Deuxième evaluation de la pertinence de la Recommandation N° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police compte tenu des nouveaux développements en la matière, faite en 1998

TABLE DES MATIÈRES

I. MANDAT OCCASIONNEL

1. Nom du Comité auquel le mandat est destiné: GROUPE DE PROJET SUR LA PROTECTION DES DONNÉES (CJ-PD)
2. Source du mandat: Décision N° CM/547/180193 du Comité des Ministres et décision des Délégués des Ministres du, du 7-8 février 1995, 528ème réunion, point 10.1.a.
3. Délai dans lequel le mandat doit être exécuté: Décembre 1998
4. Texte du mandat:
« Evaluer tous les quatre ans la pertinence de la Recommandation N° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police ».
5. Désignation du comité auquel le mandat Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) est notifié pour information:
Comité européen pour les problèmes criminels (CDPC)
Comité d'experts sur la déontologie de la Police et les Problèmes liés à l'exercice de la police (PC-PO).

II. CONCLUSIONS DU CJ-PD

Le Groupe de projet arrive à la conclusion que la Recommandation N° R (87) 15 offre une protection adéquate aux données à caractère personnel utilisées à des fins de police, dans les domaines qu'elle couvre, pertinents au moment de son élaboration.
Il est proposé que le CJ-PD, en consultation notamment avec le CDPC, soit chargé d'examiner la question de savoir si l'application des principes de la recommandation R (87) 15 aux pratiques policières et judiciaires actuelles, dans la lutte contre la criminalité, nécessite l'adoption d'un instrument juridique complémentaire à ladite recommandation.
Dans ce contexte, les éléments suivants, relevés dans le rapport en annexe, devraient être pris en considération pour les travaux futurs :

L'identification de cibles d'informations en matière criminelle soit de manière substantielle, en définissant des critères dans la loi, soit de manière procédurale, en définissant les autorités et les circonstances qui peuvent donner lieu à la collecte d'informations en matière criminelle ;
Les délais de conservation d'informations en matière criminelle au-delà desquels les données devraient être revues ou effacées ;
L'utilisation de données collectées dans le cadre d'une enquête concernant un crime spécifique à propos de personnes non suspectes, pour enquêter sur d'autres ;
L'appariement de données collectées depuis des sources ouvertes, telles qu'Internet ou des fichiers publics, avec des données de police, en vue de trouver des données sur des personnes qui n'étaient pas suspectées préalablement ;
La notification des personnes dont les données sont conservées par la police;
La conservation et l'utilisation de données génétiques en vue de l'identification de criminels;
L'établissement d'une autorité de contrôle pour la protection de données à caractère personnel détenues par la police;
Des instruments afin de suivre le développement de l'utilisation des méthodes d'enquête comportant la collecte, la conservation et l'utilisation de données à caractère personnel.

III. RAPPORT

i. INTRODUCTION

Le 17 septembre 1987, le Comité des Ministres a adopté la Recommandation N° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (Annexe B au présent rapport).
Dans sa Recommandation 1181 (1992), relative à la coopération policière et à la protection des données à caractère personnel dans le secteur de la police (Annexe C au présent rapport), l'Assemblée Parlementaire recommandait au Comité des Ministres, entre autres, d'élaborer une Convention consacrant les principes énoncés dans la Recommandation N° R (87) 15.

Lors de leur 478e réunion (juin 1992), le Comité des Ministres a adopté la Décision N° CM/537/220692, confiant au Groupe de projet sur la protection des données et au Comité Consultatif de la Convention 108, le mandat de formuler des avis sur la Recommandation 1181 de l'Assemblée.

A la lumière de ces avis, les Délégués des Ministres, lors de leur 486e réunion (janvier 1993), ont adopté la Décision N° CM/547/180193, confiant au Groupe le mandat d'évaluer la pertinence de la Recommandation R(87)15 en vue de sa révision éventuelle.

Le CJ-PD a procédé à une première évaluation de la Recommandation en 1994, telle que figurant au document CJ-PD (94) 7.

A la lumière de cette évaluation et des conclusions du CJ-PD, le Comité des Ministres a confié au CJ-PD, lors de sa 528e réunion, le 7 février 1995, le mandat occasionnel rappelé plus haut.

ii. RÉSUMÉ DES TRAVAUX

Lors de sa 34e réunion (14-17 octobre 1997), le CJ-PD a confié à un rapporteur, M. A. Patijn (Pays Bas), un mandat en vue de la rédaction d'un rapport sur l'évaluation de ladite recommandation, à l'échéance d'une période de quatre ans, conformément à la décision du Comité des Ministres, du 7 février 1995.

Le projet de rapport, présenté par le Rapporteur à la 35e réunion du CJ-PD, du 25-27 mars 1998, et amendé par lui à la lumière des observations faites lors des réunions suivantes du Bureau et du CJ-PD, est reproduit à l'Annexe D du présent rapport.

Lors de sa 36e réunion (28-30 octobre 1998), le Groupe de Projet a examiné et approuvé le présent Rapport Final d'Activité.

ANNEXE A

Rapport établi par M. A. PATIJN, Expert au sein du CJ-PD au titre des Pays-Bas

La protection des données et la police. Evaluation de la Recommandation R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police

1. Généralités

Le Comité des Ministres a décidé de réviser la Recommandation R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (Décision CM/547/180193). La précédente évaluation remonte à 1994 ; elle a donné lieu à un rapport qui figure dans le document CJ-PD (94) 7. Le rapport tel qu'adopté par le Comité des Ministres établit que la recommandation doit faire l'objet d'une révision périodique tous les quatre ans. L'évaluation suivante avait été fixée à 1998. Le présent document est donc un projet d'évaluation (Un précédent projet a été distribué en mars 1998.) La présente version tient compte des observations communiquées par la Belgique, l'Allemagne, la Hongrie, l'Irlande et les Pays-Bas.

Dans l'intervalle, la Recommandation a été mentionnée dans deux accords internationaux : d'une part, l'article 115, par. 1, de la Convention d'application de l'Accord de Schengen indique que la Recommandation doit être prise en compte dans le cadre des contrôles effectués par l'autorité de contrôle (notons qu'il a été décidé dans le Traité d'Amsterdam que l'Accord de Schengen serait intégré au Traité sur l'Union européenne) ; d'autre part, l'article 14, paragraphe 1, de la Convention Europol prévoit que les données de police doivent être traitées dans le respect de la Recommandation du Conseil de l'Europe adoptée en 1987. Ces deux références rendent donc plus difficile une éventuelle modification des termes de la Recommandation. Du point de vue formel au moins, la modification de la Recommandation impliquerait celle des deux Conventions précitées. Pour l'heure, il n'est apparu aucune difficulté sérieuse qui justifierait de modifier la Recommandation ; aussi est-il proposé qu'elle ne soit pas révisée.

La Recommandation de 1987 traite des données de police telles qu'on les concevait dans la première moitié des années 80. Le crime organisé n'était pas encore devenu une préoccupation de portée internationale. Les fichiers d'informations en matière criminelle n'étaient pas aussi sophistiqués qu'à l'heure actuelle. A cette époque, la police conservait principalement des données sur les personnes qu'elle soupçonnait d'avoir commis une infraction pénale. Ces informations étaient indépendantes de celles qui pouvaient figurer dans le casier judiciaire. La Recommandation R (84) 10 du Conseil de l'Europe sur le casier judiciaire et la réhabilitation des condamnés traite plus précisément de cette question. Mais les temps ont changé, et cette évolution pose la question de l'utilité d'un nouvel instrument international qui approfondirait certaines questions spécifiques.

