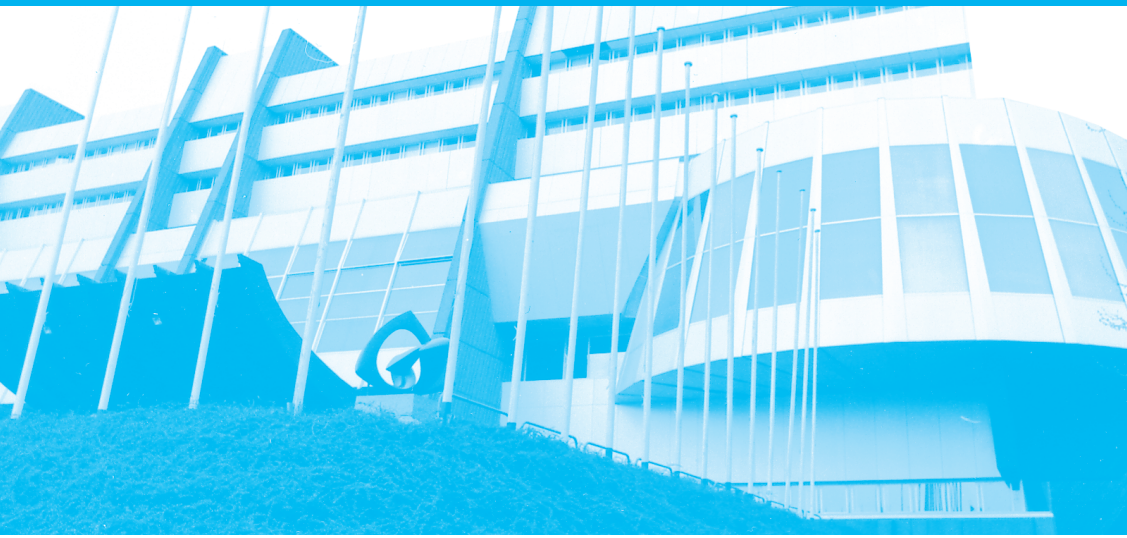
PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE DU PROFILAGE



Recommandation CM/Rec(2021)8

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DANS LE CADRE DU PROFILAGE

Recommandation CM/Rec(2021)8
adoptée par le Comité des Ministres
du Conseil de l'Europe
le 3 novembre 2021

Conseil de l'Europe

Édition anglaise :
Protection of individuals with regard to automatic processing of personal data in the context of profiling

Couverture et mise en page :
Division de la production des documents et des publications (DPDP), Conseil de l'Europe

Imprimé dans les ateliers du Conseil de l'Europe

Table des matières

RECOMMANDATION CM/REC(2021)8 **5**

Annexe à la Recommandation CM/Rec(2021)8 8

Recommandation CM/Rec(2021)8

(adoptée par le Comité des Ministres le 3 novembre 2021, lors de la 1416e réunion des Délégués des Ministres)

Le Comité des Ministres, en vertu de l'article 15.*b* du Statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Rappelant que les technologies numériques permettent le traitement de données à grande échelle, y compris pour les données à caractère personnel, dans le secteur public comme dans le secteur privé, utilisées à des fins très diverses, notamment pour des services largement acceptés et appréciés par la société et les personnes ;

Constatant que les données sont notamment traitées par le biais de calcul, de comparaison, de corrélation et autres techniques statistiques, dans le but de dégager des profils ou modèles qui pourraient être utilisés de maintes manières à des fins et usages différents par l'appariement des données de plusieurs personnes ;

Considérant qu'en observant et en reliant un grand nombre de données même anonymes, les techniques de profilage peuvent avoir des incidences pour les personnes concernées en les plaçant dans des catégories prédéterminées, très souvent à leur insu ;

Considérant que le manque de transparence, voire l'invisibilité, du profilage et le manque de précision qui peut découler de l'application automatique de règles d'inférence préétablies peuvent faire peser de graves menaces sur les droits et libertés de chacun ;

Notant que les données traitées dans le cadre du profilage peuvent comprendre des catégories particulières de données à caractère personnel – notamment des données biométriques – dont une mauvaise utilisation peut entraîner des dommages irréversibles pour les personnes concernées lorsque de telles données peuvent être utilisées pour accéder à divers services et pour réaliser des actions pouvant avoir des effets juridiques ;

Considérant en particulier que la protection des droits fondamentaux, notamment les droits à la vie privée et à la protection des données à caractère personnel, garantit l'existence de sphères de vie différentes et indépendantes où chaque personne peut contrôler l'usage des informations qui la concernent ;

Considérant la vulnérabilité particulière de certaines personnes concernées par le profilage, y compris les enfants, et la possible gravité des conséquences d'un tel profilage, parfois pour le reste de leur vie ;

Conscient de l'intensification et de la diversification du profilage des personnes, dans toutes les sphères d'activité ;

