Mercredi 6 octobre 2021

P9_TA(2021)0405

L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales

Résolution du Parlement européen du 6 octobre 2021 sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales (2020/2016(INI))

(2022/C 132/02)

Le Parlement européen,

— vu le traité sur l'Union européenne, et notamment ses articles 2 et 6, et le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

— vu la charte des droits fondamentaux de l'Union européenne (la «Charte»), et notamment ses articles 6, 7, 8, 11, 12, 13, 20, 21, 24 et 47,

— vu la convention de sauvegarde des droits de l'homme et des libertés fondamentales,

— vu la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108), et son protocole d'amendement («Convention 108+»),

— vu la charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement de la Commission européenne pour l'efficacité de la justice (CEPEJ) du Conseil de l'Europe,

— vu la communication de la Commission du 8 avril 2019 intitulée «Renforcer la confiance dans l'intelligence artificielle axée sur le facteur humain» (COM(2019)0168),

— vu les lignes directrices en matière d'éthique pour une intelligence artificielle digne de confiance, publiées par le groupe d'experts de haut niveau de la Commission sur l'intelligence artificielle le 8 avril 2019,

— vu le livre blanc de la Commission du 19 février 2020 intitulé «Intelligence artificielle — Une approche européenne axée sur l'excellence et la confiance» (COM(2020)0065),

— vu la communication de la Commission du 19 février 2020 intitulée «Une stratégie européenne pour les données» (COM(2020)0066),

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

— vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ([2]),

— vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE ([3]),

— vu la 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») ([4]),

([1]) JO L 119 du 4.5.2016, p. 1.
([2]) JO L 119 du 4.5.2016, p. 89.
([3]) JO L 295 du 21.11.2018, p. 39.
([4]) JO L 201 du 31.7.2002, p. 37.

Mercredi 6 octobre 2021

— vu le règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI ([5]),

— vu sa résolution du 19 juin 2020 sur les manifestations contre le racisme après la mort de George Floyd ([6]),

— vu sa résolution du 14 mars 2017 sur les incidences des mégadonnées pour les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi ([7]),

— vu l'audition tenue par la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) le 20 février 2020 sur l'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales,

— vu le rapport de la commission LIBE concernant sa mission aux États-Unis en février 2020,

— vu l'article 54 de son règlement intérieur,

— vu les avis de la commission du marché intérieur et de la protection des consommateurs et de la commission des affaires juridiques,

— vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures (A9-0232/2021),

A. considérant que les technologies numériques en général et, plus particulièrement, la prolifération du traitement et de l'analyse des données grâce à l'intelligence artificielle (IA) sont sources de grandes promesses et d'immenses risques; que de grands progrès ont été accomplis ces dernières années dans le développement de l'IA, en faisant de celle-ci l'une des technologies stratégiques du 21e siècle; qu'elle est susceptible de générer des avantages substantiels en matière d'efficacité, de précision et de facilité, et ainsi d'apporter un changement positif à l'économie et à la société européennes, mais qu'elle fait également peser de lourds risques sur les droits fondamentaux et les démocraties fondées sur l'état de droit; que l'IA ne doit pas être considérée comme une fin en soi, mais comme un outil pour servir les personnes, dans le but ultime d'accroître le bien-être humain, les capacités humaines et la sécurité;

B. considérant que, malgré les progrès constants en matière de vitesse de traitement informatique et de capacité de mémoire, il n'existe pas encore de programmes pouvant égaler la flexibilité humaine face à des domaines plus larges ou à des tâches nécessitant une compréhension du contexte ou une analyse critique; que certaines applications d'IA ont atteint le niveau de performance des experts et professionnels humains pour certaines tâches spécifiques (technologie au service du droit, par exemple), et peuvent fournir des résultats à une vitesse radicalement plus élevée et à une échelle bien plus grande;

C. considérant que certains pays, y compris plusieurs États membres, ont davantage recours aux applications d'IA, ou aux systèmes d'IA intégrés, à des fins répressives et judiciaires, ce qui tient en partie à l'absence de réglementation ou à une réglementation autorisant l'utilisation de l'IA à certaines fins, quand dans d'autres pays, la réglementation l'interdit; considérant que le recours de plus en plus fréquent à l'IA dans le domaine du droit pénal tient, en particulier, à la promesse que cette technologie permettrait de réduire certains types de criminalité et de prendre des décisions plus objectives; que cette promesse, toutefois, ne se concrétise pas toujours;

D. considérant que les libertés et droits fondamentaux consacrés par la charte devraient être garantis tout au long du cycle de vie de l'IA et des technologies connexes, notamment lors de leur conception, développement, déploiement et utilisation, et devraient être respectés en toutes circonstances dans le travail d'application des lois;

E. considérant qu'il convient de développer la technologie de l'IA de telle manière qu'elle soit axée sur les personnes, mérite la confiance du public et travaille toujours au service de l'humain; que les systèmes d'IA doivent offrir la garantie ultime d'être conçus de façon à pouvoir être arrêtés, à tout moment, par un opérateur humain;

F. considérant que les systèmes d'IA doivent être conçus pour la protection et le bien de tous les membres de la société (en tenant compte, dès leur conception, des populations vulnérables et marginalisées), être non discriminatoires et sûrs, garantir l'explicabilité et la transparence de leurs décisions, et respecter l'autonomie humaine et les droits fondamentaux, afin d'être fiables, comme l'explique le groupe d'experts de haut niveau sur l'intelligence artificielle dans ses lignes directrices en matière d'éthique;

([5]) JO L 135 du 24.5.2016, p. 53.
([6]) JO C 362 du 8.9.2021, p. 63.
([7]) JO C 263 du 25.7.2018, p. 82.

