requiert une représentativité statistique des données d'entraînement, une documentation pertinente sur les performances d'un système d'IA, des obligations d'archivage des décisions, mais également la possibilité d'interpréter ces dernières. À titre d'exemple, l'article 9 prévoit un système de gestion des risques documenté et tenu à jour pour les systèmes d'IA dits « à haut risque », à savoir ceux qui présentent des risques importants pour la santé, la sécurité ou les droits fondamentaux des personnes. Ce processus doit permettre l'identification et l'analyse des risques prévisibles associés à chaque système d'IA, l'estimation et l'évaluation des risques susceptibles d'apparaître lorsque le système est utilisé dans des conditions de mauvaise utilisation ou encore l'adoption de mesures appropriées de gestion des risques. L'approche par les risques consiste à autoriser sur le marché européen ces systèmes d'IA sous réserve du respect de certaines exigences obligatoires et d'une évaluation *ex ante* de la conformité. La classification d'un système d'IA comme étant à haut risque dépend de la fonction que ce système remplit mais également de sa finalité et de ses modalités d'utilisation (conformément à la législation en matière de sécurité des produits). Le chapitre 1 du titre III définit deux

catégories de systèmes d'IA à haut risque : ceux destinés à être utilisés en tant que composants de sécurité de produits (objet d'une évaluation *ex ante* de la conformité par un tiers) et les autres systèmes d'IA autonomes qui soulèvent des questions quant au respect des droits fondamentaux, listés à l'annexe III. Cette liste comprend un nombre limité de systèmes d'IA pour lesquels les risques recensés se sont déjà matérialisés ou sont susceptibles de se matérialiser<sup>18</sup>.

Le problème est que si le projet de règlement, à l'instar du livre blanc sur l'IA, insiste sur la nécessité de respecter les droits fondamentaux et lutter contre les biais discriminatoires, en créant les conditions justes et équitables à l'utilisation d'une IA fiable, la Commission ne semble pas être allée au bout de la logique. Si la recherche des biais systémiques est mise en avant, par la documentation, il n'existe pas de moyen de mesurer précisément la discrimination. En outre, l'équité ne fait pas l'objet d'une définition juridique<sup>19</sup>. Puisque les biais algorithmiques sont liés aux pratiques discriminatoires, assurer l'équité des algorithmes revient, en définitive, à éliminer les discriminations. À cet égard, il est possible de se référer à des indicateurs techniques pour identifier, évaluer et atténuer les biais statistiques, sources de potentielles discriminations<sup>20</sup>. Dans le champ disciplinaire anglo-saxon du fair *machine learning* (FairML) les chercheurs ont élaboré des outils comme la parité statistique/démographique<sup>21</sup>, les erreurs conditionnelles<sup>22</sup> et les rapports de cote conditionnels<sup>23</sup> pour fournir des critères opératoires aptes à mesurer différents types de biais. Bien que ces méthodes ne soient pas mentionnées dans le projet de règlement européen, certains de ces indicateurs, comme l'effet disproportionné

<sup>18</sup> La Commission se réserve la possibilité d'étendre la liste des systèmes d'IA à haut risque en appliquant un ensemble de critères et une méthode d'évaluation des risques.

<sup>19</sup> La notion d'équité a été abondamment traitée par un champ universitaire transdisciplinaire, l'éthique de l'IA (*AI Ethics*). L'objet de cette nouvelle discipline est l'étude des enjeux éthiques posés par l'essor de l'IA mais aussi le développement de dispositifs normatifs tels que des métriques, des procédures algorithmiques, des chartes éthiques (sur le modèle de soft law) ainsi que des outils techniques variés. La littérature en FairML qui regroupe une communauté d'informaticiens constitue l'une des sous-disciplines académiques de l'éthique de l'IA. Pour quelques exemples récents d'approche de l'équité par la littérature FairML : P. Saleiro, B. Kuester, L. Hinkson, J. London, A. Stevens, A. Anisfeld, K. T. Rodolfa, R. Ghani. *Aequitas : A Bias and Fairness Audit Toolkit*. arXiv, 11 2018. N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, A. Galstyan. *A survey on bias and fairness in machine learning*. ACM Computing Surveys (CSUR), 54(6), 1-35 (2021). Pour une approche centrée sur les rapports entre droit de l'UE et l'IA: S. Wachter, B. Mittelstadt, C. Russell, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI* (2020). Computer Law & Security Review 41 (2021): 105567., Available at SSRN: <https://ssrn.com/abstract=3547922> or <http://dx.doi.org/10.2139/ssrn.3547922>.

