Autorité de contrôle instituée par 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

Rapport rendant compte de l'exécution de la mission de l'autorité de contrôle pendant l'année 2013

SOMMAIRE

I. Missions légales

La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, entrée en vigueur le 1er décembre 2002, prévoit à son article 17, que

« *(1) Font l'objet d'un règlement grand-ducal :*

(a) 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.

Le règlement grand-ducal 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,

(b) les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique, et

(c) 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) ».

La loi du 27 juillet 2007 portant modification de la loi du 2 août 2002 a complété l'article 17, paragraphe 1er, par un point d) ayant la teneur suivante :

« *d) la création et l'exploitation, aux fins et conditions visées sous (a), d'un système de vidéosurveillance des zones de sécurité. Est à considérer comme telle tout lieu accessible au public qui par sa nature, sa situation, sa configuration ou sa fréquentation présente un risque accru d'accomplissement d'infractions pénales.*
Les zones de sécurité sont fixées dans les conditions prévues par règlement grand-ducal ».

Le paragraphe 2 de l'article institue un régime de contrôle dans les termes suivants :

« *(2) Le contrôle et la surveillance des traitements mis en œuvre tant en application d'une disposition de droit interne qu'en application d'une convention internationale est exercé par une autorité de contrôle composée du Procureur Général d'Etat, ou de son délégué qui la préside, et de deux membres de la Commission nationale nommés, sur proposition de celle-ci, par le ministre.*

L'organisation et le fonctionnement de l'autorité de contrôle font l'objet d'un règlement grand-ducal.

L'autorité de contrôle est informée immédiatement de la mise en œuvre d'un traitement de données visé par le présent article. Elle veille à ce que ces traitements soient effectués conformément aux dispositions légales qui les régissent.

Pour l'exercice de sa mission, l'autorité de contrôle a un accès direct aux données traitées. Elle peut procéder, quant aux traitements effectués, à des vérifications sur place et se faire communiquer tous renseignements et documents utiles à sa mission. Elle peut également charger un de ses membres à procéder à des missions de contrôle spécifique qui sont exécutées dans les conditions indiquées ci-dessus. L'autorité de contrôle fait opérer les rectifications et radiations nécessaires. Elle présente chaque année au ministre un rapport rendant compte de l'exécution de sa mission.

Le droit d'accès aux données visées au présent article ne peut être exercé que par l'intermédiaire de l'autorité de contrôle. Celle-ci procède aux vérifications et investigations utiles, fait opérer les rectifications nécessaires et informe la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution ».

La loi du 5 juin 2009 relative à l'accès des autorités judiciaires, de la Police et de l'Inspection générale de la Police à certains traitements de données à caractère personnel mis en œuvre par 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 à donné à l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police la teneur suivante :

« L'autorité de contrôle instituée 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 contrôle et surveille le respect des conditions d'accès prévues par le présent article. Le rapport à transmettre par l'autorité de contrôle au ministre en exécution de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel contient une partie spécifique ayant trait à l'exécution de sa mission de contrôle exercé au titre du présent article. Le ministre en fait parvenir chaque année une copie à la Chambre des députés.»

Dans sa mission de surveillance et de contrôle, l'autorité de contrôle doit veiller à ce que les traitements automatisés de données à caractère personnel effectués par le corps de la police grand-ducale, l'inspection générale de la police et l'administration des douanes et accises pour les besoins de la prévention, de la recherche et de la constatation et de la poursuite des infractions soient conformes aux dispositions légales qui les régissent.

Pour l'exercice de sa mission, l'autorité de contrôle

- est informée immédiatement de la création d'un traitement de données;
- a accès direct aux banques de données visées;
- peut procéder, quant aux traitements effectués, à des vérifications sur place;
- peut se faire communiquer tous renseignements et documents utiles;
- peut charger ses membres de procéder à des missions de contrôle spécifique;
- fait opérer les rectifications et radiations nécessaires.

Par ailleurs, la loi a investi l'autorité de contrôle de la mission d'exercer, pour compte des personnes concernées, leur droit d'accès à des données traitées dans les banques de données de police. Ce système d'accès est qualifié de droit d'accès indirect.

L'autorité de contrôle présente au ministre compétent, à savoir ayant la Communication dans ses attributions, un rapport rendant compte de l'exécution de sa mission. Alors que, pour les exercices précédents, l'autorité a présenté des rapports couvrant deux années, elle a décidé de présenter un rapport annuel pour 2013, au regard notamment de l'importance des missions effectuées en relation avec le Service de renseignement et du départ à la retraite d'un de ses membres au courant de l'année 2014.

L'article 32, paragraphe 2, de la loi modifiée du 2 août 2002 investit la commission nationale pour la protection des données du droit de publier son rapport annuel. A l'instar du régime qui régit le rapport annuel de la CNPD, l'autorité de contrôle a publié ses rapports antérieurs sur le site Internet de la Commission nationale. Elle envisage de procéder à une publication identique du présent rapport. Les rapports de l'autorité commune de contrôle Schengen et de l'autorité commune Europol font systématiquement l'objet d'une publication au niveau européen et national.

L'autorité de contrôle propose à Monsieur le Ministre de transmettre le présent rapport à la Chambre des Députés. Une telle communication est d'ailleurs exigée à l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police, précitée.

II. Composition de l'autorité de contrôle

Le 3 novembre 2002, Monsieur le Procureur général d'Etat Jean-Pierre Klopp avait délégué Monsieur Georges Wivenes, premier avocat général, nommé depuis aux fonctions de Procureur général d'Etat adjoint, aux fins de présider l'autorité de contrôle. Cette délégation a été confirmée par Monsieur le Procureur général d'Etat Robert Biever, en fonction depuis le 1er septembre 2010.

Par arrêté ministériel du 18 novembre 2002, Monsieur Pierre Weimerskirch, membre effectif de la commission nationale pour la protection des données a été nommé membre de l'autorité de contrôle.

Par arrêté ministériel du 21 décembre 2005, Monsieur Thierry Lallemang, membre effectif de la CNPD, a été nommé membre de l'autorité de contrôle.

III. Réunions et fonctionnement de l'autorité de contrôle

En dehors des réunions lors des visites au service de renseignement, l'autorité de contrôle s'est réunie formellement, à 4 reprises, au cours de l'exercice 2013. Les membres de l'autorité ont été en contact régulier par voie de courrier électronique ou téléphonique sur des questions urgentes.

D'après le paragraphe 2 de l'article 17 de la loi du 2 août 2002, « l'organisation et le fonctionnement de l'autorité de contrôle font l'objet d'un règlement grand-ducal ».

L'adoption de ce règlement n'a jamais été considérée par l'autorité comme une condition juridique préalable à l'exécution des missions légales. Dans une approche pragmatique, les tâches administratives ont été assurées par les membres de l'autorité. Pour les questions budgétaires, il a été fait recours à la CNPD et au parquet général.