Eu égard aux dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (STE n° 108, ci-après la « Convention 108 »), telle que modernisée par le Protocole d'amendement[1] (STCE n° 223), et convaincu de l'intérêt de faciliter l'application de ces principes dans le contexte du profilage ;

Soulignant qu'il appartient aux États membres de veiller au respect des cadres législatifs et réglementaires applicables, et d'assurer des garanties procédurales, organisationnelles et matérielles ainsi que l'accès à des recours effectifs à l'encontre de tous les acteurs concernés, tout en promouvant un environnement où l'innovation technologique respecte et renforce les droits de l'homme, et se conforme à l'obligation fondamentale selon laquelle toute restriction aux droits de l'homme doit être nécessaire et proportionnée dans une société démocratique, et mise en œuvre conformément à la loi ;

1. Le Protocole d'amendement à la Convention 108 (STCE n° 223) a été ouvert à la signature le 10 octobre 2018, et la convention ainsi modernisée doit encore entrer en vigueur. Il sera ci-après fait référence à la « Convention 108+ ».

Constatant que la situation a considérablement évolué depuis l'adoption de la Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, et que les méthodes et l'impact du profilage ont changé radicalement ;

Gardant à l'esprit que les technologies numériques recèlent un potentiel important d'innovation et de croissance, et que la réalisation de ces objectifs doit être ancrée dans les valeurs communes des sociétés démocratiques ;

Notant que l'évolution rapide des technologies utilisées et des capacités des algorithmes s'accompagne d'une augmentation constante du volume de données à caractère personnel traitées et que, tout en ouvrant la voie à l'innovation et à la croissance, cette convergence de facteurs peut également engendrer des risques au niveau tant individuel que collectif ;

Observant que ces développements rendent nécessaire l'actualisation de la Recommandation CM/Rec(2010)13 en tenant dûment compte de la Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme,

Recommande aux gouvernements des États membres :

- de prendre en compte les principes énoncés à l'annexe de la présente recommandation, qui remplace la Recommandation CM/Rec(2010)13 susmentionnée, dans leur loi et pratiques ;
- de veiller à ce que la présente recommandation et son annexe soient traduites et diffusées aussi largement que possible auprès des autorités et des parties prenantes compétentes, notamment auprès des autorités indépendantes, des organisations de défense des droits de l'homme, des organisations de la société civile et du secteur privé ;
- de promouvoir l'acceptation et l'application des principes contenus dans l'annexe à cette recommandation par toutes les parties prenantes, s'assurant que les acteurs du secteur privé participant à la conception, au développement et à la réalisation d'activités de profilage se conforment aux lois applicables et assument leurs responsabilités en matière de respect des droits de l'homme.

Annexe à la Recommandation CM/Rec(2021)8

1. Définitions

1.1. Aux fins de la présente recommandation :

a. « 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, des ressources ou des efforts déraisonnables au regard des moyens dont dispose le responsable du traitement.

b. « Catégories de données traitées » signifie les différents types de données utilisées lors du traitement de profilage, peu importe leurs sources et leur nature.

c. « Profilage » désigne toute forme de traitement automatisé de données à caractère personnel, notamment au moyen de systèmes d'apprentissage automatique, consistant à utiliser ces données 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.

d. « Profil » désigne un ensemble de données attribué à une personne, qui caractérise une catégorie de personnes ou qui est destiné à être appliqué à une personne.

e. « Modèle » est une abstraction mathématique utilisée, par exemple, dans les méthodes d'apprentissage automatique, qui fournit une description simplifiée des données pour réaliser la tâche à effectuer.

f. « Intelligence artificielle » (IA) désigne un système qui est soit fondé sur des logiciels, soit intégré dans des dispositifs matériels, et qui fait preuve d'un comportement intelligent, notamment en collectant et traitant des données, en analysant et en interprétant son environnement, et en prenant des mesures, avec un certain degré d'autonomie, pour atteindre des objectifs spécifiques.

g. « Traitement utilisant des procédés d'apprentissage automatique » (*machine learning*) signifie un traitement utilisant des méthodes particulières d'intelligence artificielle fondé 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.

h. « Système automatisé de prise de décision » se réfère à un système qui utilise un raisonnement automatisé pour assister ou remplacer un processus décisionnel qui serait sans cela effectué par des êtres humains.

i. « Services d'intermédiaires en ligne » désigne les services de la société de l'information qui permettent aux utilisateurs soit de recevoir des informations (services de recherche en ligne), des biens ou des services, soit d'entrer en relation (service d'accès à des réseaux sociaux).

j. « Traitements de profilage à risque élevé » peut notamment désigner :

i. le profilage dont le fonctionnement entraîne des effets juridiques ou qui ont un impact significatif pour la personne concernée ou pour le groupe de personnes identifié par le traitement de profilage ;

ii. le profilage qui – en raison du public visé, du contexte ou de la finalité du traitement – en particulier dans une situation de déséquilibre dans le pouvoir d'information, comporte un risque d'affecter ou d'influencer indûment les personnes concernées, notamment lorsqu'il s'agit de mineurs ou d'autres personnes vulnérables ;

iii. le profilage qui implique des données relevant des catégories particulières de données au sens de l'article 6 de la Convention 108+ ou ayant pour finalité de les détecter ou les prédire ;

iv. le profilage affectant un très grand nombre de personnes, notamment celui opéré par des services d'intermédiaires en ligne pour leur bénéfice propre ou pour celui de tiers.

