Recommandation CM/Rec(2010)13 et exposé des motifs

Instruments juridiques

La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage

Recommandation CM/Rec(2010)13
et exposé des motifs

Publishing
Editions

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage

Recommandation CM/Rec(2010)13
adoptée par le Comité des Ministres
du Conseil de l'Europe
le 23 novembre 2010
et exposé des motifs

Editions du Conseil de l'Europe

Edition anglaise :

The protection of individuals with regard to automatic processing of personal data in the context of profiling (Recommendation CM/Rec(2010)13 and explanatory memorandum)

ISBN 978-92-871-7074-3

Editions du Conseil de l'Europe
F-67075 Strasbourg Cedex
http://book.coe.int

ISBN 978-92-871-7073-6

Imprimé dans les ateliers du Conseil de l'Europe

1. Recommandation CM/Rec(2010)13, adoptée par le Comité des Ministres du Conseil de l'Europe le 23 novembre 2010, sur proposition du Comité européen de coopération juridique (CDCJ).

2. Cette publication contient le texte de la Recommandation CM/Rec(2010)13 et son exposé des motifs.

Recommandation CM/Rec(2010)13

du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage[1]

(adoptée par le Comité des Ministres le 23 novembre 2010, lors de la 1099e réunion des Délégués des Ministres)

Le Comité des Ministres,

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

Constatant que les technologies de l'information et de la communication (TIC) permettent la collecte et le traitement de données à grande échelle, y compris pour les données à caractère personnel, dans le secteur public comme dans le secteur privé ; constatant que les TIC sont utilisées à des fins très diverses, notamment pour des services largement acceptés et appréciés par la société, les consommateurs et l'économie ; constatant par ailleurs que le développement continu de technologies convergentes pose de nouveaux défis en matière de collecte et de traitement ultérieur des données ;

Constatant que la collecte et le traitement peuvent se produire dans différentes situations à différentes fins et concerner différents types de données, telles que les informations sur la circulation et les demandes d'internautes, les habitudes d'achat, activités, mode de vie et comportement des consommateurs, les informations concernant les usagers d'appareils de télécommunication, y compris les données de géolocalisation, ainsi que celles provenant en particulier des réseaux sociaux, des systèmes de vidéo-surveillance, des systèmes biométriques et des systèmes d'identification par radiofréquence (FRID) préfigurant l'« internet des objets » ; constatant qu'il est souhaitable d'évaluer les différentes situations et fins d'une manière différenciée ;

1. Lors de l'adoption de cette recommandation: en application de l'article 10.2.*c* du Règlement intérieur des Délégués des Ministres, la Déléguée du Royaume-Uni a réservé le droit de son Gouvernement de s'y conformer ou non.

Constatant que les données ainsi collectées sont notamment traitées par des logiciels de calcul, de comparaison et de corrélation statistique, dans le but de dégager des profils qui pourraient être utilisés de maintes manières à différentes fins et pour différents usages par l'appariement des données de plusieurs individus ; constatant que le développement des TIC permet de réaliser ces opérations à un coût relativement faible ;

Considérant que, par cette mise en relation d'un grand nombre de données individuelles, mêmes anonymes, la technique du profilage peut avoir des incidences pour les personnes concernées en les plaçant dans des catégories prédéterminées, très souvent à leur insu ;

Considérant que les profils, lorsqu'ils sont attribués à une personne concernée, permettent de générer des nouvelles données à caractère personnel qui ne sont pas celles que la personne concernée a communiquées au responsable de traitement ou dont elle peut raisonnablement présumer la connaissance par le responsable de traitement ;

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 risquent de faire peser de graves menaces sur les droits et libertés de l'individu ;

Considérant en particulier que la protection des droits fondamentaux, et notamment le droit à la vie privée et à la protection des données à caractère personnel, suppose l'existence de sphères de vie différentes et indépendantes où chaque individu peut contrôler l'usage qu'il/elle fait de son identité ;

Considérant que le recours au profilage peut être dans l'intérêt légitime de la personne qui l'utilise comme de celle qui se le voit appliquer, notamment en conduisant à une meilleure segmentation des marchés, en permettant l'analyse du risque ou de la fraude, ou encore en adaptant l'offre à la demande par la fourniture de meilleurs services ; et considérant que le profilage peut donc présenter des avantages pour l'utilisateur, l'économie et la société dans son ensemble ;

Considérant néanmoins que le profilage d'un individu peut avoir pour conséquence de le priver de manière injustifiée de l'accès à certains biens ou services et porte donc atteinte au principe de non-discrimination ;

Considérant par ailleurs que les techniques de profilage, lorsqu'elles mettent en évidence des corrélations entre des données sensibles au sens de l'article 6 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108, ci-après la « Convention n° 108 ») et d'autres données, peuvent permettre de générer de nouvelles données sensibles concernant une personne identifiée ou identifiable ; considérant par ailleurs que ce profilage peut exposer les individus à des risques particulièrement élevés de discrimination et d'atteintes à leurs droits personnels et à leur dignité ;

Considérant que le profilage des enfants peut avoir des conséquences graves pour eux durant toute leur vie et, étant donné qu'ils ne sont pas à même d'exprimer seuls un consentement libre, spécifique et éclairé lors de la collecte de données à caractère personnel à des fins de profilage, il est nécessaire de prendre des mesures spécifiques et appropriées de protection de l'enfance afin de tenir compte de l'intérêt supérieur de l'enfant et du développement de sa personnalité, conformément à la Convention des Nations Unies relative aux droits de l'enfant ;

Considérant que l'utilisation de profils, même de manière légitime, sans précautions ni garanties particulières, est susceptible de porter gravement atteinte à la dignité de la personne de même qu'à d'autres libertés et droits fondamentaux, y compris aux droits économiques et sociaux ;

Persuadé qu'il est donc nécessaire de réglementer le profilage en termes de protection des données à caractère personnel, afin de sauvegarder les libertés et droits fondamentaux des individus, notamment le droit à la vie privée, et de prévenir la discrimination fondée sur le sexe, la race ou l'origine ethnique, la religion ou les convictions, le handicap, l'âge ou l'orientation sexuelle ;

Rappelant à cet égard les principes généraux relatifs à la protection des données de la Convention n° 108 ;

Rappelant que toute personne doit avoir le droit d'accéder aux données la concernant et considérant qu'elle devrait connaître la logique qui sous-tend le profilage ; sachant que ce droit ne devrait pas porter atteinte aux droits et libertés d'autrui, en particulier ne pas nuire aux secrets commerciaux, à la propriété intellectuelle ou au droit d'auteur protégeant les logiciels ;

Rappelant la nécessité de respecter les principes déjà établis par d'autres recommandations pertinentes du Conseil de l'Europe, en particulier la

Recommandation Rec(2002)9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance et la Recommandation Rec(97)18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques ;

Tenant compte de la Convention du Conseil de l'Europe sur la cybercriminalité (STE n° 185 – Convention de Budapest), qui contient des dispositions relatives à la conservation, à la collecte et à l'échange de données, conformément aux conditions et sauvegardes visant à assurer une protection adéquate des droits de l'homme et des libertés ;

Tenant compte à la fois de l'article 8 de la Convention européenne des droits de l'homme (STE n° 5), tel qu'il est interprété par la Cour européenne des droits de l'homme, et des risques nouveaux engendrés par l'utilisation des technologies de l'information et de la communication ;

Considérant que la protection de la dignité humaine et d'autres droits et libertés fondamentaux dans le cadre du profilage ne peut être effective que si, et seulement si, toutes les parties prenantes contribuent ensemble à un profilage loyal et licite des individus ;

Tenant compte du fait que la mobilité des individus, la mondialisation des marchés et l'utilisation des nouvelles technologies nécessitent des échanges d'informations transfrontières, y compris dans le cadre du profilage, et requièrent une protection des données équivalente dans tous les Etats membres du Conseil de l'Europe,

Recommande aux gouvernements des Etats membres :

1. d'appliquer l'annexe à la présente recommandation à la collecte et au traitement des données à caractère personnel utilisées dans le cadre du profilage en prenant notamment des mesures pour que les principes contenus dans l'annexe à la présente recommandation soient reflétés dans leur droit et leur pratique ;

2. d'assurer une large diffusion des principes contenus dans l'annexe à la présente recommandation parmi les personnes, les autorités publiques et les organismes publics et privés, notamment ceux qui concourent ou recourent au profilage, tels que les concepteurs et fournisseurs de logiciels, les concepteurs de profils, les fournisseurs de services de communication électronique et les prestataires de service de la société de l'information,

ainsi que parmi les instances compétentes en matière de protection des données et les organismes de normalisation ;

3. d'inciter ces personnes, autorités publiques et organismes publics et privés à introduire et à promouvoir des mécanismes d'autorégulation, tels que des codes de conduite, qui assurent le respect de la vie privée et la protection des données, et à mettre en place des technologies inspirées de l'annexe à la présente recommandation.

Annexe à la Recommandation CM/Rec(2010)13

1. Définitions

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.

b. L'expression « données sensibles » désigne les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou les autres convictions, et les données à caractère personnel relatives à la santé ou à la vie sexuelle ou concernant des condamnations pénales, ainsi que les autres données définies comme sensibles par le droit interne.

c. Le terme « traitement » recouvre toute opération ou ensemble d'opérations effectués partiellement ou totalement à l'aide de procédés automatisés, et appliqués à des données à caractère personnel, telles que l'enregistrement, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, l'appariement ou l'interconnexion, ainsi que l'effacement ou la destruction.

d. Le terme « profil » désigne un ensemble de données qui caractérise une catégorie d'individus et qui est destiné à être appliqué à un individu.

e. Le « profilage » est une technique de traitement automatisé des données qui consiste à appliquer un « profil » à une personne physique, notamment afin de prendre des décisions à son sujet ou d'analyser ou de prévoir ses préférences, comportements et attitudes personnels.

f. L'expression « service de la société d'information » désigne tout service, fourni normalement contre rémunération, à distance, par voie électronique.

g. L'expression « responsable du traitement » comprend la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou avec la collaboration d'autres, détermine les finalités et les moyens de la collecte et du traitement des données à caractère personnel.

h. Le mot « sous-traitant » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

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, doit être garanti lors de la collecte et du traitement de données à caractère personnel visés par la présente recommandation.

2.2. Les Etats 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, 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.

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.

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. 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. Quand le consentement est requis, il incombe au responsable du traitement de prouver que la personne concernée a accepté le profilage 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. Aux fins d'assurer un consentement libre, spécifique et éclairé au profilage, les prestataires de services de la société de l'information devraient assurer, par défaut, un accès non profilé aux informations relatives à leurs services.

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

3.9. Le responsable du traitement devrait prendre des mesures appropriées pour corriger les facteurs d'inexactitude des données et limiter les risques d'erreurs inhérents au profilage.

3.10. Le responsable du traitement devrait réévaluer périodiquement et dans un délai raisonnable la qualité des données et des inférences statistiques utilisées.

C. Données sensibles

3.11. 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. Tout consentement obligatoire doit être explicite lorsque le traitement porte sur des données sensibles.

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 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 ;
- les effets envisagés de l'attribution du profil à la personne concernée.

4.2. 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.

4.3. 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.

4.4. 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.

4.5. Les dispositions énoncées aux principes 4.2, 4.3 et 4.4 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.

4.6. L'information de 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 ;

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 ;

c. les finalités poursuivies par le profilage effectué et les catégories de personnes ou d'organismes auxquels les données à caractère personnel peuvent être communiquées.

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, la personne concernée n'est pas tenue de formuler un justificatif.

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.

6. Exceptions et restrictions

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

Le droit interne devrait prévoir les sanctions et recours appropriés en cas de violation des dispositions du droit interne donnant effet aux principes de la présente recommandation.

8. Sécurité des données

8.1. Des mesures techniques et d'organisation appropriées devraient être prises 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.

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.

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

8.3. 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.

8.4. 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.

8.5. Des mesures appropriées devraient être mises en place pour éviter que des résultats statistiques anonymes et agrégés utilisés dans le cadre du profilage ne puissent déboucher sur une réidentification des personnes concernées.

9. Autorités de contrôle

9.1. Les Etats 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 Etats membres peuvent prévoir :

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

Exposé des motifs

I. Avant-propos

Le droit à la vie privée comme un droit fondamental

1. Le Conseil de l'Europe, dont le siège se trouve à Strasbourg (France), est la doyenne des organisations politiques européennes. Créé en 1949, il recouvre aujourd'hui la quasi-totalité du continent européen, avec 47 Etats membres.

2. La première et l'une des plus importantes conventions établies par le Conseil de l'Europe est la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, plus communément appelée « Convention européenne des droits de l'homme » (STE n° 5, ci-après « la CEDH »), qui a été ouverte à la signature en 1950. Elle crée la Cour européenne des droits de l'homme (ci-après « la Cour »), juridiction internationale compétente pour statuer sur des requêtes individuelles ou étatiques alléguant des violations des droits civils et politiques, tels qu'énoncés par la CEDH. Ses arrêts ont force obligatoire pour les Etats concernés et, dès lors, conduisent les gouvernements à modifier tantôt leur législation, tantôt leur pratique administrative dans de nombreux domaines.

3. L'article 8 de la CEDH énonce en son premier alinéa : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. » L'alinéa 2 précise qu'il ne peut y avoir d'ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi nationale et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la défense d'un certain nombre de buts légitimes.

4. Sur ce fondement, la Cour a eu l'occasion de préciser, à l'occasion d'arrêts, que les mesures d'ingérence, même si elles visent à protéger la démocratie, ne devraient pas la détruire au motif de la défendre[2]. La Cour a également dégagé une jurisprudence selon laquelle l'article 8 peut engendrer, de surcroît, des obligations positives inhérentes à un « respect » effectif de la vie privée. Conformément à cette théorie dite des « obligations positives »,

2. Arrêt *Malone c. Royaume-Uni* du 2 août 1984, Cour européenne des droits de l'homme (Plénière), n° 8691/79, Série A, paragraphe 82.

l'action de l'Etat consiste alors à mettre en place les mesures nécessaires, y compris législatives, pour garantir le respect concret et effectif des droits découlant de l'article 8 de la CEDH.

5. Ainsi, la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale, consacrée par cet article 8 en vertu duquel la législation nationale se doit de prévoir des garanties appropriées pour empêcher toute utilisation de données à caractère personnel non conforme aux garanties prévues dans cet article et pour assurer la protection efficace des données à caractère personnel enregistrées contre les usages impropres et abusifs[3].

