Avis conjoint 05/2021

de l'EDPB et du CEPD

sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle)

18 juin 2021

Synthèse

Le 21 avril 2021, la Commission européenne a présenté sa proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (ci-après la «proposition»). Le comité européen de la protection des données (EDPB) et le CEPD se rallient aux préoccupations formulées par le législateur quant à l'utilisation de l'intelligence artificielle (IA) au sein de l'Union européenne (UE) et soulignent que la proposition a de très importantes **implications en matière de protection des données**.

L'EDPB et le CEPD notent que la **base juridique** de la proposition est en premier lieu l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE). En outre, la proposition est également fondée sur l'article 16 du TFUE dans la mesure où elle contient des règles spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, notamment des restrictions à l'utilisation de systèmes d'IA pour l'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives. L'EDPB et le CEPD rappellent que, conformément à la jurisprudence de la Cour de justice de l'Union européenne (CJUE), l'article 16 du TFUE fournit une base juridique appropriée dans les cas où la protection des données à caractère personnel constitue l'un des objectifs ou éléments essentiels des règles adoptées par le législateur de l'Union. L'application de l'article 16 TFUE implique également la **nécessité d'assurer un contrôle indépendant du respect** des exigences relatives au traitement des données à caractère personnel, comme l'exige également l'article 8 de la charte des droits fondamentaux de l'Union européenne.

En ce qui concerne le **champ d'application de la proposition**, l'EDPB et le CEPD se félicitent vivement de son extension à la fourniture et à l'utilisation de systèmes d'IA par les institutions, organes ou agences de l'UE. Toutefois, l'**exclusion de la coopération internationale en matière répressive du champ d'application** de la proposition suscite de vives inquiétudes pour l'EDPB et le CEPD, étant donné qu'une telle exclusion crée un risque important de contournement (par exemple, de la part des pays tiers ou d'organisations internationales exploitant des applications à haut risque sur lesquelles s'appuient les autorités publiques de l'UE).

L'EDPB et le CEPD **se félicitent de l'approche fondée sur les risques** qui sous-tend la proposition. Toutefois, cette approche devrait être clarifiée et la notion de «risque pour les droits fondamentaux» alignée sur le RGPD et le règlement (UE 2018/1725 (RPDUE), étant donné que des aspects liés à la protection des données à caractère personnel entrent en jeu.

L'EDPB et le CEPD partagent le constat exprimé dans la proposition selon lequel la classification d'un **système d'IA comme étant à haut risque ne signifie pas nécessairement qu'il est licite** en soi et peut être déployé par l'utilisateur en tant que tel. Il se peut que le responsable du traitement ait à **respecter d'autres exigences découlant de la législation de l'UE en matière de protection des données**. De surcroît, le respect des obligations légales découlant de la législation de l'Union (y compris en matière de protection des données à caractère personnel) devrait être une condition préalable à l'entrée sur le marché européen d'un produit muni du marquage CE. À cette fin, l'EDPB et le CEPD estiment que **l'obligation de garantir le respect du RGPD et du RPDUE devrait figurer au chapitre 2 du titre III**. En outre,

l'EDPB et le CEPD estiment nécessaire d'adapter la procédure d'évaluation de la conformité de la proposition de manière à ce que des tiers effectuent toujours des évaluations ex ante de la conformité des systèmes d'IA à haut risque.

Compte tenu du risque élevé de discrimination, la proposition interdit la «notation sociale» lorsqu'elle est effectuée «au cours d'une période donnée» ou «par les autorités publiques ou pour le compte de celles-ci». Toutefois, les entreprises privées, telles que les fournisseurs de services de médias sociaux et d'informatique en nuage, peuvent également traiter de grandes quantités de données à caractère personnel et procéder à une notation sociale. Par conséquent, **la future réglementation en matière d'IA devrait interdire tout type de notation sociale**.

L'identification biométrique à distance des personnes dans des espaces accessibles au public présente un risque élevé d'intrusion dans leur vie privée, ce qui a de graves répercussions sur les attentes des populations en matière d'anonymat dans les espaces publics. Pour ces raisons, l'EDPB et le CEPD **demandent une interdiction générale de toute utilisation de l'IA en vue d'une reconnaissance automatisée des caractéristiques humaines dans des espaces accessibles au public** - 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 - dans n'importe quel contexte. Il est également recommandé d'**interdire les systèmes d'IA qui classent les individus à partir des données biométriques dans des groupes** en fonction de l'origine ethnique, du sexe, ainsi que de l'orientation politique ou sexuelle, ou d'autres motifs de discrimination au sens de l'article 21 de la charte. Par ailleurs, l'EDPB et le CEPD estiment que l'utilisation de l'IA pour **déduire les émotions d'une personne physique est hautement indésirable et devrait être interdite.**

L'EDPB et le CEPD saluent **la désignation du CEPD comme l'autorité compétente et l'autorité de surveillance du marché pour la supervision des institutions, agences et organes de l'Union**. Cependant, le rôle et les tâches du CEPD devraient être précisés, notamment en ce qui concerne son rôle d'autorité de surveillance du marché. En outre, la future réglementation en matière d'IA devrait clairement établir l'**indépendance des autorités de surveillance** dans l'exécution de leurs tâches de surveillance et d'exécution.

La désignation des autorités de protection des données (APD) en tant qu'autorités de contrôle nationales garantirait une approche réglementaire plus harmonisée, contribuerait à l'interprétation cohérente des dispositions relatives au traitement des données et éviterait les contradictions dans leur application entre les États membres. Par conséquent, l'EDPB et le CEPD considèrent que **les autorités de protection des données devraient être désignées comme autorités de contrôle nationales conformément à l'article 59 de la proposition.**

La proposition attribue un rôle prédominant à la Commission au sein du «Comité européen de l'intelligence artificielle» (le «Comité»). Ce rôle va à l'encontre de la nécessité, pour un organisme européen de l'IA, d'être indépendant de toute influence politique. Pour garantir son indépendance, le futur règlement sur l'intelligence artificielle devrait donner **plus d'autonomie au Comité européen de l'intelligence artificielle** et faire en sorte qu'il puisse agir de sa propre initiative.

Compte tenu de la diffusion des systèmes d'IA dans le marché unique et de la probabilité d'affaires transfrontières, il est indispensable d'harmoniser l'application de la législation et de répartir correctement les compétences entre les autorités de contrôle nationales. L'EDPB et le CEPD suggèrent d'envisager **un**

mécanisme garantissant un point de contact unique pour les personnes concernées par la législation ainsi que pour les entreprises, pour chaque système d'IA.

En ce qui concerne les **bacs à sable**, l'EDPB et le CEPD **recommandent de préciser leur champ d'application et leurs objectifs**. La proposition devrait également indiquer clairement que la base juridique de ces bacs à sable devrait être conforme aux exigences établies dans le cadre existant en matière de protection des données.

Le **système de certification** décrit dans la proposition **n'a pas de relation claire avec la législation de l'UE en matière de protection des données** ainsi qu'avec les autres législations de l'UE et des États membres applicables à chaque «domaine» de systèmes d'IA à haut risque et ne tient pas compte des **principes de minimisation des données et de protection des données dès la conception** comme l'un des aspects à prendre en considération **avant l'obtention du marquage CE**. Par conséquent, l'EDPB et le CEPD recommandent de modifier la proposition afin de clarifier la relation entre les certificats délivrés au titre dudit règlement et les certifications, sceaux et marques de protection des données. Enfin, les APD devraient être associées à l'élaboration et à l'établissement de normes harmonisées et de spécifications communes.

En ce qui concerne les **codes de conduite**, l'EDPB et le CEPD estiment qu'il est **nécessaire de préciser** si la protection des données à caractère personnel doit être considérée comme faisant partie des «exigences supplémentaires» auxquelles ces codes de conduite peuvent répondre, et de veiller à ce que les «spécifications et solutions techniques» ne soient pas incompatibles avec les règles et principes du cadre existant de l'UE en matière de protection des données.

TABLE DES MATIERES

L'EDPB et le contrôleur européen de la protection des données

vu l'article 42, paragraphe 2, du règlement (UE) 2018/1725 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[1],

vu l'accord sur l'Espace économique européen (EEE) et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[2],

vu la demande d'avis conjoint du Contrôleur européen de la protection des données et du comité européen de la protection des données du 22 avril 2021 sur la proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle (législation en matière d'intelligence artificielle),

ONT ADOPTÉ L'AVIS CONJOINT SUIVANT

1 INTRODUCTION

1. L'avènement des systèmes d'intelligence artificielle («IA») constitue une étape très importante dans l'évolution des technologies et dans la manière dont les humains interagissent avec elles. L'IA est un ensemble de technologies clés qui modifieront profondément notre vie quotidienne, que ce soit sur le plan sociétal ou économique. Au cours des prochaines années, des décisions majeures sont attendues en ce qui concerne l'IA, car elle nous aide à surmonter certains des plus grands défis auxquels nous sommes confrontés aujourd'hui dans de nombreux domaines, allant de la santé à la mobilité, en passant par l'administration publique et l'éducation.

