Rapport sur la troisième évaluation de la Recommandation n° R (87) 15 visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police (2002)

INTRODUCTION

1. Le Comité des Ministres, par sa Décision n° CM/537/220692 adoptée en juin 1992, a chargé le groupe de projet sur la protection des données (CJ-PD) de formuler un avis sur la Recommandation 1181 de l'Assemblée relative à la coopération policière et la protection des données à caractère personnel dans le secteur de la police. En janvier 1993, par sa Décision n° CM/547/180193, il a chargé le CJ-PD d' *« évaluer la pertinence de la Recommandation n° (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 de son champ d'application et du principe 5.4 (Communication internationale), ayant à l'esprit les principes contenus dans la Recommandation 1181 (1992) de l'Assemblée »*. En outre, par une décision adoptée le 7 février 1995, il a considéré *« que 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 devrait être évaluée régulièrement. Il a donc décidé que la prochaine évaluation serait effectuée en septembre 1998, puis tous les quatre ans »*. Conformément à ce mandat, deux rapports d'évaluation ont été établis, en 1994 et en 1998.

2. Conformément au mandat du CJ-PD (*« préparer l'évaluation de la Recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, évaluation qui sera transmise au Comité des Ministres avant la fin de l'année 2002, à sa demande et par l'intermédiaire du CDCJ »*), le troisième rapport d'évaluation sera présenté au Comité des Ministres en 2002, par l'intermédiaire du Comité européen de coopération juridique (CDCJ). Etant donné les liens étroits entre les tâches de son Groupe de travail sur la protection des données et les données policières et judiciaires en matière pénale (CJ-PD/GT-PJ), et le contenu de la Recommandation n° R (87) 15, le CJ-PD a décidé de confier à son Groupe de travail l'élaboration d'un projet de rapport sur la troisième évaluation de cette Recommandation. Ce rapport a été soumis au CJ-PD pour révision et approbation lors de sa 40ème réunion plénière du7 au 9 octobre2002.

3. Lors de la préparation du rapport sur la troisième évaluation de la Recommandation n° R (87) 15 il a été pris en compte : des deux évaluations précédentes ; du Séminaire régional sur « La protection des données dans le secteur de la police », organisé par le Conseil de l'Europe en 1999 dans le cadre de ses « Activités pour le développement et la consolidation de la stabilité démocratique » (ADACS) et en tant que contribution au Pacte de stabilité pour l'Europe du sud-est ; des résultats du Projet « Lutte contre la criminalité et protection des données à caractère personnel » (Programme FALCONE) qui a été lancé sur l'initiative des commissions italienne et portugaise pour la protection des données et approuvé et parrainé par la Commission des Communautés européennes ; ainsi que des faits nouveaux survenus depuis la dernière évaluation, en particulier de la jurisprudence de la Cour européenne des Droits de l'Homme en la matière .

4. Conformément aux instructions ci-dessus, et ayant à l'esprit les documents et activités susmentionnés, le rapport sur la troisième évaluation de la Recommandation R(87)15 visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police a été élaboré. Afin de préparer ce troisième rapport d'évaluation, le CJ-PD a examiné la Recommandation n° R (87) 15 et est convenu que les principes qu'elle contient sont toujours pertinents et a considéré qu'il n'est pas nécessaire de les réviser à présent. En outre, le groupe de travail a signalé que des instruments juridiques internationaux, tels l'Accord de Schengen et la Convention Europol, font référence à la recommandation. En conséquence, le CJ-PD ne recommande ni la révision de la Recommandation n° R(87)15, ni la préparation d'une nouvelle recommandation dans le secteur de

la police. Le CJ-PD a noté cependant, depuis le dernier rapport d'évaluation en 1998, beaucoup de nouveaux développements dans ce secteur qui méritent d'être examinés. Le CJ-PD a convenu qu'il serait possible d'aborder ces nouveaux développements par une interprétation téléologique de la présente recommandation.

5. Le CJ-PD a révisé et adopté le rapport sur la troisième évaluation de la Recommandation n° (87) 15 visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police lors de sa 40ème réunion du 7 au 9 octobre 2002. Le CJ-PD a soumis ce rapport au CDCJ lui demandant de transmettre le rapport sur la troisième évaluation au Comité des Ministres en 2002.

6. Compte tenu de la composition multidisciplinaire[1] du Groupe de travail (CJ-PD/GT-PJ) qui a préparé le premier projet de rapport sur la troisième évaluation, de la conclusion du rapport sur la deuxième évaluation de la Recommandation n° R (87) 15 (*« […] donner de nouvelles orientations aux législateurs des Etats membres […]. Ces orientations pourraient être définies en étroite collaboration avec le CDPC ; 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 »*], ainsi que des questions concernées (données policières et judiciaires en matière pénale), le CJ-PD a suggéré que le CDCJ envoie la version définitive du rapport, pour information, au Comité européen pour les problèmes criminels (CDPC) et, sous réserve de l'accord de ce dernier, à ses comités compétents, notamment au Comité d'experts sur l'éthique de la police et les problèmes liés à l'exercice de la police (PC-PO) et au Comité d'experts sur le fonctionnement des conventions européennes dans le domaine pénal (PC-OC).