2. Principes généraux

2.1. Le respect des libertés et des droits fondamentaux, notamment les droits à la dignité humaine et à la vie privée mais également à la liberté d'expression, et du principe de non-discrimination et des impératifs de justice sociale, de diversité culturelle et de démocratie devraient être garantis, dans le secteur public comme dans le secteur privé, lors du traitement de profilage visé par la présente recommandation.

2.2. Les traitements de profilage devraient contribuer au bien-être des personnes, ou pour le moins ne pas les affecter négativement, comme au développement d'une société inclusive, démocratique et durable.

2.3. Dans le cadre de l'utilisation croissante de mégadonnées *(big data),* des données à la fois personnelles et non personnelles sont collectées. Par ailleurs, avec des traitements automatisés, fondés notamment sur l'utilisation de systèmes d'apprentissage automatique, il est difficile de savoir a priori quelles données permettront des corrélations ou des prédictions relatives à une personne concernée. Dans de tels cas, pour que les données à caractère personnel soient traitées de façon loyale, les organisations devraient garantir la pertinence et la qualité de toutes les données, y compris les données non personnelles, qui pourraient permettre les corrélations ou prédictions relatives à une personne concernée.

2.4. Tous les systèmes automatisés de prise de décision sont conçus par des êtres humains et impliquent un certain degré d'intervention humaine dans leur fonctionnement. Les êtres humains sont ultimement responsables de la manière dont un système reçoit ses entrées (par exemple, qui collecte les données alimentant un système), de la manière dont le système est utilisé et de la manière dont les sorties d'un système sont interprétées et appliquées. Les systèmes (spécialement ceux fondés sur l'IA) doivent permettre une intervention humaine opérationnelle chaque fois que cela est approprié ou nécessaire pour assurer leur fonctionnement légitime, notamment au regard des principes de loyauté et de non-discrimination.

2.5. Les États membres devraient encourager 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)* et pendant toute la durée du traitement des données, notamment grâce à l'utilisation de technologies renforçant la protection de la vie privée. Ils devraient également prendre des mesures appropriées pour lutter contre le développement et l'utilisation de technologies qui visent, totalement ou partiellement, au contournement illicite des mesures technologiques de protection de la vie privée.

2.6. Les traitements de profilage ne doivent pas engendrer de discriminations vis-à-vis de personnes ni vis-à-vis de groupes ou collectivités. Ils ne doivent porter atteinte ni à la dignité des personnes ni à la démocratie. L'utilisation de systèmes automatisés de prise de décision devrait préserver l'autonomie de l'intervention humaine dans le processus décisionnel.

2.7. Les traitements de profilage ne devraient pas avoir pour but la manipulation des personnes concernées ou de leurs proches, notamment au regard de leurs choix ou opinions.

2.8. Au moins lorsque le consentement de la personne concernée est requis, les prestataires de services et, en particulier, les services d'intermédiaires en ligne devraient offrir aux personnes concernées la possibilité d'accepter le profilage et de choisir entre les différentes finalités ou degrés de profilage. Les personnes concernées devraient être informées de toutes les conséquences de leur choix.

2.9. Les États membres devraient veiller à ce que le cadre juridique applicable aux traitements de profilage assure qu'ils restent proportionnés aux finalités poursuivies et à la nature et à la gravité des risques encourus par les personnes concernées ou les groupes visés. Les besoins spécifiques des micros, petites et moyennes entreprises, et des différents secteurs devraient être pris en compte. Si les activités de profilage réalisées sont de nature à présenter un risque élevé, le même niveau de rigueur devrait être appliqué quelle que soit la taille de l'entreprise.

2.10. L'utilisation de systèmes automatisés de prise de décision fondés sur les technologies de l'IA pour le profilage présente des risques supplémentaires en raison d'erreurs et de biais possibles et de la difficulté de justifier les décisions prises et d'assurer la transparence et, par conséquent, empêche le plein exercice des droits des personnes concernées. La conception, l'élaboration et la mise en œuvre des systèmes automatisés de prise de décision fondés sur l'IA exigent une attention particulière et continue au regard des risques créés, ainsi que leur évaluation par des équipes pluridisciplinaires et indépendantes.

2.11. Les traitements de profilage mettent en jeu différents acteurs dont il importe d'analyser la qualité et le rôle afin de déterminer leurs responsabilités, éventuellement conjointes, surtout en cas de partage de données.