2. Toutefois, ces avancées promises ne sont pas exemptes de risques. En effet, les risques sont très pertinents étant donné que les effets individuels et sociétaux des systèmes d'IA n'ont pas, dans une large mesure, été expérimentés. Générer du contenu, faire des prédictions ou prendre une décision de manière automatisée, comme le font les systèmes d'IA, au moyen de techniques d'apprentissage automatique ou de règles d'inférence logiques et probabilistes, ne sont pas des activités similaires à celles exécutées par des humains, au moyen d'un raisonnement créatif ou théorique, en assumant l'entière responsabilité des conséquences.

3. L'IA augmentera le nombre de prédictions qui peuvent être effectuées dans de nombreux domaines à partir de corrélations mesurables entre les données, invisibles aux yeux de l'homme mais visibles par les machines, en facilitant notre vie et en résolvant un grand nombre de problèmes, tout en érodant cependant notre capacité à donner une interprétation causale aux résultats, de telle sorte que les notions de transparence, de contrôle humain, de responsabilité et d'obligation de rendre compte des résultats seront sérieusement remises en question.

[1] JO L 295 du 21.11.2018, p. 39.
[2] Dans le présent document, on entend par «États membres» les «États membres de l'EEE».

4. Dans de nombreux cas, les données (à caractère personnel et non personnel) dans le domaine de l'IA constituent la clé de voûte des décisions autonomes, ce qui aura inévitablement une incidence sur la vie des individus à différents niveaux. C'est la raison pour laquelle, dès le stade actuel, l'EDPB et le CEPD affirment fermement que la proposition de règlement établissant des règles harmonisées en matière d'intelligence artificielle (législation en matière d'intelligence artificielle) (ci-après la «proposition»)[3] a **d'importantes implications en matière de protection des données**.

5. Confier la tâche de décider à des machines, sur la base de données, créera des risques pour les droits et libertés des personnes, aura une incidence sur leur vie privée et pourrait nuire à des groupes, voire à des sociétés dans leur ensemble. L'EDPB et le CEPD soulignent que les droits à la vie privée et à la protection des données à caractère personnel, en contradiction avec l'hypothèse de l'autonomie décisionnelle des machines qui sous-tend le concept d'IA, constituent un pilier des valeurs de l'UE telles qu'elles sont reconnues dans la Déclaration universelle des droits de l'homme (article 12), la convention européenne des droits de l'homme (article 8) et la charte des droits fondamentaux de l'Union européenne (ci-après la «Charte») (articles 7 et 8). Concilier la perspective de croissance offerte par les applications de l'IA et la centralité et la primauté de l'homme vis-à-vis des machines est un objectif très ambitieux mais nécessaire.

6. L'EDPB et le CEPD se félicitent de l'association à la réglementation de toutes les parties prenantes à la chaîne de valeur de l'IA et de l'introduction d'exigences spécifiques pour les fournisseurs de solutions, étant donné qu'ils jouent un rôle important dans les produits qui utilisent leurs systèmes. Toutefois, les responsabilités des différentes parties (utilisateur, fournisseur, importateur ou distributeur d'un système d'IA) doivent être clairement circonscrites et attribuées. En particulier, lors du traitement de données à caractère personnel, il convient d'accorder une attention particulière à la cohérence de ces rôles et responsabilités avec les notions de responsable du traitement et de sous-traitant des données relevant du cadre de protection des données, étant donné que les deux normes ne concordent pas.

7. La proposition accorde une place importante à la notion de contrôle humain (article 14), que l'EDPB et le CEPD accueillent favorablement. Toutefois, comme indiqué précédemment, en raison de l'incidence potentielle importante de certains systèmes d'IA sur des personnes physiques ou des groupes de personnes, une véritable centralité humaine devrait s'appuyer sur un contrôle humain hautement qualifié et un traitement licite dans la mesure où ces systèmes sont fondés sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour s'acquitter de leur mission, de manière à garantir le respect du droit à ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé.

8. En outre, en raison de la nature intensive en données de nombreuses applications d'IA, la proposition devrait promouvoir l'adoption d'une approche de protection des données dès la conception et par défaut à tous les niveaux, en encourageant la mise en œuvre effective des

[3] COM(2021) 206 final.

principes de protection des données (tels qu'envisagés à l'article 25 du RGPD et à l'article 27 du RPDUE) au moyen de technologies de pointe.

9. Enfin, l'EDPB et le CEPD soulignent que cet avis conjoint n'est fourni qu'à titre d'analyse préliminaire de la proposition, sans préjudice d'une évaluation et d'un avis complémentaires sur ses effets et sa compatibilité avec la législation de l'UE en matière de protection des données.

2 ANALYSE DES PRINCIPES CLÉS DE LA PROPOSITION

2.1 Champ d'application de la proposition et relation avec le cadre juridique existant

10. Selon l'exposé des motifs, la **base juridique** de la proposition est en premier lieu l'article 114 du TFUE, qui prévoit l'adoption de mesures visant à assurer l'établissement et le fonctionnement du marché intérieur[4]. En outre, la proposition est fondée sur l'article 16 du TFUE *dans la mesure où elle contient des règles spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel*, notamment des restrictions à l'utilisation de systèmes d'IA pour l'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives.[5]

11. L'EDPB et le CEPD rappellent que, conformément à la jurisprudence de la CJUE, l'article 16 du TFUE fournit une base juridique appropriée dans les cas où la protection des données à caractère personnel constitue l'un des objectifs ou éléments essentiels des règles adoptées par le législateur de l'Union[6]. L'application de l'article 16 TFUE implique également la nécessité d'assurer un contrôle indépendant du respect des exigences relatives au traitement des données à caractère personnel, comme l'exige également l'article 8 de la Charte.

12. Le CEPD et l'EDPB rappellent qu'il existe déjà un cadre complet de protection des données adopté sur la base de l'article 16 du TFUE, à savoir le règlement général sur la protection des données (RGPD)[7], le règlement sur la protection des données pour les institutions, organes et organismes de l'Union européenne (RPDUE)[8] et la directive en matière de protection des données dans le domaine répressif (la «directive»)[9]. Selon la proposition, seules les restrictions

[4] Exposé des motifs, p. 5.
[5] Exposé des motifs, p. 6. Voir également considérant 2 de la proposition.
[6] Avis du 26 juillet 2017, *PNR Canada*, procédure d'avis 1/15, ECLI:EU:C:2017:592, point 96.
[7] 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, JO L 119 du 4.5.2016, p. 1).
[8] 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 (JO L 295 du 21.11.2018, p. 39).
[9] 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 (JO L 119 du 4.5.2016, p. 89).

supplémentaires concernant le traitement des données biométriques contenues dans la proposition peuvent être considérées comme fondées sur l'article 16 du TFUE et donc comme ayant la même base juridique que le RGPD, le RPDUE ou la directive. Cela a des implications importantes pour la relation entre la proposition et le RGPD, le RPDUE et la directive d'une manière plus générale, comme indiqué ci-dessous.

13. En ce qui concerne le **champ d'application de la proposition**, l'EDPB et le CEPD se félicitent vivement que la proposition s'étende à l'utilisation des systèmes d'IA par les institutions, organes ou agences de l'UE. Étant donné que l'utilisation de systèmes d'IA par ces entités peut également avoir une incidence significative sur les droits fondamentaux des personnes, comme dans les États membres de l'UE, il est indispensable que le nouveau cadre réglementaire en matière d'IA s'applique à la fois aux États membres de l'UE et aux institutions, organes et organismes de l'UE afin de garantir une approche cohérente dans l'ensemble de l'Union. Étant donné que les institutions, organes et organismes de l'UE peuvent agir à la fois en tant que fournisseurs et utilisateurs de systèmes d'IA, l'EDPB et le CEPD estiment qu'il est tout à fait approprié d'inclure ces entités dans le champ d'application de la proposition sur la base de l'article 114 du TFUE.

