COMMISSION
EUROPÉENNE

Bruxelles, le 19.2.2020
COM(2020) 65 final

LIVRE BLANC

Intelligence artificielle

Une approche européenne axée sur l'excellence et la confiance

Livre blanc sur l'intelligence artificielle
Une approche européenne axée sur l'excellence et la confiance

L'intelligence artificielle (IA) se développe rapidement. Elle va entraîner des changements dans nos vies en améliorant les soins de santé (précision accrue des diagnostics ou meilleure prévention des maladies, par exemple), en rendant l'agriculture plus efficiente, en contribuant à l'adaptation au changement climatique et à l'atténuation de ses effets, en augmentant l'efficacité des systèmes de production par la maintenance prédictive, en renforçant la sécurité des Européens et de bien d'autres façons que nous commençons à peine à entrevoir. Mais elle s'accompagne aussi d'un certain nombre de risques potentiels, tels que l'opacité de la prise de décisions, la discrimination fondée sur le sexe ou sur d'autres motifs, l'intrusion dans nos vies privées ou encore l'utilisation à des fins criminelles.

Dans un contexte de vive concurrence mondiale, il convient d'adopter une approche européenne solide, fondée sur la stratégie européenne pour l'IA présentée en avril 2018[1]. Pour tirer le meilleur parti possible des opportunités qu'offre l'IA et relever les défis qu'elle pose, l'UE doit se montrer unie dans l'action et définir une manière qui lui est propre de promouvoir le développement et le déploiement de l'IA, en s'appuyant sur les valeurs européennes.

La Commission est résolue à favoriser les avancées scientifiques, à préserver l'avance technologique de l'UE et à faire en sorte que les nouvelles technologies soient au service de tous les Européens — c'est-à-dire qu'elles améliorent leur quotidien tout en respectant leurs droits.

M[me] Ursula von der Leyen, présidente de la Commission, a annoncé dans ses orientations politiques[2] une approche européenne coordonnée relative aux implications humaines et éthiques de l'IA, ainsi qu'une réflexion sur une meilleure utilisation des mégadonnées pour promouvoir l'innovation.

La Commission prône donc une approche axée sur la régulation et l'investissement, qui poursuit le double objectif de promouvoir le recours à l'IA et de tenir compte des risques associés à certaines utilisations de cette nouvelle technologie. Le présent Livre blanc vise à définir des options stratégiques concernant la manière d'atteindre ces objectifs. Il ne traite pas du développement et de l'utilisation de l'IA à des fins militaires. La Commission invite les États membres, les autres institutions européennes et toutes les parties prenantes, y compris les entreprises, les partenaires sociaux, les organisations de la société civile, les chercheurs, le public en général et toute partie intéressée, à réagir aux options présentées ci-dessous et à contribuer à la prise de décision future de la Commission dans ce domaine.

1. INTRODUCTION

Étant donné que la technologie numérique occupe une place de plus en plus centrale dans tous les aspects de la vie des citoyens, il faut que ces derniers puissent lui faire confiance. Elle ne pourra être adoptée que si elle est digne de confiance. C'est une chance pour l'Europe, qui est profondément attachée aux valeurs et à l'état de droit et possède une capacité avérée à fabriquer des produits et fournir des services complexes, sûrs et fiables, dans des secteurs aussi divers que l'aéronautique, l'énergie, l'automobile et les équipements médicaux.

La croissance économique et le bien-être sociétal actuels et futurs de l'Europe reposent de plus en plus sur la valeur créée par les données. L'IA est l'une des plus importantes applications de l'économie

[1] L'intelligence artificielle pour l'Europe, COM(2018) 237 final
[2] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_fr.pdf

fondée sur les données. Aujourd'hui, la plupart des données sont liées aux consommateurs et elles sont stockées et traitées dans une infrastructure centralisée dans le nuage. Demain, en revanche, les données seront beaucoup plus abondantes et une grande partie d'entre elles proviendra de l'industrie, des entreprises et du secteur public, et sera stockée sur des systèmes très divers, notamment des calculateurs situés en périphérie de réseau. Cela ouvre de nouvelles perspectives pour l'Europe, qui occupe une position de premier plan dans le secteur des applications industrielles et interentreprises numérisées, mais qui affiche une relative faiblesse dans le domaine des plateformes pour consommateurs.

En termes simples, l'IA associe des technologies qui combinent données, algorithmes et puissance de calcul. Les progrès en matière de calcul et la disponibilité croissante des données sont donc des moteurs essentiels de l'essor actuel de l'IA. L'Europe peut combiner ses atouts technologiques et industriels avec une infrastructure numérique de haute qualité et un cadre réglementaire fondé sur ses valeurs fondamentales pour **devenir un acteur mondial de premier plan en matière d'innovation dans l'économie fondée sur les données et dans ses applications**, comme indiqué dans la stratégie européenne pour les données[3]. Sur cette base, elle peut mettre en place un écosystème d'IA qui fera bénéficier l'ensemble de la société et de l'économie européennes des avantages de la technologie:

- pour les **citoyens**, cela se traduira, par exemple, par des soins de santé de meilleure qualité, des appareils ménagers moins souvent en panne, des systèmes de transport plus sûrs et plus propres, et des services publics améliorés;
- les **entreprises**, pour leur part, pourront par exemple développer une nouvelle génération de produits et de services dans les domaines où l'Europe a une longueur d'avance (construction mécanique, transports, cybersécurité, agriculture, économie verte et circulaire, soins de santé et secteurs à forte valeur ajoutée tels que la mode et le tourisme); et
- dans le domaine des services d'**intérêt public**, par exemple, les coûts de fourniture de services (transports, éducation, énergie et gestion des déchets) seront réduits, la durabilité des produits sera améliorée[4] et les services répressifs disposeront d'outils appropriés pour assurer la sécurité des citoyens[5], avec des garanties adéquates en matière de respect des droits et des libertés.

Compte tenu de l'incidence potentiellement considérable de l'IA sur notre société et de la nécessité d'instaurer la confiance, il est capital que l'IA européenne soit fondée sur nos valeurs et nos droits fondamentaux, tels que la dignité humaine et la protection de la vie privée.

Il faut en outre considérer les incidences des systèmes d'IA non seulement du point de vue de l'individu mais aussi du point de vue de la société dans son ensemble. L'utilisation des systèmes d'IA peut jouer un rôle considérable dans la réalisation des objectifs de développement durable, et en ce qui concerne le soutien du processus démocratique et des droits sociaux. Avec les propositions qu'elle a formulées récemment dans le pacte vert pour l'Europe[6], l'UE montre l'exemple pour ce qui est de

[3] COM(2020) 66 final.

[4] L'IA et la transformation numérique en général sont essentiels à la réalisation des ambitions que l'Europe s'est fixées dans le cadre de son pacte vert. Toutefois, l'empreinte environnementale actuelle du secteur des TIC est estimée à plus de 2 % de l'ensemble des émissions mondiales. La stratégie numérique européenne qui accompagne le présent Livre blanc propose des mesures en faveur de la transformation verte du secteur du numérique.

[5] L'IA peut fournir des outils permettant de mieux protéger les Européens contre les actes criminels et terroristes. Ces outils pourraient, par exemple, permettre de détecter la propagande terroriste en ligne, de mettre au jour des transactions suspectes dans la vente de produits dangereux, d'identifier des objets cachés ou des substances ou produits illicites dangereux, de prêter assistance aux citoyens en cas d'urgence et de guider les premiers intervenants.

[6] COM(2019) 640 final.

relever les défis climatiques et ceux liés à l'environnement. Les technologies numériques telles que l'IA sont des facteurs déterminants pour atteindre les objectifs fixés dans le cadre du pacte vert. L'importance de l'IA ne cessant de croître, il faut dûment tenir compte de l'incidence environnementale des systèmes d'IA tout au long de leur cycle de vie et sur l'ensemble de la chaîne d'approvisionnement, c'est-à-dire en ce qui concerne l'utilisation des ressources pour l'entraînement des algorithmes et le stockage des données.

Il faut adopter une approche européenne commune en matière d'IA pour parvenir à une échelle suffisante et éviter la fragmentation du marché unique. La mise en place d'initiatives à l'échelle nationale pourrait nuire à la sécurité juridique, affaiblir la confiance des citoyens et empêcher l'apparition d'une industrie européenne dynamique.

Le présent Livre blanc expose des options qui permettront un développement sûr et digne de confiance de l'IA en Europe, dans le plein respect des valeurs et des droits des citoyens européens. Ses principaux piliers sont les suivants:

- Le cadre de politique publique définissant les mesures destinées à harmoniser les efforts aux niveaux européen, national et régional. Par un partenariat entre les secteurs privé et public, le cadre vise à mobiliser des ressources pour parvenir à un «**écosystème d'excellence**» tout au long de la chaîne de valeur, en commençant par la recherche et l'innovation, et à créer les incitations appropriées pour accélérer l'adoption de solutions fondées sur l'IA, notamment par les petites et moyennes entreprises (PME).
- Les éléments clés d'un futur cadre réglementaire pour l'IA en Europe, qui créera un «**écosystème de confiance**» unique en son genre. Pour ce faire, il devra garantir le respect des règles de l'UE, notamment celles qui protègent les droits fondamentaux et les droits des consommateurs, en particulier pour les systèmes d'IA à haut risque exploités dans l'UE[7]. La création d'un écosystème de confiance est un objectif stratégique en soi, qui devrait susciter chez les citoyens la confiance nécessaire pour adopter les applications d'IA et donner aux entreprises et aux organismes du secteur public la sécurité juridique voulue pour innover au moyen de l'IA. La Commission soutient fermement l'approche décrite dans la communication intitulée: «Renforcer la confiance dans l'intelligence artificielle axée sur le facteur humain»[8], et elle tiendra également compte des contributions obtenues lors de la phase pilote des lignes directrices en matière d'éthique élaborées par le groupe d'experts de haut niveau sur l'IA.

La stratégie européenne pour les données, qui accompagne le présent Livre blanc, vise à permettre à l'Europe de devenir l'économie tirant parti de ses données la plus attrayante, la plus sûre et la plus dynamique au monde, en mettant à sa disposition des données qui contribueront à améliorer, d'une part, les processus de décision et, d'autre part, la qualité de vie de tous ses citoyens. Cette stratégie définit un certain nombre de mesures, notamment en ce qui concerne la mobilisation des investissements privés et publics, nécessaires pour atteindre cet objectif. Enfin, les implications de l'IA, de l'internet des objets et d'autres technologies numériques pour la législation en matière de sécurité et de responsabilité sont analysées dans le rapport de la Commission accompagnant le présent Livre blanc.

[7]Même si d'autres dispositions doivent être mises en place pour prévenir et lutter contre l'utilisation abusive de l'IA à des fins criminelles, elles ne relèvent pas du présent Livre blanc.
[8] COM(2019) 168.

2. TIRER PARTI DES ATOUTS EXISTANTS SUR LES MARCHÉS INDUSTRIELS ET PROFESSIONNELS

L'Europe est bien placée pour tirer parti du potentiel de l'IA, non seulement en tant qu'utilisatrice, mais aussi en tant que créatrice et productrice de cette technologie. Elle dispose d'excellents centres de recherche et de start ups innovantes, occupe une position de premier plan au niveau mondial en ce qui concerne la robotique et possède en outre des secteurs manufacturier et de fourniture de services compétitifs, dans des domaines aussi divers que l'automobile, les soins de santé, l'énergie, les services financiers ou l'agriculture. Elle a également mis en place une solide infrastructure de calcul (ordinateurs à haute performance), qui est essentielle au fonctionnement de l'IA. L'Europe détient en outre d'importants volumes de données publiques et industrielles, dont le potentiel est actuellement sous-exploité. Sa supériorité industrielle est reconnue dans le domaine des systèmes numériques sûrs et fiables à faible consommation d'énergie, qui sont essentiels à la poursuite du développement de l'IA.

Exploiter la capacité de l'UE à investir dans les technologies et infrastructures de nouvelle génération, ainsi que dans les compétences numériques telles que l'éducation aux données, renforcera la souveraineté technologique de l'Europe en matière de technologies et infrastructures clés génériques pour l'économie des données. Les infrastructures devraient aider à créer des réserves européennes communes de données à partir desquelles on pourrait développer une IA digne de confiance, c'est-à-dire fondée sur les valeurs et les règles européennes.

L'Europe devrait tirer parti de ses atouts pour renforcer sa position dans les écosystèmes et tout au long de la chaîne de valeur, de certains secteurs de fabrication du matériel jusqu'aux services en passant par le logiciel. C'est déjà le cas dans une certaine mesure. L'Europe produit plus d'un quart de tous les robots industriels et robots de service professionnels (par exemple, pour l'agriculture de précision, la sécurité, la santé et la logistique), et joue un rôle important dans le développement et l'utilisation d'applications logicielles destinées aux entreprises et aux organisations (applications interentreprises telles que les logiciels de planification des ressources de l'entreprise, de conception et d'ingénierie), et d'applications permettant de soutenir l'administration en ligne et l'«entreprise intelligente».

