Conseil de
l'Union européenne

Bruxelles, le 12 septembre 2022
(OR. en)

12302/22

Dossier interinstitutionnel:
2021/0106(COD)

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

AVIS DU SERVICE JURIDIQUE [1]

Origine:	Service juridique
Objet:	Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle – Pertinence des articles 114 et 16 du TFUE en tant que bases juridiques en ce qui concerne les dispositions applicables aux autorités répressives et judiciaires

I. INTRODUCTION

1. La proposition de règlement établit des règles harmonisées pour la mise sur le marché et la mise en service de systèmes d'intelligence artificielle (ci-après "systèmes d'IA") dans l'Union (ci-après "proposition de règlement")[2].

[1] Le présent document contient des avis juridiques faisant l'objet d'une protection au titre de l'article 4, paragraphe 2, du règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, et non rendus accessibles au public par le Conseil de l'Union européenne. Le Conseil se réserve la faculté de faire valoir tous ses droits en cas de publication non autorisée.

[2] Doc. 8115/21.

2. Lors de la réunion du groupe "Télécommunications et société de l'information" du 7 avril 2022, le Service juridique du Conseil (SJC) est intervenu sur la question de la pertinence de la double base juridique (articles 16 et 114 du TFUE) pour la proposition de règlement relatif aux systèmes d'IA. Les explications ont confirmé que les articles 16 et 114 du TFUE étaient à juste titre les bases juridiques de la proposition et que le recours à l'article 87, paragraphe 2, du TFUE, au lieu de l'article 114, ne convenait pas. À la demande du groupe, le présent avis expose par écrit et approfondit l'intervention du représentant du SJC lors de cette réunion.

3. Les systèmes d'IA sont définis à l'article 3, paragraphe 1, de la proposition de règlement. En général, ils correspondent à certains types de logiciels. La proposition de règlement s'applique tant aux fournisseurs qui mettent des systèmes d'IA sur le marché qu'à ceux qui mettent des systèmes d'IA en service. En outre, la proposition de règlement s'applique également aux utilisateurs. Un fournisseur peut être une personne physique ou morale, une autorité/agence publique qui développe ou fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque. Un utilisateur peut être toute personne physique ou morale, autorité publique, agence ou autre organisme utilisant sous sa propre autorité un système d'IA.

4. Selon les définitions de l'article 3, les autorités répressives et judiciaires pourraient être considérées comme des fournisseurs et/ou des utilisateurs d'un système d'IA. Les systèmes d'IA dont la destination, définie par le fournisseur, est le maintien de l'ordre ou l'administration de la justice sont classés comme étant à haut risque en vertu de l'annexe III. En tant que tels, ils sont soumis à des exigences essentielles (gestion des risques, tests, gouvernance des données, documentation technique, transparence, contrôle humain, exactitude, robustesse et cybersécurité) et à des obligations (en ce qui concerne par exemple les systèmes de gestion de la qualité, la documentation technique, l'évaluation de la conformité, les mesures correctives, le devoir d'information, les obligations des importateurs et des distributeurs), ainsi qu'à des normes et à l'évaluation de la conformité. Ces règles harmonisées s'inspirent de celles qui s'appliquent à la sécurité des produits dans la directive 2006/42/CE (machines)[3] et le règlement (UE) 2017/745 (dispositifs médicaux)[4].

5. Quant aux systèmes d'IA se caractérisant par l'exploitation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives, ils relèvent de la catégorie des systèmes d'IA interdits. Cette interdiction d'utiliser des systèmes d'IA comporte néanmoins des exceptions. En effet, l'utilisation de tels systèmes peut ou non être autorisée par les États membres. Si ces systèmes sont autorisés, ils sont soumis à des restrictions et à des garanties détaillées afin de limiter leur utilisation à ce qui est strictement nécessaire et de préserver le droit fondamental à la protection des données à caractère personnel. Ces restrictions et garanties sont prévues dans la proposition de règlement sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE) et doivent être complétées par le droit national. L'article 5, paragraphe 1, point d), et paragraphes 2, 3 et 4, de la proposition de règlement constitue une *lex specialis* par rapport à la directive (UE) 2016/680 (directive en matière de protection des données dans le domaine répressif), qui a été adoptée sur la base de l'article 16, paragraphe 2, du TFUE.

---

[3] Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24).

[4] Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1).

Conformément à l'article 5, paragraphe 1, point d), l'utilisation de ces systèmes se limite aux objectifs suivants:

i) la recherche ciblée de victimes potentielles spécifiques de la criminalité, notamment d'enfants disparus;

ii) la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques ou la prévention d'une attaque terroriste;

iii) la détection, la localisation, l'identification ou les poursuites à l'encontre de l'auteur ou du suspect d'une infraction pénale visée à l'article 2, paragraphe 2, de la décision relative au mandat d'arrêt européen[5] et punissable dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins trois ans, déterminées par le droit de cet État membre.

