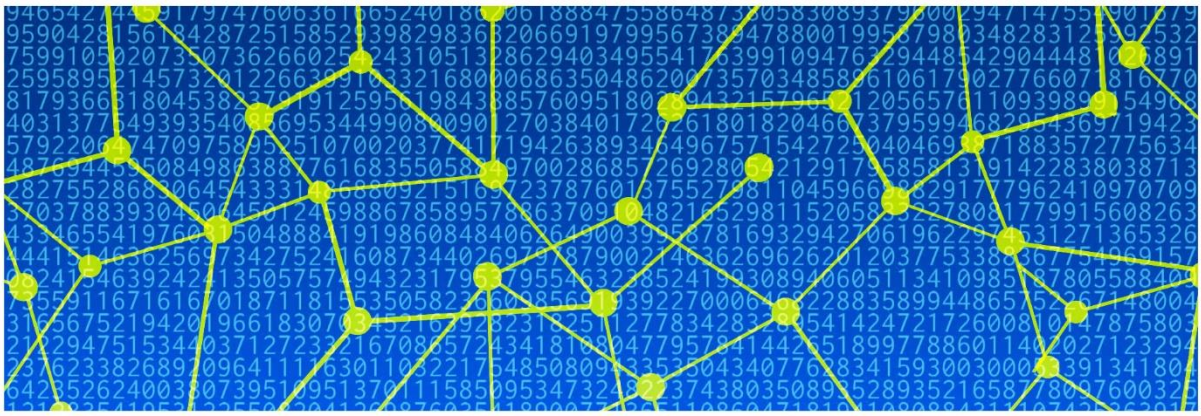

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 4/2020

Avis du CEPD sur le Livre blanc de la Commission européenne intitulé «Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance»

EDPS

29 juin 2020

Synthèse

Le 19 février 2020, la Commission européenne a publié un Livre blanc intitulé «Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance». Ce document fait partie d'un ensemble plus vaste de documents stratégiques, qui comprend également une communication intitulée «Une stratégie européenne pour les données».

Le Livre blanc poursuit un double objectif: définir des options stratégiques afin de promouvoir le recours à l'intelligence artificielle (IA) et tenir compte «des risques associés à certaines utilisations de cette nouvelle technologie». Pour y parvenir, le Livre blanc propose une série de mesures visant à promouvoir le développement et l'adoption de l'IA ainsi qu'un nouveau cadre réglementaire qui répondrait aux préoccupations spécifiques que suscite l'IA et auxquelles le cadre actuel ne peut pas répondre.

Le présent avis expose le point de vue du CEPD sur le Livre blanc dans son ensemble, ainsi que sur certains de ses aspects spécifiques, tels que l'approche proposée fondée sur les risques, l'application de la réglementation en matière d'IA ou les exigences particulières relatives à l'identification biométrique à distance (y compris la reconnaissance faciale).

Le CEPD reconnaît l'importance et l'impact croissants de l'intelligence artificielle. Toutefois, l'IA comporte des risques qui lui sont propres et n'est pas une panacée qui résoudra tous les problèmes. Quiconque adopte une technologie, en particulier les administrations publiques qui traitent de grandes quantités de données à caractère personnel, devrait prendre en considération les avantages, les coûts et les risques qu'elle entraîne.

Le CEPD se réjouit des très nombreuses références du Livre blanc à une **approche européenne de l'IA**, fondée sur les **valeurs et les droits fondamentaux de l'UE**, ainsi que de la prise en compte de la nécessité de **se conformer à la législation européenne en matière de protection des données**.

Par conséquent, les recommandations formulées dans le présent avis visent à clarifier et, le cas échéant, à renforcer les garanties et les contrôles en matière de protection des données à caractère personnel, en tenant compte du contexte spécifique de l'intelligence artificielle.

À cet effet, le CEPD recommande en particulier que tout nouveau cadre réglementaire relatif à l'IA:

- **s'applique tant** aux États membres de l'UE qu'aux institutions, organes et organismes de l'UE;

- soit conçu dans l'optique de **protéger de tout effet négatif** non seulement les personnes physiques, mais également les communautés et la société dans son ensemble;

- propose **un système de classification des risques plus solide et plus nuancé**, garantissant que tout dommage important potentiel découlant des applications d'IA soit compensé par des mesures d'atténuation appropriées;

- inclue une analyse d'impact **définissant clairement les lacunes réglementaires** qu'il entend combler;

- **évite les chevauchements** entre les différentes autorités de contrôle et inclue un mécanisme de coopération.

En ce qui concerne l'identification biométrique à distance, le CEPD est favorable à l'idée d'un **moratoire sur le déploiement, dans l'espace public de l'UE, d'un système automatisé de reconnaissance de caractéristiques humaines**, non seulement des visages, mais aussi de la démarche, des empreintes digitales, de l'ADN, de la voix, de la pression sur des touches et d'autres signaux biométriques ou comportementaux, de sorte qu'un débat démocratique et éclairé puisse avoir lieu, jusqu'au moment où l'UE et les États membres disposeront de toutes les garanties appropriées, y compris un cadre juridique complet assurant la proportionnalité des différentes technologies et différents systèmes pour chaque type d'utilisation spécifique.

Le CEPD se tient à la disposition de la Commission, du Conseil et du Parlement européen pour tout avis supplémentaire et espère être consulté en temps utile, comme le prévoit l'article 42 du règlement (UE) 2018/1725. Les commentaires figurant dans le présent avis sont sans préjudice de tout commentaire supplémentaire futur sur des points particuliers et/ou au cas où de nouvelles informations seraient disponibles.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, ci-après le «RGPD»)[1],

vu la 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil[2],

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE[3] (ci-après le «RPDUE»), et notamment son article 57, paragraphe 1, point h), et son article 58, paragraphe 3, point c),

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION ET CONTEXTE

1. Le Livre blanc de la Commission intitulé «Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance»[4] (ci-après le «Livre blanc») s'inscrit dans le cadre de l'initiative nº 10 («Une approche européenne de l'intelligence artificielle») et relève du chapitre «Une Europe adaptée à l'ère du numérique» du programme de travail 2020 de la Commission.

2. Le CEPD observe que le Livre blanc a un lien étroit avec la «Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Une stratégie européenne pour les données»[5] (ci-après la «stratégie pour les données»), sur laquelle le CEPD a adopté un avis distinct[6].

3. Le 29 janvier 2020, le CEPD a été consulté par la Commission sur le projet de Livre blanc et a présenté des observations informelles préliminaires. Le CEPD se réjouit que son avis ait été sollicité à un stade précoce de la procédure et encourage la Commission à maintenir cette bonne pratique.

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 119 du 4.5.2016, p. 89.
[3] JO L 295 du 21.11.2018, p. 39.
[4] COM(2020) 65 final.
[5] COM(2020) 66 final.
[6] Avis 3/2020 du CEPD sur la stratégie européenne pour les données, https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf (en anglais).

4. Le Livre blanc fait l'objet d'une consultation publique. La consultation vise à recueillir des avis sur le Livre blanc dans son ensemble, ainsi que sur certains aspects particuliers de celui-ci. Une consultation publique similaire avait eu lieu sur la communication de la Commission européenne «Une stratégie européenne pour les données».

5. Le présent avis approfondit certaines des observations informelles formulées par le CEPD et apporte une contribution plus ciblée à la Commission à la lumière de la consultation publique. Par ailleurs, le présent avis est sans préjudice de tout commentaire supplémentaire que le CEPD pourrait formuler sur la base d'informations additionnelles disponibles ultérieurement, notamment dans le cadre des futures consultations législatives sur les actes juridiques prévus dans le Livre blanc et dans le programme de travail de la Commission.

6. Bien que les institutions, organes et organismes de l'Union européenne soient soumis au RPDUE et non au RGPD, les deux règlements poursuivent les mêmes objectifs et les principes qui les fondent sont identiques[7]. Pour refléter cette cohérence, toute référence à une disposition du RGPD dans le présent avis sera accompagnée de la mention de la disposition correspondante du RPDUE entre parenthèses.

7. Afin de parvenir à une **approche cohérente dans l'ensemble de l'Union**, le CEPD recommande que tout nouveau cadre réglementaire en matière d'IA s'applique tant aux États membres qu'aux institutions, organes et organismes de l'UE. **Lorsque les institutions, organes et organismes de l'Union ont recours à l'intelligence artificielle («IA»), ils devraient être soumis aux mêmes règles que celles qui s'appliquent dans les États membres de l'UE.**

2. OBJECTIFS GÉNÉRAUX ET VISION

8. Le CEPD se réjouit des très nombreuses références du Livre blanc à une approche européenne de l'IA, fondée sur **les valeurs et les droits fondamentaux de l'UE**, ainsi que de la prise en compte de la nécessité de se conformer à la législation européenne en matière de protection des données. Parallèlement, le CEPD espère que **cet engagement ferme se retrouvera pleinement dans tout nouveau cadre réglementaire européen concernant l'IA** afin de respecter effectivement les valeurs et les droits fondamentaux, notamment la dignité humaine, le pluralisme, l'égalité, la non-discrimination, l'État de droit, le respect de la légalité et la protection de la vie privée et des données à caractère personnel.