6. La CEDH consacre également, dans son article 10, le droit fondamental à la liberté d'expression. Le droit à la liberté d'expression inclut explicitement la « liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence des autorités publiques et sans considération de frontière ». Cette liberté de recevoir des informations est considérée comme s'étendant à la « liberté de rechercher des informations ». L'exercice de cette liberté de recevoir, de communiquer ou de rechercher des informations à l'aide des technologies d'information et de communication suppose un anonymat car, sans une telle garantie raisonnable, la crainte d'une ingérence de la part des autorités publiques ou de compagnies privées serait légitime, même si cette ingérence se limite à une simple observation et à un enregistrement du comportement des internautes.

La Convention n° 108 et son Protocole additionnel

7. Dans les années qui ont suivi l'adoption de la CEDH, il est apparu de plus en plus nécessaire de développer la protection juridique de la vie privée de manière plus spécifique et systématique par souci d'efficacité et pour faire face à la montée des risques nouveaux d'atteinte à la vie privée nés des technologies de l'information.

8. C'est ainsi que fut élaborée la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108)[4], que l'on nomme « Convention n° 108». Elle fut élaborée en

3. Par ailleurs, dans la Charte des droits fondamentaux de l'Union européenne, le droit à la protection des données à caractère personnel constitue un droit à part avec le droit au respect de la vie privée et familiale.
4. Voir www.coe.int/dataprotection.

même temps que les « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel » de l'Organisation de coopération et de développement économiques (OCDE). Des Etats non membres du Conseil de l'Europe, tels que l'Australie, le Canada, le Japon et les Etats-Unis d'Amérique, ont participé à l'élaboration de la Convention n° 108[5].

9. La Convention n° 108 a été ouverte à la signature le 28 janvier 1981. A la date de l'adoption de la recommandation, 44 Etats membres du Conseil de l'Europe l'ont ratifiée ; d'autres l'ont signée et préparent sa ratification.

10. Elle constitue un instrument juridique contraignant avec une vocation universelle car le Comité des Ministres a affirmé sa volonté d'examiner les demandes d'adhésion provenant des Etats qui ne sont pas membres du Conseil de l'Europe[6].

11. Le 15 juin 1999, le Comité des Ministres a adopté des amendements à la Convention n° 108 pour permettre l'adhésion des Communautés européennes[7].

12. La Convention n° 108 établit des principes applicables au secteur public comme au secteur privé et ayant trait à la qualité des données, au traitement des données sensibles, à la nécessité d'informer la personne concernée, au droit d'accès et de rectification.

13. Elle prévoit également la libre circulation des données à caractère personnel entre les Parties à la Convention. Cette libre circulation ne saurait être restreinte pour les seules raisons de protection des données à caractère personnel. L'objectif de cette disposition est, et reste, de permettre le transfert à l'intérieur d'un périmètre géographique de pays qui offrent un niveau adéquat de protection des données à caractère personnel.

14. Les garanties existantes ont été renforcées par un Protocole additionnel[8] qui prévoit une obligation pour les Parties de se doter d'une ou de plusieurs autorités exerçant un contrôle en toute indépendance, ainsi qu'une obligation de ne pas permettre, en principe, le flux des données à destination

5. Rapport explicatif à la Convention n° 108, paragraphe 15 (ISBN 978-92-871-0442-7).
6. CM(2008)81.
7. CM(98)182.
8. Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181).

de pays ou d'organisations n'offrant pas un niveau de protection adéquat. Le refus de transfert vers un Etat n'offrant pas de garanties adéquates ou vers un Etat tiers, non Partie à la Convention n° 108, est donc possible[9].

Activités normatives du Conseil de l'Europe en matière de protection des données

15. Même si les dispositions de la Convention n° 108, à l'heure actuelle, relèvent de l'ordre juridique interne de la plupart des Etats membres du Conseil de l'Europe, la complexité des questions relatives à la protection efficace des données à caractère personnel – au vu, notamment, de l'apparition constante des nouvelles technologies et des pratiques – appelle une analyse et une solution innovatrices. Face à ces défis, les autorités nationales chargées de la protection des données ou les commissaires à la protection des données se trouvent au premier rang pour aborder ces questions complexes et apporter des solutions appropriées. Les tribunaux contribuent, par ailleurs, à la protection de l'individu face aux atteintes à la vie privée.

16. Le Comité des Ministres a adopté plusieurs recommandations fondées sur la Convention n° 108[10]. Il convient de s'assurer que la collecte et le traitement de données dans un secteur donné (banque, assurance, santé, police

9. Protocole additionnel, article 2.

10. Recommandation Rec(2002)9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance (18 septembre 2002) ;
Recommandation n° R (99) 5 sur la protection de la vie privée sur Internet (23 février 1999) ;
Recommandation n° R (97) 18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques (30 septembre 1997) ;
Recommandation n° R (97) 5 sur la protection des données médicales (13 février 1997) ;
Recommandation n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunications, eu égard notamment aux services téléphoniques (7 février 1995) ;
Recommandation n° R (91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics (9 septembre 1991) ;
Recommandation n° R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes (13 septembre 1990) ;
Recommandation n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi (18 janvier 1989) ;
Recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (17 septembre 1987) ;
Recommandation n° R (86) 1 relative à la protection des données à caractère personnel utilisées à des fins de sécurité sociale (23 janvier 1986) ;
Recommandation n° R (85) 20 relative à la protection des données à caractère personnel utilisées à des fins de marketing direct (25 octobre 1985) ;

etc.) ou effectués à l'aide d'une technique ou d'une technologie particulière (carte à puce, vidéosurveillance, marketing direct), ou encore relatifs à une catégorie particulière de données (sensibles, biométriques, etc.), sont toujours conformes aux principes généraux établis par la Convention n° 108.

17. Ces recommandations s'adressent aux gouvernements de l'ensemble des Etats membres du Conseil de l'Europe. Bien qu'elles ne soient pas juridiquement contraignantes, elles constituent des normes de référence et contiennent une invitation à considérer la possibilité d'adopter et d'appliquer le droit interne conformément à des principes énoncés dans les recommandations.

18. Tout en continuant à reconnaître l'absolue nécessité d'une législation, il convient également de promouvoir, parmi les acteurs de la société de l'information, un régime d'autorégulation visant à rendre plus effective la protection de la vie privée et des données face aux vastes réseaux de télécommunication sans frontières, à la croissance des flux des données personnelles et au développement constant des technologies d'information et de communication.

Les travaux du Conseil de l'Europe sur le profilage

19. En 2008, une équipe d'experts scientifiques a présenté un rapport sur l'application de la Convention n° 108 au mécanisme de profilage[11] lors de la 24e réunion plénière du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après le « T-PD »).

20. Le rapport mettait notamment en avant les pratiques de l'utilisation de nombreuses technologies, telles que les hyperliens transclusifs *(web bugs)* ou les témoins informatiques (« cookies »), potentiellement cumulables et permettant, par nature, l'observation et la traçabilité des individus à leur insu, non seulement par les sites visités mais également par des compagnies

---

(suite note 10)
(Recommandation n° R (83) 10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques (23 septembre 1983) [remplacée par la Recommandation n° R (97) 18] ;
Recommandation n° R (81) 1 relative à la réglementation applicable aux banques de données médicales automatisées (23 janvier 1981) [remplacée par la Recommandation n° R (97) 5].
11. Le rapport peut être consulté sur le site www.coe.int/dataprotection sous la rubrique « Rapports et études T-PD ».

tierces établies en dehors du territoire des Etats membres du Conseil de l'Europe. Le rapport démontrait également que ces pratiques, largement répandues mais peu connues du grand public, étaient potentiellement constitutives d'une atteinte au respect de la vie privée des personnes concernées.

21. La présentation du rapport a été suivie d'une discussion au sein du T-PD, en particulier sur les conclusions du rapport qui plaidait en faveur de l'élaboration d'une nouvelle recommandation en la matière. Lors de sa 1050e réunion le 13 mars 2009, le Comité des Ministres a examiné l'opportunité de mener des travaux dans ce domaine et a chargé le Comité européen de coopération juridique (ci-après le « CDCJ ») de préparer, en coopération étroite avec le T-PD, une recommandation sur le profilage[12]. C'est sur la base de cette décision qu'a été élaboré le projet de recommandation sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage.

22. Le projet de recommandation a fait l'objet d'une consultation publique ayant permis de recueillir les commentaires de plusieurs parties prenantes, telles que des fournisseurs d'accès à internet, des associations de publicitaires en ligne et des représentants d'associations de commerce et de consommateurs. La Commission européenne, la Chambre internationale de commerce et l'Association francophone des autorités de protection des données personnelles ont, entre autres, également contribué aux travaux eu égard à leurs compétences.

23. Le texte a été transmis au CDCJ, qui l'a approuvé lors de sa 85e réunion plénière (11-14 octobre 2010) et l'a par la suite transmis au Comité des Ministres en vue de son adoption.

24. Il est enfin nécessaire de souligner que, au jour de son adoption, la recommandation sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage constitue le premier texte normatif international contenant un ensemble de principes susceptibles d'être appliqués d'une manière générale à tous les traitements des données à caractère personnel ayant recours aux techniques de profilage.

12. CM/Del/Dec(2009)1050/10.6F / 13 mars 2009.

II. Introduction

25. Le concept du « World Wide Web » est apparu au début des années 1990 et s'est développé de manière exponentielle dans tous les pays de la planète. La « toile » a progressivement mis en communication des institutions avec des hommes par le biais de serveurs web. Parallèlement, l'internet a mis en communication les hommes entre eux tout d'abord par le biais du courrier électronique, ensuite par l'intermédiaire des blogs et, plus récemment, par le biais des réseaux sociaux, ce qu'il est convenu d'appeler le web 2.0 ou le web participatif.

26. A l'horizon se profile déjà une nouvelle étape technique du développement des réseaux mondiaux de télécommunication où il ne s'agira plus seulement d'interconnecter les individus entre eux, mais aussi de doter les objets entourant les hommes, dans un premier temps, d'une intelligence logicielle, et, dans un deuxième temps, d'une capacité de communication sur un réseau local relié à internet. Les premières applications de la technologie « Radio Frequency Indentification » (RFID) préfigurent ce que pourra être demain le monde dit de l' « intelligence ambiante ».

27. Ainsi, l'internet de demain ne sera pas seulement une interconnexion des êtres humains entre eux mais aussi une interconnexion des objets devenus « intelligents » (internet des objets) qui entourent le citoyen dans sa vie de tous les jours et accompagnent ses mouvements et les événements quotidiens de sa vie. Dans ce monde ainsi qualifié d' « intelligence ambiante », les objets observeront et analyseront en permanence, et probablement à leur insu, les comportements des êtres humains qui les entourent afin d'interagir avec eux de manière dynamique.

28. On pourrait ainsi imaginer que le téléviseur relié à internet informe le frigo de la date du prochain match de football. Le frigo passerait directement commande du nombre de bières nécessaires, sur la base des consommations de bière antérieures lors du dernier match de football à la télévision. La machine à laver intelligente pourrait, grâce à la lecture des puces RFID incorporées dans les vêtements, trier le linge et adapter son programme de lavage à chaque textile particulier. Le pacemaker pourrait probablement composer un numéro d'urgence après avoir détecté un début de crise cardiaque du sujet et transmettre instantanément la localisation du malade et son dossier médical complet aux services d'urgence.

29. Parallèlement, cette évolution s'accompagne d'une croissance importante des capacités de stockage, de traitement et de communication des données qui permet l'accumulation de données relatives à des groupes plus ou moins larges de population au sein de vastes bases de données et la confrontation aléatoire ou non des données enregistrées, et ainsi de « profiler » des catégories de personnes, de prédire « statistiquement » leurs comportements futurs et de classer tel ou tel individu identifié ou non par rapport à ces profils. Ainsi l'analyse des données du panier d'un client de supermarché se présentant à telle heure dans tel quartier permet d'affirmer que ce panier correspond à tel profil de consommateur ; on en déduit alors a priori qu'il doit être intéressé par telle ou telle offre de produit ou de service.

30. Couplé à l'émergence progressive d'une société d'objets intelligents, connecté à terme au réseau internet et couplé à de nombreux mécanismes diffusés et couramment utilisés (comme les cookies, les *web bugs*, etc.) au niveau mondial sur les sites à grand trafic, le phénomène de profilage sera accentué et rendu permanent. Cette connaissance intime de l'individu, d'une ampleur, d'une ubiquité et d'une efficacité inédites, permettrait non seulement de démarcher chaque individu en particulier en fonction de son profil, mais aussi d'adapter le prix de chaque bien ou service de manière dynamique en fonction de l'élasticité de la demande de chaque personne.

31. L'évolution de ce réseau appelle de nombreuses réflexions. Les applications multiples des technologies décrites présentent indéniablement des avantages importants pour la personne concernée mais elles créent aussi des risques non négligeables d'abus et d'atteintes aux droits et libertés fondamentales. En effet, des acteurs, parmi lesquels certains, déjà bien implantés dans la société de l'information et de la communication, pourraient utiliser ces informations dans leur intérêt propre, à l'insu de la personne concernée et sans offrir de contrepartie équitable. Des garanties appropriées devraient être développées afin de ne pas permettre aux fruits de cette nouvelle société de l'information et de la communication de porter atteinte aux droits et libertés fondamentales de cette même société. Le dispositif de l'information accrue, qui souligne les caractéristiques principales des technologies, permettrait leur utilisation optimale et, en même temps, une meilleure protection des droits des personnes concernées. L'inclusion et l'éducation numériques devraient également jouer un rôle important.

32. Les évolutions techniques récentes permettent aujourd'hui, notamment par l'analyse automatique des trajectoires et des regards, de mesurer

les réponses émotionnelles et les centres d'intérêt des individus, même si ceux-ci n'en sont pas conscients. Des expériences actuellement en cours montrent que le secteur du marketing s'intéresse à cette technique nouvelle de mesure de l'émotion en temps réel.

33. On pourrait aussi souligner les risques de voir les données de santé exploitées par les compagnies d'assurance médicale pour déterminer des tarifs spécifiques et surtout pour exclure certaines personnes de leurs offres. Cette individualisation du traitement des dossiers compromet l'idée même de l'assurance basée sur le partage du risque.

