CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2016

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2016

Missions

La Commission nationale pour la protection des données (CNPD) est une autorité indépendante instituée par la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Elle est chargée de veiller à l'application des lois qui protègent les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée et leurs données à caractère personnel.

Sa mission s'étend également à assurer le respect des dispositions de la loi modifiée du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques.

Superviser et assurer la transparence par :

- L'examen préalable des traitements soumis à autorisation ;
- La publicité réalisée au moyen du registre des traitements notifiés ;
- Les investigations suite à des plaintes ou de sa propre initiative ;
- L'intervention suite à des violations de données dans le secteur des communications électroniques.

Informer et guider avec :

- La sensibilisation du public aux risques potentiels ;
- Les renseignements concernant les droits des citoyens et les obligations des responsables des traitements de données ;
- L'explication des règles légales.

Conseiller et coopérer à travers :

- Les avis relatifs aux projets de loi et aux mesures réglementaires ou administratives concernant le traitement de données personnelles ;
- Les suggestions et recommandations adressées au gouvernement, notamment au sujet des conséquences de l'évolution des technologies ;
- L'approbation de codes de conduite sectoriels, la promotion des bonnes pratiques et la publication de lignes d'orientations thématiques.

Valeurs

La CNPD exerce avec **indépendance** les missions qui lui ont été attribuées. Elle détermine ses propres priorités dans les limites de son cadre légal. Elle choisit ses priorités notamment sur base de critères comme la gravité et l'envergure de la violation de la loi et l'étendue des individus affectés.

L'**expertise** est très importante pour la CNPD qui est dédiée à un travail de qualité. A cette fin, la CNPD s'efforce de travailler avec des équipes interdisciplinaires et elle investit dans le développement continu de ses employés pour améliorer leurs connaissances et leurs compétences.

La CNPD assure la **transparence** à l'égard de ses résultats et de ses choix, ce qui génère un support pour son travail et invite au dialogue. La CNPD est ouverte, honnête et visible. En interne, elle promeut une atmosphère positive et ouverte.

LA CNPD est fière d'œuvrer pour la protection d'un droit fondamental. Elle témoigne de son **engagement** dans son travail et son personnel et constitue un acteur à part entière de la société.

Table des matières

1 Avant-propos 12

2 Les activités en 2016 16

2.1 Supervision de l'application de la loi 18
- *2.1.1 Formalités préalables* 18
- *2.1.2 Transferts de données hors Union européenne* 21
- *2.1.3 Les chargés de la protection des données* 24
- *2.1.4 Demandes de vérification de licéité et plaintes* 25
- *2.1.5 Contrôles et investigations* 28
- *2.1.6 Secteur des communications électroniques* 29

2.2 Avis et recommandations 30
- *2.2.1 Lutte contre le terrorisme* 31
- *2.2.2 Administration transparente et réutilisation des informations du secteur public* 32
- *2.2.3 Service de Renseignement de l'Etat* 33
- *2.2.4 Accord Luxembourg/Etats-Unis pour l'échange d'informations de détection du terrorisme* 35
- *2.2.5 Traitement de données concernant les élèves et la jeunesse* 35
- *2.2.6 Laboratoire National de santé* 37
- *2.2.7 Archivage* 38
- *2.2.8 Echange de données à caractère personnel et d'informations en matière policière* 39
- *2.2.9 Abus de marché* 40
- *2.2.10 Revenu d'inclusion sociale* 41

2.3 Information du public 42
- *2.3.1 Actions de sensibilisation du public* 42
- *2.3.2 Reflets de l'activité de la Commission nationale dans la presse* 44
- *2.3.3 Outil de communication : le site Internet* 44
- *2.3.4 Formations et conférences* 45

2.4 Conseil et guidance 47
- *2.4.1 Concertation avec les organisations représentatives sectorielles, les principaux acteurs économiques, l'Etat et les organismes publics* 47
- *2.4.2 Demandes de renseignements* 48

2.5 Coopération avec les instituts de recherche luxembourgeois 48

2.6 Travail au niveau international 49
2.6.1 Le groupe « Article 29 » 50
2.6.2 Le « Groupe de Berlin » 53
2.6.3 Le groupe de travail international sur l'Education au numérique 55
2.6.4 Conférence de printemps des autorités européennes à la protection des données 56
2.6.5 Conférence internationale des commissaires de la protection des données 57

3 Les temps forts de 2016 **58**
3.1 Nouveau règlement général sur la protection des données 58
3.2 Transferts internationaux de données : conséquences de l'arrêt « Schrems » et adoption du « Privacy Shield » 62

4 Perspectives **66**

5 Ressources, structures et fonctionnement **70**
5.1 Rapport de gestion relatif aux comptes de l'exercice 2016 70
5.2 Personnel et services 74
5.3 Organigramme de la Commission nationale 75

6 La Commission nationale en chiffres **76**

7 Annexes
Avis et décisions
- Avis relatif au projet de loi n°6921 portant: 1) modification du Code d'instruction criminelle; modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; 3) adaptation de la procédure pénale face aux besoins liés à la menace terroriste (Délibération n°147/2016 du 12 février 2016) 78
- Avis relatif au projet de loi n°6810 concernant une administration transparente et ouverte et au projet de loi n°6811 modifiant la loi du 4 décembre 2007 concernant la réutilisation des informations du secteur public (Délibération n°196/2016 du 26 février 2016) 104
- Avis complémentaire à l'égard du projet de loi n°6593 portant modification de la loi du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'Etat et de diverses autres lois (Délibération n°252/2016 du 4 mars 2016) 118

Table des matières

- Avis à l'égard de l'avant-projet de loi portant organisation d'un registre électronique national des entreprises de transport par route (Délibération n°496/2016 du 23 mai 2016) 125

- Avis relatif au projet de loi n°6850 portant mise en place d'un statut spécifique pour certaines données traitées par le Service de Renseignement de l'Etat (Délibération n°566/2016 du 13 juin 2016) 133

- Avis relatif aux « Procédures de mise en œuvre du Protocole d'Accord conclu entre le Gouvernement du Grand-Duché de Luxembourg et les Etats-Unis d'Amérique pour l'échange d'informations de détection du terrorisme » (Délibération n°568/2016 du 20 juin 2016) 137

- Avis relatif au projet de loi n°6708 relative au contrôle de l'exportation, du transfert, du transit et de l'importation des biens de nature strictement civile, des produits liés à la défense et des biens à double usage ; au courtage et à l'assistance technique ; au transfert intangible de technologie ; à la mise en œuvre de résolutions du Conseil de sécurité des Nations unies et d'actes adoptés par l'Union européenne comportant des mesures restrictives en matière commerciale à l'encontre de certains Etats, régimes politiques, personnes, entités et groupes ainsi que sur le projet de règlement grand-ducal portant exécution de la présente loi relative au contrôle des exportations (Délibération n°611/2016 du 6 juillet 2016) 139

- Avis à l'égard du projet de règlement grand-ducal fixant les modalités d'application de la législation portant organisation des services de taxis (Délibération n°612/2016 du 6 juillet 2016) 143

- Avis relatif aux avant-projets de règlements grand-ducaux 1) précisant les données accessibles et les données communiquées en exécution des articles 4 et 6 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves, 2) pris en exécution de l'article 5 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves, et 3) fixant le modèle et les modalités de délivrance, d'utilisation et de retrait de la carte d'élève « myCard » (Délibération n°613/2016 du 6 juillet 2016) 145

- Avis relatif au projet de règlement grand-ducal pris en exécution de la future loi portant réorganisation du Service de Renseignement de l'Etat et au projet de règlement grand-ducal pris en exécution de la loi du 15 juin 2004 relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité
  (Délibération n°639/2016 du 13 juillet 2016) 150

- Avis complémentaire à l'égard du projet de loi n°6893 relative à la reconnaissance des qualifications professionnelles
  (Délibération n°660/2016 du 20 juillet 2016) 156

- Avis relatif au projet de loi portant modification 1) de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, 2) de la loi modifiée du 28 mai 2009 concernant le Centre de rétention et 3) de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales
  (Délibération n°683/2016 du 28 juillet 2016) 157

- Avis complémentaire relatif au projet de loi n°6921 portant :
  1) modification du Code d'instruction criminelle ;
  2) modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ;
  3) adaptation de la procédure pénale face aux besoins liés à la menace terroriste
  (Délibération n°803/2016 du 14 septembre 2016) 163

- Avis relatif au projet de loi n°7052 portant modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques
  (Délibération n°804/2016 du 14 septembre 2016) 164

- Avis relatif au projet de loi n°7064 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse et portant modification de la loi du 18 mars 2013 relative aux traitements des données à caractère personnel concernant les élèves
  (Délibération n°829/2016 du 14 octobre 2016) 165

- Avis à l'égard du projet de loi n°6977 sur la nationalité luxembourgeoise et portant abrogation de :
  1. la loi du 23 octobre 2008 sur la nationalité luxembourgeoise ;

Table des matières

2. la loi du 7 juin 1989 relative à la transposition des noms et prénoms des personnes qui acquièrent ou recouvrent la nationalité luxembourgeoise
(Délibération n°837/2016 du 14 octobre 2016) 169

- Deuxième avis complémentaire à l'égard du projet de loi n°6893 relative à la reconnaissance des qualifications professionnelles
(Délibération n°838/2016 du 14 octobre 2016) 173

- Avis relatif au projet de loi n°6913 sur l'archivage
(Délibération n°839/2016 du 14 octobre 2016) 174

- Avis relatif au projet de loi n°7049 portant modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.
(Délibération n°850/2016 du 14 octobre 2016) 192

- Avis relatif au projet de loi n°6995 portant modification de l'article 23 du Code d'instruction criminelle et de la loi du 7 août 2012 portant création de l'établissement public « Laboratoire national de santé »
(Délibération n°856/2016 du 14 octobre 2016) 195

- Avis relatif au projet de loi n°7079 portant modification de la loi modifiée du 4 septembre 1990 portant réforme de l'enseignement secondaire technique et de la formation professionnelle continue, d'autres dispositions légales, et au projet de règlement grand-ducal modifiant le règlement grand-ducal modifié du 9 janvier 2009 sur la jeunesse
(Délibération n° 864/2016 du 28 octobre 2016) 203

- Avis 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) 206

- Avis relatif aux projets de loi n° 7054 et 7055 (Paquet législatif « Klimabank an nohalteg Wunnen »)
  (Délibération n°980/2016 du 25 novembre 2016) 218

- Avis relatif au projet de loi n°7020 portant mise en œuvre de la réforme fiscale
  (Délibération n°981/2016 du 25 novembre 2016) 223

- Avis à l'égard de l'avant-projet de loi modifiant la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés, et d'autres dispositions légales
  (Délibération n°983/2016 du 25 novembre 2016) 227

- Avis relatif au projet de loi n°7022 relative aux abus de marché et portant : 1. mise en œuvre du règlement (UE) n°596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission ; 2. transposition de: a) la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché (directive relative aux abus de marché) ; b) la directive d'exécution (UE) 2015/2392 de la Commission du 17 décembre 2015 relative au règlement (UE) n°596/2014 du Parlement européen et du Conseil en ce qui concerne le signalement aux autorités compétentes des violations potentielles ou réelles dudit règlement ; 3. modification de la loi modifiée du 11 janvier 2008 relative aux obligations de transparence des émetteurs ; et 4. abrogation de la loi modifiée du 9 mai 2006 relative aux abus de marché
  (Délibération n°1003/2016 du 2 décembre 2016) 229

- Avis relatif au projet de loi n°7061 modifiant certaines dispositions du Code de la sécurité sociale
  (Délibération n°1005/2016 du 2 décembre 2016) 243

- Avis à l'égard du projet de règlement grand-ducal concernant les subsides accordés aux clubs sportifs affiliés auprès d'une fédération sportive agréée
  (Délibération n°1027/2016 du 22 décembre 2016) 249

Table des matières

- Avis à l'égard du projet de règlement grand-ducal concernant le contrôle médico-sportif obligatoire des membres licenciés actifs des fédérations sportives agréées
(Délibération n°1028/2016 du 22 décembre 2016) 251

- Avis à l'égard de l'avant-projet de loi relatif au revenu d'inclusion sociale
(Délibération n°1029/2016 du 22 décembre 2016) 255

Participations aux travaux internationaux

- Documents adoptés par le groupe de travail européen « Article 29 » en 2016 261

HD
31
4G

1 Avant-propos

Le collège :
Thierry Lallemang, Tine A. Larsen, Christophe Buschmann

Après 4 années de débats et plus de 4000 amendements, le règlement général sur la protection des données (RGPD) a été adopté définitivement par le Parlement européen le 14 avril 2016. Avec ses 99 articles et 200 considérants, le texte marque un tournant pour la protection des données.

Les dispositions du nouveau règlement, dont l'objectif est de redonner aux citoyens le contrôle de leurs données personnelles tout en responsabilisant davantage les entreprises et administrations, seront directement applicables dans l'ensemble des Etats membres de l'Union européenne à compter du 25 mai 2018.

Durant la phase de transition vers ce nouveau cadre législatif, une des priorités de la CNPD est de sensibiliser les citoyens,

responsables du traitement et sous-traitants sur les principaux changements auxquels ils doivent se préparer.

À cet effet, la CNPD et le Service des médias et des communications (SMC) ont organisé le 11 octobre 2016 une conférence dans la Maison du Savoir à Esch/Belval. Devant une audience de plus de 500 personnes, le Premier ministre et ministre des Communications et des Médias, Xavier Bettel, a tenu un discours sur les défis et opportunités du nouveau règlement européen pour le Luxembourg.

Cette conférence a marqué le début d'une série d'événements spécialement conçus ensemble avec l'initiative « Digital Lëtzebuerg » pour présenter le nouveau règlement aux différents acteurs concernés et les guider dans son implémentation. Du 14 jusqu'au 18 novembre 2016, des séances d'information spécialisées sur l'impact du RGPD dans certains secteurs clés de l'économie luxembourgeoise ont été organisées. Des orateurs spécialisés dans les domaines des finances, de la santé, des technologies de l'information et des start-ups ont répondu tout au long de cette semaine aux questions des responsables de traitements et sous-traitants.

Parmi les faits marquants de l'année 2016, il faut également évoquer la conclusion de l'accord « Privacy Shield » en juillet entre les Etats-Unis et la Commission Européenne. Cet accord sur les flux transatlantiques de données personnelles entend répondre aux faiblesses des précédents accords dits « Safe Harbor », négociés en 2001 et invalidés par la Cour de justice de l'Union européenne en octobre 2015 (arrêt dans l'affaire C-362/14 - Maximillian Schrems/Data Protection Commissioner).

À côté de l'adoption de ces deux textes majeurs en matière de protection des données, la CNPD a eu en 2016 une année particulièrement chargée.

Le régulateur luxembourgeois a contribué davantage au processus législatif que les années précédentes en avisant 30 projets de loi ou mesures réglementaires dont la thématique touchait à la protection des données, soit 17 plus que l'année passée. A titre d'exemple peuvent être cités les avis concernant la lutte contre le terrorisme, l'administration transparente et la réutilisation des informations du secteur public, le statut spécifique des données traitées par le Service de Renseignement de l'Etat, le traitement de données concernant les élèves, l'échange de données en matière policière, l'archivage ou encore le revenu d'inclusion sociale.

Le travail consultatif de la CNPD ne se limitait toutefois pas à ces avis. La Commission nationale a également donné des recommandations aux entreprises, administrations ou associations qui la contactaient pour vérifier si leurs traitements de données étaient conformes à la loi. À ce titre, la Commission nationale a participé à 198 réunions et répondu à 430 demandes de renseignement par écrit.

Au-delà du simple renseignement, la CNPD est également de plus en plus sollicitée dans le cadre des déclarations préalables des traitements de données. En 2016, elle a reçu 1.003 notifications (+39% par rapport à 2015) et 1449 demandes d'autorisation (+30% par rapport à 2015).

