CONSEIL DE L'EUROPE
COMITÉ DES MINISTRES

RECOMMANDATION N° R (87) 15

DU COMITÉ DES MINISTRES AUX ÉTATS MEMBRES

VISANT À RÉGLEMENTER L'UTILISATION DE DONNÉES À CARACTÈRE PERSONNEL DANS LE SECTEUR DE LA POLICE[1]

(adoptée par le Comité des Ministres le 17 septembre 1987, lors de la 410e réunion des Délégués des Ministres)

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

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

Conscient de l'usage croissant des données à caractère personnel faisant l'objet d'un traitement automatisé dans le secteur de la police et des avantages éventuels qui découlent du recours à l'ordinateur et à d'autres moyens techniques dans ce domaine ;

Considérant en outre l'inquiétude soulevée par la menace éventuelle d'un abus des procédés de traitement automatisé pour la vie privée de l'individu ;

Reconnaissant, d'une part, la nécessité de concilier l'intérêt de la société à la prévention et à la répression des infractions pénales et au maintien de l'ordre public et, d'autre part, les intérêts de l'individu et le droit au respect de sa vie privée ;

Tenant compte des dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 et en particulier des dérogations permises par l'article 9 ;

Gardant à l'esprit les dispositions de l'article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales,

Recommande aux gouvernements des Etats membres :

— de s'inspirer dans leurs droit et pratique internes des principes annexés à la présente recommandation, et

— de faire connaître les dispositions annexées à cette recommandation et en particulier les droits que sa mise en œuvre confère à l'individu.

---

1. Lors de l'adoption de cette recommandation :

— en application de l'article 10.2.*c* du Règlement intérieur des réunions des Délégués des Ministres, le Délégué de l'Irlande a réservé le droit de son Gouvernement de se conformer ou non à cette recommandation, la Déléguée du Royaume-Uni a réservé le droit de son Gouvernement de se conformer ou non aux principes 2.2 et 2.4 de la recommandation, et le Délégué de la République Fédérale d'Allemagne a réservé le droit de son Gouvernement de se conformer ou non au principe 2.1 de la recommandation ;

— en application de l'article 10.2.*d* dudit Règlement intérieur, le Délégué de la Suisse s'est abstenu tout en précisant qu'il réserve le droit de son Gouvernement de se conformer ou non à cette recommandation, et que son abstention ne doit pas être interprétée comme exprimant une désapprobation de la recommandation dans son ensemble.

Annexe à la Recommandation n° R (87) 15

Champ d'application et définitions

Les principes énoncés dans la présente recommandation s'appliquent à la collecte, à l'enregistrement, à l'utilisation et à la communication à des fins de police des données à caractère personnel qui font l'objet d'un traitement automatisé.

Aux fins de la présente recommandation, l'expression « données à caractère personnel » couvre toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme « identifiable » si cette identification nécessite des délais, des coûts et des activités déraisonnables.

L'expression « à des fins de police » couvre l'ensemble des tâches incombant aux autorités de police pour la prévention et la répression des infractions pénales et le maintien de l'ordre public.

L'expression « organe responsable » (maître du fichier) désigne l'autorité, le service ou tout autre organisme public qui est compétent selon le droit interne pour décider de la finalité d'un fichier automatisé, des catégories de données à caractère personnel qui doivent être enregistrées et des opérations qui leur seront appliquées.

Un Etat membre peut étendre les principes énoncés dans la présente recommandation aux données à caractère personnel ne faisant pas l'objet d'un traitement automatisé.

Un traitement de données ne devrait pas être effectué par voie manuelle dans le but d'échapper aux dispositions de la présente recommandation.

Un Etat membre peut étendre les principes énoncés dans la présente recommandation aux données afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique.

Les dispositions de la présente recommandation ne sauraient être interprétées comme limitant ou affectant d'une autre manière la faculté pour un Etat membre d'étendre, le cas échéant, certains des principes de celle-ci à la collecte, à l'enregistrement et à l'utilisation de données à caractère personnel à des fins de sécurité de l'Etat.

Principes de base

Principe 1 — Contrôle et notification

1.1. Chaque Etat membre devrait disposer d'une autorité de contrôle indépendante et extérieure à la police, chargée de veiller au respect des principes énoncés dans la présente recommandation.

1.2. L'introduction de nouveaux moyens techniques pour le traitement de données ne devrait être admise que si toutes les mesures raisonnables ont été prises pour s'assurer que leur utilisation est conforme à l'esprit de la législation existante sur la protection des données.

1.3. L'organe responsable devrait consulter à l'avance l'autorité de contrôle chaque fois que l'introduction de procédés de traitement automatisé soulève des questions concernant la mise en œuvre de la présente recommandation.

1.4. Les fichiers permanents automatisés devraient être déclarés à l'autorité de contrôle. Cette déclaration devrait spécifier la nature de chaque fichier déclaré, l'organe responsable de ce traitement, ses finalités, les types de données qu'il contient et les destinataires auxquels les données sont communiquées.