9. Le CEPD rappelle que, conformément à l'article 5 du RGPD et à l'article 4 du RPDUE, le traitement des données à caractère personnel devrait toujours respecter **les principes généraux** de légalité, d'équité et de transparence, de limitation de la finalité, de minimisation des données, d'exactitude, de limitation de la conservation, d'intégrité et de confidentialité ainsi que de responsabilité du responsable du traitement.

10. Le Livre blanc déclare poursuivre un double objectif: définir des options stratégiques afin de promouvoir le recours à l'IA et tenir compte «des risques associés à certaines utilisations de cette nouvelle technologie». Compte tenu de ces objectifs, le CEPD partage l'avis de la

[7] Lorsque les dispositions du règlement (UE) 2018/1725 suivent les mêmes principes que celles du règlement (UE) 2016/679, conformément à la jurisprudence de la Cour de justice, il convient d'interpréter les deux ensembles de dispositions de manière homogène, notamment parce que l'économie du RPDUE doit être comprise comme équivalente à l'économie du RGPD (voir considérant 5 du RPDUE, faisant référence à l'arrêt de la Cour du 9 mars 2010, *Commission européenne/République fédérale d'Allemagne*, C-518/07, ECLI:EU:C:2010:125, point 28).

Commission selon lequel il convient de «définir clairement l'IA aux fins du présent Livre blanc ainsi que de toute initiative future d'élaboration de politiques». Le CEPD regrette toutefois que le document présente plus d'une définition et n'adopte pas clairement l'une d'elles: le Livre blanc définit d'abord l'IA comme étant «la combinaison de données, d'algorithmes et d'une puissance de calcul»; le CEPD considère toutefois que cette définition est trop ambiguë, dans la mesure où elle s'applique également à d'autres technologies (par exemple, les «mégadonnées»). Plus loin, le Livre blanc fait référence aux définitions figurant dans la communication de la Commission européenne sur l'IA pour l'Europe et aux travaux du groupe d'experts de haut niveau sur l'IA. Le Livre blanc se termine sans avoir défini l'IA aux fins du «nouvel instrument juridique». Le CEPD est d'avis qu'avec **le Livre blanc, la Commission européenne a manqué une occasion de proposer une définition claire de l'IA**, qui servirait à encadrer la portée des actions et les éventuelles propositions législatives futures. De ce fait, il sera malaisé de comprendre quelle sera la portée d'une éventuelle législation fondée sur ce Livre blanc. Le CEPD considère que toute définition d'un futur instrument juridique devrait au moins tenir compte des éléments suivants: un modèle de prise de décision, un algorithme qui traduit ce modèle en code calculable, les données utilisées par ce code comme intrant et l'environnement qui entoure son utilisation[8].

11. Pour atteindre ses objectifs, le Livre blanc déclare que l'un des principaux piliers sur lesquels il s'appuie pour mettre en place un cadre politique consiste à «créer les incitations appropriées pour accélérer l'adoption de solutions fondées sur l'IA». En outre, le Livre blanc juge «*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»[9]. En qualifiant l'IA de technologie «essentielle», le Livre blanc semble supposer qu'elle est la technologie la plus appropriée, indépendamment des modèles de gestion appliqués par les autorités publiques et des risques que pose son utilisation. Le CEPD est d'avis **qu'il n'existe pas de «solution technologique miracle»**. À l'instar de toute autre technologie, l'intelligence artificielle n'est qu'un outil et elle devrait être conçue pour servir l'humanité. Comme toute autre technologie, l'IA présente des avantages et des inconvénients et tant les autorités publiques que les entités privées devraient déterminer au cas par cas si une application d'IA est la meilleure option pour obtenir des résultats d'intérêt public.

12. Dans le même ordre d'idées, le Livre blanc affirme que «[l]es 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**» (caractères gras ajoutés). Le Livre blanc ne fournit aucune référence à des données scientifiques étayant cette allégation et risque de favoriser un **recours aveugle** à l'IA. Il ne définit pas les critères utilisés pour évaluer le niveau de maturité de l'IA dans des domaines d'application spécifiques[10]. Le CEPD suggère donc qu'une analyse plus approfondie et

[8] Ces éléments pourraient trouver une source d'inspiration dans les documents suivants: Groupe d'experts à haut niveau sur l'intelligence artificielle «A definition of Artificial Intelligence: Main capabilities and disciplines», https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341 et AlgorithmWatch, «Automating Society Taking Stock of Automated Decision-Making in the EU (2019)», https://algorithmwatch.org/wp-content/uploads/2019/02/Automating_Society_Report_2019.pdf (en anglais).

[9] Livre blanc sur l'IA, section 4.F.

[10] Si l'on prenait en compte le nombre d'études menées depuis 2013 sur l'utilisation de l'IA dans les soins de santé comme substitut de la maturité, on constaterait des niveaux de maturité assez différents (par exemple, 531 études sur le traitement et l'analyse d'images, 45 études sur l'analyse pathologique ou 10 études sur la gestion des maladies); voir Journal of Biomedical Informatics, Volume 100, décembre 2019, «Transforming healthcare with big data

quantifiée que celle que l'on trouve actuellement dans le Livre blanc, fondée sur des sources identifiées, renforcerait la position de la Commission et contribuerait au débat public sur le Livre blanc en relevant la qualité des arguments.

13. Le CEPD considère également que certaines applications d'IA (comme la reconnaissance faciale en direct) interfèrent avec les droits et libertés fondamentaux dans une telle mesure qu'elles pourraient remettre en cause l'essence même de ces droits et libertés. En raison du stade précoce de développement ou du déploiement de l'IA et de l'absence de vision exhaustive de ses effets sur notre société, la Commission européenne devrait préconiser l'application stricte du principe de précaution. Cette réflexion sera développée dans les sections suivantes.

3. NÉCESSITÉ D'UN CADRE JURIDIQUE MODIFIÉ

14. Le CEPD salue l'appel lancé en faveur d'une **application et du contrôle effectifs et entiers de la législation existante de l'UE** ainsi que d'une évaluation minutieuse et objective de la nécessité de procéder à de futurs ajustements législatifs.

15. Le CEPD souscrit également à l'approche proposée dans le Livre blanc selon laquelle, en ce qui concerne les systèmes d'IA exploités dans l'UE, «*il est indispensable que les exigences soient applicables à tous les opérateurs économiques […], qu'ils soient ou non établis dans l'UE*», ce qui est conforme à l'approche retenue par le législateur européen pour la protection des données à caractère personnel, notamment le RGPD.

16. **Le cadre juridique européen en matière de protection des données est neutre du point de vue technologique et ne fait pas obstacle à l'adoption réussie de nouvelles technologies, en particulier l'IA**. Au contraire, il vise à **encourager l'application de toute technologie** au traitement de données à caractère personnel dans le plein respect des valeurs et des droits fondamentaux des citoyens européens.

17. Le Livre blanc affirme que son objectif est de réduire au minimum les risques liés à l'utilisation de l'IA et il recense les principaux d'entre eux, comme «l'application des règles visant à protéger les droits fondamentaux» ainsi que les «questions liées à la sécurité et à la responsabilité». Le premier type de risques est ensuite décrit comme portant 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». Dans la section 5.B, le Livre blanc précise les risques et les situations dans lesquelles le cadre réglementaire de l'Union pourrait nécessiter une amélioration afin d'en garantir la bonne application:

    - le risque concernant l'«Application effective et [le] contrôle de la législation existante de l'UE et des États membres» s'articule autour de l'opacité de l'IA, qui sera abordée dans la section 4.3 consacrée à la responsabilité et à l'application des règles (voir plus loin);

    - le risque concernant les «Limitations du champ d'application de la législation existante de l'UE» est axé sur le cadre réglementaire de l'UE relatif à la sécurité des produits;

analytics and artificial intelligence: A systematic mapping study», https://www.sciencedirect.com/science/article/abs/pii/S1532046419302308

- le risque relatif aux «Fonctionnalités modifiées par des systèmes d'IA», décrites dans le Livre blanc[11], n'est ni nouveau ni exclusivement lié aux applications d'IA. Le CEPD regrette que le Livre blanc n'explique pas plus en détail pourquoi les mises à jour de logiciels qui ajoutent de nouvelles fonctionnalités présentent des problèmes de conformité différents de ceux que posent les modifications de fonctionnalités de systèmes qui ne sont pas fondés sur l'IA;

- le risque associé à l'«Incertitude concernant la répartition des responsabilités…» semble être lié à la législation de l'Union sur la sécurité des produits. Étant donné que les responsables du traitement des données et les sous-traitants doivent se conformer aux exigences du RGPD en ce qui concerne les applications d'IA lors du traitement de données à caractère personnel, il convient de définir clairement ces rôles afin de répartir adéquatement les responsabilités. Une analyse d'impact relative à la protection des données (AIPD) est un instrument utile pour faciliter la répartition des responsabilités;

- le risque relatif aux «Modifications du concept de sécurité» concerne des «risques que la législation actuelle de l'UE n'aborde pas explicitement» et qui sont liés au cadre réglementaire de l'UE en matière de sécurité des produits.