Avec le nouveau règlement européen, les contraintes déclaratives seront nettement réduites. Le corollaire de cet allègement drastique est une forte responsabilisation des entreprises tout en leur offrant une plus grande liberté dans la conception de leur politique de gestion des données personnelles. À tout moment,

elles devront être capables de démontrer la pertinence et l'adéquation des mesures techniques et organisationnelles mises en œuvre pour garantir le respect des nouvelles obligations introduites par le règlement, comme la protection des données dès la conception et la protection des données par défaut.

D'année en année, les plaintes se maintiennent à un niveau similaire. En 2016, 185 personnes ont fait appel aux services de la CNPD lorsqu'elles ont estimé qu'il y a eu une violation de la loi ou une entrave à l'exercice de leurs droits. Ceci est dû au fait que la CNPD reçoit de plus en plus de plaintes transfrontalières, étant donné que le Luxembourg abrite de nombreux sièges d'entreprises multinationales qui traitent les données de tous les clients européens au Grand-Duché. Dès l'entrée en vigueur de la réforme, cette tendance risque de s'accroître en raison de la facilité pour le citoyen européen d'adresser une plainte contre ce type d'entreprise auprès de son autorité nationale qui transmettra cette plainte à la CNPD.

77 plaintes ont conduit à des contrôles et investigations pour suspicion de violation des dispositions légales en matière de protection des données. Il s'agissait entre autres d'entreprises qui surveillaient leurs employés de manière illégale, de demandes d'accès, de rectification ou d'effacement non respectées ou encore de communications de données illégales à des tiers.

Le nouveau règlement européen renforce le rôle de supervision de la CNPD et privilégie le contrôle a posteriori plutôt qu'a priori. Il permet aussi à l'autorité luxembourgeoise d'infliger des amendes qui se doivent d'être effectives, proportionnées et dissuasives. Amenée à être moins administrative, la tâche de la CNPD sera davantage proactive et sur le terrain.

Esch-sur-Alzette, le 19 juin 2017

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Le siège de la CNPD à Belval

2

Les activités en 2016

L'année 2016 en un coup d'œil

Janvier

19 - La CNPD participe au colloque « La genèse et les conséquences de l'arrêt Schrems »
26 - La CNPD organise, ensemble avec l'Université du Luxembourg, un panel à la conférence internationale Computers, Privacy and Data Protection à Bruxelles
28 - Journée de la protection des données
28 - La CNPD, en collaboration avec l'APDL et Security made in Lëtzebuerg, organise une conférence sur le métier de chargé de la protection des données
28 - La CNPD et l'APDL présentent la fiche du chargé de la protection des données

Février

18 - La CNPD participe au workshop « EU law for the financial sector: the rules on data security and data protection »
12 - La CNPD avise le projet de loi n°6921 relatif à la lutte contre le terrorisme
23 - La CNPD donne une présentation à la conférence « Protection des données et vie privée : défis, enjeux et limites à la lumière des évolutions récentes » de CREO
26 - La CNPD émet un avis relatif au projet de loi n°6810 concernant une administration transparente et ouverte et au projet de loi n°6811 concernant la réutilisation des informations du secteur public

Mars

8-9 - La CNPD intervient lors de la conférence de printemps de l'ALFI sur le thème du Safe Harbour

Avril

21 - La CNPD intervient à l'Advanced Data Collection and Risks Industry Workshop
26 - La CNPD intervient lors du petit-déjeuner HR One sur la thématique de la surveillance des employés au travail

Mai

4 - Le règlement général sur la protection des données est publié dans le Journal officiel de l'Union européenne
13 - La CNPD participe au Information Security Education Day (ISED) sur le thème du Big Data
26-27 - La CNPD participe à la Conférence européenne des autorités de protection des données à Budapest

Juin

13 - La CNPD avise le projet n°6850 portant mise en place d'un statut spécifique pour certaines données traitées par le SRE
18-19 - La CNPD donne des cours de formation à L'Institut National d'Administration Publique (INAP)
20 - La CNPD donne son avis relatif aux « Procédures de mise en œuvre du Protocole d'Accord conclu entre le Gouvernement du Grand-Duché de Luxembourg et les Etats-Unis d'Amérique pour l'échange d'informations de détection du terrorisme »

DELIBERATIONS

1.060
Délibérations adoptées
(+29% par rapport à 2015)

30
Avis relatifs à des projets ou propositions de loi ou mesures réglementaires
(+130% par rapport à 2015)

33
Demandes d'agréments pour les chargés de la protection des données

FORMALITES PREALABLES

1.003
Notifications reçues
(+39% par rapport à 2015)

1.449
Demandes d'autorisations
(+30% par rapport à 2015)

8.005
Déclarants (depuis 2002)

GUIDANCE

198
Réunions

430
Demandes de renseignement par écrit
(+27% par rapport à 2015)

PLAINTES ET INVESTIGATIONS

185
Plaintes

77
Investigations

VIOLATIONS DE DONNEES (COMMUNICATIONS ELECTRONIQUES)

1
Notification

Juillet

6 - La CNPD avise les avant-projets de règlements grand-ducaux relative aux traitements des données concernant les élèves et la carte d'élève « myCard »
12 - La Commission européenne adopte le « Privacy Shield »

Septembre

6 - La CNPD participe au séminaire de l'European Data Protection Law Review à Cologne sur le nouveau règlement en matière de protection des données et le Privacy Shield
30 - La CNPD participe au séminaire de l'Union Internationale des Avocats (UIA) à la Cour de Justice de l'UE sur le thème de la protection des données personnelles dans les services financiers (FinTech), d'assurance et médicaux

Octobre

11 - La CNPD et le Service des médias et des communications (SMC) organisent une conférence sur les principaux changements du nouveau règlement général sur la protection des données
14 - La CNPD avise le projet de loi n°6995 portant création du Laboratoire National de Santé
14 - La CNPD se prononce sur le projet de loi n°6913 concernant l'archivage
14 - La CNPD avise le projet de loi n°7049 portant modification de la loi du 2 août 2002 relative à la protection des données
17-20 - La CNPD participe à la 38ème Conférence internationale des commissaires de la protection des données et de la vie privée à Marrakech

Novembre

14-18 - La CNPD et le Service des médias et des communications (SMC) organisent des séances d'information spécialisées sur l'impact du nouveau règlement général sur la protection des données dans certains secteurs clés de l'économie luxembourgeoise
17 - La CNPD émet un avis sur le projet de loi n°6976 relatif à l'échange de données à caractère personnel et d'informations en matière policière
22 - La CNPD participe à une table ronde lors des Luxembourg Internet Days sur l'Internet des Objets

Décembre

2 - La CNPD avise le projet de loi n°7022 relatif aux abus de marché

2 Les activités en 2016

Le registre public

La loi prévoit la tenue d'un registre public des traitements auprès de la CNPD (http://www.cnpd.public.lu/fr/registre). Ce registre permet aux citoyens de vérifier si un responsable (entreprise, administration, etc.) a déclaré ses traitements et s'il est susceptible de détenir des informations les concernant.

Figurent dans ce registre :
- les traitements notifiés à la CNPD,
- les traitements autorisés par la CNPD et
- les traitements surveillés par les chargés de la protection des données (figurant sur leurs registres transmis à la CNPD).

Ne figurent pas dans le registre public :
- les traitements de données exemptés de déclaration et
- les traitements qui n'ont pas été autorisés.

Le travail de la Commission nationale pendant l'année 2016 était axé sur les activités suivantes :

- Le traitement des notifications et des autorisations préalables ;
- L'analyse des plaintes et demandes de vérification de licéité ;
- Les contrôles et investigations ;
- Les avis concernant les projets de loi et mesures réglementaires ;
- L'information et la sensibilisation du public ;
- Le conseil et la guidance des acteurs publics et privés ;
- Les activités internationales et en particulier la participation aux travaux sur le plan européen.

2.1 Supervision de l'application de la loi

2.1.1 Formalités préalables

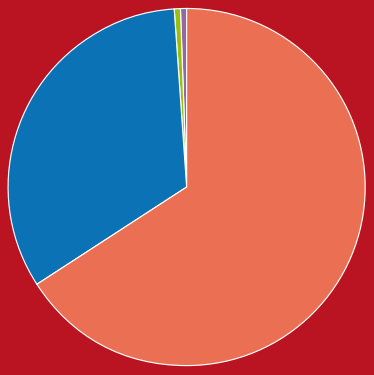
Le législateur luxembourgeois prévoit que tout traitement de données à caractère personnel doit en principe être notifié à la Commission nationale. Les traitements les plus courants sont exempts de déclaration, tandis que certains traitements plus « sensibles » requièrent une autorisation préalable de la CNPD.

Le nombre total des traitements de données déclarés depuis 2003 s'élève à 26.614. En tout,

Quels sont les traitements soumis à autorisation ?

- Surveillance et surveillance sur le lieu de travail
- Traitement de données biométriques (contrôle de l'identité de personnes)
- Traitement de données génétiques (dans certains cas)
- Interconnexion de données
- Utilisation ultérieure de données pour d'autres objectifs (p.ex. statistiques)
- Traitements relatifs au crédit et à la solvabilité de personnes
- Cas spécifiques : transfert de données vers un pays hors UE ne présentant pas un niveau de protection adéquat

Statistiques demandes d'autorisation 2016



8.005 déclarants/responsables se sont ainsi conformés aux devoirs de déclaration imposés par la loi depuis 2002.

Avec le nouveau règlement européen sur la protection des données qui entrera en vigueur en mai 2018, certaines démarches administratives seront simplifiées. Les obligations de déclaration pour les organismes qui traitent des données à caractère personnel seront notamment supprimées.

2.1.1.1 Les notifications préalables

Les traitements de données à caractère personnel non exemptés de déclaration et non soumis à autorisation préalable doivent faire l'objet d'une notification préalable.

Au total, la CNPD a reçu 1.003 notifications préalables en 2016, ce qui constitue une augmentation de 39% par rapport à l'année précédente. Il existe deux types de notifications : les notifications ordinaires et les engagements formels de conformité.

Notifications ordinaires

En 2016, la CNPD a reçu 975 notifications ordinaires. La finalité invoquée le plus souvent était l'administration du personnel. D'autres raisons citées pour traiter des données personnelles dans le cadre de notifications étaient : la gestion de la clientèle, la comptabilité, la gestion des fournisseurs ou encore la recherche scientifique.

Engagements formels de conformité

La loi prévoit, à côté des notifications ordinaires, une forme simplifiée de notification (« notification unique »). Cette notification unique se limite aux traitements déterminés par la Commission nationale par le biais de « décisions uniques ». Lorsque les traitements en question correspondent en tous

Les activités en 2016

points aux conditions fixées dans les décisions uniques afférentes, le responsable du traitement adresse à la Commission nationale un engagement formel par lequel il déclare que le traitement est conforme à la description figurant dans la décision unique.

Par sa décision n°108/2007 du 14 septembre 2007, la Commission nationale a défini les modalités des traitements de données que les employeurs (chefs d'entreprise, chefs d'établissement ou leurs délégués) sont amenés à opérer dans le cadre de l'organisation et du déroulement des élections des délégués du personnel, des délégations des jeunes travailleurs et des représentants du personnel dans les comités mixtes d'entreprise et les conseils d'administration des sociétés anonymes. La CNPD a reçu 28 engagements formels de conformité en 2016.

2.1.1.2 Les autorisations préalables

Les traitements présentant un risque particulier au regard de la vie privée des personnes

concernées ne sont possibles que moyennant une autorisation de la Commission nationale. Ces dossiers nécessitent toujours une analyse détaillée et une appréciation circonstanciée et pondérée au cas par cas.

Au total, la CNPD a reçu 1.449 demandes (demandes d'autorisation et engagements formels de conformité) en 2016. Ce chiffre constitue une augmentation de 30% par rapport à l'année précédente.

Demandes d'autorisation

Le nombre des demandes d'autorisation reçu par la CNPD est en augmentation constante depuis 2011 : 1338 demandes lui ont été soumises en 2016 (contre 969 en 2015). Ce chiffre représente le nombre annuel le plus élevé de demandes que la CNPD a reçu depuis sa création.

La grande majorité des demandes en 2016 étaient relatives à la surveillance sur le lieu du travail (66%). 50% concernaient l'exploitation de caméras de surveillance et 7% le contrôle des déplacements de véhicules et de personnes grâce à la géolocalisation Le nombre de requêtes en matière de vidéosurveillance, de géolocalisation et d'enregistrement des conversations téléphoniques ont augmenté tandis que celle concernant la surveillance des outils informatiques ont diminué.

Engagements formels de conformité

En plus des demandes d'autorisation, la Commission nationale a reçu 111 engagements formels de conformité en 2016. La loi prévoit une procédure allégée d'autorisation (« autorisation unique ») pour certains traitements déterminés par la Commission nationale. Il s'agit actuellement de la surveillance électronique des horaires et des accès. Pour pouvoir bénéficier d'une telle autorisation, le responsable du traitement doit adresser un engagement formel par lequel il déclare que le traitement est conforme à la description figurant dans la décision unique de la Commission nationale.

2.1.2 Transferts de données hors Union européenne

En principe, il est interdit de transférer des données à caractère personnel vers des pays en dehors de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande). Les pays de l'EEE ont transposé les dispositions de la directive 95/46/CE sur la protection des données dans leur législation nationale et assurent un niveau de protection suffisant.

Cette interdiction ne concerne pas les transferts vers les pays reconnus comme « adéquats » par la Commission européenne. C'est le cas de d'Andorre, de l'Argentine, du Canada, des Iles Féroé, de l'Ile de Man, de Guernesey, de Jersey, de la Nouvelle Zélande, d'Israël, de l'Uruguay, de la Suisse, et dans certains cas seulement, des Etats-Unis d'Amérique (voir ci-dessous la section « EU-U.S. Privacy Shield Framework »).

Le responsable du traitement transmettant des données vers un pays tiers doit offrir des garanties suffisantes au regard de l'utilisation qui sera faite des données par le destinataire, ainsi qu'au regard de l'exercice des droits des personnes concernées.

La loi prévoit des exceptions à ce principe d'interdiction. D'autres moyens existent pour permettre aux responsables du traitement

Les activités en 2016

d'apporter un niveau de protection suffisant pour transférer des données vers des pays tiers.

Les dérogations légales

L'article 19 (1) de la loi modifiée du 2 août 2002 et la directive 95/46/CE prévoient des exceptions au principe d'interdiction de transferts (consentement de la personne concernée, nécessité pour l'exécution d'un contrat conclu dans l'intérêt de la personne concernée, intérêt public important…). Ces dérogations légales ne s'appliquent toutefois que pour des transferts de données qui ne peuvent être qualifiés de répétés, massifs ou structurels.

D'autres exceptions sont plus courantes : les clauses contractuelles types et les règles d'entreprise contraignantes (BCR - Binding Corporate Rules) pour les multinationales.

Les clauses contractuelles types

Il s'agit des accords conventionnels passés entre les exportateurs et destinataires des données ou d'autres mesures de protection qui constituent des garanties suffisantes pour encadrer les transferts de données personnelles. Aux termes de l'article 19 (3) de la loi modifiée du 2 août 2002, il appartient à la Commission nationale de vérifier si les sauvegardes et garanties

sont suffisantes, ces dernières pouvant résulter notamment de l'application des clauses contractuelles types approuvées par la Commission européenne.

Les règles d'entreprise contraignantes

Les règles d'entreprise contraignantes (« Binding Corporate Rules ») constituent un outil susceptible d'assurer une protection adéquate des données à caractère personnel lorsque celles-ci sont transférées ou traitées en dehors de l'Union européenne.

Elles représentent une alternative juridique intéressante pour les groupes de sociétés qui se voient amenés à transférer régulièrement des données à caractère personnel de leurs sociétés établies sur le territoire de l'UE vers d'autres entités du groupe situées dans des pays tiers. Les entreprises peuvent adopter ces règles de leur propre initiative et les appliquer aux transferts de données entre les sociétés qui font partie d'un même groupe.

Les « BCR » présentent de nombreux avantages pour un groupe d'entreprises multinationales :

- Conformité avec la directive 95/46/CE ;
- Limitation des obligations administratives pour chaque transfert ;
- Uniformisation des pratiques relatives à la protection des données au sein d'un groupe ;
- Guide interne en matière de protection des données personnelles ;
- Moyen plus flexible et adapté à la culture d'entreprise ;
- Possibilité de placer la protection des données au rang de « préoccupation éthique du groupe ».