34. Au-delà du secteur du marketing direct, il est possible que la technique de profilage soit développée et utilisée dans d'autres contextes relatifs à l'intérêt public sans, parfois, être visible ou faire l'objet d'une quelconque forme de contrôle ou de protection.

35. On peut ainsi imaginer l'intérêt que posséderait un parti politique, une association ou un groupe d'activistes à pouvoir profiler de manière très fine chacun des électeurs et, éventuellement, à adapter en temps réel la présentation électronique de son programme politique en fonction d'un profil donné. Il serait également techniquement possible qu'un gouvernement ou un groupe d'activistes utilise de manière massive le profilage sur les réseaux de télécommunication, y compris sur les réseaux privés, pour détecter les individus les plus rebelles, les discriminer ou les écarter.

36. Dans le secteur public, la possibilité de corréler des informations en provenance de multiples bases de données utilisant des identifiants uniques permet même de détecter a priori les présumés bénéficiaires de certains avantages sociaux et les personnes suspectées de fraude, ou d'aider, le cas échéant, à la recherche de criminels. Sans doute, cette identification est légitime si elle est accompagnée par les garanties suffisantes qui vont permettre à chacun de contester la « vérité » sortie de l'ordinateur.

37. Au-delà de ces applications dans les secteurs public ou privé, quelques enjeux supplémentaires majeurs relatifs à la collecte des données de plus en plus massives et au profilage encore plus fin qu'elle induit devraient être soulignés. Premièrement, le volume important d'informations propres à un individu et issues des objets intelligents sera tel qu'il permettra l'identification, le traçage et la géolocalisation de chaque individu à tout moment. Dans ce contexte, la possibilité de préserver l'anonymat ou plutôt celle de ne pas appliquer le profil est de plus en plus difficile, voire impossible, d'un

point de vue technique. Deuxièmement, il serait par ailleurs possible, à partir du recoupement d'informations a priori anodines sur un individu transmises par les réseaux, de déduire, avec un taux d'erreur marginal, certaines données sensibles relatives à sa santé, à sa religion, à ses préférences sexuelles ou à son appartenance syndicale.

II.1. Caractéristiques du profilage

38. Le profilage appréhendé dans le cadre de la présente recommandation se déroule en trois étapes techniquement distinctes :

– une étape de collecte et d'entreposage massifs *(data warehousing)* des observations numérisées des comportements et caractéristiques des individus. Ces observations peuvent être nominatives, codées ou anonymes ;

– une étape d'analyse et de « forage » *(data mining)* de ces données permettant l'établissement de corrélations entre certains comportements/caractéristiques et d'autres comportements ou caractéristiques ;

– une étape d'inférence au cours de laquelle, à partir de certaines variables comportementales ou caractéristiques observables propres à un individu généralement identifié, de nouvelles caractéristiques ou variables comportementales présentes, passées ou futures, sont déduites.

39. Il est à noter que les deux premières étapes (entreposage et forage des données) peuvent s'effectuer sur des données anonymisées ou codées. Dans le cas de données anonymisées, il n'est pas techniquement possible d'identifier l'individu concerné par les observations. Si des données codées sont utilisées, un tiers de confiance est capable de procéder à cette identification par décodage. La possibilité, même théorique, d'une capacité de « désanonymisation » des données « anonymes » signifie de facto que ces données ne sont pas anonymisées de manière effective.

40. En règle générale, la troisième étape se déroule par rapport à une personne identifiée ou identifiable et est appliquée comme mentionné ci-dessous, dans des domaines de plus en plus variés et utilisés par un nombre accru d'acteurs.

41. Sans doute est-il important de distinguer la technique de profilage parmi les systèmes d'aide à la décision. Une sélection des individus sur la base de leurs caractéristiques réelles ne constitue pas un profilage. Par exemple, la sélection, par une banque, des clients riches gagnant plus

de 10 000 euros par mois et possédant un patrimoine d'au moins 1 million d'euros constitue une sélection objective qui, au contraire du profilage, n'est pas empreinte d'une marge d'erreur. Techniquement, cette sélection requiert une simple requête sur un serveur *Structured Query Language (SQL)* et ne nécessite pas de forage. Même si le banquier peut parler, dans le langage commun, d'un « profil de client riche », ce type de profilage, qui constitue en fait une sélection de personnes sur base de données exactes qui leur sont propres, n'est pas du profilage, au sens de la présente recommandation. Le profilage, dans le cadre de cette recommandation, nécessite un processus d'extrapolation statistique partiellement exact et donc, aussi, partiellement inexact.

42. Il convient de noter que les pronostics et les techniques criminalistiques et criminologiques, ainsi que les méthodes d'analyse opérationnelle, ne sont pas visés par la présente recommandation dans la mesure où ils ne portent que sur l'établissement d'un phénomène général sur une population et n'impliquent pas l'utilisation de l'information obtenue pour des décisions ou des mesures relatives à une personne déterminée.

43. En ce qui concerne le profilage dans le secteur bancaire, il est utilisé afin de déterminer l'évaluation des risques de leurs clients futurs ou présents *(credit scoring)*. Il s'agit, dans ce contexte, sur la base de l'analyse de milliers ou de millions d'historiques de bons et de mauvais payeurs, de pouvoir identifier les caractéristiques individuelles qui sont corrélées avec le remboursement ou non du crédit. Lors de la conclusion d'un contrat de prêt personnel, la banque posera au candidat emprunteur un certain nombre de questions d'apparence anodine dont les réponses vont permettre de calculer la probabilité, pour un individu déterminé, de rembourser correctement ou non l'argent prêté. On comprend bien, dans le cas précis du *credit scoring*, que la caractéristique de « bon » ou « mauvais » payeur attribuée à un individu est toujours empreinte d'une certaine marge d'erreur. Néanmoins, l'utilisation de ce type de profilage va permettre à la banque de réduire, en moyenne, son risque de mauvaise appréciation de crédit. Ce profilage risque d'aboutir à des erreurs de deux types : octroyer un prêt à une personne qui ne le remboursera pas et refuser un prêt à une personne qui l'aurait remboursé. Ce type d'erreur n'a toutefois pas de conséquences économiques dommageables pour la banque si ces erreurs restent marginales. En d'autres termes, l'utilisation de la technique du profilage peut procurer à des acteurs économiques, des gouvernements ou d'autres institutions diverses des

avantages globaux mais elle crée fatalement des erreurs par rapport à une minorité d'individus et nécessite donc un nombre de précautions à prendre.

44. Un autre exemple du profilage est celui pratiqué dans le cadre de la recherche médicale et relatif à la détection de maladies génétiques. A partir de l'analyse de données génétiques de milliers ou de millions de patients et de données relatives à une maladie génétique particulière, les systèmes de forage sont capables d'établir des corrélations entre la présence ou l'absence de certaines caractéristiques génétiques et une maladie génétique particulière, toujours avec une certaine marge d'erreur. On peut ainsi déduire la propension qu'aurait un patient possédant certaines caractéristiques génétiques de développer cette maladie. Il devient alors possible d'identifier les sujets à risque afin de les inciter à des mesures préventives en vue de diminuer la survenance de la maladie, ou, par exemple, d'augmenter leur prime d'assurance-vie.

45. Dans le domaine fiscal, les administrations publiques recourent dès à présent à des techniques de profilage afin d'identifier les contribuables susceptibles, plus que d'autres, d'éluder l'impôt de manière frauduleuse. Il serait légitime pour l'Etat de procéder à des contrôles ciblés sur base du profilage, étant bien entendu qu'un profil défavorable ne peut équivaloir à une présomption de fraude, mais seulement orienter des enquêtes de l'administration.

46. Dans le domaine commercial, le profilage permet d'adapter le prix d'un bien ou d'un service en fonction du profil du consommateur. Cette capacité technique d'adapter le prix d'un bien ou d'un service en fonction du profil du consommateur est bel et bien réelle. Ce risque est démultiplié sur le réseau internet dans la mesure où le prix d'un même bien ou service est affiché à des endroits différents (sur les écrans des terminaux des consommateurs), contrairement aux magasins où l'étiquette de prix est la même pour tous. Or, l'adaptation du prix en fonction du profil d'un client constitue un traitement de données relatives à ce client et le profilage de la clientèle doit s'opérer au regard des principes de la Convention n° 108. Tirer parti de l'argument que le contexte technologique actuel réduit ce risque menacerait en fait le principe de neutralité technologique que sous-tend la recommandation.

II.2. Comment appliquer les principes de la Convention n° 108 aux activités de profilage

47. A travers les exemples invoqués ci-dessus, il apparaît clairement que, si le développement rapide et l'utilisation des techniques de profilage font

courir des risques nouveaux aux individus, certaines mesures de protection doivent être renforcées et détaillées, de manière à maintenir le niveau de protection des libertés et de la vie privée, tel que préconisé par le Conseil de l'Europe déjà en 1981.

48. Le profilage n'est jamais une finalité au sens de l'article 5 de la Convention nº 108, mais, à l'instar de l'automatisation, il représente un procédé technique permettant au responsable du traitement d'atteindre plus facilement une finalité déterminée. Ainsi, dans les exemples cités ci-dessus, la finalité de la banque est la gestion du risque du crédit, la finalité de la recherche médicale est la prévention des maladies génétiques et la finalité du gouvernement consiste en la lutte contre la fraude fiscale.

49. Le profilage constitue une méthode particulière de traitement des données à caractère personnel permettant au responsable du traitement d'atteindre un objectif. Or l'utilisation de la technique de profilage est en principe intrinsèquement porteuse de certains risques substantiels que nous détaillons ci-après.

II.3. Risques du profilage

Invisibilité des traitements effectués et des données traitées

50. En règle générale, dans les traitements de données classiques n'ayant pas recours au profilage, les données personnelles sont des données exactes et relatives à des individus identifiés ou indentifiables. Dans ce contexte, en général, la personne concernée connaît ou peut subodorer la nature des informations dont le responsable du traitement dispose à son sujet. Dans la mesure où le profilage fait apparaître des données nouvelles pour un individu, à partir de données relatives à d'autres personnes que lui-même, la personne concernée ne peut pas soupçonner a priori l'existence des mécanismes de corrélation qui auraient pour effet de lui attribuer, sur base d'un calcul de probabilités, certaines caractéristiques d'autres individus.

51. Ainsi, par exemple, le client d'une banque ayant eu des incidents de remboursement d'un prêt peut légitimement s'attendre à ce que cette banque lui refuse un nouveau prêt ou lui demande des garanties particulières. Corollairement, le client d'une banque n'ayant jamais eu d'incident de crédit ou même n'ayant jamais bénéficié d'un crédit ne peut pas, a priori, imaginer que la banque, à l'issue d'un formulaire de demande comportant des questions d'apparence anodine, utilise ses réponses, via les techniques

de profilage, pour le ranger dans une catégorie de personnes plus ou moins solvables à laquelle, *stricto sensu*, il n'appartient pas.

52. Les traitements de données ayant recours au profilage présentent a priori une transparence nettement moins grande pour les personnes concernées que d'autres types de traitement de données à caractère personnel. Cela étant, le responsable du traitement doit fournir à la personne concernée une information plus aisément compréhensible lors du profilage et le droit d'accès doit être renforcé, à la fois au regard du fait que ses données sont utilisées en cours du profilage et du fait qu'un profil lui est appliqué.

Opposabilité des données d'autrui

53. Cette manière d'attribuer à un individu particulier des données « à caractère personnel », qui appartiennent en fait à d'autres personnes, crée un phénomène nouveau. En pratique, l'individu est responsable de ses propres actes et se voit imputer de manière sociale ou légale la responsabilité de ceux-ci. Dans le cas du profilage, l'individu se voit attribuer – voire opposer – les données personnelles d'autres individus qu'il ne connaît pas et avec lesquels il ne fait que partager certaines caractéristiques communes. Si un traitement recourant au profilage poursuit une finalité prédictive, il s'agira d'attribuer à une personne identifiée ou identifiable les caractéristiques comportementales d'un groupe présentant certaines caractéristiques communes avec cette personne pour en déduire des caractéristiques nouvelles de la personne concernée. Telle est une des caractéristiques du profilage : il peut créer de nouvelles données à caractère personnel à partir de données relatives à un groupe.

La certitude de l'incertitude

54. Comme le profilage repose sur l'utilisation de statistiques, la probabilité de l'attribution erronée d'une caractéristique particulière à une personne identifiée ou identifiable est réelle. Il est, par exemple, évident qu'une donnée prédictive relative à un individu, extrapolée à partir des données relatives à des comportements antérieurs d'un groupe, ne peut pas, toujours, être correcte. On peut ainsi généralement calculer des taux d'erreurs de premier type ou de deuxième type (premièrement, la probabilité d'inclure une personne dans une catégorie alors qu'elle ne devrait pas y être et, deuxièmement, celle de l'en exclure alors qu'elle devrait y figurer). En matière de *credit scoring*, l'utilisation d'un système de profilage pourrait

aboutir à accorder des prêts à des personnes qui ne les rembourseront pas ou à refuser des prêts à des personnes qui les auraient remboursés. En matière de lutte antiterroriste, l'utilisation de listes noires basées sur des inférences statistiques amènera fatalement au refoulement de passagers non terroristes et n'apporte aucune garantie absolue du refoulement des passagers terroristes. Ces exemples, même s'ils ne permettent pas de douter de la légitimité de la finalité du profilage, démontrent, toutefois, la nécessité de la mise en place de certaines garanties.

55. En pratique, l'usage des techniques de profilage met en péril – de manière normalement marginale, mais néanmoins certaine – l'exactitude des données, telle qu'exigée par l'article 5.*d* de la Convention n° 108. Le profilage devrait respecter le principe de l'exactitude des données. Pour limiter ce risque d'opposer à un individu des données inexactes, il convient, en particulier dans les domaines les plus sensibles, de renforcer les droits d'accès de la personne concernée, non seulement par rapport à ses données, mais aussi par rapport à la logique du traitement des données dont elles font ou ont fait l'objet. Le droit d'opposition doit également être renforcé, dans la mesure où le profilage fait courir à la personne concernée un risque de se voir attribuer des données inexactes.