Conformément à l'article 5, paragraphe 3, l'utilisation de ces technologies par les services répressifs doit être subordonnée à l'autorisation préalable octroyée par une autorité judiciaire ou administrative. Toutefois, dans une situation d'urgence dûment justifiée, il est possible de commencer à utiliser le système sans autorisation et de demander l'autorisation en cours d'utilisation ou lorsque celle-ci a pris fin.

En vertu de l'article 5, paragraphe 4, un État membre peut décider d'autoriser l'utilisation de systèmes d'identification biométriques à distance "en temps réel" dans des espaces accessibles au public à des fins répressives et définir les modalités nécessaires à la demande, à la délivrance et à l'exercice des autorisations préalables, ainsi que les infractions pénales concernées.

6. Les bases juridiques de la proposition de règlement sont l'article 16 du TFUE (protection des données à caractère personnel) et l'article 114 du TFUE (fonctionnement du marché intérieur). Par conséquent, la question se pose de savoir si ces bases juridiques sont appropriées au regard des règles harmonisées applicables aux systèmes d'IA fournis ou utilisés par les autorités répressives et judiciaires.

[5] Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

7. Le présent avis examine tout d'abord la question de savoir si l'article 114 du TFUE constitue une base juridique adéquate dans le contexte particulier des autorités répressives mentionnées dans plusieurs dispositions de la proposition de règlement, c'est-à-dire en ce qui concerne les systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public et les systèmes d'IA à haut risque visés à l'annexe III, point 6. Par conséquent, il aborde la question de savoir si l'article 87, paragraphe 2, du TFUE (coopération policière) constituerait une base juridique plus idoine pour couvrir la fourniture et l'utilisation de systèmes d'IA par les autorités répressives, plutôt que l'article 114 du TFUE (section II). Par analogie, la conclusion de la présente note pourra s'appliquer aux autorités judiciaires visées à l'annexe III concernant les systèmes d'IA à haut risque.

8. La présente note examine également la pertinence de la base juridique supplémentaire que constitue l'article 16 du TFUE, ainsi que l'application des protocoles n° 21 et n° 22 dans le contexte de l'utilisation par les services répressifs de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public (section III).

II. PERTINENCE DE L'ARTICLE 114 DU TFUE EN TANT QUE BASE JURIDIQUE

9. Il est de jurisprudence constante que le choix de la base juridique d'un acte de l'Union ne dépend pas de la conviction d'une institution quant au but poursuivi, mais doit se fonder sur des éléments objectifs susceptibles de contrôle juridictionnel, à savoir notamment le but et le contenu de l'acte. Si l'examen d'un acte démontre que celui-ci poursuit une double finalité ou qu'il a une double composante et si l'une de celles-ci est identifiable comme principale ou prépondérante, tandis que l'autre n'est qu'accessoire, cet acte doit être fondé sur une seule base juridique, à savoir celle exigée par la finalité ou la composante principale ou prépondérante. À titre exceptionnel, uniquement s'il est établi que l'acte poursuit à la fois plusieurs objectifs, qui sont liés d'une façon indissociable, sans que l'un soit second et indirect par rapport à l'autre, un tel acte pourra être fondé sur les différentes bases juridiques correspondantes, à moins que ces bases juridiques prévoient des procédures qui sont incompatibles. Il y a également lieu de noter que la première phrase de l'article 114, paragraphe 1, du TFUE indique clairement que les dispositions de cet article s'appliquent "*[s]auf si les traités en disposent autrement*". En conséquence, le recours à l'article 114 du TFUE n'est justifié que si aucune disposition plus spécifique ne peut constituer la base juridique pour l'adoption de l'acte en cause[6]. Dès lors qu'il existe, dans le traité, une disposition plus spécifique pouvant constituer la base juridique de l'acte en cause, celui-ci doit être fondé sur cette disposition[7].

---

6 Avis du SJC du 17 mai 2016, 9007/16, point 6.

7 Arrêt du 29 avril 2004, *Commission/Conseil*, C-338/01, EU:C:2004:253, point 60.

A. OBJECTIF DE LA PROPOSITION DE REGLEMENT

10. La proposition de règlement harmonise la mise sur le marché, la mise en service et l'utilisation d'un type particulier de logiciel (systèmes d'IA). Le fait que les autorités publiques et les opérateurs privés puissent être des fournisseurs ou des utilisateurs de tels systèmes d'IA n'est pas incompatible en soi avec la base juridique de l'article 114 du TFUE[8].

11. En outre, le fait que les autorités répressives ou ceux agissant pour leur compte puissent figurer parmi les fournisseurs ou les utilisateurs de ces systèmes d'IA ne suffit pas à justifier le recours à l'article 87 du TFUE comme base juridique. L'objectif et le contenu de la proposition de règlement doivent être analysés afin de déterminer si cela est nécessaire.

