Strasbourg, 7 novembre 2019

T-PD(2019)07BISrev

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL

CONVENTION 108

Profilage et la Convention 108+ : Pistes pour une actualisation

DG I – Droits de l'Homme et État de droit

Note liminaire :

Les auteurs du rapport (Profilage et la Convention 108+ : Rapport sur l'évolution de la situation après l'adoption de la Recommandation(2010)13 sur le profilage), partant de la structure de la Recommandation sur le profilage (adoptée par le Comité des Ministres le 23 novembre 2010), proposent dans le présent document les modifications et ajouts qu'ils considèrent nécessaires au maintien de la pertinence de la recommandation de 2010, au vu de l'évolution technologique, des usages qui en sont fait et des nouveaux textes normatifs de référence.

1. Définitions

1.1. Aux fins [de la présente Recommandation] :

a. L'expression « données à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable (« personne concernée »). Une personne physique n'est pas considérée comme « identifiable » si cette identification nécessite des délais ou des activités déraisonnables au regard des moyens dont dispose le responsable du traitement.
b. L'expression « catégories de données traitées », signifie les différents types de données à caractère personnel ou non, utilisées lors du traitement de profilage, peu importe leurs sources et leurs natures.
c. L'expression « données sensibles » désigne les données à caractère personnel énumérées à l'article 6 de la Convention 108+.
d. Les expressions « traitement », « responsable du traitement » et « sous-traitant » se réfèrent aux définitions données par la Convention 108+ dans son article 2.
e. Le terme « profilage » désigne « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique*. »
f. Le terme « profil » désigne *« un ensemble de données qui caractérise une catégorie d'individus et qui est destiné à être appliqué à un individu* »
g. Le terme « modèle » est une abstraction mathématique utilisée dans les méthodes d'apprentissage automatique, qui fournit une description simplifiée des données pour résoudre la tâche à effectuer.
h. Le terme « intelligence artificielle » (IA) désigne tout « *Ensemble de sciences, théories et techniques dont le but est de reproduire par une machine des capacités cognitives d'un être humain. Les développements actuels visent, par exemple, à pouvoir confier à une machine des tâches complexes auparavant déléguées à un humain*. »
i. L'expression « traitement utilisant des procédés d'apprentissage automatique » (*machine learning*), signifie un traitement utilisant des méthodes particulières d'intelligence artificielle qui se fonde sur des approches statistiques pour donner

aux ordinateurs la capacité d' « apprendre » à partir de données, c'est-à-dire d'améliorer leurs performances à résoudre des tâches sans être explicitement programmés pour chacune.

j. L'expression « apprentissage profond » (*deep learning*) signifie un ensemble de méthodes d'apprentissage automatique tentant de modéliser avec un haut niveau d'abstraction des données grâce à des architectures articulées de différentes transformations non linéaires.

k. Le terme « mégadonnées » (*big data)* désigne des ensembles de données extrêmement volumineux et hétérogènes, qui peuvent être analysés par ordinateur en vue d'en extraire des inférences statistiques sur les schémas, les tendances et les corrélations de données.

l. Le terme « services d'intermédiation en ligne » : les services de la société de l'information qui permettent aux utilisateurs soit d'offrir des informations (services de recherche en ligne), des biens ou des services, soit d'entrer en relation (service d'accès à des réseaux sociaux).

m. Le terme « traitements de profilage à risque élevé », désigne :
    i. les traitements de profilage dont le fonctionnement entraîne des effets juridiques ou ont un impact significatif pour la personne concernée ou pour le groupe de personnes identifié par le traitement de profilage ;
    ii. les traitements de profilage qui, en raison du public visé et du contexte, entraînent un risque de manipulation des personnes concernées ;
    iii. les traitements de profilage ayant pour objet des données relevant des catégories particulières de données ou ayant pour finalité de les détecter ou les prédire ;
    iv. les traitements de profilage opérés par des services d'information en ligne disposant d'une large part du marché, sur base de l'utilisation de leurs services.

2. Principes généraux

2.1. Le respect des libertés et des droits fondamentaux, et notamment du droit à la vie privée et du principe de non-discrimination mais également des impératifs de justice sociale, de diversité culturelle et de démocratie, doit être garanti lors de la collecte et du traitement de profilage visés par la présente recommandation. Les traitements de profilage doivent contribuer tant au bien-être des individus qu'au développement d'une société inclusive, démocratique et durable.