Les liens entre ces différents risques et les lacunes législatives spécifiques entraînant la nécessité d'une nouvelle réglementation restent flous. L'analyse d'impact de toute proposition relative à un cadre réglementaire en matière d'IA devrait clairement inclure ces liens.

18. Au cours du second semestre de 2019, plus de 350 organisations ont transmis leurs observations[12] sur les lignes directrices du groupe d'experts de haut niveau pour une IA digne de confiance[13]. Dans le cadre de ces observations, le Livre blanc indique que la transparence[14], la traçabilité[15] et le contrôle humain[16], qui sont des exigences essentielles des lignes directrices du groupe d'experts à haut niveau[17], «dans de nombreux secteurs économiques, [...] ne sont pas spécifiquement couvert[e]s par la législation en vigueur». Le CEPD est d'avis que le RGPD reflète pleinement les exigences essentielles mentionnées et s'applique à la fois aux secteurs public et privé traitant des données à caractère personnel. La transparence est exigée par l'article 5, paragraphe 1, point a), du RGPD (principe de licéité, de loyauté et de transparence) [*article 4, paragraphe 1, point a), du RPDUE*] et aux articles 12 à 14 du RGPD (exigences d'informations transparentes) [*articles 14 à 16 du RPDUE*], tandis que le contrôle humain est spécifiquement abordé à l'article 22 du RGPD [*article 24 du RPDUE*] et plus

[11] «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» (italique ajouté).
[12] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57590 (en anglais)
[13] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
[14] «Cette exigence est étroitement liée au principe de l'explicabilité et comprend la transparence des éléments pertinents d'un système d'IA: les données, le système et les modèles économiques», Lignes directrices du groupe d'experts de haut niveau sur l'IA (page 22).
[15] «Les ensembles de données et les processus permettant au système d'IA de rendre une décision, y compris les processus de collecte et d'étiquetage de données, ainsi que les algorithmes utilisés, devraient être documentés selon les normes les plus strictes afin de permettre la traçabilité ainsi qu'une amélioration de la transparence. Ce principe s'applique également aux décisions rendues par le système d'IA. Cela permet de déterminer les raisons pour lesquelles une décision d'IA était erronée ce qui, en retour, pourrait contribuer à éviter de futures erreurs. La traçabilité facilite donc l'auditabilité ainsi que l'explicabilité», Lignes directrices du groupe d'experts de haut niveau sur l'IA (page 22).
[16] «Les systèmes d'IA devraient soutenir l'autonomie et la prise de décisions humaines, conformément au principe du respect de l'autonomie humaine», Lignes directrices du groupe d'experts de haut niveau sur l'IA (page 19).
[17] Observations provenant de la consultation publique sur les lignes directrices publiées par le groupe d'experts de haut niveau sur l'IA.

largement à l'article 5, paragraphe 2, du RGPD (responsabilité) [*article 4, paragraphe 2, du RPDUE*]. Cette question ne semble dès lors pas être un problème pour la législation de l'UE en matière de protection des données.

19. Certaines applications d'IA, comme une police prédictive[18], peuvent avoir des effets négatifs, tels qu'un contrôle policier excessif sur les communautés et les personnes physiques. Parallèlement, les règles relatives à la protection des données sont conçues au premier chef pour protéger les personnes physiques et peuvent ne pas être adaptées pour traiter des risques pour des *groupes de personnes*. Étant donné qu'aucune personne physique précise ne fait l'objet d'une discrimination lorsque, par exemple, un quartier se transforme lentement en une zone très patrouillée, il pourrait également être difficile d'appliquer la législation contre la discrimination. Le CEPD recommande donc fortement que toute réglementation sur l'IA soit conçue dans l'optique de **protéger contre *tout* effet négatif** non seulement pour les personnes physiques, mais aussi pour les communautés et la société dans son ensemble. À cet égard, le CEPD invite la Commission à concevoir des modèles de gouvernance inclusive qui responsabiliseraient les organisations représentant la société civile (comme les ONG et d'autres associations à but non lucratif) afin qu'elles puissent, elles aussi, contribuer à évaluer l'impact des applications d'IA sur des communautés particulières et sur la société en général.

20. Le CEPD partage l'avis de la Commission selon lequel tout futur cadre juridique doit prendre en considération des éléments relatifs à la qualité et à la traçabilité des données, ainsi qu'à la transparence et au contrôle humain et des critères spécifiques pour les systèmes d'identification biométrique. Le CEPD souscrit pleinement à ces exigences, qui correspondent à certains des principes directeurs énoncés dans la **déclaration sur l'éthique et la protection des données dans le secteur de l'IA**, adoptée par la 40e Conférence internationale des commissaires à la protection des données et de la vie privée (ICDPPC), qui s'est tenue à Bruxelles[19]. En outre, le CEPD recommande d'examiner également les autres principes directeurs énoncés dans la déclaration de l'ICDPPC, tels que la conception et le développement responsables en appliquant les principes de respect de la vie privée dès la conception et par défaut et la responsabilisation de l'individu.

21. Le CEPD reconnaît les risques que l'utilisation de l'IA peut représenter pour un large éventail de droits fondamentaux, y compris, mais certainement sans s'y limiter, le respect de la vie privée et la protection des données à caractère personnel[20]. Le CEPD fait toutefois valoir qu'en outre, une surveillance accrue et des formes inappropriées de gouvernance (par exemple, par la classification et la prévision de l'apprentissage automatique, y compris le comportement des personnes, avec ou sans reconnaissance faciale) devraient aussi être considérées comme des facteurs de risque importants pour l'IA, notamment en raison de leur effet dissuasif potentiel sur plusieurs autres droits fondamentaux. Par ailleurs, alors que le Livre blanc recense deux sources de risques pour les personnes physiques – les séries de données biaisées et la conception erronée du système d'IA –, le CEPD considère que d'autres sources de risques

[18]AI & Global Governance: Turning the Tide on Crime with Predictive Policing https://cpr.unu.edu/ai-global-governance-turning-the-tide-on-crime-with-predictive-policing.html

[19]https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_ai-declaration_adopted_fr.pdf La Conférence internationale des commissaires à la protection des données et de la vie privée, rebaptisée Global Privacy Assembly, a été la première enceinte internationale regroupant les autorités chargées de la protection des données et de la vie privée pendant plus de quarante ans.

[20] Voir aussi le document de l'Agence des droits fondamentaux «Facial recognition technology: fundamental rights considerations in the context of law enforcement», 27 novembre 2019, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (en anglais).

devraient également être prises en compte, comme la qualité insuffisante des données ou les risques découlant de l'utilisation de l'IA (tels que la tendance humaine à accorder une confiance aveugle à des systèmes automatisés de prise de décisions[21]).

22. Alors que le CEPD convient que des biais pourraient également affecter les systèmes d'IA qui apprennent pendant leur fonctionnement, le Livre blanc poursuit en affirmant que lorsque le système d'IA «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 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» (accent ajouté). Le CEPD ne partage pas cette appréciation. **La conception des applications d'IA devrait tenir compte des biais potentiels dans les données de formation et, le cas échéant, dans les données opérationnelles.** Les biais peuvent et doivent être mesurés et corrigés *pendant le fonctionnement* des systèmes d'IA dans la mesure où ils peuvent être mesurés et corrigés pendant leur développement[22].

4. ÉVALUATION DU FUTUR CADRE RÉGLEMENTAIRE DE L'IA

4.1. Principe de précaution et approche fondée sur les risques

23. Le Livre blanc suit une approche fondée sur les risques pour «garantir la proportionnalité de l'intervention réglementaire», c'est-à-dire limiter l'applicabilité du cadre réglementaire proposé. Le Livre blanc propose d'ajouter certains critères juridiques, complétant les exigences existantes, pour les applications d'IA *à haut risque*.

24. En ce qui concerne les risques que représentent les applications d'IA traitant des données à caractère personnel pour les personnes concernées, cette réglementation complémentaire semble inutile, étant donné que l'approche fondée sur les risques déjà consacrée par les articles 32 (sécurité du traitement) et 35 (analyse d'impact relative à la protection des données) du RGPD [*articles 33 et 35 du RPDUE*] est homogène et doit être adaptée aux besoins spécifiques de chaque application. En février 2020, le comité européen de la protection des données a conclu[23] qu'il était «prématuré de réviser le texte législatif à ce stade».

25. La stratégie fondée sur les risques du Livre blanc indique (page 21): «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 [les] deux critères *cumulatifs*», à savoir un *secteur* à haut risque et *l'utilisation et l'impact* de l'application d'IA (accent ajouté).