Au cours des dernières années, la CNPD a gagné de l'expérience dans ce domaine en prenant le rôle de chef de file dans l'examen des chartes « BCR » du groupe eBay en 2009 et du groupe ArcelorMittal en 2013.

En 2016, la CNPD a pousuivi l'analyse des chartes BCR de trois entreprises multinationales. Elle a par ailleurs examiné et approuvé les règles d'entreprise contraignantes de deux groupes multinationaux lui soumises par d'autres autorités de protection des données européennes.

Le « EU-U.S. Privacy Shield Framework »[1]

Aux Etats-Unis, seules les entreprises qui ont volontairement adhérés au « EU-U.S. Privacy Shield Framework » peuvent librement recevoir des données provenant de l'Union européenne. Les entreprises établies dans l'UE peuvent transférer les données personnelles qu'elles traitent à destination des sociétés américaines figurant sur la liste « EU-U.S. Privacy Shield Framework », de la même manière que s'opèrent les transferts vers les pays reconnus comme « adéquats » par la Commission européenne. A travers un mécanisme de « self certification », les entreprises américaines qui le désirent peuvent s'inscrire sur un registre tenu par le Département du Commerce américain. Au-delà de cette obligation formelle, ces entreprises devront respecter les obligations et les garanties de fond prévues par le « Privacy Shield ».

Ces principes, négociés entre les autorités américaines et la Commission européenne en juillet 2016, sont basés sur ceux de la directive européenne 95/46/CE sur la protection des données. Ils entendent par ailleurs répondre aux faiblesses des précédents accords dits « Safe Harbor », négociés en 2001 et invalidés par la Cour de justice de l'Union européenne en octobre 2015.

En novembre 2015, la CNPD avait informé les entreprises luxembourgeoises que les transferts de données personnelles vers les Etats-Unis d'Amérique n'étaient plus possibles sur base de la décision « Safe Harbor » et évoquaient les autres outils juridiques qui permettaient toujours de transférer

[1] Voir partie 3.2 pour plus d'informations à ce sujet.

des données vers les Etats-Unis d'Amérique, pour le cas où ces entreprises désireraient poursuivre de tels transferts. Suite à cette information, la CNPD a reçu un nombre important de demandes d'autorisation en vue du transfert de données vers des pays tiers.

Formalités

Si une entreprise veut transférer des données personnelles du Luxembourg vers un destinataire n'assurant pas un niveau de protection suffisant, elle devra, selon les cas :

- soit demander une autorisation préalable à la CNPD si elle base ses transferts sur les clauses contractuelles types de la Commission européenne, de clauses contractuelles « ad hoc », ou de règles contraignantes d'entreprises (BCR) préalablement validées au niveau européen ;

- soit introduire une notification préalable auprès de la CNPD (ou une modification de notification en cas de notification préexistante) si les transferts sont basés sur l'une des dérogations de l'article 19 paragraphe (1) de la loi, ou si les données sont transférées vers une société ayant adhéré au « EU-U.S. Privacy Shield Framework ». Cependant, si la collecte des données ou le premier traitement des données opéré par le responsable du traitement au Luxembourg est soumis à l'autorisation préalable de la CNPD, le transfert fera également l'objet de cette autorisation. De même, si le traitement initial est exempté du devoir de déclaration, aucune formalité préalable ne sera nécessaire, sauf exception prévue dans la loi (voir la liste des traitements exemptés du devoir de déclaration).

Au total, la CNPD a été saisie de 438 demandes de transfert en 2016. Ce chiffre a presque triplé par rapport à l'année précédente. La majorité des demandes émanaient d'entreprises du secteur financier. Le pays de destination était le plus souvent les Etats-Unis.

De plus en plus d'entreprises collaborent avec des partenaires commerciaux et offrent leurs produits et services sur des marchés hors d'Europe. Le développement des échanges commerciaux et la mondialisation ont entraîné un accroissement des transferts de données à caractère personnel dans le cadre de projets de centralisation et d'« outsourcing » de la gestion du personnel, de la clientèle ou des fournisseurs, ainsi que dans le contexte de l'externalisation de leurs activités informatiques.

2.1.3 Les chargés de la protection des données

Tout responsable du traitement dispose de la faculté de désigner

Fiche du chargé de la protection des données

En 2016, la CNPD et l'APDL (Association pour la Protection des Données au Luxembourg) ont présenté leur fiche sur le chargé de la protection des données personnelles (ou « data protection officer ») à l'occasion de la journée de la protection des données.

Cette fiche a pour objectif d'apporter des précisions sur le rôle et la fonction de la personne en charge d'assurer le respect de la protection des données personnelles au sein d'une organisation.

La fiche se base tant sur la législation luxembourgeoise en place (loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel) que sur les retours d'expérience des professionnels concernés (DPO, Juristes…).

APDL

CNPD

CHARGÉ DE LA PROTECTION DES DONNÉES PERSONNELLES

Fonction

Conditions d'exercice/organisation

un chargé de la protection des données. Avant la modification de la loi en 2007, il n'était pas possible de désigner une personne salariée de l'organisme responsable du traitement. Il fallait par conséquent recourir à un chargé externe inscrit sur la liste des personnes agréées par la CNPD afin d'exercer cette fonction. Depuis 2007, sur suggestion de la CNPD, les salariés peuvent également être désignés comme chargés, à condition que ces derniers bénéficient d'une certaine indépendance vis-à-vis des responsables du traitement qui les ont désignés et qu'ils disposent du temps approprié pour pouvoir s'acquitter de leurs missions.

Les responsables ayant désigné un chargé de la protection des données sont exemptés du devoir de notification des traitements qu'ils mettent en œuvre. Ces derniers doivent cependant figurer dans le registre des traitements que le chargé doit établir, tenir à jour de façon permanente et transmettre tous les quatre mois à la CNPD.

Le chargé doit surveiller le respect des dispositions de la loi et des règlements d'exécution. A cet effet, il dispose d'un pouvoir d'investigation et d'un droit d'information auprès du responsable de traitement et, corrélativement, d'un droit d'informer le responsable de traitement des formalités à accomplir afin de se conformer aux dispositions légales et réglementaires en la matière. Le chargé doit en outre consulter la Commission nationale en cas de doute quant à la conformité à la loi des traitements mis en œuvre sous sa surveillance.

Avec la désignation d'un chargé, l'expertise de la protection des données fait son entrée dans les entreprises et autres organismes. Le nouveau règlement européen, qui entrera en vigueur en 2018, prévoit que les autorités publiques et les entreprises qui effectuent certains traitements de données à risques doivent désigner un délégué à la protection des données.

Au total, 122 entreprises, associations et organismes publics ont désigné un chargé de la protection des données. À la fin de l'année 2016, 135 personnes physiques ou morales étaient agréées pour exercer l'activité de chargé de la protection des données.

2.1.4 Demandes de vérification de licéité et plaintes

En 2016, 185 personnes ont fait appel aux services de la CNPD lorsqu'elles ont estimé qu'il y a eu une violation de la loi ou

une entrave à l'exercice de leurs droits. Le nombre de plaintes que la CNPD reçoit chaque année se maintient à un niveau similaire depuis 2013.

58% des plaintes provenaient de citoyens d'autres États membres de l'UE. Cela résulte de la présence de nombreuses sociétés multinationales ayant choisi d'établir leur siège européen au Luxembourg. Pour ces acteurs, la CNPD est l'autorité compétente pour assurer le respect de la législation nationale en matière de protection des données.

Environ 53% des plaintes visaient des entreprises offrant des services sur Internet.

Motifs des plaintes

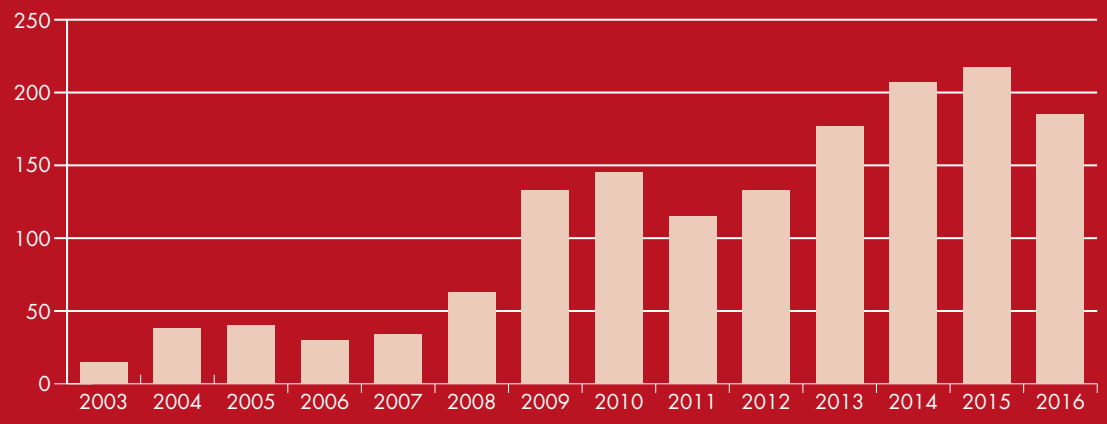
Dans 24% des cas, les plaignants ont demandé à la CNPD de vérifier la licéité de certaines pratiques administratives ou commerciales. Ils ont notamment remis en cause :

- les conditions générales de commerces ou de services en ligne ;
- la durée de conservation des données collectées (p.ex. : historique d'achat) ;
- l'ouverture automatique d'un compte à leur nom ;
- la demande de documents comme la carte d'identité ou la facture d'électricité/de gaz à des fins de vérification d'identité ;
- la collecte excessive de données pour pouvoir participer à des concours ou lors du recrutement de nouveaux employés ;
- la publication des données à caractère personnel en ligne.

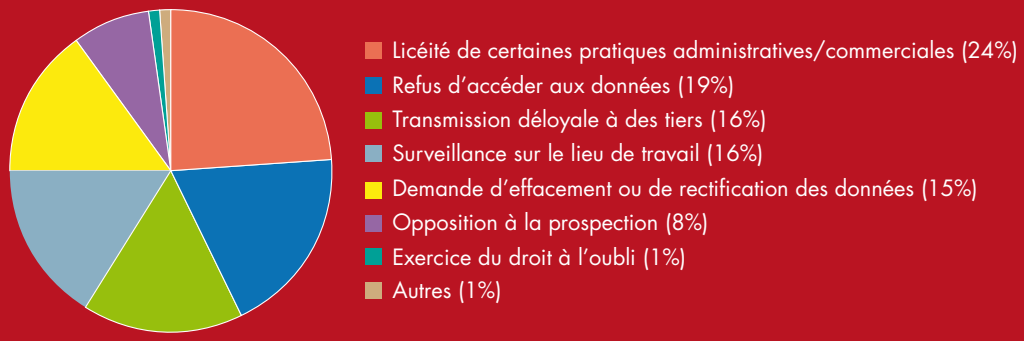
Un nombre important de plaintes (19%) a été motivé par le non-respect du droit d'accès par les responsables du traitement. Ceux-ci ont refusé aux citoyens d'accéder à leurs données, ignoré leurs requêtes ou ne leur ont pas donné assez de renseignements par rapport aux obligations légales à respecter en matière de droit d'information et d'accès. À ce titre, les fermetures, respectivement les suspensions de comptes clients, notamment par les sociétés de commerce en ligne, font l'objet de plaintes récurrentes. Dans de telles situations, les citoyens ne comprennent pas toujours les raisons pour lesquelles le statut de leur compte a changé en raison des informations parfois insuffisantes qui leurs sont fournies par les sociétés. Souvent, ils veulent une confirmation que leurs données ne font plus l'objet d'un traitement.

La transmission non autorisée de données à des tiers a également conduit à un certain nombre de plaintes (16%). Cela inclut par exemple celles concernant l'envoi

Evolution du nombre de plaintes



Motif des plaintes



de courriels à des personnes auxquelles ils n'étaient pas destinés ou l'envoi de courriels confidentiels mais distribués de façon collective et visible à tous les destinataires (« CC » au lieu de « BCC »). Un autre exemple concernait des entreprises qui conservaient des données personnelles de leurs clients en ligne sans les protéger suffisamment. En effet, chacun qui connaissait l'URL pouvait accéder à ces données.

La majorité des requêtes liées à la surveillance sur le lieu du travail (16% des plaintes) concernaient la vidéosurveillance. Des plaignants ont également contacté la CNPD lorsqu'ils ont estimé que leurs conversations téléphoniques avaient été enregistrées illégalement ou que des dispositifs de géolocalisation non autorisés avaient été installés dans leurs voitures de fonction. D'autres plaintes concernaient la prise de photos de salariés sans leur accord.

Les demandes d'effacement ou de rectification de données auxquelles les suites souhaitées n'avaient pas été réservées, ont constitué 15% des plaintes reçues en 2016. Il s'agissait, entre autres, de :

- demandes de fermetures de comptes auprès de services en ligne ;
- demandes d'effacement de données personnelles sur des sites Internet ou encore de
- demandes d'effacement d'articles de presse dans lesquels les plaignants étaient cités.

Les plaintes relatives au droit d'opposition et à la prospection sont de plus en plus courantes

(8% des plaintes). La CNPD a dû intervenir à plusieurs reprises lors d'envois de courriels ou de SMS non sollicités ou encore dans des cas où les plaignants ont voulu connaître l'origine des données utilisées par les organisations/sociétés en vue de les prospecter.

Finalement, la CNPD a obtenu gain de cause dans le traitement de plusieurs plaintes concernant le droit au déréférencement dans les moteurs de recherche. Toute personne résidant au Luxembourg peut saisir la CNPD à la suite d'un refus de déréférencement, en cas de non-réponse ou de réponse non satisfaisante.

2.1.5 Contrôles et investigations

Pour veiller au respect de la législation applicable en matière de protection des données, la Commission nationale dispose de pouvoirs d'investigation au titre desquels elle peut directement accéder aux locaux où a lieu le traitement ainsi qu'aux données faisant l'objet du traitement. Il y a lieu de rappeler qu'en vertu des dispositions de la loi, ce pouvoir d'investigation exclut les locaux d'habitation.

La CNPD n'intervient donc pas seulement lorsque des cas d'atteinte à la législation sur la protection des données lui sont signalés, mais aussi de sa propre initiative, notamment dans un but de prévention.

Elle a effectué 77 contrôles et investigations en 2016, que ce soit dans le cadre de la surveillance sur le lieu de travail ou lorsqu'elle a constaté une violation des dispositions légales en matière de protection des données. Il a pu s'agir d'un contrôle sur place où une intervention rapide de la CNPD était nécessaire ou d'une simple investigation par courrier.

Surveillance sur le lieu du travail

Presque un quart des contrôles concernaient des entreprises qui n'avaient pas respecté :

- les dispositions légales en matière de surveillance sur le lieu du travail ou encore
- les obligations posées par les autorisations de la CNPD.

Concrètement, il était question de sociétés qui avaient surveillé illégalement leurs employés sans autorisation préalable. L'autorité de contrôle luxembourgeoise a demandé à ces responsables du traitement de cesser immédiatement l'utilisation desdits dispositifs de surveillance et leur a rappelé que le non-respect de la loi était passible de sanctions pénales.

Dans d'autres cas, les responsables du traitement disposaient d'une autorisation, mais ne respectaient pas les obligations posées dans celle-ci. Il s'agissait notamment du non-respect de l'obligation d'informer

les salariés de l'existence d'un dispositif de surveillance.

Autres investigations

La CNPD est par ailleurs intervenue lorsqu'elle a pris connaissance :

- de demandes d'accès, de rectification ou d'effacement non respectées par les responsable du traitement (31% des investigations) ;

- de communications de données illégales à des tiers (16% des investigations) ;

- de demandes d'opposition non respectées par le responsable de traitement (9% des investigations) ;

- de collectes de données excessives et encore

- de mesures de sécurité insuffisantes pour protéger des données personnelles.