12. D'une façon générale, la proposition de règlement vise, y compris en ce qui concerne les systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public et les systèmes d'IA à haut risque, à garantir un niveau de protection cohérent et élevé dans l'ensemble de l'Union tout en évitant que des disparités n'entravent la libre circulation des systèmes d'IA et des produits et services connexes au sein du marché intérieur. Elle établit des obligations uniformes pour les opérateurs et garantit la protection uniforme des raisons impérieuses d'intérêt général et des droits des citoyens dans l'ensemble du marché intérieur (considérant 2). Plus précisément, la proposition de règlement établit des règles régissant la mise sur le marché et la mise en service de certains systèmes d'IA, garantissant ainsi le bon fonctionnement du marché intérieur et permettant à ces systèmes de bénéficier du principe de libre circulation des marchandises et des services (considérant 5). D'une façon générale, la proposition vise à mettre en place une IA fiable dès la conception, applicable à tous les niveaux, avec un ensemble complet de règles pour le développement, la commercialisation et l'utilisation de produits, services et systèmes fondés sur l'IA. Étant donné que l'IA a déjà trouvé sa place dans un grand nombre de services et de produits et que ce processus se poursuivra à l'avenir, la proposition suit une logique de marché intérieur en établissant un "cadre pour la sécurité des produits" articulé autour d'un ensemble de quatre catégories de risques. Elle impose des exigences pour l'entrée sur le marché et la certification des systèmes d'IA à haut risque au moyen d'une procédure de marquage CE obligatoire.

---

[8] Voir l'avis juridique du SJC (ST 11395/14, points 39 à 41) et des précédents tels que les directives (UE) 2016/2102, 2014/24/UE, 2014/25/UE et 2014/23/UE.

13. Aucun des objectifs déclarés de la proposition de règlement ne vise à garantir des objectifs de sécurité publique. Même si des objectifs de sécurité publique doivent être atteints indirectement grâce au processus d'harmonisation de la mise sur le marché/de la mise en service/de l'utilisation de systèmes d'IA par les autorités répressives, la Cour[9], interprétant l'article 87, paragraphe 2, du TFUE à la lumière de l'article 67 du TFUE, a indiqué que, pour qu'un acte de l'Union, eu égard à sa finalité et à son contenu, soit fondé sur le premier de ces articles, il devait être directement lié aux objectifs énoncés à l'article 67 du TFUE (à savoir, en l'espèce, la prévention de la criminalité et la coopération policière). Cela est exclu dans le contexte de la proposition de règlement, étant donné que les seules règles harmonisées relatives à l'utilisation de ces systèmes par les autorités répressives sont soit (1) des règles de type "sécurité des produits" applicables de manière uniforme à tous les fournisseurs et utilisateurs en ce qui concerne la mise sur le marché, la mise en service ou l'utilisation des systèmes d'IA, soit (2) des règles relatives à la protection des données à caractère personnel, pour lesquelles l'article 16 du TFUE a été ajouté en tant que base juridique (voir partie III ci-dessous).

14. Dans une autre affaire[10], même si l'objectif de la modification de la directive sur les armes à feu consistait à assurer un niveau plus élevé de sécurité publique en rapport avec la menace terroriste et d'autres formes de criminalité, la Cour a jugé que l'harmonisation des aspects relatifs à la sécurité des marchandises était l'un des éléments essentiels aux fins d'assurer le bon fonctionnement du marché intérieur, des réglementations disparates en cette matière étant susceptibles de créer des obstacles aux échanges[11].

---

9 Arrêt du 6 mai 2014, *Commission européenne/Parlement européen et Conseil de l'Union européenne*, C-43/12, EU:C:2014:298.

10 Arrêt du 3 décembre 2019, *République tchèque/Parlement européen*, C- 482/17, EU:C:2019:1035.

11 Ibid., point 57: "*Or, la particularité des armes à feu étant, contrairement à ce que prétend la République de Pologne, leur dangerosité non seulement pour les utilisateurs, mais également pour le grand public, ainsi que la Cour l'a déjà relevé au point 54 de l'arrêt du 23 janvier 2018, Buhagiar e.a. (C- 267/16, EU:C:2018:26), des considérations de sécurité publique apparaissent, ainsi que le rappelle le cinquième considérant de la directive 91/477, indispensables dans le cadre d'une réglementation sur l'acquisition et la détention de ces marchandises.*" Voir également l'arrêt du 23 janvier 2018, *Albert Buhagiar e.a./Minister for Justice*, C-267/16, EU:C:2018:26, point 54: "*À cet égard, il importe de faire observer que, au vu du risque pour la sécurité des personnes que présentent les armes à feu, leur libre circulation n'a pu être atteinte qu'au moyen d'un encadrement strict des conditions de leur transfert entre États membres, parmi lesquelles figure le principe de l'autorisation préalable délivrée par les États membres concernés par un transfert de telles marchandises.*"

15. Les objectifs de la proposition de règlement, y compris l'article 5, paragraphe 1, point d), et paragraphes 2, 3 et 4, relatif à l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives, ainsi que les dispositions relatives aux systèmes d'IA à haut risque visés à l'annexe III, point 6, ne sont pas directement liés à un objectif de sécurité publique. Au contraire, la proposition répond aux principales préoccupations liées à la manière dont les systèmes d'IA affectent la santé, la sécurité et les droits fondamentaux. Par conséquent, les dispositions pertinentes sont directement liées à l'objectif consistant à garantir des conditions de concurrence équitables lors de la mise sur le marché, de la mise en service ou de l'utilisation de systèmes d'IA dans le marché intérieur, tout en protégeant la santé, la sécurité et les droits fondamentaux des utilisateurs.