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

A. Licéité

3.1. Le traitement des données à caractère personnel dans le cadre du profilage devrait être loyal, licite et proportionné, et devrait poursuivre des finalités spécifiques et légitimes, sans jamais être effectué d'une manière incompatible avec ces finalités initiales. Le traitement de données à caractère personnel dans le cadre du profilage ayant une finalité compatible ne peut être effectué que s'il est prévu par le droit interne ou s'il est fondé sur le consentement, conformément au principe 3.4 qui prévoit des garanties spécifiques appropriées en ce qui concerne ces données.

3.2. Les données personnelles utilisées dans le cadre du profilage devraient être adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont collectées et pour lesquelles elles seront traitées. Dans les systèmes d'apprentissage automatique *(machine learning),* il est difficile de connaître a priori quelles données permettront des corrélations significatives. Toutefois, il est important de limiter le traitement de profilage à des catégories de données dont la personne concernée peut raisonnablement s'attendre (attentes légitimes) à ce qu'elles soient prises en considération au vu des finalités du profilage.

3.3. Les données à caractère personnel utilisées dans le cadre du profilage devraient être, ou au moins être conservées, sous une forme qui permet l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées. Si cela est possible pour les finalités dans lesquelles les données sont traitées, elles devraient être anonymisées.

3.4. Sauf indication contraire ci-après, le traitement de données à caractère personnel dans le cadre du profilage ne peut être effectué que :

- si la loi nationale le prévoit expressément afin de garantir les droits et libertés de personnes concernées ainsi que leur intérêt légitime ; ou
- si la personne concernée ou son représentant légal a donné son consentement libre, spécifique, éclairé et non équivoque. Dans le cas de profilage à risque élevé, le consentement doit être explicite ; ou
- 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 ; ou
- s'il 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 à caractère personnel sont communiquées ; ou
- s'il est nécessaire aux fins de l'intérêt légitime du responsable du traitement ou du/des tiers auxquels le profil ou les données sont communiquées, à condition que ne prévalent pas les libertés et droits fondamentaux de la personne concernée ou qu'il ne s'agisse pas de catégories particulières de données. La nécessité devrait être explicitement motivée par le responsable du traitement ; ou
- s'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ou d'autres personnes.

3.5. Lorsque le profilage est fondé sur le consentement, le traitement dans le cadre du profilage des données à caractère personnel des personnes qui ne peuvent pas exprimer elles-mêmes leur consentement libre, spécifique, éclairé et non équivoque devrait être interdit à moins qu'un consentement spécifique soit donné par leur représentant légal ou que ce traitement soit dans l'intérêt légitime de la personne concernée ou pour un intérêt public substantiel prépondérant, et à condition que des garanties appropriées soient prévues par une loi.

3.6. Dans la mesure du possible, les prestataires de services et les plateformes devraient offrir différents services plus ou moins personnalisés, voire non personnalisés, en fonction du service offert, afin de garantir à la personne concernée un choix en ce qui concerne l'intensité du profilage. Pour qu'il soit libre, le consentement suppose pour la personne concernée, la possibilité d'un choix éclairé. Le consentement au profilage ne devrait pas pouvoir être exigé comme condition de la prestation d'un service. Quand le profilage est fondé sur le consentement, il incombe au responsable du traitement de prouver que la personne concernée a accepté explicitement le profilage au-delà de ce qui était nécessaire à l'exécution de la prestation et ce après avoir été informée conformément au chapitre 4 et conformément aux exigences relatives au consentement prévues au principe 3.4.

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. Afin de garantir que le consentement au profilage est libre, spécifique, éclairé et non équivoque, les services d'intermédiaires en ligne devraient, par défaut, garantir un accès non personnalisé à l'information concernant leurs services.

3.9. 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, si elles constituent une mesure nécessaire et proportionnée dans une société démocratique, et si elles sont assorties de garanties appropriées.

B. Qualité des données et des algorithmes

3.10. Le responsable du traitement et, le cas échéant, les sous-traitants 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.

3.11. Le responsable 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, ainsi que l'impact de l'utilisation du profilage sur les droits de la personne concernée.

3.12. Lorsqu'ils acquièrent des données ou des algorithmes d'un tiers, le responsable du traitement et le cas échéant le sous-traitant devraient 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.

C. Catégories particulières de données

3.13. Le traitement de données sensibles définies à l'article 6 de la Convention 108+ dans le cadre du profilage ne devrait être autorisé que si des garanties appropriées sont prévues par la loi et que ces données sont nécessaires pour les finalités légales et spécifiques du traitement.

3.14. Le traitement qui a pour finalité la détection ou la prédiction des origines raciales ou ethniques, des opinions politiques, de l'appartenance syndicale, des croyances religieuses ou autres convictions, de la santé ou la vie sexuelle devrait être interdit et ne devrait être autorisé que si des garanties appropriées sont prévues par la loi et que les données sont absolument nécessaires pour les finalités légales et spécifiques du traitement. Dans le cas où un consentement est demandé, il devrait être explicite dès lors que le traitement concerne de telles données.