2.2. Les Etats membres encouragent l'élaboration et la mise en œuvre de procédures et de systèmes respectant la protection de la vie privée et des données, dès la phase de planification (*privacy by design*), notamment grâce à l'utilisation de technologies renforçant la protection de la vie privée. Ils devraient également prendre des mesures appropriées contre le développement et l'utilisation de technologies qui visent, totalement ou partiellement, au contournement illicite des mesures techniques de protection de la vie privée.

2.3. Conformément au 4ème alinéa du préambule de la Convention 108+ : «Rappelant que le droit à la protection des données à caractère personnel est à considérer au regard de son rôle dans la société et qu'il est à concilier avec d'autres droits de l'homme et libertés fondamentales, …», les traitements de profilage ne peuvent engendrer des discriminations tant vis-à-vis de personnes que vis-à-vis de groupes ou collectivités. Ils ne peuvent porter atteinte ni à la dignité des personnes ni à la démocratie

2.4. Les traitements de profilage ne peuvent avoir pour but la manipulation des personnes concernées vulnérables.

2.5. L'utilisation de systèmes automatisés de prise de décision devrait préserver l'autonomie de l'intervention humaine dans le processus décisionnel.

2.6. Dans toute la mesure du possible, les prestataires de services et, en particulier, les services intermédiaires devraient offrir aux personnes concernées utilisatrices le choix entre le profilage ou l'absence de profilage, voire entre différents degrés de profilage en fonction de la finalité des traitements proposés.

2.7. Les États membres devraient veiller à maintenir la réglementation des traitements de profilage proportionnée aux finalités poursuivies par ceux-ci, à la nature et à la gravité des risques encourus par les personnes concernées, les groupes visés ou l'intérêt général.

2.8. Les traitements de profilage mettent en jeu différents acteurs dont il importe d'analyser la qualité et le rôle afin de déterminer leurs responsabilités.

2.9. L'utilisation des technologies d'intelligence artificielle dites d'apprentissage profond à des fins de profilage constitue un risque supplémentaire par la présence possible d'erreurs, de biais et la difficulté de rendre transparentes les justifications des décisions prises ou proposées et donc le plein exercice des droits des personnes concernées. Leur conception, leur élaboration et leur mise en œuvre exige une attention particulière et continue au regard des risques créés et leur évaluation par des équipes pluridisciplinaires, indépendantes.

3. Conditions régissant la collecte et le traitement de données à caractère personnel dans le cadre du profilage

A. Licéité

3.1. La collecte et le traitement des données à caractère personnel dans le cadre du profilage devraient être loyaux, licites et proportionnés, et devraient poursuivre des finalités déterminées et légitimes.

3.2. Les données à caractère personnel utilisées dans le cadre du profilage devraient être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont collectées ou seront traitées.

Cette disposition méritera un commentaire dans la mesure où, dans les systèmes de '*machine learning*' il est difficile de connaître *a priori,* les données qui permettront les corrélations significatives et que, par ailleurs, il est important de limiter le traitement de profilage à des catégories de données dont la personne concernée peut raisonnablement s'attendre à ce qu'elles soient prises en considération au vu des finalités légitimes du profilage (exemple : le profilage pour les priorités en matière d'accès au logement qui prendrait en compte la consommation de films sentimentaux sur une plateforme de films en ligne).

3.3. Les données à caractère personnel utilisées dans le cadre du profilage ne devraient être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

3.4. Sauf ce qui pourrait être dit plus loin, la collecte et le traitement de données à caractère personnel dans le cadre du profilage ne peuvent être effectués que :

a. si la loi le prévoit ; ou
b. si la loi l'autorise et :
   - si la personne concernée ou son représentant légal a donné son consentement libre, spécifique et éclairé ;
   - si le profilage est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'application de mesures précontractuelles prises à la demande de celle-ci ;
   - si le profilage est nécessaire à l'exécution d'une tâche d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données personnelles sont communiquées ;
   - si le profilage est nécessaire à la réalisation de l'intérêt légitime du responsable du traitement ou du/des tiers au(x)quel(s) les données sont communiquées, à condition que ne prévalent pas les libertés et droits fondamentaux de la personne concernée ;
   - si le profilage est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée.

3.5. La collecte et le traitement dans le cadre du profilage des données à caractère personnel des personnes qui ne peuvent pas exprimer seules leur consentement libre, spécifique et éclairé devraient être interdits à moins que cela soit dans l'intérêt légitime de la personne concernée ou pour un intérêt public prépondérant, et à condition que des garanties appropriées soient prévues par une loi.