L'Europe est à la pointe du déploiement de l'IA dans l'industrie manufacturière. Plus de la moitié des grandes entreprises du secteur manufacturier ont intégré au moins un élément d'IA à leur processus de production[9].

La recherche européenne doit sa force, en partie, au programme de financement de l'UE qui a permis d'agir de manière concertée, d'éviter les doubles emplois et de mobiliser des investissements publics et privés dans les États membres par effet de levier. Au cours des trois dernières années, le financement de l'UE en faveur de la recherche et de l'innovation dans le domaine de l'IA a atteint 1,5 milliard d'euros, soit une augmentation de 70 % par rapport à la période précédente.

Toutefois, le montant des investissements consacrés à la recherche et à l'innovation en Europe reste bien inférieur aux investissements publics et privés alloués à ce domaine dans d'autres régions du monde. Quelque 3,2 milliards d'euros ont été investis dans l'IA en Europe en 2016, contre environ 12,1 milliards d'euros en Amérique du Nord et 6,5 milliards d'euros en Asie[10]. L'Europe doit réagir en augmentant considérablement ses niveaux d'investissement. Le plan coordonné dans le domaine de l'intelligence artificielle[11] mis au point avec les États membres est un bon point de départ pour

[9] Devant le Japon (30 %) et les États-Unis (28 %). Source: Cap Gemini (2019).
[10] "10 imperatives for Europe in the age of AI and automation", McKinsey, 2017.
[11] COM(2018) 795.

renforcer la coopération en matière d'IA en Europe et créer des synergies permettant de maximiser les investissements dans la chaîne de valeur de l'IA.

3. SAISIR LES OPPORTUNITÉS FUTURES: PRENDRE LA NOUVELLE VAGUE DE DONNÉES

Actuellement, l'Europe affiche certes une relative faiblesse dans le domaine des applications pour consommateurs et des plateformes en ligne, ce qui constitue un désavantage concurrentiel pour l'accès aux données, mais d'importants changements se préparent en ce qui concerne la valeur des données et leur réutilisation transsectorielle. Le volume des données produites dans le monde augmente rapidement et devrait passer de 33 zettaoctets en 2018 à 175 zettaoctets en 2025[12]. Chaque nouvelle vague de données représente, pour l'Europe, une occasion de prendre la première place mondiale dans l'économie tirant parti des données. En outre, les modes de stockage et de traitement des données vont connaître des bouleversements radicaux au cours des cinq prochaines années. À l'heure actuelle, 80 % des opérations de traitement et d'analyse des données qui ont lieu dans le nuage se déroulent dans des centres de données et des installations informatiques centralisées, et 20 % dans des objets connectés intelligents, tels que des voitures, des appareils domestiques ou des robots industriels, ainsi que dans des installations informatiques proches de l'utilisateur (*edge computing* ou traitement des données à la périphérie). D'ici à 2025, ces proportions sont appelées à changer dans une mesure considérable.[13].

L'Europe occupe le premier rang mondial dans le domaine de l'électronique de faible puissance, une technique essentielle pour la prochaine génération de processeurs spécialisés pour l'IA. Or, ce dernier marché est actuellement dominé par des acteurs extérieurs à l'UE. Des projets tels que l'initiative relative à un processeur européen, qui porte sur le développement de systèmes informatiques de faible puissance tant pour le calcul à haute performance de nouvelle génération que pour le traitement des données à la périphérie, et l'entreprise commune pour la technologie numérique, qui devrait commencer ses travaux en 2021, pourraient changer la donne. L'Europe est également aux avant-postes en ce qui concerne les solutions neuromorphiques [14] qui conviennent parfaitement à l'automatisation des processus industriels (industrie 4.0) et des modes de transport. Elles peuvent permettre d'accroître de plusieurs ordres de grandeur l'efficacité énergétique.

Les récents progrès accomplis dans le domaine de l'informatique quantique vont entraîner des augmentations exponentielles des capacités de traitement[15]. L'Europe peut être à l'avant-garde de cette technologie grâce au niveau élevé de sa recherche universitaire en informatique quantique, ainsi qu'au très bon positionnement de l'industrie européenne dans le domaine des simulateurs quantiques et des environnements de programmation pour l'informatique quantique. Les initiatives européennes visant à accroître la disponibilité d'installations d'essai et d'expérimentation quantique rendront possible l'application de ces nouvelles solutions quantiques dans un certain nombre de secteurs industriels et universitaires.

En parallèle, l'Europe continuera à jouer un rôle de premier plan dans les fondations algorithmiques de l'IA, en s'appuyant sur sa propre excellence scientifique. Il faut jeter des ponts entre les disciplines qui, aujourd'hui, progressent séparément, telles que l'apprentissage automatique et l'apprentissage profond (caractérisées par une explicabilité limitée, la nécessité de disposer d'un volume important de données

[12] IDC, 2019.
[13] Gartner 2017.
[14] Par «solutions neuromorphiques», on entend tout système de circuits intégrés à très grande échelle qui imite les architectures neurobiologiques présentes dans le système nerveux.
[15] Les ordinateurs quantiques seront capables de traiter, en quelques fractions de seconde, des ensembles de données de taille plusieurs fois supérieure à ceux que traitent les ordinateurs actuels les plus performants, ce qui permettra le développement de nouvelles applications d'IA dans tous les secteurs.

pour entraîner les modèles et apprendre par l'intermédiaire de corrélations) et les approches symboliques (dans le cadre desquelles les règles sont créées par l'intervention humaine). Le fait de combiner un raisonnement symbolique avec des réseaux neuronaux profonds peut aider à améliorer l'explicabilité des résultats de l'IA.

4. UN ÉCOSYSTÈME D'EXCELLENCE

Pour construire un écosystème d'excellence capable de soutenir le développement et de favoriser l'adoption de l'IA dans l'ensemble de l'économie et de l'administration publique de l'UE, il faut renforcer l'action à plusieurs niveaux.

A. COOPÉRATION AVEC LES ÉTATS MEMBRES

Conformément à l'annonce faite dans le cadre de sa stratégie sur l'IA adoptée en avril 2018[16], la Commission a présenté en décembre 2018 un plan coordonné - élaboré en concertation avec les États membres - pour favoriser le développement et l'utilisation de l'IA en Europe[17].

Ce plan propose quelque 70 actions conjointes en faveur d'une coopération plus étroite et plus efficace entre les États membres et la Commission dans des domaines clés tels que la recherche, l'investissement, la commercialisation, les compétences et les talents, les données et la coopération internationale. Ce plan, dont l'exécution devrait prendre fin en 2027, fera l'objet d'un suivi et de réexamens réguliers.

L'objectif est de maximiser l'impact des investissements dans la recherche, l'innovation et le déploiement, d'évaluer les stratégies nationales en matière d'IA, de s'inspirer du plan coordonné dans le domaine de l'IA avec les États membres et de le développer:

- *Action 1: en tenant compte des résultats de la consultation publique sur le Livre blanc, la Commission proposera aux États membres une révision du plan coordonné en vue d'une adoption d'ici à la fin 2020.*

Le financement au niveau de l'UE dans le domaine de l'IA devrait permettre d'attirer et de mutualiser les investissements dans des domaines où l'action requise va au-delà de ce qu'un État membre peut réaliser seul. L'objectif est d'attirer, dans l'UE, un montant total de plus de 20 milliards d'euros[18] d'investissements par an dans l'IA au cours de la prochaine décennie. Pour stimuler les investissements publics et privés, l'UE mettra à disposition des fonds au titre du programme pour une Europe numérique, du programme Horizon Europe et des Fonds structurels et d'investissement européens afin de répondre aux besoins des régions moins développées et des zones rurales.

Le plan coordonné pourrait également placer le bien-être sociétal et environnemental au nombre des principes fondamentaux de l'IA. La contribution des systèmes d'IA à la résolution des problèmes les plus urgents, tels que le changement climatique et la détérioration de l'environnement, est prometteuse. Cela doit impérativement se faire d'une manière qui soit respectueuse de l'environnement. L'IA peut et devrait procéder elle-même à un examen critique de l'utilisation des ressources et de la consommation d'énergie et être entraînée à prendre des décisions ayant des effets positifs pour l'environnement. La Commission envisagera, avec les États membres, des options visant à favoriser et à promouvoir les solutions d'IA qui correspondent à ces critères.

[16] L'intelligence artificielle pour l'Europe, COM(2018) 237.
[17] Un plan coordonné dans le domaine de l'intelligence artificielle, COM (2018) 795.
[18] COM(2018) 237.

B. CIBLER LES EFFORTS DE LA COMMUNAUTÉ DE LA RECHERCHE ET DE L'INNOVATION

L'Europe ne peut plus se satisfaire de la situation actuelle, caractérisée par une fragmentation telle qu'aucun des centres de compétence n'atteint la taille nécessaire pour rivaliser au niveau mondial avec les instituts les plus éminents. Il est impératif de créer davantage de synergies et de réseaux entre les multiples centres de recherche européens sur l'IA et d'harmoniser leurs efforts en vue d'améliorer l'excellence, de retenir et d'attirer les meilleurs chercheurs et de développer les meilleures technologies. L'Europe doit se doter d'un centre «phare» de la recherche, de l'innovation et de l'expertise qui coordonnerait ces efforts, qui constituerait une référence mondiale en matière d'excellence dans le domaine de l'IA et qui serait en mesure d'attirer les investissements et les chercheurs les plus talentueux de la discipline.

Les centres et les réseaux devraient se concentrer sur les secteurs dans lesquels l'Europe a le potentiel nécessaire pour devenir un champion mondial, tels que l'industrie, la santé, les transports, la finance, les chaînes de valeur agroalimentaires, l'énergie/l'environnement, la sylviculture, l'observation de la terre et l'espace. Dans tous ces domaines, la course au leadership mondial est lancée, et l'Europe dispose d'un potentiel, de connaissances et d'une expertise considérables[19]. La création de sites d'essai et d'expérimentation destinés à appuyer le développement et le déploiement ultérieur d'applications d'IA novatrices est tout aussi importante.

- *Action 2: la Commission facilitera la création de centres d'essai et d'excellence faisant appel à des investissements européens, nationaux et privés, y compris éventuellement un nouvel instrument juridique. La Commission a proposé de consacrer un montant ambitieux au soutien de centres d'essai de calibre mondial établis en Europe dans le cadre du programme pour une Europe numérique et de compléter ces mesures, le cas échéant, par des actions de recherche et d'innovation dans le cadre du programme Horizon Europe au titre du cadre financier pluriannuel pour la période 2021-2027.*

C. COMPÉTENCES

L'approche européenne en matière d'IA devra aller de pair avec une action résolument axée sur les compétences afin de combler les déficits dans ce domaine[20]. La Commission présentera prochainement un renforcement de la stratégie en matière de compétences, qui vise à faire en sorte que tous les Européens puissent bénéficier de la transformation verte et du virage numérique de l'économie de l'UE. Certaines des initiatives envisagées pourraient viser à aider les régulateurs sectoriels à améliorer leurs compétences en matière d'IA, en vue d'une mise en œuvre efficace et efficiente des règles pertinentes. La révision du plan d'action en matière d'éducation numérique permettra de mieux utiliser les données et les technologies fondées sur l'IA, telles que l'analyse prédictive et l'analyse de l'apprentissage, afin d'améliorer les systèmes d'enseignement et de formation et de les adapter à l'ère numérique. Le plan vise aussi à accroître la sensibilisation à l'IA à tous les niveaux d'enseignement afin de préparer les citoyens à des décisions de plus en plus influencées par l'IA.

Le développement des compétences nécessaires pour travailler dans le domaine de l'IA et la mise à niveau des compétences de la main-d'œuvre pour s'adapter à la transformation induite par l'IA figureront parmi les priorités de la révision du plan coordonné sur l'IA qui sera élaborée avec les États

[19] Le futur Fonds européen de la défense et la coopération structurée permanente offriront également des possibilités de recherche et de développement dans le domaine de l'IA. Il conviendra de synchroniser ces projets avec les programmes civils européens de plus large portée consacrés à l'IA.

[20] https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu

membres. Ce plan pourrait aussi prévoir de transformer la liste d'évaluation des lignes directrices en matière d'éthique en un «programme» indicatif destiné aux développeurs de l'IA qui deviendrait une ressource mise à la disposition des établissements de formation. Il conviendra d'entreprendre des efforts particuliers pour augmenter le nombre de femmes formées et employées dans ce domaine.