Les fichiers *ad hoc,* constitués à l'occasion d'affaires particulières, devraient également être déclarés à l'autorité de contrôle soit dans des conditions arrêtées avec celle-ci eu égard à leur spécificité, soit conformément à la législation nationale.

Principe 2 — Collecte des données

2.1. La collecte de données à caractère personnel à des fins de police devrait se limiter à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. Toute exception à cette disposition devrait faire l'objet d'une législation nationale spécifique.

2.2. Lorsque des données concernant une personne ont été collectées et enregistrées à son insu, elle devrait, si les données ne sont pas détruites, être informée, si cela est possible, que des informations sont détenues sur son compte, et ce, dès que l'objet des activités de police ne risque plus de subir un préjudice.

2.3. La collecte de données par le biais de moyens techniques de surveillance ou d'autres moyens automatisés devrait être prévue dans des dispositions spécifiques.

2.4. La collecte de données sur des individus pour l'unique motif qu'ils ont telle origine raciale, telles convictions religieuses, tel comportement sexuel ou telles opinions politiques ou qu'ils appartiennent à tels mouvements ou organisations qui ne sont pas interdits par la loi devrait être prohibée. La collecte de données concernant ces facteurs ne peut être effectuée que si elle est absolument nécessaire pour les besoins d'une enquête déterminée.

Principe 3 — Enregistrement des données

3.1. Dans la mesure du possible, l'enregistrement de données à caractère personnel à des fins de police ne devrait concerner que des données exactes et se limiter aux données nécessaires pour permettre aux organes de police d'accomplir leurs tâches légales dans le cadre du droit interne et des obligations découlant du droit international.

3.2. Les différentes catégories de données enregistrées devraient être différenciées, dans la mesure du possible, en fonction de leur degré d'exactitude ou de fiabilité et en particulier les données fondées sur des faits devraient être différenciées de celles fondées sur des opinions ou appréciations personnelles.

3.3. Lorsque des données qui ont été collectées à des fins administratives sont destinées à un enregistrement permanent, elles devraient être enregistrées dans un fichier séparé. En tout cas, des mesures devraient être prises pour que les données administratives ne soient pas soumises aux règles applicables aux données de police.

Principe 4 — Utilisation des données par la police

4. Sous réserve du principe 5, les données à caractère personnel collectées et enregistrées par la police à des fins de police devraient servir exclusivement à de telles fins.

Principe 5 — Communication des données

5.1. *Communication au sein de la police*

La communication de données entre services de police en vue d'une utilisation à des fins de police ne devrait être permise que s'il existe un intérêt légitime à cette communication dans le cadre des attributions légales de ces services.

5.2.i. *Communication à d'autres organes publics*

La communication de données à des organes publics ne devrait être permise que, si dans un cas déterminé :

a. il y a obligation ou autorisation légales claires ou autorisation de l'autorité de contrôle, ou si

b. ces données sont indispensables au destinataire pour accomplir sa tâche légale propre et pour autant que le but de la collecte ou du traitement exécuté par ce destinataire n'est pas incompatible avec celui prévu à l'origine et que les obligations légales de l'organe communiquant ne s'y opposent pas.

5.2.ii. Une communication est, en outre, exceptionnellement permise si, dans un cas déterminé :

a. la communication est, sans aucun doute, dans l'intérêt de la personne concernée et si, soit celle-ci y a consenti, soit les circonstances permettent de présumer sans équivoque un tel consentement, ou si

b. la communication est nécessaire pour éviter un danger grave et imminent.

5.3.i. *Communication à des personnes privées*

La communication de données à des personnes privées ne devrait être permise que si, dans un cas déterminé, il y a obligation ou autorisation légales claires ou autorisation de l'autorité de contrôle.

5.3.ii. Une communication à des personnes privées est exceptionnellement permise si, dans un cas déterminé :

a. la communication est, sans aucun doute, dans l'intérêt de la personne concernée et si, soit celle-ci y a consenti, soit les circonstances permettent de présumer sans équivoque un tel consentement, ou si

b. la communication est nécessaire pour éviter un danger grave et imminent.

5.4. *Communication internationale*

La communication de données à des autorités étrangères devrait se limiter à des services de police. Elle ne devrait être permise que :

a. s'il existe une disposition légale claire découlant du droit interne ou international,

b. si, à défaut d'une telle disposition, la communication est nécessaire à la prévention d'un danger grave et imminent ou à la répression d'une infraction pénale grave de droit commun,

et dans la mesure où il n'est pas porté atteinte aux réglementations internes relatives à la protection de la personne concernée.

5.5.i. *Demandes de communication*

Sous réserve des dispositions spécifiques de la législation nationale ou d'accords internationaux, les demandes de communication de données devraient contenir des indications sur l'organe ou la personne dont elles émanent ainsi que sur leur objet et leur motif.