<sup>20</sup> P. Besse, *Statistique & Règlement Européen des Systèmes d'IA*. 2021. hal-03253111v3.

<sup>21</sup> La parité statistique exige que la réalisation de la prédiction ne soit pas corrélée à une variable sensible (comme l'origine ethnique). Cette condition d'égalité étant rarement atteinte en pratique, on exigera de l'algorithme l'écart le plus faible entre les probabilités. Il s'agit de la contrainte du *disparate impact*.

<sup>22</sup> Il s'agit de rechercher si les taux d'erreur de prévision sont les mêmes pour chaque groupe. L'erreur doit être indépendante de la variable sensible (ex : l'origine ethnique). La mesure consiste en un rapport de probabilité : probabilité de se tromper pour le groupe sensible (minorité ethnique) sur la probabilité de se tromper pour l'autre groupe.

<sup>23</sup> Comme les erreurs sont souvent dissymétriques, il peut être utile d'évaluer les faux positifs et les faux négatifs. L'indicateur est mesuré par l'estimation de 2 rapports de probabilités : rapports des taux de faux positifs du groupe sensible (minorité ethnique) sur le taux de faux positifs de l'autre groupe et rapport des taux de vrais positifs.

(*disparate impact*<sup>24</sup>) sont juridiquement consacrés aux États-Unis<sup>25</sup>. La prise en compte de l'indicateur de l'équité statistique dans le droit positif américain (droit du travail<sup>26</sup>) explique que les logiciels produits aux États-Unis anticipent le risque juridique en proposant des algorithmes de recrutement intégrant une méthode d'atténuation des biais. Ces formules visant à garantir l'équité des algorithmes, *via* des statistiques ethniques, implique une réflexion politique de l'UE sur ses valeurs : est-il opportun de '*débiaiser*' les algorithmes en promouvant en Europe des actions du type *discriminations positives* pour éliminer les biais qui reproduisent et renforcent les discriminations historiques et sociétales ? Il importe de rappeler que le recours aux statistiques ethniques est une pratique controversée, voire interdite, dans de nombreux États européens. De plus, si les *data scientists* ont élaboré des définitions mathématiques pour lutter contre les discriminations injustes perpétrées par des algorithmes, ces formalisations peuvent poser problème car elles sont souvent incompatibles les unes avec les autres. En effet, il est mathématiquement impossible de remplir simultanément certaines des conditions d'équité. En outre, ces définitions axiomatiques sont réductrices en ce qu'elles ne permettent pas de répondre aux enjeux concrets contextuels que pose l'équité dans une société donnée<sup>27</sup>.

Si l'équité ne se résume pas à une définition juridique, elle ne se réduit pas non plus à une équation mathématique. Pas plus que les mathématiques, le droit n'offre de réponse toute faite lorsqu'il s'agit d'appréhender les risques inhérents aux systèmes d'IA caractérisés par leur opacité et leur complexité croissantes. L'impuissance du droit vient de ce qu'il est pratiquement impossible de démontrer une violation de la réglementation relative aux droits fondamentaux quand il s'agit de décisions algorithmiques. Si les pratiques discriminatoires doivent permettre d'engager la responsabilité des auteurs à l'origine de ces pratiques interdites, en matière d'IA, il est extrêmement difficile d'identifier les causalités et, partant, de chercher la responsabilité des différents acteurs impliqués dans la chaîne décisionnelle.

La responsabilité est à la fois un principe éthique et juridique, au même titre que la transparence. En matière de régime de responsabilité, l'UE peut s'appuyer sur les règles existantes en matière

<sup>24</sup> Mesurer l'effet disparate consiste à estimer le rapport de deux probabilités : la probabilité d'un résultat favorable pour un candidat issu du groupe sensible (minorité ethnique) sur la même probabilité pour un candidat issu de l'autre groupe (non défavorisé).