16. À la lumière de ce qui précède, le principal objectif de la proposition de règlement est d'améliorer le fonctionnement du marché intérieur au sens de l'article 114 du TFUE, et les objectifs visés à l'article 67 du TFUE ne sont liés à cet objectif principal que de façon indirecte et accessoire.

B. TENEUR DE LA PROPOSITION DE REGLEMENT

17. La proposition de règlement contient essentiellement des règles sur les éléments nécessaires pour mettre un produit spécifique (un logiciel d'IA) sur le marché (ou pour le mettre en service), de façon à garantir que ce produit est sûr et qu'il respecte les droits fondamentaux. Elle définit un ensemble complet de règles pour le développement, la commercialisation et l'utilisation de produits, services et systèmes fondés sur l'IA. La proposition de règlement n'oblige pas les autorités répressives à utiliser un système d'IA légalement mis sur le marché et ne réglemente pas directement la manière dont elles devraient utiliser un tel système d'IA. En revanche, elle définit clairement les situations dans lesquelles l'utilisation prévue est considérée comme étant à haut risque pour la simple raison qu'un système d'IA sera utilisé par les autorités répressives ou judiciaires.

18. Au demeurant, l'article 29 de la proposition de règlement contient des règles relatives aux conditions d'utilisation des systèmes d'IA à haut risque, mais une telle disposition n'est pas sectorielle, elle a une portée limitée (principalement en ce qui concerne les notices d'utilisation accompagnant le produit) et est intrinsèquement liée aux obligations imposées aux développeurs de systèmes d'IA en vertu de la proposition de règlement. En outre, une certaine marge de manœuvre est laissée aux États membres pour prévoir de nouvelles règles relatives à l'utilisation de ces systèmes d'IA à haut risque. En ce qui concerne les systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public utilisés à des fins répressives (article 5), la proposition réglemente en partie l'utilisation de ces systèmes du point de vue de la protection des données sur la base de l'article 16 du TFUE (voir la partie III ci-dessous).

19. Par ailleurs, il appartient aux seuls États membres de décider de prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation de tels systèmes d'identification biométrique à distance "en temps réel". Les conditions spécifiques d'une telle utilisation doivent encore être fixées dans le droit national, mais elles doivent respecter les garanties et critères généraux énoncés dans le règlement: autorisation préalable octroyée par une autorité judiciaire ou administrative, modalités de la demande, de la délivrance et de l'exercice de l'autorisation préalable, ainsi que l'indication des infractions pénales pour lesquelles ces systèmes peuvent être utilisés.

20. Les systèmes d'IA sont un type de logiciel particulier. Les règles harmonisées applicables à la mise sur le marché ou à la mise en service/l'utilisation de systèmes d'IA sont donc du type de celles concernant la sécurité des produits. Elles s'appliquent de manière uniforme, sans distinction entre les utilisateurs publics et privés. Conformément aux considérants concernés de la proposition de règlement, il convient donc de garantir un niveau de protection cohérent et élevé dans toute l'Union. Dans le même temps, il convient d'éviter les divergences qui entravent la libre circulation des systèmes d'IA et des produits et services connexes au sein du marché intérieur. Ce résultat serait atteint en établissant des obligations uniformes pour les opérateurs et en garantissant la protection uniforme des raisons impérieuses d'intérêt général et des droits des citoyens dans l'ensemble du marché intérieur conformément à l'article 114 du TFUE[12].

21. La proposition de règlement contient plusieurs références aux services répressifs, à la gestion des contrôles aux frontières et à l'administration de la justice à l'annexe III relative aux systèmes d'IA à haut risque (points 6, 7 et 8 respectivement). Il s'agit notamment d'une énumération détaillée et exhaustive correspondant à l'article 6, paragraphe 2, en plus des autres systèmes considérés comme à haut risque du fait des risques afférents à la sécurité du produit énoncés à l'article 6, paragraphe 1. En effet, conformément à l'article 6, paragraphe 1, certains systèmes d'IA doivent être considérés par définition comme étant à haut risque en raison de leur dangerosité attendue et des risques élevés qu'ils présentent pour les droits fondamentaux, la santé et la sécurité. Les autres systèmes considérés comme à haut risque et figurant sur les listes à l'annexe III comprennent ceux utilisés dans les domaines de l'éducation, la gestion des infrastructures critiques, l'emploi, l'identification et la catégorisation biométriques ainsi que l'accès aux services publics et privés essentiels.