RAPPORT

a) Différences entre données judiciaires et données policières

7. Dans la procédure pénale, des données à caractère personnel peuvent être traitées simultanément, y compris dans des documents identiques, par la police et par les autorités judiciaires. Les écoutes téléphoniques sont un bon exemple de la nature hybride de certaines données : en cas d'autorisation de l'écoute par un juge, les données sont recueillies par la police avant d'être transmises à nouveau à une autorité judiciaire. Dans certains cas, par conséquent, les limites entre les deux catégories s'estompent : certaines données policières sont transmises au secteur judiciaire, tandis qu'une partie des données judiciaires reste dans le secteur policier. Ceci peut rendre difficile la distinction entre données judiciaires et données policières et ne doit pas servir de prétexte pour éviter d'appliquer les principes de protection des données dans ces secteurs ou de déterminer qui est le maître du fichier et

[1] Le CJ-PD a nommé les quatre experts suivants :
- M. Marc BUNTSCHU, Suisse (Chef suppléant du Secrétariat du Préposé fédéral à la protection des données)
- M. Giovanni BUTTARELLI, Italie (Secrétaire général de la Garante per la Protezione dei Dati Personali)
- M. Alexander PATIJN, Pays-Bas (Conseiller juridique au ministère de la Justice)
- Mme Kinga SZURDAY, Hongrie (Conseillère juridique principale au ministère de la Justice).

Conformément au mandat du CJ-PD, le Comité européen pour les problèmes criminels (CDPC) et ses comités subordonnés compétents peuvent également entrer dans la composition du CJ-PD/GT-PJ. C'est ainsi que trois autres experts ont été admis à siéger au CJ-PD/GT-PJ :
- M. Hughes BRULIN, Belgique (Conseiller juridique adjoint, Direction générale de la Législation pénale et des Droits de l'Homme du ministère de la Justice) a été nommé par le Comité européen pour les problèmes criminels (CDPC).
- Mme Elenor GROTH, Suède (Conseillère juridique au ministère de la Justice) a été nommée par le Comité d'experts sur l'éthique de la police et les problèmes liés à l'exercice de la police (PC-PO).
- M. Philippe BIJU-DUVAL, France (Adjoint au Chef, bureau du Droit communautaire et du Droit comparé, ministère de la Justice - service des Affaires européennes et internationales) a été nommé par le Comité d'experts sur le fonctionnement des conventions européennes dans le domaine pénal (PC-OC).

quels sont les différents degrés de responsabilité impliqués par chaque opération de traitement. Néanmoins, il est clair que chaque niveau d'autorité doit respecter les règles qui sont les siennes.

8. Il convient de trouver des critères permettant de déterminer les règles spécifiques à appliquer. A cette fin, conformément à l'article 2.d de la Convention 108, le terme *maître du fichier* désigne *« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées »*. Il est donc indispensable que la législation nationale de chaque pays détermine clairement si le maître du fichier de données est l'autorité de police ou de justice. En outre, la finalité du traitement des données peut aussi servir de critère complémentaire.

9. Etant donné les considérations ci-dessus, le Groupe de travail a formulé la conclusion suivante :

I. Différences entre données judiciaires et données policières
Afin d'établir une distinction entre données judiciaires et données policières, il conviendrait d'indiquer clairement qui est le maître du fichier, au sens de l'article 2, paragraphe 2, alinéa d. de la Convention 108, en ce qui concerne les données judiciaires et les données policières. Il n'est pas nécessaire que le maître du fichier en ce sens soit la même autorité que l'autorité responsable des décisions relatives aux enquêtes pénales ou de la conduite de ces enquêtes. Un soin particulier doit être accordé à empêcher toute échappatoire en matière de responsabilités, en particulier dans les cas de collecte et d'utilisation par la police de données à caractère personnel sur la base d'une décision judiciaire autorisant le recours à des méthodes intrusives telles que l'interception de télécommunications.

b) Types de fichiers détenus par la police

10. Conformément au paragraphe 36 du Mémorandum explicatif de la Recommandation n° R (87) 15, le terme « fichier de police » désigne toutes les données à caractère personnel structurées ou organisées, gérées par les services de police et répondant à leurs besoins en matière de prévention ou de répression des infractions pénales ou de maintien de l'ordre public. Selon cette définition, les fichiers permettent à la police d'extraire des informations relatives à des personnes identifiées ou identifiables.

11. Ces fichiers sont de divers types, selon la finalité pour laquelle ils ont été créés. Du point de vue de la protection des données, le classement des fichiers de police dans une catégorie particulière est très important car il déterminera le type de contrôle qui sera exercé sur les données à caractère personnel qui y sont contenues.

12. Le principe 1.4 de la Recommandation n° R (87) 15 affirme que « 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. »

13. Le CJ-PD a examiné les divers types de fichiers détenus par la police et fait une distinction entre « fichiers permanents » et « fichiers ad hoc » (constitués à l'occasion d'affaires particulières), conformément à la terminologie employée dans la Recommandation n° R(87)15. Le CJ-PD a convenu que les « fichiers d'analyse » prévus par la Convention Europol, ainsi que ce que l'on appelle des

« fichiers temporaires » ou des « fichiers de travail » dans d'autres contextes, étaient considérés comme des fichiers ad hoc au sens du Principe 1.4, paragraphe 2 de la Recommandation n° R(87)15.