Dans ses rapports antérieurs, l'autorité de contrôle avait considéré que *« compte tenu de la charge croissante de travail, au niveau européen, mais aussi au niveau national avec l'entrée en vigueur de nouvelles réglementations en matière policière, ... il serait indiqué d'adopter ce règlement à l'effet de créer un secrétariat à rattacher soit à la CNPD, soit au Parquet général, chargé des tâches administratives »*. L'autorité de contrôle maintient ces considérations. Les demandes individuelles d'accès aux fichiers du service de renseignement dont l'autorité a été saisie depuis fin 2012 ont été gérées, pour l'essentiel, par le président avec l'assistance du secrétariat du parquet général.

L'autorité a signalé, dans ses rapports antérieurs, que le Comité d'évaluation Schengen qui avait procédé au cours de la période fin 2008 – début 2009 à un contrôle du Luxembourg, avait souligné, dans son rapport du 7 mai 2009, la nécessité de doter l'autorité de contrôle des moyens financiers et en personnel nécessaires pour exécuter ses missions et d'adopter le règlement grand-ducal prévu à l'article 17 paragraphe (2) de la loi modifiée du 2 août 2002. Aucune suite n'a été réservée à cette recommandation du comité européen que l'autorité de contrôle a régulièrement rappelée dans ses rapports successifs. Une nouvelle évaluation Schengen est en cours ; les évaluateurs posent, encore, la question des moyens financiers et humains de l'autorité de contrôle.

IV. Contrôles effectués auprès de l'administration des douanes

Au niveau de l'Union européenne, le règlement (CE) n° 515/97 du Conseil du 13 mars 1997 relatif à l'assistance mutuelle entre les autorités administratives des États membres et à la collaboration entre celles-ci et la Commission en vue d'assurer la bonne application des réglementations douanière et agricole a créé un système d'information automatisé commun (custom information system-CIS) géré par les administrations douanières des États membres ainsi que par la Commission. Il comprend une base de données centrale accessible à partir de terminaux placés dans chacun des États membres et à la Commission.

Le système CIS aide à prévenir, rechercher et poursuivre les infractions aux réglementations douanière et agricole de la Communauté. Il renforce l'efficacité des procédures de coopération et de contrôle des autorités douanières, grâce à la diffusion rapide des informations et des renseignements. Le système permet également d'échanger des données, de façon régulière ou occasionnelle, sur les marchandises circulant entre le territoire douanier communautaire et les pays tiers.

Le 27 juin 2013, les membres de l'autorité de contrôle ont eu une réunion à la Direction générale des Douanes. Les points suivants ont été abordés :

1. CIS

Les responsables de la douane confirment que l'Administration n'a qu'un seul terminal CIS. Pour l'heure, le service de la Division antidrogues et produits sensibles dispose de cet accès. Les consultations seraient rares, une tous les deux mois. L'outil est qualifié de non utile.

2. Traitements nationaux des données relevant de l'article 17 de la loi du 2 août 2002

L'administration des douanes a des compétences en matière de prévention, de constat et de répression des infractions dans les domaines très divers tels les transports routiers, l'environnement, la sécurité des chantiers, le travail clandestin, la lutte contre la toxicomanie etc.

Ses agents disposent, dans ces domaines, des attributions de la police judiciaire impliquant notamment l'établissement de procès-verbaux transmis aux parquets, à l'instar de la police.

Trois problèmes ont été évoqués :

*L'Administration gère une base de données (DO-COM) recevant l'ensemble des rapports d'activités que les agents établissent régulièrement.

Ces données concernant les différents services sont librement accessibles à tous les agents du service concerné. Le retraçage des accès est possible ; par contre, un mécanisme de justification de l'accès n'est pas prévu ; de même aucun système d'élimination des données n'est prévu.

*L'Administration a accès à une série de banques de données externes.

Certains accès sont organisés par un règlement, à savoir :

- règlement grand-ducal du 13 juin 1988 autorisant la création et l'exploitation d'une banque de données pour le compte du service de la police des étrangers su Ministère de la Justice ; article 3 ; ce règlement est expiré le 31 décembre 1996.
- règlement grand-ducal du 7 juin 1993 autorisant la prorogation de l'exploitation de la banque de données nominatives des propriétaires, porteurs, détenteurs et vendeurs d'armes prohibées, article 3 ; ce règlement est expiré en 2003.

Pour d'autres accès, tels que p.ex. aux fichiers autorisation d'établissements, RPNI, il n'y a pas de base juridique.

Certaines données sont accessibles par l'intermédiaire d'une plate-forme informatique commune avec d'autres administrations, telle la base de données TVA de l'Administration de l'Enregistrement.

*Les procès-verbaux sont conservés sous forme scannée ; ils sont accessibles au sein de chaque service. Il n'est opéré aucune distinction entre une partie opérationnelle et une partie archives. Le retraçage des accès est possible ; par contre, un mécanisme de justification de l'accès n'est pas prévu; de même aucun mécanisme de suppression n'est appliqué.

Les données sur les avertissements taxés sont incluses dans ce fichier.

L'autorité de contrôle rappelle et regrette que le traitement des données par l'Administration des Douanes ne fait toujours pas l'objet d'un règlement grand-ducal ce qui rend aléatoire toute opération de contrôle. L'autorité de contrôle avait déjà mis en évidence cette carence dans ses rapports antérieurs sans que ses mises en garde aient été considérées par les

instances responsables. Notons toutefois que suite à la réunion du 27 juin 2013, le directeur adjoint a fait parvenir une première ébauche d'un avant–projet de loi

La nécessité de la mise en place d'un cadre légal et réglementaire devient d'autant plus évidente que l'administration des douanes s'est vue attribuer des compétences dans le domaine de la prévention et de la recherche des infractions qui sont parallèles à celles de la police grand-ducale et que cette évolution se poursuit.

V. Contrôles effectués auprès de la police grand-ducale

1) Interpol

Un nombre déterminé d'agents de la police grand-ducale a la possibilité de consulter les données d'Interpol. Interpol a développé une nouvelle application destinée à être installée auprès des polices nationales des Etats membres. Ce nouveau système fonctionne au Luxembourg au bureau central Interpol (un poste de travail) ; la police judiciaire bénéficie des mêmes accès.

2) Europol

Dans ses rapports antérieurs, l'autorité de contrôle a eu l'occasion de relever que *« les données traitées par Europol sont très techniques et se prêtent moins à un travail d'enquête policière.*

... les relations entre la police luxembourgeoise et Europol se limitent à un échange de courrier électronique au nombre d'un à deux messages par jour. Les fichiers dits AWF (action files) qui sont opérationnels auprès d'Europol ne sont guère utilisés.