4. Information

4.1. Lorsque des données à caractère personnel relatives à une personne sont collectées auprès de la personne concernée dans le cadre du profilage, le responsable du traitement devrait lui communiquer, au plus tard quand les données sont obtenues, les informations suivantes :

a. l'utilisation de ses données, ou celle qui est prévue, dans le cadre du profilage par le responsable du traitement et/ou des tiers ;

b. les bases légales et les finalités poursuivies par le profilage effectué ;

c. les catégories de données utilisées dans le contexte du profilage ;

d. l'identité du responsable du traitement et sa localisation ou sa résidence habituelle et, le cas échéant, celle de son représentant ;

e. l'existence de garanties appropriées lorsque cela est requis, comme c'est notamment le cas s'agissant des données spéciales ;

f. les catégories de personnes ou d'organismes auxquels les données à caractère personnel ou les résultats du traitement de profilage peuvent être communiqués, et les objectifs de cette communication ;

g. les conditions de l'exercice du droit d'accès, d'opposition, de rectification, ou d'effacement, comme prévu par le principe 5 de la présente annexe ainsi que le droit de déposer une plainte auprès de l'autorité compétente ;

h. toute information nécessaire à la garantie du caractère loyal du recours au profilage, telle que :

- la possibilité, le cas échéant, pour les personnes concernées, de refuser le consentement ou de le retirer, et les conséquences d'un retrait ;
- les personnes ou les organismes auprès desquels d'autres données à caractère personnel sont ou seront collectées ;
- le caractère obligatoire ou facultatif de la réponse aux questions utilisées pour collecter les données, et les conséquences pour les personnes concernées d'une absence de réponse ;
- la durée de conservation des données à caractère personnel ;
- le cas échéant, l'impact potentiel du profilage sur la personne concernée ;
- des informations utiles sur le raisonnement qui sous-tend le profilage ou sur le modèle utilisé par le responsable du traitement des données.

4.2. Lorsque les données à caractère personnel ne sont pas obtenues auprès de la personne concernée, celle-ci devrait être informée par le responsable du traitement, au minimum au moyen d'une information générale, des éléments visés au principe 4.1 dès le traitement des données à caractère personnel ou, si une communication de ces données à un tiers est envisagée, au plus tard lors de la première communication des données. Outre les informations énumérées au principe 4.1, les informations devraient inclure l'origine des données collectées, la base juridique de la transmission ou du partage de données et la possibilité de s'opposer à cette transmission ou ce partage.

4.3. L'information fournie à la personne concernée devrait l'être d'une manière compréhensible et adaptée aux circonstances. Lorsque des données à caractère personnel sont traitées dans le cadre du profilage, le responsable du traitement pourrait 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 spécifiées au principe 4.1 au moyen d'un lien vers le site web du responsable du traitement.

4.4. Lorsque des données à caractère personnel précédemment collectées sans intention d'appliquer des méthodes de profilage sont ensuite traitées de manière licite dans le cadre du profilage, le responsable du traitement devrait être tenu de donner les informations visées aux principes 4.1 et 4.2.

4.5. Les principes 4.2, 4.3 et 4.4 portant sur l'information de la personne concernée ne s'appliquent pas si la personne concernée a déjà été informée. En outre, lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, les principes 4.2, 4.3 et 4.4 ne s'appliquent pas si :

a. l'information se révèle impossible à fournir ou si cela implique des efforts disproportionnés ; ou

b. les restrictions au droit à l'information sont prévues par le droit interne.

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 qu'elles aient été utilisées sous une forme pseudonymisée ou non, et toute autre information complémentaire nécessaire pour garantir un traitement loyal et transparent (y compris les ensembles de données anonymisées utilisées dans le traitement) et, en cas d'utilisation de profils, les données déduites par l'utilisation du système de profilage ;

b. le raisonnement qui sous-tend le traitement des données à caractère personnel la concernant et qui a été utilisé pour lui attribuer un profil, au moins en cas de décision automatisée et, dans le cas d'utilisation de traitement fondée sur l'apprentissage automatique, le modèle qui préside au fonctionnement de l'algorithme. Dans ce cas, l'information doit être propre à permettre à la personne concernée de comprendre les raisons des décisions ou projets de décisions prises à son encontre ;

c. les finalités poursuivies par le profilage effectué ;

d. les catégories de personnes ou d'organismes auxquelles les données à caractère personnel, le profil ou le résultat du traitement peuvent être communiqués, ainsi que le droit de s'y opposer ;

e. le nom et l'adresse de la personne en charge du recours des personnes concernées contre la décision ou le projet de décision, comme prescrit au principe 5.8.

5.2. Les personnes concernées devraient pouvoir obtenir dans les meilleurs délais l'effacement ou la rectification de leurs données à caractère personnel traitées en violation des dispositions de cette recommandation, notamment lorsque l'utilisation ou la prédiction porte sur des catégories spéciales de données sans les garanties appropriées prescrites par le droit national.