G. considérant que l'Union, de concert avec les États membres, assume la responsabilité essentielle de veiller à ce que les décisions relatives au cycle de vie et à l'utilisation des applications d'IA dans le domaine de la justice et de l'application des lois soient prises de manière transparente et, en particulier, ne perpétuent pas les discriminations, biais ou préjugés là où ils existent; considérant que les choix stratégiques en la matière devraient respecter les principes de nécessité et de proportionnalité en vue de garantir la constitutionnalité et d'assurer une justice équitable et humaine;

H. considérant que les applications d'IA peuvent offrir de grandes possibilités dans le domaine répressif, notamment pour ce qui est d'améliorer les méthodes de travail des services répressifs et des autorités judiciaires, et de lutter plus efficacement contre certains types de criminalité, en particulier la criminalité financière, le blanchiment de capitaux et le financement du terrorisme, les abus sexuels et l'exploitation sexuelle en ligne commis sur des enfants, ainsi que certains types de cybercriminalité, et qu'elles contribuent ainsi à la sûreté et à la sécurité des citoyens de l'Union, tout en comportant néanmoins des risques importants pour les droits fondamentaux des populations; considérant qu'il serait disproportionné d'utiliser l'IA de manière généralisée aux fins de la surveillance de masse;

I. considérant que de multiples personnes, organisations, composants de machines, algorithmes de logiciels et utilisateurs humains interviennent dans le développement et l'exploitation des systèmes d'IA destinés aux autorités policières et judiciaires, et que ces tâches sont souvent réalisées dans des environnements complexes et difficiles; considérant que les applications d'IA destinées aux domaines répressif et judiciaire ne sont pas toutes au même stade de développement, certaines se trouvant encore à l'étape de la conceptualisation, du prototypage ou de l'évaluation, quand d'autres ont déjà été approuvées et sont désormais utilisées; que de nouvelles possibilités d'utilisation pourraient se présenter à l'avenir, à mesure que la technologie gagnera en maturité grâce aux recherches scientifiques qui se poursuivent dans le monde entier;

J. considérant qu'il est impératif d'établir un modèle clair pour l'attribution de la responsabilité juridique des effets potentiellement préjudiciables des systèmes d'IA dans le domaine du droit pénal; que les dispositions réglementaires dans ce domaine devraient toujours maintenir la responsabilité humaine et doivent viser avant tout à éviter tout effet néfaste;

K. considérant qu'il incombe en définitive aux États membres de garantir le plein respect des droits fondamentaux lorsque des systèmes d'IA sont utilisés dans les domaines répressif et judiciaire;

L. considérant que la relation entre la protection des droits fondamentaux et l'efficacité de la police doit toujours être au cœur des discussions visant à savoir s'il convient d'utiliser l'IA dans le secteur répressif et, dans l'affirmative, à déterminer la manière de l'utiliser — étant entendu que sont prises, dans ces discussions, des décisions qui pourraient avoir des conséquences à long terme sur la vie et la liberté des personnes; considérant que cela est particulièrement important puisque l'IA pourrait devenir un élément permanent de l'écosystème de notre justice pénale en fournissant des analyses et une assistance dans le cadre des enquêtes;

M. considérant que l'IA est utilisée par les services répressifs dans des applications telles que les technologies de reconnaissance faciale, qui permettent par exemple de consulter des bases de données de suspects et d'identifier des victimes de la traite des êtres humains ou des enfants victimes d'exploitation sexuelle ou d'abus sexuels, la reconnaissance automatique des plaques minéralogiques, l'identification des orateurs, l'identification de la parole, les technologies de lecture sur les lèvres, la surveillance auditive (les algorithmes de détection des coups de feu), la recherche et l'analyse autonomes des bases de données identifiées, les prévisions (police prédictive et analyse des foyers de criminalité), les outils de détection des comportements, les outils avancés d'autopsie virtuelle pour aider à établir la cause du décès, les outils autonomes permettant de détecter la fraude financière et le financement du terrorisme, le suivi des médias sociaux (moissonnage et collecte de données pour l'exploration des connexions), et les systèmes de surveillance automatisée qui comportent différentes possibilités de détection (telles que la détection des battements du cœur et les caméras thermiques); que les applications susmentionnées, tout comme d'autres applications potentielles ou futures des technologies d'IA dans le domaine répressif, peuvent présenter des degrés très divers de fiabilité, de précision et d'incidence sur la protection des droits fondamentaux et sur la dynamique des systèmes de justice pénale; que nombre de ces outils sont utilisés dans des pays tiers mais seraient considérés comme illégaux en vertu de l'acquis et de la jurisprudence de l'Union en matière de protection des données; que le déploiement systématique d'algorithmes, même avec un faible taux de faux positifs, peut entraîner bien plus de fausses alertes que de vraies alertes;

N. considérant que les outils et applications d'IA sont également utilisés par les autorités judiciaires dans plusieurs pays du monde, y compris pour étayer les décisions relatives à la détention provisoire et lors de la fixation des peines, du calcul des probabilités de récidive et de la détermination de la probation, ainsi que pour le règlement en ligne des litiges, la gestion de la jurisprudence et la facilitation de l'accès à la législation; que ces outils et applications ont abouti à déformer la réalité et à réduire les chances des personnes de couleur et d'autres minorités; et que, à l'heure actuelle, dans l'Union européenne, à l'exception de quelques États membres, leur utilisation est essentiellement limitée au domaine civil;

O. considérant que l'utilisation de l'IA par les services répressifs comporte un certain nombre de risques potentiellement élevés et, dans certains cas, inacceptables, pour la protection des droits fondamentaux des personnes, tels que l'opacité du processus décisionnel, différents types de discrimination et d'erreurs inhérents à l'algorithme sous-jacent qui peuvent