5.5.ii. *Conditions de la communication*

La qualité des données devrait, pour autant que possible, être vérifiée au plus tard avant leur communication. Dans toute communication de données et dans la mesure du possible, les décisions juridictionnelles ainsi que les décisions de ne pas poursuivre devraient être mentionnées et les données fondées sur des opinions ou des appréciations personnelles être vérifiées à la source avant d'être communiquées ; leur degré de fiabilité ou d'exactitude devrait être indiqué.

S'il s'avère que les données ne sont plus exactes et à jour, elles ne devraient pas être communiquées ; si des données périmées ou inexactes ont été communiquées, l'organe expéditeur devrait autant que possible informer de leur non-conformité tous les organes destinataires auxquels les données ont été transmises.

5.5.iii. *Garantie concernant la communication*

Les données communiquées à d'autres organes publics, à des personnes privées ou à des autorités étrangères ne devraient être utilisées à d'autres fins que celles spécifiées dans la demande de communication.

Toute utilisation à d'autres fins devrait être subordonnée à l'accord de l'organe expéditeur, sans préjudice des dispositions des paragraphes 5.2 à 5.4.

5.6. *Mise en relation de fichiers et accès direct (accès* on line*)*

La mise en relation de fichiers avec d'autres fichiers utilisés à des fins différentes est soumise à l'une des conditions suivantes :

a. l'octroi d'une autorisation par l'organe de contrôle aux fins d'une enquête sur un délit particulier, ou

b. la conformité à une disposition légale claire.

L'accès direct (accès *on line*) à un fichier ne devrait être admis que s'il est conforme à la législation interne qui devrait tenir compte des principes 3 à 6 de la présente recommandation.

Principe 6 — Publicité, droit d'accès aux fichiers de police, droit de rectification et droit de recours

6.1. L'autorité de contrôle devrait prendre des mesures afin de s'assurer que le public est informé de l'existence des fichiers faisant l'objet d'une notification ainsi que de ses droits vis-à-vis de ces fichiers. La mise en œuvre de ce principe devrait tenir compte de la spécificité des fichiers *ad hoc*, en particulier de la nécessité d'éviter que l'accomplissement d'une tâche légale des organes de police ne soit entravé gravement.

6.2. La personne concernée devrait pouvoir obtenir l'accès à un fichier de police à des intervalles raisonnables et sans délais excessifs conformément aux modalités prévues par le droit interne.

6.3. La personne concernée devrait pouvoir obtenir, le cas échéant, la rectification des données la concernant, contenues dans un fichier.

Les données à caractère personnel que l'exercice du droit d'accès a révélées inexactes ou qui sont apparues excessives, inexactes ou non pertinentes en application de l'un des autres principes contenus dans cette recommandation devraient être effacées ou corrigées ou bien faire l'objet d'une déclaration rectificative ajoutée au fichier.

De telles mesures d'effacement ou de rectification devraient s'étendre, dans la mesure du possible, à tous les documents annexés au fichier de police et, si elles ne sont pas exécutées immédiatement, elles devraient l'être, au plus tard, lors de l'enregistrement ou de la communication de données suivants.

6.4. L'exercice des droits d'accès, de rectification ou d'effacement ne saurait faire l'objet d'une restriction que dans la mesure où une telle restriction serait indispensable pour l'accomplissement d'une tâche légale de la police ou nécessaire pour la protection de la personne concernée ou des droits et libertés d'autrui.

Dans l'intérêt de la personne concernée, une communication écrite peut être exclue par la loi, dans des cas d'espèce.

6.5. Un refus ou une restriction de ces droits devraient être motivés par écrit. La communication de la motivation ne pourrait être refusée que dans la mesure où cela serait indispensable pour l'accomplissement d'une tâche légale de la police ou nécessaire pour la protection des droits et libertés d'autrui.

6.6. Au cas où l'accès serait refusé, la personne concernée devrait disposer d'un recours auprès de l'autorité de contrôle ou d'un autre organe indépendant qui s'assurera que le refus est bien fondé.

Principe 7 — Durée de conservation et mise à jour des données

7.1. Des mesures devraient être prises pour que les données à caractère personnel conservées à des fins de police soient effacées si elles ne sont plus nécessaires aux fins pour lesquelles elles avaient été enregistrées.

A cette fin, il convient notamment de prendre en considération les critères suivants : nécessité de garder des données à la lumière des conclusions d'une enquête pour un cas donné ; prononcé d'une décision définitive et notamment acquittement ; réhabilitation ; prescription ; amnistie ; âge de la personne concernée ; catégories particulières de données.

7.2. Des règles destinées à fixer des périodes de conservation pour les différentes catégories de données à caractère personnel ainsi que des contrôles périodiques sur leur qualité devraient être établis en accord avec l'autorité de contrôle ou conformément au droit interne.

Principe 8 — Sécurité des données

8. L'organe responsable devrait prendre toutes les mesures nécessaires pour garantir aux données la sécurité physique et logique adéquate, et pour empêcher l'accès ou la communication non autorisés ou l'altération.

A cette fin, il faudrait tenir compte des différents contenus et caractéristiques des fichiers.