<sup>25</sup> Civil Rights act & Code of Federal Regulations. Title 29, Labor : Part 1607 Uniform guidelines on employee selection procedures. La législation américaine exige que le ratio ne soit pas inférieur à 80% (seuil de 0,8, « eighty percent rule »).

<sup>26</sup> L'effet disproportionné (disparate impact) fait référence aux pratiques en matière d'emploi qui affectent négativement un groupe vulnérables (personnes issues d'une minorité). Cet indicateur a été repris en tant que métrique de biais.

<sup>27</sup> Michelle Seng Ah and Floridi, Luciano and Singh, Jatinder, Formalising trade-offs beyond algorithmic fairness: lessons from ethical philosophy and welfare economics (July 31, 2020). Available at SSRN: <https://ssrn.com/abstract=3679975>.

de responsabilité du fait des produits et en matière de protection des données personnelles<sup>28</sup>.

Certains systèmes d'IA, en particulier ceux qui permettent une prise de décisions autonomes, exigent de revoir le régime juridique en matière de sécurité et le droit civil relatif à la responsabilité<sup>29</sup>. En effet, le droit positif peine à offrir une réparation lorsque le fait génératrice du préjudice est un système d'IA<sup>30</sup>. Ce qui rend difficile l'application d'un régime de responsabilité classique est la pluralité des acteurs impliqués dans l'élaboration d'un système d'IA (programmation, fabrication, fourniture des données) jusqu'à sa mise en œuvre (exploitation, utilisation). Si l'intrication rend difficile la recherche des schémas de causalité, la Commission recommande que le fournisseur assume la responsabilité de la mise sur le marché/en service d'un système d'IA à haut risque. Compte tenu des risques pour la sécurité, la Commission propose de définir des responsabilités spécifiques pour les utilisateurs. Ces derniers devraient être tenus d'utiliser ces systèmes d'IA conformément à la notice d'utilisation. D'autres obligations sont prévues en matière de surveillance et de fonctionnement des systèmes d'IA. Concernant l'évaluation de la conformité des systèmes, celle-ci devrait être réalisée par le fournisseur sous sa propre responsabilité, à l'exception des systèmes d'IA destinés à l'identification biométrique à distance de personnes, pour lesquels l'intervention d'un organisme notifié est requise. S'agissant des fabricants, la Commission prévoit qu'ils ont la responsabilité de la conformité de ces systèmes avec le projet de règlement. Les importateurs et les distributeurs devraient aussi être soumis à des obligations puisqu'il est prévu que ces derniers s'assurent, lorsqu'un système d'IA à haut risque est sous leur responsabilité, que les conditions de stockage ou de transport ne compromettent pas sa conformité aux exigences énoncées par le règlement.

Il reste que le concept juridique de responsabilité est mis en difficulté par les systèmes d'IA dans la mesure où le régime légal ne peut s'appliquer que dans les cas où il est possible de définir le produit et ses relations. S'agissant de la responsabilité du concepteur de l'algorithme, que faire lorsque le produit est un vaste réseau socio-technique dont les limites et les causalités

<sup>28</sup> L'UE dispose d'une réglementation stricte en termes de responsabilité du fait des produits. S'agissant de la sécurité des réseaux et des systèmes d'information, elle dispose également des règles les plus strictes en matière de protection des données à caractère personnel.

<sup>29</sup> Les robots évolués et les produits de l'internet des objets, par exemple, peuvent agir d'une façon non envisagée lors de leur mise en service.