3.6. Afin qu'il soit libre, le consentement suppose, pour la personne concernée, la possibilité d'un choix informé. Dans toute la mesure du possible, les prestataires de services et les plateformes devraient offrir différents services plus ou moins profilés voire non profilé en fonction du service offert, afin de garantir le choix de la personne concernée en ce qui concerne l'intensité du profilage. Le consentement au traitement de profilage ne peut être exigé comme condition de l'exécution d'une prestation. Quand le consentement est requis, il incombe au responsable du traitement de prouver que la personne concernée a accepté explicitement le traitement de profilage au-delà de ce qui était nécessaire à l'exécution de la prestation et après avoir été informée conformément au chapitre 4.

3.7. Dans la mesure du possible et à moins que le service requis nécessite de connaître l'identité de la personne concernée, toute personne devrait avoir accès aux informations relatives à un bien ou à un service ou avoir accès à ce bien ou à ce service sans devoir communiquer de données à caractère personnel au fournisseur du bien ou au prestataire du service.

3.8. La diffusion et l'utilisation, à l'insu des personnes concernées, de logiciels visant à l'observation ou à la surveillance dans le cadre du profilage de l'usage d'un terminal donné ou de réseaux de communications électroniques ne devraient être autorisées que si elles sont expressément prévues par le droit interne et assorties de garanties appropriées.

B. Qualité des données et des algorithmes

3.9. Le ou les responsables du traitement devraient prendre des mesures appropriées pour corriger les facteurs d'inexactitude des données et limiter les risques d'erreurs et de biais inhérents au profilage.

3.10. Le ou les responsables du traitement et le cas échéant les sous-traitants devraient réévaluer périodiquement et, dans un délai raisonnable, la qualité des données et des inférences statistiques utilisées.

3.11. Lorsqu'il(s) acquier(en)t des données ou des algorithmes d'un tiers, le ou les responsables du traitement veillera(ont) à obtenir de ce tiers la documentation nécessaire à la vérification de la qualité des données et des algorithmes et de leur adéquation à la finalité poursuivie par le traitement.

3.12. Lorsque le traitement de profilage est un traitement à risque élevé, le ou les responsables devrai(en)t mettre à la disposition de l'autorité de contrôle les mesures de contrôle et de correction prises.

C. Catégories particulières de données

3.13. La collecte et le traitement de données sensibles dans le cadre du profilage sont interdits sauf si ces données sont nécessaires pour les finalités légitimes et spécifiques du traitement et pour autant que le droit interne prévoit des garanties appropriées. Lorsque le traitement de profilage porte sur des données sensibles, le consentement aux traitements de telles données doit être explicite.

3.14. Le traitement qui a pour finalité la détection ou la prédiction des appartenances politiques, des opinions philosophiques, syndicales ou religieuses devrait de même être soumis à des garanties appropriées.

4. Information

4.1. Lorsque des données à caractère personnel sont collectées dans le cadre du profilage, le responsable du traitement devrait donner aux personnes concernées les informations suivantes :

a. l'utilisation de leurs données dans le cadre du profilage ;
b. les finalités poursuivies par le profilage effectué ;
c. les catégories de données à caractère personnel utilisées ;
d. l'identité du responsable du traitement et, le cas échéant, celle de son représentant ;
e. l'existence de garanties appropriées ;
f. toute information nécessaire à la garantie du caractère loyal du recours au profilage, telle que :
   – les catégories de personnes ou d'organismes auxquels les données à caractère personnel ou les résultats du traitement de profilage peuvent être communiquées, et les objectifs de cette communication ;
   – la possibilité, le cas échéant, pour les personnes concernées, de refuser le consentement ou de le retirer, et les conséquences d'un retrait ;
   – les conditions de l'exercice du droit d'accès, d'opposition ou de rectification, ainsi que le droit de déposer une plainte auprès de l'autorité compétente ;
   – les personnes ou les organismes auprès desquels les données à caractère personnel sont ou seront collectées ;
   – le caractère obligatoire ou facultatif de la réponse aux questions qui font l'objet de la collecte des données à caractère personnel, et les conséquences, pour les personnes concernées, d'un défaut de réponse ;
   – la durée d'enregistrement ;
   – le cas échéant, l'impact potentiel du profilage sur la personne concernée.