Proposition: Il est proposé que le Comité des Ministres modifie sa décision initiale d'évaluer périodiquement la Recommandation de 1987, afin que périodiquement la question de l'élaboration d'un instrument international complémentaire soit examinée.

Le présent rapport contient des éléments qui pourraient être utiles pour répondre à la question de savoir si l'élaboration d'un instrument complémentaire est souhaitable. Il propose que le Comité des Ministres recommande que les législateurs nationaux traitent expressément de certaines questions relatives à la protection des données dans la législation nationale sur la protection des données, dans

le code national de procédure pénale ou dans le droit national ou régional régissant le fonctionnement de la police.

2. Remarques générales

La tension qui existe entre les pouvoirs de la police et les droits de l'homme est inévitable. La police doit avoir des pouvoirs suffisants pour pouvoir remplir sa mission, mais il y a nécessairement interférence entre les pouvoirs dont elle dispose et le respect de la vie privée ; c'est pourquoi il convient de limiter ces pouvoirs autant qu'il est possible. L'équilibre à respecter entre les pouvoirs nécessaires de la police et les limitations à leur apporter pour sauvegarder la vie privée évolue continuellement en fonction des progrès des technologies de l'information. Ces dernières permettent en effet aux criminels de parvenir plus efficacement à leurs fins, mais elles permettent aussi à la police de remplir plus efficacement sa mission. Toutefois, en l'absence d'une réglementation suffisante, les nouvelles possibilités dont dispose la police peuvent avoir des incidences sur la vie privée des citoyens. L'article 8 de la Convention européenne des Droits de l'Homme (CEDH) exige dans ce cas la mise en place de fondements juridiques, car l'utilisation concrète des technologies doit s'accompagner de sauvegardes juridiques destinées à préserver la vie privée. La tension entre les pouvoirs (qui doivent être suffisants) de la police et la protection de la vie privée devient ainsi une force créatrice qui débouche sur l'élaboration de nouvelles lois et permet de préserver la qualité de la vie dans des sociétés démocratiques en mutation.

Tout d'abord, au niveau national, le législateur doit rester constamment attentif à cette problématique. Il importe de prendre en compte la pression des besoins sociaux mais, dans le domaine de la criminalité, ces besoins diffèrent selon les pays plus que dans d'autres domaines de la société. Ensuite, au niveau international, il est important d'examiner la possibilité d'harmoniser les règles s'il apparaît qu'il existe des éléments communs dans le droit des différents pays du Conseil de l'Europe.

Ces remarques générales valent pour toutes les formes d'ingérence dans la vie privée, qu'il s'agisse de perquisition ou d'interception de télécommunications. La protection des données n'est qu'un aspect parmi d'autres, qui ne présente à ce titre aucun caractère exceptionnel. C'est néanmoins lui qui est au cœur du présent document.

Proposition: Il est proposé de dresser dans un premier temps une liste de questions sur lesquelles l'attention des législateurs nationaux serait attirée, avant toute tentative d'harmonisation des approches nationales. Ensuite, on pourra se demander s'il est opportun de réglementer certains éléments au niveau international. Ce travail devra être mené en coopération étroite avec le CD-PC, compétent sur les questions pénales, car il implique les deux domaines du droit.

3. Les données en matière criminelle sont-elles des données sensibles?

Parmi les changements survenus récemment, les principaux concernent les enquêtes judiciaires. Les données à caractère personnel collectées et traitées dans l'exercice d'autres tâches policières, telles le maintien de l'ordre public ou l'assistance à ceux qui en ont besoin, n'ont guère changé au cours de la période d'évaluation. Pour ce type de données, la Recommandation semble suffisante. On peut en revanche envisager l'élaboration d'un instrument complémentaire pour les données collectées et traitées dans le but de réprimer des infractions pénales. Dans la suite du présent document, ces données sont appelées "données en matière criminelle". Ce sont les seules qui seront prises en compte dans le présent document.

Les données en matière criminelle doivent-elles être considérées comme des données sensibles? L'article 6 de la Convention n° 108 ne les mentionne pas en tant que telles ; il indique simplement que les mêmes principes s'appliquent aux données relatives à des condamnations pénales et à celles

habituellement qualifiées de données sensibles. Il s'ensuit que ces données ne peuvent être traitées que si le droit interne prévoit des garanties appropriées, mais l'article n'évoque que les condamnations pénales, et pas les données en matière criminelle concernant des personnes qui n'ont pas encore été condamnées. On peut néanmoins se demander si dans la pratique, ces données ne sont pas souvent plus sensibles encore, dès lors qu'aucun tribunal impartial n'a encore condamné l'intéressé sur la base d'éléments recueillis légalement et conformément à l'article 6 de la Convention européenne des Droits de l'Homme. Sans compter que, dans la plupart des cas, une personne condamnée par un tribunal dispose d'un droit de recours. Etant donné que la situation d'une personne au sein de la société peut être perturbée plus gravement encore par des données reposant sur des soupçons que par des données fondées sur une condamnation – en particulier lorsque les données en question sortent du cadre de la police -, les données en matière criminelle au sens large sont considérées comme sensibles aux fins du présent document.

Rappelons que la Directive 95/46/CE appréhende les données en matière criminelle sous un angle plus large. Le paragraphe 5 de l'article 8, consacré aux catégories particulières de traitements, requiert des garanties appropriées pour toutes les données relatives à des infractions, qu'elles concernent des condamnations pénales, des suspects, des informations en matière criminelle ou toutes autres données à caractère personnel collectées au cours d'une enquête judiciaire. Cette directive est applicable aux sujets relevant du droit communautaire, tels que les compagnies d'assurance qui traitent des données en matière criminelle concernant des personnes qui ont tenté de les escroquer. En revanche, eu égard à l'article 3, paragraphe 2, elle n'est pas applicable aux fichiers de police en tant que tels. La question qui se pose dans le cadre du présent rapport est de savoir si les données issues de traitements entrant dans le champ d'application de la directive peuvent être communiquées à la police. Ainsi, nous examinerons ci-après, au paragraphe 6, l'utilisation de fichiers publics à des fins de police. Etant donné que la plupart des fichiers publics relèvent du droit communautaire, le traitement des données qu'ils contiennent à des fins de police devrait, au sein de l'Union européenne, être apprécié à la lumière de l'article 13, paragraphe 1, alinéa d de la directive.

4. Plusieurs domaines juridiques – objet du présent document

La Recommandation R (87) 15 sur les données de police vise à donner un caractère concret aux principes de la Convention n° 108 appliqués au secteur de la police. Dans la plupart des pays qui ont ratifié cette Convention et qui appliquent donc certaines règles sur la protection des données, le secteur de la police est concerné par ces dispositions générales. Certains pays ont édicté des règles spéciales sur la protection des données dans le secteur de la police. Les règles relatives à la collecte des données trouvent généralement leur origine dans le code de procédure pénale ou dans une loi spécifique régissant la police. Dans certains cas, ces textes contiennent également des dispositions sur l'utilisation et la durée de stockage de données en matière criminelle particulières (ex.: utilisation et stockage de données après interception de communications, ou emploi d'autres méthodes d'investigation indiscrètes permettant de recueillir une quantité indéfinie de données à caractère personnel).