14. Toutefois, l'EDPB et le CEPD sont vivement préoccupés par l'exclusion de la coopération internationale en matière répressive du champ d'application défini à l'article 2, paragraphe 4, de la proposition. Cette exclusion crée un risque important de contournement (par exemple, de la part de pays tiers ou d'organisations internationales exploitant des applications à haut risque sur lesquelles s'appuient les autorités publiques de l'UE).

15. Le développement et l'utilisation de systèmes d'IA impliqueront souvent le traitement de données à caractère personnel. Il est de la plus haute importance de veiller à la clarté de la relation entre la présente proposition et la législation existante de l'UE en matière de protection des données. La proposition est sans préjudice et complète le RGPD, le RPDUE et la directive. Alors que les considérants de la proposition précisent que l'utilisation des systèmes d'IA doit toujours être conforme à la législation en matière de protection des données, **l'EDPB et le CEPD recommandent vivement de préciser à l'article 1er de la proposition que la législation de l'Union en matière de protection des données à caractère personnel**, en particulier le RGPD, le RPDUE, la directive «Vie privée»[10] et la directive, s'applique à tout traitement de données à caractère personnel entrant dans le champ d'application de la proposition. De même, il devrait être précisé dans le considérant correspondant que la proposition ne vise pas à affecter l'application de la législation de l'Union en vigueur régissant le traitement des données à caractère personnel, y compris les missions et les pouvoirs des autorités de contrôle compétentes pour vérifier le respect de ces instruments.

[10] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») telle que modifiée par la directive 2006/24/CE et la directive 2009/136/CE.

2.2 Approche fondée sur les risques

16. L'EDPB et le CEPD **se félicitent de l'approche fondée sur les risques** qui sous-tend la proposition. Celle-ci s'appliquerait à tous les systèmes d'IA, y compris ceux qui n'impliquent pas le traitement de données à caractère personnel mais qui peuvent néanmoins avoir une incidence sur les intérêts ou les libertés et droits fondamentaux.

17. L'EDPB et le CEPD notent que certaines dispositions de la proposition ne tiennent pas compte des risques pour les groupes de personnes ou pour la société dans son ensemble (par exemple, les effets collectifs ayant une importance particulière, comme la discrimination de groupe ou l'expression d'opinions politiques dans les espaces publics). L'EDPB et le CEPD recommandent que les risques sociétaux posés par les systèmes d'IA soient également évalués et atténués.

18. L'EDPB et le CEPD sont d'avis que l'approche fondée sur les risques adoptée par la proposition devrait être clarifiée et que la notion de «risque pour les droits fondamentaux» devrait être **alignée sur le RGPD**, dans la mesure où des aspects liés à la protection des données à caractère personnel entrent en jeu. Qu'il s'agisse d'utilisateurs finaux, simplement de personnes concernées ou d'autres personnes concernées par le système d'IA, l'absence de toute référence dans le texte à la personne concernée par le système d'IA apparaît comme un angle mort dans la proposition. En effet, les obligations imposées aux acteurs vis-à-vis des personnes concernées devraient découler plus concrètement de la protection de l'individu et de ses droits. Par conséquent, l'EDPB et le CEPD invitent instamment les législateurs à aborder explicitement, dans la proposition, les **droits et les voies de recours dont disposent les personnes** soumises à des systèmes d'IA.

19. L'EDPB et le CEPD prennent acte du choix de fournir une liste exhaustive des **systèmes d'IA à haut risque**. Ce choix pourrait avoir un «effet noir et blanc», avec des capacités d'attraction limitées dans des situations à haut risque, compromettant ainsi l'approche globale fondée sur les risques qui sous-tend la proposition. En outre, la liste des systèmes d'IA à haut risque figurant aux annexes II et III de la proposition ne comprend pas certains types de cas d'utilisation impliquant des risques importants, tels que l'utilisation de l'IA pour déterminer la prime d'assurance ou pour évaluer des traitements médicaux ou à des fins de recherche médicale. L'EDPB et le CEPD soulignent également que ces annexes devront être régulièrement mises à jour pour s'assurer que leur champ d'application est approprié.

20. La proposition impose aux **fournisseurs** du système d'IA de procéder à une évaluation des risques; toutefois, dans la plupart des cas, les responsables du traitement (des données) seront les **utilisateurs** plutôt que les fournisseurs des systèmes d'IA (par exemple, un utilisateur d'un système de reconnaissance faciale est un «responsable du traitement» et n'est donc pas lié par les exigences imposées aux fournisseurs d'IA à haut risque en vertu de la proposition).

21. De surcroît, il ne sera **pas toujours possible pour un fournisseur d'évaluer toutes les utilisations** du système d'IA. Ainsi, l'évaluation initiale des risques sera plus générale que celle réalisée par l'utilisateur du système d'IA. Même si l'évaluation initiale des risques par le fournisseur n'indique pas que le système d'IA est «à haut risque» au titre de la proposition,

cela ne devrait pas exclure **une évaluation ultérieure (plus détaillée)** (analyse d'impact relative à la protection des données au titre de l'article 35 du RGPD, de l'article 39 du RPDUE ou de l'article 27 de la directive) **qui devrait être effectuée par l'utilisateur du système**, compte tenu du contexte d'utilisation et des cas d'utilisation spécifiques. L'interprétation de la question de savoir si, en vertu du RGPD, du RPDUE et de la directive, un type de traitement est susceptible d'engendrer un risque élevé doit être faite indépendamment de la proposition. Toutefois, la classification d'un système d'IA comme présentant un «risque élevé» en raison de son incidence sur les droits fondamentaux[11] **déclenche une présomption de «risque élevé» au titre du RGPD, du RPDUE et de la directive dans la mesure où des données à caractère personnel sont traitées.**

22. **L'EDPB et le CEPD partagent le constat exprimé dans la proposition selon lequel la classification d'un système d'IA comme étant à haut risque ne signifie pas nécessairement qu'il est licite en soi et qu'il peut être déployé par l'utilisateur en tant que tel. Le responsable du traitement peut avoir à respecter d'autres exigences découlant de la législation de l'UE en matière de protection des données.** En outre, le raisonnement sous-jacent à l'article 5 de la proposition, selon lequel, contrairement aux systèmes interdits, les systèmes à haut risque peuvent être en principe autorisés, doit être abordé et écarté dans la proposition, d'autant plus que le marquage CE proposé n'implique pas que le traitement de données à caractère personnel qui y est associé soit licite.

23. Toutefois, le respect des obligations légales découlant de la législation de l'Union (y compris en matière de protection des données à caractère personnel) devrait être une condition préalable à l'entrée sur le marché européen d'un produit muni du marquage CE. À cette fin, l'EDPB et le CEPD **recommandent d'inclure, au chapitre 2 du titre III de la proposition, l'obligation de garantir le respect du RGPD et du RPDUE**. Ces exigences font l'objet d'un audit (par un tiers) avant le marquage CE, conformément au principe de responsabilité. Dans le cadre de cette évaluation par un tiers, l'analyse d'impact initiale à réaliser par le fournisseur sera particulièrement pertinente.

24. Compte tenu des complexités engendrées par le développement de systèmes d'IA, il convient de souligner que les caractéristiques techniques des systèmes d'IA (par exemple, le type d'approche IA) pourraient entraîner des risques plus importants. Par conséquent, toute évaluation des risques liés au système d'IA devrait tenir compte des **caractéristiques techniques** ainsi que **de ses cas d'utilisation spécifiques et du contexte** dans lequel le système fonctionne.

[11] L'Agence des droits fondamentaux de l'Union européenne (FRA) a déjà répondu à la nécessité de réaliser des analyses d'impact sur les droits fondamentaux lors de l'utilisation de l'IA ou de technologies connexes. Dans son rapport de 2020 intitulé «Getting the future right — Artificial intelligence and fundamental rights» *[Préparer l'avenir - L'intelligence artificielle et les droits fondamentaux]*, la FRA a recensé des «pièges dans l'utilisation de l'IA, par exemple dans la prédiction policière, les diagnostics médicaux, les services sociaux et la publicité ciblée» et a souligné que «les organisations privées et publiques devraient procéder à des évaluations de la manière dont l'IA pourrait porter atteinte aux droits fondamentaux» afin de réduire les incidences négatives sur les individus.

25. À la lumière de ce qui précède, l'EDPB et le CEPD recommandent de préciser dans la proposition que **le fournisseur** procède à une évaluation initiale des risques liés au système d'IA en cause **en tenant compte des cas d'utilisation** (à préciser dans la proposition - complétant, par exemple, l'annexe III, paragraphe 1, point a), lorsque les cas d'utilisation des systèmes biométriques de l'IA ne sont pas mentionnés), et que l'**utilisateur** du système d'IA, en sa qualité de responsable du traitement des données au titre de la législation de l'UE en matière de protection des données (le cas échéant), applique l'analyse d'impact sur la protection des données comme le prévoient l'article 35 du RGPD, l'article 39 du RPDUE et l'article 27 de la directive, en tenant compte non seulement des caractéristiques techniques et du **cas d'utilisation**, mais **aussi du contexte spécifique** dans lequel l'IA fonctionnera.