56. Il sera aussi demandé au responsable du traitement une diligence particulière pour utiliser, dans les deux premières étapes (entreposage de données et forage) des données exactes et à jour, nonobstant le fait que ces données soient relatives à des personnes identifiées ou identifiables. Les algorithmes de forage devront être conçus et testés selon les règles de l'art, de manière à minimiser les risques d'erreur des deux types mentionnés ci-dessus. Dans certains cas, il sera préconisé de recourir à des données anonymes exactes. Dans ce cas, la réglementation du traitement de données anonymes pourrait, de prime abord, apparaître comme une extension du champ d'application de la Convention n° 108. Le profilage a pour effet de créer des nouvelles données à caractère personnel à partir de données anonymes : tant les données (éventuellement anonymes) entreposées, qui servent de matière première à cette création, que le mécanisme de création de ces nouvelles données doivent être conçus, voire adaptés, afin d'aboutir, au terme du processus de profilage, à des données personnelles les plus exactes possibles, conformément à l'article 5.*d* de la Convention n° 108. Dans la mesure où il est évident que la qualité de ces deux ingrédients de base du profilage est décisive pour une exactitude maximale des données

à caractère personnel générées *in fine* au terme du processus de profilage, l'article 5.*d* impose de prendre toutes les mesures de sécurité raisonnables propres à garantir cette qualité.

57. Ainsi, par exemple, si une compagnie d'assurance contre le vol de véhicules module la prime en fonction de l'historique des vols de véhicules dans le quartier de l'assuré, il serait légitime d'exiger de la compagnie d'assurance qu'elle utilise des statistiques récentes et à jour ainsi qu'un programme d'analyse récent et sécurisé, nonobstant le fait que ces données concernant les vols de véhicule seraient des données parfaitement anonymisées. Un dernier argument vient du fait que les trois étapes décrites propres au profilage, même si elles utilisent dans les deux premières étapes des données anonymes, aboutissent, dans la troisième, à une application du résultat à des personnes identifiées ou identifiables. Dans la mesure où les trois étapes sont indissociables, elles doivent toutes être considérées comme participant à un traitement des données à caractère personnel, comme il est expliqué dans le rapport des experts à la base de la présente recommandation.

58. Enfin, au vu des risques induits, les traitements de données ayant recours au profilage doivent être, dans certains domaines sensibles, purement et simplement interdits ou soumis à des conditions particulières. En effet, même si, en général, l'on peut admettre que la personne concernée puisse exercer un droit d'accès ou d'opposition par rapport à l'utilisation du profilage dans des traitements peu sensibles, on ne peut pas conditionner l'accès à des biens et services fondamentaux, comme le droit au logement ou au travail, au seul résultat – parfois erroné – d'un traitement de données ayant recours au profilage. Sans doute, chaque Etat membre aura à se prononcer sur ce point en fonction du contexte et des garanties que pourrait présenter le système de profilage proposé.

Décontextualisation des données

59. Comme mentionné dans le rapport des experts[13], l'obligation de respecter le droit de la personne à la vie privée impose que les responsables de traitement ne traitent des données que d'une seule sphère de sa vie privée. Cela tend à garantir l'étanchéité des différentes sphères de la vie de l'individu et de respecter la finalité de chaque donnée utilisée.

13. *Supra* 12.

60. Donc, le banquier qui souhaite évaluer la solvabilité de quelqu'un ne doit pas se soucier des relations sociales de son client. En d'autres termes, seules les données relatives aux sphères de la vie affectés par la finalité du traitement devraient être prises en compte.

61. Cette division de la vie privée en tiroirs étanches les uns par rapport aux autres ne possède malheureusement aucun pendant technique. Bien souvent la personne concernée possédera les mêmes identifiants (généralement nom, prénom, date de naissance, adresse) dans chacune des sphères. Il est techniquement possible que les techniques de profilage traitent de données recueillies dans différentes « sphères » de la vie privée de l'individu. La mise en œuvre des techniques de forage décrites plus haut permet alors d'établir des corrélations statistiques entre des caractéristiques comportementales appartenant à des sphères disjointes de la vie privée. Il serait donc ainsi possible, par exemple, grâce à l'analyse sur une grande échelle de paniers d'achats anonymes et de caractéristiques relatives à des comportements sexuels, d'identifier des corrélations entre des habitudes d'achat et l'hétérosexualité ou l'homosexualité d'un individu. Cette corrélation peut alors être utilisée de manière logique en sens inverse : à partir du profil d'un panier d'achat, il devient théoriquement possible de présumer avec une certaine marge d'erreur – généralement quantifiable – l'hétérosexualité ou l'homosexualité d'un individu identifié ou identifiable. Cela pour dire que le profilage peut être utilisé pour extrapoler des données sensibles de données qui ne sont pas considérées comme telles, et ce, avec un degré raisonnable de certitude.

62. Ce risque de croisement de données issues de sphères disjointes de la vie privée s'accroît lorsque le profilage s'opère à partir du terminal de télécommunication d'un internaute. En effet, par nature, le terminal n'est pas dédié à une sphère de vie particulière, mais intervient de manière habituelle dans toutes les sphères de la vie d'un individu. Typiquement, un individu sera enclin à utiliser le même terminal pour communiquer avec sa famille, son employeur, ses amis, son médecin, son syndicat, son banquier ou son amant. Ainsi, concrètement, dans le cas de l'utilisation de moteurs de recherche généraux, l'hébergeur du moteur de recherche possède une vision « globale » d'un individu identifié[14]. C'est dire que le terminal joue aujourd'hui

14. Ne fût-ce que temporairement par une adresse IP statique, voire, à plus long terme, par une adresse IPv4 fixe ou une adresse IPv6 dynamique incorporant l'adresse Media Access Control (MAC), à savoir un identifiant de carte réseau, voire encore par le biais d'un cookie rémanent.

un rôle technique crucial et même décisif dans la collecte des données de télécommunication des usagers des réseaux de télécommunication.

63. Le terminal est devenu aujourd'hui un outil, un lieu, dont l'utilisation est génératrice de nombreuses données comportementales et à partir duquel s'opèrent de nombreux traitements de données à caractère personnel relatives à la même personne et concernant des sphères de sa vie privée qui doivent rester techniquement disjointes les unes des autres. C'est pourquoi la recommandation insiste sur la nécessité de réglementer le fonctionnement des terminaux et, notamment, des navigateurs web, ainsi que d'interdire les logiciels qui visent à la surveillance de l'usage d'un terminal ou des réseaux de communication, à moins que cela ne soit prévu par le droit interne assorti des garanties appropriées[15].

64. Le rappel du principe de la proportionnalité et du caractère loyal du traitement des données justifie également les limites posées à la collecte de données n'ayant aucun lien avec la finalité première du traitement.

III. Commentaires sur les dispositions de la recommandation

III.1. Préambule

65. Le préambule énonce les considérations qui ont amené le Comité des Ministres à adresser la recommandation aux gouvernements des Etats membres.

66. Dans le contexte de la présente recommandation, le Comité des Ministres constate que le développement constant des nouvelles technologies de l'information et de la communication (volume des données stockées et transmises, rapidité de calcul et sophistication des algorithmes de traitement) permet aujourd'hui, dans un premier temps, de collecter et de traiter divers types de données à caractère personnel relatives à plusieurs individus et, dans un deuxième temps, d'interconnecter ces données entre elles à des fins d'établissement de profils.

67. Il observe, par ailleurs, que les usages multiples de ces nouvelles technologies présentent indéniablement des avantages importants pour

15. Article 5, 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).

la personne concernée ; elles créent néanmoins des risques non négligeables, radicalement nouveaux, d'abus et d'atteintes aux droits et libertés fondamentales. En effet, le recours au profilage est souvent opéré à l'insu des individus concernés et risque dès lors de porter atteinte à la loyauté du traitement des données dans la mesure où la personne concernée ignore l'existence ou la logique du profilage dont elle fait l'objet. Dans ce cas, elle ne peut ni comprendre la logique du traitement sous-jacent, ni exercer un droit d'accès ou d'opposition à ce traitement.

68. Il reconnaît l'importance qu'il y a, dans le domaine de l'utilisation des techniques de profilage, de promouvoir et de garantir la protection des données à caractère personnel, notamment la protection des données sensibles telle que le prévoit l'article 6 de la Convention n° 108.

69. Finalement, le Comité des Ministres définit comme objectif de cette recommandation l'établissement de procédures appropriées qui garantissent que la collecte et le traitement des données à caractère personnel relatifs au profilage se font dans le respect des droits et libertés fondamentales des individus et qui, en particulier, assurent un équilibre approprié entre le recours au profilage et le droit au respect de la vie privée. L'initiative du Comité des Ministres est rendue nécessaire dans un contexte de mobilité des individus et de mondialisation du marché, contexte qui exige une protection équivalente des individus dans tous les Etats membres du Conseil de l'Europe.

70. Cette recommandation s'appliquera sans préjudice de l'application d'autres normes légales. En particulier, l'article 8 de la CEDH garantit le droit au respect de la vie privée des personnes physiques, qu'elles soient ou non identifiables, et la Convention sur la cybercriminalité (STE n° 185) interdit l'accès non autorisé à un système d'information, peu importe que ce système soit constitué par le serveur d'une entreprise ou par le terminal d'un utilisateur identifiable ou non.

III.2. Dispositif de la recommandation

71. La question du champ d'application s'est posée lors de la rédaction de la recommandation. La solution tendant à limiter le champ d'application à la collecte et au traitement des données à caractère personnel dans le cadre du profilage circonscrit au secteur privé a été aussitôt écartée. Premièrement, une telle distinction aurait soulevé des difficultés pour circonscrire les notions de secteur privé et de secteur public dans une société

où les autorités publiques ont de plus en plus recours à une délégation des tâches, dont ils étaient investis initialement, au profit des sociétés privées. On pourrait citer l'exemple d'une société privée, chargée du transfert de détenus, qui a recours aux techniques de profilage.

72. Deuxièmement, une réglementation du profilage se limitant au secteur privé uniquement aurait été discriminatoire en créant une distorsion de concurrence entre les acteurs qui concourent ou recourent au profilage. De plus, cette distinction aurait conduit à l'affaiblissement de la protection des personnes concernées, le profilage conduisant souvent à l'allocation de droits ou à l'attribution de bénéfices à celles-ci. Il est évident que les risques liés au profilage opéré par le secteur public – même si ce profilage peut s'appuyer sur des raisons légitimes souvent évidentes (lutte contre la fraude fiscale ou sociale, identification de personnes susceptibles de bénéficier d'aides particulières, etc.) – sont importants dans la mesure où ces profilages peuvent viser des catégories importantes de la population, entraîner des décisions ayant un impact important sur les individus profilés négativement et recourir à des données nombreuses en provenance de l'ensemble des administrations.

73. Troisièmement, la distinction secteur privé/public ne figure pas dans les dispositions de la Convention n° 108, notamment parce que ces notions peuvent avoir une signification différente d'un pays à l'autre et peuvent dépendre du régime spécifique attribué par un Etat à un secteur d'activité donné.

74. Les gouvernements des Etats membres sont donc encouragés à appliquer les principes contenus dans l'annexe à la recommandation à toute collecte et tout traitement des données à caractère personnel utilisées dans le cadre du profilage.

75. Toutefois, la possibilité d'une dérogation était prévue en suivant l'exemple d'autres instruments juridiques du Conseil de l'Europe. En effet, comme le prévoit le chapitre 6, les Etats ont la possibilité de ne pas appliquer les dispositions des chapitres 3, 4 et 5 pour raison de sécurité publique, de prévention ou de répression des infractions pénales (lutte contre la criminalité de manière générale, activités liées au renseignement, etc.), ou d'intérêts monétaires de l'Etat, ce qui s'entend notamment des mesures de lutte contre la fraude fiscale ou sociale. Les raisons de ces dérogations peuvent également avoir trait à la protection de la personne concernée et

des droits et libertés d'autrui. Ces dérogations sont fondées sur l'article 9 de la Convention n° 108.

76. Le chapitre 6 rappelle cependant, conformément à l'article 8, paragraphe 2, de la CEDH, que les dérogations doivent être prévues par la loi et constituer une mesure nécessaire dans une société démocratique. La Cour a élaboré une jurisprudence riche pouvant contribuer à l'interprétation et à l'application pratique de ce chapitre (notamment au regard des définitions prévues par la loi et d'une mesure nécessaire dans une société démocratique).

77. Par ailleurs, il est recommandé aux gouvernements des Etats membres de prendre des mesures pour que les principes contenus dans l'annexe soient reflétés dans leur droit et dans leur pratique.

78. Les gouvernements sont également encouragés à diffuser largement le contenu de l'annexe à la recommandation parmi les personnes, les autorités publiques, les organismes publics et privés – notamment ceux qui concourent ou recourent au profilage, tels que les instances compétentes en matière de protection des données –, les associations de protection des consommateurs ou de promotion des libertés civiles, et les organismes de normalisation.

79. Ils sont invités à encourager, pour autant que cela concerne des opérations de profilage, la définition et la promotion des codes de conduite au service du respect de la vie privée, moyennant par exemple la mise en place de technologies inspirées de l'annexe à la recommandation.

III.3. Annexe à la recommandation CM/Rec(2010)13

1. Définitions

80. Le chapitre 1 établit les définitions de certains concepts centraux de la recommandation.

81. Les expressions « responsable du traitement » et « sous-traitant » ont déjà été définies dans le cadre d'autres exposés des motifs de recommandations sectorielles spécifiques adoptées par le Comité des Ministres[16] dans le

16. Exposés des motifs de la Recommandation Rec(2002)9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance, et de la Recommandation n° R (97) 18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques.

domaine de la protection des données et, pour ce motif, ne nécessitent pas d'explication supplémentaire dans le cadre de cette recommandation.

82. « Données à caractère personnel » : la définition, qui a déjà été utilisée dans d'autres recommandations, est conforme à celle de la Convention n° 108, telle qu'interprétée dans le rapport explicatif de celle-ci. Toutefois, il est nécessaire d'apporter quelques précisions à cette définition, eu égard à la question particulière du profilage.

83. La Convention n° 108 limite son champ d'application aux seules données à caractère personnel puisque ce type de données, contrairement aux données anonymes, permet techniquement aux responsables de traitement, pour chaque individu identifié ou identifiable, d'utiliser un identifiant comme clé d'accès à cet individu dans d'autres traitements de données à caractère personnel.