La ligne de démarcation entre la protection des données, la procédure pénale et la réglementation de la police ne passe pas au même endroit dans tous les pays. Les règles de procédure pénale varient considérablement entre les pays, même si elles sont conformes au cadre établi par la Convention européenne des Droits de l'Homme. Il existe aussi des variations entre les Etats membres du point de vue de l'acuité et de la nature de la délinquance qu'ils connaissent, et des politiques qu'ils appliquent en matière pénale. Les besoins sociaux urgents changent eux aussi d'un pays à l'autre, et ils ont des incidences légitimes sur les pouvoirs accordés à la police. Le CJ-PD n'a pas pour mandat de formuler des propositions en matière de règles de procédure pénale, mais il reste compétent pour l'application dans les codes de procédure pénale des principes régissant la protection des données. Il

n'est ni possible ni souhaitable de tenter de réaliser une harmonisation en profondeur des règles relatives à la protection des données pour le cas spécifique des données en matière criminelle, mais, du point de vue de la protection des données et compte tenu des progrès constants de l'informatique et des menaces qu'elle peut représenter pour la vie privée, on peut néanmoins poser certaines questions destinées à attirer l'attention des législateurs nationaux sur ces menaces afin qu'ils en tiennent compte dans la décision qu'ils prendront de réglementer au non ce domaine.

5. Informations en matière criminelle

5.1 Portée du concept d'information criminelle
Un phénomène nouveau, qui n'est pas spécifiquement traité dans la Recommandation R(87) 15, est celui d'information en matière criminelle. Cette expression n'est pas dénuée d'ambiguïté. On peut établir plusieurs distinctions.

a. Les données «solides» et les données «vagues». Les données de police concernant des délinquants peuvent être (1) des données provenant de sources attestées ou (2) des données fondées sur de très vagues indications concernant l'implication éventuelle d'une personne dans le crime organisé. Nous qualifierons les premières de données «solides», les secondes de données «vagues». Ces dernières données peuvent même provenir d'une source anonyme dont la fiabilité est totalement incertaine. La nature de l'information peut néanmoins être telle que l'on peut juger le stockage nécessaire pendant une période limitée, afin que la police puisse travailler correctement.

b. Les données sur les personnes suspectées d'avoir commis une infraction spécifique ou sur lesquelles certaines indications permettent de penser qu'elles en commettent ou en préparent une, seules ou dans le cadre d'une organisation. Les pouvoirs de la police et de la justice étant limités dans la plupart des codes de procédure pénale aux cas où il y a suspicion à l'égard d'une personne concernant une infraction spécifique, les nouvelles technologies de l'information servent de plus en plus à stocker des données sur les délinquants en tant que personnes, sans relation avec telle ou telle infraction. Ces données peuvent être «vagues» ou «solides» comme expliqué plus haut. Elles n'ont pas forcément la valeur d'une forte présomption à l'encontre d'une personne, condition nécessaire à l'exercice des pouvoirs que le code de procédure pénale confère à la police. Néanmoins, de nombreux pays collectent de telles données, sur la base desquelles il arrive que l'on établisse un profil du criminel supposé (comportement, fréquentations, mode de vie) sans que ces recherches aient vraiment un rapport avec une infraction particulière. Ces données sont utilisées pour tout type de délit, qu'il soit déjà commis ou que l'on s'attende à ce qu'il le soit. Elles ne servent pas uniquement dans le cadre de l'enquête, ni comme élément de preuve dans une affaire pénale donnée. Tant qu'aucune règle précise n'est prévue dans le code de procédure pénale ou dans le droit (régional) de la police, ces données sont régies par les principes généraux s'appliquant à la protection des données. Pour les besoins du présent document, l'expression «informations en matière criminelle» sera utilisée dans ce deuxième sens.

Autrement dit, les données ne sont pas considérées comme des «informations en matière criminelle» si elles sont recueillies dans le cadre d'une enquête judiciaire et qu'il existe des raisons plausibles de soupçonner une personne d'avoir commis une infraction pénale donnée, indépendamment du fait de savoir si :

(1) ces données ne servent que dans le cadre de l'instruction d'une affaire particulière ou si elles serviront éventuellement plus tard dans des enquêtes sur d'autres infractions;

(2) ces données ont été recueillies dans le cadre ou non des pouvoirs accordés par le code de procédure pénale.

Dans certains pays, de telles données ne peuvent être retenues comme éléments de preuve lors d'un procès. Elles ne servent qu'à guider l'enquête de la police, mais peuvent toutefois devenir pertinentes au cours d'un jugement si la défense met en cause la manière dont les moyens de preuve ont été recueillis. On peut alors contester la légalité de leur stockage, car les moyens de preuve en question sont viciés au départ.

5.2 Question concernant les informations en matière criminelle

S'agissant de la collecte et du stockage d'informations en matière criminelle, il convient de répondre à plusieurs questions.

5.2.1 Qui peut faire l'objet d'informations en matière criminelle ?

Le droit au respect de la vie privée implique que ces informations ne peuvent concerner indifféremment toute personne ; la loi doit donc définir les critères permettant de définir les "cibles" potentielles de telles informations. Ces critères seront variables selon les législations nationales et peuvent être de fond ou de forme. Les critères de fond concernent par exemple la restriction qui veut que l'on ne recueille d'informations en matière criminelle que dans les cas de crimes organisés ou de crimes représentant une menace pour la société. Un critère de forme est par exemple le fait qu'un ministère de la Justice, un ministère des Affaires intérieures, un juge ou un procureur donnent mandat pour collecter, pendant une période limitée et, si possible, dans une zone géographique déterminée, des informations en matière criminelle sur un groupe bien défini de personnes soupçonnées d'être impliquées dans un secteur rigoureusement circonscrit de la criminalité. La question à laquelle il faut alors répondre est de savoir si ce mandat devrait être un document accessible au public, soit dès le départ, soit dès que sa divulgation ne risquerait plus de compromettre la bonne marche de l'enquête.

5.2.2 Stockage de données sur des personnes liées à des cibles d'informations en matière criminelle
Le principe consiste à traiter les données en matière criminelle concernant un groupe de personnes – que la loi doit définir avec précision –, à l'égard desquelles il n'y a pas encore de raisons concrètes de penser qu'elles ont commis un délit. L'établissement du profil de ces personnes, du point de vue de leurs comportements criminels, oblige à stocker des données concernant également des tierces personnes non soupçonnées, même si elles ne répondent pas aux critères des cibles d'informations en matière criminelle. On peut à cet égard distinguer deux types de tierce personne :

(1) la tierce personne avec laquelle les cibles des informations en matière criminelle sont en contact, soit physiquement (d'après les observations concrètes), soit par voie de télécommunications (d'après ce qu'a montré la surveillance électronique de ses moyens de communication, c'est-à-dire téléphone, fax, courrier électronique, etc.);

(2) la tierce personne qui informe la police (informateurs, qui sont souvent eux-mêmes des délinquants) : compte rendu de toutes les conversations de l'informateur avec la police, voire de son comportement, pour pouvoir déterminer sa fiabilité et maintenir une surveillance des policiers qui sont en contact avec lui.

Les données concernant les tierces personnes visées aux points (1) et (2) doivent être conservées séparément des données sur les "cibles" des informations en matière criminelle puisqu'elles sont collectées pour des finalités différentes. Les données en (1) doivent être limitées au strict nécessaire pour permettre d'avoir une idée claire du sujet. Le stockage n'autorise pas à établir le profil de ces contacts. Les données en (2) peuvent être plus étendues pour permettre de juger, en cas de

contestation, la légalité de la collecte des données (et donc la recevabilité des moyens de preuve) auprès de ces informateurs. Il peut en résulter que les données réunies sur les personnes en (2) sont plus complètes que sur les personnes en (1) dans la mesure où la collecte des données répond dans les deux cas à des fonctions différentes.