En outre, un centre «phare» pour la recherche et l'innovation en matière d'IA en Europe attirerait des chercheurs talentueux du monde entier en raison des possibilités qu'il pourrait offrir. Il permettrait également d'accroître et de diffuser l'excellence dans les compétences qui s'implantent et se développent partout en Europe.

- *Action 3: mettre en place et soutenir, par l'intermédiaire du pilier «compétences avancées» du programme pour une Europe numérique, des réseaux d'universités et d'établissements d'enseignement supérieur de premier plan pour attirer les meilleurs professeurs et chercheurs et proposer des programmes de masters de classe internationale dans le domaine de l'IA.*

Outre la mise à niveau des compétences qu'elles nécessitent, la conception et l'utilisation des systèmes d'IA dans l'environnement de travail ont aussi une incidence directe sur les employeurs et les travailleurs. La participation des partenaires sociaux revêtira une importance capitale pour garantir une approche axée sur le facteur humain de l'IA au travail.

D. ACCORDER UNE PLACE DE CHOIX AUX PME

Il sera également important de veiller à ce que les PME puissent avoir accès à l'IA et l'utiliser. Pour ce faire, il conviendra de renforcer encore les pôles d'innovation numérique[21] et la plateforme d'IA à la demande[22] et d'encourager la collaboration entre les PME. Ces objectifs pourront être atteints au moyen du programme pour une Europe numérique. Tous les pôles d'innovation numérique devraient aider les PME à comprendre et à adopter l'IA, mais il importe qu'au moins un pôle d'innovation par État membre ait un niveau élevé de spécialisation en IA.

Les PME et les start ups auront besoin d'un accès au financement pour adapter leurs processus ou pour innover en utilisant l'IA. Avec le futur fonds d'investissement pilote de 100 millions d'euros dans le domaine de l'IA et de la chaîne de blocs, la Commission prévoit d'améliorer encore l'accès au financement dans le domaine de l'IA au titre d'InvestEU[23]. L'IA est explicitement mentionnée parmi les domaines éligibles pour l'utilisation de la garantie InvestEU.

- *Action 4: la Commission collaborera avec les États membres pour faire en sorte qu'au moins un pôle d'innovation numérique par État membre ait un niveau élevé de spécialisation en IA. Les pôles d'innovation numérique peuvent bénéficier d'un soutien dans le cadre du programme pour une Europe numérique.*
- *La Commission et le Fonds européen d'investissement lanceront, au premier trimestre 2020, un programme pilote de 100 millions d'euros afin de fournir un financement en fonds propres aux développements innovants dans le domaine de l'IA. Sous réserve de l'accord final sur le CFP, la Commission a l'intention de développer considérablement cet instrument à partir de 2021 par l'intermédiaire d'InvestEU.*

[21] ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.
[22] www.Ai4eu.eu.
[23] Europe.eu/investeu.

E. PARTENARIAT AVEC LE SECTEUR PRIVÉ

Il est également essentiel de veiller à ce que le secteur privé soit pleinement associé à la définition du programme de recherche et d'innovation et que les co-investissements qu'il fournit atteignent le niveau requis. Pour ce faire, il faut mettre en place un partenariat public-privé de grande envergure et s'assurer de l'adhésion au projet des dirigeants des entreprises.

- *Action 5: dans le contexte d'Horizon Europe, la Commission mettra en place un nouveau partenariat public-privé dans le domaine de l'IA, des données et de la robotique afin de conjuguer les efforts, d'assurer la coordination de la recherche et de l'innovation dans le domaine de l'IA, de coopérer avec d'autres partenariats public-privé dans le cadre du programme Horizon Europe et de collaborer avec les installations d'essai et les pôles d'innovation numérique susmentionnés.*

F. ENCOURAGER LE SECTEUR PUBLIC À ADOPTER L'IA

Il est essentiel que les administrations publiques, les hôpitaux, les services d'utilité publique et de transport, les autorités de surveillance financière et d'autres domaines d'intérêt public commencent rapidement à déployer dans leurs activités des produits et des services fondés sur l'IA. Les domaines de la santé et des transports, notamment, feront l'objet d'une attention particulière car, dans ces secteurs, la technologie est parvenue à la maturité nécessaire à un déploiement à grande échelle.

- *Action 6: la Commission entamera des dialogues sectoriels ouverts et transparents, en accordant la priorité aux prestataires de soins de santé et aux opérateurs de service public, afin de présenter un plan d'action pour faciliter le développement, l'expérimentation et l'adoption. Les dialogues sectoriels serviront à élaborer un programme spécifique consacré à l'adoption de l'IA qui soutiendra les marchés publics portant sur des systèmes d'IA et contribuera à transformer les processus de passation de marchés publics proprement dits.*

G. GARANTIR L'ACCÈS AUX DONNÉES ET AUX INFRASTRUCTURES DE CALCUL

Les domaines d'action définis dans le présent Livre blanc complètent le plan présenté en parallèle dans le cadre de la stratégie européenne pour les données. L'amélioration de l'accès aux données et de leur gestion revêt une importance fondamentale. Sans données, il est impossible de développer des applications d'IA et d'autres applications numériques. L'énorme volume de nouvelles données qui va être généré à l'avenir donne à l'Europe l'occasion de se placer aux avant-postes de la transformation des données et de l'intelligence artificielle. La promotion de pratiques responsables en matière de gestion de données et de la conformité des données aux principes FAIR contribuera à instaurer la confiance et à garantir le caractère réutilisable des données[24]. Il est tout aussi important d'investir dans les technologies et infrastructures de calcul clés.

La Commission a proposé, dans le cadre du programme pour une Europe numérique, d'affecter plus de 4 milliards d'euros au soutien de l'informatique quantique et du calcul à haute performance, et notamment du traitement des données à la périphérie et de l'IA et des infrastructures de données et en nuage. Ces priorités sont abordées plus en détail dans la stratégie européenne pour les données.

[24] Faciles à trouver, accessibles, interopérables et réutilisables (FAIR), comme indiqué dans le rapport final et dans le plan d'action du groupe d'experts de la Commission sur les données FAIR, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

H. ASPECTS INTERNATIONAUX

L'Europe est bien placée pour jouer un rôle moteur, au niveau mondial, dans la constitution d'alliances autour de valeurs partagées et dans la promotion d'une utilisation éthique de l'IA. Les travaux de l'UE sur l'IA ont déjà influencé les débats internationaux. Lors de l'élaboration de ses lignes directrices en matière d'éthique, le groupe d'experts de haut niveau a associé à ses travaux un certain nombre d'organisations non membres de l'UE et plusieurs observateurs gouvernementaux. En parallèle, l'UE a pris une part active à l'élaboration des principes éthiques de l'OCDE sur l'IA[25]. Le G20 a ensuite approuvé ces principes dans sa déclaration ministérielle de juin 2019 sur le commerce et l'économie numérique.

En parallèle, l'UE reconnaît que des travaux importants sur l'IA sont en cours dans d'autres enceintes multilatérales telles que le Conseil de l'Europe, l'Organisation des Nations unies pour l'éducation, la science et la culture (UNESCO), l'Organisation de coopération et de développement économiques (OCDE), l'Organisation mondiale du commerce et l'Union internationale des télécommunications. Au sein de l'ONU, l'UE participe au suivi du rapport du groupe de haut niveau sur la coopération numérique, et notamment de sa recommandation sur l'IA.

L'UE continuera à coopérer sur l'IA avec des partenaires partageant les mêmes valeurs, mais aussi avec des acteurs mondiaux, selon une approche qui promeut les règles et les valeurs de l'UE (par exemple, le soutien à la convergence réglementaire ascendante, l'accès aux ressources essentielles, notamment les données, ou la création de conditions de concurrence équitables). La Commission suivra attentivement les politiques des pays tiers qui limitent les flux de données et luttera contre les restrictions injustifiées dans le cadre de négociations commerciales bilatérales et en utilisant les moyens d'action fournis par l'Organisation mondiale du commerce. La Commission est convaincue que la coopération internationale sur les questions d'IA doit obéir à une approche qui promeut le respect des droits fondamentaux, notamment la dignité humaine, le pluralisme, l'inclusion, la non-discrimination et la protection de la vie privée et des données à caractère personnel[26], et s'efforcera d'exporter les valeurs de l'UE dans le monde entier[27]. Il est indéniable que le développement et l'utilisation responsables de l'IA peuvent se révéler déterminants pour réaliser les objectifs de développement durable et atteindre les buts fixés par le Programme 2030.

5. UN ÉCOSYSTÈME DE CONFIANCE: UN CADRE RÉGLEMENTAIRE POUR L'IA

À l'instar de toute technologie nouvelle, l'utilisation de l'IA crée à la fois des possibilités et des risques. Les citoyens craignent d'être impuissants à défendre leurs droits et leur sécurité lorsqu'ils sont confrontés à l'asymétrie de l'information en matière de prise de décision algorithmique, et les entreprises sont préoccupées par l'insécurité juridique. Si l'IA peut contribuer à renforcer la sécurité des citoyens et à leur permettre de jouir de leurs droits fondamentaux, elle suscite également chez eux une certaine méfiance quant à ses effets indésirables potentiels, voire à son utilisation à des fins malveillantes. Ces préoccupations doivent être prises en compte. Outre le manque d'investissement et de compétences, le déficit de confiance constitue aussi un frein considérable à un recours plus généralisé à l'IA.

[25] https://www.oecd.org/going-digital/ai/principles/

[26] Dans le cadre de l'instrument de partenariat, la Commission financera un projet de 2,5 millions d'euros qui facilitera la coopération avec des partenaires partageant les mêmes valeurs, afin de promouvoir les lignes directrices de l'UE en matière d'éthique dans le domaine de l'IA et d'adopter des principes communs et des conclusions opérationnelles.

[27] Présidente Von der Leyen, Une Union plus ambitieuse — Mon programme pour l'Europe, p. 17.

Aussi, le 25 avril 2018, la Commission a présenté une stratégie en matière d'IA[28] qui aborde les aspects socio-économiques parallèlement à l'accroissement des investissements dans la recherche, l'innovation et les capacités en matière d'IA dans l'ensemble de l'UE. Elle a établi un plan coordonné[29] avec les États membres afin d'harmoniser les stratégies. La Commission a également mis sur pied un groupe d'experts de haut niveau, qui a publié en avril 2019 des lignes directrices pour une IA digne de confiance[30].

La Commission a publié une communication[31] dans laquelle elle salue les sept exigences essentielles énumérées dans les lignes directrices du groupe d'experts de haut niveau, à savoir:

- facteur humain et contrôle humain,
- robustesse technique et sécurité,
- respect de la vie privée et gouvernance des données,
- transparence,
- diversité, non-discrimination et équité,
- bien-être sociétal et environnemental, et
- responsabilisation.

Les lignes directrices contiennent également une liste d'évaluation pratique à l'usage des entreprises. Au cours du second semestre de 2019, plus de 350 organisations l'ont utilisée à titre d'essai et ont fait part de leurs réactions. Le groupe de haut niveau procède actuellement à une révision de ses lignes directrices en fonction des réactions reçues et devrait terminer ses travaux d'ici à juin 2020. Le principal résultat de ce retour d'information est que les régimes législatifs ou réglementaires existants tiennent déjà compte d'un certain nombre d'exigences, mais que, dans de nombreux secteurs économiques, celles qui concernent la transparence, la traçabilité et le contrôle humain ne sont pas spécifiquement couvertes par la législation en vigueur.

Outre cet ensemble de lignes directrices non contraignantes du groupe de haut niveau, et conformément aux orientations politiques de la présidente, un cadre réglementaire européen clair permettrait de susciter la confiance des consommateurs et des entreprises à l'égard de l'IA et, partant, d'accélérer l'adoption de cette technologie. Ce cadre devrait être cohérent avec d'autres actions visant à promouvoir la capacité d'innovation et la compétitivité de l'Europe dans ce domaine. Il doit également produire des résultats optimaux sur les plans social, environnemental et économique et garantir le respect de la législation, des principes et des valeurs de l'UE. Cela est particulièrement important dans les domaines où des atteintes directes aux droits des citoyens sont les plus susceptibles de se produire, par exemple l'utilisation d'applications d'IA par l'appareil judiciaire et répressif.

Les développeurs et les déployeurs d'IA sont déjà soumis à la législation européenne sur les droits fondamentaux (c'est-à-dire la protection des données, le respect de la vie privée, la non-discrimination), sur la protection des consommateurs, et sur la sécurité des produits et la responsabilité du fait des produits. Les consommateurs entendent jouir du même niveau de sécurité et bénéficier des mêmes droits, qu'un produit ou un système soit fondé sur l'IA ou non. Or certaines spécificités de l'IA (telles que l'opacité) peuvent compliquer l'application et le contrôle de l'application de cette législation. Il faut, dès lors, examiner si la législation actuelle est en mesure de faire face aux risques

[28] COM(2018) 237.
[29] COM(2018) 795.
[30] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top
[31] COM(2019) 168.

liés à l'IA et si son respect peut être assuré efficacement, si elle doit être adaptée, ou si une nouvelle législation s'impose.