26. En outre, certains des termes mentionnés à l'annexe III de la proposition, par exemple les termes «services privés essentiels», ou petit fournisseur utilisant l'IA à des fins d'évaluation de la solvabilité pour leur propre usage, devraient être clarifiés.

2.3 Utilisations interdites de l'IA

27. L'EDPB et le CEPD considèrent que les **formes intrusives d'IA**, en particulier celles qui peuvent porter atteinte à la dignité humaine, doivent être considérées comme des systèmes d'IA interdits en vertu de l'article 5 de la proposition au lieu d'être simplement classées comme «à haut risque» à son annexe III, telles que celles visées au point 6. Cela s'applique en particulier aux comparaisons de données qui, à grande échelle, concernent également les personnes qui n'ont pas ou peu donné lieu à une observation policière ou à un traitement qui porte atteinte au principe de limitation de la finalité prévu par la législation en matière de protection des données. L'utilisation de l'IA dans le domaine de la police et de l'application de la loi requiert des règles spécifiques à chaque zone, précises, prévisibles et proportionnées, qui doivent tenir compte des intérêts des personnes concernées et des effets sur le fonctionnement d'une société démocratique.

28. L'article 5 de la proposition risque d'évoquer simplement les «valeurs» et l'interdiction des systèmes d'IA en contradiction avec ces valeurs. En effet, les critères visés à l'article 5 pour «considérer» les systèmes d'IA comme interdits **limitent le champ d'application de l'interdiction** dans une mesure telle qu'elle pourrait se révéler dépourvue de sens dans la pratique [par exemple, «cause ou est susceptible de causer un préjudice physique ou psychologique [...]» à l'article 5, paragraphe 1, points a) et b); la limitation aux autorités publiques visée à l'article 5, paragraphe 1, point c); la formulation vague et au point c), i) et ii); la limitation à l'identification biométrique à distance «en temps réel» uniquement, sans définition claire, etc.].

29. En particulier, l'utilisation de l'IA à des fins de «notation sociale», comme le prévoit l'article 5, paragraphe 1, point c), de la proposition, peut conduire à une discrimination et va à l'encontre des valeurs fondamentales de l'UE. La proposition interdit uniquement ces pratiques lorsqu'elles sont menées «au cours d'une période donnée» ou «par les autorités publiques ou pour le compte de celles-ci». Les entreprises privées, notamment les fournisseurs de services de médias sociaux et d'informatique en nuage, peuvent traiter de grandes quantités de données à caractère personnel et procéder à une notation sociale. Par conséquent, **la proposition devrait**

interdire tout type de notation sociale. Il convient de signaler que, dans le contexte répressif, l'article 4 de la directive limite déjà considérablement, sinon interdit dans la pratique, ce type d'activités.

30. **L' identification biométrique à distance** des personnes dans des espaces accessibles au public présente un risque élevé d'intrusion dans leur vie privée. Par conséquent, l'EDPB et le CEPD **estiment qu'une approche plus stricte est nécessaire**. L'utilisation de systèmes d'IA pourrait poser de graves problèmes de proportionnalité, étant donné qu'elle pourrait impliquer le traitement de données d'un nombre inconsidéré et disproportionné de personnes concernées aux fins de l'identification de quelques personnes seulement (par exemple, les passagers dans les aéroports et les gares ferroviaires). La nature **fluide** des systèmes d'identification biométrique à distance présente également des problèmes de transparence et pose des questions liés à la base juridique du traitement au titre du droit de l'Union (la directive, le RGPD, le RPDUE et d'autres dispositions législatives applicables). Le problème concernant la manière d'informer correctement les personnes au sujet de ce traitement n'est toujours pas résolu, de même que l'exercice effectif et en temps utile de leurs droits. Il en va de même pour **son effet irréversible et grave sur les attentes** (raisonnables) **des populations en matière d'anonymat dans les espaces publics**, ce qui a un effet négatif direct sur l'exercice de la liberté d'expression, de réunion, d'association et de libre circulation.

31. L'article 5, paragraphe 1, point d), de la proposition contient une **liste exhaustive de cas exceptionnels** dans lesquels l'identification biométrique à distance en temps réel dans des espaces accessibles au public est autorisée à des fins répressives. L'EDPB et le CEPD considèrent que **cette approche est erronée** sur plusieurs points: Premièrement, il est difficile de comprendre ce qu'il faut entendre par «délai significatif» et de quelle manière il convient de le considérer comme une circonstance atténuante, compte tenu du fait qu'un système d'identification de masse est en mesure d'identifier des milliers de personnes en quelques heures seulement. En outre, le caractère intrusif du traitement ne dépend pas toujours de l'identification en temps réel ou non. L'identification biométrique à distance a posteriori dans le cadre d'une manifestation politique est susceptible d'avoir un effet dissuasif important sur l'exercice des libertés et droits fondamentaux, tels que la liberté de réunion et d'association et, plus généralement, les principes fondateurs de la démocratie. Deuxièmement, le caractère intrusif du traitement ne dépend pas nécessairement de sa finalité. L'utilisation de ce système à d'autres fins, telles que la sécurité privée, représente les mêmes menaces pour les droits fondamentaux que sont le respect de la vie privée et familiale et la protection des données à caractère personnel. Enfin, même avec les limitations prévues, le nombre potentiel de suspects ou d'auteurs d'infractions sera presque toujours «suffisant» pour justifier l'utilisation continue de systèmes d'IA pour la détection de suspects, malgré les autres conditions énoncées à l'article 5, paragraphes 2 à 4, de la proposition. Le raisonnement qui sous-tend la proposition semble omettre le fait que, lors du contrôle des zones ouvertes, les obligations découlant de la législation de l'UE en matière de protection des données doivent être respectées non seulement pour les suspects mais aussi pour tous ceux qui, dans la pratique, font l'objet d'un suivi.

32. Pour toutes ces raisons, l'EDPB et le CEPD **demandent une interdiction générale de toute utilisation de l'IA en vue d'une reconnaissance automatisée des caractéristiques humaines dans des espaces accessibles au public, tels que les visages, mais aussi la démarche, les empreintes digitales, l'ADN, la voix, la pression sur des touches et d'autres signaux biométriques ou comportementaux, dans tous les contextes**. L'approche actuelle de la proposition consiste à recenser et répertorier tous les systèmes d'IA qu'il convient d'interdire. Par conséquent, pour des raisons de cohérence, **les systèmes d'IA pour l'identification à distance à grande échelle dans les espaces en ligne** devraient être interdits en vertu de l'article 5 de la proposition. Compte tenu de la directive, du RPDUE et du RGPD, l'EDPB et le CEPD ne peuvent discerner comment ce type de pratique serait en mesure de satisfaire aux exigences de nécessité et de proportionnalité, deux notions qui découlent en définitive de ce qui est considéré comme acceptable par la CJUE et la Cour européenne des droits de l'homme.

33. En outre, l'EDPB et le CEPD **recommandent une interdiction**, tant pour les autorités publiques que pour les entités privées, **des systèmes d'IA classant les individus à partir de données biométriques (par exemple, à partir de la reconnaissance faciale) dans des groupes en fonction de l'origine ethnique, du sexe, ainsi que de l'orientation politique ou sexuelle, ou d'autres motifs de discrimination interdits par l'article 21 de la Charte, ou** des systèmes d'IA dont la validité scientifique n'est pas prouvée ou qui sont en conflit direct avec les valeurs essentielles de l'UE [par exemple, le polygraphe, annexe III, section 6, point b) et section 7, point a)]. En conséquence, la «**catégorisation biométrique**» devrait être **interdite en vertu de l'article 5**.

34. Le **fait d'être déterminé ou classé par un ordinateur quant à son comportement futur, indépendamment de sa propre volonté, porte également atteinte à la dignité humaine**. Les systèmes d'IA destinés à être employés par les services répressifs pour effectuer des évaluations individuelles des risques sur des personnes physiques afin d'évaluer le risque qu'une personne physique se rende coupable d'une infraction pénale ou de récidive [voir annexe III, section 6, point a)], ou pour prédire la survenance ou la répétition d'une infraction pénale réelle ou potentielle sur la base du profilage d'une personne physique ou de l'évaluation des traits et caractéristiques de la personnalité ou du comportement infractionnel passé [voir annexe III, section 6, point e)], utilisés en fonction de leur destination, conduiront à une sujétion majeure de la prise des décisions policières et judiciaires, réduisant ainsi l'être humain concerné à l'état d'objet. Ces systèmes d'IA touchant à l'essence du droit à la dignité humaine devraient être interdits en vertu de l'article 5.