<sup>30</sup> La directive sur la responsabilité du fait des produits, par exemple, n'est pas adaptée au monde numérique car elle ne permet pas de répondre aux défis posés par les technologies émergentes. De même, la directive *Machines* ne traite pas de certains aspects des nouvelles technologies numériques.

sont imprécises ?<sup>31</sup> De même, faut-il engager la responsabilité des constructeurs d'un algorithme à l'origine de discriminations indirectes lorsqu'elles ne sont pas délibérées et qu'elles découlent de biais structurels historiques ? En effet, même en l'absence de biais d'échantillonnage, et en amont de la construction de l'algorithme, des biais seront structurellement présents dans les données, du fait des inégalités présentes dans la société. La question est d'autant plus complexe que l'opération de vérification est difficile. En matière d'accès à l'emploi, par exemple, la méthode du *testing* consistant à envoyer des dossiers de candidature comparables à l'exception de la caractéristique discriminatoire/variable sensible (origine ethnique) s'avère peu efficace pour détecter une discrimination perpétrée par un algorithme<sup>32</sup>. Conformément aux recommandations du groupe d'experts, la mise en place d'une documentation *ex ante* s'avère indispensable pour les systèmes à haut risque. L'évaluation devrait porter sur la représentativité statistique des données d'entraînement, les risques de dérives, les erreurs et biais potentiels. Afin d'auditer efficacement ladite documentation, des compétences techniques et juridiques sont requises<sup>33</sup>. Le recours à cette méthode devrait permettre d'identifier les responsabilités humaines.

Certaines voix<sup>34</sup> préconisent à l'UE de s'orienter vers un régime de responsabilité propre à l'IA, à savoir un régime de responsabilité objective aggravée. Dans la mesure où ce régime est axé sur la réalisation d'un risque caractérisé résultant d'une activité d'un système d'IA potentiellement dangereux, il implique l'identification préalable des risques prévisibles. La question demeure s'agissant des risques imprévisibles inhérents aux systèmes d'IA : sur qui faire peser les risques non prévisibles ? Sur la population ou sur ceux qui en sont à l'origine et en tirent un bénéfice ? Il importe, en ce domaine, de procéder à un partage équitable des responsabilités en s'attachant à identifier, via la traçabilité, le degré d'implication de chaque acteur dans la réalisation du dommage.

<sup>31</sup> J.-M. John-Mathews, *AI Ethics in Practice, Challenges and Limitations*, Thèse, 2021.

<sup>32</sup> Si le *testing* peut permettre une action en justice s'agissant de discriminations directes, appliqué dans une enquête systématique, cette méthode ne se révèle pas efficace (coûts élevés et recours à des méthodes fictives).

<sup>33</sup> P. Besse, *Détecter, évaluer les risques des impacts discriminatoires des algorithmes d'IA*, 2020. hal-02616963.

<sup>34</sup> L'apparition des véhicules autonomes, par exemple, pose la question de la responsabilité du détenteur du véhicule. Werro F., Perritaz V., *Les véhicules connectés : un changement de paradigme pour la responsabilité civile?*, in : F. Werro T. Probst (éd.), *Journées du droit de la circulation routière 23-24 juin 2016*, Berne 2016.

Les risques de discriminations liées aux biais algorithmiques et aux erreurs de décisions (faux négatifs et faux positifs) ne sont pas les seules menaces qui pèsent sur les droits fondamentaux. Dans la mesure où les données sont au cœur des systèmes d'IA, il importe de revenir sur la protection juridique des données personnelles. À l'instar du RGPD, le projet de règlement sur l'IA vise à renforcer la protection de celles-ci. Aux termes de l'article 16 du TFUE, « toute personne a droit à la protection des données à caractère personnel la concernant ». Au regard des spécificités de l'IA quant à la dépendance vis-à-vis des données et l'opacité des algorithmes, son usage peut porter atteinte à certains droits fondamentaux comme le respect de la vie privée et, son corolaire, la protection des données personnelles (articles 7 et 8). D'après le droit de l'UE, la protection des données s'impose à toute information concernant une personne physique identifiée ou identifiable. Suivant cette définition, il n'y a pas lieu d'appliquer les garanties aux informations anonymes, ces données ne faisant pas référence à une personne identifiée. Pour autant, les évolutions technologiques ont modifié les conditions dans lesquelles une personne peut désormais être identifiable. L'anonymisation est illusoire dès lors qu'une combinaison d'informations anonymes permet d'identifier une personne physique. En outre, les données faisant directement référence à une personne physique ne sont pas les seules susceptibles de causer un préjudice sous l'angle du droit des données personnelles. La collecte de données à des fins d'influence sur le comportement peut avoir un impact significatif sur les individus (objets connectés, *smart cities*). À la lumière des défis posés par les nouvelles technologies et les progrès techniques, c'est bien le concept juridique de donnée personnelle qui tend aujourd'hui à être remis en question au point que certains évoquent la *mort de l'anonymat*. Le dépassement de la notion trouve sa source dans la « datafication ubiquitaire » et les « pouvoirs d'inférence statistique »<sup>35</sup>. Certains auteurs ont préconisé, en conséquence, de modifier le cadre juridique pour prendre en compte les « inférences » opérées à partir des données personnelles<sup>36</sup>, plutôt que de se focaliser sur les données elles-mêmes et leur accès, comme le fait le droit dérivé de l'UE. En effet, comme il est possible d'inférer des informations sur les personnes à partir de données anonymes, la logique juridique consistant à restreindre ou encadrer l'accès aux données personnelles se révèle largement inefficace. Les auteurs invitent à changer de paradigme pour concentrer la réglementation sur l'usage des données et des connaissances inférées sur les