être aggravés par des boucles de rétroaction, et des risques pour la protection de la vie privée et des données à caractère personnel, la protection de la liberté d'expression et d'information, la présomption d'innocence, le droit à un recours effectif et à un procès équitable, ainsi que des risques pour la liberté et la sécurité des personnes;

P. considérant que les systèmes d'IA utilisés par les services répressifs et judiciaires sont également vulnérables aux attaques menées par l'intermédiaire de l'IA contre les systèmes d'information et à la technique de l'empoisonnement de données, laquelle consiste à inclure une série de données erronées pour fausser les résultats; que, dans ces situations, les dommages qui en résultent sont potentiellement encore plus importants et peuvent entraîner un préjudice exponentiel pour les individus comme pour les groupes;

Q. considérant que le déploiement de l'IA dans les domaines répressif et judiciaire ne devrait pas être réduit à la simple question de la faisabilité technique, mais être davantage considéré comme une décision politique concernant la conception et les objectifs des systèmes répressifs et de justice pénale; que le droit pénal moderne repose sur l'idée que les autorités réagissent à une infraction après qu'elle a été commise, sans partir du principe que tous les citoyens sont dangereux et doivent être constamment surveillés afin de prévenir les actes répréhensibles potentiels; que les techniques de surveillance fondées sur l'IA remettent profondément en question ce raisonnement et qu'il est donc urgent que les législateurs du monde entier évaluent de manière approfondie les conséquences de l'autorisation de déploiement de technologies qui réduisent le rôle des êtres humains dans l'application des lois et les décisions de justice;

1. rappelle que, étant donné que le traitement de grandes quantités de données est au cœur de l'IA, le droit à la protection de la vie privée et le droit à la protection des données à caractère personnel s'appliquent à tous les domaines de l'IA et que le cadre juridique de l'Union en matière de protection des données et de la vie privée doit être pleinement respecté; rappelle donc que l'Union a déjà établi des normes de protection des données pour les services répressifs, qui constituent un fondement pour toute future réglementation en matière d'IA aux fins d'une utilisation par les services répressifs et judiciaires; rappelle que le traitement des données à caractère personnel devrait être licite et loyal, que les finalités du traitement devraient être déterminées, explicites et légitimes, que le traitement devrait être adéquat, pertinent et non excessif au regard des finalités pour lesquelles les données sont traitées, qu'il devrait être exact et mis à jour et que les données inexactes devraient être rectifiées ou effacées, sauf si des restrictions s'appliquent, que les données ne devraient pas être conservées plus longtemps que nécessaire, que des délais clairs et appropriés devraient être fixés pour l'effacement et pour un réexamen périodique de la nécessité de stocker ces données, et que celles-ci devraient être traitées de façon sécurisée; souligne également qu'il convient d'empêcher l'identification éventuelle de personnes par une application d'IA utilisant des données précédemment anonymisées;

2. réaffirme que toutes les solutions d'IA à des fins répressives et judiciaires doivent également respecter pleinement les principes de non-discrimination, de liberté de circulation, de présomption d'innocence et de droits de la défense, y compris le droit au silence, de liberté d'expression et d'information, de liberté de réunion et d'association, d'égalité devant la loi, d'égalité des armes et de droit à un recours effectif et à un procès équitable, conformément à la charte et à la convention européenne des droits de l'homme; souligne que toute utilisation de l'IA incompatible avec les droits fondamentaux doit être interdite;

3. reconnaît que la vitesse à laquelle les applications d'IA sont développées dans le monde ne permet pas de dresser une liste exhaustive des applications et impose donc d'adopter un modèle de gouvernance clair et cohérent garantissant à la fois les droits fondamentaux des personnes et la clarté juridique pour les développeurs, compte tenu de l'évolution constante de la technologie; estime toutefois, compte tenu du rôle et de la responsabilité des autorités policières et judiciaires et de l'impact de leurs décisions prises 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, que l'utilisation des applications d'IA doit être classée comme à haut risque lorsqu'elle est susceptible d'avoir une incidence significative sur la vie des personnes;

4. estime à cet égard que tous les outils d'IA développés ou utilisés par les services répressifs ou judiciaires devraient, au minimum, être sûrs, solides, sécurisés et adaptés à l'usage prévu, respecter les principes d'équité, de minimisation des données, de responsabilité, de transparence, de non-discrimination et d'explicabilité, et que leur développement, déploiement et utilisation devraient être soumis à une évaluation des risques et à un contrôle strict de la nécessité et de la proportionnalité, les garanties devant être proportionnées aux risques repérés; souligne que la confiance des citoyens dans l'utilisation de l'IA développée, déployée et utilisée dans l'Union est subordonnée au plein respect de ces critères;

5. reconnaît la contribution positive de certains types d'applications d'IA au travail des autorités répressives et judiciaires dans toute l'Union; souligne, à titre d'exemple, l'amélioration de la gestion de la jurisprudence grâce à des outils offrant des options de recherche supplémentaires; estime que de nombreuses autres possibilités d'utilisation de l'IA par les services

répressifs et judiciaires pourraient être explorées, tout en prenant en considération les cinq principes de la charte éthique d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, adoptée par la Commission européenne pour l'efficacité de la justice (CEPEJ), et en accordant une attention particulière aux «utilisations à envisager avec les plus extrêmes réserves», signalées par la CEPEJ;