14. Le CJ-PD a également convenu que les deux types de fichiers – permanents et ad hoc – pouvaient contenir des « informations criminelles » (parfois appelées « données douces »), qui sont des données non vérifiées et dont le lien avec les objectifs de la police doit être établi. Les données de ce type, qui donnent des indications non confirmées ou font naître des soupçons sur la participation d'une personne à une ou plusieurs infractions pénales, peuvent poser des problèmes du point de vue de la protection des données car elles peuvent être traitées à des fins différentes, voire à des fins générales de prévention, même si elles ne sont ni suffisantes ni exactes. Ces informations criminelles, en tant que phénomène nouveau non spécifiquement traité dans la Recommandation n° R(87)15, ont fait l'objet d'un examen dans le rapport de la deuxième évaluation de cette Recommandation, et certaines propositions ont été faites (voir document CJ-PD(2002)01). L'autre type de données contenues dans les fichiers permanents et ad hoc sont les données dites « solides », qui ont déjà été vérifiées. La principale différence entre ces « données solides » et les « informations criminelles » ou « données vagues » est le degré d'exactitude ou de fiabilité (à cet égard voir le Principe 2, paragraphe 2 de la Recommandation n° R(87)15).

15. Du point de vue de la protection des données, le contrôle exercé sur les fichiers permanents est plus strict, du moins en termes de notification, communication et stockage, que celui qui est exercé sur les fichiers ad hoc. Néanmoins, le caractère non-permanent de ces fichiers ad hoc devrait inciter les autorités de protection des données à contrôler la qualité de ces données de manière plus fréquente. S'agissant des fichiers ad hoc, il convient de garder présent à l'esprit que, conformément au Principe 1.4 de la Recommandation n° R (87) 15, les fichiers ad hoc ayant été créés en relation avec une enquête particulière doivent également être notifiés à l'autorité de contrôle, conformément aux conditions définies par cette dernière, compte tenu du caractère particulier de ces fichiers, ou conformément à la législation nationale. C'est pourquoi le CJ-PD a examiné ces fichiers ad hoc dans le détail.

16. Il est convenu que l'on pouvait distinguer deux types de fichiers ad hoc :

- les fichiers ad hoc constitués pour résoudre une infraction pénale déterminée qui a déjà été commise ;

- les fichiers ad hoc constitués pour réunir des informations au sujet d'un phénomène criminel particulier, par exemple dans un secteur donné de la société qui, selon certains indices, serait touché par la criminalité. Parmi ces fichiers figurent les « fichiers d'analyse », qui sont largement utilisés pour collecter de grandes quantités de données afin d'obtenir des informations sur des secteurs éventuellement criminels de la société. Comme on l'a vu plus haut, ces fichiers ne sont pas nécessairement limités dans le temps.

17. Un fichier ad hoc établi afin d'obtenir des informations au sujet d'un phénomène criminel particulier ne peut être constitué que s'il est nécessaire pour la prévention d'un danger réel dans le sens du principe 2.1 de la Recommandation n° R (87) 15. Ces fichiers peuvent remplir une fonction proactive, afin de rassembler des informations pour la prévention d'un crime ou pour identifier des auteurs. Il serait peut-être nécessaire que le droit fournisse des garanties de procédure spécifiques afin d'assurer que le critère de danger réel soit respecté. La décision de constituer le fichier peut être limité à une certaine autorité et le principe de transparence dans le sens de l'article 8.a de la Convention 108 devrait être pris en compte. Une dérogation du principe de transparence n'est possible que si les conditions de l'article 9 de la Convention 108 sont remplies. Le droit peut également prévoir une procédure qui oblige un contrôle de la nécessité de maintenir ces types de fichiers ad hoc, par exemple par l'autorité qui a décidé de constituer le dossier.

18. Pour la constitution d'un tel fichier, les catégories de personnes et les catégories de données collectées au sujet de ces personnes devraient être précisées d'une manière exhaustive et devraient être en principe transparentes. La personne concernée devrait donc pouvoir établir si elle peut figurer dans le fichier et, si c'est le cas, quels types de données la concernant peuvent être enregistrées.[2] Quelques exemples de ce type de fichier ad hoc sont les suivants : une série de viols non élucidés pendant une certaine période dans une zone géographique donnée. Un autre exemple encore pourrait être l'exécution de missions de police dans le cas d'un événement particulier, tel qu'un match de football ou une réunion importante de responsables politiques. Comme fichiers ad hoc de nature plus durable, on peut citer les fichiers constitués pour réunir des informations criminelles sur des activités terroristes durables ou des formes particulières de criminalité organisée. De même, un fichier créé pour réunir des données sur les hooligans afin de lutter contre la violence liée à de futurs matchs de football (et non à un seul match) peut être qualifié de fichier ad hoc plus durable.

19. Des fichiers ad hoc constitués afin d'obtenir des informations au sujet d'un phénomène criminel particulier devraient être distingués des fichiers ad hoc constitués pour une enquête portant sur une infraction pénale particulière, afin de permettre aux autorités d'instruction d'engager des poursuites.

20. L'échange de données entre différents fichiers ad hoc n'est possible que s'il existe un intérêt légitime au sens défini au principe 5.1 de la Recommandation R (87) 15. Des systèmes d'indexation et des critères de recherche peuvent être mis en place à l'intérieur des fichiers permanents et entre eux et à l'intérieur des fichiers ad hoc pour déterminer si un tel intérêt légitime est présent. S'agissant d'un fichier ad hoc créé pour obtenir des connaissances au sujet d'infractions pénales graves, l'établissement de liens avec d'autres fichiers ad hoc est plus problématique car ces dossiers contiennent généralement de nombreuses données collectées sur la base de critères plus lâches. Néanmoins, la gravité des infractions pénales concernées peut justifier la mise en place d'un système d'indexation entre des fichiers ad hoc de ce type, afin d'identifier la présence ou non d'informations utiles dans un autre fichier créé à des fins d'analyse.