4.2. Lorsque des données à caractère personnel sont collectées dans le cadre du profilage, le responsable du traitement devrait indiquer par une icône, l'existence d'une activité de profilage. Cette icône devrait permettre à toute personne d'obtenir de manière automatique les informations reprises au Principe 4.1. au travers d'un lien vers le site web du responsable de traitement.

4.3. Lorsque les données à caractère personnel sont collectées auprès de la personne concernée, le responsable du traitement devrait l'informer, au plus tard au moment de la collecte, des éléments visés au Principe 4.1.

4.4. Lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, celle-ci devrait être informée par le responsable du traitement des éléments visés au principe 4.1, dès l'enregistrement des données à caractère personnel ou, si une communication des données à caractère personnel à un tiers est envisagée, au plus tard lors de la première communication des données à caractère personnel.

4.5. Lorsque des données à caractère personnel sont collectées sans intention d'appliquer des méthodes de profilage mais traitées par la suite dans le cadre du profilage, le responsable du traitement devrait être tenu de donner les mêmes informations que celles visées au principe 4.1.

4.6. Les dispositions énoncées aux principes 4.3, 4.4 et 4.5 d'informer la personne concernée ne s'appliquent pas :

a. si la personne concernée a déjà été informée ;
b. si l'information se révèle impossible à fournir ou implique des efforts disproportionnés ;
c. si le traitement ou la communication des données personnelles à des fins de profilage sont expressément prévus par le droit interne.

Dans les cas visés aux alinéas b et c, des garanties appropriées devraient être prévues.

4.7. L'information fournie à la personne concernée devrait être appropriée et adaptée aux circonstances.

5. Droits des personnes concernées

5.1. La personne concernée qui a fait, ou qui fait, l'objet d'un profilage devrait pouvoir, à sa demande, obtenir du responsable du traitement, dans un délai raisonnable et sous une forme compréhensible, les informations suivantes :

a. les données à caractère personnel qui la concernent et les catégories de données pseudonymisées ou anonymisées utilisées dans le cadre du traitement ;
b. la logique qui sous-tend le traitement des données à caractère personnel la concernant et qui a été utilisée pour lui attribuer un profil, au moins en cas de décision automatisée et, dans le cas d'utilisation de traitement basée sur l'apprentissage automatique

(*machine learning*) qui préside au fonctionnement de l'algorithme. Dans ce cas, l'information doit être telle qu'elle permette à la personne concernée de comprendre la justification des décisions ou propositions de décision prises à son encontre ;

c. les finalités poursuivies par le profilage effectué ;
d. les catégories de personnes ou d'organismes auxquels les données à caractère personnel, le profil ou le résultat du traitement peuvent être communiqués ainsi que le droit de s'y opposer.

5.2. Les personnes concernées devraient pouvoir obtenir, selon le cas, la rectification, l'effacement ou le verrouillage de leurs données, lorsque le profilage dans le cadre du traitement de données à caractère personnel s'effectue en méconnaissance des dispositions du droit interne donnant effet aux principes énoncés dans la présente recommandation.

5.3. Sauf si une loi prévoit le profilage dans le cadre du traitement de données à caractère personnel, la personne concernée devrait avoir le droit de s'opposer, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à l'utilisation de ses données dans le cadre du profilage. En cas d'opposition justifiée, le profilage ne devrait plus impliquer l'utilisation des données personnelles de la personne concernée. Quand le but du traitement est la prospection commerciale, politique, religieuse, syndicale ou philosophique, la personne concernée n'est pas tenue de fournir de justification.

5.4. S'il existe des motifs de restreindre les droits énoncés dans le présent paragraphe en application du chapitre 6, cette décision devrait être communiquée à la personne concernée par tout moyen permettant d'en garder la trace, avec mention des raisons juridiques et matérielles d'une telle restriction.

Il est possible d'omettre cette mention pour une raison nuisant au but de la restriction. Dans ce cas, la personne concernée devrait être informée des modalités de contestation de cette décision devant l'autorité de contrôle nationale compétente, une autorité judiciaire ou un tribunal.

5.5. Dans le cas où une personne concernée est soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur la seule base d'un profilage, elle devrait pouvoir s'opposer à cette décision, à moins :

a. que la loi l'autorise et précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée, notamment en lui permettant de faire valoir son point de vue ;
b. que la décision ait été prise dans le cadre de l'exécution d'un contrat auquel la personne concernée est partie ou en application des mesures précontractuelles prises à la demande de celle-ci et que les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée soient mises en place.