[21] «En effet, la nature soi-disant fiable des solutions d'IA fondées sur les mathématiques peut pousser les personnes qui s'appuient sur des algorithmes pour prendre leurs décisions à faire confiance au tableau des individus et de la société suggéré par les procédés analytiques. Cette attitude peut en outre être renforcée par la menace de sanctions potentielles si une décision a été prise en ignorant les résultats des procédures analytiques», Intelligence artificielle et protection des données: enjeux et solutions possibles, rapport demandé par le Conseil de l'Europe au professeur Alessandro Mantelero, https://rm.coe.int/intelligence-artificielle-et-protection-des-donnees-enjeux-et-solution/168091f8a5

[22] Tay, l'agent conversationnel (*chatbot*) intelligent de Microsoft, suit un cours accéléré sur le racisme sur Twitter https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter?CMP=twt_a-technology_b-gdntech

[23] Contribution du comité européen de la protection des données à l'évaluation du RGPD au titre de l'article 97 (p. 4), https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en (en anglais).

26. Le CEPD avance les suggestions suivantes pour le cas où un nouveau cadre réglementaire devrait être adopté.

27. Sur les critères *cumulatifs* en cas de risque élevé, le CEPD considère que le concept de «haut risque» exposé dans le Livre blanc est trop étroit, étant donné qu'il semblerait exclure les personnes physiques d'une protection adéquate contre les applications d'IA susceptibles de porter atteinte à leurs droits fondamentaux. Le Livre blanc reconnaît que la définition ne couvre pas tous les cas en déclarant qu'«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».

28. Le CEPD est d'avis que l'approche visant à déterminer le niveau de risque que représente l'utilisation d'applications d'IA devrait être **plus solide** et **plus nuancée** et tenir compte des *Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679* du comité européen de la protection des données[24].

29. Compte tenu du principe de précaution, le CEPD recommande donc que le processus de détermination d'un risque élevé soit modifié comme suit lors du traitement de données à caractère personnel:

    - pour satisfaire le critère de l'«utilisation et de l'impact dommageables» du Livre blanc, le responsable du traitement devrait être tenu de procéder à une analyse d'impact relative à la protection des données afin de déterminer si l'application d'IA doit être considérée comme étant à haut risque;
    - les critères permettant de déterminer le niveau de risque devraient refléter les lignes directrices susmentionnées du comité européen de la protection des données et devraient donc inclure: une évaluation ou une notation, la prise de décisions automatisée ayant un effet juridique ou similaire significatif; le suivi systématique; les données sensibles; les données traitées à grande échelle; les ensembles de données qui ont été appariés ou combinés; les données relatives aux personnes concernées vulnérables; l'utilisation innovante ou l'application de solutions technologiques ou organisationnelles; le transfert de données au-delà des frontières extérieures de l'Union européenne; la question de savoir si le traitement en soi «empêche les personnes concernées d'exercer un droit ou d'utiliser un service ou un contrat»;
    - en outre, la Commission devrait reconnaître que les «risques, qui sont liés à un impact négatif potentiel sur les droits, libertés et intérêts des personnes concernées, devraient être déterminés en prenant en considération des critères objectifs spécifiques tels que la nature des données à caractère personnel (par exemple, des données sensibles ou non), la catégorie de personnes concernées (par exemple, des mineurs ou non), le nombre de personnes concernées affectées et la finalité du traitement. La gravité et la probabilité des effets sur les droits et libertés de la personne concernée constituent des

[24] Le comité européen de la protection des données a adopté les lignes directrices du groupe de travail «Article 29» de 2017 concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement «est susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679 (WP 248 rév. 01) lors de sa première réunion plénière le 25 mai 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

éléments à prendre en considération aux fins d'évaluer les risques pour la vie privée de l'individu»[25];

- le critère du «secteur» mentionné dans le Livre blanc devrait servir non pas de critère, mais de présomption qu'il est nécessaire, *par défaut*, de procéder à une évaluation (c'est-à-dire à une AIPD) des risques posés par l'application d'IA et que tout risque de ce type pourrait être encore plus grave que dans un autre secteur.

30. La notion du risque d'impact utilisée dans le Livre blanc paraît également définie de manière trop restrictive. Outre «l'impact sur les parties concernées», le CEPD considère que l'évaluation du niveau de risque lié à une utilisation donnée de l'IA devrait également reposer sur des **considérations sociétales plus larges**, notamment l'impact sur la démocratie, le respect de la légalité et l'État de droit, l'intérêt public, une surveillance générale potentiellement renforcée, l'environnement[26] et (des concentrations de) puissance sur le marché.

31. S'agissant de l'incidence spécifique sur les personnes physiques, le Livre blanc reconnaît que les dommages causés par l'IA peuvent être à la fois matériels et immatériels[27]. Toutefois, en ce qui concerne le type de dommage pris en considération pour déterminer le niveau de risque (élevé), le Livre blanc envisage un éventail beaucoup plus restreint de dommages et de risques[28]. Pour déterminer si des applications d'IA doivent être considérées comme présentant un risque élevé, le CEPD recommande à la Commission de ne pas se limiter à des considérations aussi étroites et de plutôt tenir compte systématiquement du **très large éventail de dommages et de risques qui pèsent sur les personnes physiques**.

32. En outre, bien que le Livre blanc reconnaisse (page 13) que les applications d'IA peuvent générer des risques résultant de «failles dans la conception globale des systèmes d'IA [...] ou de l'utilisation de données sans correction de biais éventuels», le CEPD recommande qu'il reconnaisse également que les applications d'IA peuvent aussi générer des risques en raison de leur caractère partial, voire arbitraire, d'une erreur dans l'attribution des variables ou de la non-classification de certaines données. Il devrait reconnaître en outre que des risques peuvent également résulter de l'*acte proprement dit* de délégation à des machines (en l'espèce, l'IA) de tâches qui étaient auparavant assignées à des êtres humains. **La décision de «résoudre» un problème sociétal à l'aide d'une application d'IA engendre des risques supplémentaires, qui doivent être analysés à l'aune d'un prétendu gain d'efficacité.**

[25] Groupe de travail «Article 29», 2014, *Déclaration concernant le rôle d'une approche fondée sur les risques dans les cadres juridiques relatifs à la protection des données*, p. 4 (en anglais).
[26] L'impact environnemental d'une formation à une application d'IA et celui de l'utilisation de l'IA pourraient nuire gravement aux objectifs environnementaux de l'UE: https://www.technologyreview.com/2019/06/06/239031/training-a-single-ai-model-can-emit-as-much-carbon-as-five-cars-in-their-lifetimes/
[27] «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», Livre blanc, page 12.
[28] «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 immatériel important; dont les effets ne peuvent être évités par les personnes physiques ou morales», Livre blanc, page 20.

À titre d'exemple, ces systèmes nécessitent une quantité considérable de données qui doivent être collectées et stockées, ce qui crée des risques en matière de protection de la vie privée et de sécurité; les applications d'IA risquent de ne pas être en mesure de prendre en considération des facteurs humains qui ne ressortent pas des données; les applications d'IA peuvent bénéficier d'une confiance humaine excessive et avoir l'apparence d'une vérité objective ou l'aura d'une fiabilité scientifique. Par conséquent, lorsqu'une application d'IA traite des données à caractère personnel, la nécessité et la proportionnalité du traitement doivent être démontrées[29].

33. Sur le nouveau cadre *uniquement* destiné aux applications d'IA *à haut risque*, le Livre blanc reconnaît les risques et les dommages *spécifiques* à l'IA que peuvent entraîner les applications d'IA (voir haut de la page 14). Pour y faire face, il propose de mettre à jour certains instruments législatifs de l'UE et, dans la mesure où tous les risques et dommages ne seraient pas couverts par la législation actuelle, de présenter des garanties spécifiques à l'IA dans un nouveau «cadre réglementaire pour l'IA».

34. Or, les mises à jour de la législation de l'UE suggérées dans le Livre blanc (section B) ne couvrent pas *tous* ces dommages et ces risques et les nouvelles garanties proposées (section D) ne couvrent que les risques résultant d'applications d'IA *à haut risque*. Si le CEPD comprend bien, alors que le Livre blanc reconnaît des types de risques et de dommages très variés causés spécifiquement par des applications d'IA, les mesures qu'il suggère ne résoudraient qu'une partie d'entre eux, à savoir la catégorie «à haut risque».

35. Cette approche ne reflète pas le principe de précaution appliqué par l'Union européenne dans la législation relative à la protection des données à caractère personnel[30]. L'approche suivie dans le RGPD (et dans le RPDUE) est également fondée sur les risques, mais – c'est un élément capital – elle est structurée en différents niveaux, alors que le Livre blanc sur l'IA semble adopter une approche du «tout ou rien»:

    - les règles du RGPD s'appliquent en partant du principe qu'il n'existe pas de traitement de données à caractère personnel «à risque zéro». Tout traitement de données à caractère personnel implique des risques (bien qu'ils puissent être minimes), en particulier le traitement automatisé et le traitement au moyen de nouvelles technologies. Par conséquent, en tout état de cause, différentes obligations devraient être remplies pour toutes les opérations de traitement. *En outre*, lorsque les risques augmentent (risque élevé), les obligations augmentent également;
    - à la différence de cette approche, le Livre blanc semble proposer que seules les applications d'IA à haut risque nécessitent des obligations supplémentaires spécifiques (en plus des obligations déjà applicables) et, si les risques diminuent, les obligations supplémentaires disparaissent.