21. Les fichiers ad hoc créés pour enquêter sur une infraction pénale particulière peuvent, cependant, contenir une quantité indéterminée de données, celles-ci pouvant être nécessaires pour garantir au suspect un procès équitable. Les éléments de preuve éventuels, y compris les éléments d'exonération de responsabilité, ne peuvent être supprimés, même s'ils portent sur des tierces parties liées de manière indirecte à l'enquête sur une infraction pénale. L'utilisation d'un système d'indexation entre des fichiers ad hoc de ce deuxième type ne peut être justifiée que sur la base d'un lien concret clairement identifié au préalable. On peut aussi considérer qu'un tel lien concret est présent lorsqu'il existe des raisons de penser que l'utilisation d'un système d'indexation entre des fichiers ad hoc différents peut permettre d'obtenir les éléments de preuve en question ou de vérifier l'exactitude des données. Le système d'indexation ne peut, cependant, être utilisé pour « aller à la pêche aux informations » dans tous les fichiers, dans le cadre d'une enquête sur une infraction pénale, de quelque nature qu'elle soit. Les atteintes arbitraires aux droits fondamentaux des tierces personnes, en particulier en ce qui concerne le droit au respect de la vie privée, pourront ainsi être évitées.

22. La police peut être amenée à contrôler des données à caractère personnel n'ayant pas encore fait l'objet d'une évaluation quant à leur inclusion dans un fichier permanent ou dans un fichier ad hoc. Les disques durs ou les carnets d'adresses saisis au cours d'une perquisition sont des exemples de telles données. Les copies de disques durs, les transcriptions d'écoutes téléphoniques ou les courriers électroniques interceptés peuvent aussi contenir des données à caractère personnel

[2] L'article 12.1 de la Convention Europol et l'article 6 de l'Acte du Conseil du 3 novembre 1998 adoptant les règles applicables aux fichiers d'Europol créés à des fins d'analyse (1999/C26/01) sont des exemples qui remplissent ces critères.

dénuées de pertinence du point de vue des finalités policières ou judiciaires. Ces données devraient être conservées ou enregistrées séparément avant d'être évaluées et éventuellement incluses dans un fichier de police. L'utilisation de ces données à d'autres fins ne peut être envisagée que pour empêcher une menace immédiate grave comme celle d'une agression terroriste.

23. Etant donné les considérations ci-dessus, le Groupe de travail a formulé les conclusions suivantes :

II. Fichiers permanents

Il conviendrait, lors de la création de fichiers permanents, de spécifier les finalités pour lesquelles ils ont été créés ainsi que les critères d'inclusion de données à caractère personnel à l'autorité de contrôle, afin de permettre aux personnes de prévoir si leurs données peuvent y être stockées ou non.

III. Fichiers ad hoc constitués pour enquêter sur une infraction pénale particulière

La collecte de données pour un fichier ad hoc qui a été constitué pour enquêter sur une infraction pénale particulière est liée à la finalité du fichier. Il peut s'ensuivre qu'un fichier contienne une variété indéterminée de données, ne serait-ce que pour éviter le risque d'en exclure les données d'exonération de responsabilité. L'utilisation non sélective de données de ce type, quelles que soient les finalités de cette utilisation par la police, peut équivaloir à une surveillance générale de la personne sur laquelle portent les données et conduire par conséquent à une atteinte arbitraire à ses droits et libertés fondamentales, en particulier sa vie privée. L'utilisation de données à caractère personnel contenues dans un fichier ad hoc aux fins d'un autre fichier ad hoc créé en relation avec une enquête spécifique ne peut être considérée comme compatible avec les finalités pour lesquelles le premier fichier a été créé que lorsqu'il existe entre les deux fichiers ou entre les données à caractère personnel contenues dans les fichiers un lien concret justifiant une telle utilisation. Des données qui sont apparemment sans rapport avec la finalité, par exemple les résultats d'une interception de télécommunications ou la saisie d'un disque dur, devraient être supprimées ou *renvoyées*.

IV. Fichiers ad hoc créés pour l'analyse d'un phénomène criminel particulier

Il conviendrait que les fichiers ad hoc créés pour l'analyse d'un phénomène criminel particulier définissent avec un degré certain de précision les catégories de personnes au sujet desquelles des données peuvent être stockées, ainsi que les catégories de données concernant ces personnes. Dans les cas d'infractions pénales graves, il peut être nécessaire d'établir des comparaisons entre deux fichiers ad hoc de ce type. Lorsque la comparaison permet d'établir un lien concret, les données du premier fichier ad hoc pourraient aussi être utilisées aux fins du second fichier ad hoc et inversement.

V. Systèmes d'indexation

Les risques que font peser les fichiers ad hoc sur les droits et les libertés fondamentales, en particulier le droit au respect de la vie privée, pourraient être déjoués au moyen de sauvegardes matérielles et procédurales compensatoires s'appliquant à l'utilisation des données. Des règles spécifiques, en particulier, doivent s'appliquer à l'utilisation des systèmes d'indexation permettant d'accéder aux données de différents fichiers ad hoc. Ces règles devraient maintenir un équilibre entre l'obligation de protéger les droits et les libertés fondamentales, en particulier le droit au respect de la vie privé, et la nécessité d'utiliser les données pour lutter efficacement contre les infractions pénales.