35. Par ailleurs, l'EDPB et le CEPD estiment que l'utilisation de l'IA pour **déduire les émotions d'une personne physique est hautement indésirable et devrait être interdite,** sauf dans certains cas bien précis d'utilisation, notamment à des fins de santé ou de recherche (par exemple, les patients pour lesquels la reconnaissance de l'émotion est importante), toujours avec des garanties appropriées en place et, bien entendu, sous réserve de toutes les autres conditions et limites en matière de protection des données, y compris la limitation de la finalité.

2.4 Systèmes d'IA à haut risque

2.4.1 Nécessité d'une évaluation ex ante de la conformité par des tiers externes

36. L'EDPB et le CEPD se félicitent que les systèmes d'IA présentant un risque élevé fassent l'objet d'une évaluation préalable de la conformité avant de pouvoir être mis sur le marché ou mis en service d'une autre manière dans l'UE. En principe, ce modèle réglementaire est bien accueilli, car il offre un bon équilibre entre la propension à l'innovation et un niveau élevé de protection proactive des droits fondamentaux. Pour qu'ils puissent être utilisés dans des environnements spécifiques tels que les processus décisionnels des institutions de service public ou des infrastructures critiques, il convient de définir les moyens d'étudier leur code source complet.

37. Toutefois, l'EDPB et le CEPD préconisent d'adapter la procédure d'évaluation de la conformité prévue à l'article 43 de la proposition de manière à ce qu'une **évaluation ex ante de la conformité par un tiers soit généralement effectuée pour l'IA à haut risque.** Bien qu'une évaluation de la conformité par un tiers pour le traitement à haut risque de données à caractère personnel ne soit pas une exigence du RGPD ou du RPDUE, les risques posés par les systèmes d'IA doivent encore être pleinement compris. L'inclusion générale d'une obligation d'évaluation de la conformité par un tiers renforcerait donc davantage la sécurité juridique et la confiance dans tous les systèmes d'IA à haut risque.

2.4.2 Le champ d'application du règlement doit également couvrir les systèmes d'IA déjà utilisés

38. Conformément à l'article 43, paragraphe 4, de la proposition, les systèmes d'IA à haut risque devraient faire l'objet d'une nouvelle procédure d'évaluation de la conformité chaque fois qu'une modification importante est apportée. Il est juste de veiller à ce que les systèmes d'IA respectent les exigences du règlement relatif à l'IA tout au long de leur cycle de vie. Les systèmes d'IA qui ont été mis sur le marché ou mis en service avant l'application du règlement proposé (ou 12 mois après cette date pour les systèmes d'information à grande échelle énumérés à l'annexe IX) sont exclus du champ d'application, à moins que ces systèmes ne subissent d'«importantes modifications» de leur conception ou de leur destination (article 83).

39. Or, le seuil des «importantes modifications» n'est pas clair. Le considérant 66 de la proposition précise un seuil plus bas pour la réévaluation de la conformité «chaque fois qu'ils subissent une modification susceptible d'avoir une incidence sur leur conformité». Un seuil similaire serait approprié pour l'article 83, au moins pour les systèmes d'IA à haut risque. En outre, afin de combler toute lacune en matière de protection, il est nécessaire que les systèmes d'IA déjà mis en place et en service - après une certaine phase de mise en œuvre - respectent également toutes les exigences du règlement relatif à l'IA.

40. Les multiples possibilités de traitement des données à caractère personnel et les risques externes nuisent également à la sécurité des systèmes d'IA. L'accent mis, à l'article 83, sur les «importantes modifications de leur conception ou de leur destination» ne comporte pas de référence à l'évolution des risques externes. Il convient donc d'inclure à l'article 83 de la

proposition une référence aux modifications du scénario des menaces découlant de risques externes, tels que les cyberattaques, les attaques adversaires et les plaintes motivées des consommateurs.

41. En outre, comme l'entrée en application devrait intervenir 24 mois après l'entrée en vigueur du futur règlement, le CEPD et l'EDPB estiment qu'il n'est pas approprié d'exempter les systèmes d'IA déjà mis sur le marché pour une période encore plus longue. Alors que la proposition prévoit également que les exigences du règlement doivent être prises en considération dans l'évaluation de chaque système d'information à grande échelle prévue par les actes juridiques énumérés à l'annexe IX, l'EDPB et le CEPD estiment que les exigences relatives à la mise en service des systèmes d'IA devraient être applicables à partir de la date d'application du futur règlement.

2.5 Gouvernance et Comité européen de l'IA

2.5.1 Gouvernance

42. L'EDPB et le CEPD saluent la désignation du CEPD comme l'autorité compétente et l'autorité de surveillance du marché pour la supervision des institutions, agences et organes de l'Union lorsqu'ils relèvent de la présente proposition. Le CEPD est prêt à remplir son nouveau rôle de régulateur de l'IA pour l'administration publique de l'UE. En outre, le rôle et les tâches du CEPD ne sont pas suffisamment détaillés et devraient être précisés dans la proposition, notamment en ce qui concerne son rôle d'autorité de surveillance du marché.

43. L'EDPB et le CEPD prennent acte de l'allocation des ressources financières, qui est prévue pour le Comité et le CEPD, agissant en tant qu'organisme notifiant, dans la proposition. Toutefois, l'accomplissement des nouvelles tâches prévues pour le CEPD, que ce soit en tant qu'organisme notifié, nécessiterait des ressources financières et humaines nettement plus importantes.

44. Premièrement, parce que le libellé de l'article 63, paragraphe 6, dispose que le CEPD agit en tant qu'«autorité de surveillance du marché» pour les institutions, agences et organes de l'Union qui relèvent du champ d'application de la proposition, ce qui ne précise pas si le CEPD doit être considéré comme une «autorité de surveillance du marché» pleinement incarnée, comme le prévoit le règlement (UE) 2019/1020. Cela soulève des questions sur les fonctions et les pouvoirs du CEPD dans la pratique. Deuxièmement, et pour autant qu'il soit répondu par l'affirmative à la première question, il n'apparaît pas clairement comment le rôle du CEPD, tel que prévu dans le RPDUE, peut répondre à la tâche prévue à l'article 11 du règlement (UE) 2019/1020, qui comprend «la surveillance efficace du marché des produits mis à disposition en ligne» ou «des contrôles physiques et des examens de laboratoire sur la base d'échantillons adéquats». Il existe un risque que l'exécution de la nouvelle série de tâches sans apporter de précisions supplémentaires dans la proposition compromette le respect de ses obligations en tant que contrôleur de la protection des données.

45. Toutefois, l'EDPB et le CEPD soulignent que certaines dispositions de la proposition définissant les missions et les pouvoirs des différentes autorités compétentes au titre du règlement relatif à l'IA, leurs relations, leur nature et la garantie de leur indépendance ne

semblent pas claires à ce stade. Alors que le règlement UE 2019/1020 dispose que l'autorité de surveillance du marché doit être indépendante, le projet de règlement n'exige pas que les autorités de surveillance soient indépendantes, et impose même qu'elles rendent compte à la Commission de certaines tâches effectuées par les autorités de surveillance du marché, qui peuvent être des institutions différentes. Si la proposition prévoit également que les APD seront les autorités de surveillance du marché des systèmes d'IA utilisés à des fins répressives (article 63, paragraphe 5), cela signifie également qu'elles seront, le cas échéant par l'intermédiaire de leur autorité de contrôle nationale, soumises à des obligations de déclaration à la Commission (article 63, paragraphe 2), ce qui semble incompatible avec leur indépendance.

46. Par conséquent, l'EDPB et le CEPD estiment que ces dispositions doivent être clarifiées afin d'être cohérentes avec le règlement UE 2019/1020, le RPDUE et le RGPD, et que la proposition devrait clairement établir que les autorités de surveillance au titre du règlement relatif à l'IA doivent être totalement indépendantes dans l'accomplissement de leurs tâches, étant donné qu'il s'agirait d'une garantie essentielle pour la surveillance et l'application correctes du futur règlement.