5.6. En toute hypothèse et non seulement dans les cas visés au Principe 5.5, lorsque le système de traitement de profilage émet une décision ou un projet de décision, il est recommandé que :

a. les responsables tiennent compte de toutes les particularités des données et ne se fondent pas simplement sur des informations ou des résultats décontextualisés du traitement ;
b. en cas de traitements à risque élevé, le responsable mette en place un service où une personne physique informera la personne concernée des opérations algorithmiques qui sous-tendent le traitement de données, y compris les conséquences pour elle de ces opérations. Dans ce cas, l'information doit être telle qu'elle permette à la personne concernée de comprendre la justification des décisions ou propositions de décision prises à son encontre ;
c. dans ce cas, la personne physique nommée par le responsable doit pouvoir, sur la base d'arguments raisonnables, décider de ne pas se baser sur les résultats des recommandations découlant de l'utilisation du traitement de profilage ;
d. en présence d'indications permettant de penser qu'il y a eu discrimination directe ou indirecte fondée sur le fonctionnement du traitement de profilage, les responsables du traitement et les sous-traitants apportent la preuve de l'absence de discrimination.

5.7. Les personnes affectées par une décision fondée sur un traitement de profilage ont le droit de contester celle-ci devant une autorité compétente.

5.8. Sauf consentement explicite, la personne concernée doit pouvoir s'opposer par un moyen facile à la cession ou au partage soit de données à des fins de profilage par des tiers soit de résultats de traitement de profilage.

6. Exceptions et restrictions

6.1. Lorsque cela est nécessaire dans une société démocratique pour des raisons de sécurité nationale, de sûreté publique, de défense des intérêts monétaires du pays, de prévention ou de répression des infractions pénales, ou à la protection des personnes concernées ou des droits et libertés d'autrui, les Etats membres n'appliquent pas les dispositions des chapitres 3, 4 et 5 de la présente recommandation, pour autant que cela soit prévu par la loi.

7. Recours

7.1. Le droit interne devrait prévoir les sanctions et recours appropriés en cas de violation des dispositions pertinentes du droit interne.

8. Sécurité des données

Dispositions générales

8.1. Des mesures techniques et d'organisation appropriées devraient être prises, en particulier sur base des principes du *'privacy by design'* et '*privacy by default'* , pour assurer la protection des données à caractère personnel, traitées conformément aux dispositions du droit interne donnant effet aux principes de la présente recommandation, contre la destruction – accidentelle ou illicite – et la perte accidentelle, ainsi que contre l'accès, la modification et la communication non autorisés ou toute autre forme de traitement illicite.

8.2. Ces mesures devraient assurer un niveau de sécurité des données approprié compte tenu de l'état de la technique, de la nature sensible des données collectées et traitées dans le cadre du profilage, et de l'évaluation des risques potentiels. Elles devraient être réévaluées périodiquement et dans un délai raisonnable.

8.3. Les responsables du traitement devraient, conformément au droit interne, établir un règlement interne approprié, dans le respect des principes pertinents de la présente recommandation.

8.4. Si nécessaire, les responsables du traitement devraient désigner une personne indépendante chargée de la sécurité des systèmes d'information et de la protection des données, et compétente pour donner des conseils sur ces questions.

8.5. Les responsables du traitement devraient choisir des sous-traitants qui apportent des garanties suffisantes concernant les aspects techniques et organisationnels des traitements à effectuer, et devraient s'assurer que ces garanties sont respectées et que, en particulier, les traitements sont conformes à leurs instructions.

8.6. Les responsables du traitement devraient évaluer le risque de ré-identification en tenant compte des délais, efforts ou ressources nécessaires au regard de la nature des données, du contexte de leur utilisation, des techniques de ré-indentification disponibles et des coûts correspondant. Les responsables du traitement devraient démontrer l'adéquation des mesures d'anonymisation des données et garantir l'efficacité de la pseudonymisation ou anonymisation ;
Les mesures techniques peuvent être combinées avec des obligations juridiques ou contractuelles afin de prévenir toute ré-identification possible des personnes concernées. Les responsables du traitement devraient réévaluer régulièrement le risque de ré-identification, eu égard aux avancées technologiques relatives aux techniques d'anonymisation.