La transmission de données de la police grand-ducale vers Europol se fait essentiellement par l'intermédiaire de l'officier de liaison luxembourgeois auprès d'Interpol. Ce dernier obtient des informations figurant dans ce qu'il était convenu d'appeler le fichier central de la police et transmet ces informations aux officiers de liaison des autres Etats membres. Le nombre de ces demandes se chiffre à quelques milliers par an ».

Ces observations valent également pour la période couverte par le présent rapport. Plusieurs applications d'Europol sont opérationnelles auprès de la police, en particulier auprès du service de la police judiciaire.

En 2013, l'autorité de contrôle à participé à une étude européenne sur les unités nationales Europol. Un rapport non public a été adopté par l'Autorité commune de contrôle européenne au mois d'octobre 2013.

3) Schengen

Le système d'information Schengen (SIS) est accessible pour tous les terminaux installés dans les différents services de la police. La consultation de ces données fait l'objet d'un enregistrement systématique.

Au niveau du système d'information Schengen, il faut distinguer les mécanismes suivants :

- Article 95 de la Convention d'application de l'accord de Schengen :

Il s'agit de données relatives aux personnes recherchées pour arrestation et extradition. L'intégration dans le SIS se fait sur demande de l'autorité judiciaire compétente. Les données comportent l'indication du motif du signalement et permettent un repérage du dossier concernant la personne concernée.

Dans le cadre d'un contrôle organisé au niveau européen par l'Autorité commune de contrôle Schengen, l'autorité luxembourgeoise a procédé à une inspection des données traitées au titre de l'article 95 par la police grand-ducale. A ce titre, un rapport contenant un certain nombre de suggestions et de recommandations relatives au traitement des données en rapport avec les signalements de personnes recherchées pour arrestation et extradition a été établi par l'Autorité commune de contrôle européenne qui fut adopté le 19 mars 2013.

- Article 96 :

Sont visées les données relatives aux étrangers signalés aux fins de non-admission. L'intégration se fait sur demande du ministre de la justice.

- Article 97 :

Ce texte concerne les données relatives aux personnes disparues ou placées provisoirement en sécurité. L'intégration de données dans le SIS se fait encore sur demande de l'autorité judiciaire compétente.

- Article 98 :

Les données en cause concernent les témoins et les personnes citées à comparaître dans des procédures pénales. Ici encore l'autorité judiciaire est compétente pour l'intégration des données dans le SIS.

- Article 99 :

Les données relatives aux personnes ou aux véhicules signalés aux fins de surveillance discrète ou de contrôle spécifique sont intégrées sur demande des autorités judiciaires

4) SIS II

La mise en place du système Schengen II au niveau européen a pris six ans. En effet, si le Règlement (CE) n°1987/2006 du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération est entré en vigueur début 2007, le système n'est devenu opérationnel qu'au mois d'avril 2013.

Les membres de l'autorité de contrôle ont eu une réunion à la direction de la Police grand-ducale en date du 25 juin 2013 lors de laquelle le SIS II a, entre autres, été un sujet de discussion :

Le SIS II est appliqué depuis le 9 avril 2013 et fonctionne à la satisfaction des utilisateurs.

Le SIS au Danemark a été victime d'une cyber attaque ; 1500 signalements luxembourgeois sont affectés. La Commission européenne a pris l'initiative d'une « reprise en mains »

A été abordée également la question d'une mise en œuvre de directives européennes :
La directive dite initiative suédoise sur la coopération policière, la directive sur l'échange d'informations en matière d'infraction à la circulation routière qui fait actuellement l'objet d'un projet de loi de transposition.

Les responsables de la police proposent, en ce qui concerne les signalements, un mécanisme de contrôle commun pour les trois systèmes Interpol, Europol et Schengen. Les membres de l'autorité n'y voient pas d'objection dès lors que les conditions d'accès pour les différents systèmes sont respectées.

5) Coopération au titre du Traité de Prüm

Par la loi du 22 décembre 2006 a été approuvé le Traité entre le Royaume de Belgique, la République fédérale d'Allemagne, le Royaume d'Espagne, la République française, le Grand-Duché de Luxembourg, le Royaume des Pays-Bas et la République d'Autriche relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminali.transfrontalière et la migration illégale, ainsi que de la Déclaration commune, signés à Prüm le 27 mai 2005.

Dans le cadre de la coopération policière mise en place par le traité de Prüm, la police grand-ducale a accès, à la date du 31 décembre 2008, aux fichiers véhicules automobiles pour l'Allemagne et l'Autriche. (L'accès pour la France est devenu opérationnel début 2009). L'accès des polices étrangères aux fichiers luxembourgeois est également opérationnel.

6) Bureau commun de coopération policière

Depuis 2003 un centre international de coopération policière et douanière fonctionne à Luxembourg. Ce centre a été créé sur base d'un accord bilatéral avec la France ainsi qu'un accord trilatéral avec l'Allemagne et la Belgique. Des policiers, gendarmes et douaniers des pays limitrophes sont représentés au côté des policiers luxembourgeois. Le centre est destiné à assurer l'échange d'informations policières issues de la région transfrontalière et ceci entre unités policières.

7) Traitements nationaux

La saisine des procès-verbaux et rapports figurant dans ce qu'il était convenu d'appeler le fichier central de la police par scanning sur support électronique a été achevée fin 2007. Ont été éliminés les documents concernant les personnes nées avant 1910 ou les personnes décédées. Aucun tri n'a été effectué selon des critères de classement sans suite de l'affaire par le Parquet, de décision de non-lieu ou d'acquittement, de prescription des faits ou de la peine, de réhabilitation légale ou judiciaire.

Les données ainsi saisies sont intégrées dans la partie II de l'actuelle banque de données Ingepol (voir ci-après) et accessibles aux officiers de police judiciaire.

Pendant la période couverte par le présent rapport, le traitement des données de police a continué à être régi par le règlement modifié du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale.

A la date du 31 décembre 2013, le règlement grand-ducal prévu à l'article 17 de la loi du 2 août 2002 et appelé à remplacer le règlement Ingepol actuel n'a toujours pas été adopté.

Par règlement grand-ducal du 9 mai 2010 portant modification du règlement grand-ducal modifié du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale, l'autorisation prévue à l'article 1er du règlement de 1992 a été prorogée au 1er mai 2011.

Par règlement grand-ducal du 2 juin 2011 portant modification du règlement grand-ducal modifié du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale, l'autorisation prévue à l'article 1er du règlement de 1992 a été prorogée au 1er juin 2012.

Par règlement grand-ducal du 7 juin 2012 portant modification du règlement grand-ducal modifié du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale, l'autorisation prévue à l'article 1er du règlement de 1992 a été prorogée au 1er juin 2014.