47. L'EDPB et le CEPD tiennent à rappeler que les autorités de protection des données appliquent déjà le RGPD, le RPDUE et la directive concernant les systèmes d'IA utilisant des données à caractère personnel, afin de garantir la protection des droits fondamentaux et plus particulièrement du droit à la protection des données. Par conséquent, les APD disposent déjà, dans une certaine mesure, comme l'exige la proposition pour les autorités de contrôle nationales, d'une compréhension des technologies de l'IA, des données et du calcul des données, des droits fondamentaux, ainsi que d'une expertise dans l'évaluation des risques que présentent les nouvelles technologies pour les droits fondamentaux. En outre, lorsque les systèmes d'IA sont fondés sur le traitement de données à caractère personnel ou traitent des données à caractère personnel, les dispositions de la proposition sont directement liées au cadre juridique en matière de protection des données, ce qui sera le cas pour la plupart des systèmes d'IA relevant du champ d'application du règlement. En conséquence, il y aura des interconnexions de compétences entre les autorités de surveillance au titre de la proposition et les APD.

48. Partant, la désignation des autorités de protection des données en tant qu'autorités de contrôle nationales garantirait une approche réglementaire plus harmonisée, contribuerait à l'interprétation cohérente des dispositions relatives au traitement des données et éviterait les contradictions entre les États membres lors de son application. Il serait également profitable à toutes les parties prenantes de la chaîne de valeur de l'IA de disposer d'un point de contact unique pour toutes les opérations de traitement de données à caractère personnel relevant du champ d'application de la proposition et de limiter les interactions entre deux organismes de réglementation différents pour le traitement qui sont concernés par la proposition et le RGPD. Par conséquent, l'EDPB et le CEPD estiment que **les autorités de protection des données devraient être désignées comme autorités de contrôle nationales conformément à l'article 59 de la proposition**.

49. En tout état de cause, dans la mesure où la proposition contient des règles spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel adoptées sur la base de l'article 16 du TFUE, le respect de ces règles, notamment les restrictions à l'utilisation de systèmes d'IA pour l'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives, **doit être soumis au contrôle d'autorités indépendantes**.

50. Toutefois, la proposition ne contient aucune disposition explicite qui attribuerait la compétence pour assurer le respect de ces règles au contrôle d'autorités indépendantes. La seule référence aux autorités de contrôle compétentes en matière de protection des données au titre du RGPD, ou de la directive, figure à l'article 63, paragraphe 5, de la proposition, mais uniquement en tant qu'organismes de «surveillance du marché» et alternativement avec certaines autres autorités. L'EDPB et le CEPD estiment que cette mise en place ne garantit pas le respect de l'exigence de contrôle indépendant énoncée à l'article 16, paragraphe 2, du TFUE et à l'article 8 de la Charte.

2.5.2 Le Comité européen de l'IA

51. La proposition établit un «Comité européen de l'intelligence artificielle» (CEIA). L'EDPB et le CEPD reconnaissent la nécessité d'une application cohérente et harmonisée du cadre proposé, ainsi que la participation d'experts indépendants à l'élaboration de la politique de l'UE en matière d'IA. Parallèlement, la proposition prévoit de conférer un rôle prépondérant à la Commission. En effet, non seulement cette dernière ferait partie du CEIA, mais elle la présiderait également et disposerait d'un droit de veto pour l'adoption du règlement intérieur du CEIA. Cela contraste avec la nécessité d'un organe européen de l'IA indépendant de toute influence politique. Par conséquent, l'EDPB et le CEPD estiment que le futur règlement relatif à l'IA devrait conférer **plus d'autonomie au CEAI**, afin de lui permettre de garantir réellement l'application cohérente du règlement dans l'ensemble du marché unique.

52. L'EDPB et le CEPD notent également qu'aucun pouvoir n'est conféré au CEIA en ce qui concerne l'application du règlement proposé. Toutefois, compte tenu de la diffusion des systèmes d'IA dans le marché unique et de la probabilité d'affaires transfrontières, il est indispensable d'harmoniser l'application de la législation et de répartir correctement les compétences entre les autorités de contrôle nationales. L'EDPB et le CEPD recommandent donc que les mécanismes de coopération entre les autorités de contrôle nationales soient précisés dans le futur règlement relatif à l'IA. L'EDPB et le CEPD suggèrent d'imposer un mécanisme garantissant un point de contact unique pour les personnes concernées par la législation ainsi que pour les entreprises, pour chaque système d'IA, et que, pour les organisations dont l'activité couvre plus de la moitié des États membres de l'UE, le CEIA puisse désigner l'autorité nationale chargée de faire appliquer le règlement relatif à l'IA pour ce système d'IA.

53. En outre, compte tenu de l'indépendance des autorités qui composent le Comité, celui-ci est habilité à agir de sa propre initiative et pas seulement à fournir conseil et assistance à la Commission. L'EDPB et le CEPD soulignent donc la nécessité d'une extension de la mission confiée au Comité, qui ne correspond pas non plus aux tâches énumérées dans la proposition.

54. Pour atteindre ces objectifs, le **CEIA dispose de pouvoirs suffisants et appropriés** et son statut juridique doit être clarifié. En particulier, pour que le champ d'application matériel du futur règlement reste pertinent, il semble nécessaire d'associer à son évolution les autorités chargées de son application. Par conséquent, l'EDPB et le CEPD recommandent que le CEIA soit habilité à proposer à la Commission des modifications de l'annexe I définissant les techniques et approches en matière d'IA et de l'annexe III énumérant les systèmes d'IA à haut risque visés à l'article 6, paragraphe 2. Le CEIA devrait également être consulté par la Commission avant toute modification de ces annexes.

55. L'article 57, paragraphe 4, de la proposition prévoit des échanges entre le Comité et d'autres organes, bureaux, agences et groupes consultatifs de l'Union. Compte tenu de leurs travaux antérieurs dans le domaine de l'IA et de leur expertise en matière de droits de l'homme, l'EDPB et le CEPD recommandent de considérer l'Agence des droits fondamentaux comme l'un des observateurs auprès du Comité.

3 INTERACTION AVEC LE CADRE DE PROTECTION DES DONNEES

3.1 Relation entre la proposition et la législation existante de l'UE en matière de protection des données

56. Une relation clairement définie entre la proposition et la législation existante en matière de protection des données est une condition préalable essentielle pour garantir et préserver le respect et l'application de l'acquis de l'UE dans le domaine de la protection des données à caractère personnel. Ce droit de l'Union, en particulier le RGPD, le RPDUE et la directive, doit être considéré comme une condition préalable sur laquelle de nouvelles propositions législatives peuvent s'appuyer sans affecter ou interférer avec les dispositions existantes, y compris en ce qui concerne la compétence des autorités de surveillance et la gouvernance.

57. De l'avis du comité européen de la protection des données et du CEPD, il importe donc d'éviter clairement, dans la proposition, toute incohérence et tout conflit éventuel avec le RGPD, le RPDUE et la directive, et ce, non seulement pour des raisons de sécurité juridique, mais aussi pour éviter que la proposition n'ait pour effet de compromettre directement ou indirectement le droit fondamental à la protection des données à caractère personnel, tel qu'établi par l'article 16 du TFUE et l'article 8 de la Charte.

58. En particulier, les machines d'auto-apprentissage ne pourraient protéger les données à caractère personnel des individus que si elles sont intégrées dès la conception. La possibilité immédiate d'exercer les droits des personnes au titre de l'article 22 (prise de décision individuelle automatisée, y compris le profilage) du RGPD ou de l'article 23 du RPDUE, indépendamment des finalités du traitement, est également essentielle. À cet égard, les autres droits des personnes concernées liés au droit de suppression et au droit de rectification conformément à la législation sur la protection des données, doivent être prévus dès le départ dans les systèmes d'IA, quelle que soit l'approche ou l'architecture technique choisie en la matière.

59. L'utilisation de données à caractère personnel pour l'apprentissage des systèmes d'IA peut donner lieu à des schémas de prise de décision biaisés au cœur du système d'IA. Par conséquent, diverses garanties, et en particulier un contrôle humain qualifié dans le cadre de ces processus, devraient être requises pour que les droits des personnes concernées soient respectés et garantis, ainsi que pour éviter tout effet négatif pour les individus. Les autorités compétentes devraient également être en mesure de proposer des lignes directrices pour évaluer les biais dans les systèmes d'IA et contribuer à l'exercice du contrôle humain.