---

[12] Un cadre juridique de l'Union établissant des règles harmonisées sur l'intelligence artificielle est donc nécessaire pour favoriser le développement, l'utilisation et l'adoption de l'intelligence artificielle dans le marché intérieur, tout en garantissant un niveau élevé de protection des intérêts publics, comme la santé, la sécurité et la protection des droits fondamentaux, tels qu'ils sont reconnus et protégés par le droit de l'Union. Pour atteindre cet objectif, des règles régissant la mise sur le marché et la mise en service de certains systèmes d'IA devraient être établies, garantissant ainsi le bon fonctionnement du marché intérieur et permettant à ces systèmes de bénéficier du principe de libre circulation des marchandises et des services (cf. considérants 2 et 5 de la proposition).

22. Toutefois, ces règles relatives aux systèmes d'IA à haut risque ne précisent pas si les autorités répressives et judiciaires (ou les autorités dans d'autres domaines recensés) devraient ou non utiliser ces systèmes. Le règlement proposé ne produira qu'indirectement ses effets sur le développement réel des systèmes d'IA susceptibles d'être utilisés par les autorités répressives, ainsi que sur les systèmes d'IA en usage actuellement et à l'avenir. Ainsi les règles évoquent-elles des systèmes d'IA "*destinés à être utilisés*" par ces autorités (voir par exemple l'article 3, paragraphe 12, l'article 8, paragraphe 2, et l'annexe III). Lorsqu'un système d'IA est inscrit sur la liste des systèmes d'IA à haut risque, cela entraîne pour conséquence que l'on applique un ensemble de règles particulières en matière de gestion des risques, de gouvernance des données et de spécifications techniques. Les utilisateurs de ces systèmes d'IA à haut risque doivent respecter les notices d'utilisation, tenir des journaux et effectuer des analyses d'impact relatives à la protection des données.

23. En outre, les obligations de l'utilisateur autres que celles liées à la notice d'utilisation peuvent être fixées dans le droit de l'Union ou le droit national et sans préjudice de la faculté de l'utilisateur d'organiser ses propres ressources et activités aux fins de la mise en œuvre des mesures de contrôle humain indiquées par le fournisseur (article 29, paragraphe 2, de la proposition de règlement). Ces règles prévoient, en ce qui concerne les systèmes d'IA à haut risque, des garanties supplémentaires en matière de droits fondamentaux.

24. À la lumière de ce qui précède, il convient de souligner que la proposition de règlement ne contient pas de règles ayant pour objet de permettre ou d'empêcher qu'un système d'IA à haut risque mis sur le marché soit utilisé par les autorités répressives. Les règles proposées auront pour effet que tout système d'IA développé ou utilisé par des autorités répressives sera classé de façon particulière ("à haut risque") en raison de l'usage auquel il est destiné. Cet usage serait régi par le droit national et, dans une certaine mesure, décidé par les autorités répressives elles-mêmes. En effet, la proposition de règlement fixe, à l'article 29, des conditions minimales d'utilisation (se limitant aux notices d'utilisation) pour les systèmes d'IA à haut risque, y compris ceux figurant sur les listes des points 6, 7 et 8 de l'annexe III, qui seront complétées par des dispositions de droit national. Par conséquent, conformément à la jurisprudence de la Cour, il convient d'établir une distinction entre d'une part, l'objectif visé par le règlement proposé, qui n'est pas de réglementer l'utilisation de systèmes d'IA par les autorités répressives, et d'autre part, les effets qu'il peut produire indirectement[13], qui sont dénués de pertinence aux fins de l'analyse du caractère approprié de la base juridique.

25. Les domaines visés aux points 6, 7 et 8 (concernant respectivement les autorités répressives, la migration et l'administration de la justice) ne sont pas prédominants parmi les systèmes d'IA à haut risque. En effet, suivant le règlement proposé, un système d'IA à haut risque n'est pas nécessairement un système figurant sur les listes de l'annexe III. La plupart des systèmes à haut risque sont en fait ceux indiqués de façon générique à l'article 6, paragraphe 1, points a) et b), de la proposition de règlement (en lien avec la sécurité des produits). D'autres systèmes d'IA à haut risque figurent sur des listes à l'annexe III, qui comprend des points 1 (identification biométrique), 2 (infrastructures critiques), 3 (éducation et formation professionnelle) et 4 (emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant) ayant trait à des domaines autres que la justice et les affaires intérieures ("JAI"). Tous les utilisateurs de ces systèmes d'IA à haut risque sont soumis à un régime uniforme établi non pas en raison de leur statut particulier (par exemple le fait qu'ils soient un opérateur économique ou une autorité publique), mais dans une perspective de protection de la santé, de la sécurité et des droits fondamentaux.