[29] La raison qui sous-tend la mise en œuvre du système d'IA doit être clairement exposée et, dans le cas du rapport coût-efficacité et de l'efficacité, elle doit être bien étayée.
[30] Groupe de travail «Article 29», 2014, Déclaration concernant le rôle d'une approche fondée sur les risques dans les cadres juridiques relatifs à la protection des données, p. 4 (en anglais).

36. Le principe de précaution tel qu'il est traditionnellement appliqué dans l'UE[31] exige des mesures de précaution lorsque: 1) des risques inconnus sont impossibles à évaluer ou 2) il existe des risques graves, mais la probabilité qu'ils surviennent ne peut être prédite de manière adéquate Dans la pratique, le principe de précaution abaisse le seuil d'intervention réglementaire (réglementaire ou autre)[32] et son application au contexte de l'IA semble particulièrement pertinente[33]. Par conséquent, de l'avis du CEPD, il convient *néanmoins* d'éviter ou d'atténuer autant que faire se peut les risques et les dommages qui *ne satisfont pas* aux critères pour être considérés comme «à haut risque». À cet effet, le CEPD suggère que si la Commission devait présenter un nouveau cadre réglementaire spécifique à l'IA, un certain nombre de garanties raisonnables devraient s'appliquer à *toutes* les applications d'IA, *indépendamment* du niveau de risque, comme la mise en place de mesures techniques et organisationnelles (y compris la documentation[34]), la transparence complète concernant les objectifs, l'utilisation et la conception des systèmes algorithmiques mis en œuvre[35], la solidité du système d'IA ou la mise en œuvre et la transparence des mécanismes de responsabilité, de recours et de contrôle indépendants disponibles.

37. Alors que dans son approche de l'IA, la Commission s'efforce de ne pas «être excessivement normati[ve]» afin d'éviter de créer «une charge disproportionnée, en particulier pour les PME» (page 20), une telle approche pourrait, en revanche, aboutir à la création d'une charge disproportionnée pour les droits fondamentaux et les intérêts des personnes physiques. Le CEPD suggère de s'inspirer du débat similaire qui avait eu lieu durant les discussions et les négociations du RGPD et est d'avis que l'**approche par niveaux qui en a résulté dans le RGPD établit un meilleur équilibre entre les charges et les avantages**.

38. Le CEPD fait en outre remarquer que la protection des droits fondamentaux pourrait justifier, dans certains scénarios, non seulement des garanties spécifiques, mais aussi une **limitation claire de l'utilisation de l'IA lorsque certaines utilisations de la technologie sont, de toute évidence, incompatibles avec les droits fondamentaux**[36]. Le CEPD suggère dès lors que

[31] La Commission reconnaît que le principe de précaution s'applique dans les cas «où les données scientifiques sont insuffisantes, peu concluantes ou incertaines, mais où, selon des indications découlant d'une évaluation scientifique objective et préliminaire, il y a des motifs raisonnables de s'inquiéter que les effets potentiellement dangereux [...] soient incompatibles avec le niveau choisi de protection». Voir communication de la Commission européenne sur le recours au principe de précaution, COM(2000) 1 final, disponible à l'adresse: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52000DC0001&qid=1598550184977&from=FR

[32] Plutôt que des interdictions, des moratoires ou des suppressions progressives, les mesures de précaution peuvent aisément prendre la forme de normes renforcées, de stratégies de confinement, d'accords de licence, de mesures de contrôle, d'exigences en matière d'étiquetage, de dispositions relatives à la responsabilité ou de mécanismes d'indemnisation. Voir article 191, paragraphe 2, TFUE; voir aussi affaire C-180/96, Royaume-Uni/Commission, 1998, Rec. p. I-2269, point 99.

[33] Le CEPD considère que ce principe s'applique aux risques pour la vie privée et la protection des données à caractère personnel et il suggère dès lors d'envisager son application pour les risques liés à l'IA. Voir Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné, note de bas de page nº 53, p. 27: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_fr.pdf

[34] Une documentation transparente est un outil interne indispensable pour permettre aux responsables du traitement de gérer efficacement la responsabilité et pour le contrôle ex post par les autorités chargées de la protection des données, ainsi que pour l'exercice des droits par les personnes concernées. Cela va au-delà des informations à fournir aux personnes concernées et pourrait renforcer la protection jusqu'à ce qu'un mécanisme de vérification ex ante à part entière – et toutes les ressources, le savoir-faire et le consensus politique qu'il requiert – soit mis en place.

[35] Les secrets d'affaires et les droits de propriété intellectuelle ne sont qu'un moyen de défense partiel contre les exigences de transparence et ne peuvent être invoqués que dans la mesure strictement nécessaire pour protéger les intérêts de leurs titulaires.

[36] Le CEPD suggère également que des considérations éthiques interviennent dans l'utilisation qui est faite d'une application d'IA.

certains scénarios d'IA à haut risque devraient **être interdits dès le départ**: en suivant l'approche européenne du principe de précaution et, en particulier lorsque l'impact sur les personnes physiques et sur la société dans son ensemble n'est pas encore tout à fait compris, il conviendrait d'envisager une interdiction temporaire. Le CEPD considère que ces scénarios potentiels devraient être expressément abordés dans un éventuel cadre réglementaire futur. Il suggère de reprendre l'approche «prudente» et «adaptée aux risques» proposée par la Commission allemande d'éthique en matière de données, en interdisant totalement ou partiellement les systèmes algorithmiques «ayant un potentiel de dommage intenable»[37].

39. Outre les nouvelles exigences que la Commission pourrait imposer pour les applications d'IA et conformément aux principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, la Commission devrait également insister sur **l'obligation faite au secteur privé d'exercer un devoir de diligence et de prendre des mesures continues, documentées, proactives et réactives en faveur de la protection des droits de l'homme**. Les analyses de risques, qui font sens dans des environnements techniques où les opérateurs traitent leurs propres risques opérationnels, peuvent ne pas avoir la portée nécessaire pour évaluer l'impact sur les droits fondamentaux et une analyse d'impact relative à la protection des données (AIPD) (qui tienne également compte d'autres droits que le droit à la protection des données, le cas échéant) est plus appropriée.

4.2. Analyse d'impact relative à la protection des données

40. L'analyse d'impact relative à la protection des données (AIPD) prévue à l'article 35 du RGPD [*article 39 du RPDUE*] est un outil de **gestion des risques** en matière de droits et de libertés des personnes physiques. Une AIPD est obligatoire avant le traitement de données au moyen de technologies innovantes si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Le CEPD regrette que le Livre blanc ne mentionne pas explicitement les AIPD, en dépit de son engagement de réduire au minimum les risques liés à l'utilisation de l'IA sur «l'application des règles visant à protéger les droits fondamentaux».

41. Le déploiement de systèmes d'IA remplira très probablement au moins l'un des critères énoncés à l'article 35, paragraphe 3, du RGPD [*article 39, paragraphe 3, du RPDUE*][38]. En outre, l'article 35, paragraphe 4, du RGPD [*article 39, paragraphe 4, du RPDUE*] autorise les autorités chargées du contrôle de la protection des données de chaque État membre de l'UE (et le CEPD) à publier une liste des types d'opérations de traitement qui sont soumis à l'exigence de réalisation d'une AIPD. Le comité européen de la protection des données a publié des orientations supplémentaires concernant la détermination des cas où une AIPD est obligatoire[39]. Les autorités de contrôle de Pologne, d'Italie, de Grèce, d'Autriche et de République tchèque, notamment, imposent une AIPD pour certaines ou toutes les utilisations

[37] https://datenethikkommission.de/wp-content/uploads/191023_DEK_Kurzfassung_en_bf.pdf

[38] Les traitements de données sont soumis à l'obligation de réaliser une AIPD lorsque: 1) il existe une évaluation systématique et approfondie de données à caractère personnel fondée sur un traitement automatisé, y compris un profilage, et sur la base de laquelle sont prises des décisions qui produiront des effets importants d'ordre juridique ou similaire; 2) le traitement implique une grande quantité de données sensibles ou des données relatives à des condamnations ou des infractions pénales ou 3) le traitement implique le contrôle systématique de vastes zones accessibles au public.

[39] Le groupe de travail «Article 29» a adopté un document intitulé «Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) 2016/679», qui contient des lignes directrices détaillées sur le moment où une AIPD doit être réalisée et les modalités selon lesquelles elle doit l'être.

de systèmes d'IA (en Pologne, par exemple, une AIPD est requise pour «l'évaluation de la solvabilité, au moyen d'algorithmes d'IA», tandis qu'en République tchèque, une AIPD est demandée pour les «systèmes experts automatisés incluant une IA» lorsqu'ils sont utilisés à des fins d'analyse ou de profilage de systèmes informatiques d'IA).