Dans le rapport pour 2011 et 2012, l'autorité de contrôle avait relevé ce qui suit :

> *La prorogation du règlement Ingepol de 1992 en 2011 est intervenue par un règlement du 2 juin 2011 qui a été publié au Mémorial A n° 124 du 17 juin 2011 et qui est entré en vigueur, en vertu de l'arrêté royal grand-ducal 22 octobre 1842 réglant le mode de publication des lois et règlements, le 21 juin 2011. Entre le 1er mai 2011, date d'expiration du règlement de 1992, en vertu du règlement du 9 mai 2010, et le 21 juin 2011 la banque de données Ingepol n'avait pas de base règlementaire.*
>
> *La prorogation du règlement Ingepol de 1992 en 2012 est intervenue par un règlement du 7 juin 2011 publié au Mémorial A n° 124 du 27 juin 2012 qui est entré en vigueur, en vertu de l'arrêté royal grand-ducal 22 octobre 1842 réglant le mode de publication des lois et règlements, le 1er juillet 2012. Entre le 1er juin 2012, date d'expiration du règlement de 1992 en vertu du règlement du 2 juin 2011 et le 1er juillet 2012, la banque de données Ingepol n'avait pas de base règlementaire.*
>
> *De telles périodes de « vide juridique » sont inadmissibles. L'autorité de contrôle n'entend pas entend dans une discussion sur la possibilité de rétablir « rétroactivement » la base juridique d'un traitement de données.*
>
> *Le règlement du 7 juin 2012 porte prorogation du règlement de 1992 pour une période de 2 ans, ce qui répond, le cas échéant, aux problèmes exposés ci-dessus, mais ce qui montre également que le pouvoir réglementaire n'envisage pas, dans un proche avenir, l'adoption d'une base réglementaire nouvelle, plus moderne, fondée sur l'article 17 de la loi du 2 août 2002.*

L'autorité de contrôle rappelle que la reconduction systématique du règlement de 1992 constitue une réponse inadéquate.

L'article 17 de la loi de 2002 requiert l'adoption d'un règlement dont l'objectif est de mettre en œuvre toutes les exigences de licéité et de légitimité prévues dans la loi et de garantir la sécurité du traitement et les droits individuels. Il est, par ailleurs, discutable que l'articulation des catégories de données, les types de données et le système de traitement envisagé dans le règlement de 1992 réponde à la réalité du traitement des données opéré actuellement par la police grand-ducale.

Dans ce contexte, lors d'une réunion interministérielle au Ministère de la Justice en date du 10 décembre 2013, il a été proposé de créer un groupe de travail interministériel qui serait chargé d'élaborer le ou les projets de loi et de règlement grand-ducal nécessaires à la mise en œuvre du « paquet protection des données en matière pénale », dont le remplacement du règlement grand-ducal Ingepol de 1992.

Lors d'une réunion du 25 juin 2013, les membres de l'autorité du contrôle ont discuté avec la direction de la Police grand-ducale les problèmes suivants :

- Accès des membres du personnel civil, qui actuellement n'ont pas la qualité d'officier de police judiciaire, aux fichiers internes et externes ;
- Problématique du journal dit des incidents, qui constitue le rapport d'activités établi tous les jours par les agents : contenu de ces rapports, épuration ou élimination du rapport ou de certaines données personnelles après établissement d'un rapport ou procès-verbal à l'intention du parquet, portée de l'accès de ce journal des incidents aux autres agents ;
- Problème du feed-back de la part de la justice sur la suite réservée aux procès-verbaux, en particulier en cas de classement, d'acquittement ou de non-lieu (Ingepol, art 6) ;
- Problème des procès-verbaux portant sur des mineurs ;
- Mise en place du logiciel « Großschadenslage » (mesures à prendre en cas de survenance d'accidents majeurs ou de catastrophes naturelles) ;
- Fiches d'hébergement ;
- Données relatives au trafic : mise en parallèle des données fournies par les opérateurs de communication électroniques avec les données des demandes de la police.

8) Fiches d'hébergement

Le règlement grand-ducal du 1er avril 2011 relatif aux fiches à tenir par les logeurs exploitant un service d'hébergement touristique, pris en exécution de la loi du 24 juin 2008 relative au contrôle des voyageurs dans les établissements d'hébergements, est entré en vigueur le 1er avril 2013.

En date du 26 juin 2013, l'autorité de contrôle a procédé à un contrôle auprès de la Police grand-ducale pour vérifier si le traitement des données relatives aux voyageurs dans les établissements d'hébergements opéré par la police était conforme aux dispositions légales et réglementaires.

L'autorité de contrôle a pu constater que le traitement de données personnelles en question est bien effectué en conformité avec la loi.

L'autorité de contrôle a fait les constats suivants :

La police grand-ducale traite les données relatives aux voyageurs dans les établissements d'hébergements dans un fichier temporaire.

La base de données dont la police grand-ducale est le responsable du traitement, contient uniquement les données limitativement énumérées à l'article 2 du règlement grand-ducal. L'accès aux données est restreint au bureau responsable de la gestion des fiches d'hébergement. Les données sont effacées soixante-douze heures après leur transmission, à moins que leur maintien au-delà de ce délai ne soit nécessaire pour la prévention, la recherche ou la constatation d'une infraction.

Cependant, la police grand-ducale n'avait pas connaissance de la durée de rétention des données auprès de leur sous-traitant le CTIE. Sur ce point la Police Grand Ducale a été invitée à vérifier ce point auprès du CTIE afin de garantir que la durée de rétention légale de 72 heures ne soit dépassée.

Le temps de rétention du backup technique de la base de données relative au système de fiches d'hébergement électroniques est de 14 jours. Il faut néanmoins préciser qu'il ne s'agit pas d'un système d'archivage (avec éventuellement moyen de pouvoir sélectivement restaurer la base de données des fiches d'hébergement électroniques à un instant), mais bien d'un backup technique dans le but d'un 'desaster recovery', afin de pouvoir recréer l'intégralité des bases de données dans le cas d'un incident technique grave.

9) Système de vidéosurveillance des zones de sécurité (Visupol)

L'article 17, paragraphe 1 lettre (d) de la loi du 2 août 2002, telle que modifiée par la loi du 27 juillet 2007, permet la fixation de zones de sécurité soumises à un système de vidéosurveillance par voie de règlement grand-ducal.

Le règlement grand-ducal du 1er août 2007 autorisant la création et l'exploitation par la Police d'un système de vidéosurveillance des zones de sécurité a fixé les conditions de la vidéosurveillance et les modalités et délais de conservation des enregistrements.