<sup>35</sup> M. Pégny, Pour un développement des IAs respectueux de la vie privée dès la conception. 2021. hal-03104692.

<sup>36</sup> S. Wachter et B. Mittelstadt, « A right to reasonable inferences: re-thinking data protection law in the age of big data and AI », *Colum. Bus. L. Rev.*, 2019, 494.

personnes. Force est d'admettre que le RGPD qui constitue un modèle juridique inégalé dans la protection des données à caractère personnel présente, en pratique, des limites avérées...que le projet de règlement sur l'IA n'entend pourtant pas prendre en compte.

### **III. L'équation complexe d'une IA *made in Europe* : entre protection des principes éthiques et soutien à l'innovation**

Si la nécessité d'un encadrement de l'IA ne fait pas de doute, il est impératif de trouver un point d'équilibre entre la protection des personnes physiques et la promotion de l'innovation. À cet égard, le titre V du projet contient des mesures spécifiques pour réduire la charge réglementaire des start-ups et des petites et moyennes entreprises (PME), et propose un cadre en matière de gouvernance, de surveillance et de responsabilité susceptible d'offrir un environnement contrôlé pour le développement des technologies novatrices. Ces mesures visent à aider les « petits utilisateurs » de systèmes d'IA à haut risque à se conformer aux nouvelles règles. C'est dans ce cadre juridique propice à l'innovation que sont envisagées des mesures de soutien comme les « bacs à sable réglementaires » qui constituent une nouvelle forme de contrôle réglementaire en ce qu'ils offrent un espace sûr pour l'expérimentation. L'article 53 encourage les États membres à mettre en place ces instruments afin de garantir une innovation responsable. La mise en place des bacs à sable réglementaires sur l'IA est un moyen de faciliter le développement, la mise à l'essai et la validation de systèmes d'IA innovants avant leur mise sur le marché. Ces outils ont pour objectif d'accélérer l'accès aux marchés de ces systèmes, en supprimant les obstacles pour les plus jeunes entreprises. Il est néanmoins précisé que le constat d'un risque pour la santé, la sécurité ou les droits fondamentaux, lors des tests de ces systèmes, doit donner lieu à des mesures d'atténuation immédiates et, à défaut, conduire à la suspension du processus de développement du modèle. Les participants au bac à sable réglementaire sont tenus de coopérer avec les autorités compétentes et d'agir de bonne foi pour atténuer tout risque important pour la sécurité et les droits fondamentaux susceptible de survenir au cours de l'expérimentation dans le bac à sable.