2.1.6 Secteur des communications électroniques

2.1.6.1 Violations de données dans le secteur des communications électroniques

Conformément au règlement (UE) No. 611/2013 de la Commission européenne du 24 juin 2013, les fournisseurs de services de communications électroniques accessibles au public, tels que les entreprises de téléphonie fixe/mobile ou les fournisseurs d'accès à Internet, doivent avertir la CNPD endéans les 24 heures suivant le constat d'une violation de sécurité et de confidentialité des données à caractère personnel et, de surcroît, informer leurs abonnés au cas où l'incident constaté est susceptible d'affecter défavorablement le niveau de protection de leur vie privée et des données les concernant.

Afin de faciliter la tâche aux fournisseurs de services de communications électroniques, la Commission nationale a élaboré un formulaire de notification d'une violation de sécurité. Celui-ci est disponible sur le site Internet de la CNPD et reprend toutes les questions pertinentes auxquelles les fournisseurs devront répondre dans une telle situation.

En 2016, une seule violation de données dans le secteur des communications électroniques a été signalée à la CNPD.

2.1.6.2 Rétention de données de trafic et de localisation

La directive européenne 2006/24/CE sur la rétention des données avait été transposée au niveau national par la loi du 24 juillet 2010 modifiant la loi du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques. L'objectif de cette directive était de conserver pendant un certain délai les données que traitent les opérateurs de télécommunications et les fournisseurs d'accès à Internet pour les besoins de la recherche, de la détection et de la poursuite d'infractions. Un des enjeux majeurs de cette directive était le maintien de l'équilibre entre, d'une part, l'accès aux données traitées par des fournisseurs de communications électroniques dans le cadre de la lutte contre le terrorisme et la criminalité grave, et d'autre part, la protection de la vie privée des citoyens.

Or, la directive a été annulée par la Cour de justice de l'Union européenne en date du 8 avril 2014 par l'arrêt « Digital Rights Ireland ». Les lois de transposition nationales n'ont toutefois pas été modifiées en conséquence et la Commission nationale n'a pas reçu d'instruction dans ce cadre par son Ministère de tutelle. Elle continue à lui transmettre annuellement en vue de leur continuation à la Commission européenne des statistiques sur la conservation des données au titre des articles 5 et 9. A cet effet, les fournisseurs de services ou opérateurs conservent et continuent à la Commission nationale, sur demande de celle-ci, les informations comprenant notamment :

- *« les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,*

- *le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,*

- *les cas dans lesquels les demandes de données n'ont pas pu être satisfaites. »*

En 2016, les autorités compétentes ont fait 4.398 demandes auprès des opérateurs. Ce chiffre a augmenté par rapport à l'année 2015 où 3.159 demandes avaient été faites.

2.2 Avis et recommandations

Conformément à l'article 32 paragraphe (3) lettre (e) de la loi modifiée du 2 août 2002, la Commission nationale a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement*

Les séances de délibération de la Commission nationale

Le collège se réunit en séance de délibération en principe une fois par semaine. Une partie importante de ces séances est consacrée à l'examen des dossiers de demande d'avis ou d'autorisation. Au cours de 32 séances en 2016, la Commission nationale a adopté 1060 délibérations, dont notamment :

- 974 autorisations ;
- 30 avis relatifs à des projets ou propositions de loi et mesures réglementaires ;
- 40 décisions concernant les chargés de la protection des données.

de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi ».

En 2016, la Commission nationale a émis 30 avis dans le cadre de projets de loi ou de règlements grand-ducaux. Une sélection des avis est résumée ci-après. Tous les avis peuvent être consultés sur le site Internet de la CNPD à l'adresse https://cnpd.public.lu/fr/publications/rapports/index.html.

2.2.1 Lutte contre le terrorisme

Suite à la demande du Ministre de la Justice, la Commission nationale s'est prononcée au sujet du projet de loi n°6921 portant 1) modification du Code d'instruction criminelle ; 2) modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; 3) adaptation de la procédure pénale face aux besoins liés à la menace terroriste.

Dans son avis du 12 février 2016, elle a commenté les points suivants que le projet de loi propose d'ajouter à la législation luxembourgeoise ou de modifier :

- L'extension du champ d'application de l'article 24-1 du Code d'instruction criminelle (repérage ou localisation des communications électroniques en cas de crime flagrant) : Entretemps, la modification projetée de l'article 24-1 du Code d'instruction criminelle a été retirée par amendement gouvernemental.
- L'introduction en droit luxembourgeois de l'enquête sous pseudonyme (Article 48-26 du Code d'instruction criminelle) : la CNPD a notamment suggéré de prohiber le recours, de manière délibérée, aux noms de personnes réellement existantes pour ce qui est des pseudonymes à utiliser.
- L'article 48-27 du Code d'instruction criminelle qui autorise le procureur d'Etat ou le juge d'instruction de requérir les opérateurs de télécommunications et les fournisseurs d'un service de télécommunications d'identifier l'abonné ou l'utilisateur habituel de leurs services ou d'identifier les services auxquels une personne donnée est abonnée ou qu'elle utilise habituellement.
- Les articles 88-1 à 88-4 du Code d'instruction criminelle relatives au contrôle des communications : la CNPD a notamment rendu attentif aux problèmes de sécurité considérables engendrés par la captation de données informatiques. Elle a également pointé les insuffisances du texte proposé en matière d'information des personnes concernées et de voies de recours.

- L'article 41 de la loi modifiée du 2 août 2002 : Cet article évite de devoir procéder, comme en l'état actuel du droit, à des perquisitions auprès des opérateurs pour obtenir les informations recherchées, et après mise en vigueur de l'article 48-27 tel que proposé, de devoir adresser des réquisitions aux opérateurs. L'instrument est censé permettre un accès direct et à distance par voie de communication électronique aux informations en question.

Dans son avis complémentaire du 14 septembre 2016, la CNPD s'est penchée sur des amendements prévoyant notamment davantage de précisions relatives à l'article 41 projeté de la loi modifiée du 2 août 2002 (devenu l'article 10bis projeté de la loi modifiée du 30 mai 2005).

2.2.2 Administration transparente et réutilisation des informations du secteur public

La Commission nationale a avisé conjointement le projet de loi n°6810 concernant une administration transparente et ouverte et le projet de loi n°6811 modifiant la loi du 4 décembre 2007 concernant la réutilisation des informations du secteur public. Elle a souligné dans son avis que ces initiatives législatives concomitantes doivent aboutir à la définition d'un cadre juridique où l'accès aux documents administratifs, la réutilisation des données publiques et la protection de la vie privée et des données à caractère personnel trouvent un équilibre.

Administration transparente et ouverte

Dans son avis, la CNPD a souligné qu'un temps d'adaptation devra nécessairement être laissé aux administrations pour se conformer au nouveau cadre juridique de diffusion des documents administratifs, dans la mesure où le projet de loi érige en principe l'obligation de diffusion des documents administratifs et fait de leur communication sur demande une exception.

S'agissant de la limitation du droit d'accès, la CNPD a salué les efforts mis en œuvre par les auteurs du projet de loi en vue d'assurer la protection d'intérêts privés fondamentaux qui peuvent entrer en conflit avec le droit d'accès. Elle s'est toutefois interrogée sur l'articulation qui sera faite en pratique de la loi modifiée du 2 août 2002 et du projet de loi n°6810.

Compte tenu des risques de réidentification qui pourraient exister, la CNPD a par ailleurs souligné que les administrations devront faire preuve d'une certaine vigilance et prévoir des garanties adéquates en présence

de documents administratifs contenant des données à caractère personnel (occultation et disjonction des mentions non communicables).

En outre, elle a estimé que les administrations devraient s'interroger préalablement à la publication et au partage en ligne de documents administratifs sur les risques existants. Ainsi, ces administrations pourront décider d'une accessibilité plus ou moins large des documents qu'elles détiennent, en fonction du risque pour les données en cause (diffusion des documents sur Internet auprès du grand public et sans restriction d'accès, mise en ligne de documents subordonnée à des conditions d'accès restreintes, consultation sur place de documents etc).

Réutilisation des informations du secteur public

Bien que de nombreuses informations publiques visées par le projet de loi n°6811 ne portent pas sur des données à caractère personnel, la Commission nationale a noté que les organismes relevant du secteur public détiennent un volume important de données à caractère personnel.

Afin de pallier l'accessibilité accrue des données à caractère personnel contenues dans des documents du secteur public et les risques d'usage abusif de ces données, la CNPD a recommandé de faire référence de manière plus explicite dans le projet de loi au cadre juridique applicable à la protection des données.

En ce qui concerne la responsabilité des organismes visés par le projet de loi, la CNPD s'est rallié à la recommandation du Groupe de travail « Article 29 » selon laquelle les organismes concernés devraient procéder à des évaluations d'impact sur la protection des données avant de rendre disponible à des fins de réutilisation, des informations du secteur public (Avis 6/2013 du Groupe de travail « Article 29 »). En outre, un principe de proportionnalité devrait être appliqué minutieusement par les organismes responsables de traitements dans le choix des méthodes, des modalités et des degrés de détail envisagés pour rendre les informations publiquement disponibles.

Autant que faire se peut, seuls des documents ou informations publiques rendus anonymes (notamment par agrégation de données) devraient être mis à disposition à des fins de réutilisation. A défaut, toute réutilisation ultérieure d'informations publiques comportant des données à caractère personnel devrait reposer sur une base juridique appropriée (par exemple, un consentement ou une obligation légale). En toute hypothèse, la CNPD a rappelé que des données à caractère personnel pourraient être rendues disponibles à des fins de réutilisation, si nécessaire et sous réserve de garanties adéquates.

Enfin, dans le respect du principe de limitation de finalité, la CNPD a rappelé que les organismes du secteur public pouvaient encadrer les conditions de réutilisation de certains documents, notamment par le biais de licences.

2.2.3 Service de Renseignement de l'Etat

Statut spécifique pour certaines données traitées par le Service de Renseignement de l'Etat

La Commission nationale a rendu un avis au sujet du projet de loi n°6850 portant mise en place d'un statut spécifique pour certaines données à caractère personnel traitées par le Service de Renseignement de l'Etat.

Selon les auteurs du projet, celui-ci consacre une assise légale à la conservation des dossiers composant « les archives historiques » du Service de Renseignement de l'Etat en vue d'en autoriser des exploitations scientifiques à des fins historiques.

En exécution d'une des recommandations soulevées par la Commission d'enquête de « confier le traitement, l'utilisation et la conservation à l'Institut culturel de Archives nationales

de Luxembourg », les archives historiques du Service de Renseignement de l'Etat ont été déménagées le 3 octobre 2013 aux Archives nationales qui les a acceptées en vue de leur mise en dépôt au sens de l'article 21 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Elles y sont déposées dans un local sécurisé, compte tenu de la classification des pièces y contenues, à laquel le Service de Renseignement de l'Etat n'a plus accès sans autorisation des Archives nationales.

La finalité de cette exploitation scientifique objective des archives historiques est d'examiner, si le Service de renseignement a, pendant la période visée, effectué un espionnage de la vie et des activités politiques à Luxembourg ou s'il s'est tenu à l'observation des menaces contre l'Etat luxembourgeois telles que les menaces se présentaient pendant la Guerre Froide.

En outre, l'objet du projet de loi est de garantir une objectivité du travail scientifique et historique et de régler certains aspects juridiques touchant notamment à l'accès des pièces classifiées au sens de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité et au sort à réserver aux données à caractère personnel au sens de la loi sur la protection des données.

La CNPD a notamment formulé des observations relatives au stockage des données traitées, ainsi qu'au droit d'accès par les personnes concernées.

Traitements de données effectués par le Service de Renseignement de l'Etat et par l'Autorité nationale de Sécurité

En date du 13 juillet 2016, la CNPD a rendu un avis relatif à un projet de règlement grand-ducal pris en exécution de la loi du 5 juillet 2016 portant réorganisation du Service de Renseignement de l'Etat et à un projet de règlement grand-ducal pris en exécution de la loi du 15 juin 2004 relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité

L'autorité de contrôle a analysé les deux projets de règlements notamment au regard de ses propres observations formulées dans l'avis du 28 juin 2013 sur deux précédent projets de règlement relatifs au Service de Renseignement de l'Etat et l'Autorité nationale de Sécurité.

Elle a entre autres suggéré de porter le délai de conservation des fichiers de journalisation de trois ans à cinq ans.

2.2.4 Accord Luxembourg/ Etats-Unis pour l'échange d'informations de détection du terrorisme

La Commission nationale a avisé le document « Procédures de mise en œuvre du Protocole d'Accord conclu entre le Gouvernement du Grand-Duché de Luxembourg et les Etats-Unis d'Amérique pour l'échange d'informations de détection du terrorisme ».

Ledit document est censé faire figure d'« implementing procedures to be agreed between the Parties arising under this Memorandum of Understanding » telles que prévues par différentes dispositions du Protocole d'Accord conclu entre le Gouvernement du Grand-Duché de Luxembourg et les Etats-Unis d'Amérique pour l'échange d'informations de détection du terrorisme qui a fait l'objet du projet de loi d'approbation n°6759.

Dans son avis, la Commission nationale a limité son analyse aux aspects devant faire l'objet de telles « implementing procedures » en vertu dudit Protocole d'Accord.

La CNPD s'est notamment penchée sur les voies de recours, alors que le Protocole d'Accord et la procédure de mise en œuvre prévoient un recours que pourra exercer la personne concernée.

La CNPD a constaté que le texte de procédure de mise en œuvre (tout comme le Protocole d'Accord) ne précise pas devant qui le recours doit être exercé. La CNPD a soulevé la question de savoir s'il s'agit d'une réclamation auprès de l'institution même qui a traité les données plutôt que d'un recours devant une autorité (administrative ou judiciaire) indépendante.

Par ailleurs, la portée de ce « recours » risque d'être très limitée. En effet, au regard des textes du Protocole d'accord et des Procédures de mise en oeuvre, il semblerait que le « recours » ne puisse pas porter sur toutes questions de licéité et de conformité aux règles de protection des données mais seulement sur des questions relatives à l'exactitude des données. Dans le cas où ce serait ainsi, la Commission nationale se demande s'il faut alors comprendre que d'autres règles ou principes sujets à contestations en seraient exclus, telles que la proportionnalité du traitement, la durée de conservation des données ou le respect des finalités du traitement.
Elle estime que le recours prévu dans les procédures de mise en œuvre s'apparente plus au droit de rectification à exercer auprès du responsable du traitement qu'à une véritable voie de recours.

Enfin, pour pouvoir exercer un recours à l'encontre d'un traitement de données, il faut avoir connaissance de l'existence de ce traitement. Ceci pourrait s'avérer difficile en l'espèce, puisque le Protocole d'accord ne prévoit pas de dispositions relatives au droit à l'information ou au droit d'accès.

2.2.5 Traitement de données concernant les élèves et la jeunesse

Traitement des données concernant les élèves et la carte d'élève « MyCard »

La Commission nationale s'est prononcée au sujet :

- de l'avant-projet de règlement grand-ducal précisant les données accessibles et les données communiquées en exécution des articles 4 et 6 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves,

- de l'avant-projet de règlement grand-ducal pris en exécution de l'article 5 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves, et

- de l'avant-projet de règlement grand-ducal fixant le modèle et les modalités de délivrance, d'utilisation et de retrait de la carte d'élève « myCard ».

2 Les activités en 2016

Les avant-projets de règlements grand-ducaux ont pour objectif de compléter la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves (ci-après la « loi du 18 mars 2013 »), notamment

(i) en fixant le détail des données à caractère personnel pouvant être accédées ou communiquées dans le cadre des différents cas de figure énumérés limitativement aux articles 4 et 6 de la loi,

(ii) de fixer les critères et les conditions d'accès aux données, les modalités d'octroi et de retrait des autorisations d'accès, la périodicité de la révision des accès et la durée de leur validité conformément à l'article 5 de la loi, et

(iii) d'arrêter le modèle ainsi que les modalités de délivrance, d'utilisation et de retrait de la carte d'élève « myCard » conformément à l'article 3, paragraphe (1), point 5 de la loi.