84. Ainsi, par exemple, la mention de l'identité « civile » d'un individu (nom, prénom, adresse) sur un ticket de caisse permettrait à un supermarché d'accéder à des sources de données externes (annuaire, moteur de recherche, des services de cartographie en ligne) et de connaître d'autres informations relatives aux clients. Dans le contexte actuel, on ne saurait cependant réduire cette notion d'identité aux seuls nom et adresse. Le numéro unique délivré automatiquement à ses clients ou à ses visiteurs virtuels par une entreprise, un groupe d'entreprises ou un opérateur autorise également cette recherche et ces connexions. Ainsi, un simple numéro de client permettrait techniquement aux supermarchés de connaître, vis-à-vis d'un client particulier, non seulement le contenu de son panier d'achat du jour, mais aussi l'historique complet de ses achats antérieurs, voire, si la carte est munie d'une puce RFID, l'historique des parcours du client dans ce magasin. Dans le cadre du profilage, de nombreuses caractéristiques individuelles décrivent le comportement des individus. A partir du moment où ces caractéristiques sont nombreuses et précises, il devient possible d'identifier chaque individu en particulier sur la base du comportement qui lui est propre et unique. Dans le cadre du profilage, un individu n'est véritablement anonyme que si la valeur des données recueillies à son sujet n'est pas unique – en d'autres termes, si deux individus différents dans un contexte donné possèdent les mêmes caractéristiques. Ainsi, par exemple, parmi une foule de clients, les caractéristiques « porte des lunettes solaires et un chapeau jaune » ne permettront pas d'identifier un individu particulier si, et seulement si, dans

cette foule se trouvent deux personnes différentes portant chacune des lunettes solaires et un chapeau jaune.

85. D'autre part, à suivre des considérations sociologiques, psychologiques, voire philosophiques, on peut se demander si la combinaison de multiples caractéristiques comportementales relatives à un individu ne constitue pas son identité. La définition de « données à caractère personnel » par la Directive européenne 95/46 CE le laisse entendre lorsqu'elle considère qu'est réputée identifiable une personne qui peut être identifiée, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Ne serait-ce pas la combinaison d'un nombre important de caractéristiques individuelles qui identifierait (au sens commun) un individu, même si cet individu partage ces caractéristiques avec d'autres ? Dans le cadre de la recommandation, il est considéré que les données sont à caractère personnel si les caractéristiques relatives à une personne physique, peu importe leur nature (physique, physiologique, culturelle, économique, sociale), sont uniques dans le traitement des données prises en considération.

86. « Données sensibles » : la définition reprend la liste énoncée à l'article 6 de la Convention n° 108. Toutefois, conformément à l'article 11, d'autres catégories – telles que les données sur l'appartenance syndicale ou le revenu – peuvent être définies comme sensibles par le droit interne. Par ailleurs, peuvent être considérées comme étant sensibles les données qui, n'ayant pas été expressément définies comme telles, reçoivent néanmoins de la part d'un Etat un haut niveau de protection.

87. « Personne identifiable » : une personne est dite identifiable lorsqu'elle peut être identifiée par l'utilisation de moyens disponibles, peu importe que cette utilisation implique ou non le recours à un tiers. A l'inverse, la donnée est anonyme si l'identification n'est possible que moyennant le recours à des activités déraisonnables[17].

88. « Activités déraisonnables » : ce sont des opérations excessivement longues, coûteuses et compliquées pour le responsable du traitement ou une tierce partie au regard de leurs activités normales. Elles se rapportent, notamment, à des moyens techniques dont on dispose afin d'identifier les

17. Voir aussi paragraphe 26.*b* de l'exposé des motifs de la Recommandation Rec(2002)9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance.

données et de percer leur anonymat. De la sorte, compte tenu des progrès rapides des technologies et des méthodes informatiques, les délais et les efforts pour identifier une personne qui seraient aujourd'hui considérés comme « déraisonnables » pourraient ne plus l'être à l'avenir.

89. « Traitement » : l'article 2.*c* de la Convention n° 108 stipule que la notion de « traitement automatisé » s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion.

90. Le rapport explicatif de la Convention n° 108 précise à son paragraphe 31 que, « en raison de l'évolution rapide de la technologie du traitement des données, il a été jugé opportun de donner du " traitement automatisé " une définition assez générale et susceptible d'une interprétation flexible. » En effet, cette définition a démontré au cours des années sa flexibilité et sa capacité à être appliquée à de nouvelles situations et technologies. Dans cette optique, il conviendrait de mettre en relief certaines de ces nouvelles situations et de montrer de quelle manière elles tombent dans le champ de la définition du traitement automatisé et ainsi, dans la mesure où les autres conditions d'application de la Convention n° 108 sont remplies, dans le champ de la Convention n° 108.

91. « Collecte » : même si la notion de collecte de données à caractère personnel n'est pas mentionnée dans la définition du traitement automatisé à l'article 2.*c* de la Convention n° 108, elle est mentionnée à côté du traitement dans un certain nombre de recommandations ultérieures. Pour cette raison, cela réaffirme que la notion de traitement automatisé doit être interprétée comme comprenant la notion de collecte réalisée en vue d'un traitement automatisé.

92. Cette interprétation s'applique quelle que soit la façon dont la collecte est réalisée : la collecte des données peut être réalisée par des moyens automatiques ou manuellement, le point essentiel étant que des opérations de traitement automatisé soient appliquées à ces données. De même, les collectes réalisées à l'aide de moyens technologiques tels que des webcams ou des téléphones mobiles, dans la mesure où elles sont liées à d'autres opérations de traitement au sens de l'article 2.*c* de la Convention n° 108, font partie de la notion de traitement automatisé au sens de la convention.

93. « Communication » : ce terme recouvre toute forme de mise à disposition de données à un tiers et, notamment, la transmission, la diffusion et l'interconnexion. Il peut s'agir d'une mise à disposition active en réponse à une demande individuelle ou globale d'un tiers. Il peut également s'agir d'une mise à disposition passive par l'autorisation donnée à un tiers d'avoir accès en ligne à des données à caractère personnel[18].

94. Il a été décidé de maintenir la référence explicite à ce concept dans le texte de la recommandation car cela contribue à une meilleure compréhension de certains principes (par exemple l'obligation d'informer au stade de la collecte).

95. « Profil » : il constitue un ensemble de caractéristiques propres à un groupe d'individus et, corollairement, à chaque individu appartenant au groupe. Ainsi le panier d'achat d'un parent au foyer, les données de géolocalisation des personnes assistant à un match de football et les transactions bancaires d'un investisseur dynamique sur le marché boursier sont caractéristiques en ce sens qu'ils sont propres aux groupes de personnes analysées. Le panier d'achat type du parent au foyer ne sera pas celui d'un étudiant ; les déplacements d'un supporter d'un club de football ne seront pas ceux d'une personne se rendant à son travail et les transactions bancaires d'un spéculateur en bourse ne correspondront pas au profil de l'investisseur « bon père/mère de famille », qui ne spécule pas sur le marché boursier. Le profilage consiste à appliquer à un individu particulier le profil d'un groupe auquel les données collectées à son propos permettent de l'identifier. Cette opération aura pour effet de créer de nouvelles caractéristiques relatives à l'individu identifié ou identifiable ainsi profilé. Ainsi, en examinant un panier d'achat, il serait possible d'identifier un parent au foyer ayant deux enfants en bas âge et friands de chocolat ; en observant des données de géolocalisation, on pourra identifier le fait qu'une personne est supporter d'un club de football particulier et est prête à faire tous les déplacements même lointains pour suivre son équipe ; et en analysant les transactions bancaires, il serait possible d'attribuer un profil de risque particulier à un investisseur. Le profilage crée donc de nouvelles données à caractère personnel. A l'instar de l'automatisation ou des systèmes d'aide à la décision, le profilage n'est pas une finalité au sens de la Convention n° 108 mais plutôt une modalité technique qui permet d'atteindre une finalité, qui peut être,

18. Si la communication implique le transfert transfrontière, des dispositions supplémentaires seront appliquées.

suivant les cas, par exemple, la lutte contre la fraude, le marketing ou le recrutement de travailleurs.

96. « Profilage » : une opération de profilage comporte trois étapes. La première étape consiste à collecter sur une grande échelle des données relatives à des comportements individuels. Il peut s'agir d'un panier d'achat, d'un relevé de télécommunications, d'une liste de déplacements dans les transports publics, etc. Les données relatives à ces comportements individuels peuvent être anonymisées ou codées.

97. Dans une deuxième étape, ces données résultant d'observations individuelles font l'objet d'une analyse par ordinateur permettant de corréler certaines caractéristiques de comportements. Grâce à des outils et algorithmes statistiques, il devient ainsi possible d'identifier des liens entre certains comportements. Ni le bon sens humain, ni la logique humaine n'interviennent lors de l'établissement de ces corrélations. C'est bel et bien la puissance de calcul de l'ordinateur et la sophistication des algorithmes utilisés qui permettent de mettre à jour des corrélations souvent invisibles à l'œil nu ou inaccessibles à la raison humaine, sans toutefois les expliquer. Ainsi, quel lien peut-on faire a priori entre la consommation de chocolat, la résidence dans telle cité et la capacité de rembourser un crédit ? Par ailleurs, les méthodes statistiques utilisées établissent un coefficient de probabilité de la corrélation ainsi mise à jour.

98. Dans une troisième étape, la corrélation ainsi établie est appliquée à une personne identifiée ou identifiable afin de déduire, avec une certaine marge d'erreur, certaines de ses caractéristiques passées, présentes ou futures. Cette application présente cependant toujours un risque d'erreur qui justifie la recommandation prise. Comme il a été expliqué dans l'introduction, l'individu se voit en effet attribuer certaines caractéristiques présentes ou futures qui ne sont pas les siennes et qui ne font pas partie de son histoire personnelle, mais qui sont celles d'un groupe auquel il est ou sera censé appartenir plus au moins probablement.

99. Le texte entend répondre à l'objection suivant laquelle la recommandation excéderait l'objet même de la Convention n° 108 dans la mesure où cette recommandation couvre ou plutôt pourrait couvrir, au moins dans les étapes 1 et 2, des traitements de données à caractère non personnel, c'est-à-dire des données anonymisées. Comme expliqué dans l'introduction, à cette objection il est répondu que cette recommandation doit porter, ne

serait-ce qu'accessoirement, sur la collecte et le traitement de données anonymes dans la mesure où le traitement de ces données anonymes dans les étapes 1 et 2 conditionne de manière décisive la légitimité ou la sécurité du traitement lors de la troisième étape et que les trois étapes constituent, en réalité, un processus continu. Ainsi, par exemple, ne sera-t-il pas superflu d'exiger des responsables de traitement d'utiliser des données anonymes exactes, intègres et mises à jour lors de la première étape d'entreposage des données. Et cela même si, a priori et en principe, la Convention n° 108 ne porte pas sur des données anonymes. En fait, d'une certaine manière, la substance même de ces données anonymes peuvent se retrouver, a posteriori et de manière inattendue, dans le profil d'une personne identifiée ou identifiable, par le biais du profilage.

100. « Service de la société de l'information » : cette définition correspond à celle de la Convention du Conseil de l'Europe sur l'information et la coopération juridique concernant les « Services de la société de l'information » (STE n° 180) et de la Directive 98/48/CE portant modification de la Directive 98/34/CE prévoyant une procédure d'information dans le domaine des normes et réglementations techniques, en vigueur dans les Etats membres de l'Union européenne.

101. Aux fins de la présente définition :

– « à distance » signifie un service fourni sans la présence simultanée et physique des parties ;

– « par voie électronique » signifie un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fil, par radio, par moyens optiques ou par d'autres moyens électromagnétiques ;

– « à la demande individuelle d'un destinataire de service » signifie un service fourni par transmission de données à la suite d'une demande individuelle. Les services non sollicités, c'est-à-dire les services fournis sans avoir été demandés individuellement, ne sont donc pas couverts.

102. En outre, les « services de la société de l'information » qui rentrent dans le champ d'application de la recommandation sont normalement fournis contre rémunération. Cela concerne la rémunération directe et indirecte. Un service fourni sans contrepartie économique ou sociétale directe, mais

financé directement ou indirectement par le marketing, rentre dans cette définition de « services de la société de l'information ».

2. Principes généraux

103. Lors de la rédaction du texte de la recommandation, il est apparu nécessaire de souligner un certain nombre de principes ayant un caractère général et n'ayant pas comme but la création d'obligations légales. Ces dispositions servent à éclairer l'interprétation et la mise en œuvre d'autres dispositions de l'annexe.

104. Le principe 2.1 rappelle que les opérations de collecte et de traitement des données à caractère personnel opérées dans le cadre de l'utilisation de méthodes de profilage doivent respecter les libertés et droits fondamentaux des individus, et en particulier leur droit au respect de la vie privée et l'interdiction de la discrimination.

105. Ce principe affirme que, au-delà de la stricte application de la Convention n° 108, il importe d'être attentif de manière plus large à la façon dont les techniques de profilage peuvent porter atteinte à la vie privée, entendue comme la capacité d'autodétermination des individus. Ainsi, il se peut que le profilage publicitaire particulièrement ciblé, même conforme aux lois de protection des données, constitue une limitation indue des capacités de choix de l'individu.

106. Le principe de la non-discrimination n'est pas perçu, dans le cadre de la recommandation, comme une interdiction d'un traitement différencié. En effet, la différence dans le traitement des individus, comme conséquence du profilage, est acceptée à condition d'être justifiée.

107. Cette approche est conforme à la position adoptée par la Cour dans sa jurisprudence relative à l'article 14 de la CEDH qui a affirmé à maintes reprises qu'une distinction est discriminatoire uniquement si elle « manque de justification objective et raisonnable », c'est-à-dire si elle ne poursuit pas un « but légitime » ou s'il n'existe pas de « rapport raisonnable de proportionnalité » entre les moyens employés et le but visé. Par ailleurs, les Etats jouissent d'une certaine marge d'appréciation pour déterminer si et dans quelle mesure des différences entre des situations à d'autres égards analogues justifient des distinctions de traitement.

108. Sans doute, le profilage permet, et c'est son objectif, de différencier les utilisateurs d'un service ou les citoyens. Ainsi, il permet d'offrir aux

personnes la publicité appropriée à leurs besoins, de calculer le coût d'un produit en fonction des caractéristiques et de la qualité du consommateur ou, précisément, de réserver le bénéfice d'avantages sociaux aux personnes identifiées a priori comme relevant d'un certain profil. De telles utilisations du profilage peuvent être considérées comme légitimes. Ce qui est proscrit, c'est le recours à des techniques de profilage conduisant à des effets négatifs, arbitraires et contraires à la loi, ainsi le refus d'un service ou d'un produit à des personnes a priori profilées comme étrangères ou ne partageant pas l'opinion philosophique du fournisseur ou profilées comme ayant ou devant avoir un passé judicaire, sans que le critère mis en avant par le profilage ne soit justifié ou en lien pertinent avec la qualité ou les caractéristiques du produit ou du service.