Compte tenu de la vitesse à laquelle évolue l'IA, le cadre réglementaire doit prévoir une marge pour d'éventuels aménagements. Les modifications éventuelles devraient se limiter à des problèmes nettement circonscrits pour lesquels il existe des solutions réalisables.

Les États membres font observer l'absence actuelle d'un cadre européen commun. La commission fédérale allemande pour l'éthique des données a préconisé un système de réglementation fondé sur cinq niveaux de risque, allant d'une absence de réglementation pour les systèmes d'IA les plus inoffensifs à une interdiction totale pour les plus dangereux. Le Danemark vient de lancer un prototype de label éthique en matière de données. Malte a mis en place un système volontaire de certification pour l'IA. Si l'UE ne se dote pas d'une approche européenne, il existe un risque réel de fragmentation du marché intérieur, ce qui porterait atteinte aux objectifs de confiance, de sécurité juridique et d'adoption par le marché.

Un cadre réglementaire européen solide pour une IA digne de confiance protégera tous les Européens et contribuera à la création d'un marché intérieur fluide en vue du développement plus poussé et de l'adoption de l'IA, ainsi qu'au renforcement de la base industrielle de l'Europe dans le domaine de l'IA.

A. DÉFINITION DU PROBLÈME

L'IA peut avoir de nombreux effets positifs, notamment en matière de renforcement de la sécurité des produits et des procédés, mais aussi des effets négatifs. Elle peut être préjudiciable tant sur le plan matériel (en matière de sécurité et de santé des personnes: pertes humaines, dommages aux biens) qu'immatériel (atteinte à la vie privée, restrictions du droit à la liberté d'expression, dignité humaine, discrimination à l'embauche par exemple), et impliquer des risques de types très divers. L'objectif d'un éventuel cadre réglementaire devrait consister à définir des moyens de réduire au minimum les divers risques de préjudice pouvant se présenter, notamment les plus sérieux.

Les principaux risques liés à l'utilisation de l'IA concernent l'application des règles visant à protéger les droits fondamentaux (notamment la protection des données à caractère personnel, le respect de la vie privée et la non-discrimination), ainsi que les questions liées à la sécurité[32] et à la responsabilité.

Risques pour les droits fondamentaux, notamment la protection des données à caractère personnel, le respect de la vie privée, et la non-discrimination

Le recours à l'IA peut porter atteinte aux valeurs sur lesquelles l'UE est fondée et entraîner des violations des droits fondamentaux[33], tels que les droits à la liberté d'expression et de réunion, la dignité humaine, l'absence de discrimination fondée sur le sexe, l'origine raciale ou ethnique, la religion ou les convictions, le handicap, l'âge ou l'orientation sexuelle, selon le cas, la protection des données à caractère personnel, le respect de la vie privée[34] ou le droit à un recours juridictionnel effectif et à un procès équitable, ainsi que la protection des consommateurs. Ces risques peuvent

[32] Il s'agit notamment de questions de cybersécurité et de problèmes liés aux applications d'IA dans les infrastructures critiques ou à l'utilisation de l'IA à des fins malveillantes.

[33] Selon les recherches du Conseil de l'Europe, l'utilisation de l'IA pourrait avoir une incidence sur de nombreux droits fondamentaux, https://rm.coe.int/algorithms-and-human-rights-fr/1680795681.

[34] Le règlement général sur la protection des données et la directive «vie privée et communications électroniques» (un nouveau règlement «vie privée et communications électroniques» est en cours de négociation) contiennent des mesures pour faire face à ces risques mais il pourrait être nécessaire d'examiner si les systèmes d'IA impliquent des risques supplémentaires. La Commission assurera un suivi et une évaluation continus de l'application du RGPD.

résulter de failles dans la conception globale des systèmes d'IA (y compris en ce qui concerne le contrôle humain) ou de l'utilisation de données sans correction de biais éventuels (par exemple, un système entraîné uniquement ou principalement avec des données tirées de profils masculins fournit de moins bons résultats en ce qui concerne les femmes).

L'IA peut remplir de nombreuses fonctions précédemment réservées aux seuls êtres humains. Par conséquent, les particuliers et les entités juridiques feront de plus en plus l'objet d'actions et de décisions prises par ou à l'aide de systèmes d'IA, qui peuvent parfois être difficiles à comprendre ou à contester efficacement si nécessaire. De plus, l'IA accroît les possibilités de suivre et d'analyser les habitudes quotidiennes des individus. Par exemple, il existe un risque potentiel que l'IA puisse être utilisée, en violation des règles de l'UE en matière de protection des données et d'autres règles, par des autorités publiques ou d'autres entités à des fins de surveillance de masse et par des employeurs pour observer le comportement de leurs employés. Dans la mesure où elle permet d'analyser de grandes quantités de données et de repérer les corrélations entre celles-ci, l'IA peut également être utilisée pour retracer et désanonymiser les données concernant certaines personnes, créant ainsi de nouveaux risques pour la protection des données à caractère personnel, même au départ d'ensembles de données qui ne contiennent pas a priori de telles données. Certains intermédiaires en ligne ont aussi recours à l'IA pour hiérarchiser certaines informations à fournir à leurs utilisateurs et pour modérer les contenus. Les données traitées, la manière dont les applications sont conçues et les possibilités d'intervention humaine peuvent porter atteinte aux droits à la liberté d'expression, à la protection des données à caractère personnel, au respect de la vie privée et aux libertés politiques.

Certains algorithmes d'IA peuvent, lorsqu'ils sont utilisés pour prédire la récidive d'actes délictueux, présenter des biais de nature sexiste et raciale et fournissent des prédictions de la probabilité de récidive différentes selon qu'il s'agit de femmes ou d'hommes ou de ressortissants nationaux ou d'étrangers. *Source: Tolan S., Miron M., Gomez E. and Castillo C., Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia", Best Paper Award, International Conference on AI and Law, 2019*

Certains programmes d'IA pour l'analyse faciale sont entachés de biais de nature sexiste ou raciale, qui se traduisent par un faible taux d'erreur dans la détermination du sexe des hommes à peau claire mais un taux d'erreur élevé dans la détermination du sexe des femmes à peau foncée. Source: *Joy Buolamwini, Timnit Gebru; Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018.*

Les biais et la discrimination sont des risques inhérents à toute activité sociétale ou économique. Les décisions prises par des humains ne sont pas à l'abri d'erreurs et de biais. Cependant, s'ils entachent l'IA, les mêmes biais pourraient avoir un effet bien plus important, entraînant des conséquences et créant des discriminations pour beaucoup de personnes en l'absence des mécanismes de contrôle social qui régissent le comportement humain[35]. Ces biais peuvent également prendre naissance lorsque le système «apprend» pendant qu'il fonctionne. Dans les cas où il aurait été impossible d'empêcher ou de prévoir l'émergence de ces biais lors de la phase de conception, les risques ne découleront pas d'une

[35] Le Comité consultatif de l'égalité des chances entre les femmes et les hommes, qui relève de la Commission, élabore actuellement un avis sur l'intelligence artificielle, qu'il devrait adopter début 2020 et dans lequel il analyse notamment les incidences de l'intelligence artificielle sur l'égalité des sexes. La stratégie de l'UE en matière d'égalité entre les hommes et les femmes (2020-2024) porte également sur le lien entre l'IA et l'égalité hommes-femmes; le réseau européen des organismes de promotion de l'égalité (Equinet) devrait publier, début 2020, un rapport de Robin Allen et Dee Masters intitulé «Regulating AI: the new role for Equality Bodies – Meeting the new challenges to equality and non-discrimination from increased digitalisation and the use of AI».

erreur dans la conception initiale du système mais seront plutôt la conséquence pratique des corrélations ou des structures repérées par le système dans un grand ensemble de données.

Les particularités qui caractérisent de nombreuses technologies de l'IA, notamment l'opacité («effet de boîte noire»), la complexité, l'imprévisibilité et le comportement partiellement autonome, peuvent rendre difficile la vérification de la conformité aux règles du droit de l'UE en vigueur destinées à protéger les droits fondamentaux et peuvent entraver le contrôle de l'application de celles-ci. Les autorités répressives et les personnes concernées ne disposent pas nécessairement de moyens suffisants pour vérifier comment une décision donnée, résultant de l'utilisation de l'IA, a été prise et, par conséquent, pour déterminer si les règles applicables ont été respectées. Les particuliers et les entités juridiques peuvent se heurter à des difficultés en ce qui concerne l'accès effectif à la justice lorsque ces décisions sont susceptibles d'avoir des effets négatifs pour eux.

Risques pour la sécurité et le bon fonctionnement du régime de responsabilité

Les technologies de l'IA peuvent présenter de nouveaux risques pour la sécurité des utilisateurs lorsqu'elles sont intégrées dans des produits et des services. Par exemple, à la suite d'une faille dans la technologie de reconnaissance des objets, une voiture autonome peut se tromper en identifiant un objet sur la route et causer un accident entraînant des lésions corporelles et des dommages matériels. Comme dans le cas des droits fondamentaux, ces risques peuvent être dus à des défauts de conception de la technologie d'IA, à des problèmes liés à la disponibilité et à la qualité des données ou à d'autres problèmes découlant de l'apprentissage automatique. Si certains de ces risques ne se limitent pas aux produits et services reposant sur l'IA, l'utilisation de celle-ci peut les accroître ou les aggraver.

L'absence de règles claires en matière de sécurité pour faire face à ces risques peut, outre les risques pour les individus concernés, créer une insécurité juridique pour les entreprises qui commercialisent leurs produits reposant sur l'IA dans l'UE. Les autorités de surveillance du marché et les autorités répressives peuvent se trouver dans une situation où elles ne savent pas si elles peuvent intervenir, parce qu'elles n'y sont peut-être pas habilitées et/ou ne disposent pas des capacités techniques appropriées pour inspecter les systèmes[36]. L'insécurité juridique risque donc de faire baisser les niveaux de sécurité globaux et de nuire à la compétitivité des entreprises européennes.

Si les risques pour la sécurité devaient se matérialiser, l'imprécision des exigences applicables et les caractéristiques précitées des technologies de l'IA rendraient difficile toute tentative de reconstituer l'historique des décisions potentiellement problématiques résultant de l'utilisation de systèmes d'IA. De ce fait, il serait ensuite difficile pour les personnes ayant subi un préjudice d'obtenir réparation au titre de la législation actuelle de l'UE et des États membres en matière de responsabilité.[37].

La directive sur la responsabilité du fait des produits prévoit qu'un fabricant est responsable des dommages causés par un produit défectueux. Or, avec un système fondé sur l'IA tel que la voiture autonome, il peut être difficile de prouver la défectuosité du produit le dommage survenu et le lien de cause à effet entre les deux. De plus, il peut être malaisé de déterminer de quelle manière et dans quelle mesure la directive sur la responsabilité du fait des produits s'applique à certains types de défauts, notamment s'ils résultent de faiblesses dans la cybersécurité du produit.

[36] Citons l'exemple des montres intelligentes pour enfants. Ce produit ne causerait pas un préjudice direct à l'enfant qui la porte, mais, en l'absence de niveau minimum de sécurité, la montre pourrait facilement être utilisée pour avoir accès à l'enfant. Les autorités de surveillance du marché peuvent éprouver des difficultés à intervenir lorsque le risque n'est pas lié au produit en tant que tel.

[37] Les implications de l'IA, de l'internet des objets et d'autres technologies numériques pour la législation en matière de sécurité et de responsabilité sont analysées dans le rapport de la Commission accompagnant le présent Livre blanc.

Par conséquent, la difficulté de reconstituer l'historique des décisions potentiellement problématiques prises par des systèmes d'IA, évoquée plus haut à propos des droits fondamentaux, concerne également les questions liées à la sécurité et à la responsabilité. Les personnes ayant subi un préjudice peuvent ne pas disposer d'un accès effectif aux éléments de preuve nécessaires pour entreprendre une action en justice, par exemple, et leurs possibilités de recours peuvent se révéler moins efficaces que dans les cas où les dommages sont causés par des technologies traditionnelles. Ces risques augmenteront avec la généralisation du recours à l'IA.

B. ADAPTATIONS POSSIBLES DU CADRE LÉGISLATIF EXISTANT DE L'UE POUR TENIR COMPTE DE L'IA

En matière de sécurité et de responsabilité des produits, il existe dans l'UE un vaste corpus législatif[38] comprenant des règles sectorielles, complété par les législations nationales, qui est pertinent et potentiellement applicable à un certain nombre d'applications d'IA qui apparaissent.