6. souligne que toute technologie peut être détournée, et demande dès lors un contrôle démocratique strict et une surveillance indépendante de toute technologie fondée sur l'IA utilisée par les autorités répressives et judiciaires, en particulier celles pouvant être détournées à des fins de surveillance de masse ou de profilage de masse; constate donc avec une vive inquiétude le potentiel de certaines technologies d'IA utilisées dans le secteur répressif à des fins de surveillance de masse; souligne l'obligation légale de prévenir la surveillance de masse au moyen de technologies d'IA, qui par définition ne respectent pas les principes de nécessité et de proportionnalité, et d'interdire l'utilisation d'applications qui pourraient y conduire;

7. souligne que l'approche adoptée dans certains pays tiers en ce qui concerne le développement, le déploiement et l'utilisation de technologies de surveillance de masse empiète de manière disproportionnée sur les droits fondamentaux et qu'elle ne devrait donc pas être suivie par l'Union; souligne dès lors que les garanties contre l'utilisation abusive des technologies d'IA par les autorités répressives et judiciaires doivent également être réglementées de manière uniforme dans toute l'Union;

8. met en évidence le potentiel de parti pris et de discrimination découlant de l'utilisation des applications d'IA, telles que l'apprentissage automatique, y compris des algorithmes sur lesquels reposent ces applications; note que des biais peuvent être inhérents à des séries de données sous-jacentes, en particulier lorsque des données historiques sont utilisées, ou peuvent être introduits par les concepteurs des algorithmes ou générés lorsque les systèmes sont mis en œuvre dans des conditions réelles; fait observer que les résultats produits par les applications d'IA sont nécessairement influencés par la qualité des données utilisées, et que ces biais inhérents ont tendance à se renforcer progressivement et ainsi à perpétuer et amplifier les discriminations existantes, en particulier pour les personnes appartenant à certains groupes ethniques ou à certaines communautés racialisées;

9. souligne que de nombreuses technologies d'identification fondées sur des algorithmes qui sont utilisées aujourd'hui commettent un nombre disproportionné d'erreurs d'identification et de catégorisation et portent donc préjudice aux personnes racialisées, aux personnes appartenant à certaines communautés ethniques, aux personnes LGBTI, aux enfants et aux personnes âgées, ainsi qu'aux femmes; rappelle que les personnes ont non seulement le droit d'être correctement identifiées, mais également le droit de ne pas être identifiées du tout, sauf si la loi l'exige pour des raisons d'intérêt public impérieuses et légitimes; souligne que les prédictions de l'IA fondées sur les caractéristiques d'un groupe particulier de personnes finissent par amplifier et reproduire les formes existantes de discrimination; estime que des efforts importants devraient être déployés pour éviter les discriminations automatisées et les biais d'automatisation; demande de solides garanties supplémentaires lorsque les services répressifs ou judiciaires utilisent les systèmes d'IA directement sur des mineurs ou pour des tâches en lien avec des mineurs;

10. met en exergue l'asymétrie de pouvoir entre ceux qui utilisent les technologies d'IA et ceux qui sont soumis à leur traitement; souligne qu'il est impératif que l'utilisation des outils d'IA par les autorités répressives et judiciaires ne devienne pas un facteur d'inégalité, de fracture sociale ou d'exclusion; met en évidence l'impact de l'utilisation des outils d'IA sur les droits de la défense des suspects, la difficulté d'obtenir des informations utiles sur leur fonctionnement et, partant, la difficulté de saisir la justice pour contester leurs résultats, en particulier pour les personnes faisant l'objet d'une enquête;

11. prend note des risques liés, en particulier, aux fuites de données, aux atteintes à la sécurité des données et à l'accès non autorisé aux données à caractère personnel et à d'autres informations liées, par exemple, aux enquêtes pénales ou aux affaires judiciaires traitées par des systèmes d'IA; souligne que les aspects liés à la sécurité et à la sûreté des systèmes d'IA utilisés par les services répressifs et judiciaires doivent être soigneusement examinés et suffisamment solides et résilients pour prévenir les conséquences potentiellement catastrophiques d'attaques malveillantes contre les systèmes d'IA; met l'accent sur l'importance de la sécurité dès la conception, ainsi que d'une surveillance humaine spécifique avant l'utilisation de certaines applications critiques, et demande dès lors que les autorités répressives et judiciaires n'utilisent que les applications d'IA qui respectent le principe de la protection de la vie privée et des données dès la conception de manière à éviter tout détournement d'usage;

12. souligne qu'aucun système d'IA utilisé par les services répressifs ou judiciaires ne devrait pouvoir porter atteinte à l'intégrité physique d'êtres humains ni octroyer des droits ou imposer des obligations légales aux personnes;

13. reconnaît qu'il est difficile d'établir correctement la responsabilité juridique des dommages potentiels, compte tenu de la complexité du processus de développement et de fonctionnement des systèmes d'IA; estime qu'il est nécessaire de créer un régime clair et équitable pour l'attribution de la responsabilité juridique des conséquences négatives potentielles de ces

technologies numériques avancées; souligne, toutefois, que l'objectif doit être, avant tout, d'éviter que de telles conséquences ne se produisent effectivement; appelle, par conséquent, au respect du principe de précaution dans toutes les applications d'IA dans le cadre répressif; souligne que la responsabilité juridique doit in fine incomber à une personne physique ou morale, qui doit toujours être identifiée en cas de décisions prises à l'aide de l'IA; souligne donc la nécessité de garantir la transparence des structures des sociétés qui produisent et gèrent les systèmes d'IA;