En effet, les nouvelles technologies ne sauraient se développer au détriment des individus. C'est pourquoi, la proposition de règlement de la Commission entend mettre en balance les risques de l'IA pour les personnes et la société, d'une part, et ses bénéfices socio-économiques, d'autre part. Les risques doivent ainsi être calculés en tenant compte de l'incidence sur les droits et la sécurité. L'harmonisation des législations et des innovations technologiques s'inscrit à la fois dans le respect des droits humains et la défense des intérêts commerciaux de l'UE. L'approche

adoptée par la Commission consiste à rechercher un équilibre entre des exigences minimales pour encadrer les risques liés à l'IA et l'établissement d'un cadre normatif suffisamment souple pour ne pas entraver son développement. En outre, la question des coûts de mise sur le marché ne peut être négligée. La poursuite de tels objectifs s'apparente à la recherche de la quadrature du cercle, comme tendent à le montrer les réactions contrastées suscitées par la publication du projet de règlement sur l'IA : si les associations de défense des libertés jugent le texte *laxiste* sur la garantie des droits (manque de fermeté sur l'interdiction de l'identification biométrique, multiplication des dérogations pour l'utilisation des systèmes d'IA à haut risque), entrepreneurs et investisseurs du numérique s'inquiètent de l'impact négatif de certaines obligations sur les *startups*. Les critiques formulées par les opérateurs ne sont pas à prendre à la légère car une réglementation trop contraignante et source d'incertitudes pourrait pousser les entreprises européennes à ne pas investir. Des reproches similaires ont été émis lors de l'entrée en vigueur du RGPD, dont les dispositions, axées sur la protection des droits fondamentaux, sont susceptibles de limiter le développement de certaines technologies<sup>37</sup>.

Cette tension entre protection des droits et innovation parcourt également les positions, et oppositions, des États membres à l'égard de ladite proposition. Il reste que les États européens semblent s'accorder sur le postulat de la Commission, à savoir l'existence d'un risque technologique, plus ou moins élevé, en matière d'IA. On relèvera que lors des consultations, les parties intéressées se sont, pour la plupart, prononcées en faveur de l'approche par les risques, jugée préférable à une réglementation globale de tous les systèmes d'IA. Elles ont également demandé de définir précisément les systèmes d'IA à haut et à faible risque. Sur ce dernier point, le projet de règlement mérite d'être davantage discuté puisqu'il ne définit pas positivement ce qu'il faut entendre par « système d'IA à faible risque ». En appréhendant les systèmes d'IA de façon sectorielle en fonction de leur degré de dangerosité, la Commission entend exclure, du moins encadrer rigoureusement, les systèmes d'IA classés à *haut risque*. Si l'approche est difficilement critiquable dans son principe, il est loisible d'interroger le choix des critères qui ont concrètement guidé la Commission (présence de biais, risque de discrimination, problème de transparence et de responsabilité). En outre, la notion de *haut risque* est suffisamment vague pour englober aussi bien des atteintes à l'intégrité physique des personnes que des menaces sur

<sup>37</sup> Dans le secteur de la santé, par exemple, les règles de consentement entravent le traitement des données médicales utilisées à des fins d'études

les droits fondamentaux (respect de la vie privée, droit à la dignité humaine, non-discrimination). Dans ces hypothèses, le danger n'est pas le même, même si la proposition ne semble pas appliquer un traitement différencié au niveau de l'évaluation ou de la mise sur le marché de ces systèmes. Une approche plus nuancée permettrait de garantir un niveau de sécurité plus approprié.

Au regard de la littérature foisonnante en matière d'IA, la Commission avait l'embarras du choix s'agissant des options normatives pour appréhender les systèmes d'IA : *soft law*, réglementation contraignante, approche horizontale. Elle a finalement opté pour une réglementation qui se veut équilibrée en proposant une approche normative consistant à encadrer, proportionnellement au degré d'intensité du risque, l'utilisation des systèmes d'IA. Ainsi, pour les systèmes d'IA présentant un risque faible, de simples codes de conduite, sans caractère contraignant, suffisent à encadrer les pratiques. Pour les systèmes d'IA interagissant avec les personnes physiques, ceux basés sur la détection d'émotions ou la catégorisation biométrique, une obligation d'information est prévue (article 52). Les systèmes d'IA présentant un risque élevé devraient être interdits. Si certaines pratiques sont prohibées, certains systèmes jugés à haut risque doivent être strictement réglementés. Cette approche peut être saluée dans la mesure où les bonnes intentions des opérateurs, telles qu'elles peuvent découler de l'adhésion à des chartes éthiques, ne sauraient suffire à changer les pratiques habituelles. La protection des usagers passe nécessairement par l'adoption d'un règlement visant à encadrer l'utilisation des systèmes d'IA et contraindre les concepteurs à respecter des exigences minimales.