---

[13] Voir l'arrêt de la Cour du 21 juin 2018, *République de Pologne/Parlement européen, Conseil de l'Union européenne*, C-5/16, EU:C:2018:483, points 63 à 68; et l'arrêt de la Cour du 22 juin 2022, *Leistritz AG/LH*, C-534/20, EU:C:2022:495, point 28.

26. Le règlement proposé contient donc des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA, qu'ils soient utilisés par des opérateurs privés ou des autorités publiques, y compris de manière accessoire[14], ou par des autorités répressives et judiciaires.

27. En dehors de l'utilisation de systèmes pour l'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives, soumise à des règles particulières sur le traitement des données à caractère personnel (voir la partie III ci-dessous), la proposition de règlement ne contient pas de règles harmonisées quant à l'utilisation de systèmes d'IA à haut risque. Comme expliqué aux points 18 et 19 ci-dessus, la référence à l'utilisation de systèmes d'IA à haut risque a essentiellement trait aux notices d'utilisation accompagnant le produit (article 29) et est liée aux obligations imposées aux développeurs. Comme indiqué au point 22, la décision quant à la question de savoir si les autorités répressives ou judiciaires peuvent ou non utiliser un système d'IA à haut risque qui est légalement mis sur le marché en vertu du règlement proposé relève du droit national et des autorités nationales.

28. Par conséquent, l'article 87, paragraphe 2, du TFUE, et en particulier son point a), ne constitue pas une base juridique idoine pour le règlement proposé. Les règles figurant dans la proposition ne favorisent ni n'entravent la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes. Simplement, lorsque de telles activités sont menées par des autorités répressives, il faudra qu'un certain nombre de conditions non spécifiques et harmonisées soient respectées afin de sauvegarder les droits des utilisateurs. De même, le développement de techniques d'enquête communes ne figure pas parmi les objectifs déclarés de la proposition de règlement. Les exigences proposées quant à l'utilisation de systèmes d'IA à haut risque ne sont pas propres au domaine JAI et ne concernent pas la coopération policière *stricto sensu* telle que définie dans le TFUE.

---

14 Voir l'avis de la Cour sur la *convention d'Istanbul*, A-1/19, EU:C:2021:198, en particulier les points 298 et 301.

29. En ce qui concerne les dispositions de l'article 5, paragraphe 4, de la proposition de règlement, tout État membre garde la possibilité de décider d'autoriser l'utilisation de systèmes pour l'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives. S'il prend cette décision, ledit État membre a l'obligation de définir les modalités nécessaires à la demande, la délivrance et l'exercice de l'autorisation préalable ainsi que les infractions pénales concernées par les enquêtes ou les poursuites pour lesquelles l'utilisation est autorisée[15]. Les résultats des discussions au sein du Conseil amènent à conclure que ces règles proposées n'auraient pas pour effet de conférer de nouveaux pouvoirs aux autorités nationales respectives. Il s'agit plutôt d'encadrer le recours à des mécanismes existants ou futurs afin d'assurer la protection du droit à la vie privée et des données à caractère personnel.

30. À la lumière de ce qui précède, l'article 114 du TFUE constitue la seule base juridique appropriée pour des règles harmonisées sur les systèmes d'IA à haut risque, y compris ceux utilisés par les autorités répressives et judiciaires, et aucune base juridique JAI figurant dans la troisième partie, titre V, du TFUE, telle que l'article 87 du TFUE, n'est, en ce qui concerne ces règles harmonisées, justifiée ou appropriée.

[15] Il est à relever que l'article 5, paragraphe 4, de la proposition présente certaines caractéristiques similaires à celles de l'article 15, paragraphe 1, de la directive 2002/58 sur le commerce électronique. La possibilité y est notamment prévue pour les États membres de déroger à certaines interdictions inscrites dans le droit de l'Union. Compte tenu de la jurisprudence constante, les dispositions nationales visant à déroger à ces interdictions relèveront nécessairement du champ d'application du droit de l'Union qui, à son tour, déclenchera l'application de la charte à leur égard.