Par règlement ministériel du 27 septembre 2007, trois zones de sécurité ont été désignées pour la Ville de Luxembourg, à savoir :

– Zone A: la zone située en Luxembourg-Ville, quartier du Limpertsberg – Glacis;
– Zone B: la zone située en Luxembourg-Ville, quartier de la Ville Haute – centre Aldringen;
– Zone C: la zone située en Luxembourg-Ville, quartier de la Gare;

Ce règlement a été remplacé par le règlement ministériel du 10 novembre 2009 qui a ajouté une quatrième zone de sécurité soumises à la vidéosurveillance :

– Zone D: la zone située autour du stade «Josy Barthel», 3, rue du Stade, L-2547 Luxembourg.

Le règlement de 2009 a été remplacé par le règlement ministériel du 10 novembre 2010 ; ce dernier par un règlement du 10 novembre 2011, lui-même remplacé par un règlement ministériel du 10 novembre 2012 qui a cessé d'être en vigueur le 10 novembre 2013. Le règlement de 2012 a été remplacé par un nouveau règlement ministériel du 7 octobre 2013 qui cessera d'être e vigueur le 7 octobre 2014.

Par règlement ministériel du 25 avril 2012 une nouvelle zone de sécurité a été désignée
-Zone E: la zone située en Luxembourg-Ville, quartier du Kirchberg autour du Centre de Conférences Kirchberg. Contrairement au règlement ministériel du 10 novembre 2012, le règlement du 25 avril 2012 ne contient pas de date à laquelle il cessera d'être en vigueur.

L'autorité rappelle qu'en vertu de l'article 10 du règlement grand-ducal du 1er août 2007 autorisant la création et l'exploitation par la Police d'un système de vidéosurveillance des zones de sécurité, *« chaque zone de vidéosurveillance peut être prorogée annuellement ».*

L'article 10 du prédit règlement grand-ducal du 1er août 2007 prévoit que « ...., *la vidéosurveillance de chaque zone de sécurité peut être prorogée annuellement par le ministre suite à une évaluation de l'utilité et de la nécessité de la vidéosurveillance de chaque zone de sécurité...* ».

L'autorité de contrôle s'est vu communiquer, sur demande, copie des avis du directeur général de la Police grand-ducale et du procureur d'Etat de Luxembourg émis lors de l'adoption du règlement ministériel du 27 octobre 2013.

A la suite d'une demande individuelle d'accès aux enregistrements du système de vidéo surveillance, l'autorité de contrôle a sollicité auprès de la police grand-ducale des renseignements sur deux caméras de surveillance situées place du Marché aux Herbes en face de l'entrée de la Chambre des Députés et du Palais grand-ducal. Ces caméras sont marquées par des panneaux indiquant le numéro de la délibération de la Commission nationale pour la protection des données autorisant leur installation sur demande, pour le Palais grand-ducal de la Police, et pour la Chambre, de cette dernière. Il ne s'agit pas d'installations techniques relevant du système Visupol, même si, l'aspect extérieur des panneaux est de nature à susciter des confusions dans l'esprit du passant non averti.

VI. Contrôles auprès du Service de renseignement

En vertu de l'article 17 de la loi du 2 août 2002, l'autorité de contrôle est également compétente pour surveiller les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique.

1. L'absence de règlement grand-ducal

L'article 17 de la loi de 2002 prévoit que les traitements relatifs à la sûreté de l'Etat, à la défense et à la sécurité publique font l'objet d'une autorisation par voie de règlement grand-ducal, à l'instar de ce qui est prévu pour les traitements de données par la police.

La loi du 15 juin 2004 portant organisation du service de renseignement de l'Etat reprend, à l'article 4, expressément l'exigence de l'adoption d'un règlement au sens de l'article 17 de la loi de 2002 en disposant que : *« Le traitement, par le Service de Renseignement, des informations collectées dans le cadre de sa mission est mis en œuvre 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 ».*

Or, depuis l'entrée en vigueur de la loi de 2004, aucun règlement grand-ducal n'a été adopté.

En droit, l'autorité ne considère pas que la loi de 2004 qui donne au service de renseignement la mission de *« rechercher, d'analyser et de traiter, dans une perspective de prévention, les renseignements relatifs à toute activité qui menace ou pourrait menacer la sécurité »* constitue une base juridique suffisante rendant superflue l'adoption d'un règlement. On ne saurait pas davantage soutenir que la loi de 2004 constitue une loi spéciale qui est venue limiter la portée de la loi de 2002 sur la protection des données ; le renvoi opéré, à l'article 4 de la loi de 2004, précité, à l'article 17 de la loi de 2002 met en évidence que le traitement des données par le service de renseignement reste soumis aux conditions et modalités de la loi de 2002, en particulier de l'article 17. De même, l'absence de règlement ne saurait être palliée par des règles d'organisation interne ou des pratiques internes du service, au demeurant parfaitement opaques, qui seraient conformes aux exigences de la loi de 2002.

L'article 17 de la loi du 2 août 2002 prévoit encore, au paragraphe 2 que *« L'autorité de contrôle est informée immédiatement de la mise en oeuvre d'un traitement de données visé par le présent article. Elle veille à ce que ces traitements soient effectués conformément aux dispositions légales qui les régissent. »*

Depuis 2004, l'autorité n'a jamais été informée de la mise en oeuvre des traitements effectués par le service de renseignement. Ce n'est que dans le cadre des contrôles individuels opérés depuis 2013 que l'autorité a été en mesure de prendre connaissance des différents traitements de données opérés par le service de renseignement.

De même, la loi du 15 juin 2004 relative à la classification des pièces et habilitations de sécurité prévoit à l'article 23 que *« Le traitement, par l'Autorité nationale de Sécurité, des informations collectées dans le cadre de ses missions est mis en oeuvre par voie de règlement grand-ducal tel que prévu à l'article 17 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. ».*

Ici encore, aucun règlement n'a été adopté.

L'autorité de contrôle a été informée que des projets de règlement grand-ducal seraient en élaboration. La CNPD a avisé les textes en projet en date du 28 juin 2013.

2. L'habilitation de sécurité

Alors que, pour les exercices antérieurs, l'autorité de contrôle a été dans l'impossibilité d'exercer sa mission de surveillance faute de délivrance par l'autorité nationale de sécurité d'une habilitation de sécurité, cette pièce a finalement été fournie aux membres de l'autorité en date du 14 février 2013.

L'établissement de cette habilitation a été effectué sans que les membres de l'autorité aient été soumis à un contrôle préalable de la part de l'instance à contrôler.

Sans entendre revenir sur cette situation de blocage due à la position de refus d'accès adoptée par les responsables du service de renseignement, l'autorité note qu'une attitude plus ouverte aurait utilement pu être prise depuis des années.