Bien que la Commission ait cherché à adopter, au plan technologique, une certaine neutralité — comme l'atteste sa définition large et évolutive des systèmes logiciels — la classification pyramidale qu'elle opère, s'agissant des possibles menaces liées à l'usage de certains systèmes d'IA, révèle des positions très tranchées. L'approche par les risques entend se fonder sur la potentialité du préjudice subi par les personnes physiques. L'interdiction a pour fondement un dommage éventuel (non réalisé), ce qui pose la question de son appréciation. L'opportunité d'une approche aussi dogmatique peut être discutée dans la mesure où cette position *a priori* pourrait priver l'UE de certaines pratiques avantageuses. La position de la Commission est néanmoins parfaitement assumée en ce qu'elle se veut protectrice des personnes et des droits fondamentaux : l'interdiction des systèmes de notation sociale (scoring social) en témoigne (article 5). Il importe de souligner que cette interdiction ne semblait, à l'origine, destinée qu'aux

autorités publiques, les autres acteurs n'y étant, dans la version présentée par la Commission, apparemment pas assujettis. Or, dans un texte de compromis de novembre 2021<sup>38</sup>, la présidence slovène du Conseil de l'UE a proposé d'étendre ladite interdiction aux entités privées<sup>39</sup>. S'agissant de l'interdiction des systèmes d'identification biométrique à distance, des exceptions sont possibles lorsque ces systèmes sont utilisés par des autorités publiques en matière pénale. Ces dérogations risquent de vider le régime de l'interdiction de sa substance. La doctrine n'a pas manqué de critiquer le manque de justification de la Commission sur cet aspect<sup>40</sup>. De nombreuses autorités, comme le Comité européen de la protection des données ou le contrôleur européen de la protection des données, ont appelé à un régime plus conséquent et des interdictions plus fermes<sup>41</sup>.

En toute hypothèse, la proposition de la Commission offre un cadre juridique assez incertain pour le développement des systèmes d'IA. Comme le texte n'est pas définitif, la question du choix des critères et du manque de clarté des qualifications adoptées ne manquera pas de se poser. Il reste que si l'approche par les risques se justifie, dans le contexte politique et juridique de l'UE, cette vision n'est pas dépourvue d'idéologie. Les principes éthiques et plus largement axiologiques sont au cœur de la réflexion de la Commission comme l'atteste le considérant 15 du projet de règlement qui indique que si l'IA peut être utilisée à des fins positives, « cette technologie peut aussi être utilisée à mauvais escient et fournir des outils nouveaux et puissants à l'appui de pratiques de manipulation, d'exploitation et de contrôle social (...) contraires aux valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'état de droit ». Le cadre normatif proposé par la Commission se situe assurément au confluent de l'éthique et du droit, ce qui est, en termes de stratégie, le moyen le plus habile pour favoriser son adoption par les citoyens européens. En effet, le développement de l'IA en Europe est subordonné à son acceptabilité et celle-ci n'est possible que si les systèmes d'IA sont jugés dignes de confiance. Pour que l'UE ait une chance d'être un acteur de

<sup>38</sup> <https://data.consilium.europa.eu/doc/document/ST-13802-2021-REV-1/en/pdf>

<sup>39</sup> Un tel changement pourrait avoir des conséquences pour le secteur bancaire et financier dans la mesure où les prêts sont calculés en fonction du risque de non-remboursement. D'autant plus que le Conseil a étendu la définition pour inclure l'exploitation d'une « situation sociale ou économique ». Une distinction existe néanmoins entre la notation sociale (interdite) et les pratiques d'évaluation des personnes (autorisées), même si l'évaluation d'un individu pour déterminer sa solvabilité ou son éligibilité à un contrat d'assurance mérite une attention particulière en raison des potentiels biais discriminatoires présents dans les algorithmes.