En ce qui concerne la protection des droits fondamentaux et des droits des consommateurs, le cadre législatif de l'UE comprend des dispositions législatives telles que la directive sur l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique[39], la directive sur l'égalité de traitement en matière d'emploi et de travail[40], les directives sur l'égalité de traitement entre hommes et femmes en matière d'emploi et de travail et dans l'accès à des biens et services[41], ainsi qu'un certain nombre de règles relatives à la protection des consommateurs[42] et à la protection des données à caractère personnel et au respect de la vie privée, notamment le règlement général sur la protection des données et d'autres règles sectorielles applicables à la protection des données à caractère personnel telles que la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel[43]. En outre, les règles relatives aux exigences en matière d'accessibilité applicables aux produits et services définies dans l'acte législatif européen sur l'accessibilité entreront en vigueur à partir de 2025[44]. Par ailleurs, le respect des droits fondamentaux est impératif lors de la mise en œuvre d'autres actes législatifs de l'UE, notamment dans le domaine des services financiers, de la migration ou de la responsabilité des intermédiaires en ligne.

Si la législation de l'UE reste, en principe, pleinement applicable qu'il y ait ou non recours à l'IA, il importe de déterminer si son application peut suffire à faire face aux risques créés par les systèmes d'IA ou s'il est nécessaire d'adapter certains instruments juridiques spécifiques.

Par exemple, les acteurs économiques demeurent pleinement responsables de la garantie de la conformité de l'IA aux règles en vigueur en matière de protection des consommateurs. Toute

[38] Le cadre juridique de l'UE relatif à la sécurité des produits se compose de la directive relative à la sécurité générale des produits (directive 2001/95/CE), qui constitue un filet de sécurité, et d'un certain nombre de règles sectorielles applicables à différentes catégories de produits telles que les machines, les avions, les voitures, les jouets ou les dispositifs médicaux, qui visent à assurer un niveau élevé de santé et de sécurité. La législation en matière de responsabilité du fait des produits est complétée par différents régimes de responsabilité civile pour les dommages causés par des produits ou des services.

[39] Directive 2000/43/CE.

[40] Directive 2000/78/CE.

[41] Directive 2004/113/CE. Directive 2006/54/CE.

[42] Telles que la directive relative aux pratiques commerciales déloyales (directive 2005/29/CE) et la directive relative aux droits des consommateurs (directive 2011/83/CE).

[43] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

[44] Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services.

exploitation algorithmique du comportement des consommateurs en infraction avec les dispositions existantes est interdite et les violations seront sanctionnées en conséquence.

La Commission estime que le cadre législatif pourrait être amélioré pour faire face aux risques et situations suivants:

- *Application effective et contrôle du respect de la législation existante de l'UE et des États membres*: les spécificités de l'IA créent des difficultés pour l'application correcte des législations européenne et nationale et le contrôle de leur respect. En raison du manque de transparence (opacité de l'IA), il est difficile de déceler et de prouver d'éventuelles infractions à la législation, notamment aux dispositions juridiques qui protègent les droits fondamentaux, mais aussi d'imputer la responsabilité et de remplir les conditions requises pour prétendre à une indemnisation. Par conséquent, afin de garantir une application et un contrôle du respect de la législation efficaces, il peut être nécessaire d'adapter ou de clarifier les dispositions législatives existantes dans certains domaines, par exemple en ce qui concerne la responsabilité, comme le précise le rapport qui accompagne le présent Livre blanc.

- *Limitations du champ d'application de la législation existante de l'UE*: la mise sur le marché des produits occupe une place centrale dans la législation de l'UE en matière de sécurité des produits. Si, dans la législation de l'UE relative à la sécurité des produits, le logiciel doit, lorsqu'il est intégré au produit final, être conforme aux règles applicables en matière de sécurité des produits, il reste à savoir si, en dehors de certains secteurs auxquels des règles explicites sont applicables[45], un logiciel autonome est couvert par la législation de l'UE en matière de sécurité des produits. La législation générale de l'UE en matière de sécurité actuellement en vigueur s'applique aux produits et non aux services, et donc pas non plus, en principe, aux services fondés sur la technologie de l'IA (par exemple, les services de santé, les services financiers ou les services de transport).

- *Fonctionnalités modifiées par des systèmes d'IA*: l'intégration de logiciels, notamment d'IA, dans certains produits et systèmes peut modifier le fonctionnement de ces derniers au cours de leur cycle de vie. C'est le cas, en particulier, pour les systèmes qui nécessitent de fréquentes mises à jour logicielles ou qui dépendent de l'apprentissage automatique. Ces caractéristiques peuvent créer de nouveaux risques qui n'étaient pas présents lorsque le système a été mis sur le marché. La législation existante, principalement axée sur les risques pour la sécurité présents au moment de la mise sur le marché, ne prend pas suffisamment en compte ces risques.

- *Incertitude concernant la répartition des responsabilités entre différents opérateurs économiques de la chaîne d'approvisionnement:* d'une manière générale, la législation de l'UE relative à la sécurité des produits impute la responsabilité au producteur du produit mis sur le marché et de l'ensemble de ses composants, tels que les systèmes d'IA. Mais si l'IA est ajoutée, après la mise sur le marché du produit, par une partie qui n'est pas le producteur, les règles manquent de clarté. En outre, la législation de l'UE en matière de responsabilité du fait des produits prévoit des dispositions en matière de responsabilité des producteurs et renvoie

[45] Par exemple, un logiciel destiné par le fabricant à être utilisé à des fins médicales est considéré comme un dispositif médical en vertu du règlement relatif aux dispositifs médicaux [règlement (UE) 2017/745].

aux règles nationales en matière de responsabilité pour ce qui est de la responsabilité des autres acteurs de la chaîne d'approvisionnement.

- *Modifications du concept de sécurité:* l'utilisation de l'IA dans les produits et services peut donner naissance à des risques que la législation actuelle de l'UE n'aborde pas explicitement. Il peut s'agir de risques liés aux menaces informatiques, de risques pour la sécurité des personnes (liés, par exemple, aux nouvelles applications d'IA dans le domaine des appareils domestiques), de risques résultant de la perte de connectivité, etc. Ces risques peuvent être présents au moment de la mise sur le marché des produits ou résulter de mises à jour logicielles ou de l'auto-apprentissage en cours d'utilisation du produit. L'UE devrait tirer le meilleur parti possible des outils dont elle dispose pour améliorer sa base de connaissances sur les risques potentiels liés aux applications d'IA, notamment en s'appuyant sur l'expérience de l'Agence de l'Union européenne pour la cybersécurité (ENISA) en matière d'évaluation des menaces dans le domaine de l'IA.

Comme il est précisé plus haut, plusieurs États membres étudient déjà les possibilités de légiférer au niveau national pour relever les défis posés par l'IA, ce qui accroît le risque de fragmentation du marché. Des règles nationales divergentes sont des sources d'entraves potentielles pour les entreprises qui souhaitent vendre et exploiter des systèmes d'IA dans le marché unique. L'établissement d'une approche commune au niveau de l'UE permettrait aux entreprises européennes de bénéficier d'un accès fluide au marché et favoriserait leur compétitivité sur les marchés mondiaux.

Rapport sur les implications de l'intelligence artificielle, de l'internet des objets et de la robotique en matière de sécurité et de responsabilité

Ce rapport, qui accompagne le présent Livre blanc, analyse le cadre juridique applicable. Il dresse l'inventaire des incertitudes entourant l'application de ce cadre en ce qui concerne les risques spécifiques posés par les systèmes d'IA et autres technologies numériques.

Il conclut que la législation actuelle sur la sécurité des produits offre déjà une interprétation étendue de la notion de sécurité qui permet de protéger contre tous types de risques liés aux produits en fonction de leur utilisation. Dans un souci de sécurité juridique accrue, des dispositions couvrant explicitement les nouveaux risques liés aux technologies numériques émergentes pourraient cependant être adoptées.

- Le comportement autonome de certains systèmes d'IA au cours de leur cycle de vie peut entraîner d'importantes modifications dans les produits, lesquelles peuvent influer sur la sécurité et, partant, nécessiter une nouvelle évaluation des risques. De plus, il peut être nécessaire de prévoir, par précaution, une supervision humaine tout au long du cycle de vie des produits et systèmes d'IA dès leur conception.
- Il pourrait également être envisagé d'imposer des obligations expresses aux producteurs en ce qui concerne les risques pour la sécurité mentale des utilisateurs, le cas échéant (par exemple, en cas de collaboration avec des robots humanoïdes).
- La législation de l'Union relative à la sécurité des produits pourrait contenir des exigences spécifiques concernant les risques que comportent des données erronées en matière de sécurité au stade de la conception, ainsi que des mécanismes garantissant le maintien de la qualité des données tout au long de l'utilisation des produits et systèmes d'IA.
- Des exigences en matière de transparence pourraient permettre de remédier au problème de l'opacité des systèmes fondés sur des algorithmes.
- Lorsque la sécurité est en jeu, il peut s'avérer nécessaire d'adapter et de préciser les règles actuelles dans le cas où un logiciel autonome est commercialisé tel quel ou téléchargé dans un produit après sa mise sur le marché.
- Compte tenu de la complexité croissante des chaînes d'approvisionnement du point de vue des nouvelles technologies, l'adoption d'exigences expresses de coopération entre les opérateurs économiques de la chaîne d'approvisionnement et les utilisateurs pourrait offrir une sécurité juridique.

Les caractéristiques des technologies numériques émergentes telles que l'IA, l'internet des objets et la robotique peuvent comporter des risques pour les cadres applicables en matière de responsabilité et réduire leur efficacité. Certaines de ces caractéristiques pourraient entraver la recherche d'une relation entre un préjudice et une personne, comme l'exigent la plupart des régimes nationaux reposant sur la faute. Il pourrait s'ensuivre une nette augmentation des frais à supporter par les victimes et devenir difficile d'intenter des recours en responsabilité contre d'autres parties que les producteurs et de les étayer.

- Les personnes qui ont subi un préjudice associé à des systèmes d'IA doivent bénéficier du même degré de protection que les personnes lésées par d'autres technologies, mais l'innovation technologique doit tout de même pouvoir se poursuivre.
- Une analyse approfondie de toutes les options conduisant à la réalisation de cet objectif s'impose, parmi lesquelles d'éventuelles modifications de la directive sur la responsabilité du fait des produits et la poursuite d'une harmonisation ciblée des règles nationales en matière de responsabilité. Par exemple, la Commission cherche à recueillir des idées sur la nécessité d'atténuer, et dans quelle mesure, les conséquences de la complexité en adaptant la charge de la preuve imposée par les régimes de responsabilité nationaux applicables aux préjudices causés par l'exploitation d'applications d'IA.

Au vu des développements qui précèdent, la Commission conclut qu'en plus des adaptations éventuelles de la législation en vigueur, il peut s'avérer nécessaire de prévoir de nouvelles mesures législatives spécifiquement consacrées à l'IA afin de garantir l'adéquation du cadre juridique de l'UE avec les réalités commerciales et technologiques actuelles et prévues.

C. CHAMP D'APPLICATION D'UN FUTUR CADRE RÉGLEMENTAIRE DE L'UE

Un aspect essentiel du futur réglementaire spécifique relatif à l'IA consiste à déterminer son champ d'application. L'hypothèse de travail est que le cadre réglementaire s'appliquerait aux produits et services qui dépendent de l'IA. Il importe, dès lors, de définir clairement l'IA aux fins du présent Livre blanc ainsi que de toute initiative future d'élaboration de politiques.

Dans sa communication sur l'IA pour l'Europe, la Commission a proposé une première définition de l'IA[46], qui a ensuite été affinée par le groupe d'experts de haut niveau[47].

Dans tout nouvel instrument juridique, la définition de l'IA devra être suffisamment souple pour tenir compte des progrès techniques tout en étant suffisamment précise pour garantir la sécurité juridique nécessaire.

Aux fins du présent Livre blanc ainsi que des débats qui pourront avoir lieu sur d'autres initiatives éventuelles, il semble important de préciser les principaux éléments dont se compose l'IA, à savoir les «données» et les «algorithmes». L'IA peut être intégrée dans des dispositifs matériels. Dans le cas des techniques d'apprentissage automatique, qui constituent l'une des branches de l'IA, les algorithmes sont entraînés à reconnaître des structures à partir d'un ensemble de données afin de déterminer les actions à prendre pour atteindre un objectif donné. Les algorithmes peuvent continuer leur apprentissage en cours d'utilisation. Si les produits d'IA peuvent agir de manière autonome en percevant leur environnement et sans suivre un ensemble d'instructions préétabli, leur comportement est dans une large mesure défini et circonscrit par leurs développeurs. L'humain détermine et programme les objectifs auxquels doit répondre l'optimisation d'un système d'IA.