109. Le principe 2.2 *a* un double contenu. Le premier point se retrouve déjà dans certains textes de l'Union européenne et concerne la promotion de ce qu'il est coutume d'appeler des technologies renforçant la protection de la vie privée *(privacy enhancing technologies or ¨privacy by design¨)*. Il s'agit notamment de promouvoir des logiciels permettant aux internautes de pouvoir s'opposer ou de consentir[19], le cas échéant, de manière éclairée ou explicite, à la collecte de données à des fins de profilage ; ou permettant l'accès, voire la correction, par la personne concernée, du profil qui lui est attribué. Certains logiciels vont permettre une plus grande transparence et donner les moyens d'éduquer les utilisateurs.

110. Le second point est plus novateur et consiste à introduire, dans le domaine de la protection des données le même principe que celui déjà appliqué en matière de protection de la propriété intellectuelle. Il s'agit d'encourager les mesures appropriées contre le développement et la mise en œuvre de toute technologie qui aurait pour but de contourner l'efficacité des mesures visant à protéger le respect de la vie privée. Il ne peut être admis par exemple que, par des *web bugs* ou trous de sécurité dans les logiciels d'un prestataire de service, la société de l'information ou les experts puissent collecter des données alors même que la personne concernée avait souhaité se protéger contre ce traitement en installant des logiciels nouveaux ou en paramétrant des logiciels existants.

19. Voir l'avis 2/2010 du Groupe de travail « Article 29 » sur la protection des données sur la publicité comportementale en ligne, notamment, l'analyse des caractéristiques d'un consentement.

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

A. Licéité

111. Les principes 3.1, 3.2 et 3.3 énoncent les principes essentiels, découlant de l'article 5 de la Convention n° 108, et l'appliquent aux traitements utilisant la méthode du profilage. Par exemple, l'utilisation d'une telle technique doit être loyale et licite, ce qui interdit la collecte de données par des moyens non transparents ou pour des finalités non avouées. Ainsi, par exemple, les données collectées en ayant utilisé des moteurs de recherche ne devraient pas être utilisées dans le cadre de systèmes de profilage à des fins publicitaires sans que la personne concernée n'en soit avertie ou que le consentement préalable ne soit obtenu, ainsi que reflété au principe 3.4. La licéité du profilage peut être contestée lorsque le profilage poursuit un but discriminatoire. Enfin, l'utilisation de méthodes de profilage devrait être mise au service de la poursuite de buts spécifiés et légitimes.

112. Le principe 3.2 souligne la nécessité du caractère adéquat des données traitées. Cet alinéa mérite plusieurs commentaires. Par définition, le profilage travaille sur des inférences statistiques non prévisibles a priori. Ainsi, si on traite de la consommation de chocolat et que l'on découvre une inférence entre cette consommation et le goût pour des destinations lointaines, faudra-t-il dire a posteriori qu'il s'agit – statistiquement du moins – d'une donnée pertinente à celui qui veut vendre des voyages exotiques, alors qu'elle ne l'était point a priori ? Le Conseil de l'Europe estime que la pertinence doit s'apprécier de manière plus large certes, mais en toute hypothèse elle doit exclure des données dont la nature ne présente a priori aucun lien avec le résultat attendu. En d'autres termes, si le but est la vente d'un produit de grande consommation, il n'est pas pertinent de s'interroger sur la réussite scolaire des personnes concernées, sur leur possession d'un poisson rouge, ou leur lecture d'Astérix. L'utilisation de telles données dans le cadre des opérations de *data mining* peut certes révéler des corrélations mais celles-ci sont opérées hors contexte de l'utilisation normale de telles données, et cette utilisation heurte les prévisions raisonnables de la personne à qui on oppose un profil construit sur de telles données. Le caractère loyal du traitement s'y oppose donc.

113. Le principe 3.3 applique aux traitements utilisant des méthodes de profilage le principe de conservation limitée des données stockées. La limitation de l'utilisation d'un profil appliqué à une personne ne devrait pas excéder

la période nécessaire à l'accomplissement des finalités pour lesquelles la donnée est collectée et traitée. Cette règle devrait tenir compte de l'intérêt du maintien dans le temps des données collectées à propos d'un individu de manière à faire évoluer le profil de celui-ci. Ainsi, si un grand magasin obtient mon consentement pour m'envoyer de la publicité en fonction de mon profil d'acheteur, il importe que les données relatives à mes achats puissent être conservées tout au long de mon contrat avec le fournisseur. Par ailleurs, quand la relation contractuelle n'existe pas et que le consentement a été dûment obtenu afin d'envoyer de la publicité fondée sur le profil d'achat de la personne concernée, il conviendrait de recommander que les données ayant trait à l'achat soient sauvegardées pour une durée limitée (par exemple 12 mois, comme le souligne le programme de loyauté en Italie).

114. Le principe 3.4 porte sur l'application des conditions générales de licéité au processus du profilage. Il est à noter que le principe 3.4 s'applique au processus de profilage en tant que tel et non à la finalité qui recourt à ce processus. Ainsi, si le recours à une technique de profilage a lieu dans le cadre d'opérations de marketing, en sus des conditions de légitimité qui entourent le traitement à des fins de marketing, le principe 3.4 ajoute des conditions de légitimité propres à l'utilisation dans le cadre de ce traitement marketing de techniques de profilage. Ainsi, si l'Etat est légitimement habilité à lutter contre la fraude, faudra t-il encore prévoir qu'il soit habilité à créer des *data warehouses* et employer des techniques de *data mining*.

115. L'alinéa *a* concerne de façon spécifique des situations dans lesquelles le profilage est prévu par la loi, notamment la détection de personnes à risque, de potentiels fraudeurs ou de personnes devant bénéficier d'avantages sociaux. L'expression « si la loi le prévoit » signifie que le droit interne contient des règles qui prévoient expressément les dispositions et les sauvegardes ou les exceptions aux principes considérés dans la recommandation. Pour satisfaire l'exigence imposée par « si la loi le prévoit », une ingérence aux libertés et droits fondamentaux, et notamment à la vie privée des personnes, doit donc avoir une base légale en droit interne et avoir été commise en conformité avec celle-ci[20].

116. L'expression « si la loi le prévoit » devrait recouvrir deux cas de figure. Premièrement, la loi peut prévoir le profilage en réglementant la possibilité

20. Paragraphe 50, exposé des motifs à la Recommandation n° R (97) 18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques.

– et non l'obligation – de profiler. Par exemple, les services fiscaux sont habilités à contrôler les revenus des citoyens si une fraude est suspectée. Il est important que la réglementation en matière d'impôts prévoie la possibilité d'utiliser les méthodes du profilage pour détecter ces cas et réglemente l'utilisation de ces techniques de profilage. Cela ne signifie pas que les autorités fiscales vont utiliser ces possibilités.

117. Deuxièmement, le profilage peut être nécessaire pour le respect d'une obligation légale et, dans ce cas, l'utilisation des techniques de profilage doit être rendue possible par la loi. L'obligation légale peut rendre le profilage nécessaire afin que le responsable du traitement puisse se conformer à la loi. Un exemple pourrait concerner la législation relative au blanchiment d'argent. Les banques sont tenues de détecter des opérations qui pourraient être considérées comme du blanchiment d'argent et, de ce fait, sont habilitées par la loi à utiliser les mécanismes du profilage.

118. Dans ces cas, où le profilage est nécessaire pour assurer le respect d'une obligation légale, le recours aux techniques de profilage ne serait admis que si ce recours est prévu par la loi.

119. L'alinéa *b* concerne spécifiquement le profilage à caractère facultatif. Dans ces cas, le profilage doit être « autorisé » par la loi. L'expression « si la loi l'autorise » se rapporte au profilage conforme aux principes de cette recommandation, qui n'est pas explicitement interdit par le droit interne. En outre, le principe 3.4.*b* précise que le profilage puise sa légitimité dans :

– le consentement libre, spécifique et éclairé de la personne concernée. Le consentement peut être utilisé comme une base légale pour le profilage. Le consentement, comme base légale de profilage, n'a pas reçu de portée indépendante mais a été délibérément placé parmi les principes de licéité pour laquelle une condition préalable commune (ne pas être explicitement interdite par la loi) devrait être remplie. Cela tend à couvrir les hypothèses, connues dans certains Etats, où le recours au profilage est illégal même si le consentement de la personne concernée a été obtenu au préalable. Le consentement doit être libre, spécifique et éclairé[21]. Par exemple, sur internet, le consentement peut se faire en

21. Voir le 16e considérant de la recommandation : « Rappelant que toute personne doit avoir le droit d'accéder aux données la concernant et considérant qu'elle devrait connaître la logique qui sous-tend le profilage ; sachant que ce droit ne devrait pas porter atteinte aux droits et libertés d'autrui, en particulier ne pas nuire aux secrets commerciaux, à la propriété intellectuelle ou au droit d'auteur protégeant les logiciels ».

cliquant sur un bouton d'acceptation (« j'accepte »). Dans d'autres cas, l'information peut être implicite, notamment en procurant un hyperlien vers une page qui détaillera la technique de profilage utilisée pour le traitement. Il convient de souligner que le consentement pourrait également être donné par le représentant légal de la personne concernée (par exemple le parent d'un enfant mineur) ;

– l'exécution d'un contrat conclu avec la personne concernée. Il s'agit ici d'utiliser le profilage dans le cadre de l'exécution d'un contrat ou de l'application de mesures précontractuelles. En outre, ce contrat pourrait avoir été conclu à la suite de la demande de la personne concernée. On peut inclure l'exemple du profilage effectué par une banque lors de la demande d'un prêt personnel afin d'évaluer la solvabilité probable d'un emprunteur. Il convient de noter que c'est l'utilisation de la technique de profilage qui doit apparaître nécessaire pour l'exécution du contrat ou de l'application de mesures précontractuelles ;

– l'exécution d'une tâche d'intérêt public ou d'une obligation légale. Ainsi, par exemple, une banque pourrait être amenée à devoir profiler ses clients, à la suite d'une obligation légale de dénoncer des mouvements d'argent suspects à des organismes gouvernementaux chargés de la lutte contre le blanchiment d'argent et d'utiliser la technique du profilage pour arriver à cette fin ;

– 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. Un exemple pourrait être l'utilisation du profilage afin de détecter la possibilité d'une fraude par une compagnie d'assurance dans le cas d'un contrat d'assurance. Les difficultés proviennent de l'interprétation de ce que pourrait être un « intérêt légitime » et de leur mise en balance avec les libertés et droits fondamentaux des personnes concernées. Dans ce cas, la préoccupation ultime ne serait pas tant le risque supplémentaire que la technique de profilage fait courir, mais un test général de la légitimité, de la proportionnalité et de la sécurité du traitement. Ainsi l'utilisation du profilage à des fins de marketing est soumise à un double critère de légitimité : « la finalité de marketing est-elle légitime ? » et, si oui, « est-il légitime, pour atteindre cette légitimité, d'utiliser des techniques de profilage ? » ;

– la sauvegarde de l'intérêt vital de la personne concernée. On pourrait ainsi, par exemple, songer au cas d'un profilage génétique effectué sur les membres d'une même famille afin d'identifier des prédispositions à contracter certaines maladies. Cela permettrait alors un traitement préventif par rapport aux membres de la famille dont la vie serait menacée. Cependant, ces cas demeurent des cas exceptionnels.

120. Le principe 3.5 recommande d'interdire en principe le profilage de personnes ne pouvant librement exprimer leur consentement, en particulier, par exemple, les personnes atteintes d'incapacité ainsi que les enfants, au sens de la Convention des Nations Unies relative aux droits de l'enfant. Il est considéré qu'une telle interdiction de principe est nécessaire au vu des risques de manipulation et de discrimination négative que représente le profilage par rapport à ces catégories de personnes. L'interdiction peut être levée par les Etats membres lorsque l'utilisation du profilage poursuit l'intérêt légitime des personnes concernées (ainsi, pour la prévention d'un danger particulier dont ces personnes doivent être averties, ou pour le bénéfice d'une aide dont elles ont spécifiquement besoin) ou dans le cadre d'un intérêt public consacré par la loi et prévoyant des garanties appropriées.

121. Le principe 3.6 stipule que, quand le consentement de la personne concernée est requis, c'est au responsable du traitement de démontrer qu'il a totalement satisfait à son obligation d'information dont le contenu est détaillé dans le chapitre 4.

122. Le principe 3.7 porte sur l'accès anonyme aux biens et aux services, et rappelle le principe dit de « minimalisation » des données à caractère personnel. En particulier sur internet, l'individu qui souhaite s'informer par rapport à des biens et services, ou y avoir un accès, ne devrait, a priori, donner aucune autre information que les caractéristiques de ces biens et services. L'identification, qui permettrait d'assurer la sécurité d'une transaction, ne devrait survenir qu'au moment où l'individu passe une commande et pour l'exécution de celle-ci. L'accès aux informations relatives aux biens et services devrait donc, autant que possible, consister en un accès anonyme et non profilé. Sachant qu'il est techniquement possible de faire varier l'information disponible en fonction de l'utilisateur, un accès non profilé d'un individu à l'information en ligne est également une condition préalable à l'exercice efficace de la liberté d'expression.

123. Le principe 3.8 recommande que ne soient pas autorisées la diffusion et l'utilisation de logiciels visant l'observation ou la surveillance de l'usage d'un terminal ou de réseaux de communication et qui permettraient ainsi la collecte de données et le recours à des méthodes de profilage, et ce à l'insu des personnes concernées, à moins que le droit interne ne le stipule expressément et ne prévoit des garanties appropriées. Ainsi, on peut difficilement accepter que, grâce à des trous de sécurité des logiciels proposés sur le marché, certains puissent s'introduire dans l'ordinateur d'un individu ou simplement surveiller toutes ou certaines utilisations du terminal ou du réseau, de manière à constituer des profils d'internaute.

124. Le texte proposé ne vise pas d'autres opérations concernant le traitement de communications par des entreprises privées qui, comme la plupart des Etats membres le prévoient déjà, enregistrent des communications électroniques lorsque cet enregistrement est opéré dans le cadre d'une pratique d'affaires légitime, afin de permettre, par exemple, la preuve d'une transaction commerciale ou non.