<sup>40</sup> <https://blog.leclubdesjuristes.com/artificial-intelligence-act-lunion-europeenne-invente-la-pyramide-des-risques-de-lintelligence-artificielle/>

<sup>41</sup> [https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en). Voir aussi l'avis de la CNCDH du 7 avril 2022 : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045593731>.

premier plan en matière d'innovation, il est indispensable que l'IA *made in Europe* se démarque des modèles concurrents d'IA en promouvant un cadre réglementaire qui favorise un « écosystème de confiance unique en son genre », pour reprendre une formule tirée du livre blanc de l'IA. On relèvera toutefois que la Chine a récemment adopté une stratégie similaire, en se dotant d'une réglementation, entrée en vigueur en mars 2022, visant à encadrer strictement les algorithmes<sup>42</sup>. Celle-ci vise à promouvoir les innovations technologiques en matière d'IA tout en veillant à prévenir les abus et la mauvaise utilisation des technologies de recommandation algorithmique. Avec ce nouveau cadre normatif, la Chine est l'un des premiers États à réglementer les systèmes algorithmiques en exigeant que leurs utilisateurs respectent les principes éthiques de transparence et d'explicabilité. La question de la faisabilité technique de la législation chinoise, des recours possibles en cas de violation et, plus généralement, celle de son respect, non seulement par les entreprises mais aussi par le gouvernement, demeure un enjeu considérable<sup>43</sup>.

Sur le plan sociétal de l'éthique de l'IA, il semblerait que l'UE puisse se démarquer des modèles chinois et russes en se prononçant contre une interdiction absolue des systèmes de reconnaissance faciale et biométrique à distance, cette technologie étant abondamment utilisée par les gouvernements de Beijing et de Moscou<sup>44</sup>. Telle ne semble pas être la voie choisie à l'heure actuelle, l'UE ayant opté pour un compromis - critiqué par les organisations de protection des droits de l'homme<sup>45</sup> - entre les intérêts des citoyens et ceux des gouvernements qui prétendent avoir besoin de cette technologie innovante pour améliorer la lutte contre la criminalité et le terrorisme.

*Last but not least*, l'IA « *made in Europe* » devrait prendre en compte l'impact environnemental dans la mesure où la transition numérique va de pair avec la transition verte. Si l'essor du numérique peut nous aider à réduire l'empreinte carbone, il arrive que les technologies consomment plus d'énergie qu'elles n'en économisent. On peut regretter, à cet égard, que l'éthique environnementale occupe une place anecdotique dans le projet de règlement de la

<sup>42</sup> *Provisions on the Management of Algorithmic Recommendations for Internet Information Services* (« Algorithm Provisions », January 4, 2022) ; *Draft Provisions on the Management of Deep Synthesis in Internet Information Service* (« Draft Deep Synthesis Provisions », January 28, 2022).

<sup>43</sup> Les experts doutent que la Chine renonce à une technologie aussi efficace que la reconnaissance faciale. <https://www.techtarget.com/searchenterpriseai/news/252514781/Chinas-AI-regulations-face-technical-challenge>.

<sup>44</sup> J. Nocetti, The outsider Russia in the race for Artificial Intelligence, December 2020. Russia/NIS Center. Études de l'Ifri. Reports 34. Disponible en ligne : [https://www.ifri.org/sites/default/files/atoms/files/nocetti\\_russia\\_artificial\\_intelligence\\_2020.pdf](https://www.ifri.org/sites/default/files/atoms/files/nocetti_russia_artificial_intelligence_2020.pdf)

<sup>45</sup> <https://www.ldh-france.org/la-commission-europeenne-doit-interdire-les-pratiques-de-surveillance-de-masse-biometrique/>

Commission<sup>46</sup>. Afin d'encourager la frugalité numérique, les coûts environnementaux générés par certaines applications de l'IA devraient également être rangés dans la balance bénéfices-risques.

---

<sup>46</sup> Au-delà des considérants du règlement qui se bornent à évoquer la question de la durabilité environnementale, l'article 69 indique qu'il faut encourager l'élaboration de codes de conduite destinés à favoriser l'application volontaire aux systèmes d'IA d'exigences liées, par exemple, à la viabilité environnementale. Mais il n'y a pas de dispositions contraignantes en ce sens.