Avis de la Commission nationale pour la protection des données relatif au projet de loi n°6976 relatif à l'échange de données à caractère personnel et d'informations en matière policière et portant :
1) transposition de la décision - cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne ;
2) mise en oeuvre de certaines dispositions de la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière

Délibération n° 966/2016 du 17 novembre 2016

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

Par courrier du 22 mars 2016, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n°6976 relatif à l'échange de données à caractère personnel et d'informations en matière policière et portant :
1) transposition de la décision - cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne ;
2) mise en oeuvre de certaines dispositions de la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

Outre les deux textes à transposer ou à mettre en œuvre, le présent avis se réfèrera aussi à :
- la *décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale* qui définit, de manière générale, des règles communes à tous les Etats membres pour la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale
- la *directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative 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, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil* dont le champ d'application. A la différence de son texte prédécesseur, la décision-cadre 2008/977/JAI, n'est pas limité aux échanges de données entre les Etats membres de l'Union européenne, mais, au contraire, couvre aussi les situations internes à un Etat-membre et les transferts de données vers des pays tiers

1. Appréciation générale du projet de loi

1.1. Les données pouvant faire l'objet de transmissions

En vertu du principe de disponibilité consacré par le projet de loi sous avis et les deux textes européens à mettre en œuvre, toute information disponible pour l'autorité policière d'un pays participant aux échanges de données doit aussi être disponible aux autorités policières des autres pays participants.

Concrètement, les informations détenues par la Police grand-ducale et mais aussi celles qui lui sont accessibles pourront, voire devront être transmises à toutes les autorités visées par les articles 1 et 18 du projet de loi selon les conditions fixées par celui-ci.

Vu l'étendue importante des données pouvant être transmises, il est d'autant plus important que les traitements de données qui sont effectués, à la base, au niveau national, par la Police grand-ducale respectent les règles relatives à la protection des données, au risque que des irrégularités ne soient en quelque sorte « exportées » par le biais des échanges mis en place en vertu du projet de loi sous avis. Or, la CNPD constate que la législation nationale relative aux traitements de données opérés par la Police grand-ducale n'est pas conforme aux principes régissant la protection des données. Pourtant on entend permettre par le biais du projet de loi sous examen d'échanger des données au niveau international.

En effet, la CNPD voudrait, une fois de plus, relever que le règlement grand-ducal modifiée du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale (« règlement Ingepol ») ne répond pas à toutes les exigences juridiques de protection des données découlant de la loi modifiée du 2 août 2002, ni de la décision-cadre 2008/977/JAI précitée et qu'il aurait dû être remplacé par un nouvel règlement grand-ducal obligatoire en exécution de l'article 17 paragraphe (1) lettre (a) de la loi modifiée du 2 août 2002, soit depuis plus de 14 ans. Dans ses rapports annuels, l'autorité de contrôle spécifique « Article 17 » a d'ailleurs régulièrement critiqué la prorogation annuelle du règlement Ingepol depuis l'adoption de la loi modifiée du 2 août 2002 ainsi que l'absence d'adoption d'un nouvel règlement grand-ducal.

1.2. Journalisation des accès et autres mesures de sécurité

Pour pouvoir sanctionner des abus et des accès non autorisés et pour faciliter les recours des personnes concernées, il est primordial que les opérations de transmissions de données puissent être retracées.

Le défaut de journalisation rendrait d'ailleurs difficile voire impossible le contrôle par les autorités de contrôle ou les autorités judiciaires tel que prévu notamment par l'article 30 paragraphe 5. de la décision 2008/615/JAI.

Des mesures garantissant la traçabilité des communications sont notamment prescrites par les articles 22 paragraphe 2. lettre f) de la décision-cadre 2008/977/JAI, 30 de la décision 2008/615/JAI et 29 paragraphe 2. lettre f) de la directive 2016/680.

Selon le commentaire des articles, l'article 3 paragraphe 3 régissant les demandes à formuler en vue d'une communication des données est censé garantir la traçabilité. Cependant, le projet de loi sous avis ne règlemente pas la durée de conservation des demandes de transmissions de

données, ni celles des transmissions elles-mêmes. Il est donc possible que, déjà peu de temps après une transmission, aucune trace de cette transmission des données ne subsiste.

Par ailleurs, en cas de communication électronique des données, aucune conservation de fichiers log n'est prévue, en dehors de l'hypothèse de transmissions se faisant par le biais de systèmes européens tels que Europol, SIS II etc.

A nouveau, étant donné que le règlement grand-ducal à prendre sur base de l'article 17 de la loi de 2002 fait défaut, rien n'est prévu en droit national de sorte que le présent projet de loi devra contenir des dispositions spécifiques à ce sujet.

La Commission nationale constate que, de manière plus générale, le projet de loi ne contient pas d'exigences particulières relatives à la sécurité et la confidentialité des données échangées. Or, vu le caractère extrêmement sensible des données en jeu, elle estime nécessaire de prévoir de telles mesures dans la loi.

En effet les articles 9 de la décision - cadre 2006/960/JAI et 29 paragraphe (1) de de la décision 2008/615/JAI exigent de telles mesures de sécurité du droit national. Or, le droit national fait défaut en l'absence de règlement grand-ducal pris sur la base de l'article 17 de la loi de 2002.

Par ailleurs, le texte ne précise rien sur les modalités et conditions des moyens de transmission des données (quelles communications peuvent ou doivent être effectuées par écrit, quelles communications peuvent être effectuées par fax, par e-mail etc.?) mais évoque, en son article 12, seulement tous les canaux de coopération policière auxquels participe le Luxembourg. Or de telles précisions seraient nécessaires pour déterminer les mesures de sécurité adaptées.

1.3. Voies de recours et droit d'être indemnisé

Les textes européens applicables exigent l'existence de recours devant l'autorité de contrôle compétente[1] et/ou[2] de recours juridictionnels[3].

La Commission nationale se demande quelles pourraient être les recours juridictionnels applicables aux communications de données régies par la loi projetée.

En ce qui concerne la possibilité de recours devant l'autorité de contrôle, on peut également se poser des questions sur la compétence de l'autorité de contrôle prévue à l'article 17 de la loi modifiée du 2 août 2002. Si la compétence de cette autorité est mentionnée dans le commentaire des articles, le texte du projet de loi ne l'évoque pas. La simple communication de données de la Police grand-ducale vers les autorités de police d'autres pays ou les échanges entre différentes unités de la Police grand-ducale ne semble pas poser problème. En revanche, si une transmission est - en vertu des articles 5 paragraphe (2) ou 20 paragraphe (2) - autorisée par le Procureur d'Etat ou le juge d'instruction en ce qui concerne les données provenant d'une enquête en cours, respectivement d'une instruction préparatoire en cours, les choses sont moins

[1] Cf notamment les articles 31 de la décision 2008/615/JAI, 25 paragraphe 3. de la décision-cadre 2008/977/JAI et 52 de la directive 2016/680

[2] Au regard de l'31 de la décision 2008/615/JAI, l'existence d'un des deux types de recours est suffisante, alors que directive 2016/680 exige les deux

[3] Cf notamment les articles 31 de la décision 2008/615/JAI, 25 paragraphe 3. de la décision-cadre 2008/977/JAI et 54 de la directive 2016/680

claires. La CNPD partage aussi les soucis du Parquet général[4] et de la Commission consultative des Droits de l'Homme[5] relatives à la compétence de l'autorité de contrôle pour les transmissions de données de la Police grand-ducale vers des administrations.

En ce qui concerne la portée du droit d'accès indirect prévu par l'article 17 précité, il faut mentionner que la personne concernée ne peut pas se voir confirmer - par l'autorité de contrôle - qu'une violation de ses droits a effectivement eu lieu. En effet, aux termes de l'article 17 de loi modifiée du 2 août 2002, l'autorité de contrôle « *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.*»

Ceci n'exclut pas, mais complique un éventuel recours en responsabilité de la victime qui veut être indemnisé. En effet, une personne hésitera à intenter une action en responsabilité si elle ne sait même pas si une violation de la loi a effectivement eu lieu ou non.

Mentionnons que le droit à une réparation est prévu par les articles 56 de la directive 2016/680, 31 de la décision 2008/615/JAI et 19 de la décision-cadre 2008/977/JAI.

1.4. Sanctions

La CNPD regrette que le projet de loi ne prévoie pas de sanctions pénales en cas de violations des règles édictées par le projet de loi.

Mentionnons qu'en vertu des articles 24 de la décision-cadre 2008/977/JAI et 57 de la directive 2016/680, les Etats membres de l'Union européenne sont tenus de prévoir des sanctions effectives afin d'assurer le respect des règles y énoncées.

Des sanctions pénales semblent d'autant plus nécessaires que la loi modifiée du 2 août 2002 (comprenant des sanctions pénales) – qui couvre également la matière policière – va disparaître prochainement sous sa forme actuelle en raison de la mise en conformité de la législation luxembourgeoise au 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 (Règlement général sur la protection des données), et abrogeant la directive 95/46/CE.

2. Echanges de données avec les institutions, organes et agences de l'Union européenne

En ce qui concerne plus particulièrement les échanges avec les institutions, organes et agences de l'Union européenne, il serait, dans un but de transparence, préférable que les institutions concernées soient nommément désignées en se référant aux textes européens respectifs.

3. Les transferts de données vers des pays tiers

3.1. Le champ d'application

[4] Avis du 28 avril 2016, page 5
[5] Avis du 7 juillet 2016, pages 5 et 7

L'article 1er du projet qui prévoit, en principe, la possibilité de la transmission de données à des pays tiers se réfère a priori au chapitre premier en son intégralité (et non seulement à la première section de ce chapitre).

Mais vu les dispositions de l'article 15, il semble clair que la consultation et la comparaison automatisées de profils ADN, la consultation automatisée de données dactyloscopiques et la consultation automatisée de données relatives à l'immatriculation des véhicules soient réservées aux échanges de données entre Etats-membres liés par la décision 2008/615/JAI.

En vertu de l'article 11 du projet de loi, la communication spontanée (sans demande) de données est réservée à la coopération avec les autorités policières des autres Etats membres de l'Union européenne et des pays associés à l'espace Schengen ainsi qu'avec les institutions, organes et agences de l'Union européenne.

Une approche plus restrictive en matière de transmissions spontanées vers des pays tiers est certainement de mise, surtout quand il ne s'agit pas de prévenir des infractions précises mais plutôt des « troubles à l'ordre public » (termes utilisés par l'article 11 du projet de loi)[6].

On peut cependant se demander s'il n'y a pas d'échange de données spontané avec des pays tiers dans l'hypothèse où la Police luxembourgeoise a connaissance d'infractions graves, par exemple de nature terroriste, qui sont sur le point de se produire sur le territoire d'un Etat tiers. Des informations de ce genre seraient-elles alors transmises en dehors de tout cadre légal ou y a-t-il d'autres textes légaux qui s'appliquent?

La CNPD estime qu'il serait préférable que le texte précise de manière plus explicite quels types d'échanges de données ne peuvent être effectués qu'entre pays membres de l'Union européenne et les pays associés à l'espace Schengen et quels types d'échanges peuvent être effectués également avec des pays tiers.

Le projet de loi ne précise pas de manière expresse s'il s'applique uniquement aux relations avec des Etats ayant conclu un accord ou traité bilatéral ou multilatéral réglant l'échange de données en matière policière. A défaut de précision, il faut admettre qu'un tel accord n'est pas requis.

Si la future loi s'applique en dehors d'accords avec les pays destinataires des données, il est d'autant plus important que les règles de la loi sont strictes et protectrices des droits des citoyens. En effet, une fois la transmission des données vers le pays tiers effectuée, celle-ci échappe au champ d'application de la décision - cadre 2006/960/JAI et de la décision 2008/615/JAI et d'autres textes de l'Union qui garantissent les droits des personnes concernées dans les pays recevant des données de la part des autorités luxembourgeoises.

3.2. Appréciation

Le fait pour les pays européens de mettre en place un échange de données facilité selon le principe de disponibilité témoigne d'une relation de confiance particulière entre les Etats-

[6] La transmission (spontanée ou sur demande) de données à caractère personnel en rapport avec des personnes présentant un danger pour l'ordre public est également prévue par l'article 14 de la décision 2008/615/JAI, mais uniquement dans le contexte particulier des manifestations de grande envergure à dimension transfrontalière. En revanche, l'article 7 de la décision - cadre 2006/960/JAI (que l'article 11 du projet de loi est censé transposer) n'impose une communication spontanée de données que dans le contexte d'«*infractions visées à l'article 2, paragraphe 2, de la décision - cadre 2002/584/JAI* » (mandat d'arrêt européen).

membres de l'Union européenne, pays qui ont tous un niveau de droits de l'homme et de protection des données élevé, les standards en matière de droits de l'homme et de protection des données étant sanctionnés notamment par la jurisprudence de la Cour de justice de l'Union européenne.

On peut donc s'étonner que le présent projet de loi assimile les Etat-tiers aux Etats membres de l'Union européenne sur bon nombre de points.

Certes, l'article 7 paragraphe (1) (tout comme l'article 20 paragraphe (2)) exclut la transmission des données « *s'il existe des éléments qui indiquent que les données à caractère personnel et informations demandées sont disproportionnées ou sans objet au regard des finalités pour lesquelles elles ont été demandées*».

Or, il se pose la question de savoir ce qui se passe si les données demandées ne sont pas disproportionnées en soi, mais que, vu l'absence de législation ayant un niveau adéquat de protection des données dans le pays tiers requérant, il y a un risque sérieux que le traitement qui en sera fait ne respectera pas les principes les plus élémentaires en matière de protection des données.

On peut aussi s'étonner du fait que, l'article 7 du projet de loi n'exclut pas expressément la transmission de données aux fins de la recherche ou de la poursuite d'infraction politiques. A titre d'exemple d'une telle disposition, on peut citer l'article 4 de la loi modifiée du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale qui exclut l'entraide « *si la demande d'entraide a trait à des infractions susceptibles d'être qualifiées par la loi luxembourgeoise soit d'infractions politiques, soit d'infractions connexes à des infractions politiques* ».

Dans ce contexte, il faudrait également que l'article 3 paragraphe (3) du projet de loi exige des autorités demanderesses de données d'indiquer l'infraction qui est à la base de la demande. Certes, le formulaire « Annexe B » joint au projet de loi et à la décision - cadre 2006/960/JAI comporte une rubrique à ce sujet, mais on peut supposer que ce formulaire ne sera utilisé qu'entre les pays membres de l'Union européenne et non dans les rapports avec les pays tiers.

La CNPD note aussi que l'article 3 paragraphe (3) du projet de loi n'exige pas de manière expresse une description des faits à la base de la demande. Or, une telle description est nécessaire pour pouvoir déceler si une infraction politique est « *déguisée* » en infraction de droit commun par l'autorité de l'Etat requérant. A titre d'exemple, on peut songer aux Etats qui accusent des opposants politiques de terrorisme.

3.3. L'utilisation à des fins autres

L'utilisation des données à des fins autres pour lesquelles elles ont été transmises se heurte au principe de finalités qui est un des principes de base de la protection des données. Et elle est d'autant plus problématique dans l'hypothèse d'une transmission des données aux autorités de pays n'ayant pas les mêmes standards en matière de protection des données ou de droits de l'homme que l'Union européenne.

Si la décision - cadre 2006/960/JAI et la décision 2008/615/JAI ne prohibent pas cette utilisation, elles l'encadrent néanmoins (dans les échanges de données entre pays membres de l'Union européenne).

Or, les pays non-membres de l'Union européenne n'étant pas lié par ces textes, il y a un danger qu'ils agissent comme bon leur semble sur cette question.

Par ailleurs, le formulaire « Annexe A » joint au projet de loi et à la décision - cadre 2006/960/JAI permet aux autorités de l'Etat communiquant les données d'exclure cette utilisation[7].

Or, on peut présumer que ce formulaire n'est pas utilisé dans les échanges de données entre le Luxembourg et des pays tiers. Et le texte du projet de loi lui-même n'exige pas des autorités luxembourgeoises de fournir des précisions à ce sujet en cas de transfert de données vers un pays tiers.

3.4. Transfert ultérieur dans un autre pays

Vu les risques inhérents aux transferts de données vers des pays tiers, il faudrait exclure que les données transmises par le Luxembourg à un pays tiers puissent être transmises par celui-ci à un autre Etat. Or, le texte sous avis ne prévoit rien à ce sujet. Il serait préférable que toute communication de données à un pays tiers contienne impérativement une mention excluant expressément une communication ultérieure à un autre Etat.

Il est à noter que pour la transmission (beaucoup moins sensible) de données du Luxembourg vers un autre pays membre de l'Union européenne, une telle communication ultérieure – même à l'intérieur de l'Union européenne – est encadrée légalement et nécessiterait le cas échéant l'accord des autorités luxembourgeoises ayant effectué la première transmission de données.[8]

3.5. Incidence de la directive 2016/680

La directive 2016/680 consacre, aux articles 35 à 40, des règles très précises relatives aux transferts de données vers des pays tiers.

Le CNPD comprend que la transposition de la directive 2016/680 en son intégralité est complexe et prendra du temps. Cependant, il conviendrait, dans la mesure du possible, en tenir compte dès à présent pour le présent projet de loi.

En particulier, en cas de transfert de données vers un pays n'ayant pas un niveau de protection des données adéquat, il serait indiqué d'exiger des garanties appropriées telles que prévues par l'article 37 de la directive qui permet un transfert vers un pays tiers si «
a) des garanties appropriées en ce qui concerne la protection des données à caractère personnel sont fournies dans un instrument juridiquement contraignant; ou

---

[7] Extrait du formulaire « Annexe A » :

Informations transmises en application de la décision-cadre : 2006/960JAI*: informations et renseignements fournis	
1.	L'utilisation des informations ou des renseignements fournis
❑	n'est autorisée qu'aux fins pour lesquelles ceux-ci ont été communiqués ou pour prévenir un danger immédiat et sérieux pour la sécurité publique;
❑	est également autorisée à d'autres fins, sous réserve des conditions suivantes (facultatif):.....;

[8] Voire notamment l'article 3 paragraphe 5. de la décision - cadre 2006/960/JAI et l'article 27 de la décision 2008/615/JAI

b) le responsable du traitement a évalué toutes les circonstances du transfert et estime qu'il existe des garanties appropriées au regard de la protection des données à caractère personnel. »

3.6. Conclusion

A ce stade, la CNPD se demande s'il ne faudrait pas exclure du projet de loi tout transfert de données vers un pays tiers à part ceux effectués en vertu d'accords bilatéraux ou multilatéraux.

4. Les échanges de données avec les agents des administrations ayant la qualité d'officier de police judiciaire.

Les échanges de données avec les agents des administrations ayant la qualité d'officier de police judiciaire peuvent être effectués dans les deux sens, c'est-à-dire de la Police grand-ducale à destination des agents des administrations ayant la qualité d'officier de police judiciaire et vice-versa.

Pour ce qui concerne les transmissions de données en direction des agents des administrations ayant la qualité d'officier de police judiciaire, l'article 18 paragraphe (1) donne une base égale à la transmission de données accessibles à la Police en vertu l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police, transmission des données qui s'avère parfois nécessaire à l'acquittement des missions des agents des administrations ayant la qualité d'officier de police judiciaire

En ce qui concerne la transmission de données dans le sens inverse, c'est-à-dire à destination de la Police grand-ducale, il est compréhensible que certaines données doivent parfois pouvoir être transmises des agents des administrations ayant la qualité d'officier de police judiciaire vers la Police grand-ducale, notamment en ce qui concerne les procès-verbaux constatant des infractions.

Le texte permet cependant l'échange de toutes données disponibles ou accessibles au sens de l'article 18 paragraphe (3). Cela signifierait concrètement que les officiers et agents de police judiciaire de la Police grand-ducale pourraient, le cas échéant, avoir accès aux bases de données et d'informations de dossiers des administrations dont relèvent les agents publics en question sans avoir recours à une perquisition et donc sans les garanties qui s'y attachent (décision d'un juge d'instruction sauf crime ou délit fragrant, voies de recours). Par ailleurs, selon l'article 22 du projet de loi, les données ainsi transmises pourraient être utilisées comme preuve.

Il serait préférable que le texte de loi, soit les lois régissant lesdites administrations délimitent, de manière très précise, les données pouvant être transmises des agents des administrations ayant la qualité d'officier de police judiciaire aux officiers et agents de police judiciaire de la Police grand-ducale.

La CNPD note aussi que le texte soumis pour avis ne clarifie pas si les agents publics ayant la qualité d'officier de police judiciaire sont tenus de donner suite à une demande de transmission de la part de la Police grand-ducale ou s'ils peuvent apprécier eux-mêmes l'utilité d'une telle transmission et le cas échéant la refuser.

En ce qui concerne les principes de proportionnalité et de finalité, il est renvoyé aux développements exposés ci-dessous dans la partie relative aux échanges des données avec les administrations.

5. Les échanges des données avec les administrations

5.1. Etendue des échanges de données

Par opposition aux échanges de données entre la Police et les officiers de police judiciaire des administrations - qui peuvent être effectués dans les deux sens - les échanges de données de la Police avec les administrations effectuées en vertu de l'article 18 paragraphe (2) ne peuvent se faire que dans un sens, à savoir en direction des administrations.

5.1.1. Les données auxquelles la Police grand-ducale a accès et provenant d'autres administrations

Les transmissions de données peuvent porter sur toutes données disponibles ou accessibles au sens de l'article 18 paragraphe (3). Cela inclut notamment les données issues des bases de données étatiques auxquelles la Police a accès en vertu de l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police.

La CNPD estime que la loi sur l'échange de données en matière policière ne devrait pas servir à permettre des échanges de données entre administrations par l'intermédiaire de la Police grand-ducale. En cas de nécessité, des dispositions déterminant en détail les fichiers d'administrations pouvant être accédés par d'autres administrations devraient être inscrites dans les lois régissant les administrations demanderesses de données. D'ailleurs, là où de telles dispositions existent déjà, le projet de loi en l'état actuel permettrait éventuellement de contourner ces dispositions légales.

A titre d'exemple, on peut mentionner 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 et l'article 2 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. Ces articles comportent une liste de bases de données étatiques et des catégories de données précises auxquelles le Ministère de l'Economie peut avoir accès notamment en vue de l'instruction des autorisations d'établissement. La liste ne comporte pas toutes les bases de données pouvant être accédées par la Police en vertu de l'article 34-1 de loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police. En cas d'adoption du texte sous avis, le Ministère en question pourra dès lors - par le biais de la loi projetée sur les échanges de données en matière policière et l'article 34-1 de la loi modifiée du 31 mai 1999 - obtenir de manière indirecte les données auxquelles il n'a pas accès directement en vertu de la loi du 2 septembre 2011 et du règlement grand-ducal du 28 avril 2015 précités.

La problématique est similaire pour les données issues du registre national des personnes physiques.

Certaines administrations disposent, pour l'exécution des ou d'une partie de leurs missions, d'un accès au registre en vertu d'une loi ou d'une autorisation accordée en vertu de l'article 7 de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques. Il se pose la question de savoir si, à l'avenir, des administrations ne disposant pas d'un tel accès ou celles dont l'accès est limité à seulement une partie des données du registre, pourront bénéficier – de manière indirecte - de l'accès le cas échéant plus large de la Police grand-

ducale, alors qu'en l'état actuel du droit, l'accès au registre national des personnes physiques doit être autorisé par le ministre ayant le Centre des technologies de l'information de l'Etat dans ses attributions

5.1.2. Les données d'origine policière ou judiciaire

Le projet de loi permet, en ses articles 18 et suivants, sous conditions, la transmission aux administrations par la Police de données disponibles ou accessibles. Ceci est justifié en particulier par la nécessité, pour une série d'administrations, de vérifier l'honorabilité de certaines personnes en amont ou en aval de décisions d'autorisations ou agréments.

Le commentaire des articles évoque notamment l'exemple d'« *une personne, titulaire d'un agrément pour gérer une crèche, serait poursuivie pour pédophilie tout en continuant à gérer la crèche pendant des mois voire des années, parce que l'administration étatique concernée n'a pas pu agir faute d'avoir été informée.* » Or, il faut aussi penser à l'hypothèse dans laquelle la personne poursuivie à tort est acquittée par la suite ou celle où l'affaire a fait l'objet d'un classement sans suite.

Ainsi une personne risquerait de subir une « condamnation administrative » sur base d'un rapport ou d'un procès-verbal avant que la justice n'ait pris une décision.

Le texte du projet de loi prévoit qu'en cas d'enquête ou instruction en cours, les données issues de l'enquête ou instruction ne peuvent être communiquées qu'avec l'accord du magistrat compétent. En revanche, si une affaire a par exemple déjà fait l'objet d'une ordonnance de renvoi, la transmission pourrait être décidée par un agent ou officier de police judiciaire seul.

La CNPD constate aussi que le texte ne contient aucune disposition sur la durée de conservation des données transmises aux administrations, ni de disposition relative à la mise à jour des données auprès de l'administration.

Ainsi, il y a un risque important que des données relatives à une personne dont l'affaire a été classée sans suite ou qui a entretemps été acquittée d'une infraction dont elle a été accusée à tort se trouvent toujours dans les dossiers de l'administration – sans une mise à jour ou rectification afférente.

5.1.3. Conclusion

Eu égard aux risques engendrée par la communication de données policières ou judiciaires aux administrations, la CNPD estime nécessaire que la loi prévoie de manière limitative les administrations pouvant recevoir communication de données de la part de la Police grand-ducale et les finalités ainsi que les conditions de ces communications de données.

En ce sens, elle ne peut que se rallier à l'avis du Conseil d'Etat du 15 novembre 2016 relatif au projet de loi sous examen qui estime « *qu'il y a lieu de compléter le projet sous examen par un cadre législatif précis destiné à entourer la communication de données et d'informations à des administrations tierces des garanties nécessaires à la protection de la vie privée telle que celle-ci est protégée par l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales.* »

On peut également citer l'avis du Conseil d'Etat sur le projet de loi n°6977 sur la nationalité luxembourgeoise qui, concernant l'article 104, paragraphe 2 dudit projet dit ce qui suit :
« *Or, étant donné qu'il s'agit d'une ingérence dans la vie privée des personnes, elle doit, en vertu de l'article 11(3) de la Constitution, être fixée par une loi. Une telle exception ne saurait dès lors être reléguée à un règlement grand-ducal, sauf à spécifier, en application de l'article 32(3) de la Constitution, dans la loi les fins, les conditions et les modalités suivant lesquels de tels règlements peuvent être pris.* »

5.2. La nécessité et la proportionnalité des transmissions

L'article 21 paragraphe (1) prévoit, en matière pénale, que les échanges de données se limitent aux éléments «*jugés pertinents et nécessaires pour assurer avec succès la prévention, la recherche ou la constatation d'une infraction pénale ou la manifestation de la vérité dans le cadre d'une enquête ou d'une instruction préparatoire*».

Par contre, pour ce qui est de la communication de données à des administrations, l'article 21 paragraphe (1) se borne à exiger que les données soient «*utiles à l'exécution des missions de service publics des administrations de l'Etat visées à l'article 18 paragraphe 2*»

La CNPD se demande pourquoi les auteurs du projet de loi font cette différence de formulation (*nécessité* d'un côté et *utilité* de l'autre) et si cette différence pourra donner lieu à des interprétations *a contrario* défavorables à la protection des données (de sorte qu'en matière de communication de données à des administrations, la transmission ne devrait pas forcément être *nécessaire.*)

En ce qui concerne le principe de proportionnalité, l'article 20 paragraphe (3) s'y réfère en excluant les échanges s'«*il existe des éléments qui indiquent que les données à caractère personnel et informations demandées sont disproportionnées (...) au regard des finalités pour lesquelles elles ont été demandées*». Cette disposition n'est cependant applicable qu'aux échanges de données provenant d'une enquête en cours ou d'une instruction préparatoire en cours, et non par exemple si une ordonnance de renvoi ou un jugement sur le fond est déjà intervenu, voire si les données ne proviennent pas du tout d'une enquête ou d'une instruction. En matière d'échanges internationaux par contre, cette condition est applicable à tout échange de données[9].

Là encore, la CNPD se demande si ces différences sont voulues et si elles pourront donner lieu à des interprétations a contrario imprévues.

5.3. Le principe de finalité et l'utilisation à des fins autres

La transmission de données policières vers des administrations est très délicate voire dangereuse est doit dès lors être limitée à des situations exceptionnelles et strictement limités.

Dès lors, aucune transmission de données de ce genre ne devrait avoir lieu sans détermination précise des raisons de cette transmission.

Or, au regard du texte de loi projeté, ni les demandes de transmission, ni la transmission (spontanée ou sur demande) elle-même ne doivent forcément contenir des informations relatives aux fins de la transmission. La CNPD estime que le texte devrait exiger que les demandes de transmissions de données et les transmissions de données elles-mêmes

[9] En vertu de l'article 5 paragraphe (3) renvoyant à l'article 20 paragraphe (3) et de article 7

contiennent de telles précisions, comme par exemple l'information que la transmission est demandée ou effectuée aux fins de l'instruction de la demande d'autorisation pour détention d'armes d'une personne nominativement désignée dans la demande de transmission de données et la transmission de données elle-même[10].

Par ailleurs, l'utilisation des données à des fins autres que celles pour lesquelles elles ont été transmises prévue à l'article article 21 paragraphe (2) comporte des risques additionnels et semble a priori difficilement justifiable.

Ainsi décidé à Esch-sur-Alzette en date du 17 novembre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen Présidente	Thierry Lallemang Membre effectif	François Thill Membre suppléant

[10] D'ailleurs, en matière d'échanges internationaux, au moins une indication sommaire des fins de la transmission de données est requise dans la demande en vertu de l'article 3 paragraphe (3).