3. L'accès aux données par les particuliers

Aux termes de l'article 17, paragraphe 2, dernier alinéa, de la loi du 2 août 2002,

« le droit d'accès aux données visées au présent article ne peut être exercé que par l'intermédiaire de l'autorité de contrôle. Celle-ci procède aux vérifications et investigations utiles, fait opérer les rectifications nécessaires et informe la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution »

Ce mécanisme peut être résumé en trois points :

- Pour les personnes privées, l'accès aux fichiers du service de renseignement est indirect et s'opère par l'intermédiaire de l'autorité de contrôle.
- L'autorité de contrôle procède aux vérifications et peut exiger des rectifications ou des suppressions de données.
- Elle n'est pas en droit de communiquer au particulier le contenu des fichiers ou le contenu des contrôles, mais peut seulement l'informer qu'il n'y a pas de traitement contraire à la loi.

Dans la foulée des discussions sur le fonctionnement du service de renseignement, l'autorité de contrôle a été saisie, à partir du début du mois de décembre 2012 d'une série de demandes individuelles. Elle a continué les premières demandes individuelles au service de renseignement accompagnées des considérations suivantes que l'autorité a décidé, pour des raisons de transparence, de reprendre dans le présent rapport :

« L'accès aux données constitue un droit fondamental des personnes dont les données personnelles font l'objet d'un traitement. Ce droit n'est pas seulement consacré par l'article 28 de la loi du 2 août 2002, mais encore par l'article 8 de la Charte des droits fondamentaux de l'Union européenne et par l'article 8 de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel. Les limitations au droit d'accès nécessaires pour sauvegarder la sûreté de l'Etat, prévues à l'article 29 de la loi de 2002, ne sauraient porter atteinte à la substance même du droit d'accès, mais justifient des limitations à l'accès.

L'autorité de contrôle demande à obtenir, dans les meilleurs délais, communication des données concernant les personnes mentionnées ci-dessus, afin de pouvoir effectuer ses missions en vue de la protection des droits des personnes concernées.

Dans la mesure où est en cause un droit fondamental du citoyen et compte tenu du fait que l'autorité de contrôle n'opère pas, en l'espèce, de vérification à portée générale à l'intérieur des locaux du service, aucun refus ne saurait lui être opposé, tenant à la prétendue nécessité

d'une habilitation de sécurité, impliquant un contrôle préalable effectué par l'organe qu'il s'agit de contrôler sur l'autorité appelée à exercer le contrôle.

L'autorité de contrôle exige que la communication porte non seulement sur les données actuellement traitées, mais également sur celles traitées dans le passé.

Aux termes de l'article 17 précité, l'autorité de contrôle « informe la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution ». La loi de 2002 n'interdit toutefois pas au service de renseignement, en tant que responsable du traitement, d'admettre la communication aux personnes concernées du contenu des données rassemblées. Une telle conclusion s'impose d'autant plus que, d'après l'article 4, paragraphe 3, de la loi de 2004, les données recueillies par le Service de Renseignement ne peuvent servir qu'à la réalisation des missions du service déterminées à l'article 2 et que la limitation de l'accès n'est justifiée que par la nécessité de sauvegarder la sûreté de l'Etat et doit être proportionnelle au but légitime poursuivi ».

De fin 2012 jusqu'au 31 décembre 2013, l'autorité a été saisie de 679 demandes individuelles, en ce compris les demandes portant sur des dossiers d'associations.

Dans le cadre du traitement des demandes individuelles l'autorité a effectué, en 2013, 16 visites auprès du service de renseignement de l'Etat, aux Archives nationales et dans les archives de Senningen.

En ce qui concerne les données personnelles traitées par le service de renseignement et objet des contrôles de l'autorité, il faut retenir deux critères de distinction.

Selon l'objet du dossier, il faut distinguer deux types de traitements :

- les dossiers administratifs d'enquête établis dans le cadre d'une demande d'habilitation de sécurité introduite par l'intéressé lui-même ; ces dossiers relèvent de la compétence de l'autorité nationale de sécurité (dossiers ANS) et sont régis par la loi du 15 juin 2004 relative à la classification des pièces et habilitations de sécurité;

- les dossiers de renseignement proprement dits établis à l'insu des intéressés (dossiers SRE). Ces dossiers relèvent de la compétence du service de renseignement et sont régis par la loi du 15 juin 2004 portant organisation du service de renseignement de l'Etat. D'après l'article 19 de la loi du 15 juin 2004 relative à la classification des pièces et habilitations de sécurité, les fonctions de l'autorité nationale de sécurité sont assumées par le service de renseignement.

Selon la date d'établissement des dossiers et leur mode technique de traitement, support papier porté sur micro-fiche, ou support informatique, il faut distinguer entre les archives dites historiques et les données figurant dans des traitements opérationnels actuels. Cette seconde distinction vaut pour les enquêtes de renseignement et les enquêtes en vue de la délivrance d'une habilitation de sécurité, étant entendu qu'avant les lois de 2004 précitées les deux types de données étaient traitées de la même manière sous l'égide du service de renseignement.

Les archives historiques sont constituées d'un fichier de cartes nominatives. Chaque carte renvoie, pour la personne ou l'association en cause, à un dossier conservé sous forme de

microfiches. Le fichier de cartes nominatives et les microfiches correspondantes ont été conservés au siège du service de renseignement.

En date du 23 janvier 2013 la Commission d'enquête parlementaire a opéré une saisie et une mise sous scellé *« de tous les objets, documents ou papiers ainsi que de tous les documents connexes composant la banque de données tenue sous forme de fiches individuelles établie par le Service de Renseignement de l'Etat »*; cette décision a été levée le 2 octobre 2013 au regard de la dissolution de la Chambre des Députés le 7 octobre 2013. En considération de la levée de la mise sous scellé, les archives ont été transférées aux Archives nationales où elles sont déposées dans une pièce sécurisée à laquelle le service de renseignement n'a plus seul accès. Le transfert a porté sur les dossiers historiques SRE et ANS. De l'avis de l'autorité de contrôle, ce transfert n'a pas modifié la nature juridique des données ou leur régime juridique, ni la qualité de responsable du traitement dans le chef du service de renseignement, ni les compétences de l'autorité de contrôle.

Pour répondre aux demandes individuelles, l'autorité de contrôle a eu accès aux archives du service. Pendant la période de la mise sous scellé, cet accès a été organisé sur la base de mainlevées individuelles accordées par la Commission parlementaire. Depuis le transfert des dossiers aux Archives nationales, l'autorité de contrôle a accès aux dossiers dans les locaux des Archives nationales en présence de représentants du service de renseignement et de la direction des Archives nationales. De même, l'autorité a eu accès aux traitements opérationnels.

En cas de découverte d'un dossier historique individuel, tant ANS que SRE, les microfiches ont été imprimées et le dossier sur support papier a été transmis à l'autorité de contrôle. L'autorité de contrôle a mis ces dossiers à la disposition des demandeurs en fournissant les explications nécessaires.