> Dans le cas de la conduite autonome, par exemple, l'algorithme exploite en temps réel les données fournies par le véhicule (vitesse, consommation du moteur, amortisseurs, etc.) et les capteurs balayant intégralement l'environnement de la voiture (route, signalisation, autres véhicules, piétons, etc.) pour décider de la direction, de l'accélération et de la vitesse à adopter par la voiture pour atteindre une destination donnée. En fonction des données observées, l'algorithme s'adapte à la situation routière et aux conditions extérieures, y compris le comportement des autres conducteurs, pour choisir les modalités de conduite les plus confortables et les plus sûres.

L'UE s'est dotée d'un cadre juridique strict pour assurer notamment la protection des consommateurs, lutter contre les pratiques commerciales déloyales et protéger les données à caractère personnel et la vie privée. L'acquis comprend en outre des règles spécifiques pour certains secteurs (par exemple, les soins de santé, les transports). Ces dispositions existantes du droit de l'UE continueront de s'appliquer

[46] COM(2018) 237 final, p. 1: «L'intelligence artificielle (IA) désigne les systèmes qui font preuve d'un comportement intelligent en analysant leur environnement et en prenant des mesures – avec un certain degré d'autonomie – pour atteindre des objectifs spécifiques.
Les systèmes dotés d'IA peuvent être purement logiciels, agissant dans le monde virtuel (assistants vocaux, logiciels d'analyse d'images, moteurs de recherche ou systèmes de reconnaissance vocale et faciale, par exemple) mais l'IA peut aussi être intégrée dans des dispositifs matériels (robots évolués, voitures autonomes, drones ou applications de l'internet des objets, par exemple).»

[47] Groupe d'experts de haut niveau, Définition de l'IA, p. 8: «Les systèmes d'intelligence artificielle (IA) sont des systèmes logiciels (et éventuellement matériels) conçus par des êtres humains et qui, ayant reçu un objectif complexe, agissent dans le monde réel ou numérique en percevant leur environnement par l'acquisition de données, en interprétant les données structurées ou non structurées collectées, en appliquant un raisonnement aux connaissances, ou en traitant les informations, dérivées de ces données et en décidant de la/des meilleure(s) action(s) à prendre pour atteindre l'objectif donné. Les systèmes d'IA peuvent soit utiliser des règles symboliques, soit apprendre un modèle numérique. Ils peuvent également adapter leur comportement en analysant la manière dont l'environnement est affecté par leurs actions antérieures.»

à l'égard de l'IA, mais ce cadre pourrait nécessiter certains aménagements pour tenir compte de la transformation numérique et du recours à l'IA (voir la section B). Par conséquent, les aspects déjà couverts par la législation horizontale ou sectorielle existante (par exemple, en matière de dispositifs médicaux[48], de systèmes de transport) demeureront régis par cette législation.

En principe, le nouveau cadre réglementaire pour l'IA devrait atteindre ses objectifs avec efficacité sans être excessivement normatif, au risque de créer une charge disproportionnée, en particulier pour les PME. Pour réaliser cet équilibre, la Commission estime devoir suivre une approche fondée sur les risques.

Si une telle approche est importante pour garantir la proportionnalité de l'intervention réglementaire, elle requiert néanmoins des critères précis pour différencier les diverses applications de l'IA, et notamment pour déterminer si elles sont ou non «à haut risque»[49]. Les éléments permettant d'établir qu'une application d'IA est à haut risque devraient être clairs, faciles à comprendre et applicables à toutes les parties concernées. Cela étant, même si une application d'IA n'est pas classée à haut risque, elle reste entièrement soumise aux règles de l'UE en vigueur.

Selon la Commission, une application d'IA devrait généralement être considérée comme étant à haut risque en fonction de ce qui est en jeu, en examinant si des risques importants sont associés à la fois au secteur et à l'utilisation envisagée, notamment du point de vue de la protection de la sécurité, des droits des consommateurs et des droits fondamentaux. En particulier, une application d'IA devrait être considérée comme étant à haut risque si elle remplit cumulativement les deux critères suivants:

- premièrement, l'application d'IA est employée dans un secteur où, compte tenu des caractéristiques des activités normalement menées, des risques importants sont à prévoir. Ce premier critère garantit que l'intervention réglementaire cible les domaines dans lesquels, d'une manière générale, les risques sont réputés les plus probables. Le nouveau cadre réglementaire devrait comprendre une liste précise et complète des secteurs concernés. Par exemple, les soins de santé; les transports; l'énergie et certains pans du secteur public[50]. La liste devrait être réexaminée à intervalles réguliers et modifiée, le cas échéant, en fonction des réalités;

- deuxièmement, l'application d'IA dans le secteur en question est, de surcroît, utilisée de façon telle que des risques importants sont susceptibles d'apparaître. Ce second critère prend en considération le fait que toutes les utilisations de l'IA dans les secteurs sélectionnés n'impliquent pas nécessairement des risques importants. Par exemple, si les soins de santé peuvent, d'une manière générale, faire partie des secteurs concernés, une défaillance du système de planification des rendez-vous dans un hôpital ne présentera normalement pas de risques tels qu'ils justifient une intervention législative. L'appréciation du niveau de risque d'une utilisation donnée pourrait reposer sur ses conséquences pour les parties concernées. Par exemple, les utilisations d'applications d'IA qui produisent des effets juridiques sur les droits d'une personne physique ou d'une entreprise, ou l'affectent de manière significative de façon similaire; qui occasionnent un risque de blessure, de décès ou de dommage matériel ou

[48] Ainsi, diverses considérations de sécurité et implications juridiques sont associées aux systèmes d'IA qui fournissent des informations médicales spécialisées aux médecins, aux systèmes d'IA qui fournissent des informations médicales directement aux patients et aux systèmes d'IA qui pratiquent eux-mêmes des actes médicaux directement sur un patient. La Commission étudie actuellement ces enjeux propres aux soins de santé en matière de sécurité et de responsabilité.

[49] La législation de l'UE peut établir d'autres catégories de «risques» que celles décrites ici, en fonction du domaine concerné comme, par exemple, la sécurité des produits.

[50] Le secteur public pourrait comprendre des domaines tels que l'asile, la migration, les contrôles aux frontières et le système judiciaire, la sécurité sociale et les services de l'emploi.

immatériel important; dont les effets ne peuvent être évités par les personnes physiques ou morales.

Grâce à l'application cumulative des deux critères, la portée du cadre réglementaire serait circonscrite avec précision et garantirait la sécurité juridique. Les exigences obligatoires contenues dans le nouveau cadre réglementaire sur l'IA (voir la section D) ne s'appliqueraient en principe qu'aux applications désignées comme étant à haut risque selon ces deux critères cumulatifs.

Nonobstant les considérations qui précèdent, il peut également exister des cas exceptionnels dans lesquels, compte tenu des risques, l'utilisation d'applications d'IA à certaines fins devrait être considérée comme étant à haut risque en soi, c'est-à-dire indépendamment du secteur concerné, et resterait soumise aux exigences ci-dessous[51]. À titre d'illustration, il pourrait notamment pourrait s'agir notamment des applications suivantes:

- compte tenu de son importance pour les particuliers et de l'acquis de l'UE sur l'égalité en matière d'emploi, l'utilisation d'applications d'IA dans les procédures de recrutement et dans des situations ayant une incidence sur les droits des travailleurs serait toujours considérée comme étant «à haut risque», et les exigences ci-dessous s'appliqueraient dès lors à tout moment. D'autres applications spécifiques ayant une incidence sur les droits des consommateurs pourraient être envisagées;

- l'utilisation d'applications d'IA à des fins d'identification biométrique à distance[52] et pour d'autres technologies de surveillance intrusive serait toujours considérée comme étant «à haut risque», et les exigences ci-dessous s'appliqueraient dès lors à tout moment.

D. TYPES D'EXIGENCES

Lors de l'élaboration du futur cadre réglementaire pour l'IA, il faudra déterminer les types d'exigences légales obligatoires auxquelles seront soumis les acteurs concernés. Ces exigences peuvent être davantage précisées par des normes. Comme indiqué à la section C, outre la législation déjà existante, ces exigences ne vaudraient que pour les applications d'IA à haut risque, ce qui garantirait le caractère ciblé et proportionné de toute intervention réglementaire.

Compte tenu des lignes directrices élaborées par le groupe d'experts de haut niveau et des éléments exposés ci-dessus, les exigences imposées aux applications d'IA à haut risque pourraient porter sur les éléments essentiels suivants, détaillés dans les points ci-dessous:

- données d'entraînement;
- conservation des données et des dossiers;
- informations à fournir;
- robustesse et précision;
- contrôle humain;

[51] Il importe de souligner que d'autres actes législatifs de l'UE peuvent également s'appliquer. Par exemple, la directive relative à la sécurité générale des produits peut s'appliquer à la sécurité des applications d'IA lorsque ces dernières sont intégrées dans un produit de consommation grand public.

[52] Il convient de faire la distinction entre l'identification biométrique à distance et l'authentification biométrique (processus de sûreté qui s'appuie sur les caractéristiques biologiques uniques d'une personne pour vérifier qu'elle est bien celle qu'elle prétend être). L'identification biométrique à distance consiste à établir à distance, dans un espace public et de manière continue, l'identité de plusieurs personnes au moyen d'identificateurs biométriques (empreintes digitales, image faciale, iris, réseau veineux, etc.) en les comparant aux données stockées dans une base de données.

- exigences spécifiques pour les applications d'IA utilisées à des fins données, telles que l'identification biométrique à distance.

Afin de garantir la sécurité juridique, ces exigences seront davantage clarifiées pour que tous les acteurs qui doivent les respecter s'y retrouvent facilement.

a) Données d'entraînement

Il est plus important que jamais de promouvoir, de renforcer et de défendre les valeurs et les règles de l'UE, et en particulier les droits que les citoyens tirent du droit de l'Union. Ces efforts s'étendent, sans aucun doute, également aux applications d'IA à haut risque qui sont commercialisées et utilisées dans l'UE, et qui font l'objet du présent Livre blanc.

Comme expliqué ci-dessus, l'IA ne peut exister sans données. Le fonctionnement de nombreux systèmes d'IA, ainsi que les actions et décisions qu'ils sont susceptibles d'entraîner, dépendent en grande partie de l'ensemble de données qui a été utilisé pour entraîner ces systèmes. Il convient donc, lorsqu'il s'agit des données utilisées pour entraîner les systèmes d'IA, de prendre les mesures nécessaires pour garantir le respect des valeurs et des règles de l'UE, notamment en ce qui concerne la sécurité et les règles législatives en vigueur en matière de protection des droits fondamentaux. Il pourrait être envisagé d'appliquer les exigences suivantes à l'ensemble de données utilisé pour entraîner les systèmes d'IA.

- Des exigences visant à fournir des assurances raisonnables que l'utilisation ultérieure des produits ou des services reposant sur le système d'IA est sûre, en ce qu'elle répond aux normes fixées par les règles de sécurité applicables dans l'UE (qu'elles soient existantes ou envisagées en complément). Il peut s'agir, par exemple, d'exigences garantissant que les systèmes d'IA sont entraînés par des ensembles de données suffisamment larges et qu'ils couvrent tous les scénarios pertinents nécessaires pour éviter des situations dangereuses.

- Des exigences garantissant que des mesures raisonnables sont prises pour veiller à ce que toute utilisation ultérieure des systèmes d'IA ne donne pas lieu à des cas de discrimination interdite. En particulier, ces exigences pourraient comporter des obligations d'utiliser des ensembles de données suffisamment représentatifs, notamment pour garantir la prise en compte, dans ces ensembles de données, de tous les aspects pertinents du genre, de l'appartenance ethnique et d'autres motifs possibles de discrimination interdite.

- Des exigences visant à garantir une protection adéquate de la vie privée et des données à caractère personnel lors de l'utilisation des produits et services reposant sur l'IA. Le règlement général sur la protection des données et la directive en matière de protection des données dans le domaine répressif réglementent ces questions lorsqu'elles relèvent de leur champ d'application.

b) Conservation des dossiers et des données

Compte tenu d'éléments tels que la complexité et l'opacité de nombreux systèmes d'IA et des difficultés qu'il peut y avoir à vérifier effectivement la conformité aux règles applicables et leur exécution, il convient d'établir des exigences relatives à la conservation des dossiers de programmation de l'algorithme et des données utilisées pour entraîner les systèmes d'IA à haut risque et, dans certains cas, à la conservation des données elles-mêmes. Ces exigences visent essentiellement à permettre de reconstituer l'historique des actions ou décisions potentiellement problématiques prises par les systèmes d'IA et de les vérifier. Outre que cela devrait faciliter la surveillance et l'exécution,

cela pourrait également inciter les opérateurs économiques concernés à tenir compte, à un stade précoce, de la nécessité de respecter ces règles.