VI. Utilisation incompatible des fichiers ad hoc

L'utilisation des fichiers ad hoc pour une recherche de données à caractère personnel ne pouvant pas être considérée comme un type d'utilisation compatible doit être réglementée par le code national de procédure pénale ou d'autres textes conformément à l'article 9 de la Convention 108.

c) Catégories de personnes au sujet desquelles des données peuvent être stockées

24. Dans le rapport de la deuxième évaluation de la Recommandation n° R (87) 15, il a été 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 aux crimes organisés 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 »* (voir document CJ-PD(2002)01).

25. Conformément au Principe 2 de la Recommandation n° R (87) 15, 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 réel ou à la répression d'une infraction pénale déterminée. Le paragraphe 2 de l'article 8 de la Convention européenne des Droits de l'Homme énonce qu'il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée et familiale que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire, entre autres, à la sécurité nationale, à la défense de l'ordre et à la prévention des infractions pénales. En conséquence, selon la jurisprudence de la Cour européenne des Droits de l'Homme, le stockage des données à caractère personnel pour des motifs de sécurité nationale ou de lutte contre la criminalité constitue une atteinte à la vie privée et doit avoir un fondement juridique réunissant les conditions requises par l'article 8, paragraphe 2 de la Convention européenne des Droits de l'Homme. L'arrêt le plus explicite à cet égard est celui qui a été rendu dans l'affaire Rotaru contre Roumanie, qui énonce :

« La Cour relève à cet égard que la loi n° 14/1992 prévoit, dans son article 8, que peuvent être recueillis, consignés et archivés dans des dossiers secrets des renseignements touchant à la sécurité nationale.

Or, aucune disposition du droit interne ne fixe les limites à respecter dans l'exercice de ces prérogatives. Ainsi, la loi interne ne définit ni le genre d'informations pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de données, ni les circonstances dans lesquelles peuvent être prises ces mesures, ni la procédure à suivre. De même, la loi ne fixe pas de[s] *limites quant à l'ancienneté des informations détenues et la durée de leur conservation.*

Quant à l'article 45, celui-ci habilite le SRI à reprendre, à toutes fins de conservation et utilisation, les archives ayant appartenu aux anciens organes de renseignements compétents sur le territoire de la Roumanie, et autorise la consultation des documents du SRI sur approbation du directeur.

La Cour relève que cet article ne renferme aucune disposition explicite et détaillée sur les personnes autorisées à consulter les dossiers, la nature de ces derniers, la procédure à suivre et l'usage qui peut être donné aux informations ainsi obtenues. »[3]

26. Cet arrêt est rendu relativement à la sécurité nationale, mais il est considéré comme s'appliquant également aux données policières recueillies dans des dossiers ad hoc aux fins d'analyses de phénomènes criminels spécifiques. De même, il conviendrait de spécifier les catégories de personnes au sujet desquelles des données peuvent être recueillies et stockées, le type d'informations qui peuvent être enregistrées, etc.

[3] CEDH, Rotaru contre Roumanie, Arrêt du 4 Mai 2000, Série A, paragraphe 57.

27. S'agissant des catégories de personnes au sujet desquelles des données peuvent être stockées, il convient de souligner qu'elles devraient être déterminées de manière à ce que les personnes puissent raisonnablement prévoir si leurs données peuvent être stockées ou non. Le CJ-PD a souligné que la définition de ces catégories de personnes s'applique aux fichiers de police contenant des données ayant fait l'objet d'une évaluation et considérées comme nécessaires aux fins du fichier par les autorités de police et non aux données « brutes ». Parmi ces catégories de personnes, on pourrait distinguer :

- les personnes au sujet desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction (suspects) ;

- les personnes condamnées pour avoir commis une infraction pénale ;

- les victimes de l'infraction pénale ;

- les témoins;

- les tiers par rapport à l'infraction pénale. Pourraient être incluses dans cette catégorie les personnes qui sont indirectement liées à l'enquête portant sur des infractions pénales (contacts, informateurs, des personnes dont l'identité est révélée pendant l'enquête etc.) et qui ont souvent une relation directe ou indirecte avec les sujets principaux de l'enquête. Cette catégorie comprend les personnes qui sont nécessaires à l'enquête au sujet d'une infraction pénale mais qui ne peuvent être incluses dans aucune des catégories précédentes.

28. Etant donné les considérations ci-dessus, la conclusion suivante est formulée :

VII. Catégories de personnes au sujet desquelles des données peuvent être stockées

Il conviendrait d'indiquer en ce qui concerne les dossiers ad hoc aux fins d'analyse de phénomènes criminels spécifiques, les catégories de personnes au sujet desquelles des données peuvent être collectées et stockées, ainsi que le type d'informations qui peuvent être enregistrées. Ces catégories devraient être définies avec suffisamment de précision pour que les personnes puissent raisonnablement prévoir si elles en font partie ou non.
Des données à caractère personnel au sujet de tiers par rapport à l'enquête judiciaire ne devraient être collectées et stockées que lorsqu'il y a un lien concret avec la finalité pour laquelle un fichier a été créé.
Il conviendrait d'indiquer les catégories de tiers au sujet desquels des données peuvent être collectées et stockées parce que ces tiers ont une certaine relation avec les personnes qui sont les sujets principaux de l'enquête judiciaire ou parce que la collecte de ces données est nécessaire pour satisfaire aux exigences d'un procès équitable.
Il conviendrait de prévoir un réexamen périodique des données stockées afin d'établir le caractère adéquat de la catégorie dans laquelle elles ont été stockées.

d) Durée de stockage et effacement des données

29. Le principe 7 de la Recommandation n° R (87) 15 énonce :

« 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. »

En tenant compte du principe ci-dessus, le CJ-PD a examiné la question de la durée de conservation des données à caractère personnel traitées par la police à la lumière des développements survenus pendant les dernières années concernant cette question.