125. Dans le contexte technique actuel, l'utilisateur d'internet et des réseaux de communication en général est suivi et profilé par le biais de technologies peu transparentes, notamment par des systèmes de *web bugs* et de *cookies*. Comme nous l'avons analysé plus haut, le profilage opéré en utilisant le terminal de télécommunication pose un problème important de légitimité puisque l'utilisateur se voit ainsi profilé dans les sphères de vie privée a priori distinctes mais auxquelles il accède par le biais de ce même terminal. Actuellement, des entreprises multinationales parviennent à capter sur une base individuelle une partie importante du « flot de clics » (*click stream*) de chaque internaute et peuvent ainsi constituer des profils individuels « globaux », c'est-à-dire touchant à de nombreux domaines de la vie de l'individu. Techniquement, ce type de profilage effectué par le terminal ne peut être régulé que si les fabricants des terminaux de télécommunication et les opérateurs du réseau mettent en place des mesures techniques qui empêchent la surveillance du comportement des utilisateurs et la transmission des profils en découlant à des tiers non autorisés. Ce principe n'empêche pas le profilage en ligne, mais incite l'industrie de l'information et de la communication à produire des terminaux les plus transparents possible. Ce principe fait écho au principe 2.3 énoncé plus haut.

B. Qualité des données

126. Les principes 3.9 et 3.10 demandent au responsable du traitement de faire toute diligence afin d'effectuer un profilage de qualité. Cela signifie, par exemple, qu'il serait amené à utiliser des données tant anonymes que personnelles qui soient exactes et à jour, et, d'autre part, que les règles d'inférence mises en évidence lors du *data mining* devraient présenter un taux d'erreur négatif ou positif le plus bas possible. Ainsi, il ne serait pas convenable pour une banque d'utiliser un système de profilage de mauvais payeurs en se basant sur des observations trop anciennes ou inexactes. Dans ce cas, en effet, les profils qui seraient finalement attribués aux personnes identifiées seraient vraisemblablement empreints d'une très grande marge d'erreur. Les algorithmes utilisés durant la phase de *data mining* doivent être choisis et utilisés en conformité avec les règles de l'art en la matière. Enfin, le responsable du traitement qui utilise de tels systèmes doit réévaluer périodiquement la pertinence des profils générés. Ainsi, il peut apparaître que la consommation de chocolat n'est plus considérée comme un facteur statistiquement corrélable au goût pour les voyages lointains.

127. Il faut noter que l'exactitude des données est une exigence concomitante en matière de protection des données. Cette disposition n'impose pas une surveillance quant à l'exactitude des données anonymes. Il s'agit de corriger des facteurs d'inexactitude dans la mesure où les trois étapes du profilage, dont l'application de la corrélation établie à une personne identifiée ou identifiable, constituent un processus continu. Cette exigence doit être interprétée d'une manière raisonnable par rapport à la finalité du traitement des données, car il est évident que l'impact des inexactitudes sur la personne identifiée ou identifiable ne serait évidemment pas le même si on parle, par exemple, du secteur de l'assurance ou du marketing direct.

C. Données sensibles

128. Le principe 3.11 stipule que le traitement de données sensibles dans le cadre du profilage ne peut s'effectuer que si le droit interne prévoit des garanties appropriées. Ce principe découle de l'article 6 de la Convention n° 108 qui prévoit, d'une manière non exhaustive, que les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé, à la vie sexuelle et à des condamnations pénales

ne peuvent être traitées automatiquement que moyennant des garanties appropriées prévues par le droit interne.

129. Quant au caractère légitime des exceptions à l'utilisation de données sensibles dans le cadre du profilage, elles devraient être prévues par le droit interne des Etats membres. Ainsi, par exemple, dans tous les Etats de l'Union européenne ayant transposé la Directive 95/46/CE, la liste des exceptions prévue à l'article 8 de ladite directive se trouve circonscrite dans leurs législations nationales.

130. Quant aux garanties appropriées et légitimes, celles-ci peuvent consister, par exemple, dans le consentement de la personne concernée ou dans l'encadrement par une loi du processus de profilage envisagé, afin de maintenir la confidentialité des données traitées ou résultant de l'opération de profilage, et de veiller à ce que l'utilisation des profils soit strictement réservée aux seuls traitements qui sont légitimes. Par ailleurs, le principe prévoit expressément la condition de consentement explicite au profilage lorsque celui-ci porte sur des données sensibles et requiert ainsi un consentement.

4. Information

131. Le principe 4.1 énonce les éléments d'information à fournir aux personnes concernées par le responsable du traitement et concerne deux cas de figure particuliers : la situation où les données collectées sont immédiatement utilisées en vue d'un profilage et la situation où le profilage intervient à un stade ultérieur à la collecte, mais toujours avec l'intention initiale de recourir au profilage. Le recours à des méthodes de profilage ne peut pas être dissimulé à la personne concernée, et le responsable du traitement devrait utiliser tous les moyens raisonnables (information sur le site, etc.) pour informer les personnes concernées de l'existence du profilage et de leurs droits. Cette information doit être rapide et tirer parti des potentialités des technologies de l'information et de la communication. En particulier, lorsque le profilage a lieu en ligne, ces technologies permettent une information immédiate de la personne concernée.

132. Toutefois, il est nécessaire d'indiquer que les modalités et l'étendue de cette information devraient être appropriées et adaptées aux circonstances. Aussi, il est considéré que divers moyens et formes de communication pourraient être utilisés lorsque la nature ou l'ampleur de l'opération du profilage le requièrent. De même, il est reconnu que l'information sur l'existence du recours à des méthodes de profilage pourrait, par sa nature, constituer une

charge disproportionnée pour le responsable du traitement, compte tenu de toutes ses caractéristiques possibles et des circonstances ainsi que des limites propres au moyen de communication utilisé. La terminologie utilisée et les degrés de précision de l'information devraient toutefois être de nature à permettre à la personne concernée de comprendre aisément, mais seulement dans les grandes lignes, les objectifs et l'importance du profilage. Par ailleurs, le responsable du traitement n'est pas soumis à l'obligation d'information si la législation nationale encadre le processus de profilage.

133. Une distinction devrait être faite entre une obligation d'informer de la finalité pour laquelle le profilage est effectué (4.1.*b*) et les effets envisagés de l'attribution du profil à la personne concernée (4.1.*f*, dernier alinéa). Par exemple, la finalité d'un *credit scoring* est d'évaluer la solvabilité de la personne concernée, alors que l'effet envisagé du profilage sera un octroi ou non d'un crédit ou l'octroi d'un crédit plus onéreux, etc. Les effets envisagés d'attribution d'un profil ne sont pas toujours prévisibles au moment de la collecte des données, ni au moment de l'application du profil. C'est pourquoi cette garantie a été introduite dans le principe 4.1.*f* qui concerne les garanties laissées à la discrétion des Etats membres. Par ailleurs, l'application de ces garanties devrait se faire d'une manière appropriée au regard des circonstances en l'espèce.

134. Les principes 4.2 et 4.3 distinguent deux situations dans lesquelles la personne concernée devrait recevoir l'information visée au principe 4.1, en fonction de ce que les données sont collectées directement ou non auprès d'elle. Le principe 4.3 s'est inspiré directement de l'article 11 de la Directive 95/46/CE.

135. Le principe 4.4 consacre une garantie supplémentaire au regard du principe 4.1. Comme mentionné précédemment, le profilage est un procédé technique permettant d'atteindre une finalité. Les données enregistrées sans une intention initiale de recourir au profilage pourraient être ensuite utilisées dans le cadre du profilage. Si le responsable du traitement décide d'utiliser les données pour une finalité différente de celle pour laquelle les données ont été initialement collectées, cela devrait être considéré comme étant une nouvelle collecte et un nouveau traitement. Par conséquent, le responsable du traitement devrait être tenu de fournir à la personne concernée les informations citées au principe 4.1, par exemple au moment de l'application du profil.

136. Le principe 4.5 détaille les situations dans lesquelles les dispositions énoncées aux principes 4.2, 4.3 et 4.4 ne s'appliquent pas.

137. Le principe 4.6 établit un principe de bon sens. La façon dont la personne concernée est avertie du recours à des méthodes de profilage variera suivant le contexte de l'application de la méthode de profilage. Ainsi une fenêtre surgissant *(pop-up)* peut avertir l'internaute que les bannières publicitaires qu'il reçoit sont le résultat d'un profilage. On peut imaginer qu'il en soit autrement lorsqu'une personne reçoit la visite de contrôleurs du fisc à la suite d'un profilage des contribuables.

5. Droits des personnes concernées

138. Le principe 5.1 précise que la personne concernée devrait pouvoir connaître les données à caractère personnel la concernant et la logique qui a servi de base au profilage. En effet, il est crucial d'informer la personne concernée, lors de l'exercice du droit d'accès, des méthodes et des inférences statistiques qui ont servi à son profilage, de la logique sous-tendant le traitement des données et des conséquences envisagées de l'attribution d'un profil.

139. Par ailleurs, si le profilage comporte de nouveaux risques, il devrait être entouré par des garanties spécifiques visant à les pallier.

140. Sans la compréhension de ces éléments, l'exercice efficace d'autres garanties – le droit d'opposition ou le droit de déposer une plainte auprès d'une autorité compétente – ne peut être envisageable.

141. Par exemple, si une personne reçoit une offre pour une assurance contre les dégâts des eaux, elle devrait être informée de la logique du calcul du prix de cette offre. Le profilage de son risque provient-il d'une statistique ? Quels sont les éléments la concernant qui ont été pris en considération pour le calcul de la prime d'assurance ? Ce n'est qu'en ayant ces éléments que la personne concernée pourra, le cas échéant, formuler une opposition motivée.

142. Une information sur la logique qui sous-tend le traitement ne devrait pas être limitée aux cas impliquant des décisions automatisées, car ces dernières ne sont pas la seule finalité du profilage. Les Etats peuvent étendre cette obligation à plusieurs hypothèses sans, toutefois, entraîner des efforts démesurés pour le responsable du traitement et sans qu'il soit porté une atteinte

aux droits et libertés d'autrui, en particulier aux secrets commerciaux[22]. La personne concernée n'est pas a priori fondée à obtenir la communication des données anonymes ayant servi au profilage. Par ailleurs, le responsable du traitement ne serait tenu de fournir que l'information qui sera suffisante pour comprendre les conséquences possibles de l'attribution d'un profil.

143. Le principe 5.2 est inspiré par l'article 8.*c* de la Convention n° 108 et prévoit la possibilité pour la personne concernée d'obtenir la rectification, l'effacement ou le verrouillage de ses données à caractère personnel, selon les cas.

144. Le principe 5.3 recommande de garantir à la personne concernée, sauf exceptions, le droit de s'opposer à l'utilisation de ses données dans le cadre de profilage à des fins de marketing. Ainsi, si une personne souhaite que la publicité qu'elle reçoit sur l'internet ne puisse pas être ciblée en fonction de son profil ou que le choix des sites proposés à sa consultation ne soit pas dicté par l'utilisation de son profil, elle devrait pouvoir s'y opposer sans donner de raisons particulières. Le droit de s'opposer au profilage lorsque celui-ci n'est pas effectué dans un but de marketing exige de la personne concernée la mise en avant de raisons prépondérantes et légitimes. Ainsi, celui qui s'est vu refuser un crédit parce que la localisation de son domicile, l'absence d'abonnement téléphonique et l'instabilité d'emploi constituent, cumulés, des indices statistiques de son incapacité de remboursement, pourra s'opposer à l'utilisation d'un tel profil en démontrant que le changement d'emploi était dû à des faillites successives de ses différents employeurs qui l'ont contraint à un déménagement hâtif justifié par un nouvel emploi, déménagement qui explique l'absence d'abonnement téléphonique.

145. Le principe 5.4 prévoit toutefois des garanties supplémentaires contre le recours arbitraire aux limitations aux droits énoncés dans le présent chapitre.

146. Il convient de noter que certains droits, tels que le droit de l'individu d'obtenir l'information relative aux données le concernant, peuvent être limités si les raisons citées au chapitre 6 existent (sécurité d'Etat, sûreté publique, etc.). Voir par exemple l'article 6 de la Recommandation n° R (87) 15 visant à

22. Voir le 16e considérant de la recommandation : « Rappelant que toute personne doit avoir le droit d'accéder aux données la concernant et considérant qu'elle devrait connaître la logique qui sous-tend le profilage ; sachant que ce droit ne devrait pas porter atteinte aux droits et libertés d'autrui, en particulier ne pas nuire aux secrets commerciaux, à la propriété intellectuelle ou au droit d'auteur protégeant les logiciels ».

réglementer l'utilisation de données à caractère personnel dans le secteur de la police et l'article 17 de la Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

147. Dans ce cas, les décisions motivées du refus ou de la limitation des droits devraient être communiquées à la personne concernée par tous les moyens permettant d'en garder une trace. Toutefois, la communication des motifs peut ne pas avoir lieu dans les cas où elle pourrait mettre en péril l'objectif même dans lequel cette restriction a été imposée.

148. L'origine de ce principe tient compte de la difficulté de l'exercice des diverses tâches dont un Etat est investi, notamment dans le domaine policier et du maintien de l'ordre. Une approche équilibrée devrait permettre leur exercice effectif sans dépouiller les individus de leurs droits. Par exemple, les droits en question ne peuvent être limités qu'aussi longtemps que perdure le motif de la limitation. Il convient de s'assurer que les raisons constitutives de limitation d'accès aux données sont prévues par la loi et nécessaires dans une société démocratique. La nécessité d'une telle décision, dans une société démocratique, implique l'existence d'un « besoin social impérieux » et la proportionnalité par rapport au but légitime poursuivi. Il importe de veiller à ce que les motifs avancés pour le refus ou la limitation d'accès ne servent à détourner les garanties établies en faveur de la personne concernée. Enfin, si aucune raison pour le refus ou la limitation n'a été communiquée à l'individu, les voies possibles de contestation de cette décision devraient lui être exposées.