Cette différence de fonction implique aussi que les décisions concernant les interrogatoires, les recoupements et les recherches devraient être justifiées en fonction des circonstances propres à chaque ensemble de données, compte tenu des raisons qui justifient leur traitement. L'utilisation de ces données doit être réglementée de manière plus stricte encore. L'objet des données visées au point (1) est d'apporter des informations sur une personne "cible" ; celui des données visées au point (2) est de déterminer la fiabilité de l'informateur. Le traitement par recoupement, combinaisons et recherches de données en (1) et (2) pour trouver des schémas de contacts entre des délinquants et établir de nouvelles cibles de renseignements criminels peut être considéré comme une forme d'utilisation compatible. Cela est moins évident lorsque les données sont utilisées pour répondre à un objectif qui se situe en dehors de la mission de la police. Au vu de l'article 9 de la Convention n° 108, un tel usage exigerait une base juridique explicite.

5.2.3 Pendant quelle durée peut-on stocker les informations en matière criminelle ?

La loi se doit d'être explicite sur la durée de stockage des informations en matière criminelle. On pourrait songer à un délai de quelques années à compter du jour où la dernière donnée pertinente à été ajoutée au fichier. A l'issue de cette période, on pourrait envisager un examen périodique (comme celui prévu à l'article 112 de l'Accord de Schengen). Si cet examen conclut qu'il n'existe pas de motifs suffisants pour justifier la conservation de ces données, celles-ci devraient en principe être détruites. La protection des données ne justifie pas de stocker des informations pour la simple raison "qu'elles pourraient éventuellement servir dans un avenir non prévisible". Cette formule n'exclut pas la possibilité de décider, à l'issue des examens successifs, de conserver les données, le cas échéant pour une durée indéterminée. Cette possibilité doit être acceptée chaque fois qu'il existe de bonnes raisons de le faire. On peut également penser à un système plus strict de suppression obligatoire après un certain laps de temps.

5.2.4 Remarques finales sur les informations en matière criminelle

Réglementer les informations en matière criminelle n'a de sens que si le stockage et l'utilisation de données en matière criminelle sur d'autres personnes non suspectées ne sont autorisés qu'à des fins spécifiques et pour de courtes périodes définies par la loi.

Proposition: Il est recommandé que les Etats membres définissent de manière restrictive, dans leur législation nationale, les "cibles" qui peuvent faire l'objet d'informations en matière criminelle. La loi devrait définir clairement un délai pour l'examen périodique de l'opportunité de prolonger le stockage.

6. Les données collectées par la police au cours d'une enquête judiciaire

6.1 Le problème

Les progrès rapides de l'informatique ont eu des répercussions sur le mode de fonctionnement de la police. L'outil informatique rend le travail plus efficace, aussi bien pour les criminels que pour la police. Cela signifie quelquefois que la police, pour faire son travail convenablement, doit collecter de grandes quantités de données, soit par téléchargement informatique lors d'une recherche, soit par interception de communications, ou encore par la surveillance du courrier électronique d'un

délinquant. Ce sont surtout les personnes impliquées dans le crime organisé qui sont susceptibles de procéder à des stockages et échanges massifs de données pour la gestion de leur organisation. Les données sont parfois collectées au moyen de méthodes d'investigation assez indiscrètes que la police est autorisée à employer en vertu du code de procédure pénale. Elles contiennent très souvent des données à caractère personnel en vrac; celles-ci peuvent n'avoir aucun rapport ni avec l'infraction qui fait l'objet de l'enquête, ni avec aucune autre infraction, mais elles sont néanmoins introduites dans les ordinateurs de la police pendant l'enquête judiciaire. Par "aucun rapport", on entend qu'aucune raison liée à l'enquête judiciaire spécifiquement en cours ne justifie la poursuite de leur conservation ou leur utilisation future à la lumière de l'article 8. Leur stockage ne peut être justifié que pendant le temps nécessaire pour établir qu'elles n'ont effectivement aucun rapport avec l'enquête, à moins que n'apparaissent d'autres utilisations, compatibles ou non, explicitement autorisées par la loi.

6.2 Autre utilisation

Dans quelle mesure la police est-elle autorisée à utiliser ces données dans le cadre d'autres enquêtes criminelles ? Que signifient dans ce contexte les principes de spécificité des objectifs et de compatibilité ? Quelles sont les limites de l'article de la Convention n° 108 autorisant légalement d'autres utilisations des données ?

On peut considérer que les données peuvent être utilisées pour enquêter sur une nouvelle infraction sans rapport avec l'ancienne dès lors qu'il ressort clairement des données collectées – c'est-à-dire sans recoupement ou comparaison avec des données collectées dans d'autres affaires – qu'il existe des indications suffisantes pour fonder des soupçons raisonnables concernant cette nouvelle infraction. La police est obligée de signaler toute infraction dont elle a connaissance. Il importe peu que cette connaissance résulte de l'utilisation de ses pouvoirs d'enquête dans une autre affaire, même sans aucun rapport. Ce type d'utilisation peut donc être considéré comme compatible avec l'objectif originel.

La question suivante est de savoir si elles peuvent être utilisées pour enquêter sur une infraction liée à l'ancienne infraction ou, plus largement encore, sur une infraction similaire, et aussi dans des affaires où les données elles-mêmes ne donnent lieu à aucune suspicion raisonnable. Dans certains systèmes juridiques, oui.

1. Quand les données concernant un suspect, ou même une personne condamnée par la suite, sont collectées au cours d'une même enquête, les données sur cette personne sont stockées en vue d'un usage ultérieur. Ainsi, les empreintes digitales et les photographies peuvent servir à résoudre d'éventuelles affaires ultérieures. On peut considérer qu'il s'agit là d'un usage compatible. Il y a divergence entre les Etats membres sur la nécessité de supprimer ces données en cas d'acquittement par manque de preuves lorsque la suspicion demeure. Il est moins contestable que de telles données doivent en principe être effacées lorsque l'innocence de quelqu'un a été établie ou si, par la suite, toute suspicion a été levée.

2. Les données concernant d'autres personnes que le suspect ou la personne condamnée collectées dans le cadre d'une enquête criminelle sont en principe collectées pour l'enquête particulière en question. Une utilisation à d'autres fins, par exemple pour enquêter sur des infractions futures, ne peut être considérée comme compatible avec l'utilisation d'origine. Ainsi, si une telle utilisation est jugée nécessaire, il convient de la fonder juridiquement dans le sens de l'article 9 de la Convention n° 108. On peut penser à des cas où ces données servent à mettre à jour des dossiers sur des cibles d'informations en matière criminelle.

La législation nationale devrait apporter des réponses claires à ces questions. La Convention n° 108 semble permettre une certaine lattitude.