14. estime qu'il est essentiel, tant pour l'efficacité de l'exercice des droits de la défense que pour la transparence des systèmes nationaux de justice pénale, qu'un cadre juridique spécifique, clair et précis réglemente les conditions, les modalités et les conséquences de l'utilisation d'outils d'IA dans les domaines répressif et judiciaire, ainsi que les droits des personnes visées et des procédures de réclamation et de recours efficaces et faciles d'accès, y compris des voies de recours judiciaires; souligne que les parties à une procédure pénale ont le droit d'accéder au processus de collecte des données et aux évaluations y afférentes effectuées par des applications d'IA ou obtenues par l'utilisation de telles applications; souligne que, lorsqu'elles statuent sur une demande d'extradition (ou de remise) vers un autre État membre ou un pays tiers, les autorités d'exécution engagées dans la coopération judiciaire doivent évaluer si l'utilisation d'outils d'IA dans le pays requérant pourrait manifestement compromettre le droit fondamental à accéder à un tribunal impartial; invite la Commission à publier des lignes directrices sur la manière de mener une telle évaluation dans le cadre de la coopération judiciaire en matière pénale; demande avec insistance que les États membres, conformément à la législation applicable, veillent à ce que les personnes soient informées lorsqu'elles font l'objet d'applications d'IA utilisées par les autorités répressives ou judiciaires;

15. fait remarquer que si les êtres humains ne se fient qu'aux données, profils et recommandations générés par les machines, ils ne seront pas en mesure de mener une étude indépendante; attire l'attention sur les conséquences négatives potentiellement graves, en particulier dans le domaine de l'application des lois et de la justice, d'une trop grande confiance dans la nature en apparence objective et scientifique des outils d'IA, qui fait que les personnes n'envisagent pas la possibilité que leurs résultats soient incorrects, incomplets, dépourvus de pertinence ou discriminatoires; souligne qu'il y a lieu d'éviter d'accorder une confiance démesurée aux résultats fournis par les systèmes d'IA, et souligne que les autorités doivent renforcer leur confiance et leur connaissance pour pouvoir remettre en question ou ignorer une recommandation algorithmique; considère qu'il est important d'avoir des attentes réalistes à l'égard de ces solutions technologiques et de ne pas promettre des solutions parfaites en matière d'application des lois ni la détection de toutes les infractions commises;

16. souligne que, dans les cadres judiciaires et répressifs, les décisions produisant des effets juridiques ou similaires doivent toujours être prises par un être humain, qui peut être tenu responsable des décisions prises; estime que les personnes soumises à des systèmes alimentés par l'IA doivent disposer de voies de recours; rappelle que, dans le cadre du droit de l'Union, une personne a le droit de ne pas faire l'objet d'une décision produisant des effets juridiques la concernant, ou l'affectant de manière significative, et fondée exclusivement sur un traitement automatisé des données; souligne en outre que la prise de décision individuelle automatisée ne saurait être fondée sur des catégories particulières de données à caractère personnel, à moins que des mesures appropriées pour la sauvegarde des droits et des libertés ainsi que des intérêts légitimes de la personne concernée ne soient en place; souligne que le droit de l'Union interdit tout profilage induisant une discrimination à l'encontre de personnes physiques sur la base de catégories particulières de données à caractère personnel; souligne que les décisions dans le domaine répressif ont presque toujours un effet juridique sur la personne concernée, en raison de la nature exécutive des autorités répressives et de leurs activités; observe que l'utilisation de l'IA peut influencer les décisions humaines et avoir une incidence sur toutes les étapes de la procédure pénale; estime dès lors que les autorités qui recourent aux systèmes d'IA doivent respecter des normes juridiques extrêmement élevées et garantir une intervention humaine, en particulier lors de l'analyse des données provenant de ces systèmes; exige par conséquent que l'appréciation souveraine des juges et la prise de décision au cas par cas soient maintenues; appelle de ses vœux l'interdiction de l'utilisation des technologies d'IA et des technologies connexes pour proposer des décisions judiciaires;

17. préconise l'explicabilité, la transparence, la traçabilité et la vérification des algorithmes, en tant qu'éléments indispensables de la surveillance, afin de garantir que le développement, le déploiement et l'utilisation des systèmes d'IA pour les services judiciaires et répressifs respectent les droits fondamentaux et bénéficient de la confiance des citoyens, ainsi que pour garantir que les résultats produits par les algorithmes d'IA puissent être rendus intelligibles pour les utilisateurs et les personnes soumises à ces systèmes, et que la transparence soit effective quant aux données sources et à la manière dont le système est parvenu à une conclusion donnée; fait observer que, afin de garantir la transparence technique, la solidité et la précision, seuls les outils et systèmes dont les algorithmes et la logique sont contrôlables et accessibles au moins aux autorités répressives et judiciaires, ainsi qu'aux contrôleurs indépendants, devraient être achetés par les autorités répressives et judiciaires de l'Union, de manière qu'ils puissent être évalués, contrôlés et vérifiés, et souligne qu'ils ne peuvent être fermés ou présentés comme faisant l'objet d'un droit de propriété par les fabricants; observe en outre qu'il y a lieu de fournir une documentation rédigée dans un langage clair et compréhensible traitant de la nature du service, des outils développés, des performances, des conditions de fonctionnement prévues et des risques potentiels; demande dès lors aux autorités

judiciaires et répressives d'assurer une transparence proactive et totale sur les entreprises privées qui leur fournissent des systèmes d'IA à des fins répressives et judiciaires; recommande dès lors l'utilisation de logiciels libres dans la mesure du possible;

18. encourage les autorités répressives et judiciaires à cerner et évaluer les domaines dans lesquels certaines solutions d'IA sur mesure pourraient être bénéfiques et à échanger les bonnes pratiques en matière de déploiement de l'IA; demande aux États membres et aux agences de l'Union d'adopter des procédures de passation de marchés publics appropriées pour les systèmes d'IA, lorsque ceux-ci sont utilisés dans un cadre répressif ou judiciaire, de manière à garantir leur conformité avec les droits fondamentaux et la législation applicable, en veillant également à ce que la documentation sur les logiciels et les algorithmes soient disponibles et accessibles pour examen par les autorités compétentes et de contrôle; demande, en particulier, des règles contraignantes exigeant la publication d'informations sur les partenariats public-privé, les contrats et les acquisitions, ainsi que sur la finalité pour laquelle ces outils sont acquis; souligne qu'il est nécessaire de fournir aux autorités les fonds nécessaires ainsi que de les doter des compétences spécialisées indispensables pour garantir le plein respect des exigences éthiques, juridiques et techniques liées au déploiement de l'IA;