149. Le principe 5.5 vise le cas où le recours au profilage permet à lui seul la prise d'une décision ayant des effets juridiques sur la personne concernée (exemple : telle personne a-t-elle en fonction de son profil droit à tel avantage social ?) ou affectant cette dernière de manière significative (ainsi, telle personne en fonction de son profil n'est pas digne d'un crédit de x euros). Ce principe donne à la personne concernée un droit d'opposition à la décision. Ce principe reçoit des exceptions chaque fois que la loi prévoit le recours à cette méthode ou que la décision ainsi prise est opérée dans le cadre de l'exécution d'un contrat ou de mesures précontractuelles (sous réserve du respect des principes relatifs à la licéité du profilage, à la qualité des données et du droit à l'information), le recours au profilage pour des décisions d'embauche est possible moyennant des garanties appropriées permettant

à la personne concernée de faire valoir son point de vue, en particulier au cours d'un entretien où elle aura l'opportunité de démontrer l'inexactitude de données entrant dans son profil, l'inadéquation du profil à sa situation particulière, voire d'autres arguments.

6. Exceptions et restrictions

150. Le chapitre 6 est inspiré directement de l'article 9 de la Convention n° 108 (inspiré lui-même par la deuxième partie des articles 6, 8, 10 et 11 de la CEDH) et définit les dérogations autorisées aux principes énoncés dans les chapitres 3, 4 et 5. La jurisprudence de la Cour se livre à un examen détaillé des motifs de dérogation, notamment la notion de « mesure nécessaire » susceptible de varier en fonction des situations. En prévoyant la faculté d'exceptions, la recommandation adopte une approche équilibrée en laissant aux Etats une marge de manœuvre dans les circonstances dûment justifiées.

151. Le chapitre 2 n'est pas cité dans le chapitre 6 car, comme mentionné ci-dessus, ce chapitre n'a pas pour but d'instaurer des obligations légales pouvant faire l'objet de dérogations.

7. Recours

152. Le chapitre 7 prévoit l'existence de recours appropriés pour la personne concernée en cas de violation des dispositions réglementaires donnant effet aux principes de la recommandation. Ces recours supposent l'intervention d'une autorité indépendante, qu'il s'agisse d'une instance judiciaire ou d'une autorité indépendante au sens du Protocole additionnel à la Convention n° 108, c'est-à-dire disposant de moyens d'investigation et pouvant ordonner des sanctions appropriées.

8. Sécurité des données

153. Le principe 8.1 porte sur les mesures techniques et d'organisation qui devraient être prises pour assurer la sécurité des données. La voie légale est une des voies de la mise en œuvre de la recommandation. D'autres voies pourraient être envisagées, ayant trait à la mise en place des procédures et des politiques internes dans la mesure où il ne suffit pas d'édicter des règles juridiques pour assurer une pleine protection des données à caractère personnel ; des précautions matérielles doivent aussi être prises par le responsable du traitement pour prévenir tout incident de traitement survenu accidentellement ou par malveillance.

154. Le principe 8.2 stipule qu'il incombe au responsable du traitement de mettre en place les mesures techniques et d'organisation mentionnées ci-dessus.

155. Le principe 8.3 prévoit comme garantie supplémentaire que les responsables du traitement qui recourent à des techniques de profilage présentant des risques particuliers pour les personnes concernées, et ce au regard de divers critères (nature des données traitées, impact de la décision prise ou des effets du profilage, caractère du réseau de collecte, etc.), seraient tenus, si nécessaire, de recourir à la nomination au sein de leur organisation d'une personne au statut garantissant son indépendance et chargée de veiller au respect des principes de la Convention n° 108 et de cette recommandation, et que cette personne détachée à la protection des données personnelles pourrait donner un avis sur les mécanismes de profilage mis en œuvre par un responsable du traitement.

156. La nomination d'une telle personne ne fait pas obstacle à la nomination par le responsable du traitement d'un correspondant spécialisé, ce dernier pouvant avoir des compétences plus étendues.

157. Le principe 8.4 prévoit que, dans le cas d'une sous-traitance des opérations de profilage à un tiers, le responsable du traitement devrait prévoir des garanties appropriées afin de s'assurer que son sous-traitant respecte bel et bien les conditions de licéité et de sécurité détaillées dans l'annexe à la recommandation[23].

158. Le principe 8.5 prévoit une garantie supplémentaire contre l'utilisation abusive possible des résultats statistiques utilisés dans le cadre du profilage. Cette exigence est fondée sur la Recommandation n° R (97) 18 qui définit les conditions de la licéité de la collecte et du traitement des données à caractère personnel aux fins statistiques et, notamment, son principe 3.3 qui exige que les données à caractère personnel soient rendues anonymes dès qu'elles ne sont plus nécessaires sous une forme identifiable.

9. Autorités de contrôle

159. Le principe 9.1 dispose que les Etats membres devraient charger une ou plusieurs autorités indépendantes de veiller au respect de l'application

23. Voir également l'Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant » du Groupe de travail « Article 29 » .

du droit interne mettant en œuvre les principes énoncés dans la recommandation. L'autorité indépendante, ainsi que l'étendue de ses moyens d'investigation et d'intervention, relèvent des dispositions du Protocole additionnel à la Convention nº 108[24].

160. Le principe 9.2 prévoit la possibilité d'introduire une obligation de notification ou un contrôle préalable par l'autorité de contrôle indépendante citée au principe 9.1. Il convient de souligner que ce principe n'a pas pour but d'imposer aux Etats membres la mise en place d'une obligation légale, mais prévoit de telles possibilités au cas où le traitement des données à caractère personnel ayant recours au profilage présenterait des risques spécifiques et particuliers pour la protection de la vie privée. Dans des cas où le responsable du traitement prévoit les mesures appropriées, par exemple l'avis d'un détaché à la protection des données, il est loisible pour les Etats membres d'exempter le responsable du traitement de cette obligation de notification ou de contrôle préalable.

161. Enfin, le principe 9.3 prévoit que ces autorités informent le public, par exemple dans leurs rapports annuels, du contenu de la recommandation et l'éduquent à la prise de conscience des risques liés au profilage.

24. Voir le rapport explicatif sur l'article 1, paragraphe 2.*a*, du Protocole additionnel à la Convention nº 108.

Sales agents for publications of the Council of Europe
Agents de vente des publications du Conseil de l'Europe

BELGIUM/BELGIQUE
La Librairie Européenne -
The European Bookshop
Rue de l'Orme, 1
BE-1040 BRUXELLES
Tel.: +32 (0)2 231 04 35
Fax: +32 (0)2 735 08 60
E-mail: info@libeurop.eu
http://www.libeurop.be

Jean De Lannoy/DL Services
Avenue du Roi 202 Koningslaan
BE-1190 BRUXELLES
Tel.: +32 (0)2 538 43 08
Fax: +32 (0)2 538 08 41
E-mail: jean.de.lannoy@dl-servi.com
http://www.jean-de-lannoy.be

BOSNIA AND HERZEGOVINA/
BOSNIE-HERZÉGOVINE
Robert's Plus d.o.o.
Marka Maruliça 2/V
BA-71000, SARAJEVO
Tel.: + 387 33 640 818
Fax: + 387 33 640 818
E-mail: robertsplus@bih.net.ba

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street
CDN-OTTAWA, ONT K1J 9J1
Tel.: +1 613 745 2665
Fax: +1 613 745 7660
Toll-Free Tel.: (866) 767-6766
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

CROATIA/CROATIE
Robert's Plus d.o.o.
Marasovièeva 67
HR-21000, SPLIT
Tel.: + 385 21 315 800, 801, 802, 803
Fax: + 385 21 315 804
E-mail: robertsplus@robertsplus.hr

CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE
Suweco CZ, s.r.o.
Klecakova 347
CZ-180 21 PRAHA 9
Tel.: +420 2 424 59 204
Fax: +420 2 848 21 646
E-mail: import@suweco.cz
http://www.suweco.cz

DENMARK/DANEMARK
GAD
Vimmelskaftet 32
DK-1161 KØBENHAVN K
Tel.: +45 77 66 60 00
Fax: +45 77 66 60 01
E-mail: gad@gad.dk
http://www.gad.dk

FINLAND/FINLANDE
Akateeminen Kirjakauppa
PO Box 128
Keskuskatu 1
FI-00100 HELSINKI
Tel.: +358 (0)9 121 4430
Fax: +358 (0)9 121 4242
E-mail: akatilaus@akateeminen.com
http://www.akateeminen.com

FRANCE
La Documentation française
(diffusion/distribution France entière)
124, rue Henri Barbusse
FR-93308 AUBERVILLIERS CEDEX
Tél.: +33 (0)1 40 15 70 00
Fax: +33 (0)1 40 15 68 00
E-mail: commande@ladocumentationfrancaise.fr
http://www.ladocumentationfrancaise.fr

Librairie Kléber
1 rue des Francs Bourgeois
FR-67000 STRASBOURG
Tel.: +33 (0)3 88 15 78 88
Fax: +33 (0)3 88 15 78 80
E-mail: librairie-kleber@coe.int
http://www.librairie-kleber.com

GERMANY/ALLEMAGNE
AUSTRIA/AUTRICHE
UNO Verlag GmbH
August-Bebel-Allee 6
DE-53175 BONN
Tel.: +49 (0)228 94 90 20
Fax: +49 (0)228 94 90 222
E-mail: bestellung@uno-verlag.de
http://www.uno-verlag.de

GREECE/GRÈCE
Librairie Kauffmann s.a.
Stadiou 28
GR-105 64 ATHINAI
Tel.: +30 210 32 55 321
Fax.: +30 210 32 30 320
E-mail: ord@otenet.gr
http://www.kauffmann.gr

HUNGARY/HONGRIE
Euro Info Service
Pannónia u. 58.
PF. 1039
HU-1136 BUDAPEST
Tel.: +36 1 329 2170
Fax: +36 1 349 2053
E-mail: euroinfo@euroinfo.hu
http://www.euroinfo.hu

ITALY/ITALIE
Licosa SpA
Via Duca di Calabria, 1/1
IT-50125 FIRENZE
Tel.: +39 0556 483215
Fax: +39 0556 41257
E-mail: licosa@licosa.com
http://www.licosa.com

NORWAY/NORVÈGE
Akademika
Postboks 84 Blindern
NO-0314 OSLO
Tel.: +47 2 218 8100
Fax: +47 2 218 8103
E-mail: support@akademika.no
http://www.akademika.no

POLAND/POLOGNE
Ars Polona JSC
25 Obroncow Street
PL-03-933 WARSZAWA
Tel.: +48 (0)22 509 86 00
Fax: +48 (0)22 509 86 10
E-mail: arspolona@arspolona.com.pl
http://www.arspolona.com.pl

PORTUGAL
Livraria Portugal
(Dias & Andrade, Lda.)
Rua do Carmo, 70
PT-1200-094 LISBOA
Tel.: +351 21 347 42 82 / 85
Fax: +351 21 347 02 64
E-mail: info@livrariaportugal.pt
http://www.livrariaportugal.pt

RUSSIAN FEDERATION/
FÉDÉRATION DE RUSSIE
Ves Mir
17b, Butlerova.ul.
RU-117342 MOSCOW
Tel.: +7 495 739 0971
Fax: +7 495 739 0971
E-mail: orders@vesmirbooks.ru
http://www.vesmirbooks.ru

SPAIN/ESPAGNE
Díaz de Santos Barcelona
C/ Balmes, 417-419
ES-08022 BARCELONA
Tel.: +34 93 212 86 47
Fax: +34 93 211 49 91
E-mail: david@diazdesantos.es
http://www.diazdesantos.es

Díaz de Santos Madrid
C/Albasanz, 2
ES-28037 MADRID
Tel.: +34 91 743 48 90
Fax: +34 91 743 40 23
E-mail: jpinilla@diazdesantos.es
http://www.diazdesantos.es

SWITZERLAND/SUISSE
Planetis Sàrl
16 chemin des Pins
CH-1273 ARZIER
Tel.: +41 22 366 51 77
Fax: +41 22 366 51 78
E-mail: info@planetis.ch

UNITED KINGDOM/ROYAUME-UNI
The Stationery Office Ltd
PO Box 29
GB-NORWICH NR3 1GN
Tel.: +44 (0)870 600 5522
Fax: +44 (0)870 600 5533
E-mail: book.enquiries@tso.co.uk
http://www.tsoshop.co.uk

UNITED STATES and CANADA/
ÉTATS-UNIS et CANADA
Manhattan Publishing Co
670 White Plains Road
USA-10583 SCARSDALE, NY
Tel.: +1 914 271 5194
Fax: +1 914 472 4316
E-mail: coe@manhattanpublishing.com
http://www.manhattanpublishing.com

Council of Europe Publishing/Editions du Conseil de l'Europe
FR-67075 STRASBOURG Cedex
Tel.: +33 (0)3 88 41 25 81 – Fax: +33 (0)3 88 41 39 10 – E-mail: publishing@coe.int – Website: http://book.coe.int

La Recommandation CM/Rec(2010)13 est le premier texte international à énoncer des normes minimales de protection de la vie privée dans le cadre du profilage, destinées à être mises en œuvre par le secteur privé comme par le secteur public, par le biais de la législation nationale et de l'autorégulation. Elle a été adoptée par le Conseil de l'Europe et complète la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108).

Le profilage – qui est la technique consistant à observer le comportement des individus sur internet, à collecter ainsi leurs données personnelles et à les exploiter – présente des avantages pour les entreprises, pour l'économie et pour la société ainsi que, dans certains cas, pour les individus, en permettant notamment une meilleure segmentation des marchés ou une analyse ciblée des risques et des fraudes. Cependant, l'utilisation des techniques de profilage sans précautions et garanties particulières est susceptible de porter atteinte à la dignité humaine et de priver injustement des personnes de l'accès à certains biens ou services.

La recommandation poursuit les objectifs suivants :

– fournir un cadre réglementaire cohérent, qui tend à un juste équilibre entre les intérêts en jeu ;

– garantir une protection effective des droits des personnes concernées, et garantir des procédures équitables dans les situations où d'énormes quantités de données sont traitées ;

– éviter que des personnes ne fassent l'objet de décisions – ou soient victimes d'une discrimination ou d'une stigmatisation – automatiquement, sur la base de profils.

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int

Le Conseil de l'Europe regroupe aujourd'hui 47 Etats membres, soit la quasi-totalité des pays du continent européen. Son objectif est de créer un espace démocratique et juridique commun, organisé autour de la Convention européenne des droits de l'homme et d'autres textes de référence sur la protection de l'individu. Créé en 1949, au lendemain de la seconde guerre mondiale, le Conseil de l'Europe est le symbole historique de la réconciliation.

ISBN 978-92-871-7073-6

9 789287 170736

8€/16$US

http://book.coe.int
Editions du Conseil de l'Europe