III. PERTINENCE DE L'ARTICLE 16 DU TFUE EN TANT QUE BASE JURIDIQUE SUPPLÉMENTAIRE

31. Le règlement proposé prend l'article 16 du TFUE en tant que base juridique en ce qui concerne le traitement des données à caractère personnel dans le domaine répressif, et ses considérants 25 et 26 comprennent une référence à l'article 6 *bis* du protocole n° 21 et à l'article 2 *bis* du protocole n° 22 concernant le traitement de données à caractère personnel dans le domaine de la prévention de la criminalité. L'article 16 du TFUE doit, de l'avis de la Commission, servir de base juridique exclusive aux dispositions plaçant des restrictions au traitement de données biométriques à caractère personnel de façon complémentaire par rapport à la directive (UE) 2016/680 (ci-après dénommée la "directive en matière de protection des données dans le domaine répressif"). L'article 5, paragraphe 1, point c), est formulé comme une interdiction de principe, à laquelle s'applique un ensemble de trois exceptions. Concrètement, l'utilisation de systèmes pour l'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives est interdite, sauf si cela est strictement nécessaire à des fins a) de recherches ciblées de victimes potentielles de la criminalité, b) de prévention d'attaques terroristes ou d'attaques contre l'intégrité physique/la vie d'une personne, c) de localisation, identification ou poursuite d'auteurs ou suspects d'une infraction grave (avec une référence au mandat d'arrêt européen). D'autres exigences figurant à l'article 5, paragraphes 2, 3, et 4, conditionnent cette utilisation particulière des systèmes d'IA par les autorités répressives, à savoir notamment une évaluation de la nécessité et de la proportionnalité, une autorisation préalable (sauf dans les situations d'urgence) et une décision des États membres d'autoriser ou non au niveau national l'utilisation spécifique d'outils d'IA dans de telles situations.

32. L'article 5 est une disposition détaillée qui régit une utilisation particulière des outils d'IA qui vise non seulement à compléter le cadre législatif existant de l'Union (la directive en matière de protection des données dans le domaine répressif, ayant elle-même pour base l'article 16 du TFUE), mais qui requiert également un cadre national de mise en œuvre.

33. Sur le fond, bien qu'elle soit formulée comme une interdiction, la règle spécifique de l'article 5 peut être décrite comme définissant un cadre strict et exceptionnel pour la surveillance généralisée "en temps réel", par des instruments d'IA, d'individus dans des espaces ouverts afin de les identifier. L'interdiction va également au-delà de la simple utilisation de caméras pour l'enregistrement et fait référence à l'utilisation d'outils d'IA à des fins de reconnaissance automatisée de caractéristiques humaines dans des espaces accessibles au public (caractéristiques telles que les visages, mais aussi la démarche, les empreintes digitales, l'ADN, la voix, la frappe au clavier et d'autres signaux biométriques ou comportementaux). Cela implique également l'acquisition de données et l'identification concomitantes de personnes par comparaison/vérification analytique de données. En outre, la règle doit également être appréciée au regard du fait que l'identification "en temps réel" par des utilisateurs privés dans des espaces publics peut également être autorisée (pour des événements tels que des matches de football).

34. D'autres précisions apportées par la Commission semblent indiquer qu'à l'heure actuelle, très peu d'États membres ont réglementé cette question particulière, voire aucun, l'objectif étant de permettre aux autorités répressives d'utiliser des outils d'IA pour la détection "en temps réel" d'individus dans des espaces publics. Toutefois, sur le plan pratique, bien qu'aucun élément concret n'ait été apporté pour prouver la nécessité de changer les pratiques et outils existants, il semble clair que les futures techniques d'enquête, méthodes de police scientifique et règles relatives à la collecte de preuves devront intégrer cette approche en matière d'interdiction/d'exceptions.

35. En ce qui concerne la base juridique, il apparaît que les dispositions plaçant des restrictions au traitement de données biométriques à caractère personnel de façon complémentaire (par rapport à la directive en matière de protection des données dans le domaine répressif) poursuivent l'objectif de protéger les données à caractère personnel en établissant des garanties appropriées. Un tel objectif est indissociablement lié à celui des dispositions relevant du champ d'application de l'article 114 du TFUE, sans que l'un soit second et indirect par rapport à l'autre. Le règlement proposé vise à établir un cadre général pour les systèmes d'IA selon une approche fondée sur les risques. Dans ce contexte, réglementer les systèmes d'IA de manière horizontale peut comprendre des garanties strictes applicables à ce système d'IA particulier de détection "en temps réel". Un tel système d'IA particulier comportant des garanties appropriées en matière de protection des données à caractère personnel est donc indissociable de l'objectif global d'amélioration du fonctionnement du marché intérieur et n'est pas second ou indirect par rapport à ce dernier. Le règlement proposé devrait donc être régi par une double base juridique, conformément à la jurisprudence pertinente (voir point 9 ci-dessus).

36. La question reste toutefois de savoir quelle base juridique devrait être utilisée pour réglementer le traitement des données à caractère personnel aux fins de l'utilisation de systèmes visés à l'article 5, paragraphe 1, point c), et paragraphes 2 à 4, de la proposition de règlement. En effet, l'article 87, paragraphe 2, point a), du TFUE constitue une base juridique pour les mesures prises par les services répressifs spécialisés dans la prévention ou la détection des infractions pénales et les enquêtes en la matière, en ce qui concerne la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes.