5.3. Sauf si une loi prévoit le profilage et dispose des mesures de sauvegarde des intérêts légitimes de la personne concernée, cette dernière devrait avoir le droit de s'opposer au traitement de ses données à caractère personnel à tout moment, pour des raisons qui la concernent. À moins que le responsable du traitement puisse démontrer des raisons légitimes pour le traitement qui prévalent sur les intérêts ou les droits et libertés fondamentales de la personne concernée, le profilage ne devrait plus impliquer l'utilisation de ses données à caractère personnel. Quand la finalité du traitement de profilage est la prospection commerciale directe, aucune justification ne devrait être demandée à la personne concernée.

5.4. S'il existe des motifs de restreindre les droits énoncés dans ce chapitre 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 factuelles d'une telle restriction. Il est possible d'omettre cette mention pour une raison qui nuirait au but de la restriction. Dans ce cas, la personne concernée devrait être informée des modalités de contester cette décision devant l'autorité de contrôle nationale compétente, une autorité judiciaire ou un tribunal.

5.5. Dans le cas où une personne 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'y opposer, à moins :

a. que la loi l'autorise et précise les mesures garantissant la sauvegarde des intérêts légitimes, des droits et des libertés fondamentales de la personne concernée, notamment en lui permettant de faire valoir son point de vue ;

b. que la décision soit nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou pour l'application des mesures précontractuelles prises à la demande de celle-ci et que les mesures garantissant la sauvegarde des intérêts légitimes, des droits et des libertés fondamentales de la personne concernée soient mises en place.

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

a. le responsable du traitement tienne compte de toutes les particularités des données et ne se fonde pas simplement sur des informations ou des résultats du traitement pris hors de son contexte ;

b. en cas de traitement de profilage à risque élevé, le responsable du traitement informe la personne concernée des opérations algorithmiques qui sous-tendent le traitement de données, y compris les conséquences pour elle de ces opérations. L'information devrait être telle qu'elle permette à la personne concernée de comprendre la justification des décisions ou les projets de décisions ;

c. la personne désignée par le responsable du traitement puisse, sur la base d'arguments raisonnables, décider de ne pas se fonder sur les résultats des recommandations découlant de l'utilisation du 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, le responsable 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 profilage devraient avoir le droit de recevoir toute explication utile sur cette décision, ou ce projet de décision, afin d'en comprendre la justification. La propriété intellectuelle ou l'existence de secrets commerciaux ne peuvent être contestées que lorsque les informations à fournir affectent gravement ces droits. L'invocation de ces droits et intérêts par le responsable du traitement ne peut conduire à priver la personne concernée ou le groupe affecté de la capacité de comprendre les décisions ou les projets de décision adoptés par le responsable du traitement.

5.8. Nonobstant le recours devant une autorité de contrôle ou le recours juridique, les personnes concernées devraient avoir le droit de contester le profilage devant une personne désignée par le responsable du traitement, ayant accès à toutes les informations sur le profilage et son fonctionnement, et qualifiée pour modifier ou supprimer la décision ou le projet de décision.

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

6. Exceptions et restrictions

6.1. Lorsque cela constitue une mesure nécessaire et proportionnée dans une société démocratique pour des raisons de sécurité nationale, de défense, de sûreté publique et autres raisons listées à l'article 11 de la Convention 108+, les dispositions prévues aux chapitres 3, 4 et 5 peuvent être sujettes à restrictions. De telles restrictions doivent par ailleurs être prévues par la loi et respecter l'essence des droits et des libertés fondamentales, notamment la liberté d'expression.

6.2. Les dispositions prévues aux chapitres 4 et 5 peuvent être sujettes à restrictions conformément à l'article 11.2 de la Convention 108+ à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, lorsqu'il n'existe pas de risque identifiable d'atteinte aux droits et libertés fondamentales des personnes.

7. Sécurité des données

A. Dispositions générales

7.1. Des mesures techniques et organisationnelles appropriées devraient être prises, en particulier sur la base des principes de la vie privée dès la conception *(privacy by design)* et de la vie privée par défaut *(privacy by default),* pour assurer la protection des données à caractère personnel traitées conformément aux dispositions du droit interne en application des principes de la Convention 108+, contre une destruction accidentelle ou illicite et une perte accidentelle, ainsi que contre un accès, une modification et une communication non autorisés, ou toute autre forme de traitement illicite.

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

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

7.4. Si nécessaire, les responsables du traitement devraient désigner des personnes indépendantes chargées de la sécurité des systèmes d'information et de la protection des données et compétentes pour donner des conseils sur ces questions.

7.5. Les responsables du traitement devraient choisir des sous-traitants qui apportent des garanties adéquates pour 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.

7.6. Dans les cas où les données ont été anonymisées ou pseudonymisées, les responsables du traitement devraient évaluer le risque de réidentification de la personne concernée (en tenant notamment compte des délais, efforts ou ressources nécessaires au regard de la nature des données, du contexte de leur utilisation, des techniques de réidentification disponibles et des coûts correspondants). Les responsables du traitement devraient démontrer l'adéquation des mesures de pseudonymisation ou d'anonymisation des données et garantir leur efficacité. S'il existe un risque de réidentification de la personne concernée, ces données ne peuvent plus être considérées comme anonymisées. Les mesures techniques peuvent être combinées avec des obligations juridiques ou contractuelles afin de prévenir toute possible réidentification de la personne concernée. Les responsables du traitement devraient réévaluer régulièrement le risque de réidentification, eu égard aux avancées technologiques relatives aux techniques de désanonymisation. Les États membres pourraient établir de manière régulière une liste des techniques de pseudonymisation et/ou d'anonymisation à l'usage des responsables du traitement.