19. demande que les systèmes d'IA et les processus décisionnels fassent l'objet d'une traçabilité qui, à travers une documentation obligatoire, expose leurs fonctions, définisse les capacités et les limites des systèmes et permette de retrouver l'origine des éléments déterminants d'une décision; souligne qu'il importe de conserver l'ensemble de la documentation sur les données d'entraînement, leurs contexte, finalité, exactitude et conséquences indirectes, ainsi que leur traitement de la part des créateurs et des concepteurs des algorithmes et leur conformité avec les droits fondamentaux; estime qu'il doit toujours être possible de traduire les calculs d'un système d'intelligence artificielle dans une forme compréhensible pour l'être humain;

20. demande qu'une étude d'impact obligatoire sur les droits fondamentaux soit réalisée avant la mise en œuvre ou le déploiement de tout système d'IA à des fins répressives ou judiciaires, afin d'évaluer tout risque potentiel pour les droits fondamentaux; rappelle que l'analyse d'impact préalable relative à la protection des données est obligatoire pour tout type de traitement (en particulier les traitements faisant appel aux nouvelles technologies) susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, et est d'avis que la plupart des technologies d'IA utilisées dans les domaines répressif et judiciaire sont concernées; souligne les connaissances approfondies des autorités de protection des données et des agences des droits fondamentaux pour ce qui est d'évaluer ces systèmes; insiste sur le fait que ces analyses d'impact relatives aux droits fondamentaux devraient être menées aussi ouvertement que possible et avec la participation active de la société civile; demande instamment que les analyses d'impact définissent également clairement les garanties nécessaires pour faire face aux risques décelés et qu'elles soient rendues publiques, dans toute la mesure du possible, avant le déploiement de tout système d'IA;

21. souligne que seule une gouvernance européenne solide en matière d'IA, assortie d'une évaluation indépendante, peut permettre la mise en œuvre nécessaire des principes des droits fondamentaux; demande qu'une autorité indépendante effectue un audit périodique et obligatoire de tous les systèmes d'IA utilisés par les services répressifs et judiciaires lorsque ces systèmes sont susceptibles d'avoir une incidence significative sur la vie des personnes, pour tester et évaluer les systèmes algorithmiques, le contexte, l'objectif, la précision, les performances et l'échelle de ceux-ci, et, une fois qu'ils sont en service, afin de détecter, d'examiner, de diagnostiquer et de rectifier les éventuels effets indésirables et préjudiciables, et de veiller à ce que les systèmes d'IA fonctionnent comme prévu; appelle donc de ses vœux un cadre institutionnel clair à cet effet, comprenant une surveillance réglementaire et prudentielle, pour assurer une mise en œuvre intégrale et garantir un débat démocratique pleinement éclairé sur la nécessité et la proportionnalité de l'IA dans le domaine de la justice pénale; souligne que les résultats de ces audits devraient être communiqués dans des registres publics afin que les citoyens sachent si des systèmes d'IA sont déployés et quelles mesures sont prises pour remédier aux violations des droits fondamentaux;

22. souligne que les séries de données et les systèmes algorithmiques utilisés dans les classifications, les évaluations et les prédictions aux différentes étapes du traitement des données dans le cadre du développement de l'IA et des technologies connexes peuvent également entraîner un traitement différencié et une discrimination tant directe qu'indirecte à l'encontre de groupes de personnes, en particulier étant donné que les données utilisées pour entraîner les algorithmes de police prédictive témoignent des priorités de surveillance actuelles et, par conséquent, peuvent finir par reproduire et amplifier les biais habituels; souligne dès lors que les technologies d'IA, en particulier lorsqu'elles sont déployées à des fins répressives et judiciaires, nécessitent une recherche et une contribution interdisciplinaires, notamment dans le domaine de la science et des technologies, des études critiques de la race, des études sur le handicap et d'autres disciplines attentives au contexte social, y compris en ce qui concerne le mode de fonctionnement des processus de différenciation et de classification et leurs conséquences; souligne dès lors la nécessité d'investir systématiquement dans l'intégration, à tous les niveaux, de ces disciplines dans les études et les recherches sur l'IA; souligne également qu'il est important que les équipes qui conçoivent, mettent au point, testent, entretiennent, déploient ou achètent ces systèmes d'IA à des fins répressives et judiciaires reflètent, dans la mesure du possible, la diversité de la société en général, en tant que moyen non technique de réduire les risques de discrimination;

23. souligne en outre que pour que les responsabilités et obligations soient adéquates, il est nécessaire d'assurer une formation spécialisée considérable sur les dispositions éthiques, les dangers potentiels, les limites et la bonne utilisation des technologies d'IA, en particulier pour le personnel policier et judiciaire; insiste sur le fait qu'il convient de veiller à ce que les décideurs bénéficient de formations professionnelles adaptées et des qualifications nécessaires quant aux risques de biais, car les ensembles de données peuvent contenir des données discriminatoires et reposant sur des préjugés; soutient la mise en place d'initiatives de sensibilisation et d'éducation pour veiller à ce que les personnes travaillant au sein des services répressifs ou judiciaires connaissent et comprennent les limites, les capacités et les risques relatifs à l'utilisation des systèmes d'IA, y compris le risque de biais d'automatisation; rappelle que l'inclusion, dans les séries de données d'entraînement de l'IA, d'exemples du racisme des forces de police dans l'exercice de leurs fonctions entraînera inévitablement un biais raciste dans les conclusions, notes et recommandations générées par l'IA; appelle donc de nouveau les États membres à promouvoir des politiques antidiscriminatoires et à élaborer des plans d'action nationaux contre le racisme dans le domaine de la police et de la justice;