Au regard du dispositif législatif exposé ci-dessus, l'autorité de contrôle a pu prendre inspection de tous les documents. La loi ne prévoit toutefois pas, au profit des citoyens, un droit à la communication du dossier ou de toutes les pièces d'un dossier. La transmission aux intéressés des dossiers historiques est le résultat d'une décision « politique » des responsables du service ; l'autorité de contrôle a fortement encouragé ce choix, mais n'aurait pas été en mesure de l'imposer.

Le service de renseignement est encore en droit de refuser la transmission de certaines pièces ou de certaines données, notamment pour des considérations tenant à la coopération avec des services secrets d'autres Etats. Dans un courrier de février 2013, l'autorité de contrôle est interrogée sur la distinction opérée entre les données propres au service qui sont communiquées aux intéressés et celles émanant de services dits tiers dont la communication est refusée. L'autorité a des difficultés à *« accepter que les engagements vis-à-vis de services étrangers dits partenaires l'emportent sur la loi et les droits fondamentaux des citoyens notamment dans des dossiers se rapportent à une période précédant la conclusion de conventions en la matière. »*

Au cours des investigations de la Commission d'enquête parlementaire, il s'est avéré qu'un double des dossiers historiques avait été déposé, sous forme de microfiches, au Château de Senningen. Ces archives dits back-up ont fait l'objet, le 29 avril 2013, d'une saisie judiciaire par la chambre criminelle du Tribunal d'arrondissement de Luxembourg dans le cadre du procès dit « Bommeleër ». Sur demande spécifique de l'autorité de contrôle, la présidente de

la Chambre criminelle a, par ordonnance du 1er octobre 2013, procédé à une mainlevée partielle de la saisie aux fins de permettre à l'autorité de vérifier l'existence de dossiers à la suite de demandes individuelles dont elle est saisie. L'autorité effectue un contrôle systématique des doubles des dossiers et vérifie la concordance entre les dossiers des archives principales et celles déposées en back-up. Dans une série de dossiers des divergences ont été relevées et les intéressés ont obtenu, par le biais de l'autorité, copie des documents plus complets conservés uniquement sous forme de back-up.

Par rapport à chaque demande individuelle, l'autorité a également contrôlé le fichier informatique des données faisant l'objet d'un traitement opérationnel actuel. En fonction de la décision du service de renseignement, elle a informé les intéressés du résultat de ces contrôles.

L'autorité de contrôle voudrait encore évoquer la question fondamentale de la durée de conservation des données, de leur archivage et de leur élimination.

Elle note que la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat ne comporte aucune disposition relative à la durée de conservation.

La loi du 15 juin 2004 relative à la classification des pièces et habilitations de sécurité prévoit à l'article 23 que « *les données relatives à l'enquête de sécurité sont détruites ou effacées:*

- endéans les six mois suivant la décision de refus sauf si les raisons pour lesquelles elles ont été recueillies sont toujours d'actualité;

- endéans les cinq ans après que le candidat ait cessé son activité requérant l'accès à des pièces classifiées. »

L'autorité a constaté que cette disposition n'a pas été respectée.

En 2013, la saisie des dossiers historiques par la Commission d'enquête parlementaire et des dossiers back-up par la chambre criminelle du tribunal d'arrondissement de Luxembourg a « mis entre parenthèses » la question de l'élimination des données, à tout le moins pour les dossiers dits historiques.

Par contre, en rapport avec une série de demandes individuelles, l'autorité de contrôle a ordonné que des données nominatives soient radiées dans les fichiers opérationnels. Il faut relever que ces décisions n'ont jamais donné lieu à des contestations de la part du service de renseignement; par contre, la position de l'autorité a été contestée par certains intéressés et certains députés et mise en doute par des membres de la commission parlementaire pour le contrôle du service de renseignement dans un courrier adressé à l'autorité de contrôle.

Dans un courrier à Monsieur le Président de la Chambre des Députés de décembre 2013, les membres de l'autorité ont pris position comme suit :

> *« (L'article 17 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel) ne prévoit pas l'information des personnes dont les données sont traitées que ce soit sur le contenu de celles-ci ou sur le contexte du traitement. Si les archives historiques ont été ouvertes, c'est en vertu d'une décision du responsable du traitement et du ministre de tutelle. Il est vrai que*

l'autorité, dans des courriers de fin 2012, a appelé de ses vœux une telle ouverture; elle n'était toutefois pas en mesure de l'imposer dans le cadre légal actuel. Rien n'empêche, à l'heure actuelle, le responsable du traitement ou le ministre de tutelle d'étendre la communication aux bases de données opérationnelles. L'autorité de contrôle ne pourra que saluer cette ouverture. Elle est toutefois le mauvais destinataire de soucis et préoccupations exprimés à cet égard dans la prise de position.

Si la loi exclut l'accès aux données, elle prévoit toutefois, expressément, le droit de l'autorité de procéder à des rectifications. Ce concept ne saurait être limité au redressement d'erreurs matérielles, mais doit être replacé dans le contexte du contrôle de la nécessité et de la proportionnalité du traitement qui constituent des principes de base en la matière. A cet égard, l'autorité assume une mission de sauvegarde des droits des citoyens que ceux-ci sont dans l'impossibilité d'exercer eux-mêmes. L'ordre de rectification ou de radiation met un terme à un traitement illicite; l'information que la rectification a été opérée donne tout son sens à l'information que désormais le traitement n'est plus contraire à la loi. Constater des traitements illicites sans ordonner une rectification signifie que le responsable du traitement continue d'opérer des traitements illicites, sauf à procéder lui-même d'office à des radiations, ce qu'il est d'ailleurs parfaitement en droit de faire à tout moment. La loi ne permet pas à l'autorité de geler des données illicites ou de les laisser en place tout en interdisant leur utilisation. Seul le responsable du traitement ou le ministère de tutelle pourrait s'engager dans cette voie. Sur ce point encore, les préoccupations des signataires de la prise de position devraient être adressées à une autre instance.

....

Les radiations n'ont jamais porté sur des données dans les fichiers historiques, mais sur des données de la base opérationnelle. Par rapport à ce système informatique, le terme de dossier ou de fichier est d'ailleurs techniquement inadapté. Sauf erreur de la part des membres de l'autorité, il n'a jamais été question de soumettre les bases de données actuelles à un inventaire en vue d'une analyse scientifique et historique. Cela peut bien sûr se faire si le SRE est supprimé et si l'ensemble de ses bases de données fait l'objet d'une analyse historique.