B. Dispositions particulières en matière de profilage fondées sur des systèmes d'IA utilisant des procédés d'apprentissage automatique

7.7. Afin d'assurer la confiance dans les systèmes d'IA et leur licéité, les responsables du traitement et, le cas échéant, les sous-traitants devraient veiller à l'utilisation de systèmes fiables et sûrs, notamment en ce qui concerne la mise sur pied de procédures en cas de non-fonctionnement, d'erreurs ou d'incohérences pendant toute la durée de vie du système. Ils devraient s'assurer de manière régulière et tout au long de la vie du système que celui-ci est fiable et que ses résultats sont conformes au modèle et reproductibles. Le système devrait être robuste pour résister aux attaques ou à d'autres manipulations des données ou des algorithmes.

7.8. Les responsables du traitement et, le cas échéant, les sous-traitants devraient veiller à évaluer de manière critique la qualité, la nature représentative et la quantité des données utilisées en éliminant les données inutiles et toutes celles qui pourraient biaiser les résultats. En particulier, des seuils spécifiques d'exactitude des résultats devraient être respectés. Les responsables du traitement s'assurent de la robustesse du modèle en cas d'apport de nouvelles données. Les résultats eux-mêmes devraient être évalués pour connaître leur impact sur la personne concernée, y compris le droit à la non-discrimination. Les applications d'IA devraient permettre le contrôle effectif par les personnes comme par les groupes concernés des effets de ses applications autant sur les personnes, sur les groupes que sur la société.

7.9. 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 du traitement et, le cas échéant, les sous-traitants devraient documenter l'entraînement du modèle et effectuer des évaluations d'impact régulières en traitant des risques spécifiques du profilage fondé sur des systèmes d'IA. Pour atteindre cet objectif, ils devraient s'entourer d'une équipe d'évaluation multidisciplinaire et consulter les représentants des intérêts concernés par le profilage, y compris les personnes faisant l'objet d'un 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.

8. Autorités de contrôle

8.1. Les autorités de contrôle au titre de l'article 15 de la Convention 108+ veillent au respect du droit interne mettant en œuvre les principes énoncés dans la présente recommandation.

8.2. Lorsque l'activité de profilage envisagée est de nature à présenter un risque élevé, les États membres peuvent prévoir que les responsables du traitement notifient son existence à l'autorité de contrôle et, si cette dernière le demande, qu'ils mettent à disposition tous les documents relatifs à la procédure suivie, l'évaluation elle-même et informent des mesures correctrices prises ou envisagées.

8.3. La propriété intellectuelle ou l'existence de secrets commerciaux ne peuvent conduire à priver l'autorité de contrôle de la capacité d'exercer ses pouvoirs et, par exemple, d'évaluer la prise de décision automatisée.

8.4. En ce qui concerne l'application de la présente recommandation, les autorités de contrôle devraient coopérer dans toute la mesure du possible avec les autorités de protection des consommateurs et de la concurrence, ainsi qu'avec les institutions en charge de l'égalité des chances ou de la promotion de la démocratie. Lorsqu'il existe une autorité nationale pluridisciplinaire indépendante d'évaluation des risques liés à l'IA et en particulier au profilage utilisant des procédés d'apprentissage automatiques *(machine learning),* l'autorité de contrôle devrait coordonner ses travaux avec cette institution.

8.5. Le champ d'enquête des autorités de contrôle devrait être élargi aux risques collectifs et sociétaux. Leurs avis devraient mentionner de tels risques et leurs décisions les prendre en considération.

8.6. Dans ce contexte, les autorités de contrôle devraient avoir le droit de recevoir et d'instruire des plaintes émanant d'associations et visant l'intérêt collectif d'un groupe ou l'intérêt général, et le cas échéant prononcer des sanctions.

8.7. Les autorités mentionnées ci-dessus devraient informer le public de l'application de la législation mettant en œuvre les principes énoncés dans la présente recommandation.

9. Mesures complémentaires

A. Labellisation et certification en matière de systèmes d'IA et de protection des données

9.1. Les États membres et les autorités de contrôle devraient encourager la mise en place de mécanismes indépendants et qualifiés de certification des systèmes d'IA eu égard à leur conformité aux exigences légales en matière de protection des données, en particulier pour l'entraînement et le modèle qui en résulte sur lesquels le profilage est fondé ainsi que les labels et marques de confiance associés. Cela constituerait un élément pour démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent la présente recommandation.