24. note que la police prédictive fait partie des applications d'IA utilisées dans le domaine répressif, mais attire l'attention sur le fait que, si elle permet d'analyser des séries de données en vue de l'identification de modèles et corrélations, elle ne peut répondre à la question de la causalité et prédire de manière fiable le comportement des personnes, et ne peut donc pas constituer à elle seule une base d'intervention; souligne que plusieurs villes des États-Unis ont cessé d'utiliser leurs systèmes de police prédictive à la suite d'audits; rappelle que, lors de la mission de la commission LIBE aux États-Unis en février 2020, les services de police de New York et de Cambridge (Massachusetts) ont indiqué qu'ils avaient progressivement abandonné leurs programmes de police prédictive, en raison de leur manque d'efficacité, de leur effet discriminatoire et de leur échec dans la pratique, au profit de la police de proximité; observe que ce changement a entraîné une baisse du taux de criminalité; s'oppose dès lors à ce que les autorités répressives utilisent l'IA pour prédire le comportement de personnes ou de groupes en se fondant sur des données historiques et les comportements passés, l'appartenance à un groupe, la localisation ou toute autre caractéristique de ce type, en tentant ainsi d'identifier les personnes susceptibles de commettre une infraction;

25. prend note des différents types d'utilisation de la reconnaissance faciale, tels que, entre autres, la vérification/l'authentification (c'est-à-dire la comparaison du visage d'une personne avec une photo figurant sur un document d'identité, par exemple, frontières intelligentes), l'identification (c'est-à-dire la comparaison d'une photo avec les photos d'une base de données) et la détection (c'est-à-dire la détection de visages en temps réel de sources telles que des images de vidéosurveillance et la recherche de ceux-ci dans des bases de données, par exemple dans le cadre d'une surveillance en temps réel), chacune de ces utilisations ayant des implications différentes pour la protection des droits fondamentaux; est fermement convaincu que les services répressifs ne devraient déployer des systèmes de reconnaissance faciale qu'à des fins répressives clairement justifiées, dans le plein respect des principes de proportionnalité et de nécessité et du droit applicable; réaffirme que l'utilisation des technologies de reconnaissance faciale doit au moins se faire dans le respect des exigences de minimisation des données, d'exactitude des données, de limitation du stockage, de sécurité des données et du principe de responsabilité, tout en étant légale, équitable et transparente, et en poursuivant un objectif spécifique, explicite et légitime, clairement défini dans le droit des États membres ou de l'Union; est d'avis que les systèmes de vérification et d'authentification ne peuvent continuer à être déployés et utilisés avec succès que si leurs effets négatifs peuvent être atténués et les critères susmentionnés respectés;

26. demande en outre l'interdiction permanente de l'utilisation de l'analyse et/ou de la reconnaissance automatisées, dans les espaces accessibles au public, d'autres caractéristiques humaines telles que la démarche, les empreintes digitales, l'ADN, la voix et d'autres signaux biométriques et comportementaux;

27. demande toutefois un moratoire sur le déploiement des systèmes de reconnaissance faciale à des fins répressives destinés à l'identification, à moins qu'ils ne soient utilisés qu'aux fins de l'identification des victimes de la criminalité, jusqu'à ce que les normes techniques puissent être considérées comme pleinement respectueuses des droits fondamentaux, que les résultats obtenus ne soient ni biaisés, ni discriminatoires, que le cadre juridique offre des garanties strictes contre les utilisations abusives ainsi qu'un contrôle et une surveillance démocratiques rigoureux, et que la nécessité et la proportionnalité du déploiement de ces technologies soient prouvées de manière empirique; relève que lorsque les critères susmentionnés ne sont pas remplis, les systèmes ne devraient pas être utilisés ou déployés;

28. exprime sa vive inquiétude quant à l'utilisation, par les services répressifs et les services de renseignement, de bases de données privées de reconnaissance faciale, telles que Clearview AI, qui contient plus de trois milliards d'images collectées illégalement sur les réseaux sociaux et à d'autres endroits sur l'internet, y compris des images de citoyens de l'Union; invite les États membres à obliger les services répressifs à faire savoir s'ils utilisent la technologie de Clearview AI ou des technologies équivalentes d'autres fournisseurs; rappelle que le comité européen de la protection des données a estimé que l'utilisation d'un service comme celui-ci par les autorités répressives dans l'Union «ne serait probablement pas compatible avec le régime de protection des données de l'Union»; appelle de ses vœux l'interdiction de l'utilisation des bases de données privées de reconnaissance faciale dans le domaine répressif;

29. prend note de l'étude de faisabilité de la Commission sur les modifications possibles de la décision Prüm ([8]), y compris en ce qui concerne les images faciales; prend note des recherches qui ont été menées et selon lesquelles aucun nouveau moyen d'identification potentiel, par exemple l'iris ou la reconnaissance faciale, ne serait aussi fiable dans un contexte médico-légal que l'ADN ou les empreintes digitales; rappelle à la Commission que toute proposition législative doit être fondée sur des preuves et respecter le principe de proportionnalité; prie instamment la Commission de ne pas étendre le cadre de la décision Prüm sauf s'il existe des preuves scientifiques étayées de la fiabilité de la reconnaissance faciale dans un contexte médico-légal par rapport à l'ADN ou aux empreintes digitales, après avoir effectué une étude d'impact complète et pris en considération les recommandations du contrôleur européen de la protection des données et du comité européen de la protection des données;