Il faut bien garder à l'esprit la situation à laquelle se trouve confrontée l'autorité au moment où elle procède à des contrôles et constate un traitement illicite dans la base des données opérationnelles :

soit elle « passe outre » et informe l'intéressé qu'il n'y a pas de traitement contraire à la loi ;
soit elle ordonne une radiation sans avertir l'intéressé qui sera seulement informé qu'il n'y a pas de traitement contraire à la loi ;
soit, elle ordonne la radiation et en informe l'intéressé, tout en restant légalement dans l'impossibilité de révéler le contenu des données radiées sauf autorisation spécifique du responsable du traitement.

La dernière solution est la seule qui est conforme à la loi tout en étant la plus respectueuse des droits des citoyens. Il n'y a pas d'autre solution sauf à obtenir de la part du SRE une levée du secret.

Il convient d'ajouter que, dans tous les cas où une radiation a été ordonnée, le SRE ne s'y est pas opposé. Cela ne veut pas dire que l'autorité s'est transformée en complice de radiations opérées par le SRE, qu'il peut d'ailleurs effectuer à tout moment sans informer quiconque, mais uniquement que l'autorité voulait éviter des discussions juridiques sur la nature de sa décision qui aurait pu être attaquée devant un juge par le SRE ou par le ministre de tutelle. Il est vrai que la loi, sur ce point, n'est pas claire. Il était toutefois évident que le SRE, tout en acceptant la radiation, s'opposait à une communication plus étendue qui risquait d'affecter l'efficacité de sa banque de données opérationnelles. »

Statistiques des demandes dont l'autorité a été saisie jusqu'au 31 décembre 2013

	Nombre
Demandes sans objet / absence de dossier individuel	489
Dossier historique service de renseignement (SRE)	94
Dossier autorité nationale de sécurité (ANS)	44
Dossier exclusivement dans la base de données opérationnelle dite (I-base)	2
Réponse qu'il n'y a pas de traitement contraire à la loi	18
Transmission de pièces relatives au demandeur trouvées dans un autre dossier	2
Dossier historique SRE + dossier ANS	6
Dossier historique SRE + dossier I-base	11
Dossier ANS + dossier I-base	4
Dossier historique SRE + dossier ANS + dossier I-base	2
Demandes en suspens au 31 décembre 2013	7
TOTAL	**679**

VII. Demandes d'accès Schengen

L'autorité de contrôle a publié sur le site internet de la Commission nationale pour la protection des données un guide sur l'exercice du droit d'accès ensemble avec trois lettres-types pouvant servir de modèle en vue de saisir l'autorité de contrôle d'une demande d'accès, de rectification ou de suppression relative à des données traitées dans le SIS.

Au cours de la période couverte par le présent rapport, l'autorité de contrôle a été saisie de plusieurs demandes d'exercice du droit d'accès aux données traitées dans le N.SIS, en application de l'article 109 de la Convention d'application de l'Accord de Schengen.

Ces demandes émanaient, la plupart du temps, de personnes ne résidant pas au Luxembourg. Certaines ont été transmises par des avocats établis au Luxembourg, d'autres ont été continuées à l'Autorité de contrôle par des commissions de protection des données d'autres Etats membres de l'Union européenne ou de la zone Schengen. Toutes les demandes ont été traitées immédiatement.

Au cours de l'année 2013, l'autorité de contrôle a participé à une étude européenne sur l'exercice du droit d'accès des personnes concernées dans les Etats membres de l'Union européenne. A la date du 31 décembre 2013, le rapport afférent n'était pas encore adopté.

VIII. Activités internationales

1) Autorité de contrôle commune Schengen

Conformément à l'article 115 de la Convention d'application de l'Accord de Schengen du 14 juin 1985, signée à Schengen le 19 juin 1990 et approuvée par la loi du 3 juillet 1993, ont été désignés comme représentants de l'autorité de contrôle à l'autorité de contrôle commune chargée du contrôle de la fonction de support technique du système d'information :

- Monsieur Pierre Weimerkirch et Monsieur Thierry Lallemang, membres effectifs,
- Monsieur Georges Wivenes, membre suppléant.

L'autorité commune de contrôle Schengen publie, tous les ans, un rapport d'activités auquel les auteurs du présent rapport voudraient renvoyer.

2) Autorité de contrôle commune Europol et Comité de recours Europol

La Convention du 26 juillet 1995, conclue sur la base de l'article K.3 du Traité sur l'Union européenne, portant création d'un Office européen de police (Europol) prévoit, aux articles 23 et suivants, l'instauration d'une autorité de contrôle nationale et d'une autorité de contrôle commune au sein de laquelle est constitué un comité de recours.

La loi du 29 mai 1998 portant approbation de la Convention Europol dispose, dans l'article 3, que l'autorité de contrôle prévue au paragraphe (4) de l'article 12-1 de la loi modifiée du 31 mars 1979 est désignée comme autorité de contrôle nationale « Europol ».

Les compétences de l'autorité prévue par la loi de 1979 ont passé à l'autorité de contrôle prévue à l'article 17 de la loi du 2 août 2002.

Ont été désignés membres de l'autorité de contrôle commune Europol :

- Messieurs Pierre Weimerskirch et Monsieur Thierry Lallemang, membres effectifs
- Monsieur Georges Wivenes, membre suppléant.

Monsieur Thierry Lallemang a été désigné membre et Monsieur Georges Wivenes, comme membre suppléant du comité de recours.

L'autorité commune de contrôle Europol publie régulièrement des rapports d'activité auxquels les soussignés voudraient renvoyer.

3) Autorité commune de contrôle douane

La Convention sur l'emploi de l'informatique dans le domaine des douanes du 26 juillet 1995, approuvée au Luxembourg par la loi du 20 décembre 2002, institue à l'article 17 une autorité commune de contrôle. En application de l'article 2 de la loi d'approbation parlementaire, l'autorité de contrôle est désignée pour participer à cette autorité commune.

Ont été désignés comme représentants luxembourgeois :

Messieurs Pierre Weimerskirch et Monsieur Thierry Lallemang, membres effectifs,
Monsieur Georges Wivenes, membre suppléant

Au cours de l'année 2013, les membres de l'autorité de contrôle ont assisté à

- 4 réunions de l'autorité commune de contrôle Schengen
- 4 réunions de l'autorité commune de contrôle Europol
- 4 réunions de l'autorité commune de contrôle Douanes

Les membres de l'Autorité de contrôle représentent le Luxembourg lors de ces réunions, participent aux travaux, fournissent les renseignements requis par les autorités communes et effectuent les contrôles requis.

Le présent rapport a été adopté à l'unanimité des membres de l'autorité de contrôle lors de la réunion en date d'aujourd'hui.

Luxembourg, le 14 mars 2014

Georges Wivenes	Pierre Weimerskirch	Thierry Lallemang
délégué du Procureur général président	membre de la CNPD membre	membre de la CNPD membre