6.3 Remarques finales

D'un point de vue pratique, on pourrait envisager d'autoriser la police à utiliser indistinctement les données collectées dans le cadre d'une enquête criminelle spécifique pour vérifier qu'elles ne comportent pas des éléments utiles, par exemple pour résoudre des affaires non encore résolues. Mais cette solution pourrait facilement conduire à donner à la police le pouvoir général d'enquêter sur de larges segments de la population en s'appuyant sur n'importe quelles données en matière criminelle collectées légalement au cours d'une enquête judiciaire. Si l'on s'écarte du principe "pas d'infraction, pas d'enquête", on peut se demander si une utilisation aussi large est conforme au critère de compatibilité mentionné à l'article 5, alinéa b, de la Convention n° 108. Dans l'affaire Campbell, la Cour européenne des Droits de l'Homme a jugé que l'existence de faits ou d'informations doit satisfaire un observateur objectif qu'il existe des motifs raisonnables d'utiliser de telles données pour lutter contre le crime (1992, 15 EHRR 137). Dans la mesure où le traitement de données en matière criminelle – qui sont des données sensibles – peut être considéré comme une ingérence dans la vie privée des particuliers, les cas de ce genre doivent être légitimés au sens de l'article 8, paragraphe 2, de la Convention européenne des Droits de l'Homme.
Ne sont pas concernés les recoupements, recherches et autres formes de traitement de données à caractère personnel, si elles sont autorisées par la loi, portant sur des fichiers existants, publics ou établis dans un but légitime, et dont l'utilisation est donc soumise à des restrictions.
Proposition: Il est recommandé que le pouvoir d'effectuer un contrôle ou un recoupement de données générales en vue de réprimer une infraction à partir de données de police collectées lors d'une enquête judiciaire et concernant un grand nombre de personnes qui n'ont peut-être rien à voir avec une quelconque infraction soit limité à des cas spécifiques mentionnés par le code de procédure pénale et qu'il soit accordé en vertu d'une autorisation spéciale de l'autorité judiciaire.

7. Recherches à partir de données qui ne sont pas des données de police

L'informatique a ouvert des possibilités nouvelles. Il est désormais possible de mettre en relation et de comparer de grandes bases de données pour y chercher des éléments sur une infraction ou sur des personnes encore totalement insoupçonnées. La plupart des codes de procédure pénale habilitent le pouvoir judiciaire à demander que lui soient transmis tous objets, y compris les supports d'information ou des données sans rapport avec le support. La plupart de ces pouvoirs ont été formulés à une époque où il n'y avait aucune raison d'établir une distinction entre les informations concernant une personne et celles qui concernent un grand nombre de personnes. L'informatique ayant considérablement facilité la recherche, la surveillance des communications et la combinaison de données, on peut considérer, du point de vue de la protection des données, que cette distinction a pris peu à peu une pertinence juridique. Aussi est-il recommandé que les codes de procédure pénale établissent clairement cette différenciation chaque fois qu'elle est nécessaire. Plus encore que la communication de données concernant une personne ou des personnes déterminée(s) – dont l'identité est précisée avant que les recherches ne soient entreprises et que les données ne soient soumises –, la transmission d'une grande quantité de données à caractère personnel en vrac aux fins d'une enquête judiciaire doit être subordonnée à des critères rigoureux et l'interprétation de ces critères, dans tel cas précis, doit dépendre de la décision d'une autorité (judiciaire) indépendante. On peut distinguer plusieurs situations :

(A) Depuis une période assez récente, il est possible, grâce à l'informatique, de collecter de grandes quantités de données à caractère personnel à partir de sources librement accessibles. Aussi l'Internet et les fichiers publics numérisés méritent-ils un traitement particulier.

1. L'Internet permet de collecter des données sur des individus. Comme tout un chacun, la police, dès lors qu'elle agit dans l'exercice légitime de ses fonctions, peut consulter sur Internet diverses sources, y compris étrangères. Aucune autorisation particulière n'est prévue par la législation nationale, car ces modes de consultation ne constituent pas une ingérence dans la vie privée des personnes. Des données à caractère personnel concernant une personne qui fait déjà l'objet d'une enquête judiciaire peuvent donc être recueillies et ajoutées aux données de police si elles sont utiles, ou peuvent le devenir, dans l'affaire en question. Mais il faut distinguer cette pratique de la collecte de données effectuée au hasard au sujet d'un grand nombre de personnes encore inconnues de la police. Etant donné que chacun d'entre nous peut procéder à une telle collecte, cette pratique ne peut être interdite à la police dès lors qu'elle lui est nécessaire dans l'exercice de son travail. Toutefois, on dépasse les limites de la légalité lorsque l'on croise une collecte massive de ce type avec des fichiers de police. Un recoupement général entre des données téléchargées à partir d'Internet et des fichiers de police, effectué pour pouvoir éventuellement dépister un délit, pourrait facilement impliquer une surveillance générale de larges segments de la population et, en fin de compte, une ingérence dans la sphère privée des individus sans motif légitime et suffisant. Il reste que c'est aux Etats membres qu'il appartient de réglementer ce type de croisement dans le contexte particulier de l'enquête sur une infraction pénale donnée.

2. Tous les pays possèdent des fichiers publics contenant toutes sortes de données à caractère personnel qui peuvent être consultés par tout un chacun et pour des raisons très variables, par exemple le cadastre ou les registres du commerce qui contiennent des données sur les personnes ayant des responsabilités dans la gestion de l'entreprise. Jusqu'à il y a quelques années, il était impossible de combiner ces fichiers et de faire une recherche pour mettre en évidence des relations inconnues. Mais, depuis que certains de ces fichiers publics sont accessibles sous forme numérique (sur CD-Rom ou sur Internet), il est possible d'effectuer des recherches étendues, en fonction de toutes sortes de critères et en combinant différents fichiers, sauf si des précautions techniques précises ont été prises pour empêcher de telles recherches. Le législateur a créé un fichier public dans l'idée souvent implicite que certaines informations spécifiques sur des individus pourront être consultées. Mais cela n'impliquerait pas nécessairement que ce fichier soit également accessible sous forme numérique, avec pour conséquence que les informations qu'il contient pourraient permettre de retrouver sur une personne des informations jusqu'ici inconnues. Du point de vue de la protection des données, il apparaît nécessaire de mettre en place des dispositifs de sécurité pour empêcher qu'un fichier public soit comparé sans restriction à d'autres fichiers (publics). Par exemple, il devient possible d'identifier un groupe de personnes jusque-là inconnues mais possédant un ensemble de caractéristiques prédéterminées sans que cette recherche ait un rapport quelconque avec l'objectif des fichiers en question. Divers concepts, qui sont d'ailleurs voisins, sont actuellement en vogue : la recherche de données, le recoupement de données, l'acquisition de connaissances, la gestion des sources d'information, etc.

Cette situation oblige à se demander si la police a le droit de comparer ces fichiers entre eux, ou de les comparer par exemple à ses propres fichiers pour les compléter ou pour dépister de nouvelles infractions. Là encore, il est proposé de limiter ces recoupements au cadre spécifique d'une enquête sur une infraction pénale et de les subordonner à une autorisation judiciaire ; on interdirait ainsi à la police d'effectuer une surveillance générale sur de larges segments de la population en dehors de toute enquête particulière. Les recherches sur les fichiers publics ou le croisement de plusieurs fichiers publics, s'ils sont jugés nécessaires pour dépister des infractions, devraient être expressément autorisées par la loi selon certains critères spécifiques.

(B) L'article 6 de la Directive 91/308/CEE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux prévoit une collecte générale de certaines

informations concernant les transactions inhabituelles, et ce afin de prévenir les infractions pénales. Si ces informations sont recueillies en vue de réprimer un type particulier d'infraction, elles concernent des personnes qui ne sont pas suspectes et ne remplissent pas les critères qui feraient d'elles des sujets d'informations en matière criminelle. D'après cet article, ces données ne peuvent en principe être utilisées à d'autres fins, sauf autorisation expresse de la loi. Dans un domaine spécifique, on a donc mis en place un système de surveillance générale des données concernant la population pour réprimer un type particulier d'infraction selon des critères spécifiques. Reste, pour le législateur, à répondre à la question suivante : la police a-t-elle accès – et si oui, dans quelle mesure – aux données ainsi recueillies ? Il apparaît souhaitable que la police ait accès au moins aux données financières ainsi recueillies sur les personnes qu'elle a déjà fichées en toute légitimité. Mais il est moins sûr qu'il faille autoriser la police à utiliser ces données indistinctement en dehors d'une procédure particulière donnant un fondement juridique explicite à cette utilisation.