30. En ce qui concerne la durée de stockage des données, on a fait remarquer que la règle générale était que si les données ne sont plus nécessaires à la finalité pour laquelle elles ont été recueillies ni à d'autres finalités ultérieures, elles devraient être effacées ou archivées.

31. La question de la conservation des données recueillies par la police, et en particulier leur effacement, devrait néanmoins être examinée du point de vue : de la réhabilitation des personnes condamnées; des affaires non élucidées (dans certains pays la durée pendant laquelle un dossier reste ouvert est limitée) ; de la réinsertion sociale des condamnés qui ont purgé leur peine ; et de la possibilité de reconnaître les multirécidivistes.

32. A cet égard, on a souligné que le casier judiciaire n'était pas un fichier de police dans tous les pays. En vertu de l'article 9 de la Convention 108, relatif aux exemptions et restrictions, des procédures spéciales peuvent être mises en place pour la consultation de ces fichiers à des fins appropriées, par exemple pour vérifier les antécédents de candidats à des fonctions particulières. Il faudrait toutefois tenir compte des dispositions de la Recommandation n° R (84) 10 du Conseil de l'Europe sur le casier judiciaire et la réhabilitation des condamnés.

33. Le CJ-PD a examiné la possibilité de prescrire des durées maximales pour le stockage des données. Dans l'établissement de ces durées de stockage, il convient de prendre en compte la période de prescription de l'infraction pénale à laquelle se rapportent les données. La pertinence des données du point de vue de la prévention de futures infractions pénales – dans le cas des infractions graves – peut être un critère justifiant l'allongement de la durée maximale de stockage. La procédure de réexamen dans le cadre de l'accord de Schengen prévoit l'effacement des données au bout d'un an, sauf si la police peut justifier leur non-effacement. La Recommandation n° R (87) 15 fait une distinction entre les fichiers permanents (qui peuvent être conservés pendant deux ou trois décennies) et les fichiers ad hoc, constitués pour des tâches spécifiques telles que réunions au sommet, surveillance d'organisations particulières ou manifestations publiques (dont la conservation doit être justifiée lorsque l'événement est terminé).

34. En ce qui concerne les données non confirmées contenues dans des fichiers permanents ou ad hoc, il conviendrait de procéder à des réexamens périodiques tous les trois ou cinq ans pour vérifier la qualité de ces données et se prononcer sur leur nécessité. Une fois atteinte la finalité des fichiers ad hoc, il faudrait se demander s'il y a lieu de les supprimer ou de les transférer à la banque centrale de données ou aux archives. On a soulevé le problème des données qui sont recueillies et conservées parce qu' « on ne sait jamais » quand les informations pourront être utiles. La notion de « danger réel » qui figure à l'article 2 de la Recommandation n° R (87) 15 semble exclure cela.

35. Il faudrait également instituer un réexamen périodique des données confirmées afin de vérifier leur qualité et de décider si leur stockage demeure nécessaire.

36. Etant donné les considérations ci-dessus, la conclusion suivante est formulée :

VIII. Durée de stockage et effacement de données

La durée de stockage des données à caractère personnel traitées par la police devrait être établie en fonction du principe de nécessité par rapport aux finalités pour lesquelles ces données ont été stockées.
La jurisprudence de certaines autorités de contrôle nationales de protection des données interprète strictement la « nécessité » en lui prêtant le même sens qu'à l'adjectif « indispensable » (par exemple, lorsqu'il est procédé à la collecte des données). Cependant, on peut fort bien estimer, au moment de la collecte d'informations par une autorité judiciaire, que ces données sont nécessaires, et constater ultérieurement, en fonction de l'évolution de l'enquête, qu'elles sont en fait dénuées de pertinence. Il convient autant que possible de fixer des durées de stockage maximales pour les différentes catégories de données à caractère personnel traitées par la police, dans un souci de transparence du système judiciaire. Des vérifications périodiques de la qualité des données à caractère personnel devraient être effectuées dans tous les cas. Quand les données ne sont plus nécessaires pour les finalités de police pour lesquelles elles ont été collectées, elles devraient être effacées ou stockées pour des fins de recherche historique, scientifique ou statistique. Leur stockage devrait être accompagné de garanties et mesures de sécurité afin d'empêcher leur utilisation à d'autres fins. Dans des cas exceptionnels et en conformité avec l'article 9 de la Convention 108, le droit interne peut établir des conditions pour la réutilisation de ces données pour des finalités de police, si ces données sont nécessaires à des procédures de révision ou pour une enquête criminelle particulière.

e) Vérification des antécédents de particuliers

37. Le Principe 5.3 de la Recommandation n° R (87) 15 énonce que « *la communication de données à des personnes privées ne devrait être permise que si, dans un cas déterminé, il y obligation ou autorisation légales claires de l'autorité de contrôle. 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 ».