60. Les personnes concernées devraient toujours être informées lorsque leurs données sont utilisées à des fins de formation et/ou de prévision en matière d'IA, de la base juridique de ce traitement, de l'explication générale de la logique (procédure) et de la portée du système d'IA. À cet égard, le droit des personnes à limiter le traitement (article 18 du RGPD et article 20 du RPDUE) ainsi qu'à supprimer/effacer des données (article 16 du RGPD et article 19 du RPDUE) devrait toujours être garanti dans ces cas. En outre, le responsable du traitement devrait être explicitement tenu d'informer la personne concernée des délais d'objection, de limitation, de suppression des données, etc. Le système d'IA doit être en mesure de satisfaire à toutes les exigences en matière de protection des données au moyen de mesures techniques et organisationnelles adéquates. Un droit à l'explication devrait permettre une plus grande transparence.

3.2 Bac à sable et traitement ultérieur (articles 53 et 54 de la proposition)

61. Dans les limites juridiques et morales existantes, il importe de promouvoir l'innovation européenne au moyen d'outils tels qu'un bac à sable. Un bac à sable offre la possibilité de fournir les garanties nécessaires pour renforcer la confiance et la dépendance à l'égard des systèmes d'IA. Dans des environnements complexes, il peut être difficile pour les praticiens de l'IA de mettre en balance tous les intérêts de manière appropriée. En particulier pour les petites et moyennes entreprises disposant de ressources limitées, opérer dans un bac à sable réglementaire peut fournir des informations plus rapides et, partant, favoriser l'innovation.

62. L'article 53, section 3, de la proposition dispose que les bacs à sable n'ont pas d'incidence sur les pouvoirs en matière de contrôle et de mesures correctives. Si cette clarification est utile, il est également nécessaire d'élaborer des directives ou des orientations sur la manière de trouver un bon équilibre entre, d'une part, le fait d'être une autorité de contrôle et, d'autre part, la fourniture d'orientations détaillées au moyen d'un bac à sable.

63. La section 6 de l'article 53 précise que les modalités et conditions de fonctionnement des bacs à sable sont définies dans des actes d'exécution. Il est important que des lignes directrices spécifiques soient élaborées afin de garantir la cohérence et le soutien à la mise en place et au fonctionnement des bacs à sable. Toutefois, des actes d'exécution contraignants pourraient limiter la capacité de chaque État membre à personnaliser le bac à sable en fonction de ses besoins et de ses pratiques locales. Par conséquent, l'EDPB et le CEPD recommandent que le Comité européen de l'intelligence artificielle fournisse des lignes directrices pour les bacs à sable.

64. L'article 54 de la proposition vise à fournir une base juridique pour le traitement ultérieur de données à caractère personnel en vue du développement de certains systèmes d'IA dans l'intérêt public dans le cadre du bac à sable réglementaire en matière d'IA. La relation entre l'article 54, paragraphe 1, de la proposition et l'article 54, paragraphe 2, et le considérant 41 de la proposition, et donc également avec le droit de l'Union en vigueur en matière de protection des données, reste floue. Toutefois, le RGPD et le RPDUE disposent déjà d'une base solide pour un «traitement ultérieur». En ce qui concerne, notamment, les cas où il est dans l'intérêt public d'autoriser un traitement ultérieur, la mise en balance des intérêts du responsable du traitement et des intérêts de la personne concernée ne doit pas entraver l'innovation. À l'heure actuelle, l'article 54 de la proposition ne traite pas deux questions importantes: i) dans quelles circonstances, sur la base de quels critères (supplémentaires) sont mis en balance les intérêts des personnes concernées et ii) si ces systèmes d'IA ne seront utilisés que dans le cadre du bac à sable. L'EDPB et le CEPD se félicitent de l'exigence d'une législation de l'Union ou d'un État membre lorsqu'ils traitent des données à caractère personnel collectées au titre de la directive dans un bac à sable, mais recommandent de préciser ce qui est envisagé ici, d'une manière qui soit conforme au RGPD et au RPDUE, principalement en soulignant que la base juridique de ces bacs à sable devrait être conforme aux exigences établies à l'article 23, paragraphe 2, du RGPD et à l'article 25 du RPDUE, et précisent que chaque utilisation du bac à sable doit faire l'objet d'une évaluation approfondie. Cela vaut également pour la liste complète des conditions visées à l'article 54, paragraphe 1, points b) à j).

65. Certaines considérations supplémentaires concernant la réutilisation des données figurant à l'article 54 de la proposition indiquent que l'exploitation d'un bac à sable nécessite beaucoup de ressources et qu'il est donc réaliste d'estimer que seul un petit nombre d'entreprises auraient la possibilité de participer. La participation au bac à sable pourrait constituer un avantage concurrentiel. Permettre la réutilisation des données nécessiterait une réflexion approfondie sur la manière de sélectionner les participants afin de s'assurer qu'ils entrent dans le champ d'application et d'éviter un traitement inéquitable. L'EDPB et le CEPD craignent que la possibilité de réutilisation des données dans le cadre du bac à sable diverge de l'approche adoptée dans le RGPD en matière de responsabilité, selon laquelle la responsabilité incombe au responsable du traitement, et non à l'autorité compétente.

66. En outre, l'EDPB et le CEPD estiment que, compte tenu des objectifs du bac à sable, à savoir développer, tester et valider des systèmes d'IA, ces bacs ne peuvent relever du champ d'application de la directive. Alors que la directive prévoit la réutilisation de données à des fins de recherche scientifique, les données traitées pour cette finalité secondaire seront assujetties au RGPD ou au RPDUE et non plus à la directive.

67. Ce qu'un bac à sable réglementaire englobera n'apparaît pas clairement. La question se pose de savoir si le bac à sable réglementaire proposé comprend une infrastructure informatique dans chaque État membre, assortie de motifs juridiques supplémentaires pour un traitement ultérieur, ou s'il organise simplement l'accès à l'expertise et aux orientations en matière de réglementation. L'EDPB et le CEPD invitent instamment le législateur à clarifier cette notion dans la proposition et à y indiquer clairement que le bac à sable réglementaire n'implique pas l'obligation pour les autorités compétentes de fournir son infrastructure technique. En tout état

de cause, des ressources financières et humaines doivent être mises à la disposition des autorités compétentes en conséquence de cette clarification.

68. Enfin, l'EDPB et le CEPD souhaitent insister sur le développement de systèmes d'IA transfrontières qui seront accessibles pour le marché unique numérique européen dans son ensemble. Dans le cas de tels systèmes d'IA, le bac à sable réglementaire en tant qu'outil d'innovation ne devrait pas faire obstacle au développement transfrontières. Par conséquent, l'EDPB et le CEPD recommandent une approche transfrontières coordonnée qui soit encore suffisamment accessible au niveau national pour toutes les PME, offrant un cadre commun dans toute l'Europe sans être trop restrictive. Il convient de trouver un équilibre entre la coordination européenne et les procédures nationales afin d'éviter une mise en œuvre conflictuelle du futur règlement relatif à l'IA qui ferait obstacle à l'innovation à l'échelle de l'UE.

3.3 Transparence

69. L'EDPB et le CEPD se félicitent que les systèmes d'IA à haut risque soient enregistrés dans une base de données publique (visée aux articles 51 et 60 de la proposition). Cette base de données devrait être l'occasion de fournir au grand public des informations sur le champ d'application du système d'IA et sur les défaillances et incidents connus, susceptibles de compromettre son fonctionnement, ainsi que sur les mesures correctives adoptées par les fournisseurs pour y remédier.

70. Un principe démocratique essentiel est le recours à l'équilibre des pouvoirs. Par conséquent, le fait que l'obligation de transparence ne s'applique pas aux systèmes d'IA utilisés pour détecter, prévenir, instruire ou poursuivre des infractions pénales constitue une exception trop large. Il convient de distinguer les systèmes d'IA utilisés pour détecter ou prévenir et les systèmes d'IA qui visent à enquêter, utiles à la poursuite des infractions pénales. Les garanties en matière de prévention et de détection doivent être renforcées en raison de la présomption d'innocence. En outre, l'EDPB et le CEPD déplorent l'absence d'avertissement dans la proposition, qui peut être interprétée comme un feu vert pour l'utilisation de systèmes ou d'applications d'IA à haut risque, même non prouvés.

71. Dans les cas où peu de transparence, voire aucune, peut être offerte au public pour des raisons de confidentialité, même dans une démocratie qui fonctionne bien, des garanties devraient être mises en place et ces systèmes d'IA devraient être enregistrés auprès de l'autorité de surveillance compétente et être transparents envers elle.