42. L'article 35 du RGPD [*article 39 du RPDUE*] évoque un risque potentiellement élevé «pour les droits et libertés des personnes physiques». La référence aux «droits et libertés» des personnes concernées **vise principalement les droits à la protection des données et à la vie privée**, mais s'entend également, **le cas échéant, pour d'autres droits fondamentaux**, tels que la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté ainsi que la liberté de conscience et de religion[40].

43. Il est important de souligner que les exigences du RGPD concernent une AIPD incluant non seulement une évaluation des risques, mais également une description détaillée du traitement de données envisagé. Le volet relatif à l'évaluation des risques vise à recenser les risques et les mesures à prendre pour les prévenir et les atténuer. Les risques doivent être mesurés les uns par rapport aux autres et il convient de leur attribuer une valeur ou une note afin de pouvoir les classer. Cette valeur devrait être fondée sur la probabilité et la gravité du risque. La description du traitement de données envisagé devrait inclure l'étendue, la nature, le contexte et les finalités du traitement.

44. L'AIPD requiert également une **évaluation de la nécessité et de la proportionnalité** du traitement. L'évaluation de la nécessité devrait démontrer que le déploiement de l'IA est effectivement l'outil le plus approprié pour atteindre l'objectif d'un traitement de données spécifique. S'il existe d'autres méthodes moins intrusives présentant un niveau moindre de risques potentiels susceptibles de contribuer aussi bien à atteindre la finalité du traitement, des arguments précis sont nécessaires afin d'expliquer pourquoi le responsable du traitement a plutôt choisi de recourir à l'IA.

    L'évaluation de la proportionnalité devrait tenir compte de différents facteurs, notamment:

    - l'intérêt des responsables du traitement et les droits et libertés des personnes physiques et
    - les attentes raisonnables des personnes physiques et la finalité du traitement.

    Le CEPD souligne que si l'analyse d'impact relative à la protection des données révèle que le traitement engendrerait un risque élevé pour les droits et libertés des personnes concernées, à moins que le responsable du traitement ne prenne des mesures pour atténuer le risque, il y a obligation de consulter l'autorité de contrôle conformément à l'article 36, paragraphe 1, du RGPD [*article 40, du RPDUE*]. **Le CEPD suggère donc qu'un futur cadre juridique impose l'obligation d'une analyse d'impact pour *tout* déploiement envisagé de systèmes d'IA.** Lorsque ce déploiement implique le traitement de données à caractère personnel, les exigences du RGPD relatives à l'AIPD doivent être respectées; dans les autres cas, l'analyse d'impact de l'IA proposée pourrait comprendre les éléments principaux suivants:

[40] Comité européen de la protection des données, Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248 rév.01.

1. Identification des droits fondamentaux concernés
    a. Quels sont les droits fondamentaux affectés ou potentiellement affectés?
    b. Quelle est la nature de ces droits fondamentaux? Un droit absolu est-il affecté?
2. Identification des risques qui pèsent sur ces droits pendant la phase de développement et la phase de déploiement
    a. Quels sont les facteurs de risque?
    b. Quelle est la probabilité que les risques se concrétisent?
    c. Dans quelle mesure les risques ont-ils une incidence sur les droits fondamentaux?
3. Identification des mesures d'atténuation pour les droits concernés
    a. Quelles sont les méthodes techniques ou organisationnelles disponibles pour garantir que l'essentiel des droits fondamentaux ne sera pas affecté?
4. Mise en balance des intérêts et des risques
    a. Quels sont les effets positifs/négatifs de la limitation des droits fondamentaux?
    b. Quels sont les effets positifs/négatifs du traitement pour la personne physique[41]?

Le CEPD est d'avis que l'introduction d'une telle analyse des risques est conforme à la stratégie de la Commission visant à une meilleure mise en œuvre de la Charte des droits fondamentaux par l'Union européenne[42]. Par conséquent, bien qu'il ne s'agisse pas d'une idée totalement nouvelle en soi, son application devrait être envisagée pour le traitement de données à caractère personnel au moyen de l'IA, compte tenu de l'incidence grave et du caractère innovant de la technologie.

45. Enfin, le CEPD recommande dans la mesure du possible de **publier** les résultats de ces évaluations ou, à tout le moins, les principaux résultats et conclusions de l'AIPD, afin de renforcer la confiance et la transparence.

4.3. Responsabilité et application

46. À la page 11 du Livre blanc, la Commission déclare que «certaines spécificités de l'IA (telles que l'opacité) peuvent compliquer l'application et le contrôle de l'application de cette législation». Selon le document, ces difficultés d'application nécessiteraient d'«examiner si la législation actuelle est en mesure de faire face aux risques liés à l'IA et si son respect peut être assuré efficacement, si elle doit être adaptée, ou si une nouvelle législation s'impose».

47. À la page 14, le Livre blanc détaille les particularités qui caractérisent de nombreuses applications d'IA, notamment l'«opacité ("effet de boîte noire"), la complexité, l'imprévisibilité et le comportement partiellement autonome», et il précise qu'ils «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-

[41] Voir Heleen L. Janssen, «*An approach for a fundamental rights impact assessment to automated decision-making*» International Data Privacy Law, Volume 10, Issue 1, février 2020, p. 76-106, https://doi.org/10.1093/idpl/ipz028.
[42] Communication de la Commission européenne, «*Stratégie pour la mise en œuvre effective de la Charte des droits fondamentaux par l'Union européenne*», COM(2010) 573 final, Bruxelles, 19/10/2010.

ci». Ces caractéristiques ne sont toutefois pas propres aux applications d'IA. À titre d'exemple, le traitement de données à caractère personnel au moyen de techniques de mégadonnées peut être aussi complexe et certaines applications qui n'utilisent pas l'IA (par exemple, celles qui gèrent des trains automatisés[43]) sont partiellement ou totalement autonomes.

48. L'opacité attribuée à certains types d'applications d'IA est liée à l'incapacité de l'homme d'expliquer le raisonnement qui sous-tend la décision prise par une application d'IA. Ce problème trouve son origine dans la manière dont ces applications représentent les connaissances et les expériences qu'elles utilisent pour prendre des décisions. Le CEPD suggère donc que **les procédures transparentes d'essai et d'audit**, mentionnées à la section 5.F dans le contexte des évaluations de conformité préalables, fassent partie de toute application d'IA traitant des données à caractère personnel. Rendre ces procédures accessibles au public garantirait que les autorités de contrôle puissent accomplir leurs tâches, mais renforcerait également la confiance de l'utilisateur dans les applications d'IA.

49. Si, comme le suggère le Livre blanc, l'opacité ou d'autres spécificités de l'IA requièrent une révision de la législation actuelle, **le CEPD insiste sur la nécessité d'une analyse rigoureuse des lacunes réglementaires dans les analyses d'impact**, comme l'imposent les lignes directrices de la Commission pour une meilleure réglementation[44] ainsi que l'accord interinstitutionnel entre le Parlement européen, le Conseil de l'Union européenne et la Commission européenne «Mieux légiférer»[45]. Une telle analyse décrirait les caractéristiques pertinentes de l'IA, les lacunes de la législation actuelle nécessitant une modification et l'approche des modifications proposées pour combler ces lacunes.

50. Le Livre blanc se demande si les autorités compétentes et les personnes concernées pourraient «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». Le CEPD tient à rappeler le principe de responsabilité qui sous-tend le RGPD, en vertu duquel il incombe au responsable du traitement de démontrer la conformité du traitement avec le RGPD. Les allégations concernant l'absence de biais discriminatoire humain (ou autre) dans une application d'IA devraient être vérifiables[46].

51. Le Livre blanc s'inquiète[47] du manque potentiel de moyen des autorités de contrôle pour faire appliquer la réglementation actuelle sur l'IA. Le CEPD partage cette inquiétude et souligne la nécessité de doter les autorités de contrôle des ressources nécessaires pour suivre non seulement l'évolution de l'IA, mais également tout développement technologique[48].

[43] https://en.wikipedia.org/wiki/List_of_automated_train_systems
[44] https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_fr
[45] JO L 123 du 12.5.2016, p. 1-14.
[46] Par exemple, en novembre 2019, un développeur de logiciels de premier plan a affirmé que la carte de crédit d'Apple était «sexiste» à l'égard des femmes demandant un crédit. La complexité du système d'IA n'a pas permis à l'établissement de crédit de prouver son caractère équitable. Le Département des services financiers de l'État de New York instruit actuellement le dossier.
https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html
[47] «[...] les autorités répressives peuvent se trouver dans une situation où elles [...] ne disposent pas des capacités techniques appropriées pour contrôler les systèmes».
[48] Un rapport publié en avril 2020 a évalué le personnel technique et le budget des autorités chargées de la protection des données dans l'UE depuis l'entrée en vigueur du RGPD et a critiqué le développement de leur capacité technique de répression.