30. souligne que l'utilisation des données biométriques se rapporte plus généralement au principe du droit à la dignité humaine, fondement de tous les droits fondamentaux garantis par la charte; considère que l'utilisation et la collecte de toute donnée biométrique à des fins d'identification à distance, par exemple lors d'une opération de reconnaissance faciale dans des lieux publics ou aux portiques de contrôle automatisé des passeports destinés aux vérifications aux frontières dans les aéroports, peuvent présenter des risques particuliers pour les droits fondamentaux, dont les implications peuvent varier considérablement en fonction de la finalité, du contexte et du champ d'utilisation; souligne en outre que la validité scientifique des technologies de reconnaissance des affects, telles que les caméras qui détectent les mouvements oculaires et les changements de la taille des pupilles, dans le cadre répressif est contestée; est d'avis que l'utilisation de l'identification biométrique dans le cadre répressif et judiciaire devrait toujours être considérée comme «à haut risque» et donc soumise à des exigences supplémentaires, conformément aux recommandations du groupe d'experts de haut niveau de la Commission sur l'IA;

31. manifeste sa vive inquiétude quant aux projets de recherche financés dans le cadre d'Horizon 2020 qui déploient l'intelligence artificielle aux frontières extérieures, tels que le projet iBorderCtrl, un «système intelligent de détection de mensonges» qui a été testé en Hongrie, en Lettonie et en Grèce, et qui établit le profil des voyageurs sur la base d'un entretien automatisé réalisé par webcam avant le voyage et d'une analyse de 38 micro-gestes fondée sur l'intelligence artificielle; invite donc la Commission à mettre en œuvre, par des moyens législatifs et non législatifs et, au besoin, par le biais de procédures d'infraction, l'interdiction de tout traitement des données biométriques, y compris des images faciales, à des fins répressives conduisant à une surveillance de masse dans les espaces accessibles au public; invite en outre la Commission à mettre un terme au financement de la recherche ou du déploiement de données biométriques ou de programmes susceptibles de donner lieu à une surveillance de masse dans les espaces publics; souligne, dans ce contexte, qu'il y a lieu d'accorder une attention particulière et d'appliquer un cadre strict à l'utilisation de drones dans les opérations de police;

32. soutient les recommandations du groupe d'experts de haut niveau de la Commission sur l'IA en faveur d'une interdiction de la notation à grande échelle des individus au moyen de l'IA; considère que toute forme de notation normative des citoyens à grande échelle par les autorités publiques, en particulier dans les domaines répressif et judiciaire, entraîne une perte d'autonomie, menace le principe de non-discrimination et ne peut être considérée comme conforme aux droits fondamentaux, en particulier à la dignité humaine, tels qu'énoncés dans le droit de l'Union;

33. demande une plus grande transparence de façon générale pour permettre une compréhension complète de l'utilisation des applications d'IA dans l'Union; demande aux États membres de présenter des informations complètes sur les outils dont se servent leurs autorités répressives et judiciaires, les types d'outils utilisés, les fins auxquelles ils sont utilisés et les types de criminalité auxquels ils s'appliquent et de transmettre les noms des entreprises ou organisations qui ont développé lesdits outils; invite les autorités répressives et judiciaires à informer également le grand public et à assurer une transparence suffisante quant à leur utilisation de l'IA et des technologies connexes dans l'exercice de leurs pouvoirs, y compris en communiquant les taux de faux positifs et de faux négatifs de la technologie en question; demande à la Commission de collecter et de mettre à jour les informations en un seul endroit; invite la Commission à publier et à mettre à jour également des informations sur l'utilisation de l'IA par les agences de l'Union chargées de missions répressives et judiciaires; invite le comité européen de la protection des données à évaluer la légalité de ces technologies et applications d'IA utilisées par les autorités répressives et judiciaires;

34. rappelle que les applications d'IA, y compris celles utilisées dans le cadre répressif et judiciaire, sont développées à un rythme rapide dans le monde entier; prie instamment toutes les parties prenantes européennes, y compris les États membres et la Commission, à assurer, au moyen de la coopération internationale, la participation des partenaires extérieurs à l'Union afin de relever les normes au niveau international et de trouver un cadre juridique et éthique commun et complémentaire pour l'utilisation de l'IA, en particulier pour les services répressifs et judiciaires, qui respecte pleinement la charte, l'acquis européen en matière de protection des données et, plus largement, les droits de l'homme;

([8]) Décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (JO L 210 du 6.8.2008, p. 1).

35. demande à l'Agence des droits fondamentaux de l'Union d'élaborer, en collaboration avec le comité européen de la protection des données et le contrôleur européen de la protection des données, des lignes directrices détaillées, des recommandations et des bonnes pratiques afin de préciser les critères et conditions pour le développement, l'utilisation et le déploiement des applications et des solutions d'IA destinées aux autorités répressives et judiciaires; s'engage à effectuer une étude sur la mise en œuvre de la directive en matière de protection des données dans le domaine répressif ([9]) en vue de déterminer comment la protection des données à caractère personnel a été assurée dans les activités de traitement menées par les autorités répressives et judiciaires, en particulier lors du développement ou du déploiement de nouvelles technologies; invite en outre la Commission à examiner s'il est nécessaire d'adopter des mesures législatives spécifiques pour préciser les critères et conditions pour le développement, l'utilisation et le déploiement d'applications et de solutions d'IA par les autorités répressives et judiciaires;

36. charge son Président de transmettre la présente résolution au Conseil et à la Commission.

([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).