38. En liaison avec ce principe, il a été débattu[4] de la vérification des antécédents de particuliers en vue de leur emploi éventuel dans des postes sensibles, à l'aide de données collectées par la police. Le principe 5.3.i de la Recommandation n° R (87) 15 exclut en principe la communication de données de police à des personnes privées. Néanmoins, dans certains pays, et avec le consentement de la personne concernée, le casier judiciaire et les données de police peuvent constituer le fondement d'un avis pour déterminer si une personne est adaptée à un poste spécifique. L'avis est donné par une autorité indépendante également de la personne qui postule et de la personne qui prend la décision au sujet de la demande. Les données de police peuvent également jouer un rôle important lorsqu'il s'agit d'apprécier la fiabilité d'entreprises participant à une procédure de passation de marchés publics.

[4] Des opinions divergentes ont été exprimées à cet égard : pour certains experts, ce texte sur la vérification des antécédents de particuliers serait en contradiction avec le contenu du Principe 5.3 de la Recommandation n° R(87)15 et il fallait donc le supprimer ; pour d'autres, cette question posait un nouveau problème qui devrait être traité dans le cadre de la présente évaluation, et le texte de ce paragraphe n'était pas en contradiction avec le Principe 5.3.

f) Transfert de données vers des pays tiers n'assurant pas un niveau adéquat de protection

39. Le CJ-PD a examiné la question du transfert de données vers des pays tiers n'assurant pas un niveau adéquat de protection des données. Ce type de transfert peut conduire à une atteinte aux droits et libertés fondamentales. Néanmoins, la finalité de la lutte contre la criminalité grave peut constituer un intérêt légitime qui prévaut dans le sens du deuxième alinéa de l'article 2.2.a du Protocole additionnel à la Convention 108. Le transfert peut être considéré comme justifié si des garanties spécifiques sont prévues. Des accords bilatéraux ou multilatéraux sur l'échange de données de police[5] peuvent, pour les finalités de la protection des données, contenir des dispositions qui concernent:

- les finalités de l'utilisation des données ;
- les types de données concernées par le transfert ;
- les autorités susceptibles d'assurer le contrôle des données ;
- l'interdiction s'appliquant en principe au transfert des données à d'autres autorités ou particuliers ;
- l'obligation de garantir le droit des personnes sur lesquelles portent les données à l'information sur ces données et à la rectification de des données, ainsi qu'à l'information sur le droit interne des Parties qui restreignent ces droits ;
- l'obligation d'effacer les données une fois atteintes les finalités pour lesquelles les données ont été transférées et de s'informer réciproquement des durées maximales de stockage des données prévues par la législation de chaque pays ;
- la possibilité pour les personnes sur lesquelles portent les données de disposer d'un véritable moyen de recours devant une autorité indépendante.

CONCLUSIONS

40. Le CJ-PD a demandé au CDCJ de soumettre les recommandations suivantes au Comité des Ministres :

a) il ne faudrait pas recommander, dans cette troisième évaluation, de révision de la Recommandation n° R (87) 15 visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police, du fait qu'il a été considéré que les principes énoncés dans la recommandation sont toujours pertinents et continuent à constituer un fondement pour l'élaboration de règles sur cette question et servent de point de référence pour toute activité dans ce secteur. En outre, cette recommandation est mentionnée dans d'autres instruments internationaux tels que l'Accord de Schengen et la Convention Europol.

b) la troisième évaluation de la Recommandation n° R (87) 15 devrait être la dernière des évaluations périodiques, qui ont été jusqu'à présent effectuées tous les quatre ans, sur la pertinence de cette recommandation ;

c) l'utilisation de données à caractère personnel dans le secteur de la police reste une préoccupation permanente et en conséquence des évaluations futures de questions particulières liées au développement de nouvelles techniques de traitement des données de police pourraient être effectuées si nécessaire ;

[5] Voir par exemple l'article 18.3 de la Convention Europol.

d) compte tenu des deux recommandations ci-dessus, le CJ-PD demande au CDCJ de prier le Comité des ministres de prendre une décision pour que cette troisième évaluation soit la dernière des évaluations périodiques effectuées par le CJ-PD de la pertinence de la Recommandation n° R (87) 15 mais que, si nécessaire, d'autres évaluations soient effectuées pour des questions particulières.

41. Le CJ-PD a adopté les conclusions suivantes au cours de sa troisième évaluation. Il les soumet au Comité des Ministres et demande l'autorisation de publier le rapport sur le site web du Conseil de l'Europe.

I. Différences entre données judiciaires et données policières

Afin de distinguer entre données judiciaires et données policières, il conviendrait d'indiquer clairement qui est le maître du fichier, au sens de l'article 2, paragraphe 2, alinéa d. de la Convention 108, en ce qui concerne les données judiciaires et les données policières. Il n'est pas nécessaire que le maître du fichier en ce sens soit la même autorité que l'autorité responsable des décisions relatives aux enquêtes pénales ou de la conduite de ces enquêtes. Un soin particulier doit être accordé à empêcher toute échappatoire en matière de responsabilités, en particulier dans les cas de collecte et d'utilisation par la police de données à caractère personnel sur la base d'une décision judiciaire autorisant le recours à des méthodes intrusives telles que l'interception de télécommunications.

II. Fichiers permanents

Il conviendrait, lors de la création de fichiers permanents, de spécifier les finalités pour lesquelles ils ont été créés ainsi que les critères d'inclusion de données à caractère personnel à l'autorité de contrôle, afin de permettre aux personnes de prévoir si leurs données peuvent y être stockées ou non.

III. Fichiers ad hoc constitués pour enquêter sur une infraction pénale particulière

La collecte de données pour un fichier ad hoc qui a été constitué pour enquêter sur une infraction pénale particulière est liée à la finalité du fichier. Il peut s'ensuivre qu'un fichier contienne une variété indéterminée de données, ne serait-ce que pour éviter le risque d'en exclure les données d'exonération de responsabilité. L'utilisation non sélective de données de ce type, quelles que soient les finalités de cette utilisation par la police, peut équivaloir à une surveillance générale de la personne sur laquelle portent les données et conduire par conséquent à une atteinte arbitraire à ses droits et libertés fondamentales, en particulier sa vie privée. L'utilisation de données à caractère personnel contenues dans un fichier ad hoc aux fins d'un autre fichier ad hoc créé en relation avec une enquête spécifique ne peut être considérée comme compatible avec les finalités pour lesquelles le premier fichier a été créé que lorsqu'il existe entre les deux fichiers ou entre les données à caractère personnel contenues dans les fichiers un lien concret justifiant une telle utilisation. Des données qui sont apparemment sans rapport avec la finalité, par exemple les résultats d'une interception de télécommunications ou la saisie d'un disque dur, devraient être supprimées ou renvoyées.

IV. Fichiers ad hoc créés pour l'analyse de phénomènes criminels spécifiques

Il conviendrait que les fichiers ad hoc créés pour l'analyse de phénomènes criminels spécifiques définissent avec un degré certain de précision les catégories de personnes au sujet desquelles des données peuvent être stockées, ainsi que les catégories de données concernant ces personnes. Dans les cas d'infractions pénales graves, il peut être nécessaire d'établir des comparaisons entre deux fichiers ad hoc de ce type. Lorsque la comparaison permet d'établir un lien concret, les données du premier fichier ad hoc pourraient aussi être utilisées aux fins du second fichier ad hoc et inversement.

V. Systèmes d'indexation

Les risques que font peser les fichiers ad hoc sur les droits et les libertés fondamentales, en particulier le droit au respect de la vie privée, pourraient être déjoués au moyen de sauvegardes matérielles et procédurales compensatoires s'appliquant à l'utilisation des données. Des règles spécifiques, en particulier, doivent s'appliquer à l'utilisation des systèmes d'indexation permettant d'accéder aux données de différents fichiers ad hoc. Ces règles devraient maintenir un équilibre entre l'obligation de protéger les droits et les libertés fondamentales, en particulier le droit au respect de la vie privé, et la nécessité d'utiliser les données pour lutter efficacement contre les infractions pénales.

VI. Utilisation incompatible des fichiers ad hoc

L'utilisation des fichiers ad hoc pour une recherche de données à caractère personnel ne pouvant pas être considérée comme un type d'utilisation compatible doit être réglementée par le code national de procédure pénale ou d'autres textes conformément à l'article 9 de la Convention 108.

VII. Catégories de personnes au sujet desquelles des données peuvent être stockées

Il conviendrait d'indiquer les catégories de personnes au sujet desquelles des données peuvent être collectées et stockées, ainsi que le type d'informations qui peuvent être enregistrées. Ces catégories devraient être définies avec suffisamment de précision pour que les personnes puissent raisonnablement prévoir si elles en font partie ou non.

Des données à caractère personnel au sujet de tiers par rapport à l'enquête judiciaire ne devraient être collectées et stockées que lorsqu'il y a un lien concret avec la finalité pour laquelle un fichier a été créé.

Il convient d'indiquer les catégories de tiers au sujet desquels des données peuvent être collectées et stockées parce que ces tiers ont une certaine relation avec les personnes qui sont les sujets principaux de l'enquête judiciaire ou parce que la collecte de ces données est nécessaire pour satisfaire aux exigences d'un procès équitable.

Il convient de prévoir un réexamen périodique des données stockées afin d'établir le caractère adéquat de la catégorie dans laquelle elles ont été stockées.

VIII. Durée de stockage et effacement de données

La durée de stockage des données à caractère personnel traitées par la police devrait être établie en fonction du principe de nécessité par rapport aux finalités pour lesquelles ces données ont été stockées.

La jurisprudence de certaines autorités de contrôle nationales de protection des données interprète strictement la « nécessité » en lui prêtant le même sens qu'à l'adjectif « indispensable » (par exemple, lorsqu'il est procédé à la collecte des données). Cependant, on peut fort bien estimer, au moment de la collecte d'informations par une autorité judiciaire, que ces données sont nécessaires, et constater ultérieurement, en fonction de l'évolution de l'enquête, qu'elles sont en fait dénuées de pertinence. Il convient autant que possible de fixer des durées de stockage maximales pour les différentes catégories de données à caractère personnel traitées par la police, dans un souci de transparence du système judiciaire. Des vérifications périodiques de la qualité des données à caractère personnel devraient être effectuées dans tous les cas. Quand les données ne sont plus nécessaires pour les finalités de police pour lesquelles elles ont été collectées, elles devraient être effacées ou stockées pour des fins de recherche historique, scientifique ou statistique. Leur stockage devrait être accompagné de garanties et mesures de sécurité afin d'empêcher leur utilisation à d'autres fins. Dans des cas exceptionnels et en conformité avec l'article 9 de la Convention 108, le droit interne peut établir des conditions pour la réutilisation de ces données pour des finalités de police, si ces données sont nécessaires à des procédures de révision ou pour une enquête criminelle particulière.