L'évaluation du RGPD par le comité européen de la protection des données a révélé[49] que la plupart des autorités chargées de la protection des données considéraient que leurs «ressources humaines, financières et techniques» n'étaient pas suffisantes. Il convient d'encourager la coopération et des enquêtes conjointes entre tous les organes de contrôle pertinents, y compris les autorités chargées de la protection des données.

52. Le Livre blanc indique (page 16) qu'«[e]n 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». Le CEPD est d'avis que la transparence des applications d'IA va plus loin que l'intelligibilité et inclut la fourniture aux utilisateurs d'informations claires sur l'utilisation des systèmes d'IA.

4.4. Exigences réglementaires

53. Le CEPD se réjouit de la liste des exigences réglementaires figurant à la section 5.D, qui recoupe largement la législation existante en matière de protection des données et la **déclaration susvisée sur l'éthique et la protection des données dans le secteur de l'IA**. Il estime toutefois que des exigences telles que l'absence de discrimination injuste ou la robustesse et la précision sont si fondamentales qu'elles devraient s'appliquer à tout système d'IA et pas uniquement aux applications d'IA «à haut risque».

54. Le CEPD est d'avis que la plupart des exigences décrites à la section 5.D, comme «robustesse et précision» ou «des informations devraient être clairement fournies aux citoyens lorsqu'ils interagissent avec un système d'IA et non avec un être humain», sont couvertes par les règles existantes en matière de protection des données. Le CEPD salue l'approche suivie pour l'exigence de contrôle humain, qui est conforme à la responsabilisation individuelle prévue dans la **déclaration de l'ICDPPC susvisée sur l'éthique et la protection des données dans le secteur de l'IA** et va plus loin que les exigences prévues à l'article 22 du RGPD [*article 24 du RPDUE*].

55. Le CEPD convient de l'importance d'exiger la fourniture d'informations. Néanmoins, la granularité appropriée des informations dépendra du contexte. Par conséquent, le CEPD recommande d'**élaborer des normes d'information** en vue d'harmoniser les informations fournies aux personnes physiques pour différents types de systèmes d'IA.

4.5. Contrôles et gouvernance

56. La section 5.F du Livre blanc propose une évaluation objective préalable de la conformité obligatoire pour les systèmes d'IA à haut risque. La Commission européenne définit[50] l'évaluation de la conformité comme une analyse de risques qui garantit que les produits respectent certaines règles avant de les mettre sur le marché et est menée durant les phases de conception et de production.

[49] Contribution du comité européen de la protection des données à l'évaluation du RGPD au titre de l'article 97 (p. 30), https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en (en anglais).
[50] https://europa.eu/youreurope/business/product-requirements/compliance/conformity-assessment/index_fr.htm

57. D'une part, l'évaluation préalable de la conformité vérifierait le respect des exigences réglementaires décrites à la section 5.D. D'autre part, une AIPD (qui serait obligatoire pour les systèmes d'IA à haut risque conformément au RGPD) aiderait le responsable du traitement à vérifier la conformité avec le RGPD. Le CEPD constate un conflit potentiel entre ces deux contrôles en raison du chevauchement de leurs exigences respectives. Des conclusions divergentes résultant de chacun des contrôles relatifs à un système d'IA seraient source de confusion et d'insécurité juridique et devraient donc être évitées. Le CEPD recommande dès lors que la Commission veille à ce que le futur cadre réglementaire éventuel ne crée pas de chevauchements entre les autorités de contrôle et intègre un mécanisme de coopération entre celles-ci.

58. Le Livre blanc demande la mise en place de mécanismes de conformité similaires «*si [les mécanismes d'évaluation de la conformité] n'existent pas*», mais il ne précise pas quelles seraient les autorités compétentes pour gérer ce mécanisme de conformité. Si la Commission européenne devait donner suite à la demande de création d'une Agence européenne de l'IA[51], la question de savoir comment elle éviterait un chevauchement des compétences reste sans réponse claire.

59. La section 5.G propose un mécanisme volontaire d'étiquetage pour les systèmes d'IA qui ne sont pas classés comme présentant un risque élevé. Cette étiquette serait utilisée pour les personnes qui s'engagent à respecter les exigences réglementaires énoncées à la section 5.D ou un ensemble spécifique d'exigences similaires élaborées spécialement pour ce mécanisme d'étiquetage. Toutefois, l'IA ne dispose pas de normes permettant aux développeurs d'applications d'IA de vérifier systématiquement leur conformité. En l'absence de telles normes, la valeur du mécanisme volontaire d'étiquetage serait, au mieux, limitée.

60. Le CEPD se réjouit de la référence à l'application et au contrôle de suivi *ex post* par les autorités compétentes. Ces contrôles ne devraient toutefois pas se limiter à vérifier les documents et à tester les applications. D'autres aspects, tels que le contrôle de la transparence (y compris la capacité d'expliquer comment le système prend des décisions) et les tests réalisés sur les données de formation afin de garantir leur adéquation, pourraient également être nécessaires.

61. Le CEPD souscrit pleinement aux objectifs définis par le Livre blanc pour une structure de gouvernance européenne sur l'IA («*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*»). Comme indiqué plus loin dans le document, il sera essentiel que cette structure évite de dupliquer des fonctions existantes et qu'elle fasse appel aux autorités qui existent déjà au niveau de l'UE, comme le comité européen de la protection des données.

[51] Parlement européen, Commission des affaires juridiques, Projet de rapport contenant des recommandations à la Commission concernant un cadre d'aspects éthiques en matière d'intelligence artificielle, de robotique et de technologies connexes, https://www.europarl.europa.eu/doceo/document/JURI-PR-650508_FR.pdf

5. AUTRES QUESTIONS SPÉCIFIQUES

5.1. Identification biométrique à distance

62. Le Livre blanc reconnaît les risques que pose l'identification biométrique à distance (IBD) pour les droits fondamentaux, une observation que partage le CEPD. L'identification biométrique à distance soulève deux questions: l'identification (à distance, évolutive et parfois cachée) des personnes physiques et le traitement (à distance, évolutif et parfois caché) de leurs données biométriques. Les technologies connexes à l'une ou l'autre de ces deux caractéristiques, qu'elles reposent ou non sur l'IA, peuvent être tout aussi problématiques et peuvent devoir être soumises aux mêmes limitations que l'IBD.

63. Les risques que font peser les systèmes d'IBD sur les droits et libertés des personnes, comme la reconnaissance faciale en direct dans les lieux publics, doivent être dûment recensés et atténués et ce processus devrait faire intervenir les personnes les plus affectées par l'utilisation de cette technologie. Certains des risques que comporte l'IBD proviennent du fait que les systèmes d'IBD sont facilement cachés, sans contact et sont souvent présentés comme une simple «expérience», mais ils pourraient aisément être transformés en un système complexe de surveillance omniprésent et intrusif.

64. Une fois l'infrastructure soutenant l'IBD mise en place, elle peut aisément être utilisée à d'autres fins («détournement d'usage»). D'aucuns ont récemment affirmé que des systèmes d'IBD, ou des éléments d'autres infrastructures techniques, pourraient servir à lutter contre la pandémie actuelle de différentes manières, par exemple en mesurant la distance sociale ou l'utilisation des masques ou en réalisant des contrôles de température (lorsque les caméras sont dotées de thermomètres intégrés). Certaines de ces nouvelles applications pourraient ne pas relever du champ d'application du RGPD, mais auraient néanmoins un effet paralysant sur les sociétés démocratiques. De telles utilisations de l'IA et ces détournements d'usage devraient être dûment pris en compte par toute réglementation sur l'IA.

65. Si l'IBD peut poser de graves problèmes en matière de droits fondamentaux, le CEPD tient à souligner que les technologies liées à l'IBD qui n'ont pas pour objet d'identifier des personnes physiques soulèvent quant à elles de graves préoccupations en matière de respect de la vie privée également: par exemple, la détection des émotions – fondée sur la reconnaissance faciale en temps réel – peut permettre de déduire les sentiments des personnes[52].

66. Il est extrêmement important de déterminer si la technologie est nécessaire ou proportionnée dans la situation particulière où elle sera déployée, voire si elle est souhaitable[53]. En ce qui concerne l'identification biométrique à distance, le CEPD est favorable à l'idée d'un **moratoire sur le déploiement, dans l'espace public de l'UE, d'un système automatisé de reconnaissance de caractéristiques humaines**, non seulement des visages, mais aussi de la démarche, des empreintes digitales, de l'ADN, de la voix, de la pression sur des touches et d'autres signaux biométriques ou comportementaux, de sorte qu'un débat démocratique et éclairé puisse avoir lieu, jusqu'au moment où l'UE et les États membres disposeront de toutes les garanties appropriées, y compris un cadre juridique complet assurant la proportionnalité des différentes technologies et systèmes pour chaque type d'utilisation spécifique.