Concernant le point (i), la Commission nationale a souligné qu'il existait un manque de cohérence entre la liste des autorités et entités figurant à l'article 6 de la loi du 18 mars 2013, qui peuvent recevoir

communication des données, et la liste des autorités et entités énumérées à l'article 2 de l'avant-projet de règlement grand-ducal. Elle a recommandé d'aligner la liste des tiers dans l'article 2 de l'avant-projet de règlement grand-ducal sur celle de l'article 6 de la loi du 18 mars 2013 ainsi que de suivre le même ordre dans l'énumération des tiers dans le règlement grand-ducal que dans le texte de la loi. De plus, la Commission nationale a recommandé de préciser dans le règlement grand-ducal la liste des données pouvant faire l'objet d'une communication à l'Institut national pour le développement de la formation professionnelle continue et de justifier l'inclusion des chambres professionnelles à accéder à certaines données à caractère personnel du ministère et de préciser quelles chambres professionnelles seront visées. Concernant le point (ii), la Commission nationale regrette que les auteurs du texte projeté renvoient simplement vers un approvisionnement du système de gestion des droits d'accès « de manière automatisée » par le fichier du personnel « SYCLOPE » au lieu de préciser, comme requis par le paragraphe (2) de l'article 5 de la loi du 18 mars 2013, « les critères et conditions d'accès aux données » ou de renvoyer au moins vers un descriptif dudit fichier et qu'il y a lieu de définir les critères d'accès aux données dans le règlement grand-ducal pris en exécution de la loi du 18 mars 2013. La Commission nationale a également suggéré d'intégrer une obligation de révision des accès lors de chaque changement d'affectation d'un membre du personnel.

Concernant le point (iii), la Commission nationale a préconisé de préciser davantage les modalités de retrait de la carte en soulignant qu'il était du vœu exprès du Conseil d'Etat que soient détaillés dans un règlement grand-ducal « le modèle de la carte et les modalités de délivrance et de retrait » (doc. parl. 6284/11 – amendement 11). Elle a suggéré de prévoir une désactivation des fonctionnalités électroniques de la carte en cas de non restitution de la carte au moment où l'élève quitte l'enseignement ou lorsqu'il y a eu une utilisation frauduleuse de la carte.

Jeunesse

La CNPD a émis un avis en date du 14 octobre 2016 sur le projet de loi n°7064 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse et portant modification de la loi du 18 mars 2013 relative aux traitements des données à caractère personnel concernant les élèves.

Ce projet de loi a pour objectif d'introduire l'éducation plurilingue dans certaines structures d'accueil agréées destinées aux enfants âgés de 1 à 4 ans. Cette éducation plurilingue d'enfants en bas âge serait accompagnée d'une aide accordée par l'Etat, octroyée en fonction de l'âge et de la scolarisation ou non de l'enfant, et devant être agencée avec l'aide accordée dans le cadre du chèque-service accueil.

De ce fait, certains articles du projet de loi ont notamment pour objet de permettre l'accès au Ministre ayant l'Enfance et la Jeunesse dans ses attributions à certaines données rendues nécessaires à l'administration des aides accordées par l'Etat suite à l'introduction de l'éducation plurilingue dans ces structures d'accueil agréées.

Dans son avis, la Commission nationale a attiré l'attention des auteurs du projet de loi sur les garanties qui devraient être associées à de tels accès, ainsi que sur le caractère nécessaire et proportionnel des données qui seront accédées. Il convient en effet de garantir que les accès par le Ministère compétent en matière d'Enfance et de Jeunesse aux fichiers d'autres administrations ne portent pas préjudice à la vie privée et à la protection des données à caractère personnel des administrés.

2.2.6 Laboratoire National de santé

La CNPD s'est prononcée sur le projet de loi n° 6995 qui vise à adapter certaines dispositions du droit luxembourgeois afin

d'instaurer une « unité de documentation médico-légale des violences » (projet dénommé « Opferambulanz »), dont la gestion sera confiée au Laboratoire National de Santé. Cette unité a vocation à documenter d'un point de vue médico-légal les blessures physiques subies par des personnes physiques victimes d'infractions pénales intentionnelles ou non intentionnelles.

Dans son avis, la CNPD a formulé des observations sur les modalités de pseudonymisation envisagées. En présence de données sensibles figurant dans le fichier de l'unité de documentation médico-légale des violences, elle a recommandé la mise en place d'une gestion séparée entre les données d'identification nécessaires pour recontacter les personnes concernées, d'une part, et les données détaillées concernant les violences, d'autre part, reposant notamment sur la création de deux bases de données distinctes respectant un principe de cloisonnement et sur la définition d'habilitations d'accès différenciées selon le profil et les missions du personnel du LNS.

La CNPD a noté que l'unité de documentation médico-légale des violences était censée fonctionner selon un mode décentralisé, reposant sur une collaboration étroite et des échanges d'informations entre ladite unité et les hôpitaux. Dans un souci de respect des exigences du secret professionnel, la CNPD a souligné qu'une certaine vigilance devrait être adoptée par les professionnels de santé concernés quant aux informations à partager, quant au but de l'échange et surtout quant aux limites de cet échange.

2.2.7 Archivage

La Commission nationale a donné son avis sur le projet de loi n°6913 sur l'archivage qui entend renouveler le cadre juridique en vigueur en matière d'archivage dans l'intérêt public. Bien que de nombreux documents d'archives ne comportent aucune donnée à caractère personnel, de tels documents peuvent tomber sous l'application de la loi modifiée du 2 août 2002, dès lors qu'ils se rapportent à des personnes physiques potentiellement encore vivantes ou à des personnes décédées dont la publication de données à caractère personnel a des conséquences sur la vie privée de leurs ayants droit.

La CNPD a formulé des observations sur les dispositions du projet de loi ayant trait à la répartition des responsabilités entre les acteurs intervenant dans le contexte de l'archivage, aux finalités des traitements à des fins d'archivage dans l'intérêt public, à la pertinence des données collectées à des fins d'archivage dans l'intérêt public et la durée

de conservation de ces dernières, ainsi qu'à la problématique de la réutilisation des archives. A cet égard, la CNPD a estimé primordial que les organismes concernés évaluent l'impact potentiel que la mise à disposition d'archives pourrait avoir sur les droits et libertés des personnes.

S'agissant des droits des personnes, la CNPD a noté que les auteurs du projet de loi ont souhaité aménager la protection des droits telle que prévue par la loi modifiée du 2 août 2002 en prévoyant des dispositions spécifiques dans le projet de loi sous examen. Elle a formulé plusieurs observations à cet égard. Elle a notamment souligné qu'en principe les restrictions au droit d'accès des personnes concernées sont limitativement énumérées par la loi et l'article 23 du Règlement général sur la protection des données.

S'inquiétant d'un abaissement du niveau de protection des droits par le projet de loi, elle s'est ralliée à la recommandation du Conseil d'Etat de « *remettre l'ensemble du texte proposé sur le métier, et cela à la lumière du règlement européen* » (Avis du Conseil d'Etat n°51.437).

S'agissant du développement croissant de services d'archives digitaux et de la mise à disposition de documents d'archives en ligne, la CNPD a invité à une certaine prudence et à la mise en place de mesures juridiques et techniques adéquates, afin de minimiser les risques pour la vie privée des personnes et le respect de leurs données à caractère personnel. A cet égard, elle a recommandé d'encadrer, par voie législative et non réglementaire, les restrictions à la communication de certains documents d'archives publiques. Elle a par ailleurs souligné que le raccourcissement de certains délais de communication des documents d'archives pourrait entrer en contradiction avec le droit à la protection des données.

S'agissant de la publication des archives sur internet, la Commission nationale s'est félicité de l'encadrement prévu par les auteurs du projet de loi (instauration de délais plus longs), compte tenu du risque d'atteinte disproportionnée pour la vie privée qui pourrait résulter d'une publication sur Internet de certaines informations ayant trait à la vie privée des personnes. Soucieuse par ailleurs de trouver un équilibre entre l'intérêt des chercheurs et la protection des données, elle s'est dite favorable à l'instauration de mécanismes permettant de restreindre l'accès aux archives mises en ligne à des fins de recherche, dès lors que ces dernières contiendraient des données sensibles.

2.2.8 Echange de données à caractère personnel et d'informations en matière policière

En date du 17 novembre 2016, la CNPD a rendu un avis sur le 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 œuvre 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.

La CNPD a suggéré des améliorations du texte notamment en ce qui concerne les fichiers de journalisation et les voies de recours.

A part la coopération entre autorités policières des Etats-membres de l'Union européenne, le projet de loi en question tente de régler une série d'autres cas de figure.

Ainsi, il traite des échanges de données policières avec les autorités d'Etats tiers.

A ce sujet, la CNPD a souligné les risques liés à la communication de données à des autorités de pays tiers, notamment en ce qui concerne le respect du principe de finalité et l'éventuelle communication ultérieure à d'autres Etats que l'Etat destinataire original. Elle a aussi soulevé le risque de l'utilisation des données à des fins de poursuites politiques.

Le texte règle aussi les communications de données de Police vers des administrations publiques.

Dans ce contexte, la CNPD a soulevé certaines questions relatives aux principes de nécessité et de proportionnalité. Par ailleurs, elle a mis en garde contre le risque de non-respect du principe de finalité. A ce sujet, elle a notamment suggéré d'introduire des mentions obligatoires – dans les demandes de transmission et les transmissions elles-mêmes – relatives à la raison de la transmission des données.

Elle a également donné à réfléchir qu'en cas de transmission de données de la Police grand-ducale vers des administrations avant tout jugement sur l'affaire, la personne concernée risquerait de subir une « condamnation administrative » sur base d'un rapport ou d'un procès-verbal avant même que la justice ait pris de décision.

2.2.9 Abus de marché

La Commission nationale a rendu le 2 décembre 2016 son avis sur le projet de loi n°7022, qui visait à adapter la législation

luxembourgeoise en matière d'abus de marché afin de garantir l'application intégrale et cohérente de l'ensemble des nouvelles règles européennes en la matière[2]. Elle a formulé des observations sur plusieurs éléments du projet de loi.

Quant à la coopération entre la CSSF et le Procureur d'Etat, la CNPD a soulevé que le projet de loi permettrait au Procureur d'Etat de transmettre des dossiers d'enquête contenant des données à caractère personnel à la CSSF, sans préciser si les données transmises seraient à considérer comme étant des données judiciaires au sens de l'article 8 de la loi modifiée du 2 août 2002 lors de la poursuite de la procédure par la CSSF. Cette même question se posait dans le cadre des pouvoirs d'investigation de la CSSF qui nécessitaient au préalable une autorisation judicaire du juge d'instruction. La CNPD a dès lors estimé nécessaire de préciser les règles applicables à ces genres d'enquêtes mixtes.

Quant au pouvoir de la CSSF d'exiger la communication des enregistrements téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic des entités surveillées, des émetteurs, des réviseurs d'entreprises agréés et des cabinets de révision agréés, la CNPD a considéré que le projet de loi, en incluant les trois dernières catégories d'organismes, dépassait le champ d'application défini par le règlement (UE) n°596/2014.

Quant au pouvoir de la CSSF d'exiger les enregistrements des données relatives au trafic détenus par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics avec l'autorisation judiciaire du juge d'instruction, la CNPD a estimé que la disposition n'était ni compatible avec la jurisprudence européenne récente, ni avec le projet de loi n°6763 et qu'il y avait dès lors lieu de la supprimer du projet de loi.

Quant au registre des signalements reçus tenu par la CSSF, la CNPD a recommandé d'énumérer dans le projet de loi les données traitées dans ce registre. Par ailleurs, comme le projet de loi prévoyait la possibilité pour la CSSF d'enregistrer les appels des informateurs, la CNPD a souligné la nécessité de modifier la loi modifiée du 30 mai 2005 afin de prévenir une incompatibilité entre cette dernière loi et le projet de loi. Elle a également suggéré de modifier les dispositions relatives à l'anonymat des informateurs, à l'information et les droits des personnes concernées, à la sécurité des données et à la durée de conservation des données.

Quant à l'obligation de la CSSF de coopérer avec le Procureur d'Etat et le Service de Police Judiciaire, l'Inspection du Travail et des Mines, ainsi que les autorités compétentes d'autres Etats membres et des pays tiers, la CNPD a notamment souligné la nécessité de faire figurer dans la loi les modalités d'accès et de transmission de données à caractère personnel ainsi que la nécessité d'assurer la confidentialité et la sécurité des données pendant toutes les étapes du traitement.

Quant à la publication des sanctions par la CSSF, la CNPD a précisé qu'aucune donnée autre que le nom et le prénom de la personne visée par la sanction ne devrait figurer dans la décision publiée sur le site de la CSSF.

2.2.10 Revenu d'inclusion sociale

En date du 22 décembre 2016, la CNPD a rendu son avis sur l'avant-projet de loi relatif au revenu d'inclusion sociale (Revis).

L'objectif principal de cet avant-projet de loi est d'améliorer l'inclusion sociale de chacun dans la société. Pour y parvenir, le texte a notamment recours à la simplification administrative, entre autres en mettant en place certains échanges de données entre les divers intervenants dans la procédure, ainsi que des accès à certains fichiers étatiques.

[2] Le Règlement (UE) n°596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché, la Directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché (directive relative aux abus de marché et la directive d'exécution (UE) 2015/239 de la Commission du 17 décembre 2015 relative au règlement (UE) n°596/2014 du Parlement européen et du Conseil en ce qui concerne le signalement aux autorités compétentes des violations potentielles ou réelles dudit règlement.

Ces accès touchent notamment le fichier national des personnes physiques ainsi que le fichier relatif aux affiliations du Centre commun de la sécurité sociale, dont le degré de sensibilité est évident. La Commission nationale a surtout attiré l'attention des auteurs de l'avant-projet de loi sur le caractère nécessaire et proportionnel des données qui seront accédées, ainsi que sur les mesures de sécurité qui doivent entourer de tels accès. L'avis formule, par ailleurs, des propositions de clarification quant aux rôles des divers intervenants, la durée de conservation des données ainsi que sur les différences entre les concepts de « données anonymisées » et « données pseudonymisées ».

2.3 Information du public

L'information des citoyens comme des responsables du traitement est une priorité de la Commission nationale, afin de faire connaître les droits et devoirs respectifs de chacun. Elle mène des actions de sensibilisation du public, informe le grand public à travers son site Internet et participe à des formations et conférences.

2.3.1 Actions de sensibilisation du public

Dixième journée de la protection des données

Le Conseil de l'Europe, avec le soutien de la Commission européenne, a proclamé solennellement le 28 janvier de chaque année comme Journée de la protection des données. En 2016, le 10e anniversaire de cette journée a été célébré. Le but de celle-ci est de sensibiliser les citoyens européens à l'importance de la protection de leurs données personnelles et du respect de leurs libertés et droits fondamentaux, en particulier de leur vie privée.

Pourquoi le 28 janvier ? C'est la date de l'ouverte à la signature de la « Convention 108 » du Conseil de l'Europe (28 janvier 1981). Cette dernière a été le premier instrument international juridiquement contraignant en la matière. Depuis plus de 35 ans, la convention vise à protéger toute personne contre l'utilisation abusive des données qui la concernent et à assurer la transparence quant aux fichiers et traitements des données personnelles.

La Journée de la protection des données est célébrée mondialement depuis quelques années et est appelée « Privacy Day » en dehors de l'Europe.

La CNPD a participé à plusieurs événements dans le cadre de cette journée :

Conférence « Chargé de protection. Un métier d'avenir! »

Le 28 janvier, la CNPD, en collaboration avec l'APDL, a organisé une conférence sur le métier de Chargé de protection, son rôle et sa fonction aujourd'hui et demain avec l'arrivée du nouveau règlement européen.

La fonction du chargé de la protection des données est appelée à prendre plus d'importance avec cette réforme au niveau européen, qui mise encore davantage sur la responsabilisation des entreprises et des acteurs. Dans ce sens, le règlement ne vise pas seulement les chargés, mais également les responsables de la sécurité de l'information, les juristes d'entreprise, les consultants et les avocats.

C'était l'occasion pour M. Arnaud Constant de l'APDL de présenter une fiche sur la fonction du Chargé de protection qui a été élaborée avec la CNPD. M. Georges Wantz, membre effectif de la CNPD, a présenté les nouveautés et les défis du règlement européen sur la protection des données, en particulier pour les chargés. M. Pascal Steichen de *Securitymadein.lu* a partagé son expertise sur le principe du « privacy by design ».

Panel à la conférence Computers, Privacy and Data Protection à Bruxelles

Fin janvier, l'autorité de protection des données luxembourgeoise a également organisé, ensemble avec l'Université du Luxembourg, un panel à la conférence internationale Computers, Privacy and Data Protection à Bruxelles.

Les discussions lors de ce panel ont porté sur le rôle et les pouvoirs des autorités de protection des données dans le contexte des récentes jurisprudences de la Cour de justice de l'Union européenne et à la lumière de l'entrée en vigueur du nouveau règlement européen en 2018.

Les participants étaient Dr. Franziska Boehm (Karlsruhe Institute of Technology), Dr. Hielke Hijmans (EDPS), M. Bart van der Sloot (IViR-UvA) et M. Georges Weiland (CNPD). Dr. Andra Girgiu de l'Interdisciplinary Centre for Security, Reliability and Trust (SnT) de l'Université du Luxembourg a assuré la modération.

Table ronde au Cybersecurity Breakfast: « Data Protection and Cybersecurity, new laws on the horizon! »

La CNPD a par ailleurs participé à une table ronde dans le cadre du Cybersecurity Breakfast, organisée par Securitymadein.lu et Allen&Overy.

Après la Keynote de Dr. Catherine Di Lorenzo (Avocat à la Cour, Allen&Overy), une table ronde eut lieu avec la participation de Dr. Di Lorenzo, Dr. Michèle Feltz (CNPD) et Mme Mélanie Gagnon (MGSI). La table ronde était modérée par Dr. Matthieu Farcot (Legal&Business Affairs Manager, Securitymadein.lu).

Autres actions de sensibilisation

La CNPD a également participé au Safer Internet Day. Cette journée, organisée sur initiative de la Commission européenne, engendre un large éventail d'activités qui ont eu lieu à travers le monde. BEE SECURE s'est occupé de la coordination des activités au Luxembourg. En 2016, le Safer Internet Day était placé sous le slogan: « Play your part for a better internet ».

Sans remettre en question les effets positifs d'Internet, les objectifs du Safer Internet Day 2016 étaient les suivants :

- apporter une aide aux enfants, jeunes, parents et pédagogues grâce à des informations concrètes et des conseils pratiques ;

- obtenir une participation active des institutions, organisations, associations, entreprises, initiatives et particuliers au niveau national, régional et local dans le cadre d'une campagne internationale ;

- orienter l'attention publique et médiatique sur le thème « Utiliser Internet en toute

sécurité » dans le cadre d'un projet européen (Programme Safer Internet).

2.3.2 Reflets de l'activité de la Commission nationale dans la presse

La Commission nationale est intervenue régulièrement dans les médias pour commenter les sujets ayant trait à la protection des données et à la protection de la vie privée.

En 2016, le collège a accordé 29 interviews à des multiples organes de presse. Parmi les thèmes traités, citons la réforme du cadre juridique européen en matière de protection des données, les droits des citoyens sur Internet, l'invalidation de l'accord « Safe Harbour » et l'adoption du « Privacy Shield », les radars automatiques, les cartes de paiement sans contact, les compteurs intelligents, les drones, les « dashcams », la collecte de données de Whatsapp/Facebook ou encore la surveillance sur le lieu du travail.

2.3.3 Outil de communication : le site Internet

Le site web de la Commission nationale est destiné à la fois aux responsables du traitement et au grand public.

Les responsables du traitement peuvent y accomplir les formalités prescrites par la loi. Afin de les guider de la manière la plus claire possible, la Commission nationale y met à disposition des rubriques et formulaires dédiés (ex : formulaire de demandes d'autorisation en matière de vidéosurveillance et de transferts de données vers des pays tiers, engagements formels de conformité, formulaires de notification, demande d'agrément pour les chargés de la protection des données, etc.).

Le grand public, quant à lui, peut s'informer sur les sujets qui ont dominé l'actualité dans le domaine de la protection des données et de la vie privée. Le site offre aussi une information de base sur la protection des données et sur les droits et obligations respectifs. Les internautes intéressés peuvent élargir leurs connaissances par la consultation de dossiers thématiques.

Le site permet également de consulter le registre public des traitements et enfin de contacter la Commission nationale pour toute question, demande de renseignement complémentaire ou pour déposer une plainte.

En 2016, un nouveau dossier thématique dédié au nouveau règlement européen sur la protection des données a été créé. Il contient des explications sur les nouveaux

Madame Tine A. Larsen participe au séminaire de l'UIA à la Cour de Justice de l'Union européenne.

Monsieur Thierry Lallemang (à gauche) intervient à la conférence de printemps de l'ALFI.

droits et obligations, des recommandations du groupe « Article 29 » et les présentations données lors des conférences et séances d'informations organisées par la CNPD à ce sujet.

2.3.4 Formations et conférences

À côté de l'information du grand public, la Commission nationale participe aussi régulièrement à des formations, conférences et séminaires pour sensibiliser des publics plus spécialisés aux enjeux de la protection des données.

Le 11 janvier, Mme Tine A. Larsen, présidente de la CNPD, a donné une présentation au Lions Club Luxembourg sur le thème « Europäische Datenschutzreform – Ein wirksamer Schutz der Privatsphäre im digitalen Zeitalter ».

Le 19 janvier, la présidente de la CNPD a prononcé un mot de bienvenue au colloque « La genèse et les conséquences de l'arrêt Schrems », organisé par l'Union Internationale des Avocats (UIA) en partenariat avec le Barreau de Luxembourg et l'étude d'avocats Bonn&Schmitt.

Le 27 janvier, M. Arnaud Habran du service juridique de la CNPD a participé au « FNR Infoday », organisé par le Fonds national de la recherche et destiné aux chercheurs de l'université du Luxembourg. Sa présentation a plus particulièrement porté sur la protection des données en matière de recherche scientifique.

Le 18 février 2016, M. Georges Wantz, membre effectif de la CNPD, a participé au workshop « EU law for the financial sector: the rules on data security and data protection ». Son intervention a porté sur l'impact du nouveau règlement européen en matière de protection des données sur le secteur financier.

Le 23 février, M. Thierry Lallemang, membre effectif de la CNPD, a donné une présentation, ensemble avec Mme Catherine Di Lorenzo (Allen&Overy), sur les clés pour une mise en œuvre réussie du nouveau règlement sur la protection des données. Cet exposé a été fait lors de la conférence de CREO « Protection des données et vie privée : défis, enjeux et limites à la lumière des évolutions récentes ».

Les 8 et 9 mars, M. Lallemang est intervenu à la conférence de printemps de l'ALFI (Association of the Luxembourg Fund Industry) sur le thème de « U.S. Safe Harbour : how to play by the (new) rules ? ».

Les activités en 2016

Le 14 avril, M. Alain Herrmann du service informatique et nouvelles technologies a participé à une table ronde lors du séminaire « Cyber Security – from strategic awareness to operative actions ». Cet événement a été organisé par la Chambre de Commerce et Business Sweden et l'ambassade suédoise au Luxembourg.

Le 21 avril, M. Georges Wantz a participé à l'ADaCoR (Advanced Data Collection and Risks) Industry Workshop organisé par l'Université du Luxembourg. Sa contribution a porté sur les aspects de la protection des données en matière de collecte de données.

Le 26 avril, M. Thierry Lallemang est intervenu lors du petit-déjeuner HR One sur la thématique de la surveillance des employés au travail, et plus particulièrement de la frontière entre liberté et surveillance des salariés. Lors de sa présentation, il a notamment abordé les différents types de surveillance sur le lieu de travail ainsi que leurs conditions, restrictions légales et celles imposées par la CNPD. Il a également traité le rôle spécifique de la représentation du personnel, des obligations légales à respecter par l'employeur, des sanctions et sur la réforme européenne en matière de protection des données.

Le 13 mai, M. Alain Herrmann a participé au Information Security Education Day (ISED), organisé par l'Université du Luxembourg et LIST (Luxembourg Institute of Science and Technology). Les orateurs ont essayé de répondre à la question : « How to guarantee security in the realm of Big Data & Analytics ? ».
Les 18 et 19 juin, M. Thierry Lallemang et M. Alain Herrmann ont donné des cours de formation à l'Institut National d'Administration Publique (INAP).

Le 6 septembre, la présidente de la CNPD a participé à un séminaire interactif à Cologne organisé par l'European Data Protection Law Review. Le séminaire était intitulé « How to prepare for the General Data Protection Regulation and the Privacy Shield ? ». Mme Larsen a donné une présentation sur l'impact du nouveau règlement sur les autorités de protection des données.

Le 21 septembre, Mme Andra Giurgiu du service juridique a participé à la conférence d'l'IFE Benelux intitulée « Protection des données : tout sur la nouvelle réglementation européenne – quelles sont les questions, les perspectives, les solutions ? ». Sa présentation était intitulée « Accountability according to the proposed GDPR : at the crossroads between law and technology ».

Le 29 septembre, M. Alain Herrmann a participé à une table ronde aux IT Days. Le thème de

la table ronde était : « The right CDO for your company's future – the five archetypes of a chief digital officer ».

Les 30 septembre et 1er octobre, Mme Tine A. Larsen et M. Thierry Lallemang ont participé à un séminaire organisé par l'Union Internationale des Avocats (UIA), en partenariat avec le Barreaux du Luxembourg, à la Cour de Justice de l'Union européenne sur le thème de : « Protection des données personnelles dans les services financiers (FinTech), d'assurance et médicaux : Nouveau règlement et perspectives ». Le programme scientifique a été introduit par le Président de la CJUE, M. Koen Lenaerts. Il a été suivi par l'intervention de plus de 60 orateurs, dont la présidente de la CNPD qui a prononcé son mot de bienvenue. Devant près de 300 participants provenant de 29 pays différents, M. Lallemang a modéré la session sur l'encadrement des données financières, d'assurance et médicales par les autorités de régulation. Le Ministre de la Santé, Mme Lydia Mutsch et le Ministre de la Justice, M. Félix Braz, ont prononcé des discours remarqués. Le contrôleur européen de la protection des données M. Giovanni Buttarelli, M. Dean Spielmann, juge au tribunal de l'Union européenne et M. François Biltgen, juge à la CJUE ont rappelé l'importance du respect des droits fondamentaux pour encadrer les évolutions technologiques.

Le 22 novembre, Mme Tine A. Larsen a participé à une table ronde lors des Luxembourg Internet Days sur l'Internet des objets. Le sujet de la table ronde était : « Barbarians at the Gate : Regulating IoT's Fast Track to Success … or Disaster ».

Le 24 novembre, M. Alain Herrmann a donné une conférence avec M. Joe McNamee (EDRI.org) sur le nouveau règlement général en matière de protection des données. Cet événement a été organisé par ISACA Luxembourg.

Tout au long de l'année, M. Thierry Lallemang a donné des formations sur la protection des données à l'Ecole supérieure du travail et M. Alain Herrmann a organisé des workshops sur le thème du « Privacy by Design ».

2.4 Conseil et guidance

2.4.1 Concertation avec les organisations représentatives sectorielles, les principaux acteurs économiques, l'État et les organismes publics

La sensibilité croissante du public à l'égard des questions de protection des données implique des efforts accrus de l'équipe de la CNPD, qui doit fournir une guidance appropriée aux acteurs tant du secteur public que du secteur privé. Ceux-ci se tournent vers elle pour vérifier la conformité de leurs pratiques ou projets à l'égard des dispositions légales applicables.

En 2016, la Commission nationale a participé à plus de 125 réunions avec les acteurs du secteur public et à 73 réunions avec ceux du secteur privé.

Elle était, entre autres, en relation avec les ministères, administrations et organes publics suivants :

- Service des Communications et des Médias ;
- Ministère de la Justice ;
- Ministère des Finances ;
- Ministère des Affaires étrangères et européennes ;
- Ministère de l'Economie ;
- Ministère du Logement ;
- Ministère de la Santé ;
- Ministère de l'Education nationale, de l'Enfance et de la Jeunesse ;
- Ministère des Sports ;
- Ministère du Développement durable et des Infrastructures – Département des Transports ;
- Administration de l'Environnement ;
- Administration des Services de Secours ;
- Administration pénitentiaire ;
- Parquet général ;
- Commission de surveillance du secteur financier ;

- Institut luxembourgeois de régulation ;
- Centre de gestion informatique de l'éducation ;
- Office national de l'enfance ;
- Agence nationale de la sécurité des systèmes d'information (ANSSI).

Parmi les entreprises multinationales implantées au Luxembourg, la Commission nationale a notamment rencontré Rakuten, Amazon, eBay et Paypal.

La Commission nationale est aussi intervenue périodiquement dans les travaux de la Commission Consultative des Droits de l'Homme (CCDH), de la Commission du registre national des personnes physiques et du Comité des statistiques publiques.

Dans le domaine de la recherche, elle était en lien avec le Comité National d'Ethique et de Recherche (CNER), l'IBBL (Integrated Biobank of Luxembourg), le LIST (Luxembourg Institute of Science and Technology), l'IGSS (Inspection générale de la sécurité sociale) ou encore avec le Réseau d'étude sur le marché du travail et de l'emploi (RETEL).

Dans le domaine de la santé, la Commission nationale a continué à participer activement aux travaux de l'agence « e-santé », notamment en ce qui concerne la mise en œuvre depuis 2014 d'un « Data Protection Impact Assessment » dans le cadre du dossier de soins partagés (DSP). Le collège de la CNPD participe par ailleurs aux réunions du comité de pilotage de la Caisse National de Santé (CNS) et a rencontré des représentants du Luxembourg Institute of Health (LIH) en 2016.

2.4.2 Demandes de renseignements

La Commission nationale a reçu 430 demandes de renseignement par écrit en 2016, soit 90 de plus qu'en 2015. Dans la majorité des cas, il s'agissait de requêtes relatives aux formalités à accomplir pour mettre en œuvre un traitement de données ou de questions juridiques relatives à la législation.

Plus que la moitié des demandes émanaient d'entreprises. Les autres provenaient de citoyens, d'administrations publiques et d'avocats qui s'adressent aussi régulièrement à la Commission nationale.

2.5 Coopération avec les instituts de recherche luxembourgeois

2.5.1.1 Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg

En 2011, la Commission nationale et le Centre Interdisciplinaire pour la Sécurité, la Fiabilité et la Confiance (SnT) de l'Université du Luxembourg ont lancé un programme commun de recherche intitulé « Legal issues in Data protection, Cloud Computing and Privacy ».
La coopération se base sur trois principaux domaines d'analyse :

- les nouveaux développements de la législation européenne en matière de protection des données ;
- les défis technologiques tels que le cloud computing et leurs répercussions pour les acteurs publics et privés du site luxembourgeois ;
- le concept de « privacy by design », qui garantit que la protection de la vie privée est intégrée dans les nouvelles pratiques technologiques et commerciales dès leur conception, au lieu de les ajouter ultérieurement sous forme de compléments.

Le programme de recherche commun répond à des questions fondamentales de la protection des données dans un environnement technologique moderne.
Les résultats contribueront à sensibiliser le public et aideront à définir des solutions « made in Luxembourg » qui pourront servir d'exemples pour faire face aux nouveaux défis dans ce domaine dès le début.

Dans le cadre de cette coopération, le SnT et la CNPD ont cofinancé un poste pour une chercheuse postdoctorale qui a effectué des recherches, contribué à organiser des séminaires et conférences et rédigé des publications comme l'article.

- Roles and Powers of National Data Protection Authorities - Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency? par Dr. Andra Giurgiu et Mme Tine A. Larsen[3]
- The General Data Protection Regulation: a new opportunity and challenge for the banking sector par Dr. Andra Giurgiu et M. Thierry Lallemang[4]

2.5.1.2 LIST RegTech

Depuis 2016, la CNPD et le LIST (Luxembourg Institute of Science and Technology) collaborent sur un projet de recherche RechTech (Regulatory Technology) dans le cadre du nouveau règlement général sur la protection des données (RGPD).

Dans une première phase, l'objectif est de mettre à disposition des organisations un outil d'aide à la mise en conformité qui leur permet de s'autoévaluer par rapport aux exigences du RGPD. Cet outil contient un questionnaire enrichi et donnera la possibilité aux différentes entités d'associer des preuves aux exigences (démontrer l'exercice de leur responsabilité) et de gérer un registre des traitements.

Dans une deuxième phase, le but est d'adapter le contenu de l'outil à des contextes sectoriels (finances, santé, ressources humaines, etc.).

Dans une troisième phase, la CNPD est le LIST veulent intégrer à cet outil la mise en œuvre d'une analyse d'impact relative à la protection des données.

2.6 Travail au niveau international

L'activité de la Commission nationale a également été marquée par une forte participation aux travaux européens, dominés par des dossiers complexes et technologiques. Cet engagement a été nécessaire pour appréhender la matière dans toute son envergure et sa complexité.

La Commission nationale, représentée par un ou plusieurs de ses membres, a participé en 2016 à 61 réunions et à différents groupes de travail au niveau européen. Il s'agissait notamment :

- du groupe de travail « Article 29 » (établi en vertu de l'article

[3] European Data Protection Law Review Volume 2 (2016), Issue 3, Page 342 - 352.
[4] Wolters Kluwer – ACE Comptabilité, fiscalité, audit, droit des affaires au Luxembourg.

29 de la directive 95/46/CE), qui regroupe toutes les autorités européennes ainsi que le Contrôleur européen à la protection des données (CEPD). Dans ce cadre, la Commission nationale a participé aux sous-groupes suivants :

- « Technology » ;
- « International Transfers » ;
- « Future of Privacy » ;
- « Financial matters » ;
- « Key provisions » ;
- « Cooperation » ;
- « e-Government » ;
- « Border, Travel and Law Enforcement » ;

- du « Groupe de Berlin », dédié à la protection des données dans le secteur des communications électroniques ;
- du groupe de travail international sur l'Education au numérique;
- de la conférence de printemps des commissaires européens à la protection des données à Budapest ;
- de la conférence internationale des commissaires à la protection des données et de la vie privée à Marrakesch.

Par ailleurs, les membres de l'autorité de contrôle de l'article 17 (comprenant deux membres de la CNPD) ont participé en alternance aux réunions des autorités conjointes de contrôle européennes d'Europol, du système d'information « Schengen », du système d'information européen des autorités douanières (CIS), du système d'information européen des visas (VIS) ainsi que du système d'information européen Eurodac.

2.6.1 Le groupe « Article 29 »

Le groupe de travail, institué par l'article 29 de la directive 95/46/CE sur la protection des données (ci-après le groupe « Article 29 » ou « G29 »), est un organe consultatif indépendant. L'objectif de cet organisme, réunissant l'ensemble des autorités nationales de protection des données à l'échelle européenne, est d'examiner les questions relatives à la protection des données et de promouvoir une application harmonisée de la directive dans les 28 États membres de l'Union européenne.

Le règlement général sur la protection des données et la directive en matière de police et justice vont modifier considérablement la structure actuelle et la manière de travailler du Groupe « Article 29 ». Le 25 mai 2018, le Comité européen

de la protection des données (« European data protection board ») remplacera le Groupe de l'article 29 et deviendra un organe de l'UE qui possède la personnalité juridique. Il sera composé des autorités nationales et du Contrôleur européen à la protection des données.

Parmi les sujets traités par le groupe de travail en 2016, citons :

- la mise en œuvre du nouveau règlement européen en matière de protection des données ;
- les conséquences de l'arrêt Schrems sur le Safe Harbor et l'adoption du Privacy Shield[5] ;
- la refonte de la directive « e-Privacy » ;
- l'accord FATCA (Foreign Account Tax Compliance Act) ;
- la directive MIFID II (Markets in Financial Instruments Directive) ;
- la portabilité des données ;
- l'amélioration de la coopération européenne et internationale entre autorités de protection des données ;
- les pouvoirs des autorités de protection des données dans les clauses contractuelles types et décisions d'adéquation.

Les principaux documents de travail de 2016 du groupe sont résumés ci-dessous et peuvent être téléchargés dans leur version complète sur Internet[6].

2.6.1.1 Plan d'action concernant l'implémentation du règlement européen sur la protection des données

Le 2 février 2016, le groupe de travail a présenté son plan d'action relatif à l'implémentation du règlement européen sur la protection des données. Il s'est donné comme objectif de développer des lignes directrices, des outils et des procédures pour se préparer au nouveau cadre légal qui entrera en vigueur au premier semestre 2018.

Dans son plan d'action pour l'année 2016, le G29 a fixé ses priorités concernant la transition vers le nouveau cadre juridique et la création de l'European Data Protection Board (EDPB).

Un nouveau modèle de gouvernance

Le nouveau modèle de gouvernance prévoit un rôle plus important pour les autorités de protection des données. Le modèle repose sur trois piliers : les autorités de protection des données nationales, une meilleure coopération entre les autorités et au niveau de l'EDPB pour assurer la cohérence. Le G29 souhaite anticiper cette nouvelle organisation autant que possible.

Les grandes lignes du plan d'action

Le plan est basé sur quatre priorités :

1. La mise en place de la structure administrative du EDPB (p.ex. informatique, ressources humaines, budget, etc.)
2. La préparation du « guichet unique » (« one stop shop ») et du « consistency mechanism »
3. La guidance des responsables de traitement et des sous-traitants
4. La communication relative au nouveau règlement/EDPB

2.6.1.2 Publication de données à caractère personnel dans le secteur public à des fins de transparence

Le 8 juin 2016, le G29 a adopté un avis dans lequel il explique comment appliquer les principes de protection des données à la publication de données personnelles à des fins de transparence dans le secteur public, en particulier en relation avec des mesures anti-corruption et avec la prévention de conflits d'intérêt.

Il est obligatoire pour certaines autorités publiques de rassembler, d'enregistrer et de conserver les informations sur leurs activités et leurs employés et de rendre

[5] Voir partie 3.2. pour plus de détails.
[6] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/

ces informations disponibles publiquement (souvent via leur site Internet officiel). Ce traitement est susceptible de comporter des données à caractère personnel.

L'avis du G29 s'adresse aux autorités législatives nationales, gouvernements nationaux, bureaux, agences et autres institutions compétentes dans le secteur public susceptibles de publier ce type de données. Il contient des nombreuses recommandations, qui devraient permettre à ces institutions de trouver un équilibre entre le droit à la protection des données de ces individus et l'intérêt du public que ces individus accomplissent leurs fonctions et responsabilités de manière transparente et correcte.

2.6.1.3 Révision de la directive e-Privacy

Le 19 juillet 2016, le G29 a donné son avis sur l'évaluation et la révision de la directive e-Privacy. Cette révision avait été annoncée

par la Commission européenne dans le cadre du lancement de la stratégie pour un marché unique numérique le 6 mai 2015.

Vieille de de 14 ans, la directive e-Privacy ne répond plus entièrement aux enjeux actuels des communications électroniques. Une révision est devenue nécessaire suite au développement de l'économie numérique et à l'adoption récente du règlement général sur la protection des données (Règlement 2016/679).

Cette révision devra permettre d'adapter la directive à l'ère numérique et d'assurer un haut niveau de protection aux citoyens et des conditions de concurrence équitables aux entreprises. Le nouveau cadre juridique devra être complémentaire au règlement général sur la protection des données (RGPD) et assurer la sécurité juridique.

Dans son avis, le groupe de travail a fait des recommandations concernant

- le champ d'application de la directive,
- la confidentialité des communications électroniques,
- la protection de la sécurité des communications électroniques,
- la suppression de certaines règles concernant les violations des données,
- l'harmonisation des dispositions concernant des communications non sollicitées,
- l'harmonisation des dispositions concernant les annuaires d'abonnées,
- l'identification de la ligne d'appel et
- l'application de la directive.

2.6.1.4 Lignes directrices et FAQ sur le droit à la portabilité, les délégués à la protection des données et l'autorité chef de file

Le G29 a adopté plusieurs lignes directrices et FAQ (Foires aux questions) concernant le nouveau règlement européen à l'attention des responsables du traitement et sous-traitants lors de sa séance plénière des 12 et 13 décembre 2016.

Les lignes directrices concernent le droit à la portabilité, le délégué à la protection des données personnelles ainsi que l'autorité chef de file.

L'élaboration de ces lignes directrices s'est faite en étroite collaboration avec les parties prenantes à travers, notamment, l'organisation d'un Fablab en juillet 2016 et les consultations effectuées par certaines autorités.

Le G29 a proposé de recueillir tout commentaire complémentaire que les acteurs économiques ou la société civile souhaiteraient apporter aux lignes directives adoptées jusqu'en février 2017.

Les lignes directrices sur les évaluations d'impact sur la vie privée et la certification seront finalisées en 2017.

2.6.2 Le « Groupe de Berlin »

Le Groupe de travail international sur la protection des données dans les télécommunications, mieux connu sous le nom de « Groupe de Berlin », se penche surtout sur la problématique de la protection de la vie privée dans les services de télécommunications et sur Internet.

Lors de deux réunions en 2016 à Oslo et à Berlin, le groupe a adopté des documents de travail sur :

- les questions de sécurité et de vie privée dans le cadre des services de téléphonie par l'Internet (VoIP) et d'autres technologies de communication liées et
- la biométrie et l'authentification en ligne.

Ces documents peuvent être téléchargés sur le site Internet du groupe de travail[7].

[7] http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

Les activités en 2016

2.6.2.1 *Services de téléphonie par Internet et autres technologies de communication liées*

Le Groupe de Berlin a adopté une mise à jour du document de travail sur les questions de sécurité et de vie privée dans le cadre des services de téléphonie par l'Internet (VoIP) et d'autres technologies de communication liées lors de la réunion à Oslo les 24 et 25 avril 2016.

Le document de travail contient des recommandations pour améliorer la protection de la vie privée et la sécurité dans ces services. Le groupe s'adresse aux législateurs, régulateurs, fournisseurs VoIP, développeurs de logiciels, fabricants de matériel informatique et utilisateurs. Les recommandations sont applicables à tous les services multimédias offerts par les fournisseurs de télécommunications.

Ce document de 2006 a été mis à jour en raison des nombreux développements qui ont eu lieu entretemps. Cela inclut l'étendue de l'accès des autorités

policières et services secrets révélée par Edward Snowden, les progrès concernant les systèmes de normalisation, le développement rapide des réseaux de radiotéléphonie cellulaire et des réseaux Wi-Fi.

2.6.2.2 Biométrie et identification en ligne

Le groupe de travail a adopté un document sur la biométrie et l'identification en ligne lors de la réunion à Berlin les 22 et 23 novembre 2016.

La gestion des identités et des accès aux systèmes informatiques est primordiale pour assurer la sécurité et la fonctionnalité de ces systèmes. Afin de protéger la vie privée et la sécurité des données, le contrôle des accès est nécessaire pour assurer que les bons utilisateurs puissent accéder aux systèmes informatiques et aux données personnelles qui y sont sauvegardées.

De nombreux services en ligne ont commencé à remplacer les mots de passe comme moyen d'authentification par des solutions d'authentification multi-facteurs, comme les mots de passe à usage unique (Token), les « Trusted Devices » (p.ex. smartcards) ou encore la biométrie.

L'utilisation de la biométrie pour l'authentification en ligne est une possibilité pour remédier aux manquements de l'authentification par mot de passe. Toutefois, il faut prendre en compte les risques en matière de protection des données qui découlent de son utilisation.

L'objectif du document de travail n'est toutefois pas de spécifier quand la biométrie peut être utilisée dans l'authentification en ligne. Cette décision devrait être documentée dans un PIA (Privacy Impact Assessment) lors de la phase de conception du projet et mise à jour tout au long du cycle de vie du système informatique.

Le groupe de travail a analysé les risques en matière de vie privée lorsque la biométrie est introduite et utilisée dans l'authentification et comment ces risques peuvent être minimisées de manière appropriée. En conclusion, le groupe a formulé des recommandations à l'attention des régulateurs, législateurs et utilisateurs.

2.6.3 Le groupe de travail international sur l'Education au numérique

Depuis 2015, la CNPD fait partie du groupe de travail international sur l'Education au numérique. Ce groupe compte actuellement 52 autorités de protection des données, membres actifs et observateurs.

Ce groupe de travail a adopté le premier référentiel de formation des élèves à la protection des données personnelles en octobre 2016 lors de la Conférence internationale des commissaires de la protection des données à Marrakech.

Il s'agit d'un outil de formation pratique pour promouvoir l'éducation à la protection des données dans les programmes scolaires. Le document développe en neuf domaines structurants les composantes clé de la protection des données dont la connaissance et la compréhension sont considérées comme prioritaires :

1. Les données personnelles
2. Vie privée, libertés fondamentales et protection des données personnelles
3. Comprendre l'environnement numérique – au plan technique
4. Comprendre l'environnement numérique – au plan économique
5. Appréhender la régulation des données personnelles, connaître la loi
6. Appréhender la régulation des données personnelles : maîtriser l'usage des données personnelles
7. Maîtriser mes données : apprendre à exercer mes droits

8. Maîtriser mes données : apprendre à me protéger en ligne

9. Agir dans le monde numérique : devenir un citoyen numérique

Chaque domaine permet l'identification d'un bloc de compétences générales. Leur juxtaposition et enchaînement respectent un équilibre thématique progressif. Les éducateurs pourront s'en saisir, soit en suivant la logique structurante proposée, soit, au choix, en sélectionnant tel ou tel module, selon le programme scolaire à suivre, la discipline d'enseignement et la démarche pédagogique qui leur est propre.

Ce socle commun de savoirs et d'aptitudes pratiques constitue la première étape d'une démarche visant à diffuser et à promouvoir l'acquisition de compétences numériques dans les programmes d'éducation.

2.6.4 Conférence de printemps des autorités européennes à la protection des données

L'autorité de protection des données de Hongrie (NAIH) a organisé la Conférence européenne des autorités de protection des données à Budapest les 26 et 27 mai 2016.

Plus de 100 experts européens s'étaient réunis pour cette « Spring conference » dont le sujet principal était la réforme européenne en matière de protection des données.

Le président de l'autorité hongroise, Dr. Attila Péterfalvi, a tenu le discours ouverture dans lequel il a mis l'accent sur l'importance d'une bonne coopération entre les autorités de protection des données européennes. M. Giuseppe Busia de l'autorité italienne a souligné le fait que le nouveau règlement a deux caractéristiques principales : son applicabilité directe et la capacité de créer des règles uniformes pour toute l'Union européenne. M. Giovanni Buttarelli, Contrôleur européen de la protection des données, a analysé les effets que le nouveau règlement aura en pratique.

Ces discours ont été suivis de sessions sur les sujets suivants :

- Session 1 : « Respect for data protection by the national security bodies »
- Session 2 : « GDPR - what next ? Practical implications for national legislators, DPAs, data controllers »
- Session 3 : « Modernisation of Convention No. 108 – the expectations of non-EU member states »
- Session 4 : roundtable of departing commissioners

- Session 5 : conference resolutions, reports and other organizational items

Des résolutions sur le contexte de la coopération entre les différentes autorités et sur les transferts internationaux de données à caractère personnel ont été adoptées.

La conférence de printemps de 2017 aura lieu en Chypre.

2.6.5 Conférence internationale des commissaires de la protection des données

L'autorité de protection des données du Maroc a organisé la 38ème Conférence internationale des commissaires de la protection des données et de la vie privée à Marrakech du 17 au 20 octobre 2016.

Les commissaires ont discuté des perspectives de renforcement de la coopération entre les acteurs de la protection des données et des possibilités d'ouverture de nouveaux territoires à la cause de la protection des données et de la vie privée.

Des résolutions relatives aux thèmes suivants ont été adoptées :

- résolution pour l'adoption d'un référentiel international d'éducation à la protection des données personnelles ;
- résolution sur le développement de nouveaux indicateurs de la protection des données ;
- résolution sur les défenseurs des droits de l'Homme.

3 Les temps forts de 2016

Les travaux de la Commission nationale ont été marqués par un certain nombre de dossiers, soit à l'ordre du jour par le contexte politique et/ou l'actualité, soit choisis du fait de l'importance de la thématique par rapport aux principes de la protection des données à caractère personnel.