À cette fin, le cadre réglementaire pourrait prévoir l'obligation de conserver les éléments suivants:

- des archives précises concernant l'ensemble de données utilisé pour entraîner et tester les systèmes d'IA, y compris une description des principales caractéristiques et de la manière dont l'ensemble de données a été sélectionné;

- dans certains cas justifiés, les données elles-mêmes;

- la documentation relative aux méthodes, procédures et techniques de programmation[53] et d'entraînement utilisées pour concevoir, tester et valider les systèmes d'IA, y compris, le cas échéant, celle relative à la sécurité et à l'évitement de biais pouvant donner lieu à des discriminations interdites.

Les archives, la documentation et, le cas échéant, les ensembles de données devraient être conservés pendant une période limitée et raisonnable afin de garantir l'exécution effective de la législation applicable. Des mesures devraient être prises pour ces éléments soient mis à disposition sur demande, afin notamment de permettre aux autorités compétentes de les tester ou de les inspecter. Le cas échéant, des dispositions devraient être prises pour garantir la protection des informations confidentielles, telles que celles relatives aux secrets d'affaires.

c) Fourniture d'informations

La transparence ne doit pas concerner que les exigences en matière de conservation examinées au point b). Afin d'atteindre les objectifs poursuivis – en particulier promouvoir une utilisation responsable de l'IA, renforcer la confiance et, si nécessaire, faciliter les voies de recours – il importe de fournir, de manière proactive, des informations adéquates sur l'utilisation des systèmes d'IA à haut risque.

Ainsi, les exigences suivantes pourraient être envisagées.

- Veiller à ce que des informations claires soient fournies en ce qui concerne les capacités et les limites du système d'IA, en particulier l'objectif qu'il poursuit, les conditions dans lesquelles il devrait fonctionner comme prévu et le niveau de précision attendu dans la réalisation de l'objectif spécifié. Ces informations sont particulièrement importantes pour les déployeurs des systèmes, mais elles peuvent également être pertinentes pour les autorités compétentes et les parties concernées.

- Par ailleurs, des informations devraient être clairement fournies aux citoyens lorsqu'ils interagissent avec un système d'IA et non avec un être humain. Bien que la législation de l'UE sur la protection des données contienne déjà certaines règles en la matière[54], il pourrait s'avérer nécessaire de prévoir des exigences supplémentaires pour atteindre les objectifs susmentionnés. Dans cette hypothèse, il conviendrait d'éviter la création de charges inutiles. Ainsi, aucune information de ce type ne devrait être fournie, par exemple, dans des situations

[53] Il pourrait s'agir, par exemple, de la documentation relative à l'algorithme contenant les éléments qui doivent servir à l'optimisation du modèle, les pondérations qui sont conçues dès le départ pour certains paramètres, etc.

[54] En particulier, conformément à l'article 13, paragraphe 2, point f), du RGPD, le responsable du traitement doit, au moment où les données à caractère personnel sont obtenues, fournir à la personne concernée les informations complémentaires qui sont nécessaires pour garantir un traitement équitable et transparent de l'existence d'une prise de décision automatisée et certaines informations supplémentaires.

où il est d'emblée évident pour les citoyens qu'ils interagissent avec un système d'IA. Il importe en outre que les informations fournies soient objectives, concises et facilement compréhensibles. La manière de fournir ces informations devrait être adaptée à chaque contexte particulier.

d) Robustesse et précision

Pour pouvoir être dignes de confiance, les systèmes d'IA – et certainement les applications d'IA à haut risque – doivent être robustes et précis sur le plan technique. Ces systèmes doivent donc être développés de manière responsable, en tenant dûment et correctement compte, au préalable, des risques qu'ils sont susceptibles de générer. Les systèmes d'IA doivent être développés et fonctionner de façon à garantir la fiabilité de leur comportement, tel que prévu initialement. Il convient de prendre toutes les mesures raisonnables pour réduire autant que possible le risque de préjudice.

Ainsi, les exigences suivantes pourraient être envisagées.

- Des exigences garantissant la robustesse et la précision des systèmes d'IA ou, du moins, la bonne correspondance à leur niveau de précision, dans toutes les phases de leur cycle de vie.

- Des exigences garantissant la reproductibilité des résultats.

- Des exigences garantissant que les systèmes d'IA peuvent gérer de manière adéquate les erreurs ou les incohérences dans toutes les phases de leur cycle de vie.

- Des exigences garantissant, d'une part, que les systèmes d'IA peuvent résister à la fois aux attaques directes et aux tentatives plus subtiles de manipulation des données ou des algorithmes proprement dits, et, d'autre part, que des mesures d'atténuation sont prises en pareils cas.

e) Contrôle humain

Le contrôle humain contribue à éviter qu'un système d'IA ne mette en péril l'autonomie humaine ou ne provoque d'autres effets néfastes. Une IA digne de confiance, éthique et axée sur le facteur humain n'est possible que si une participation adéquate de l'être humain est garantie lorsqu'il s'agit d'applications à haut risque.

Bien que les applications d'IA examinées dans le présent Livre blanc afin de faire l'objet d'un cadre réglementaire spécifique soient toutes considérées comme étant à haut risque, le type et le niveau appropriés de contrôle humain peuvent varier selon le cas. Le contrôle humain devra dépendre notamment de l'utilisation prévue des systèmes et de ses incidences potentielles sur les citoyens et les personnes morales concernées. Il devra également être sans préjudice des droits légaux établis par le RGPD lorsque le système d'IA traite des données à caractère personnel. À titre non exhaustif, voici quelques exemples de situations dans lesquelles un contrôle humain pourrait être exercé:

- les résultats du système d'IA ne deviennent effectifs que s'ils ont été préalablement réexaminés et validés par un être humain (ex.: la décision de rejeter une demande de prestations de sécurité sociale ne peut être prise que par un être humain);

- les résultats du système d'IA deviennent immédiatement effectifs, mais un être humain intervient par la suite (ex.: une demande de carte de crédit peut être rejetée par un système d'IA, mais cette décision doit pouvoir être réexaminée ensuite par un être humain);

- la possibilité de suivre le système d'IA pendant son fonctionnement et la capacité d'intervenir en temps réel et de le désactiver (ex.: dans une voiture autonome, un bouton ou une procédure d'arrêt peut être activée par un être humain lorsqu'il estime que la conduite de la voiture n'est pas sûre);

- pendant la phase de conception, en imposant des contraintes opérationnelles au système d'IA (ex.: une voiture autonome doit cesser de fonctionner dans certaines conditions de faible visibilité qui diminuent la fiabilité des capteurs, ou maintenir, dans une quelconque condition donnée, une certaine distance par rapport au véhicule qui précède).

f) Exigences spécifiques pour l'identification biométrique à distance

La collecte et l'utilisation de données biométriques[55] à des fins d'identification à distance[56], au moyen, par exemple, du déploiement de la reconnaissance faciale dans des lieux publics, comportent des risques particuliers en termes de droits fondamentaux[57]. L'utilisation de systèmes d'IA pour l'identification biométrique à distance a des incidences sur les droits fondamentaux qui peuvent considérablement varier selon sa finalité, son contexte et sa portée.

Les règles de l'UE en matière de protection des données interdisent en principe le traitement de données biométriques aux fins d'identifier une personne physique de manière unique, sauf dans des conditions précises[58]. Plus particulièrement, en vertu du RGPD, un tel traitement ne peut avoir lieu qu'au titre d'un nombre limité de motifs, et notamment lorsqu'il est nécessaire pour des raisons d'intérêt public important. Dans ce cas, il doit avoir lieu sur la base du droit de l'Union ou du droit d'un État membre, sous réserve des exigences en matière de proportionnalité, de respect du contenu essentiel du droit à la protection des données et de garanties adéquates. En vertu de la directive en matière de protection des données dans le domaine répressif, le traitement doit être strictement nécessaire, il doit être en principe autorisé par le droit de l'Union ou le droit d'un État membre et être assorti de garanties adéquates. Étant donné que tout traitement de données biométriques aux fins d'identifier une personne physique de manière unique constituerait une exception à une interdiction prévue par le droit de l'Union, il serait soumis à la charte des droits fondamentaux de l'UE.

---

[55] Les données biométriques sont définies comme étant «les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques [empreintes digitales]» [article 3, paragraphe 13, de la directive en matière de protection des données dans le domaine répressif; article 4, paragraphe 14, du RGPD; article 3, paragraphe 18, du règlement (UE) 2018/1725].

[56] Dans le domaine de la reconnaissance faciale, l'identification signifie qu'une comparaison est effectuée entre le modèle de l'image faciale d'une personne et de nombreux autres modèles stockés dans une base de données afin de vérifier si l'image de cette personne y est stockée. L'authentification (ou la vérification), quant à elle, correspond souvent à une comparaison «un à un». Elle permet de comparer deux modèles biométriques, généralement supposés appartenir à la même personne. Deux modèles biométriques sont comparés pour déterminer si la personne qui figure sur les deux images est bien la même. Cette procédure est, par exemple, utilisée aux portiques de contrôle automatisé des passeports destinés aux vérifications aux frontières dans les aéroports.

[57] Concernant, notamment, la dignité des personnes. Dans le même ordre d'idées, les droits au respect de la vie privée et à la protection des données à caractère personnel sont au cœur des préoccupations en matière de droits fondamentaux lorsqu'une technologie de reconnaissance faciale est utilisée. Il pourrait également y avoir des répercussions sur le droit à la non-discrimination et les droits des groupes spéciaux, tels que les enfants, les personnes âgées et les personnes handicapées. Il convient en outre de veiller à ce que le recours à cette technologie ne nuise pas à la liberté d'expression, d'association et de réunion. Voir, à cet égard, la publication intitulée «Facial recognition technology: fundamental rights considerations in the context of law enforcement», disponible à l'adresse https://fra.europa.eu/en/publication/2019/facial-recognition.

[58] Voir l'article 9 du RGPD et l'article 10 de la directive en matière de protection des données dans le domaine répressif. Voir également l'article 10 du règlement (UE) 2018/1725 (applicable aux institutions et organes de l'UE).

Il s'ensuit, conformément aux règles de l'Union en vigueur en matière de protection des données et à la charte des droits fondamentaux de l'UE, que l'IA ne peut être utilisée à des fins d'identification biométrique à distance que lorsque cette utilisation est dûment justifiée, proportionnée et assortie de garanties adéquates.

Afin de répondre aux éventuelles inquiétudes, du point de vue de la société, quant à l'utilisation de l'IA à de telles fins dans les lieux publics et d'éviter toute fragmentation du marché intérieur, la Commission lancera un vaste débat européen sur les circonstances particulières, le cas échéant, qui pourraient justifier une telle utilisation, ainsi que sur les garanties communes à mettre en place.

E. DESTINATAIRES

En ce qui concerne les destinataires des exigences légales qui vaudraient pour les applications d'IA à haut risque susmentionnées, il convient d'examiner deux questions principales.

La première question concerne la répartition des obligations entre les opérateurs économiques impliqués. De nombreux acteurs sont impliqués dans le cycle de vie d'un système d'IA. Parmi ces acteurs figurent notamment le développeur, le déployeur (l'intervenant qui utilise un produit ou service à base d'IA) et potentiellement d'autres intervenants (le producteur, le distributeur ou l'importateur, le prestataire de services, et l'utilisateur professionnel ou privé).

La Commission estime que, dans un futur cadre réglementaire, chaque obligation devrait s'appliquer à l'acteur ou aux acteurs qui sont le mieux placés pour éliminer tout risque potentiel. À titre d'exemple, bien que les développeurs de l'IA soient probablement le mieux placés pour éliminer les risques liés à la phase de développement, il se peut que leur capacité à maîtriser les risques au cours de la phase d'utilisation soit plus limitée. Dans ce cas, le déployeur devrait être soumis à l'obligation correspondante. Cela est sans préjudice de la question de savoir quelle est la partie qui devrait être réputée responsable de tout dommage causé, afin de déterminer les responsabilités à l'égard des utilisateurs finals ou de toute autre partie subissant un préjudice et de garantir l'accès effectif à la justice. En vertu de la législation de l'UE en matière de responsabilité du fait des produits, la responsabilité du fait des produits défectueux est imputée au producteur, sans préjudice des législations nationales qui peuvent aussi autoriser les demandes de réparation auprès d'autres parties.

La deuxième question est celle de la portée géographique de l'intervention législative. De l'avis de la Commission, il est indispensable que les exigences soient applicables à tous les opérateurs économiques concernés qui fournissent des produits ou des services reposant sur l'IA dans l'UE, qu'ils soient ou non établis dans l'UE. Dans le cas contraire, les objectifs de l'intervention législative susmentionnés ne pourraient pas être pleinement atteints.