[52] Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements https://journals.sagepub.com/stoken/default+domain/10.1177%2F1529100619832930-FREE/pdf (en anglais).
[53] Une étude de 2020 menée par l'Agence des droits fondamentaux de l'Union européenne a révélé que **plus de 80 % des Européens sont opposés à la transmission de leurs données faciales aux autorités**.

67. L'**utilisation de l'IBD par les pouvoirs publics** en période d'urgence nationale, par exemple en cas de crise sanitaire nationale ou transfrontière, **devrait toujours être nécessaire pour des raisons d'intérêt public supérieur, conformément au droit de l'Union ou de l'État membre, être transparente, responsable, proportionnée** à l'objectif poursuivi, **soumise à des garanties spécifiques, clairement limitée dans le temps et compatible avec l'essence des droits fondamentaux et le respect de la dignité humaine**.

5.2. Groupes vulnérables

68. Le CEPD se réjouit du fait que la Commission reconnaît les risques spécifiques que les systèmes d'IA tendent à faire peser sur les groupes de personnes vulnérables. Le Livre blanc ne prend toutefois ces risques explicitement en compte qu'en ce qui concerne «les droits au respect de la vie privée et à la protection des données à caractère personnel au cœur des préoccupations en matière de droits fondamentaux lorsqu'une technologie de reconnaissance faciale est utilisée» lorsqu'il «pourrait 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».

69. Tout d'abord, en l'absence de définition juridique formellement adoptée des groupes vulnérables, le CEPD suggère une **approche pragmatique adaptée au contexte**. Les groupes vulnérables devraient inclure les enfants, les personnes âgées et les personnes handicapées, les minorités ethniques ou les groupes historiquement marginalisés, les femmes, les communautés LGBTQIA+, les travailleurs et d'autres personnes menacées d'exclusion.

70. Par ailleurs, le CEPD considère que la question des groupes vulnérables **ne devrait pas seulement être prise en considération dans le contexte des systèmes d'identification biométrique à distance**, mais dans un contexte beaucoup plus large. Le CEPD souligne que les systèmes d'IA devraient être équitables et respectueux de la dignité humaine et des droits et libertés des personnes physiques. Dans le contexte des groupes vulnérables, l'équité implique la **non-discrimination**. Une discrimination volontaire ou involontaire est une caractéristique intrinsèque d'une prise de décision par l'homme et si l'on n'agit pas avec prudence, les systèmes d'IA peuvent refléter ce biais humain naturel. Comme le déclare à juste titre le Livre blanc, «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». Ils peuvent avoir des ramifications directes et indirectes dans de nombreux aspects de la vie, notamment sociaux, économiques et sanitaires.

71. En tout état de cause, lorsque de tels biais sont présents dans un système d'IA, il existe un risque élevé de dommages tangibles (dommages matériels aux biens, perte quantifiable) et intangibles (atteinte à la vie privée, limitations du droit à la dignité humaine). Les intérêts particuliers des groupes vulnérables devraient dès lors être pris en compte dans toute situation similaire à celles visées dans la liste ci-dessus. Le CEPD encourage la Commission à fournir une liste non exhaustive des applications de l'IA dans divers secteurs et à des fins diverses susceptibles de mettre en péril le droit à l'égalité de traitement et le droit à la non-discrimination, tels qu'ils sont consacrés par les articles 20 et 21 de la Charte des droits fondamentaux de l'Union européenne.

72. Le CEPD suggère que pour éviter ces répercussions négatives, les groupes vulnérables soient pris en considération lors du développement et de l'utilisation de l'IA. Même à un stade

précoce, lors de la formation aux systèmes d'IA, une attention particulière devrait être accordée aux groupes vulnérables, étant donné que, la plupart du temps, les erreurs de l'IA résultent d'un étiquetage incorrect des données de formation ou d'ensembles de données non représentatifs. Comme l'indique le Livre blanc, des **exigences** pourraient être envisagées afin que des «mesures raisonnables so[ie]nt 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». Ces mesures pourraient inclure, par exemple, l'exigence d'un niveau d'entrée pour évaluer la qualité des données, la possibilité d'un contrôle humain, un recours ou un «droit à une explication» lorsque le déploiement de l'IA a des répercussions négatives sur la personne, d'une façon similaire à ce que prévoient les dispositions de l'article 22, paragraphe 4, du RGPD sur la prise de décisions automatisée et le profilage.

5.3. Accès aux données

73. Le Livre blanc présente l'*edge computing* (ou traitement des données à la périphérie) comme une tendance intéressante de l'évolution et du développement de l'IA. Ce point de vue est conforme à celui exprimé dans la stratégie de la Commission européenne pour les données. Cependant, ni le Livre blanc ni la stratégie pour les données n'expliquent comment une localisation physique plus proche des données se traduirait par une meilleure disponibilité de celles-ci ou par une plus grande fiabilité de l'IA.

74. Bien que la localisation des données puisse avoir des conséquences juridiques (par exemple sur la législation ou la réglementation applicable aux transferts internationaux de données à caractère personnel), la disponibilité des données ne dépend pas de leur localisation physique, mais bien des contrôles techniques d'accès à ces données [par exemple au moyen d'interfaces de programmes d'application (API) et de formats d'échange de données]. Les données proches des utilisateurs (comme les données stockées dans une montre connectée) pourraient leur être inaccessibles à moins qu'une API ou un autre moyen technique ne permettent d'y accéder. D'autre part, les données stockées dans un *cloud* privé situé à des milliers de kilomètres pourraient être à portée de main, si le stockage en nuage est aisément accessible pour ses utilisateurs.

75. Le CEPD est d'avis que la Commission devrait promouvoir le développement et l'adoption d'interfaces de programmes d'application (API) normalisées[54]. L'adoption de ces API faciliterait l'accès aux données pour les utilisateurs autorisés, quelle que soit la localisation de ces données et en améliorerait la portabilité.

76. Le CEPD souligne que le cadre réglementaire de l'UE devrait s'appliquer aux ensembles de données publiés en dehors de l'UE, mais utilisés dans l'Union. Les applications d'IA développées ou utilisées par le secteur public européen ou par des entreprises ne peuvent pas s'appuyer sur des ensembles de données non conformes à la législation de l'UE en matière de protection des données ou contraires aux droits fondamentaux et aux valeurs de l'UE.

[54] Les établissements de crédit élaborent des API en vue d'assurer un accès «objectif, non discriminatoire et proportionné» aux données financières, comme l'impose la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

6. CONCLUSIONS

77. Le CEPD partage totalement l'avis de la Commission sur la nécessité d'une approche européenne de l'IA et, à cet égard, se félicite vivement de l'engagement pris par le Livre blanc en faveur des droits fondamentaux et des valeurs de l'UE.

78. Le CEPD est toutefois d'avis que les propositions contenues dans le Livre blanc doivent faire l'objet d'ajustements et de clarifications supplémentaires sur certains points. Parmi les sujets qui nécessiteraient une plus grande clarté dans une éventuelle proposition législative future figurent le lien entre les risques engendrés par l'IA et les lacunes législatives connexes, l'approche fondée sur les risques qui est appliquée aux systèmes d'IA et la définition de l'IA proprement dite, qui devrait permettre de définir clairement le champ d'application de la législation proposée.

79. Le CEPD recommande en outre que tout nouveau cadre réglementaire relatif à l'IA:

- **s'applique tant** aux États membres de l'UE qu'aux institutions, organes et organismes de l'UE;

- soit conçu dans l'optique de **protéger de tout effet négatif** non seulement les personnes physiques, mais également les communautés et la société dans son ensemble;

- propose **un système de classification des risques plus solide et plus nuancé**, garantissant que tout dommage important potentiel découlant des applications d'IA soit compensé par des mesures d'atténuation appropriées;

- inclue une analyse d'impact **définissant clairement les lacunes réglementaires** qu'il entend combler;

- **évite les chevauchements** entre les différentes autorités de contrôle et inclue un mécanisme de coopération.

80. En ce qui concerne l'identification biométrique à distance, le CEPD est favorable à l'idée d'un **moratoire sur le déploiement, dans l'espace public de l'UE, d'un système automatisé de reconnaissance de caractéristiques humaines**, non seulement des visages, mais aussi de la démarche, des empreintes digitales, de l'ADN, de la voix, de la pression sur des touches et d'autres signaux biométriques ou comportementaux, de sorte qu'un débat démocratique et éclairé puisse avoir lieu, jusqu'au moment où l'UE et les États membres disposeront de toutes les garanties appropriées, y compris un cadre juridique complet assurant la proportionnalité des différentes technologies et systèmes pour chaque type d'utilisation spécifique.

81. Si un nouveau cadre juridique tel que celui présenté dans le Livre blanc et dans le programme de travail de la Commission devait voir le jour, le CEPD fournira un avis supplémentaire à la Commission, comme le prévoit l'article 42 du RPDUE.

Bruxelles, le 29 juin 2020

Wojciech Rafał WIEWIÓROWSKI