72. Garantir la transparence des systèmes d'IA est un objectif très ambitieux. L'approche entièrement quantitative de la prise de décision de nombreux systèmes d'IA, fondamentalement différente de l'approche humaine reposant principalement sur un raisonnement causal et théorique, peut aller à l'encontre de la nécessité d'obtenir au préalable une explication compréhensible des résultats des machines. Le règlement devrait promouvoir de nouveaux moyens, plus proactifs et opportuns, d'informer les utilisateurs des systèmes d'IA sur le statut (décisionnel) du système à tout moment, en les avertissant rapidement des éventuels effets préjudiciables, de manière à ce

que les personnes dont les droits et libertés peuvent être lésés par des décisions autonomes de la machine puissent réagir ou remédier à la décision.

3.4 Traitement de catégories particulières de données et de données relatives aux infractions pénales

73. Le traitement de catégories particulières de données dans le domaine répressif est régi par les dispositions du cadre de l'UE en matière de protection des données, y compris la directive ainsi que sa mise en œuvre au niveau national. La proposition prétend ne pas fournir de base juridique générale pour le traitement des données à caractère personnel, y compris des catégories particulières de données à caractère personnel (voir le considérant 41). Parallèlement, l'article 10, paragraphe 5, de la proposition dispose que «les fournisseurs de ces systèmes peuvent traiter des catégories particulières de données à caractère personnel». En outre, la même disposition exige des garanties supplémentaires, en donnant également des exemples. Par conséquent, la proposition semble interférer avec l'application du RGPD, de la directive et du RPDUE. Bien que l'EDPB et le CEPD saluent la tentative de prévoir des garanties appropriées, une approche réglementaire plus cohérente est nécessaire, étant donné que les dispositions actuelles ne semblent pas suffisamment claires pour créer une base juridique concernant le traitement de catégories particulières de données et doivent être complétées par des mesures de protection supplémentaires qui doivent encore être évaluées. En outre, lorsque des données à caractère personnel ont été collectées par traitement dans le cadre de la directive, les éventuelles garanties et limitations supplémentaires découlant des transpositions nationales de la directive devront être prises en considération.

3.5 Mécanismes de mise en conformité

3.5.1 Certification

74. L'un des principaux piliers de la proposition est la certification. Le système de certification décrit dans la proposition repose sur une structure d'entités (autorités notifiantes/organismes notifiés/Commission) et sur un mécanisme d'évaluation/de certification de la conformité couvrant les exigences obligatoires applicables aux systèmes d'IA à haut risque, et s'appuie sur des normes européennes harmonisées au titre du règlement (UE) nº 1025/2012 et sur des spécifications communes devant être établies par la Commission. Ce mécanisme est différent du système de certification visant à garantir le respect des règles et principes en matière de protection des données, énoncés aux articles 42 et 43 du RGPD. Toutefois, il n'apparaît pas clairement comment les certificats délivrés par les organismes notifiés conformément à la proposition peuvent interagir avec les certifications, les sceaux et les marques en matière de protection des données prévus par le RGPD, contrairement à ce qui est prévu pour d'autres types de certifications [voir l'article 42, paragraphe 2, en ce qui concerne les certifications délivrées au titre du règlement (UE) 2019/881].

75. Dans la mesure où les systèmes d'IA à haut risque sont fondés sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour s'acquitter de leur mission, ces décalages peuvent créer des incertitudes juridiques pour tous les organismes concernés, étant

donné qu'ils peuvent conduire à des situations dans lesquelles des systèmes d'IA certifiés au titre de la proposition et munis d'un marquage CE de conformité, une fois mis sur le marché ou mis en service, pourraient être utilisés d'une manière non conforme aux règles et principes de protection des données.

76. La proposition n'établit pas de relation claire avec la législation en matière de protection des données ainsi qu'avec le droit de l'UE et des États membres applicable à chaque «domaine» des systèmes d'IA à haut risque énumérés à l'annexe III. En particulier, la proposition devrait inclure les principes de minimisation des données et de protection des données dès la conception comme l'un des aspects à prendre en considération avant l'obtention du marquage CE, étant donné le niveau élevé d'interférence possible des systèmes d'IA à haut risque avec les droits fondamentaux à la vie privée et à la protection des données à caractère personnel, et la nécessité de garantir un niveau élevé de confiance dans le système d'IA. Par conséquent, l'EDPB et le CEPD recommandent de modifier la proposition afin de clarifier la relation entre les certificats délivrés au titre dudit règlement et les certifications, sceaux et marques en matière de protection des données. Enfin, les autorités chargées de la protection des données devraient être associées à l'élaboration et à l'établissement de normes harmonisées et de spécifications communes.

77. En ce qui concerne l'article 43 de la proposition relatif à l'évaluation de la conformité, la dérogation à la procédure d'évaluation de la conformité prévue à l'article 47 semble très large, comprenant un trop grand nombre d'exceptions, telles que des motifs exceptionnels liés à la sécurité publique, à la protection de la vie et de la santé des personnes physiques, à la protection de l'environnement et à la protection d'actifs industriels et d'infrastructures d'importance majeure. Nous proposons aux législateurs d'en réduire le nombre.

3.5.2 Codes de conduite

78. Conformément à l'article 69 de la proposition, la Commission et les États membres encouragent et facilitent l'élaboration de codes de conduite destinés à favoriser l'application volontaire, par les fournisseurs de systèmes d'IA à haut risque, des exigences applicables aux systèmes d'IA à haut risque, ainsi que des exigences supplémentaires. Conformément au considérant 78 du RGPD, l'EDPB et le CEPD recommandent de recenser et de définir des synergies entre ces instruments et les codes de conduite prévus par le RGPD qui favorisent le respect de la protection des données. Dans ce contexte, il convient de préciser si la protection des données à caractère personnel doit être considérée comme une «exigence supplémentaire» pouvant être traitée par les codes de conduite visés à l'article 69, paragraphe 2. Il convient également de veiller à ce que les «spécifications et solutions techniques» visées par les codes de conduite indiqués à l'article 69, paragraphe 1, conçues pour favoriser le respect des exigences du projet de règlement relatif à l'IA, ne soient pas incompatibles avec les règles et principes du RGPD et du RPDUE. Ce faisant, le respect de ces outils par les fournisseurs de systèmes d'IA à haut risque, dans la mesure où ces systèmes sont fondés sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leur mission, représenterait une valeur ajoutée, car cela permettra de garantir que le responsable du traitement et les sous-traitants seront en mesure de remplir leurs obligations en matière de protection des données lors de l'utilisation de ces systèmes.

79. Parallèlement, le cadre juridique pour une IA digne de confiance serait complété par l'intégration des codes de conduite, de manière à favoriser la confiance dans l'utilisation de cette technologie d'une manière sûre et conforme au droit, y compris le respect des droits fondamentaux. Toutefois, la conception de ces instruments devrait être renforcée en envisageant des mécanismes visant à vérifier que ces codes fournissent des «spécifications et solutions techniques» efficaces et définissent des «objectifs clairs et des indicateurs de performance clés pour mesurer la réalisation de ces objectifs» en tant que parties intégrantes des codes en question. En outre, l'absence de toute référence à des mécanismes (obligatoires) de contrôle des codes de conduite destinés à vérifier que les fournisseurs de systèmes d'IA qui ne sont pas à haut risque respectent leurs dispositions, ainsi que la possibilité pour les différents fournisseurs d'établir (et de mettre en œuvre eux-mêmes) lesdits codes (voir le point 5.2.7 de l'exposé des motifs) pourraient affaiblir davantage l'efficacité et l'applicabilité de ces instruments.

80. Enfin, l'EDPB et le CEPD demandent des éclaircissements concernant les types d'initiatives que la Commission pourrait élaborer, conformément au considérant 81 de la proposition, «pour faciliter la suppression des obstacles techniques entravant l'échange transfrontière de données pour le développement de l'IA».

4 CONCLUSION

81. Bien que l'EDPB et le CEPD saluent la proposition de la Commission et estiment qu'un tel règlement est nécessaire pour garantir les droits fondamentaux des citoyens et résidents de l'UE, ils estiment que la proposition doit être adaptée sur plusieurs points, afin de garantir son applicabilité et son efficacité.

82. Compte tenu de la complexité de la proposition et des problèmes qu'elle vise à résoudre, il reste beaucoup à faire pour que la proposition puisse donner naissance à un cadre juridique fonctionnel, complétant efficacement le RGPD en protégeant les droits de l'homme fondamentaux tout en favorisant l'innovation. L'EDPB et le CEPD resteront à la disposition de la Commission pour lui apporter leur soutien dans ce processus.

Bruxelles, le 18 juin 2021

Pour le Comité européen de la protection des données	Pour le Contrôleur européen de la protection des données
La présidente	Le Contrôleur
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI