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

(abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données)

Rapport rendant compte de l'exécution de la mission de l'autorité de contrôle pendant la période de 2016, 2017 et 2018 (jusqu'au 19 août 2018)

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 ».

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

- doit être 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 ayant dans ses attributions la protection des données et donc pour les années concernées, le Ministre des Communications et des Médias, un rapport rendant compte de l'exécution de sa mission. Dans sa pratique des années précédentes, l'autorité présentait un rapport couvrant deux années. Comme la loi modifiée du 2 août 2002 a été abrogée par la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données et que cette dernière est entrée en vigueur en date du 20 août 2018, le présent rapport couvre la période allant du 1er janvier 2016 jusqu'au 19 août 2018. L'abrogation de la loi modifiée du 2 août 2002 a aussi entraîné la suppression de l'autorité de contrôle « Article 17 » dont les compétences et missions ont été conférées à la Commission Nationale pour la Protection des Données (CNPD) en vertu de la loi du 1er août 2018 précitée.

L'article 32, paragraphe 2, de la loi modifiée du 2 août 2002 investit la commission nationale pour la protection des données de l'obligation de rédiger un 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.

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 du 1er septembre 2010 au 1er août 2015 et par Madame le Procureur général d'Etat Martine Solovieff entrée en fonction le 1er août 2015.

Madame Marie-Jeanne Kappweiler, 1er Avocat général, a été déléguée par Madame le Procureur général d'Etat Martine Solovieff, avec effet au 16 septembre 2016 pour présider l'autorité de contrôle, en remplacement de Monsieur le Procureur général d'Etat adjoint Georges Wivenes.

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

Par arrêté ministériel du 19 novembre 2014, Madame Tine A. Larsen, présidente de la Commission nationale pour la protection des données depuis le 1er novembre 2014, a été nommée membre de l'autorité de contrôle.

III. Réunions et fonctionnement de l'autorité de contrôle

L'autorité de contrôle s'est réunie formellement à 11 reprises au cours des années 2016, 2017 et début 2018. A relever que 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 ».

Ce règlement grand-ducal obligatoire n'a jamais été adopté. L'adoption de ce règlement n'a cependant jamais été considérée par l'autorité comme une condition juridique préalable à l'exécution des missions légales, sinon elle n'aurait jamais pu commencer à exercer ses missions légales. Dans une approche pragmatique, les tâches administratives ont été assurées par les membres de l'autorité, malgré l'absence de ressources et de budget propre à l'autorité de contrôle.

Dans ses rapports antérieurs, l'autorité de contrôle a 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.

L'autorité a également signalé, dans ses rapports antérieurs, que le Comité d'évaluation Schengen de la Commission européenne qui avait procédé au cours de la période fin 2008 – début 2009 à un contrôle de l'acquis de Schengen au 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 de l'acquis de Schengen a eu lieu en 2016. A cette fin, un comité d'expert de la Commission européenne a effectué un contrôle sur place à Luxembourg entre le 25 et le 29 janvier 2016. Dans son rapport d'évaluation (document classifié RESTREINT-UE), l'équipe d'expert a de nouveau critiqué le fait que l'autorité de contrôle « Article 17 » n'était pas dotée de ressources suffisantes pour pouvoir remplir correctement ses missions dont elle est investie par le Règlement SIS II (UE) 1987/2006.

IV. Contrôles effectués auprès de l'Administration des douanes et accises

Au niveau de l'Union européen, 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.

Au niveau européen, l'autorité de contrôle a participé en 2016, 2017 et jusqu'au 19 août 2018 à 5 réunions dans le contexte du traitement des données dans le système européen « CIS » (Customs Information System).

L'autorité de contrôle rappelle et regrette que le traitement des données par l'Administration des douanes et accises 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.

La nécessité de la mise en place d'un cadre légal et réglementaire devient d'autant plus évidente que l'Administration des douanes et accises s'est vu 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.

Une visite d'une demi-journée a eu lieu en date du 16 juillet 2016 dans les locaux de la direction de l'Administration des douanes et accises.

Lors de cette visite, les membres de l'autorité de contrôle ont rappelé le mécanisme bicéphale du contrôle en vigueur au Luxembourg, la CNPD étant compétente pour les missions de

nature strictement administrative de l'Administration des douanes et accises, l'autorité de contrôle prévue à l'article 17 étant chargée de la surveillance des missions de prévention et d'enquête des infractions pénales.

Ont également été évoquées les implications des nouvelles normes de droit dérivé européen, à savoir, pour le volet administratif le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif 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, pour le volet prévention et recherche des infractions, la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

Deux sujets majeurs ont été abordés : la participation de l'Administration de douanes et accises dans les systèmes mis en place au niveau de l'Union européenne et les traitements des données au niveau national.

1. Les traitements des données au niveau national

L'Administration des douanes et accises est investie, à l'instar de la Police grand-ducale, de missions de police judiciaire par certaines lois spéciales, en particulier dans le secteur des transports, du contrôle sanitaire, de la lutte contre les stupéfiants, de la sécurité au travail etc. Dans ce cadre, elle opère des traitements de données qui soulèvent des questions juridiques similaires à celles que pose le traitement des données par la Police grand-ducale.

Les membres de l'autorité de contrôle ont rappelé les termes de 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 et le mécanisme de l'autorisation de traitements par voie de règlement grand-ducal.

Aucun règlement ni général, ni particulier, autorisant l'Administration des douanes et accises à traiter des données en matière de prévention, recherche et constatation d'infractions pénales n'a été pris. Il en va de même pour le traitement des données en matière d'avertissements taxés.

- *La question de l'accès aux banques de données externes :*

La loi modifiée du 27 juillet 1993 portant organisation de l'Administration des douanes et accises ne comporte pas de disposition sur l'accès de l'administration à des banques de données externes contrairement à l'article 34-1 de la loi modifiée du 31 mai 1999 portant création d'un corps de Police grand-ducale et d'une Inspection générale de la police.

L'accès « par voie d'arrangement » (via RIFO) que les agents de la douane avaient au traitement des données « police générale » a été supprimé.

L'administration a accès aux données du registre national des personnes physiques sur la base de l'article 7 de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques.

Il en va de même pour l'accès au registre des exploitants de taxis en application de l'article 21 de la loi du 5 juillet 2016 portant organisation des services de taxis.
Elle bénéficie d'un accès élargi à la banque de données tenue par l'Administration du cadastre sur base de l'article 36 du règlement grand-ducal du 9 mars 2009 portant fixation des conditions et modalités de délivrance de de la documentation cadastrale.

En vertu des articles 77 et 78 de la loi du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises et sur base de l'article 22 du règlement grand-ducal du 23 janvier 2003 portant exécution de la loi du 19 décembre 2002 certains agents de l'Administration des douanes et accises peuvent consulter les données RCS (accès « public ») et PCN (accès « élargi ») de la base des données y afférente tenue par le Ministère de la Justice.

En vertu de l'article 4 du Règlement grand-ducal du 16 juin 2011 (installation et utilisation des tachygraphes) l'Administration des douanes et accises a accès aux données de la Société nationale de contrôle technique, données à fournir en vue de l'obtention au Grand-Duché de Luxembourg des cartes de tachygraphe.

L'administration a encore accès au fichier des autorisations d'établissement (MMAET) exploité pour le compte du ministre ayant les Classes moyennes dans ses attributions (actuellement le Ministère de l'Economie) en vertu du règlement grand-ducal du 28 avril 2015 portant création des traitements de données à caractère personnel nécessaires à l'exécution de l'article 32 de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industrie ainsi qu'à certaines professions libérales.

L'application SAP (PSCD - Public Sector Collection & Disbursement) gérée par le Centre des technologies de l'information de l'Etat et exploitée conjointement par l'Administration de l'enregistrement et des domaines et l'Administration des douanes et accises est liée aux données du fichier des assujettis à la taxe sur la valeur ajoutée et des détenteurs de véhicules.

L'Administration des douanes et accises n'a pas accès aux fichiers suivants :
- le fichier relatif aux affiliations des salariés, des indépendants et des employeurs géré par le Centre commun de la sécurité sociale sur base de l'article 321 du Code des assurances sociales ;
- le fichier des étrangers exploité pour le compte du service des étrangers du ministre ayant l'Immigration dans ses attributions;
- le fichier des demandeurs d'asile exploité pour le compte du service des réfugiés du ministre ayant l'Immigration dans ses attributions;
- le fichier des armes prohibées du ministre ayant la Justice dans ses attributions.

L'Administration des douanes et accises est en pourparlers avec le Bureau des passeports et des visas afin d'analyser l'opportunité d'un accès au fichier des demandeurs de visa exploité pour le compte du bureau des passeports, visas et légalisations du ministre ayant les Affaires étrangères dans ses attributions.

Il est également prévu qu'elle aura un accès „e-Détachement Badge Social" à la base de données de l'Inspection du Travail et des Mines (via IAM), base de données dont la création a été autorisée par Règlement grand-ducal en date du 9 février 1995.

- *La question du traitement des données en matière de recherche et de constatation d'infractions*

Les responsables de l'Administration des douanes et accises ont exposé que des unités différentes sont responsables pour la recherche et la constatation des infractions pénales selon les différents secteurs, (lutte contre les stupéfiants, transport, santé, sécurité au travail, etc.) Seuls les agents de ces services et les responsables des inspections concernées qui surveillent la rédaction des rapports et procès-verbaux, ont accès aux données. Les rapports et procès-verbaux rédigés sont gardés en copie dans un système commun d'archives. L'accès n'est toutefois pas possible aux agents autres que ceux des services compétents.

Deux systèmes informatiques sont appliqués, un système particulier pour les données traitées dans le cadre de la lutte contre les stupéfiants et un système commun dit DOCON, pour les autres matières. Le système Lux-trust n'est pas encore appliqué.

Dans certaines matières, l'Administration des douanes et accises agit sur instruction et pour le compte d'autres administrations ou ministères. Les rapports établis en exécution de ces instructions sont communiqués aux entités concernées. Copie est gardée aux archives, de sorte que les mêmes données sont traitées dans deux administrations/ministères différents.

Dans tous les domaines sécuritaires tombant sous la compétence de l'Administration des douanes et accises, les brigades opérationnelles (Transport, Santé, ITM/Environnement) peuvent agir de leur propre initiative pour rechercher et constater des infractions dans les matières leur attribuées à titre spécifique (exemple: La brigade Transport intervient dans les domaines relevant de la matière régissant la législation du Code de la route, des tachygraphes, des licences communautaires, du transport de marchandises dangereuses, etc.).

Il se fait pourtant que la plupart des interventions des brigades opérationnelles (Transport, Santé, ITM/Environnement) repose sur l'exécution de services ordonnés par l'Inspection des opérations sécuritaires (IOS), notamment pour le suivi des demandes de contrôle émanant de la part

- des Classes moyennes (MECO) : contrôles a posteriori des révocations, annulations et suspensions d'autorisations d'établissement ; contrôles préalables pour la délivrance d'une autorisation d'établissement
- de la Direction des transports routiers (MDDI) : contrôles préalables en entreprise pour la prolongation des licences communautaires
- de la division de la Santé au Travail (MSAN) : contrôles de la médecine au travail (inventaire des postes à risques, examen médicaux des salariés)
- de l'Administration des services de l'agriculture et de l'Inspection vétérinaire (MAGR) : contrôles des équidés, des transports aliments pour animaux, bien-être animal, chiens dangereux
- de la Direction de la Santé (MSAN) : contrôles conjoints de l'installation de fumoirs, contrôles de l'hygiène alimentaire dans le secteur de la restauration
- de l'Inspection du travail et des mines (ITM) : détachement de salariés, durée de travail, travail clandestin
- de plaintes reçues de la part d'une tierce personne : contrôles en matière de droit d'établissement, de travail clandestin, de la lutte anti-tabac, etc.

Dans certaines de ces matières les agents des brigades opérationnelles participent à des équipes dites mixtes, notamment lors des contrôles de fumoirs (avec la MSAN) et de

chantiers (avec l'ITM). Les données relatives à ces opérations sont traitées par les administrations et services que la douane a assistés.

A noter que certaines collaborations avec les autorités susvisées sont retenues par écrit moyennant convention signée entre les administrations concernées et l'ADA.

Tout contrôle effectué par un agent des brigades opérationnelles donne lieu à une inscription obligatoire dans le fichier DOCON. Selon les constatations faites, il est dressé, le cas échéant, un procès-verbal, un rapport, une fiche de contrôle ou un avertissement taxé. Dès que l'application SIDOC (Système intégré de gestion des documents du CTIE) sera accessible aux brigades opérationnelles (début 2017) l'archivage des procès-verbaux, rapports et fiches de contrôles se fera exclusivement au sein de l'Inspection IOS.

Dans le secteur de la lutte contre les stupéfiants des données sont échangées entre l'Administration des douanes et accises et la Police grand-ducale. Un ordinateur de la Police, installé à Rumelange dans les locaux de la Brigade de recherches et d'investigations (BRI), permet aux agents de ladite brigade de consulter la base de données de la Police et d'y saisir leurs propres constatations en la matière. La mise à disposition de ces données se fait sur base de demandes d'accès et est encore dépourvue de base légale.

2. Les traitements de données au niveau européen

Les responsables de l'Administration des douanes et accises ont confirmé, comme dans le passé, que le système d'information européen « CIS » n'est pratiquement pas utilisé.

Dans ce contexte, les membres de l'autorité de contrôle ont informé l'Administration des douanes et accises que, sur base de deux textes européens distincts, ce système est actuellement supervisé par deux autorités de contrôles communes européennes (l'autorité de contrôle luxembourgeoise y est représentée), à savoir :

- la « Joint Supervisory Authority – Customs » qui se situe au niveau du conseil européen, et
- le « Customs Supervision Coordination Group » qui se situe au niveau du Contrôleur Européen de Protection des Données.

V. Contrôles effectués auprès de la Police grand-ducale

1. Traitements de données dans les systèmes d'information européens

a. Système d'Information Schengen deuxième génération (SIS II)

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, entré en vigueur début 2007 (ci-après « Règlement SIS II ») et la Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) (ci-après « Décision SIS II) règlementent le Système d'Information Schengen aussi au niveau national. Le système SIS II est devenu opérationnel au mois d'avril 2013.

Le Système d'Information Schengen de deuxième génération (SIS II) 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 26 de la Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) :

Il s'agit de données relatives aux personnes recherchées pour arrestation et extradition. L'intégration dans le SIS II 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.

- Article 24 du Règlement (CE) N° 1987/2006 du Parlement Européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) :

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 32 de la Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) :

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 34 de la Décision 2007/533/JAI :

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 36 de la Décision 2007/533/JAI :

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. La police grand-ducale a mis en place un système technique de consultation commun des trois systèmes Interpol, Europol et Schengen qui garantit les spécificités de chacun de ces systèmes. L'autorité de contrôle a pu vérifier le fonctionnement de ce nouveau mécanisme et a marqué son accord avec son application.

b. Evaluation du Grand-Duché de Luxembourg de l'application de l'acquis de Schengen dans les domaines de la protection des données et du système d'information Schengen

Le règlement (UE) n° 1053/2013 porte création d'un mécanisme d'évaluation et de contrôle destiné à vérifier l'application de l'acquis de Schengen. Un rapport d'évaluation faisant état des constatations et appréciations, et notamment des éventuels manquements relevés au cours de l'évaluation, est dressé sur la base d'inspections effectuées sur place portant sur des aspects spécifiques de l'acquis de Schengen.

En 2016, le Luxembourg a fait l'objet d'une telle évaluation sur l'application de l'acquis de Schengen dans le domaine de la protection des données. Une visite sur place par une équipe d'experts (composée d'experts de la Commission européenne et d'experts d'autres Etats membres de l'UE) a eu lieu pendant 5 jours (25-29 janvier 2016).

En fonction des compétences respectives entre l'autorité de contrôle et la CNPD, les membres de l'autorité de contrôle ont accompagné l'équipe d'expert lors des différents contrôles et inspections sur place dans les locaux de la Police grand-ducale.

Suite au rapport d'évaluation dressé par l'équipe d'expert, le Conseil européen a adopté une décision d'exécution à l'égard du Luxembourg et a arrêté 17 recommandations pour remédier aux manquements constatés dans le cadre de l'évaluation. Parmi les 17 recommandations, la Police grand-ducale était concernée par 4 recommandations.

Conformément à l'article 16 du règlement (UE) n° 1053/2013, l'Etat membre évalué est tenu de transmettre à la Commission et au Conseil un plan d'action destiné à remédier aux manquements constatés.

Les membres de l'autorité de contrôle ont participé à l'élaboration du plan d'action qui a été transmis par le Grand-Duché de Luxembourg aux instances européennes en date du 27 avril 2017.

L'autorité de contrôle a supervisé et suivi la mise en œuvre des mesures correctrices par la Police grand-ducale pour remédier aux manquements constatés. Au cours du premier trimestre 2018, la Police grand-ducale avait terminé l'implémentation de toutes les mesures correctrices et dès lors satisfait aux recommandations formulées par le Commission européenne et le Conseil.

c. Audit des activités de traitements de données dans le SIS II national auprès de la Police grand-ducale

Conformément à l'article 60(2) de la Décision SIS II et à l'article 44(2) du Règlement SIS II, l'autorité de contrôle nationale doit veiller à ce que soit réalisé, tous les quatre ans au minimum, un audit des activités de traitement de données dans le cadre de son N.SIS II (National SIS II), répondant aux normes internationales en matière d'audit.

A l'aide des ressources de la CNPD, l'autorité de contrôle a réalisé un tel audit dont les travaux ont duré 8 mois (mars – octobre 2017). L'audit, englobant également des visites sur place, portait sur la sécurité des données et sur le module des alertes/signalements introduits

dans le SIS II. La mission d'audit a par ailleurs pris en compte les recommandations formulées par la Commission européenne et le Conseil dans le cadre de l'Evaluation Schengen.

L'autorité de contrôle a adopté un rapport d'audit au mois d'octobre 2017. Au regard de l'objet de l'audit onze insuffisances ont été constatées, dont trois ont été évalué comme hautement risquées en termes de sécurité. Sept recommandations ont été formulées à l'adresse de la Police grand-ducale pour remédier aux insuffisances relevées.

Etant donné que l'autorité de contrôle n'existe plus, au moment de la rédaction du présent rapport, et que les compétences et missions de celle-ci ont été conférées à la CNPD depuis l'entrée en vigueur de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, la CNPD assurera le suivi de la mise en œuvre des mesures par la Police grand-ducale, afin de satisfaire aux recommandations formulées.

d. Contrôle des fichiers de logues du SIS II auprès de la Police grand-ducale

L'article 44(1) du Règlement SIS II dispose que « La ou les autorités désignées dans chaque État membre et investies des pouvoirs visés à l'article 28 de la directive 95/46/CE (les «autorités de contrôle nationales») contrôlent en toute indépendance la licéité du traitement des données à caractère personnel dans le cadre du SIS II sur leur territoire et leur transmission à partir de celui-ci, y compris pour ce qui concerne l'échange et le traitement ultérieur d'informations supplémentaires. »

Le contrôle de(s) fichier(s) de logues du SIS II constitue une mesure de contrôle sur base de l'article 44 (1) précité.

Au cours de l'été 2017, l'autorité de contrôle a procédé à une revue des logues du SIS II. L'autorité de contrôle a suivi une approche en 4 étapes pour effectuer le contrôle des logues, à savoir :

Etape 1 : Prise de connaissance générale des dispositions techniques et organisationnelles en relation avec les logues SIS II à travers des réunions dans les locaux de la PGD avec le personnel clé en charge du SIS II d'un point de vue juridique et technique. Cette étape a permis de préparer la revue subséquente.

Etape 2 : Sélection de logues à revoir et inspection sur site dans le système respectif les logues à un niveau de granularité permettant de vérifier la licéité des interrogations, impressions, modifications, créations de signalements et créations d'alias par unité organisationnelle, et identifier des cas pour lesquels une analyse plus approfondie est nécessaire. Cette étape comporte aussi la sélection d'un échantillon de logues pour lesquels une analyse de la licéité du traitement est vérifiée au cas par cas.

Etape 3 : Suivi des observations faites lors de l'étape 2.

Etape 4 : Formalisation du rapport.

Lors de ce contrôle, aucune irrégularité n'a été constatée.

e. Demandes d'accès aux données dans le SIS II

L'article 17 de la loi modifiée du 2 août 2002 a introduit un droit d'accès aux données indirect dans la mesure où la personne concernée doit exercer son droit par l'intermédiaire de l'autorité de contrôle.

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 II.

Au cours de la période couverte par le présent rapport, l'autorité de contrôle a été saisie de 12 demandes d'exercice du droit d'accès aux données traitées dans le N.SIS II (2016 : 3 demandes ; 2017 : 3 demandes, 2018 (jusqu'au 19 août 2018) : 6 demandes, en application de l'article 58 de la Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

2. Traitements de données au niveau national

Au cours de l'exercice écoulé, huit réunions et visites sur place ont eu lieu dans les locaux de la Police grand-ducale et portaient sur les sujets et problématiques suivants :

- Le 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 (Ingepol)
- Le Journal des incidents (JDI)
- Le projet du système de gestion des interventions « EinsatzLeitSystem » (ELS)
- Les données PNR
- Le fichier hébergement
- L'application SIGMA (Signalements Multiples Automatisés)
- L'Evaluation Schengen
- L'audit SIS II
- Le projet pilote « bodycams »

Parmi les problématiques ci-avant, l'autorité de contrôle voudrait souligner les éléments ci-après :

a. Suivi des problématiques soulevés dans son rapport d'activité sur 2014 et 2015 : le règlement grand-ducal modifié du 2 octobre 1992 (Ingepol) et le Journal des incidents (JDI)

Pendant la période couverte par le présent rapport, le traitement des données de police (Ingepol) 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 2015, 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 19 mai 2014 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 31 décembre 2015.

Par règlement grand-ducal du 15 décembre 2015 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 31 décembre 2016.

Par règlement grand-ducal du 23 décembre 2016 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 2018.

Comme dans ses rapports d'activité antérieurs, l'autorité de contrôle rappelle que la reconduction systématique du règlement de 1992 constitue une réponse inadéquate.

Tout comme dans le passé, l'autorité de contrôle a continué à rappeler cette position lors des entrevues qu'elle a eues avec la Police grand-ducale en 2016 et 2017.

Dans son rapport 2014/2015, l'autorité de contrôle formulait les critiques suivantes :

« *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 des traitements des données opérées actuellement par la Police grand-ducale.*

L'autorité de contrôle a noté que la Police grand-ducale opère, à côté du fichier dit central basé sur le règlement de 1992, une série d'autres traitements qui n'ont pas de base réglementaire claire, en particulier le système dit du journal des incidents.

Dans ses entrevues avec les responsables de la Police grand-ducale, l'autorité de contrôle a rappelé, une nouvelle fois l'inadéquation du système de traitement des données figurant dans le journal des incidents avec les règles sur la protection des données. Les rapports dressés tous les jours par les agents portant sur leurs activités et sur les constats effectués sont enregistrés dans une banque de données globale ouverte à tous les agents sur l'ensemble du territoire. L'autorité de contrôle a suggéré une série de pistes de réflexions pour réorganiser ce mécanisme : élimination des données une fois un rapport ou un procès-verbal établi et transmis aux parquets, limitation de l'accès d'après des critères du lieu d'affectation des agents, de leur fonction ou grade. L'autorité de contrôle n'a pas été informée que des suites auraient été réservées à ces réflexions. »

Dans un courrier adressé au mois d'avril 2016, l'autorité de contrôle a rappelé au Directeur général de la Police grand-ducale l'extrait de son rapport 2014/2015 ci-avant cité et a souligné que l'autorité de contrôle n'avait pas été informée des suites éventuelles réservées à

ses suggestions. En guise de conclusion, elle a rappelé dans son courrier sa position sur trois points fondamentaux :

- La nécessité indiscutable d'adopter le ou les règlements nécessaires au titre de l'article 17 de la loi modifiée du 2 août 2002
- La nécessité de respecter le mécanisme prévu dans le règlement Ingepol de 1992, en attendant l'adoption des nouveaux textes réglementaires
- La nécessité de revoir et de réformer le mécanisme du journal dit des incidents alors que l'autorité voit mal comment ce système pourrait, dans le respect des règles fondamentales en matière de protection des données, être maintenu dans une future règlementation

Dans son courrier de réponse adressé à l'autorité de contrôle au mois de mai 2016, le Directeur de la Police grand-ducale a pris position quant aux problématiques soulevées et a fait part de l'état d'avancement des mesures entamées par la Police.

Pour ce qui est du règlement Ingepol, l'autorité de contrôle a été informée :

- que la Police avait élaboré un nouveau projet de règlement grand-ducal sur base de l'article 17 de la loi modifiée du 2 août 2002 qui devra remplacer le règlement Ingepol de 1992. Le projet de texte, dont un article sera dédié au « Journal des incidents » ferait prochainement l'objet d'une analyse au sein du groupe de travail créé à cet effet ;
- que les conditions d'application et de mise en œuvre du règlement Ingepol avait été revues à maintes reprises et que diverses mesures avaient été prises en vue de son application conforme.

En ce qui concerne le Journal des incidents, l'autorité de contrôle a été informée :

- que tous les accès des membres du cadre policier et du cadre administratif et technique aux différentes bases de données avaient été revus, dont notamment l'accès au fichier Journal des incidents,
- que cet accès avait été limité aux seuls membres du cadre policier ayant la qualité d'officier de police judiciaire (par analogie au texte réglementaire Ingepol),
- que le mécanisme du Journal des incidents était en train d'être revu en attendant la mise en place du nouveau « Einsatzleitsystem (ELS) »,
- qu'il était envisagé de limiter l'accès au ELS par les agents de police à deux niveaux, à savoir qu'au premier niveau le fichier était accessible au seul Centre d'intervention national et qu'au deuxième niveau l'accès en serait limité au niveau régional,
- qu'au deuxième niveau, une recherche sur les activités/interventions effectuées sur l'ensemble du pays ne serait plus possible,
- que des procédures supplémentaires en amont pour prévenir des abus et des recherches arbitraires dans l'outil seraient introduites, en complément du système de journalisation permettant des contrôles a posteriori.

b. Nouveaux systèmes automatisés et applications informatiques

Lors de ses réunions et visites sur place, la Police a présenté un nouveau système de contrôle automatisé des signalements des listes des personnes hébergées, destiné à remplacer le

contrôle manuel effectué jusqu'alors, dans le cadre du fichier hébergement mis en œuvre en application de la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement et du règlement grand-ducal relatif aux fiches à tenir par les logeurs exploitant un service d'hébergement touristique.

Dans le domaine du traitement des données PNR (Passenger Name Record), la Police a présenté à l'autorité de contrôle une nouvelle application informatique en développement, en prévision de l'application de la loi implémentant la Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, à savoir la loi du 1er août 2018 relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Enfin, au cours de l'exercice couvrant le présent rapport, une autre nouvelle application dénommée SIGMA (Signalements Multiples Automatisés) a été développé par la Police. Cette application informatique répond également à une recommandation formulée par la Commission européenne et le Conseil suite à l'Evaluation Schengen qui demandait au Luxembourg de mettre en place un « Single Search Interface » entre les différents systèmes d'information européens tels que SIS II, Europol, VIS, afin de permettre aux autorités compétentes de pouvoir rechercher plus efficacement et dans le respect des règles de protection des données les signalements relatifs à des personnes et des objets.

c. Accès à des traitements externes

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 :

« Dans l'exercice des missions prévues aux articles 33 et 34, les membres de la Police ayant la qualité d'officier de police judiciaire ont accès direct, par un système informatique, aux traitements de données à caractère personnel suivants:

1. 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;

2. le fichier relatif aux affiliations des salariés, des indépendants et des employeurs géré par le Centre commun de la sécurité sociale sur base de l'article 321 du Code des assurances sociales, à l'exclusion de toutes données relatives à la santé;

3. le fichier des étrangers exploité pour le compte du service des étrangers du ministre ayant l'Immigration dans ses attributions;

4. le fichier des demandeurs d'asile exploité pour le compte du service des réfugiés du ministre ayant l'Immigration dans ses attributions;

5. le fichier des demandeurs de visa exploité pour le compte du bureau des passeports, visas et légalisations du ministre ayant les Affaires étrangères dans ses attributions;

6. le fichier des autorisations d'établissement exploité pour le compte du ministre ayant les Classes moyennes dans ses attributions;

7. le fichier des titulaires et demandeurs de permis de conduire exploité pour le compte du ministre ayant les Transports dans ses attributions;

8. le fichier des véhicules routiers et de leurs propriétaires et détenteurs, exploité pour le compte du ministre ayant les Transports dans ses attributions;

9. le fichier des assujettis à la taxe sur la valeur ajoutée, exploité pour le compte de l'Administration de l'Enregistrement et des Domaines;

10. le fichier des armes prohibées du ministre ayant la Justice dans ses attributions.

Dans l'exercice de ces mêmes missions, les membres de la Police ayant la qualité d'agent de police judiciaire ont accès direct, par un système informatique, aux fichiers visés aux points numéros 1, 2, 3, 4, 5, 6, 7, 8, et 10 de l'alinéa 1er. Il en est de même pour les membres du cadre administratif et technique de la Police, nommément désignés par le ministre ayant la Police dans ses attributions sur proposition du directeur général de la Police, en fonction de leurs attributions spécifiques. Les données à caractère personnel des fichiers accessibles en vertu des alinéas 1 et 2 sont déterminées par règlement grand-ducal.

Le système informatique par lequel l'accès direct est opéré doit être aménagé de sorte que:

(a) les membres de la Police visés aux alinéas 1 et 2 ne puissent consulter les fichiers auxquels ils ont accès qu'en indiquant leur identifiant numérique personnel, et
(b) que les informations relatives aux membres de la Police ayant procédé à la consultation ainsi que les informations consultées, la date et l'heure de la consultation sont enregistrées et conservées pendant un délai de 3 ans, afin que le motif de la consultation puisse être retracé. Les données à caractère personnel consultées doivent avoir un lien direct avec les faits ayant motivé la consultation.

Seules les données à caractère personnel strictement nécessaires, dans le respect du principe de proportionnalité, peuvent être consultées.

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.»

Le système informatique par lequel l'accès direct est effectué est opérationnel et a été aménagé sous forme de plate-forme commune appelée « Multipol ». Il est organisé de sorte que:

(a) les membres de la Police visés aux alinéas 1 et 2 ne puissent consulter les fichiers auxquels ils ont accès qu'en indiquant leur identifiant numérique personnel, et

(b) que les informations relatives aux membres de la Police ayant procédé à la consultation ainsi que les informations consultées, la date et l'heure de la consultation sont enregistrées et conservées pendant un délai de 3 ans, afin que le motif de la consultation puisse être retracé. Les données à caractère personnel consultées doivent avoir un lien direct avec les faits ayant

motivé la consultation. Seules les données à caractère personnel strictement nécessaires, dans le respect du principe de proportionnalité, peuvent être consultées.

d. 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 cessera 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 en 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.

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...* ».

Par règlement ministériel du 25 avril 2014, la vidéosurveillance dans la zone de sécurité « zone E » a été prorogée jusqu'au 25 avril 2015.

Par règlement ministériel du 1er octobre 2014, la vidéosurveillance dans les zones de sécurité « zone A, C et D » a été prorogée jusqu'au 1er octobre 2015.

Par règlement ministériel du 25 septembre 2015, la vidéosurveillance dans les zones de sécurité « zone A, C et D » a été prorogée jusqu'au 25 septembre 2016.

Par règlement ministériel du 15 avril 2015, la vidéosurveillance dans la zone de sécurité « zone E » a été prorogée jusqu'au 15 avril 2016.

Par règlement ministériel du 8 avril 2016, la vidéosurveillance dans la zone de sécurité « zone E » a été prorogée jusqu'au 8 avril 2017.

Par règlement ministériel du 20 septembre 2016, la vidéosurveillance dans les zones de sécurité « zone A, C et D » a été prorogée jusqu'au 20 septembre 2017.

Par règlement ministériel du 4 avril 2017, la vidéosurveillance dans la zone de sécurité « zone E » a été prorogée jusqu'au 4 avril 2018.

Par règlement ministériel du 15 septembre 2017, la vidéosurveillance dans les zones de sécurité « zone A, C et D » a été prorogée jusqu'au 15 septembre 2018.

Par règlement ministériel du 28 mars 2018, la vidéosurveillance dans la zone de sécurité « zone E » a été prorogée jusqu'au 28 mars 2019.

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 ».

La loi de 2004 a été abrogée et remplacée par la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat. Celle-ci prévoit en son article 10 paragraphe (1) : « *Le SRE procède au traitement des données personnelles qui sont nécessaires à*

l'accomplissement de ses missions légales. Le traitement s'effectue conformément à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Il fait l'objet d'un règlement grand-ducal prévu à l'article 17, paragraphe 1er, de la loi précitée du 2 août 2002. Tout accès aux données s'exerce en conformité avec le paragraphe 2, alinéa 5 du même article 17 ».

Depuis l'entrée en vigueur de la loi de 2016, aucun règlement grand-ducal n'a été adopté. Or, d'après les informations de l'autorité de contrôle un règlement grand-ducal serait en cours d'adoption.

Le dernier document de la procédure dont l'autorité de contrôle a connaissance est le deuxième avis complémentaire du Conseil d'Etat du 13 novembre 2018 concernant un projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par le Service de renseignement de l'État.

2. L'Autorité nationale de sécurité

La loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité a créé l'Autorité Nationale de Sécurité (ANS) chargée de veiller à la sécurité des pièces classifiées. L'ANS délivre les habilitations de sécurité qui constituent l'attestation officielle établie sur la base des informations recueillies par l'Autorité nationale de Sécurité, qui autorise l'accès à des données auxquelles un certain degré de confidentialité a été attribué. Les fonctions de l'Autorité nationale de Sécurité sont assumées par le Service de Renseignement.

A l'exception des membres du Conseil de Gouvernement et des membres de la Commission de Contrôle parlementaire, l'habilitation de sécurité n'est délivrée qu'aux personnes qui ont fait l'objet d'une enquête de sécurité.

L'enquête de sécurité a pour but de déterminer si la personne physique présente des garanties suffisantes, quant à la discrétion, la loyauté et l'intégrité pour avoir accès à des informations classifiées sans constituer un risque pour la sécurité du Grand-Duché de Luxembourg et des Etats auxquels il est lié par un accord en vue d'une défense commune, les relations internationales du Grand-Duché de Luxembourg et le potentiel scientifique ou économique du Grand-Duché de Luxembourg.

Il résulte des rapports des exercices précédents que l'autorité de contrôle a été dans l'impossibilité d'exercer sa mission de surveillance faute de délivrance par le Service de renseignement d'une habilitation de sécurité. Cette pièce n'a finalement été fournie aux membres de l'autorité qu'en date du 14 février 2013. La présidente actuelle de la CNPD, membre de l'Autorité de contrôle depuis le 19 novembre 2014 en remplacement de M. Pierre Weimerskirch, dispose d'une habilitation personnelle en vertu des fonctions qu'elle a exercées antérieurement.

L'autorité de contrôle a toujours considéré que ses membres devraient être dispensés, au titre de la future loi sur l'Agence nationale de sécurité, de la procédure d'habilitation, alors qu'il est inconcevable qu'une autorité investie d'une mission légale de contrôle puisse se trouver dans l'impossibilité d'exercer cette mission parce que l'administration concernée est en

mesure, par le biais d'une procédure d'habilitation, de lui refuser l'accès aux locaux ou aux données traitées.

A ce titre, l'autorité de contrôle relève que le projet de loi N° 6961 portant création de l'Autorité nationale de sécurité est censé répondre à cette problématique, alors que le texte en projet prévoit en son état actuel que les membres [de l'autorité de contrôle, respectivement] de la CNPD seront exempts de l'obligation d'être titulaire d'une habilitation de sécurité dans l'exercice de leurs fonctions.

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.
- 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 illégal.

Pendant l'année 2016, l'autorité de contrôle a été saisie de 6 demandes d'accès ; pour l'année 2017, il y avait 6 demandes et pour l'année 2018 (jusqu'au 19 août 2018) une seule demande.

4. Traitement des données dans les « archives historiques » du SRE

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 ces archives ; cette décision a été levée le 2 octobre 2013, à la veille de la dissolution de la Chambre des Députés précédant les élections législatives. 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.

Un double des microfiches avait été déposé au Château de Senningen. Ces archives dites back-up ont fait, le 29 avril 2013, l'objet d'une saisie judiciaire par la chambre criminelle du Tribunal d'arrondissement de Luxembourg dans le cadre du procès dit « Bommeleër ». Une mainlevée est intervenue par deux ordonnances du 15 juillet 2015 et du 21 juillet 2015 et les documents ont été transférés aux Archives nationales pour être joints à ceux déjà déposés.

La loi du 23 juillet 2016 portant mise en place d'un statut spécifique pour certaines données à caractère personnel traitées par le Service de renseignement de l'État consacre une assise légale à la conservation des dossiers composant les „archives historiques" du service de renseignement de l'Etat, en vue d'autoriser les exploitations scientifiques à des fins historiques.

Sur initiative de Monsieur le Président de l'autorité de contrôle instituée par l'article 17 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, une descente a eu lieu en date du 29 juillet 2016 dans les Archives nationales, en présence de représentants du SRE et d'un représentant des Archives Nationales.

La visite des lieux abritant les archives du SRE avait pour but de permettre la visualisation des documents et objets y entreposés en date du 2 octobre 2013 au regard des questions soulevées par le SRE, et ce à la lumière du projet de loi n° 6850 devenu la loi du 23 juillet 2016 portant mise en place d'un statut spécifique pour certaines données à caractère personnel traitées par le Service de renseignement de l'État.

Différents contrôles (dont le choix des personnes et des noms a été fait au hasard) ont été effectués dans les armoires, caisses en carton, caisses en plastique, livres de correspondance, documents opérationnels, afin de vérifier l'existence d'éventuels liens basés sur des données à caractère personnel et susceptibles de tomber dans le champ d'application de la loi du 23 juillet 2016 précitée.

A l'issue de ces contrôles, les autorités présentes sur les lieux sont venues aux conclusions suivantes :

- tous les documents et effets inventoriés sur place devraient y rester jusqu'à nouvel ordre, afin de rester à la disposition des experts-historiens à nommer en vertu de la loi précitée;

- tous les documents et autres supports physiques qui présentent un lien avec les fiches individuelles, contenues dans les armoires métalliques, sont exploitables par les historiens et tombent sous la loi précitée ;

- les autres documents devront être revus en présence d'un membre du SRE aux fins de décision future quant à une restitution éventuelle. Dans ce contexte il y lieu de tenir compte du classement des documents tel que défini à l'article 3(6) de la loi précitée.

VII. Activités internationales

1. Groupe de coordination du contrôle du SIS II « Supervision Coordination Group SIS II »

L'article 62 de la Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), prévoit que « *Les autorités de contrôle nationales et le Contrôleur européen de la protection des données, agissant chacun dans le cadre de leurs compétences respectives,*

coopèrent activement dans le cadre de leurs responsabilités et assurent la surveillance conjointe du SIS II. ..... Les autorités de contrôle nationales et le Contrôleur européen de la protection des données se réunissent à cet effet au minimum deux fois par an. ..... Le règlement intérieur est adopté lors de la première réunion. D'autres méthodes de travail sont mises au point d'un commun accord, si nécessaire. Un rapport d'activités conjoint est transmis tous les deux ans au Parlement européen, au Conseil, à la Commission et à l'instance gestionnaire. »

Ont été désignés comme représentants au groupe de coordination du contrôle du SIS II :

- Monsieur Thierry Lallemang, membre effectif,
- Madame Tine A. Larsen, membre suppléant.

Le groupe de coordination du contrôle du SIS II publie, tous les deux ans, un rapport d'activités auquel les auteurs du présent rapport voudraient renvoyer.

2. Comité de coopération Europol

Conformément au règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 (ci-après le « règlement Europol »), le Contrôleur européen de la Protection des Données (CEPD) - l'autorité indépendante de l'UE chargée de la protection des données - a pour tâche, depuis le 1er mai 2017, de contrôler la licéité du traitement de données à caractère personnel par Europol.

L'article 45 du règlement Europol a créé un Comité de coopération ayant une fonction consultative dans le cadre de la supervision du traitement de données par Europol. Il est composé d'un représentant de l'autorité de contrôle nationale de chaque État membre et du CEPD. Ce comité doit se réunir au moins deux fois par an.

Les compétences de l'autorité de contrôle nationale sont prévues à l'article 17 de la loi modifiée du 2 août 2002.

Ont été désignés membres du comité de coopération Europol :

- Monsieur Thierry Lallemang, membre effectif
- Madame Tine A. Larsen, membre suppléant

Le Comité de coopération Europol publie un rapport d'activité tous les deux ans auxquels les soussignés voudraient renvoyer.

3. Groupe de coordination du contrôle du système d'information européen des Douanes « Customs Supervision Coordination Group »

Le Règlement (CE) N° 515/97 du Conseil du 13 mars 1997 établissant un Système d'Information Douanier (SID) prévoit à l'article 37 la désignation d'une autorité de contrôle nationale (en l'occurrence l'autorité prévu à l'article 17 de la loi modifiée du 2 août 2002) et à l'article 43 une autorité de contrôle commune européenne aux fins de supervision et de contrôle du respect des règles en matière de protection.

Le Règlement (CE) 766/2008 du Parlement européen et du Conseil du 9 juillet 2008 a institué un groupe de coordination du contrôle du système d'information européen des Douanes.

Y ont été désignés comme représentants luxembourgeois :

Monsieur Thierry Lallemang, membre effectif,
Madame Tine A. Larsen, membre suppléant

Au cours des années 2016, 2017 et 2018 (jusqu'au 19 août 2018), les membres de l'autorité de contrôle ont assisté à

- 5 réunions du groupe de coordination du contrôle du SIS II
- 5 réunions du Comité de coopération Europol
- 5 réunions du groupe de coordination du contrôle du système d'information européen des 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 de contrôle européennes et effectuent les contrôles requis.

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

Luxembourg, le 8 juillet 2019.

Marie-Jeanne Kappweiler Premier Avocat général Déléguée du Procureur général	Tine A. Larsen	Thierry Lallemang
Présidente	Présidente de la CNPD Membre	Commissaire à la CNPD Membre