F. CONFORMITÉ ET MISE EN APPLICATION

Afin de garantir une IA digne de confiance, sûre et respectueuse des règles et valeurs européennes, les exigences légales applicables doivent être respectées dans la pratique et leur exécution effective doit être assurée tant par les autorités nationales et européennes compétentes que par les parties concernées. Les autorités compétentes devraient être en mesure d'enquêter sur des cas individuels, mais aussi d'évaluer l'incidence sur la société.

Compte tenu du risque élevé que posent certaines applications d'IA pour les citoyens et notre société (voir la section A), la Commission considère à ce stade qu'il serait nécessaire de réaliser une évaluation de la conformité objective et préalable pour vérifier et garantir le respect de certaines des exigences obligatoires susmentionnées pour les applications à haut risque (voir la section D). L'évaluation préalable de la conformité pourrait inclure des procédures d'essai,

d'inspection ou de certification[59]. Elle pourrait prévoir une vérification des algorithmes et des ensembles de données utilisés lors de la phase de développement.

Les évaluations de la conformité des applications d'IA à haut risque devraient être intégrées dans les mécanismes d'évaluation de la conformité qui existent déjà pour un grand nombre de produits et de services mis sur le marché intérieur de l'UE. S'ils n'existent pas, il peut s'avérer nécessaire d'établir des mécanismes similaires, sur la base des meilleures pratiques et des contributions éventuelles des parties prenantes et des organisations européennes de normalisation. Tout nouveau mécanisme devrait être proportionné et non discriminatoire et se fonder sur des critères transparents et objectifs en conformité avec les obligations internationales.

Lors de la conception et de la mise en œuvre d'un système reposant sur des évaluations préalables de la conformité, il convient de tenir particulièrement compte des éléments suivants.

- L'évaluation préalable de la conformité ne permettra peut-être pas de vérifier toutes les exigences énoncées ci-dessus. Par exemple, l'exigence relative aux informations devant être fournies ne se prête généralement pas bien à une vérification au moyen d'une telle évaluation.

- La possibilité que certains systèmes d'IA évoluent et apprennent par expérience, ce qui peut nécessiter de refaire des évaluations pendant toute la durée de vie des systèmes d'IA concernés.

- La nécessité de vérifier les données utilisées pour l'entraînement, ainsi que les méthodes, procédures et techniques de programmation et d'entraînement utilisées pour concevoir, tester et valider les systèmes d'IA.

- Si l'évaluation de la conformité révèle qu'un système d'IA ne satisfait pas aux exigences relatives, par exemple, aux données utilisées pour l'entraîner, il conviendra de remédier aux lacunes constatées, par exemple en entraînant à nouveau le système dans l'UE de manière à garantir le respect de toutes les exigences applicables.

Les évaluations de la conformité seraient obligatoires pour tous les opérateurs économiques visés par les exigences, quel que soit leur lieu d'établissement[60]. Afin de limiter la charge qui pèse sur les PME, une structure de soutien pourrait être envisagée, y compris par l'intermédiaire des pôles d'innovation numérique. La conformité pourrait en outre être facilitée par le recours à des normes et à des outils en ligne dédiés.

Toute évaluation préalable de la conformité devrait s'entendre sans fléchissement du contrôle de la conformité et de l'exécution ex post par les autorités nationales compétentes. Cela vaut pour les applications d'IA à haut risque, mais également pour d'autres applications d'IA soumises à des exigences légales, bien que le caractère à haut risque des applications en cause puisse justifier que les autorités nationales compétentes leur accordent une attention particulière. Les contrôles ex post devraient être facilités par une documentation appropriée de l'application d'IA concernée (voir la section E) et, le cas échéant, la possibilité pour des tiers, tels que les autorités compétentes, de tester

[59] Le système serait fondé sur des procédures d'évaluation de la conformité dans l'UE (voir la décision 768/2008/CE) ou sur le règlement (UE) 2019/881 (règlement sur la cybersécurité), et tiendrait compte des particularités de l'IA. Voir le «Guide bleu» relatif à la mise en œuvre de la réglementation de l'Union sur les produits, 2014.

[60] Pour ce qui est de la structure de gouvernance adéquate, y compris des organismes désignés pour effectuer les évaluations de la conformité, voir la section H.

ces applications, notamment lorsque surviennent des risques pour les droits fondamentaux, qui dépendent du contexte. Ce contrôle de la conformité devrait s'inscrire dans le cadre d'un système continu de surveillance du marché. Les aspects liés à la gouvernance sont examinés plus en détail à la section H.

En outre, que ce soit pour les applications d'IA à haut risque ou pour les autres applications d'IA, il convient de veiller à ce que les parties sur lesquelles des systèmes d'IA ont eu des effets négatifs disposent de voies de recours juridictionnel effectif. Les questions relatives à la responsabilité sont examinées plus en détail dans le rapport sur le cadre en matière de sécurité et de responsabilité qui accompagne le présent Livre blanc.

G. LABEL NON OBLIGATOIRE POUR LES APPLICATIONS D'IA QUI NE SONT PAS CONSIDÉRÉES COMME ÉTANT À HAUT RISQUE

Pour les applications d'IA qui ne sont pas considérées comme étant «à haut risque» (voir la section C) et qui ne sont donc pas soumises aux exigences obligatoires examinées ci-dessus (voir les sections D, E et F), il pourrait être envisagé, outre la législation applicable, de mettre en place un système de label non obligatoire.

Dans le cadre de ce système, les opérateurs économiques intéressés auxquels les exigences obligatoires ne s'appliquent pas pourraient décider de se soumettre, sur une base volontaire, à ces exigences ou à un ensemble spécifique d'exigences similaires spécialement établies aux fins du système non obligatoire. Les opérateurs économiques concernés recevraient alors un label de qualité pour leurs applications d'IA.

Le label non obligatoire permettrait aux opérateurs économiques concernés de signaler que leurs produits et services reposant sur l'IA sont dignes de confiance, et aux utilisateurs de facilement savoir que les produits et services concernés sont conformes à certains critères objectifs et normalisés à l'échelle de l'UE allant au-delà des obligations légales normalement applicables. Il contribuerait à renforcer la confiance des utilisateurs dans les systèmes d'IA et à promouvoir l'adoption de cette technologie.

Cette option impliquerait la création d'un nouvel instrument juridique établissant le cadre du système de label non obligatoire pour les développeurs et/ou les déployeurs de systèmes d'IA qui ne sont pas considérés comme étant à haut risque. La participation au système de label serait facultative mais, une fois que le développeur ou le déployeur aurait choisi d'utiliser le label, les exigences deviendraient contraignantes. La combinaison de contrôles ex ante et ex post devrait garantir le respect de toutes les exigences.

H. GOUVERNANCE

Il est nécessaire de mettre en place une structure de gouvernance européenne sur l'IA, qui prendrait la forme d'un cadre pour la coopération des autorités nationales compétentes, pour éviter une fragmentation des responsabilités, renforcer les capacités dans les États membres et faire en sorte que l'Europe se dote progressivement des capacités nécessaires pour tester et certifier les produits et services reposant sur l'IA. Dans ce contexte, il serait utile d'aider les autorités nationales compétentes à s'acquitter de leur mandat lorsque l'IA est utilisée.

Les travaux de la structure de gouvernance européenne pourraient être variés et consister notamment à offrir une enceinte propice à l'échange régulier d'informations et de bonnes pratiques, à recenser les tendances émergentes, et à donner des conseils en matière d'activités de normalisation et de certification. La structure de gouvernance devrait également jouer un rôle clé afin de faciliter la mise

en œuvre du cadre réglementaire, notamment en publiant des orientations, des avis et des connaissances spécialisées. À cet effet, elle devrait s'appuyer sur un réseau d'autorités nationales, ainsi que sur des réseaux sectoriels et des autorités de réglementation, tant au niveau national qu'au niveau de l'UE. Un comité d'experts pourrait par ailleurs fournir une assistance à la Commission.

La structure de gouvernance devrait garantir une participation maximale des parties prenantes. Les parties prenantes – organisations de consommateurs, partenaires sociaux, entreprises, chercheurs et organisations de la société civile – devraient être consultées sur la mise en œuvre du cadre et son développement ultérieur.

Compte tenu des structures déjà existantes, dans les domaines notamment de la finance, des médicaments, de l'aviation, des dispositifs médicaux, de la protection des consommateurs et de la protection des données, la structure de gouvernance proposée ne devrait pas faire double emploi avec des fonctions existantes. Elle devrait plutôt permettre d'établir des liens étroits avec d'autres autorités compétentes de l'UE et des États membres dans les différents secteurs concernés afin de compléter l'expertise existante et d'aider les autorités en place à assurer le suivi et le contrôle des activités des opérateurs économiques faisant intervenir des systèmes d'IA et des produits et services reposant sur l'IA.

Enfin, si cette option était retenue, la réalisation des évaluations de la conformité pourrait être confiée aux organismes notifiés désignés par les États membres. Les centres d'essai devraient faire en sorte que les systèmes d'IA puissent faire l'objet d'une vérification et d'une évaluation indépendantes conformément aux exigences énoncées ci-dessus. Une évaluation indépendante renforcera la confiance et garantira l'objectivité. Elle pourrait également faciliter le travail des autorités compétentes concernées.

L'UE possède d'excellents centres d'essai et d'évaluation, et devrait développer ses capacités dans le domaine de l'IA également. Les opérateurs économiques établis dans des pays tiers et souhaitant accéder au marché intérieur pourraient soit faire appel à des organismes désignés établis dans l'UE soit, sous réserve d'accords de reconnaissance mutuelle avec des pays tiers, faire appel à des organismes de pays tiers désignés pour effectuer cette évaluation.

La structure de gouvernance relative à l'IA et les éventuelles évaluations de la conformité dont il est question ici ne modifieraient en rien les compétences et les responsabilités des autorités compétentes, visées par le droit de l'UE en vigueur, que ce soit dans des secteurs spécifiques ou concernant des questions bien précises (finance, médicaments, aviation, dispositifs médicaux, protection des consommateurs, protection des données, etc.).

6. CONCLUSION

L'IA est une technologie stratégique qui offre de nombreux avantages aux citoyens, aux entreprises et à la société dans son ensemble, à condition qu'elle soit éthique, durable, axée sur le facteur humain et respectueuse des valeurs et droits fondamentaux. Elle offre des gains d'efficacité et de productivité significatifs qui peuvent renforcer la compétitivité de l'industrie européenne et améliorer le bien-être des citoyens. Elle peut également contribuer à relever certains des défis les plus pressants de la société, notamment la lutte contre le changement climatique et la dégradation de l'environnement, les défis liés à la durabilité et à l'évolution démographique, la protection de nos démocraties et, lorsque cela est nécessaire et proportionné, la lutte contre la criminalité.

Pour que l'Europe puisse tirer pleinement parti des possibilités offertes par l'IA, elle doit développer les capacités industrielles et technologiques nécessaires et les renforcer. Comme indiqué dans la

stratégie européenne pour les données, qui accompagne le présent Livre blanc, elle doit également prendre des mesures qui lui permettront de devenir un pôle mondial de données.

L'approche européenne en matière d'IA vise à promouvoir les capacités d'innovation de l'Europe dans le domaine de l'IA tout en soutenant le développement et l'adoption d'une IA éthique et digne de confiance dans tous les secteurs économiques de l'UE. L'IA devrait être au service des citoyens et constituer un atout pour la société.

Dans le cadre du présent Livre blanc et du rapport sur le cadre en matière de sécurité et de responsabilité qui l'accompagne, la Commission lance une vaste consultation du secteur privé, du milieu universitaire et de la société civile des États membres et les invite à formuler des propositions concrètes pour une approche européenne en matière d'IA. Cette consultation porte à la fois sur des moyens d'action visant à stimuler les investissements dans la recherche et l'innovation, à renforcer le développement des compétences et à soutenir l'adoption de l'IA par les PME, et sur les éléments clés d'un futur cadre réglementaire. Elle sera l'occasion d'entamer un dialogue approfondi avec toutes les parties concernées, qui orientera les prochaines mesures de la Commission.

La Commission invite les parties intéressées à formuler leurs observations sur les propositions exposées dans le présent Livre blanc dans le cadre d'une consultation publique ouverte disponible à l'adresse suivante: https://ec.europa.eu/info/consultations_fr. Les parties intéressées sont invitées à soumettre leurs commentaires pour le 19 mai 2020 au plus tard.

Il est d'usage que la Commission publie les observations reçues à la suite d'une consultation publique. Les auteurs peuvent cependant demander que leurs observations demeurent confidentielles en tout ou partie. Si tel est votre souhait, veuillez indiquer clairement sur la page de couverture de votre contribution que celle-ci ne doit pas être rendue publique et également envoyer à la Commission une version non confidentielle destinée à la publication.