Proposition: Il est recommandé que le code de procédure pénale permette – en vertu d'une autorisation judiciaire délivrée dans certains cas spécifiques et si cela est jugé nécessaire pour l'enquête ou pour faire cesser une infraction pénale particulière – de croiser des fichiers publics, des données financières concernant des transactions inhabituelles ou des données téléchargées à partir d'Internet avec des fichiers de police.

8. Données génétiques

Compte tenu des progrès réalisés par la science en matière d'utilisation de l'ADN comme moyen de reconnaissance des personnes, cet outil va occuper une place de plus en plus importante. A cette fin, de nombreux pays ont constitué ou sont en train de constituer des bases d'ADN. Au sein de l'Union européenne, une base transnationale est actuellement à l'étude. Du point de vue de la protection des données, on peut relever les points suivants.

La question de l'ADN fait l'objet d'un examen minutieux pour plusieurs raisons. Des personnes sont condamnées parce que leur ADN a été trouvé sur les lieux du crime. L'ADN est un élément de preuve pouvant concourir à établir la culpabilité. Dans le cas des délinquants sexuels, ces données sont stockées et utilisées lors d'enquêtes ultérieures. Le législateur devrait préciser s'il entend limiter l'utilisation de l'ADN aux infractions de nature sexuelle ou au contraire étendre le recours à la banque d'ADN aux infractions mineures telles que les mauvais traitements banals. Si la loi restreint le recours à la banque d'ADN aux infractions sexuelles, il reste que la découverte d'ADN sur les lieux d'une infraction mineure peut être utilisée pour en identifier l'auteur. Il est cependant exclu que cet ADN soit de nouveau utilisé ultérieurement au cas où de l'ADN serait découvert en une autre occasion.

L'ADN est utilisé pour identifier les auteurs d'infractions pénales graves. Il peut aussi arriver que les tests d'ADN conduisent à l'acquittement d'une personne. Le test peut en effet prouver que celle-ci n'a pas commis l'infraction. Si un test d'ADN a prouvé qu'une personne n'est pas coupable d'une infraction pénale (ou, dans un cadre plus limité, d'une infraction sexuelle), le stockage des données dans la banque d'ADN aux fins d'enquêtes sur d'éventuelles futures infractions devrait être interdit.

En pratique, il n'est pas exclu que l'ADN d'une personne puisse être utilisé pour identifier une autre personne de la même lignée génétique. Sur le plan juridique se pose alors la question de savoir si cette pratique est autorisée. Supposons par exemple que la banque d'ADN contienne l'ADN d'un père dont le fils fugitif est soupçonné (à cause de traces d'ADN) d'avoir commis une infraction sexuelle, mais que l'ADN du fils ne soit pas disponible. Peut-on utiliser l'ADN du père pour prouver que le fils est l'auteur de l'infraction? Le législateur doit décider si, d'un point de vue juridique, il existe une bonne raison pour qu'une personne dont le père figure dans la banque d'ADN soit une

cible plus facile pour les forces de l'ordre qu'une personne dont les parents n'ont jamais eu affaire à la police auparavant. On pourrait imaginer de limiter cet emploi à des cas graves et exceptionnels.

Il arrive que l'on demande à de larges fragments de la population de collaborer à l'élucidation d'une infraction en se soumettant à des tests d'ADN (ou d'autres tests biométriques, comme les empreintes digitales). Cette pratique est possible sur une base volontaire. Les autres usages de ces données, par exemple pour résoudre d'autres infractions sans consentement volontaire pour cet autre usage, doivent être considérés comme incompatibles avec l'objectif initial. Cela implique la suppression des données une fois terminée l'enquête sur l'infraction en question.

Proposition: Un groupe pluridisciplinaire étudiera dans le cadre du Conseil de l'Europe certains problèmes posés par les données génétiques. Ce groupe pourrait prendre en compte les questions évoquées plus haut.

9. Notification

En principe, toute personne doit être informée qu'elle a fait l'objet d'une collecte de données, afin qu'elle puisse former un recours effectif si elle estime qu'il y a eu ingérence dans sa vie privée (cf. article 13 de la Convention européenne des Droits de l'Homme). Dès son arrestation, un suspect doit être informé de la nature et du motif des accusations (cf. article 6 de la CEDH) portées contre lui ; lors d'une audience, il sera confronté aux éléments recueillis. Dans une enquête pénale, d'autres personnes peuvent être impliquées, en dehors du suspect lui-même. L'arrêt Klass rendu par la Cour Européenne des Droits de l'Homme le 6 septembre 1978 (Série A, n° 28) permet de différer le moment d'informer l'intéressé si cela est nécessaire pour que le travail de la police ne soit pas compromis. S'agissant d'informations en matière criminelle, cette exception est probablement applicable dans presque tous les cas.

On peut se demander dans quelle mesure les personnes doivent être informées que, dans le cadre d'une recherche, on a procédé à partir d'un système informatique à d'importants téléchargements de données à caractère personnel. La recherche en elle-même ne peut plus être compromise, de sorte que le "critère Klass" ne s'applique pas. Une dérogation à l'obligation de notification est parfois possible si l'effort exigé est disproportionné. Si une personne exerce néanmoins son droit d'accès vis-à-vis de la police, elle doit être informée que des données la concernant ont été collectées lors d'une recherche. De plus, l'intéressé peut être informé de la source des renseignements téléchargés. En principe, l'entité "source" n'est pas tenue au secret quant aux données que la police a téléchargées à partir de son système informatique. Si l'on estime nécessaire que certains responsables de fichiers taisent aux intéressés le fait que la police a recueilli des données sur eux à partir de leurs fichiers, cela doit être prévu expressément par la loi. On peut penser à des circonstances particulières dans lesquelles des agents des télécommunications ou des banquiers qui ont transmis des renseignements à la police pourraient être contraints par la loi à cacher ce fait à leurs clients. Le législateur pourrait imposer cette obligation aux serveurs Internet lorsqu'il y surveillance du courrier électronique. Sans doute faut-il considérer comme une mesure disproportionnée l'obligation générale imposée à un particulier de garder le silence face à la personne concernée lorsque des données à caractère personnel ont été communiquées à la police ou saisies par elle.

Cette situation est à distinguer de celle où des données à caractère personnel sont contrôlées et recueillies pendant une certaine période en vertu d'une autorisation légale (ex.: collecte d'informations sur les communications). La recherche serait compromise si la personne surveillée était informée par avance de cette mesure. Il s'agit par essence d'une mesure appliquée en secret, de sorte que l'intéressé ne peut être mis au courant qu'a posteriori. Pour ce type de situations, il pourrait

être utile que le législateur impose aux particuliers dont la coopération est nécessaire à la police une obligation générale de ne pas prévenir l'intéressé, et ce au moins pendant la durée de la surveillance. Mais au terme de la surveillance, l'intéressé doit en principe être informé que des données à caractère personnel le concernant ont été collectées (ex. : conversation téléphonique interceptée en vertu d'une autorisation délivrée à cet effet). Si cette information est omise en raison d'un effort disproportionné, l'intéressé doit pouvoir exercer son droit d'accès s'il le demande, sauf si cela risque de porter préjudice à la bonne exécution des tâches de la police.

Proposition: Il est recommandé que le législateur précise clairement les circonstances dans lesquelles la personne concernée doit être informée, que ce soit à l'initiative de la police ou à sa propre demande. Il y a lieu aussi de clarifier la situation du particulier qui coopère avec la police en communiquant à celle-ci des données à caractère personnel concernant un tiers.