Dispositions particulières en matière de traitements de profilage utilisant des procédés d'apprentissage automatique

8.7. Afin d'assurer la confiance dans les systèmes d'IA, les responsables de traitement et, le cas échéant, les sous-traitants veillent à l'utilisation de systèmes robustes et sûrs, notamment en ce qui concerne la mise sur pied de procédures en cas de non fonctionnement ou de fonctionnement défectueux ou erronés du système. Ils s'assurent de manière régulière tout au long de la vie du système que celui-ci est fiable et que ses résultats sont conformes au modèle et reproductibles.

8.8. Les responsables et, le cas échéant, les sous-traitants veillent à évaluer de manière critique la qualité, la nature et la quantité des données utilisées en éliminant les données inutiles et toutes celles qui pourraient biaiser les résultats. Ils s'assurent de la robustesse du modèle en cas d'apport de nouvelles données.

8.9. Les responsables et, le cas échéant, les sous-traitants veillent à la transparence du fonctionnement des systèmes et à la traçabilité des résultats du traitement. Ils veilleront à n'opposer leurs droits de propriété intellectuelle et leurs secrets d'affaire que de manière minimale et, en aucune manière, ne pourront s'opposer à la demande d'une personne concernée ou d'un groupe de pouvoir comprendre les décisions ou propositions de décisions sorties du traitement de profilage. Les applications d'intelligence artificielle devraient permettre le contrôle effectif tant par les personnes que par les groupes concernés des effets de ses applications tant sur les personnes, les groupes que la société.

8.10. Aux fins d'une évaluation continue des risques tant individuels que collectifs, et en tout cas lorsqu'il s'agit de traitements de profilage à risque élevé, les responsables de traitement et, le cas échéant, les sous-traitants devraient s'entourer d'une équipe d'évaluation multidisciplinaire et consulter les représentants des intérêts concernés par le profilage. Ce processus d'évaluation devrait être mené par des personnes dotées des qualifications professionnelles et des connaissances adéquates pour apprécier les différents impacts, y compris dans leurs dimensions juridique, sociale, éthique et technique.

9. Autorités de contrôle

9.1. Les États membres devraient charger une ou plusieurs autorités exerçant leurs fonctions en toute indépendance de veiller au respect du droit interne mettant en œuvre les principes énoncés dans la présente recommandation et disposant à cet effet des moyens d'investigation et d'intervention nécessaires, en particulier la compétence d'examiner les recours déposés par des individus.

9.2. Par ailleurs, dans le cas de traitements ayant recours au profilage et présentant des risques particuliers au regard de la protection de la vie privée et des données à caractère personnel, les États membres peuvent prévoir, en particulier en cas de traitement à risque élevé et de traitements de profilage mis en place par les autorités publiques :

a. que les responsables des traitements soient tenus de les notifier préalablement à l'autorité de contrôle ; ou
b. que ces traitements fassent l'objet d'un contrôle préalable par l'autorité de contrôle.

9.3. Les autorités de contrôle doivent coopérer dans toute la mesure du possible en ce qui concerne l'application de la présente recommandation avec les autorités de protection des consommateurs et de la concurrence de même qu'avec les institutions en charge de l'égalité des chances ou de la promotion de la démocratie.

9.4. Lors de leur analyse des traitements de profilage, les autorités de contrôle doivent étendre leur compétence à l'analyse des risques collectifs et sociétaux. Ils veilleront à ce que leurs avis mentionnent de tels risques et que leurs décisions les prennent en compte. Le cas échéant, ils provoqueront des débats en la matière. Ils attireront l'attention des Etats membres sur l'intérêt d'élargir leurs compétences en la matière.

9.5. Dans ce contexte, les autorités de contrôle devraient accueillir et instruire les plaintes émanant d'associations et visant l'intérêt collectif d'un groupe ou l'intérêt général. Le cas échéant, les autorités émettront des recommandations à ce propos.

9.6. Ces autorités devraient informer le public de l'application de la législation mettant en œuvre les principes énoncés dans la présente recommandation.

10. Mesures complémentaires

De la création d'une autorité nationale indépendante d'évaluation des risques liés à l'IA

10.1. Sans préjudice des compétences des autorités de contrôle en matière de protection des données, les Etats membres devraient créer une « Autorité nationale pluridisciplinaire indépendante d'évaluation des risques liés à l'intelligence artificielle et en particulier aux traitements de profilage utilisant des procédés d'apprentissage automatique (*machine learning*) ». Cette autorité indépendante serait en charge de l'audit, des tests et de la labellisation des systèmes d'IA des secteurs privé ou public. L'intervention de cette autorité serait obligatoire en matière d'IA utilisée pour des activités du secteur public et, sous réserve de ce qui pourrait être décidé par les Etats membres à propos des systèmes à risque élevé, volontaire pour les systèmes opérant dans le secteur privé.

10.2. Cette autorité émettrait des avis à propos, premièrement, de tout traitement de profilage individuel ou collectif envisagé par les administrations ou l'autorité de régulation pour appuyer leurs stratégies ou appliquer les réglementations, et ensuite, à propos de l'évaluation des risques liés des politiques privées ou publiques en matière de 'partage des données' et d''*open data*' et de soutien à la définition et à la mise en œuvre de 'bonnes pratiques'.

10.3. Cette autorité devrait émettre des recommandations relatives à la qualité des mégadonnées et des algorithmes de profilage afin d'assurer leur fiabilité, leur transparence et leur conformité aux législations applicables, notamment en matière de protection des données, de protection des consommateurs, de non-discrimination, de concurrence, etc.

10.4. Cette autorité travaillerait en étroite coopération avec les autorités de contrôle.

10.5. Ses avis et recommandations seraient publics.

De la labellisation et de la certification en matière de systèmes d'IA et de protection des données

10.6. Les États membres et les autorités de contrôle devraient encourager la mise en place de mécanismes indépendants et qualifiés de certification en matière de systèmes d'IA et de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent la présente recommandation. Les besoins spécifiques tant des micros, petites et moyennes entreprises que des différents secteurs devraient être pris en considération.

10.7. Les États membres peuvent prévoir des conditions d'agrément des organismes qui mettraient en place les mécanismes de contrôle visés au Principe 10.6.

10.8. La certification est volontaire et accessible via un processus transparent. Une certification en vertu du présent Principe ne diminue par la responsabilité du responsable du traitement ou du sous-traitant quant au respect de la présente recommandation ou des législations applicables.

10.9. Les responsables de traitement et les sous-traitants dont le système est certifié ou labellisé apposeront la marque de la certification ou du label au minimum sur leur sites et dans les informations à destination des personnes concernées. Ils veilleront à ce que via cette marque, toute personne puisse avoir accès au certificat ou au label.

En ce qui concerne les traitements de profilage mis en place par les autorités publiques

10.10. Les traitements de profilage opérés par les pouvoirs publics tant pour définir leurs stratégies que pour l'appliquer doivent être réalisés sur base d'une loi claire, proportionnée et nécessaire dans une société démocratique, au sens de la jurisprudence du Conseil de l'Europe.

10.11. Conformément au Principe 10. 1., la conception, la confection, l'application et le suivi des systèmes d'IA, en particulier de profilage, devraient être soumis à l'Autorité nationale pluridisciplinaire indépendante d'évaluation des risques liés à l'intelligence artificielle.

10.12. Les exigences d'accès aux documents administratifs et de motivation des décisions publiques imposent que les systèmes informatisés décisionnels ou d'aide à la prise de décision soient transparents et que les citoyens puissent nonobstant tout argument technique ou juridique, avoir accès aux raisonnements tenus par l'algorithme.

10.13. Les autorités publiques veilleront à répercuter les exigences des présentes recommandations en particulier celles qui leur sont spécifiques, vis-à-vis de leurs sous-traitants, dans le cadre des cahiers des charges.

Dispositions en matière de recherche et d'éducation

10.14. Les États membres devraient encourager, y compris en affectant des ressources, la recherche indépendante, interdisciplinaire et ouverte y compris fondamentale, en particulier en matière de fiabilité, audibilité, robustesse et de transparence des systèmes d'IA.

10.15. Les États membres devraient encourager les initiatives 'open source' en matière de conception et de diffusion des algorithmes.

10.16. Les États membres devraient affecter des ressources à l'éducation multidisciplinaire au numérique et ce à tous les niveaux de l'enseignement afin de renforcer la sensibilisation des personnes aux enjeux du numérique et, en particulier de l'IA. Ils devraient de même encourager la formation professionnelle, celle des responsables d'administrations et d'entreprises aux aspects techniques et aux enjeux sociétaux et droits de l'Homme des systèmes utilisés dans le cadre du profilage, notamment par la création de cours interdisciplinaires dans les programmes de formation de base ou continue aux métiers du numérique.