37. Comme l'avocat général l'a expliqué dans ses conclusions préalables à l'avis sur l'échanges de données PNR avec le Canada (A1/15), l'article 16 du TFUE, d'une part, et l'article 87, paragraphe 2, point a), ainsi que l'article 82, paragraphe 1, point d), du TFUE, d'autre part, ne sauraient cependant entretenir des rapports de type hiérarchique "*lex generalis – lex specialis*"[16]. L'article 16, paragraphe 2, du TFUE est la seule disposition qui s'applique aux règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités répressives des États membres dans l'exercice d'activités de prévention de la criminalité. Le simple fait que l'article 5 fasse référence à la liste des infractions graves figurant dans la décision-cadre relative au mandat d'arrêt européen ne change rien à cette appréciation: cette référence ne signifie pas que cette décision-cadre s'applique en tant que telle[17]. Il ne s'agit là que d'une technique législative permettant d'établir une liste d'infractions pénales graves sans qu'il soit nécessaire de créer une annexe distincte.

38. Il n'en demeure pas moins que la règle énoncée à l'article 5 n'est pas établie comme un moyen de délimiter davantage les conditions d'application de ces mesures liées à la JAI, mais en vue de garantir que, à l'avenir, toute utilisation de l'identification biométrique "en temps réel" par les systèmes d'IA répondra de manière adéquate aux préoccupations en matière de droits fondamentaux, et principalement à la nécessité de veiller à ce que les données biométriques soient collectées et traitées dans le respect du droit à la vie privée et aux données à caractère personnel.

    À cet égard, le règlement ne vise pas à établir une nouvelle procédure obligatoire propre à la JAI, mais s'appuie plutôt sur des moyens procéduraux ayant fait leurs preuves pour garantir le respect des droits fondamentaux.

---

16 Voir les conclusions de l'avocat général P. Mengozzi du 8 septembre 2016, *Projet d'accord entre le Canada et l'Union européenne*, avis 1/15, EU:C:2016:656, points 112 à 120.

17 Sur la mise en œuvre de cette liste d'infractions pénales graves par les États membres, voir l'arrêt de la Cour du 21 juin 2022, *Ligue des droits de l'homme/Conseil des ministres*, C-817/19, EU:C:2022:65, points 150 à 152.

39. Si l'article 16 du TFUE constitue une base juridique supplémentaire appropriée, cela soulève des questions quant à l'application de l'article 6 *bis* du protocole n° 21 et de l'article 2 *bis* du protocole n° 22. Comme expliqué aux considérants 25 et 26 de la proposition, cela signifie que lorsque les autorités répressives irlandaises ou danoises utilisent des systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins de prévention de la criminalité, et dans la mesure où l'Irlande ou le Danemark ne sont pas liés par les règles correspondantes relatives à la coopération policière ou judiciaire en matière pénale, ces deux États membres ne sont pas liés par l'article 5, paragraphe 1, point d), et paragraphes 2 et 3, de la proposition de règlement. Cela ne signifie pas que l'article 5, paragraphe 1, point d), et paragraphes 2 et 3, contiennent des règles relatives à la coopération policière, telles que des règles sur le partage d'informations entre autorités répressives. Cela signifie simplement que l'article 5, paragraphe 1, point d), et paragraphes 2 et 3, de la proposition de règlement, à l'instar de la directive (UE) 2016/680 (la "directive en matière de protection des données dans le domaine répressif"), qui est une *lex generalis* adoptée sur la base de l'article 16 du TFUE, réglemente le traitement des données biométriques à caractère personnel dans le contexte particulier des systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins de prévention de la criminalité, et rien de plus. À cet égard, la proposition de la Commission suit l'approche retenue par le législateur de l'Union pour la directive en matière de protection des données dans le domaine répressif et, de ce fait, confirme que le recours à l'article 87, paragraphe 2, du TFUE dans ce contexte ne se justifie donc pas.

40. L'ajout de l'article 16 du TFUE à l'article 114 du TFUE est justifié, en l'espèce, par le fait que l'article 5, paragraphe 1, point d), et paragraphes 2 et 3, prévoit les seuls cas de réglementation de l'utilisation de systèmes d'IA autorisés qui interfère avec le droit à la protection des données à caractère personnel, ce qui constitue une *lex specialis* par rapport au cadre de la protection des données générales. De telles règles de *lex specialis* en matière de protection des données qui affectent l'utilisation de ces systèmes d'IA sensibles ne sauraient être considérées comme secondes ou indirectes par rapport à la base juridique du marché intérieur. Par conséquent, l'ajout de l'article 16 du TFUE en tant que base juridique est suffisamment justifié dans la proposition de règlement et le recours à l'article 87, paragraphe 2, point a), du TFUE n'est pas approprié.

IV. CONCLUSION

41. Compte tenu de ce qui précède, le SJC est d'avis que:

a) le recours aux articles 16 et 114 du TFUE en tant que bases juridiques du règlement proposé est justifié et approprié;

b) le recours à l'article 87, paragraphe 2, du TFUE ou à toute autre base juridique JAI n'est ni justifié ni approprié en ce qui concerne les règles harmonisées applicables aux systèmes d'IA susceptibles d'être fournis ou utilisés par les autorités répressives ou judiciaires.