10. Flux transfrontières de données

En vertu de l'article 5.4 de la Recommandation R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, les données recueillies et stockées en toute légalité par la police peuvent être communiquées aux services de police d'autres pays. Mais ce transfert peut être refusé si un pays possède des règles spécifiques à cause du caractère sensible des données en matière criminelle ou de certaines d'entre elles (ex. : informations en matière criminelle) et que l'autre pays ne dispose pas d'une protection équivalente (article 12, Convention n° 108).
Le transfert doit être adressé aux services de police de l'autre pays. Ce principe ne remet pas en cause le fait que les services de police de l'Etat destinataire, en vertu du droit interne, puissent communiquer ces données aux organes gouvernementaux à des fins administratives. Il n'en va autrement que si l'Etat d'origine indique expressément que les données sont communiquées uniquement à des fins de police. Mais cette précision n'a d'effet que si les services de police du pays destinataire ne sont pas tenus, en vertu du droit interne, de communiquer leurs données à d'autres organes. Si une telle obligation existe dans un Etat destinataire, celui-ci devrait en informer l'Etat d'origine.

L'Accord de Schengen et Europol ont mis en place un système de protection des données satisfaisant. Il n'apparaît pas nécessaire d'élaborer de nouveaux instruments régissant spécifiquement les flux transfrontières de données de police en dehors des éléments évoqués plus haut concernant les législations nationales lesquels ne manqueront pas non plus d’avoir des effets également au niveau international.

11. Obligation de rendre compte

La protection des données et l'efficacité de l'action de la police sont parfois difficiles à concilier. Il est admis que la police a besoin de grandes quantités de données afin de prévenir des infractions ou d'enquêter sur celles-ci. Toutefois, ces données ne peuvent être exploitées sans aucune restriction; leur traitement devrait être réglementé par la loi. Afin de permettre aux autorités compétentes de légiférer en temps opportun, soit pour accorder à la police des pouvoirs supplémentaires pour qu'elle puisse s'acquitter de sa tâche, soit pour protéger les citoyens contre des ingérences injustifiées dans leur vie privée, on pourrait imaginer des instruments qui permettent aux autorités de suivre les évolutions intervenant dans ce domaine. L'un de ces instruments pourrait être l'obligation pour la police de déclarer dans quelle mesure et de quelle manière précise elle exerce certains pouvoirs qui lui sont conférés par la loi en ce qui concerne le traitement des données à caractère personnel. Par exemple, on pourrait envisager une obligation de déclarer le nombre de personnes faisant l'objet d'informations en matière criminelle. Il reste à savoir si cette déclaration devrait prendre la forme d'un rapport confidentiel au gouvernement ou d'un document public

permettant au parlement de contrôler l'usage qui est fait de pouvoirs susceptibles de toucher la vie privée.

Proposition: Les législateurs nationaux devraient envisager la possiblité de réglementer l'utilisation faite par la police de méthodes d'enquêtes impliquant la collecte, le stockage et l'exploitation de données à caractère personnel.

12. Autorité de contrôle

Les pays qui ont mis en application la Directive 95/46/CE sur la protection des données n'ont formulé aucune réserve de fond concernant les pouvoirs de l'autorité de contrôle indépendante vis-à-vis de la police, bien que cet instrument ne soit pas applicable aux fichiers de police en tant que tels. Globalement, on peut donc espérer une amélioration du contrôle et de la mise en œuvre des règles relatives à la protection des données dans le secteur de la police. Il est recommandé que les autres Etats membres du Conseil de l'Europe établissent sur leur territoire un dispositif de contrôle similaire pour les fichiers de police. Une telle mesure permettrait des échanges internationaux sans obstacles entre services de police dans le cadre de la lutte contre la criminalité organisée internationale.

Proposition: Il est proposé que les Etats membres complètent leur législation interne pour établir sur leur territoire un dispositif de surveillance indépendant des fichiers de police, et que ce dispositif ait le pouvoir effectif de faire appliquer les règles relatives à la protection des données.

13. Conclusion

Il est proposé que le Comité des Ministres du Conseil de l'Europe modifie sa décision initiale d'évaluer périodiquement la Recommandation de 1987, dans le sens où il devrait déterminer périodiquement s'il y a lieu d'élaborer un instrument international complémentaire.
Le Comité pourrait donner de nouvelles orientations aux législateurs des Etats membres en ce qui concerne au moins les questions qui suivent. Ces orientations pourraient être définies en étroite collaboration avec le CD-PC ; en effet, la frontière entre la protection des données, la procédure pénale et la législation relative à la police ne passe pas au même endroit d'un pays à l'autre et de nombreuses questions intéressent tous ces domaines du droit.

Propositions:

1. Il est proposé que les législateurs nationaux répondent explicitement à un certain nombre de questions relatives à la protection des données, soit dans la législation nationale concernant la protection des données, soit dans le code national de procédure pénale, soit dans la législation relative à la police.

2. Il est proposé que les Etats membres définissent de manière restrictive, dans leur législation nationale, les "cibles" qui peuvent faire l'objet d'informations en matière criminelle. On peut songer au crime organisé et aux crimes représentant une menace comparable pour la société. La loi devrait définir clairement un délai pour l'examen périodique de l'opportunité de prolonger le stockage.

3. Il est proposé que le pouvoir d'effectuer un contrôle ou un croisement de données générales en vue de réprimer une infraction en utilisant des données de police collectées lors d'une enquête judiciaire et concernant un grand nombre de personnes qui n'ont peut-être rien à voir avec une quelconque infraction soit limité aux cas graves spécifiquement mentionnés par le code de procédure pénale et soit accordé en vertu d'une autorisation spéciale de l'autorité judiciaire.

4. Le code de procédure pénale devrait préciser dans quels cas les fichiers de police peuvent être recoupés avec des fichiers publics, des données financières sur des transactions inhabituelles ou des données téléchargées à partir d'Internet.

5. La législation devrait préciser clairement les circonstances dans lesquelles la personne concernée doit être informée, que ce soit à l'initiative de la police ou à sa propre demande. Il y a lieu de clarifier la situation du particulier qui coopère avec la police en communiquant à celle-ci des données à caractère personnel concernant un tiers.

6. Il est proposé que les Etats membres complètent leur législation interne pour établir sur leur territoire un dispositif de surveillance indépendant des fichiers de police, et que ce dispositif ait le pouvoir effectif de faire appliquer les règles relatives à la protection des données.

7. Il est proposé que le pouvoir d'effectuer un contrôle ou un croisement de données générales en vue de réprimer une infraction en utilisant des données de police collectées lors d'une enquête judiciaire et concernant un grand nombre de personnes qui n'ont peut-être rien à voir avec une quelconque infraction soit limité aux cas graves spécifiquement mentionnés par le code de procédure pénale et soit accordé en vertu d'une autorisation spéciale de l'autorité judiciaire

8. Il est recommandé que le code de procédure pénale permette – en vertu d'une autorisation judiciaire délivrée dans certains cas spécifiques et si cela est jugé nécessaire pour l'enquête ou pour faire cesser une infraction pénale particulière – de croiser des fichiers publics, des données financières concernant des transactions inhabituelles ou des données téléchargées à partir d'Internet avec des fichiers de police.

9. Un groupe pluridisciplinaire étudiera dans le cadre du Conseil de l’Europe certains problèmes posés par les données génétiques. Ce groupe pourrait prendre en compte les questions évoquées plus haut.

10. Les législateurs nationaux devraient envisager la possibilité de réglementer l’utilisation faite par la police de méthodes d’enquêtes impliquant la collecte, le stockage et l’exploitation de données à caractère personnel.