9.2. Les États membres peuvent prévoir des conditions d'agrément des organismes qui mettraient en place les mécanismes de contrôle visés aux principes 8.1 et 8.2.

9.3. La certification est volontaire et accessible grâce à un processus transparent. Une certification en vertu du présent principe ne devrait pas diminuer la responsabilité du responsable du traitement ou du sous-traitant à l'égard du respect de la présente recommandation ou des législations applicables.

9.4. Les responsables du traitement et les sous-traitants dont le système est certifié ou labellisé indiqueront la marque de la certification ou du label au minimum sur leurs sites et dans les informations à fournir aux personnes concernées. Ils devraient veiller à ce que, grâce à cette marque, toute personne puisse avoir accès au certificat ou au label. La durée de validité de la certification devrait être limitée dans le temps.

B. Traitements de profilage mis en place par les autorités publiques

9.5. Sans préjudice des autres principes applicables de la présente recommandation, les opérations de profilage effectuées par les autorités publiques devraient être légales, proportionnées et nécessaires par rapport aux objectifs de ces opérations.

9.6. Les opérations de profilage menées par les autorités publiques, utilisant des systèmes automatisés de prise de décision, tant pour définir leurs stratégies que pour les appliquer, doivent être fondées sur la loi nationale (claire, prévisible et accessible), poursuivre un objectif légitime et être limitées à ce qui est nécessaire et proportionné pour atteindre cet objectif légitime, en prenant pleinement en considération tous les droits fondamentaux nécessaires concernés dans une société démocratique, selon l'interprétation de la jurisprudence de la Cour européenne des droits de l'homme.

9.7. La conception, le développement, l'application et le suivi des systèmes d'IA, en particulier des systèmes de profilage, devraient être soumis à l'autorité compétente pour l'évaluation des risques liés à l'IA.

9.8. Les autorités publiques devraient publier des informations sur le raisonnement qui sous-tend le traitement ou, dans le cas du recours à un traitement fondé sur l'apprentissage automatique, une explication en langage clair du modèle sur lequel le système est fondé.

9.9. Les décisions individuelles ou projets de décisions prises par les autorités publiques et fondés sur des systèmes automatisés de prise de décision devraient être transparents. Les particuliers ainsi que toute association légitime, nonobstant des motifs techniques ou juridiques, devraient pouvoir avoir accès au raisonnement qui sous-tend le traitement ou, dans le cas de l'utilisation de traitements fondés sur l'apprentissage automatique, à une explication en langage clair de la décision prise par le modèle sur lequel le système est fondé. Sans cela, une protection légale effective contre les décisions ne serait pas garantie.

9.10. Les autorités publiques devraient veiller à ce que les exigences des présentes recommandations en particulier celles qui leur sont spécifiques, soient communiquées à leurs sous-traitants, dans le cadre des cahiers des charges.

C. Dispositions en matière de recherche et d'éducation

9.11. Les États membres devraient encourager une recherche indépendante, interdisciplinaire et ouverte, y compris la recherche fondamentale, en particulier en matière de fiabilité, de vérifiabilité, de robustesse et de transparence des systèmes d'IA, et affecter des ressources à cette fin. Le cas échéant, cette recherche devrait être menée en concertation avec les représentants de la société civile.

9.12. Les États membres devraient encourager les initiatives « *open source* » en matière de conception et de diffusion libre des algorithmes.

9.13. Les États membres devraient allouer des ressources à une éducation multidisciplinaire au numérique et ce à tous les niveaux de l'enseignement, afin de renforcer la sensibilisation des personnes aux effets de l'IA et du profilage sur les droits fondamentaux. Ils devraient de même encourager la formation professionnelle, y compris celle des responsables d'administrations et d'entreprises sur les aspects techniques et sur les enjeux de société et de droits de l'homme des systèmes utilisés dans le cadre du profilage. Des cours interdisciplinaires devraient notamment être proposés dans les programmes de formation de base ou de formation continue aux métiers du numérique.

Ces dix dernières années, les techniques de profilage ont radicalement évolué, notamment avec l'introduction de l'intelligence artificielle et l'utilisation de systèmes d'apprentissage automatique. Si ces techniques peuvent présenter des avantages dans la vie quotidienne, elles peuvent avoir des incidences pour les personnes concernées en les plaçant dans des catégories prédéterminées, très souvent à leur insu. Ce manque de transparence peut présenter des risques importants pour les droits de l'homme, en particulier des personnes vulnérables, dont les enfants.

Cette recommandation, qui actualise un texte de 2010 sur le même sujet, entend aligner ses dispositions sur la « Convention 108 » modernisée sur la protection des données, dite « Convention 108+ ». La recommandation prévoit que le respect des libertés et des droits fondamentaux, notamment les droits au respect de la dignité humaine et de la vie privée, ainsi qu'à la liberté d'expression, le principe de non-discrimination et les impératifs de justice sociale, de diversité culturelle et de démocratie, devrait être garanti dans le secteur public comme dans le secteur privé pendant toutes les opérations de profilage.

PREMS 159621

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 47 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE