N° 5563²

CHAMBRE DES DEPUTES

Session ordinaire 2007-2008

PROJET DE LOI

relative à l'accès des magistrats et officiers de police judiciaire à certains traitements de données à caractère personnel des personnes morales de droit public et portant modification du code d'instruction criminelle et de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police

* * *

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(4.5.2005)

Conformément à l'article 32, paragraphe 3, lettre (e) de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après désignée „la loi du 2 août 2002"), la Commission nationale pour la protection des données a entre autres pour mission d'„être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi".

C'est dans cette optique, et faisant suite à la demande lui adressée par Monsieur le Ministre délégué aux Communications, que la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi relatif à l'accès des officiers de police judiciaire à certains traitements de données à caractère personnel des personnes morales de droit public.

*

I. REMARQUES PRELIMINAIRES

A) La résurgence des attaques terroristes et le développement de réseaux internationaux de criminalité organisée suscite naturellement des mesures de la part des Etats démocratiques visant à renforcer la sécurité des citoyens face aux menaces qui s'amplifient à l'époque de la globalisation. L'Union européenne travaille à améliorer les moyens de collaboration policière et judiciaire et à faciliter les échanges de données personnelles nécessaires dans cette perspective. La tendance à faciliter l'accès des autorités chargées de la sécurité publique et de la sûreté de l'Etat aux fichiers publics et parfois à certains fichiers privés à suscité également des initiatives législatives nouvelles au niveau national et l'avant-projet de loi sous revue s'inscrit dans cette évolution.

Il est incontestable que la prévention, la constatation et la répression des infractions pénales constitue une finalité légitime pour de telles mesures dès lors qu'elles restent conformes aux principes de l'article 8 paragraphe 2 de la Convention européenne des Droits de l'Homme et qu'en particulier elles ne dépassent pas ce qui dans une société démocratique peut être considéré comme nécessaire pour assurer la sécurité publique, la prévention de la criminalité et la protection des droits et libertés d'autrui.

Il s'agit en revanche d'être vigilant afin de contribuer à ce que les mesures nouvelles ne prennent des proportions excessives ou dépassent ce qui est nécessaire dans les Etats démocratiques pour satisfaire les besoins correspondant à la finalité légitime de protection de la sécurité des citoyens et des Etats eux-mêmes.

En d'autres termes une certaine modération apparaît de mise dans cette démarche afin d'éviter que dans le but de protéger la démocratie, les libertés et droits fondamentaux ne soient affectés de façon telle que c'est la démocratie elle-même qui se retrouve affaiblie par les mesures censées la protéger.

B) Aux termes de l'article 3 paragraphe (3) de la loi du 2 août 2002 ladite loi-cadre s'applique aux traitements de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt économique ou financier important de l'Etat, sans préjudice des dispositions spécifiques de droit national ou international régissant ces domaines.

Comme il ressort de l'exposé des motifs (document parlementaire 4735, p. 83), le législateur a en effet opté pour un champ d'application large qui s'étend également aux personnes morales ainsi qu'aux personnes publiques, aux domaines de la défense, de la sécurité publique et de la sûreté de l'Etat ainsi qu'aux activités liées au droit pénal en vue d'instaurer un régime juridique unifié capable d'offrir un niveau de sécurité juridique approprié aux personnes concernées.

L'inclusion des quatre matières susvisées (méthode adoptée par la loi portugaise et en partie par la loi belge) est permise par la Directive 95/46/CE (du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) et présente les avantages suivants:

- clarification et unification du régime juridique de la protection des données tout en autorisant à l'Etat de prévoir les limitations et dérogations nécessaires à l'exercice de la puissance publique. Certaines limitations et dérogations sont d'ores et déjà comprises dans le projet de loi … Les limitations et dérogations prévues par les lois actuellement en vigueur joueront entièrement, dès lors qu'elles touchent aux personnes morales, à la défense, la sécurité publique, la sûreté et aux activités liées au droit pénal. De plus, des lois spéciales pourront à l'avenir édicter de telles limitations et dérogations.
- modifications légères des règlements grand-ducaux existants en la matière …

Les principes du droit relatif à la protection des données s'appliquent donc en règle générale également dans les quatre matières susvisées.

C) Afin de situer les observations de la Commission nationale pour la protection des données dans le contexte légal approprié, il parait également indiqué de rappeler d'emblée la teneur de l'article 8 de la Convention européenne des Droits de l'Homme (CEDH) intitulé „Droit au respect de la vie privée et familiale" qui dispose que:

„1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui."

Il en découle que la protection de la vie privée est la règle, et que l'ingérence dans l'exercice de ce droit doit rester l'exception.

La Commission nationale ne saurait donc approuver l'introduction de dérogations nouvelles au principe de la protection de la vie privée par l'avant-projet de loi sous avis dès lors que le juste équilibre entre le principe et les exceptions reste préservé.

D) Rappelons aussi la jurisprudence de la Cour européenne des droits de l'homme selon laquelle l'enregistrement et la conservation a priori des données ne peut en aucun cas mener à des mesures de surveillance exploratoires ou générales (Arrêts Klass (arrêt du 6 septembre 1978, Publ. Cour, Série A, No 28, p. 23 et s) et Malone).

„La Cour souligne néanmoins que les Etats contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espion-

nage et le terrorisme, n'importe quelle mesure jugée par eux appropriée." (cf. arrêt Klass et autres du 6 septembre 1978, série A No 28, pp. 23-24, paras. 49-50);

„Néanmoins, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus car un système de surveillance secrète destiné à protéger la sécurité nationale crée un risque de saper, voire de détruire, la démocratie au motif de la défendre" (cf. arrêt Leander, No 10/1985/96/144, du 25 février 1987, point 60).

E) Il est intéressant de relever à cet égard que la Cour de Justice des Communautés Européennes a, elle aussi, dans un arrêt récent du 20 mai 2003, soumis le contrôle de la compatibilité de la réglementation nationale (en l'occurrence autrichienne) avec les dispositions de la directive (95/46/CE) à une vérification préalable de sa compatibilité avec l'article 8 de la Convention européenne des droits de l'homme (CEDH) sur la protection de la vie privée en soulignant que la communication, par l'employeur à un tiers, de données relatives aux revenus perçus par un travailleur ou un pensionné est une ingérence dans la vie privée au sens de l'article 8 de la CEDH qui ne peut être justifiée que si elle est prévue par la loi, poursuit un but légitime visé dans cet article et est nécessaire dans une société démocratique pour atteindre ce but (cf. Affaires jointes C-465/00, C-138/01 et C-139/01 – Rechnungshof (C-465/00) contre Österreichischer Rundfunk et autres et Christa Neukomm (C-138/01) et Joseph Lauermann (C-139/01) contre Österreichischer Rundfunk).

La marge de manoeuvre du législateur se trouve donc enfermée dans les limites posées par l'article 8 paragraphe 2 de la CEDH.

F) La Commission nationale aimerait dans ce contexte encore relever le „rapport sur l'incidence des principes de la protection des données sur les données judiciaires en matière pénale y compris dans le cadre de la coopération judiciaire en matière pénale", qui prévoit plus particulièrement sous les points 10 et 54:

„10. En vertu de l'article 3 de la Convention 108: „Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé. Le champ d'application de la Convention devrait donc en principe englober les données à caractère personnel relatives à des individus impliqués dans une procédure judiciaire et soumises à des traitements automatisés par le système judiciaire si les Parties à la Convention n'ont pas exclu ces catégories de fichiers automatisés à caractère personnel du champ d'application de la Convention, en conformité avec l'article 3, paragraphe 2, alinéa a, de la Convention 108. En outre, la Convention 108 peut aussi s'appliquer aux données judiciaires à caractère personnel ne faisant pas l'objet de traitements automatisés, pour peu que les Parties aient fait la déclaration mentionnée à l'article 3, paragraphe 2, alinéa c.

54. Des autorités nationales de contrôle de la protection des données ont été mises en place dans la quasi-totalité des pays d'Europe. Elles jouissent de compétences leur permettant d'assurer le respect et l'intégration au droit interne des principes énoncés dans la Convention 108 ainsi que des dispositions de la législation nationale en matière de la protection des données. Elles sont par conséquent également habilitées à surveiller, contrôler et vérifier l'application de ces principes dans différents secteurs. Néanmoins, dans certains pays, des autorités indépendantes de contrôle de la protection des données ont été mises en place pour contrôler les échanges d'information entre les autorités judiciaires et le traitement des données par ces mêmes autorités. Dans ces pays, on a considéré, d'une part, que les autorités de contrôle de la protection des données n'avaient en général aucune compétence juridictionnelle et que le principe de la séparation des pouvoirs législatif, exécutif et judiciaire ne permettait pas le contrôle des activités du pouvoir judiciaire. D'autre part, comme les autorités judiciaires collectent et traitent elles-mêmes des données à caractère personnel, il est apparu que ceci pouvait également être soumis à un contrôle des autorités de contrôle de la protection des données. La Convention 108 et son protocole additionnel s'appliquent aux données à caractère personnel concernant les personnes impliquées dans une procédure judiciaire et qui sont traitées par les services judiciaires, sauf dans le cas où les Parties à ces instruments internationaux ont fait une déclaration excluant explicitement ces catégories de données de leur champ d'application, conformément à l'article 3.2.a de la Convention 108."

(http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Rapports/R-Report%20on%20police%20and%20judicial%20data%20f%20090403.asp#TopOfPage

Force est de constater que les réserves formulées par le Grand-Duché de Luxembourg au titre de l'article 3.2. a) de la Convention 108 dans la loi du 19 novembre 1987 portant approbation de cette convention ne visent pas les traitements de données judiciaires, de sorte qu'il faut en conclure que les principes y arrêtés devraient s'appliquer aux données judiciaires.

En effet, l'article 2 de la loi précitée du 19 novembre 1987 dispose que:

„Le Grand-Duché de Luxembourg déclare qu'il se réserve le droit, dans les limites de l'article 3 (2) de la Convention, de ne pas appliquer la Convention

a) aux banques de données qui en vertu d'une loi ou d'un règlement sont accessibles au public;

b) à celles qui contiennent exclusivement des données en rapport avec le propriétaire de la banque;

c) à celles qui sont établies pour compte des institutions de droit international public.“

*

II. ARTICLES 24-1 ET 67-2 NOUVEAUX

A) Un champ d'application très vaste

Aux termes de l'article 24-1 nouveau du code d'instruction criminelle, ce nouveau droit d'accès par voie informatique aux données d'autres personnes morales de droit public à instaurer au bénéfice du Procureur d'Etat et des officiers de police judiciaire agissant sur son instruction aura une portée très étendue, alors que l'article sous commentaire vise indistinctement tous les administrations et services de l'Etat ainsi que tous les établissements publics. Il en est de même en ce qui concerne le juge d'instruction et des officiers de police judiciaire agissant sur commission rogatoire au voeu de l'article 67-2 nouveau du code d'instruction criminelle.

Les articles 24-1 et 67-2 nouveaux à insérer au code d'instruction criminelle (article 1er de l'avant-projet de loi sous avis) visent donc à assurer au procureur d'Etat, aux officiers de police judiciaire (ci-après dénommés en abrégé OPJ) ainsi qu'au juge d'instruction l'accès à toutes données figurant dans des fichiers des personnes morales de droit public, sauf les quelques exceptions prévues par l'avant-projet de loi sous avis.

Tomberaient donc dans le champ d'application des nouvelles dispositions des traitements de données comme ceux opérés par les établissements publics industriels et commerciaux, tels que l'Entreprise des Postes et Télécommunications, la Banque et Caisse d'Epargne de l'Etat ou le Centre thermal de Mondorf-les-Bains.

La Commission nationale estime en revanche qu'il y aurait lieu de limiter la portée des nouvelles dispositions aux fichiers détenus par les personnes morales de droit public comme l'Etat, les communes, les syndicats de communes, les établissements publics administratifs et autres administrations ou services relevant de ces personnes morales ayant pour mission l'exécution d'un service public administratif, à l'exception des entités poursuivant une activité économique ou commerciale, telles que les établissements publics industriels ou commerciaux (cf. Instruction du Gouvernement en conseil du 11 juin 2004 ayant pour objet de fixer une ligne de conduite et des règles générales en matière de création d'établissements publics et retenant la qualification soit d'un établissement public à caractère administratif (EPA), soit d'un établissement public à caractère industriel et commercial (EPIC), soit d'un établissement public à caractère culturel, social et scientifique (EPCSS), à tout établissement à créer).

Dans la mesure où l'intention des auteurs du projet consiste à limiter l'accès à des fichiers détenus – ou à des traitements de données opérés – par des services publics administratifs exerçant une mission d'intérêt général, il faudrait expressément exclure du champ d'application envisagé les personnes de droit public exerçant en tout ou en partie une activité économique.

Il convient en effet d'avoir à l'esprit qu'un accès direct de façon horizontale à un nombre impressionnant de fichiers des différents organismes publics et les moyens informatiques d'exploiter les données sont susceptibles de comporter des risques de non-respect des principes de proportionnalité et de finalité.

B) Une nouvelle forme de perquisition „perquisition électronique“

D'après le commentaire des articles, la formulation „accès par un système informatique direct“ *„est inspirée du nouvel article 60-1 du code de procédure pénale français“*.

A la lecture dudit article 60-1, il appert cependant que tant sa signification que sa portée sont différentes de celles que l'on veut lui conférer.

Il est intéressant de rappeler que le nouvel article 60-1 du code de procédure pénale français a été introduit par une loi (2003-239) du 18 mars 2003 dite „Loi pour la sécurité intérieure“, dont les dispositions les plus pertinentes pour le présent avis sont les suivantes:

„Chapitre IV – *Dispositions relatives aux investigations judiciaires*

(…)

Art. 17.– *Le code de procédure pénale est ainsi modifié:*

1° Après l'article 57, il est inséré un article 57-1 ainsi rédigé:

„**Art. 57-1.–** *Les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.*

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.

Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code.“

(…)

Art. 18.– *Le code de procédure pénale est ainsi modifié:*

1° Il est inséré, après l'article 60, un article 60-1 ainsi rédigé:

„**Art. 60-1.–** *Sur demande de l'officier de police judiciaire, qui peut intervenir par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception de ceux visés au deuxième alinéa de l'article 31 et à l'article 33 de la loi No 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, mettent à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.*

L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés à l'article 43-7 de la loi No 86-1067 du 30 septembre 1986 relative à la liberté de communication, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais.

Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3.750 EUR. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du code pénal de l'infraction prévue au présent alinéa. La peine encourue par les personnes morales est l'amende, suivant les modalités prévues par l'article 131-38 du code pénal.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises."

Force est de constater que le projet luxembourgeois entend accorder des pouvoirs exorbitants à différents acteurs du monde judiciaire et policier qui dépassent de loin les prérogatives que le législateur français a accordé aux mêmes organes à travers les articles 57-1 et 60-1 précités.

En effet, le projet sous avis instaure un accès direct par voie informatique à l'initiative des forces de l'ordre, du Procureur d'Etat et du juge d'instruction qui n'est nullement prévu par les dispositions légales françaises pour lesquelles l'officier de police judiciaire doit faire une demande expresse (cette demande pouvant intervenir par voie informatique).

Dans ce contexte, la Commission nationale aimerait encore relever que, d'après ses informations, une telle procédure d'accès facilitant les techniques comme le matching et le datawarehouse (c'est-à-dire la comparaison de données à partir de deux fichiers afin de déceler des différences), ne serait guère concevable en Allemagne, pays soucieux de préserver au maximum le strict cloisonnement des banques de données détenues par les différentes administrations publiques.

Contrairement au texte français qui prévoit une stricte séparation des fichiers des organismes publics non accessibles directement par l'extérieur, le texte luxembourgeois sous avis permet ainsi aux acteurs susmentionnés, sans requérir le consentement du responsable du traitement dudit fichier, de consulter des données traitées par autrui.

Cette interprétation du texte est corroborée par le terme „système informatique direct", le terme „direct" semble a priori être en contradiction avec l'optique du législateur français prévoyant la notification d'une demande préalable à l'organisme public.

La Commission nationale est dès lors d'avis qu'il vaudrait mieux se limiter à la logique adoptée par la loi française qui instaure en quelque sorte une forme de „perquisition électronique" adoucie dans laquelle l'OPJ bénéficie d'un „push" de la part de l'administration publique, mais non d'un „pull", c'est-à-dire d'un accès par système informatique direct, tel que retenu dans l'avant-projet de loi sous avis.

L'initiative législative se trouvant cantonnée et circonscrite par l'article 8 de la CEDH, il convient d'entourer la nouvelle forme envisagée de perquisition de garanties suffisantes, à l'instar des conditions strictes prévues par le Code d'instruction criminelle pour la perquisition „classique" qui ne permettent pas le recours à des perquisitions clandestines, c'est-à-dire effectuées à l'insu de la personne concernée, où se pose le cas échéant un problème des droits de la défense.

C) Le rôle du responsable du traitement initial

Il faut se demander si cet accès direct par un tiers n'est pas contraire aux responsabilités attachées à la notion de „responsable du traitement" dans le droit de la protection des données.

L'importance du rôle primordial joué par le responsable du traitement peut être retrouvée à l'article 2 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (adoptée par le Conseil de l'Europe à Strasbourg le 28 janvier 1981) qui définit à la lettre d) le „maître du fichier" comme étant „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".

En cas d'utilisation illicite de données à caractère personnel, c'est le maître du fichier, le responsable du traitement, qui voit sa responsabilité engagée en premier lieu, qu'elle soit de nature civile, pénale ou administrative. Il devrait donc conserver la maîtrise sur ses données au lieu de les voir passivement accédées de l'extérieur.

D) La fragilisation des règles relatives à la confidentialité et à la sécurité des données

Dans le même ordre d'idée, l'on peut s'interroger si une telle solution ne pose pas problème en termes de confidentialité des données et de sécurité des traitements au sens des articles 21, 22, 23 et 25 de la loi du 2 août 2002. Cette personne de droit public sera-t-elle toujours en mesure de respecter

les exigences afférentes posées par la loi si un accès direct est réservé à un tiers, en l'occurrence les forces de l'ordre ou le Procureur d'Etat?

Le droit de la protection des données s'appuie sur l'idée fondamentale que le responsable du traitement doit s'assurer que les données à caractère personnel qu'il détient soient traitées loyalement et licitement et ne soient pas ultérieurement traitées de manière incompatible avec les finalités déterminées et légitimes pour lesquelles il les a collectées ou obtenues. En particulier il doit s'en assurer lorsqu'il communique ces données à des destinataires y compris des sous-traitants ou lorsque des personnes placées sous son autorité directe sont habilitées à traiter les données. Il a également l'obligation de mettre en oeuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données et la sécurité des traitements.

Au regard de la définition donnée à l'article 2 lettre (s) du terme „traitement", la loi du 2 août 2002 ne prévoit que „la communication par transmission, la diffusion ou toute autre forme de mise à disposition" comme opérations appliquées à des données à caractère personnel. S'agissant d'un „push" effectué par le responsable du traitement, ces opérations constituent des modes de transmission actifs, par opposition au „pull" prévu au projet sous avis qui constitue un mode de transmission où le responsable du traitement reste passif.

Le responsable du traitement étant en quelque sorte gardien et des données et de la compatibilité des finalités des traitements, il doit aussi veiller à ce que la communication des données à caractère personnel à un tiers se fasse selon le même principe de finalité et soit compatible avec le traitement initial.

L'optique de responsabilisation empruntée par la loi du 2 août 2002 ne paraît donc guère conciliable avec le cas de figure envisagé où des données à caractère personnel pourraient être accédées, extraites, copiées par des tiers – fussent-ils les autorités judiciaires et policières dans le cadre de l'exercice de leurs missions légales – à l'insu du titulaire de ladite responsabilité (gardien de la sécurité des données et de leur utilisation loyale) qui ne pourrait plus, sinon difficilement, l'assumer.

A l'instar de l'article 4 paragraphe 2 in fine de la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat, la Commission nationale se demande dès lors s'il ne parait pas indiqué d'imposer l'obligation de consigner dans des fichiers de traçage (loggings) les accès opérés et les fichiers consultés.

E) L'exclusion des données protégées par un secret prévu par la loi

Il se pose encore la question de la praticabilité de l'exception inscrite dans le texte prévoyant que ne sont pas accessibles les données protégées par un secret prévu par la loi (ex: secret médical, fiscal ou bancaire).

Contrairement à la situation française où l'organisme public reste maitre de la sélection des informations à mettre à disposition de l'officier de police judiciaire en fonction du critère légal „données soumis (ou non) à un secret prévu par la loi", le projet sous avis (ayant adopté une approche différente) ne règle pas cette question.

Or, la Commission nationale s'interroge de quelle façon il pourra être garanti que resteront exclues de l'accès les données couvertes par un secret prévu par la loi.

L'option retenue du *„ont accès par un système informatique direct"* semble inappropriée, parce que l'accès se fera sans la personne morale de droit public liée par un secret professionnel.

Si la décision d'apprécier le caractère de confidentialité incombe à la police, au parquet ou au juge d'instruction le secret professionnel sera violé dans la mesure où l'analyse concrète des données collectées révèle leur caractère confidentiel.

Les considérations qui précèdent plaident en faveur de l'adoption d'une procédure similaire à celle inscrite dans la loi française.

La Commission nationale ne saurait soutenir une approche dans laquelle l'organisme public resterait passif, alors qu'il incombe à chaque établissement de communiquer, après avoir apprécié la légalité (dont le secret professionnel) de la demande lui adressée, quelles données doivent être communiquées à la police, au parquet ou au juge d'instruction.

*

III) RECOMMANDATION D'INTRODUIRE UN SYSTEME TECHNIQUE „BLACK BOX" au niveau des articles 41-1 et 17-1 nouveaux: une solution technique plus respectueuse de la vie privée

A) Au niveau des articles 41-1 et 17-1 nouveaux de l'avant-projet de loi sous avis, la Commission nationale exige l'introduction d'un système technique dit „black box" en suggérant au législateur d'adopter la même solution d'ores et déjà retenue à l'article 41 de la loi du 2 août 2002.

En effet, la voie très prudente empruntée par le législateur dans le cadre de l'article 41 de la loi est beaucoup plus protectrice des intérêts des personnes concernées en termes de confidentialité des données et sécurité des traitements que celle envisagée à l'article 41-1 nouveau de l'avant-projet de loi sous avis au profit de la police grand-ducale et de l'Inspection générale de la police dans l'exercice de leurs missions de police administrative, alors qu'en vertu du paragraphe 4 de l'article 41 (4) *„la procédure est entièrement automatisée suite à l'autorisation de la Commission nationale. La Commission nationale vérifiera en particulier la sécurisation du système informatique utilisé. Cette automatisation permettra l'accès à distance par voie de communication électronique."*

Si le législateur retient, pour des raisons de protection de la vie privée, une solution technique très sophistiquée pour les seules données concernant l'identité des abonnés en vertu de l'article 41 de la loi, la Commission nationale estime qu'il devrait, a fortiori, en faire de même au niveau de l'article 41-1 nouveau pour des données à caractère personnel d'autant plus sensibles détenues par des personnes morales de droit public.

B) Pour les mêmes motifs, l'article 17-1 devrait également, à son tour, faire un renvoi à l'article 41-1 nouveau qui détaillerait les modalités techniques en s'inspirant de l'article 41 actuel de la loi où la procédure est décrite.

C) La Commission nationale relève que les auteurs de l'avant-projet sous avis se sont inspirés dans une très large mesure de la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat, dont le projet de loi afférent n'a pas été soumis à l'époque pour avis à la Commission nationale, qui prévoit en son article 4:

„**Art. 4.–** ***Accès aux informations***

(1) Le traitement, par le Service de Renseignement, des informations collectées dans le cadre de sa mission est mis en oeuvre par voie de règlement grand-ducal tel que prévu par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

(2) Dans le cadre de l'exercice de sa mission, le Service de Renseignement est autorisé à accéder aux banques de données suivantes:

a. le registre général des personnes physiques et morales créé par la loi du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales;

b. la partie „recherche" de la banque de données nominatives de police générale;

c. le bulletin No 2 du casier judiciaire;

d. la banque de données des étrangers exploitée pour le compte du service de la police des étrangers au ministère de la Justice;

e. la banque de données relatives aux affiliations des salariés, des indépendants et des employeurs gérée par le centre commun de la sécurité sociale sur la base de l'article 321 du Code des assurances sociales;

f. la banque de données des véhicules routiers et de leurs propriétaires et détenteurs exploitée pour le compte du ministère des Transports.

L'accès à ces banques de données est soumis à la surveillance de l'autorité de contrôle visée à l'article 17, paragraphe (2) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. En vue de la surveillance exercée par cette autorité de contrôle, le Service de Renseignement doit mettre en oeuvre les moyens techniques permettant de garantir le caractère retraçable de l'accès.

(3) Les données recueillies par le Service de Renseignement ne peuvent servir qu'à la réalisation des missions déterminées à l'article 2.

(4) Le Service de Renseignement peut solliciter les données à caractère non personnel nécessaires à l'exercice de ses missions auprès des personnes morales de droit public ou de droit privé et de toutes personnes physiques."

La Commission nationale suggère de prévoir aussi dans le présent avant-projet de loi un tel système de traçage, qui est nécessaire de surcroît en vue d'assurer l'efficacité du contrôle exercé conformément à l'article 17-1 paragraphe 4 nouveau.

D) La Commission nationale est en outre d'avis qu'il vaudrait mieux supprimer dans l'article 17-1 paragraphe 2 nouveau la référence *„ou, en cas d'urgence dûment motivée, au contrôle de l'existence des éléments constitutifs d'une infraction pénale",* alors qu'il s'agit d'un critère de délimitation à la fois vaste et vague et que la mise en place d'un système de black box n'est guère concevable, voire praticable, avec une telle foule d'informations à gérer.

En effet, à la lecture de l'avant-projet de loi sous avis, plusieurs questions restent ouvertes:

– Qui apprécie le cas d'urgence et la motivation y relative?
– Quelles infractions pénales (crimes, délits, contraventions) sont visées?
– Quelles données à caractère personnel sont effectivement collectées et traitées?
– Est-ce que ces données à caractère personnel ne varient-elles pas en fonction de la personne morale de droit public concernée?

La Commission nationale estime dès lors qu'il faudrait prévoir une nomenclature précise des données consultées par rapport à chaque organisme public en procédant à une énumération limitative par fichier public, étant donné que les catégories de données recensées seront différentes d'une administration à l'autre.

A titre d'exemple, au niveau du Centre Commun de la Sécurité Sociale, il apparaît que les données relatives à l'employeur actuel, aux employeurs précédents ainsi qu'aux périodes d'affiliation devraient être suffisantes.

E) De façon générale, un autre point qui mériterait d'être clarifié dans ce contexte est celui de savoir ce qu'il faut entendre par „Peuvent seulement être obtenues les données qui sont nécessaires à l'identification des personnes physiques ou morales …" (cf. art. 17-1 paragraphe 2 nouveau; art. 41-1 paragraphe 2 nouveau). Qu'est-ce que cela signifie au juste? S'agit-il simplement de vérifier l'identité de la personne concernée par comparaison avec les informations détenues par les personnes morales de droit public? L'exposé des motifs ne fournit point de précisions à cet égard.

F) Par ailleurs, l'avant-projet de loi sous avis passe également sous silence la durée de conservation des données ainsi consultées, durée qui doit être proportionnée aux finalités poursuivies conformément à l'article 4 paragraphe 1er lettre d) de la loi du 2 août 2002.

*

IV) QUANT A L'ARTICLE 17-2 NOUVEAU RELATIF AU TRAITEMENT DE DONNEES „DOUCES" ET „ULTRA DOUCES"

L'exposé des motifs est muet quant à l'objectif recherché par l'introduction de l'article 17-2 dans la loi du 2 août 2002 qui, suivant la lettre d'accompagnement du ministre de tutelle, concerne le traitement de données „douces" et „ultra douces".

A défaut d'explications afférentes, la Commission nationale limite ses commentaires à quelques réflexions d'ordre général:

A) La Commission nationale constate que les données à caractère personnel traitées au titre du nouvel article 17-2 ont été pour l'essentiel reprises des articles 8, paragraphe 1er et 10, paragraphe 1er de la Convention EUROPOL du 18 juillet 1995, de sorte qu'elle n'a pas d'observations particulières à présenter au sujet des données ou catégories de données contenues dans l'avant-projet de loi sous avis, tout en rappelant le caractère extrêmement sensible de ces traitements.

B) Si l'intention des auteurs de l'avant-projet de loi consistant à faire inscrire de telles dispositions dans une loi est louable en tant que telle, les garanties appropriées qui doivent les entourer ne doivent pas être amoindries pour ce type de traitement de données.

La Commission nationale estime dès lors qu'il faut également au niveau de cette disposition légale limiter l'usage et l'accès aux données aux seuls officiers de police judiciaire, comme prévu par les autres dispositions de l'avant-projet de loi sous avis.

C) Par ailleurs, il conviendrait de soumettre explicitement le traitement des données à caractère personnel énumérées à l'article 17-2 nouveau à la surveillance de l'autorité de contrôle prévue à l'article 17 de la loi du 2 août 2002.

Dans un souci d'assurer le parallélisme avec le paragraphe 4 de l'article 17-1 nouveau prévoyant expressément une surveillance de la part de l'autorité de contrôle prévue à l'article 17 de la loi, la Commission nationale recommande d'insérer le même paragraphe 4 également à l'article 17-2 de l'avant-projet de loi sous avis.

D) 1) Si l'intention des auteurs de l'avant-projet est celle de régler par la voie législative, plutôt que réglementaire, le traitement de données „douces" et „ultra douces" par les organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises, cette approche est en tant que telle louable, mais devrait aller de pair avec le souci d'instaurer des garanties appropriées au niveau du texte légal, à l'instar de l'actuel article 17 qui prévoit (en son paragraphe 1er lettre a)) à ce sujet que l'autorisation par voie réglementaire *„déterminera le responsable du traitement, la condition de légitimité du traitement, la ou les finalités du traitement, la ou les catégories de personnes concernées et les données ou les catégories de données s'y rapportant, l'origine de ces données, les tiers ou les catégories de tiers auxquels ces données peuvent être communiquées et les mesures à prendre pour assurer la sécurité du traitement en application de l'article 22 de la présente loi"*.

Ces précisions sont nécessaires pour respecter les principes de base prévus à l'article 4 de la loi du 2 août 2002, à savoir les principes de licéité, de finalité, de transparence et de proportionnalité.

2) S'il est vrai que l'article sous avis permet de retenir comme condition de légitimité celle tirée de l'article 5 (1) (a) de la loi du 2 août 2002 prévoyant que le traitement de données peut être effectué lorsqu'il est *„nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique"* et que les finalités ont également été indiquées avec une précision suffisante *„aux fins de la prévention, de la recherche et de la constatation des infractions pénales",* il n'en reste pas moins que dans l'avant-projet de loi sous avis omet de mentionner les catégories de destinataires et la durée de conservation des données.

La Commission nationale estime que l'avant-projet de loi sous avis devrait expressément exclure toute communication à un tiers.

Quant à la durée de stockage, elle recommande de se référer aux principes dégagés (voir document cité ci-après du Conseil de l'Europe), sinon pour le moins rappeler les règles générales ancrées dans l'article 4 de la loi du 2 août 2002.

En outre, l'avant-projet de loi sous avis devrait clairement préciser les mesures organisationnelles et techniques à prendre pour assurer la confidentialité et la sécurité du traitement en application des articles 21 à 23 de la loi du 2 août 2002.

3) Dans le présent contexte, la Commission nationale aimerait attirer l'attention sur deux documents élaborés au niveau du Conseil de l'Europe:

a) Aux termes de l'article 14 du rapport sur la troisième évaluation de la Recommandation No R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, faite en 2002:

http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Rapports/Z-Rapport%203e%20EvalRec%20%2887%2915.asp#TopOfPage

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 No 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 No R(87)15).

b) Aux termes de l'article 5 de la deuxième évaluation de la pertinence de la Recommandation No R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, faite en 1998.

(http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Rapports/Y-Rapport%202e%20EvalRec%2887%2915.asp#TopOfPage)

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 No 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.

La Commission nationale fait sienne les principales observations et réserves majeures exprimées dans ces documents.

*

V) L'INSERTION D'UN DROIT D'ACCES INDIRECT

La Commission nationale considère que tant au niveau de l'article 17-1 nouveau que de l'article 17-2 nouveau, il convient d'introduire un droit d'accès qui, pour des raisons évidentes, ne saurait être qu'indirect, comme celui d'ores et déjà prévu à l'article 17 de la loi du 2 août 2002.

*

VI) SANCTIONS PENALES

A) Par analogie avec l'article 17 paragraphe 3 de la loi du 2 août 2002, il conviendrait de prévoir également des sanctions pénales aux articles 17-1 et 17-2 nouveaux.

B) En vue d'éviter des redites superflues dans la loi, et pour marquer la cohérence et simplifier la lecture du texte, la Commission nationale suggère dans ce contexte comme alternative de prévoir que la surveillance des nouvelles dispositions légales des articles 17-1 et 17-2 soit assurée par l'autorité de contrôle instaurée à l'article 17, paragraphe 2 actuel de la loi et de réserver un nouvel article 17-3 relatif aux sanctions pénales uniformes, applicables tant à l'article 17 actuel de la loi qu'aux articles 17-1 et 17-2 nouveaux, dont la teneur pourrait être celle de l'actuel paragraphe 3 de l'article 17.

*

VII) LA FIN DU REGIME GENERAL DE L'AUTORISATION PAR VOIE REGLEMENTAIRE?

De façon plus générale, la Commission nationale s'interroge quant à la portée de l'article 17-2 nouveau (qui apparaît plus étendue que l'intitulé même de l'avant-projet de loi sous avis) et sur le rôle résiduel que jouera à l'avenir l'actuel article 17 paragraphe 1er lettre (a), voire même lettres (a), (b) et (c).

En effet, à la lecture de l'avant-projet de loi sous avis, l'on peut se demander si les dispositions exorbitantes de l'article 17-2 nouveau ne conduiront pas à saper la vocation du régime général de l'autorisation par voie réglementaire visée à la lettre (a) de l'article 17 paragraphe 1er aux termes duquel font l'objet d'un règlement grand-ducal les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises.

Aux yeux de la Commission nationale, la même question peut être posée, a fortiori, pour les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique, et les traitements de données dans des domaines du droit pénal effectués en vertu de conventions internationales, d'accords intergouvernementaux ou dans le cadre de la coopération avec l'Organisation internationale de police criminelle (OIPC – Interpol), traitements qui sont visés aux lettres b) et c) de l'article 17 paragraphe 1er de la loi. Mais cela impliquerait, en parallèle, la nécessité d'adapter en ce sens la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat.

Ainsi décidé à Luxembourg en date du 4 mai 2005

La Commission nationale pour la protection des données

Gérard LOMMEL	Pierre WEIMERSKIRCH	Thierry LALLEMANG
Président	*Membre effectif*	*Membre effectif*

Service Central des Imprimés de l'Etat