ANNEXE B

Texte de la Recommandation 1181 (1992) de l'Assemblée Parlementaire du Conseil de l'Europe

RECOMMANDATION 1181 (1992)[1] relative à la coopération policière et à la protection des données à caractère personnel dans le secteur de la police

1. En conséquence de l'Accord de Schengen, les Etats européens qui coopèrent dans le cadre de cet accord procéderont à l'échange de données informatisées à caractère personnel dans le secteur de la police. Il est fort probable qu'un tel échange porte sur l'ensemble de la Communauté européenne après la disparition des contrôles aux frontières internes.

2. A l'heure actuelle, il y a déjà un échange intensif de données dans le secteur de la police parmi les Etats membres du Conseil de l'Europe, dans un cadre bilatéral ou multilatéral et par l'intermédiaire d'Interpol.

3. Pour que la lutte contre la criminalité internationale soit efficace, il est crucial qu'elle se déroule au niveau national et au niveau européen.

4. Pour être efficace, la lutte contre la criminalité suppose un échange de données dans le secteur de la police.

5. A cet égard, il est utile de rappeler la Recommandation 1044 (1986) de l'Assemblée relative à la criminalité internationale et son plaidoyer pour un centre européen de renseignements et d'information (Europol), et la Recommandation no R (87) 15 du Comité des Ministres aux Etats membres du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.

6. Il est nécessaire, cependant, qu'il y ait une protection adéquate des données à caractère personnel dans le secteur de la police, et l'on peut constater avec satisfaction que le Conseil de l'Europe a conclu, en 1981, une Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Néanmoins, pour être pleinement efficace, cela n'est pas suffisant, car cette convention n'a été ratifiée pour l'instant que par onze Etats membres.

7. L'Assemblée recommande donc au Comité des Ministres :

i. d'élaborer une convention consacrant les principes énoncés dans sa Recommandation no R (87) 15 ;

ii. de promouvoir l'application de ces principes dans l'échange de données dans le secteur de la police entre Etats membres, ainsi qu'entre Etats membres et pays tiers, par l'intermédiaire d'Interpol.

A cet égard, la mise en œuvre des principes suivants revêt une importance capitale :

a. les données doivent être exactes, pertinentes, ne pas excéder la finalité pour laquelle elles sont enregistrées et, s'il y a lieu, tenues à jour ;

[1] Texte adopté par la Commission Permanente, agissant au nom de l'Assemblée, le 11 mars 1992.Voir Doc. 6557, rapport de la commission des questions juridiques et des droits de l'homme, rapporteur : M. Stoffelen.

b. elles doivent être sélectionnées avant d'être enregistrées ;

c. tout particulier doit avoir le droit de savoir si des données à caractère personnel le concernant sont conservées ;

d. il doit avoir un droit d'accès approprié à de telles données ;

e. il doit avoir le droit de contester ces données et éventuellement de les faire rectifier ou effacer ;

f. les particuliers qui se voient refuser l'accès aux fichiers les concernant doivent avoir le droit de saisir une autorité indépendante ayant plein accès à tous les fichiers pertinents et pouvant et devant mettre en balance les intérêts contradictoires en jeu ;

g. il doit y avoir une autorité indépendante, en dehors du secteur de la police, chargée d'assurer le respect des principes énoncés dans une telle convention ;

iii. de demander instamment aux Etats membres de garantir que les données dans le secteur de la police ne puissent être échangées avec d'autres Etats membres et avec Interpol que suivant ce qui est prévu par le projet de convention proposé.

Décision No. CM/537/220692 de la 478e réunion du Comité des Ministres juin 1992

DECISION No. CM/537/220692

Mandat occasionnel

1.	Nom du Comité auquel le mandat est destiné:	GROUPE DE PROJET SUR LA PROTECTION DES DONNEES (CJ-PD)
2.	Source du mandat:	Comité des Ministres
3.	Délai dans lequel le mandat doit être exécuté:	25 septembre 1992
4.	Texte du mandat:	

Formuler un avis sur la Recommandation 1181 de l'Assemblée relatie à la coopération policière et protection des données à caractère persnnel dans le secteur de la police.

5.	Désignation du comité auquel le mandat est notifié pour information:	Comité directeur sur la coopération juridique (CDCJ)

Décision No. CM/547/180193 de la 486e réunion du Comité des Ministres
janvier 1993

DECISION No. CM/547/180193

Mandat occasionnel

1.	Nom du Comité auquel le mandat est destiné:	GROUPE DE PROJET SUR LA PROTECTION DES DONNEES (CJ-PD)
2.	Source du mandat:	Comité des Ministres
3.	Délai dans lequel le mandat doit être exécuté:	décembre 1994
4.	Texte du mandat:	

Evaluer la pertinence de la Recommandation N° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, et, en particulier, la nécessité d'une révision de ce texte, notamment du champ d'application de la Recommandation et du principe 5.4 (communication internationale), ayant à l'esprit les principes contenus dans la Recommandation 1181 (1992) de l'Assemblée.

5.	Désignation du comité auquel le mandat est notifié pour information:	Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD)

Coopération policière et protection des données à caractère personnel dans le secteur de la police, Décision du 7 février 1995

COOPERATION POLICIERE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL DANS LE SECTEUR DE LA POLICE, Recommandation 1181 (1992) de l'Assemblée parlementaire (CM/Dél/Déc/Act(93)486/19, CM(95)1, Annexe III)

Décision

Les Délégués adoptent la réponse complémentaire suivante à la Recommandation 1181 (1992) de l'Assemblée parlementaire relative à la coopération policière et à la protection des données à caractère pesonnel dans le secteur de la police:

"1. Le Comité des Ministres se réfère à ses précédentes réponses à la Recommandation 1181 (1992) de l'Assemblée parlementaire relative à la coopération policière et à la protection des données à caractère personnel dans le secteur de la police, adoptées respectivement en juin 1992 et en janvier 1993. Il souhaite rappeler à l'Assemblée parlementaire qu'ainsi qu'il l'avait indiqué dans sa réponse de janvier 1993, il a chargé le Groupe de projet sur la protection des données (CJ-PD) d'évaluer la pertinenece de la Recommandation No. R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, et, en particulier, la nécessité d'une révision de ce texte, notamment du champ d'application de la Recommandation et du principe 5.4 (communication internationale).

2. Le CJ-PD est parvenu à un certain nombre de conclusions qui ont été endossées par le Comité des Ministres. Aussi celui-ci est-il en mesure d'informer l'Assemblée qu'à son avis la Recommandation No. R (87) 15 offre une protection adéquate aux données à caractère personnel utilisées à des fins de police et qu'il n'est pas nécessaire, à ce stade, de réviser le texte ou des parties du texte. Le principe 5.4 de la Recommandation No. R (87) 15, en particulier lorsqu'il est lu conjointement avec les paragraphes 56 à 80 de son Exposé des motifs, s'avère être suffisamment flexible pour faire face aux exigences, tant actuelles que prévisibles, des accords internationaux relatifs à l'échange de données à des fins de police.

3. Cependant, ayant à l'esprit notamment la mise en œuvre de nouveaux systèmes pour partager des données à caractère personnel utilisés dans le secteur de la police, tel EUROPOL, le développement rapide des moyens technologiques et les préoccupations exprimés par l'Assemblée parlementaire, le Comité des Ministres estime que la pertinence de la Recommandation No. R (87) 15 devrait être régulièrement établie. Aussi a-t-il décidé que celle-ci serait soumise à un examen périodique, le prochain devant être effectué en décembre 1998 et par la suite tous les quatre ans."