3.1 Nouveau règlement général sur la protection des données

L'élément marquant de l'année 2016 demeure sans doute l'adoption par le Parlement Européen et le Conseil de l'Union européenne du règlement général sur la protection des données (règlement UE 2016/679). Ce nouveau règlement sera applicable à partir du 25 mai 2018 et tous les protagonistes dans le domaine de la protection des données, y compris la CNPD, se doivent d'adapter leur mode de fonctionnement à ces nouvelles obligations européennes.

La CNPD s'efforce à accompagner l'ensemble de ces acteurs dans leurs démarches de mise en conformité en proposant de nombreuses actions de sensibilisation. Ainsi, le site de la CNPD inclut désormais un dossier thématique dédié à la réforme. L'autorité de contrôle luxembourgeoise a aussi rapidement diffusé une fiche réflexe à l'attention des responsables du traitement et des sous-traitants comprenant les dix questions à se poser pour se préparer au nouveau règlement.

En octobre 2016, en collaboration avec le Service des médias et des communications (SMC), la CNPD a organisé une grande conférence d'information pour plus de 500 personnes sur les principaux changements du nouveau règlement général sur la protection des données. Cette conférence n'était que le point de départ le plus visible d'une stratégie globale d'information et de sensibilisation de l'ensemble des acteurs, ainsi que du grand public. Un mois après cette conférence, des séances d'information spécialisées sur l'impact du nouveau règlement dans certains secteurs clés de l'économie luxembourgeoise ont été organisées pour fournir une information plus ciblée aux intervenants les plus impactés par cette réforme. Ces séances ont aussi été l'occasion d'aborder des sujets plus spécifiques dans le cadre de sessions de questions/réponses. Le retour d'expérience par rapport à ces événements a permis à la CNPD d'élaborer des nouvelles actions de communication qui auront lieu en 2017 afin de continuer ce travail d'information et de sensibilisation.

En plus de cette action de sensibilisation au niveau national,

Mot de bienvenue de Madame Tine A. Larsen à la conférence d'octobre 2016.

la CNPD a activement collaboré, dans le cadre du groupe de travail de l'article 29, avec l'ensemble des autorités de régulation européennes, à l'élaboration de notes d'orientation de portée européenne sur les principaux sujets liés au règlement (délégué à la protection des données, portabilité des données …). Ces documents font l'objet d'une large diffusion sur le site web de la CNPD.

La CNPD se doit elle aussi d'évoluer et de s'adapter aux nouvelles missions qui lui seront dévolu dans le cadre du nouveau règlement. En effet, ce nouveau règlement est associé à un changement de paradigme. Le régime d'autorisations et de notifications a priori est presque entièrement remplacé par un régime de contrôle a posteriori renforcé.

Comme pour les entreprises affectées, la première démarche a été d'identifier les impacts généraux et spécifiques de cette réforme sur l'activité de la CNPD et sur son mode de fonctionnement. Suite à cette analyse, des groupes de travail ont été constitués pour élaborer un plan d'implémentation de la réforme pour que la CNPD soit prête en mai 2018 à assumer ses nouvelles fonctions.

En interne, plusieurs sujets font l'objet d'une attention particulière. Le premier concerne la création d'un service de contrôles et investigations. En effet, ce règlement érige le nouveau concept de responsabilité comme la pierre angulaire de la conformité aux principes liés à la protection des données. La CNPD aura comme mission principale de s'assurer que l'ensemble des acteurs dans ce domaine le respecte. Les contrôles et investigations deviendront à terme les principaux outils de vérification de cette conformité. Pour assurer efficacement ce rôle de supervision, la CNPD se doit

3 Les temps forts de 2016

Discours du Premier Ministre, Monsier Xavier Bettel, à la conférence d'octobre 2016.

de disposer d'outils de contrôle efficaces et efficients.

La réforme est aussi l'occasion de remettre à jour l'ensemble des procédures de la CNPD et y intégrer les nouveaux éléments instaurés par le règlement. Un des objectifs principaux du nouveau règlement est de renforcer les droits des personnes concernées et de faciliter les démarches pour faire respecter leurs droits. Par exemple, la CNPD a récemment introduit un formulaire de plainte disponible en ligne sur son site Internet[8]. Ce nouveau formulaire s'inscrit dans les démarches mises en œuvre par la CNPD dans ce domaine.

La coopération européenne entre les différentes autorités de contrôle et le futur Comité Européen de la Protection des Données est une des principales innovations de ce règlement.

En 2016, il y a eu de nombreuses réunions avec l'ensemble des autorités de contrôle européennes pour la mise en œuvre pratique de ce système de coopération tel que conçu dans le règlement. Concomitant à ces discussions au niveau européen, la CNPD élabore de nouvelles procédures internes qui intègrent ce nouveau volet de coopération européenne.

De manière générale, la CNPD a procédé en 2016 à une profonde réorganisation interne de ses services et de ses processus afin de mieux répondre aux nouveaux besoins et missions qui émergent avec la mise en œuvre de la réforme. Cette démarche sera poursuivie en 2017 et au-delà.

[8] https://cnpd.public.lu/fr/droits/faire-valoir/formulaire-plainte/index.html

De gauche à droite : Arnaud Constant, Georges Weiland, Thierry Lallemang, Tine A. Larsen, Herwig Hofmann, Mark D. Cole, Pascal Steichen, Héloïse Bock et Violaine Langlet.

Discours du Premier Ministre, Monsieur Xavier Bettel, à la conférence d'octobre 2016.

3.2 Transferts internationaux de données : conséquences de l'arrêt « Schrems » et adoption du « Privacy Shield »

Conséquences de l'arrêt « Schrems » et de l'annulation du « Safe Harbor »

Les 2 et 3 février 2016, la CNPD et ses homologues européens se sont réunis pour évaluer les conséquences de la décision de la CJUE du 6 octobre 2015 invalidant la décision « Safe Harbor »[9] sur les transferts internationaux de données depuis l'Europe vers les Etats-Unis d'Amérique.

Pour ce faire, le G29 (Groupe des autorités de protection des données européennes) a analysé le cadre légal américain et les pratiques des services de renseignement américains afin d'apprécier les conditions dans lesquelles le droit européen à la protection de la vie privée et des données ferait l'objet d'une ingérence injustifiée.

Afin d'avoir une compréhension claire et complète de la situation en Amérique et de son impact sur les transferts entre l'Europe et les Etats-Unis, le G29 a réalisé des auditions et entendu des personnes d'horizons divers originaires d'Europe ou des Etats-Unis : universitaires, entreprises, représentants de gouvernements, société civile.

Il a mené son évaluation à la lumière de la jurisprudence européenne sur les droits fondamentaux, qui fixe quatre garanties essentielles à respecter dans le cadre des activités de renseignement :

1. Les traitements doivent reposer sur des règles claires précises et compréhensibles : toute personne doit être informée du transfert de ses données et capable de comprendre ce qui en est fait ;

2. La proportionnalité au regard de la finalité poursuivie doit être démontrée : un équilibre doit être trouvé entre les finalités poursuivies par la collecte ou l'accès aux données (impératifs de sécurité publique) et les droits des individus ;

3. Un mécanisme de contrôle indépendant doit exister : il pourrait s'agir d'un juge ou de tout autre organe indépendant, dès lors qu'il a les capacités à mettre en œuvre les contrôles nécessaires.

4. Une possibilité de recours effectif doit être offerte aux citoyens : tout individu doit être en mesure de défendre ses droits devant un organe indépendant.

[9] Voir le rapport annuel 2015 de la CNPD, p. 71 et s.

Le G29 a relevé que ces quatre garanties doivent être respectées dès lors que des données personnelles sont transférées depuis l'Europe vers les Etats-Unis, mais aussi vers d'autres pays tiers. Ces garanties doivent également être respectées par les pays membres de l'Union Européenne.

A la lumière de son analyse, le G29 a reconnu les efforts faits par les Etats-Unis en 2014 et 2015 pour améliorer la protection des données des personnes non-américaines. Néanmoins, des préoccupations demeuraient quant au cadre légal américain actuel, au regard des quatre garanties, notamment celles portant sur le périmètre d'accès aux données et les possibilités de recours.

Négociation du « Privacy Shield »

Afin de remplacer la décision « Safe Harbor » invalidée par la CJUE le 6 octobre 2015, et de mettre fin à l'incertitude juridique découlant de cette décision, la Commission européenne a négocié avec ses homologues américains un nouveau mécanisme juridique, le « Privacy Shield », destiné à renforcer le niveau de protection des données transférées depuis l'Union européenne vers les Etats-Unis d'Amérique.

Dans un premier temps, la Commission Européenne a émis un projet de décision d'adéquation sur le « Privacy Shield » le 29 février 2016. Le G29 a publié son avis par rapport à ce projet le 13 avril 2016.

Le G29 a mené son analyse à la lumière du cadre juridique européen applicable en matière de protection des données (Directive 95/46/EC), ainsi que des droits fondamentaux à la vie privée et à la protection des données garantis tant par la Convention européenne des droits de l'Homme (Article 8) que par la Charte des droits fondamentaux de l'Union européenne (Articles 7 et 8).

L'objectif de cette analyse consistait à s'assurer que les transferts de données personnelles qui seront réalisés dans le cadre du Privacy Shield respectent un niveau de protection « essentiellement équivalent » aux exigences européennes, pour reprendre l'expression utilisée par la Cour de justice de l'Union européenne dans l'arrêt Schrems du 6 octobre 2015.

Le G29 a tout d'abord tenu à souligner les améliorations significatives apportées par le Privacy Shield par rapport à la décision Safe Harbor de 2001, portant notamment sur l'insertion de définitions clés, mais aussi sur les mécanismes mis en place pour assurer le contrôle du respect des principes garantis par le Privacy Shield et notamment les audits de conformité internes et externes.

Néanmoins, le G29 a fait part d'importantes préoccupations qui demeuraient en ce qui concerne le volet commercial du Privacy Shield, ainsi que l'accès par les autorités publiques aux données transférées dans le cadre de l'accord Privacy Shield.

En conclusion, le G29 a constaté certaines améliorations apportées par le Privacy Shield par rapport au Safe Harbor. Cependant, il a demandé à la Commission européenne de répondre aux sérieuses préoccupations exprimées et d'apporter les précisions nécessaires afin d'améliorer le projet de décision d'adéquation et de garantir un niveau de protection des données personnelles essentiellement équivalent au niveau exigé par l'Union européenne.

Faisant suite à ces préoccupations, la Commission européenne a adopté le 12 juillet 2016, la décision relative au bouclier de protection des données UE-Etats-Unis, dite « Privacy Shield ».

Adoption du « Privacy Shield »

Dans sa décision d'adéquation du 12 juillet 2016, la Commission européenne a tenu compte de l'avis du G29 du 13 avril 2016, mais également

du point de vue du Contrôleur européen de la protection des données (CEPD) et de la résolution du Parlement européen, pour apporter un certain nombre de clarifications et d'améliorations au précédent projet de décision d'adéquation sur le « Privacy Shield ».

La Commission européenne et les États-Unis se sont notamment mis d'accord sur de nouvelles précisions concernant la collecte de données en vrac, sur le renforcement du mécanisme de médiation et sur des obligations plus explicites pour les entreprises en ce qui concerne les limites applicables à la conservation et au transfert ultérieur des données.

Selon la Commission européenne, le « Privacy Shield » est fondé sur les principes suivants :

- **des obligations strictes pour les entreprises qui traitent des données :** le ministère américain du commerce procédera régulièrement à des mises à jour et à des réexamens concernant les entreprises participantes. Les entreprises dont la pratique ne sera pas conforme s'exposeront à des sanctions et à une radiation de la liste des entreprises adhérant au dispositif ;

- **un accès des pouvoirs publics américains soumis à des conditions claires et à des obligations de transparence.** De plus, tous les citoyens de l'Union bénéficieront pour la première fois de mécanismes de recours dans ce domaine ;

- **une protection effective des droits individuels:** tout citoyen estimant que les données le concernant ont fait l'objet d'une utilisation abusive dans ce nouveau cadre bénéficiera de plusieurs mécanismes accessibles et abordables de règlement des litiges. L'intéressé pourra également **s'adresser à son autorité nationale de protection des données**, qui collaborera avec la commission fédérale du commerce pour que les plaintes déposées par les citoyens de l'Union soient examinées et réglées. Lorsqu'un litige n'aura pas été réglé par l'un de ces moyens, un mécanisme d'arbitrage sera disponible, en dernier ressort. La possibilité d'un recours dans le domaine de la sécurité nationale ouvert aux citoyens de l'UE passera par un **médiateur indépendant** des services de renseignement des Etats-Unis ;

- **un mécanisme de réexamen annuel conjoint:** ce mécanisme permettra de contrôler le fonctionnement du bouclier de protection des données et sera mené par la Commission européenne et le ministère américain du commerce, lesquels y associeront des experts nationaux du renseignement

travaillant au sein des autorités américaines et européennes de protection des données. La Commission européenne adressera un rapport public au Parlement européen et au Conseil.

Prochaines étapes

Suite à l'adoption du Privacy Shield et conformément à la décision de la CJUE d'octobre 2015 et à l'avis du 13 avril 2016, le G29 s'est engagé à :

- aider les personnes concernées à exercer leurs droits dans le cadre du Privacy Shield, en particulier dans le cadre de la gestion de leurs plaintes ;
- informer les responsables de traitement sur leurs obligations dans le cadre du Privacy Shield ;
- publier un guide informatif à destination des citoyens ;
- proposer des suggestions relatives à la composition de l'organe européen de centralisation des plaintes (EU centralized body) et à l'organisation pratique de l'évaluation conjointe.

Le G29 a poursuivi son travail relatif aux modalités de mise en œuvre du Privacy Shield au cours de l'année 2016 :

- Il a adopté des supports d'information spécifiques à destination des individus et des entreprises. Ces outils ont été publiés sur le site du G29 et de la CNPD ;
- Il a auditionné une délégation américaine composée de représentants du ministère du commerce des Etats-Unis et de la FTC (Commission Fédérale du Commerce), des services de renseignement ainsi que du médiateur (ombudsperson) ;
- Il a confirmé assurer la responsabilité de l'organe européen de centralisation des plaintes (EU centralized body) relatives au transfert de données de citoyens européens vers les Etats-Unis à des fins de sécurité nationale.

La CNPD a participé à l'effort d'information des citoyens et des entreprises au sujet du mécanisme du « Privacy Shield », notamment en intervenant à des conférences sur le sujet, ou en publiant sur son site Internet une page dédiée à la matière[10].

Enfin, la première évaluation annuelle conjointe du Privacy Shield par la Commission européenne en collaboration avec le G29 et le ministère américain du Commerce, en septembre 2017, sera un moment clé permettant d'évaluer la robustesse et l'effectivité des garanties prévues par le Privacy Shield. La compétence des autorités de protection des données impliquées dans cette évaluation devra donc être clairement définie.

Plus particulièrement, tous les membres de l'équipe d'évaluation doivent pouvoir accéder directement à toutes les informations nécessaires à celle-ci, y compris aux éléments permettant d'évaluer la proportionnalité de la collecte et de l'accès des autorités publiques américaines aux données transférées dans le cadre du Privacy Shield.

Lors de leur participation à la procédure d'évaluation, les représentants du G29 détermineront non seulement si des préoccupations demeurent, mais également si les garanties proposées dans le cadre du Privacy Shield sont effectives.

[10] https://cnpd.public.lu/fr/dossiers-thematiques/caractere-sensible/transf-internati/privacy-shield/index.htm

4 Perspectives

Nous vivons aujourd'hui dans un monde ultra connecté dans lequel la masse de données collectées ne cesse d'augmenter. Selon une étude du STATEC[11], quasiment tous les ménages résidents (97%) avaient un accès internet chez eux en 2016. 95% des internautes se connectaient tous les jours ou presque, le plus souvent via leur smartphone (83%).

Seuls 8% des internautes au Luxembourg n'ont pas communiqué d'informations personnelles sur Internet[12] en 2016. Les informations les plus fréquemment communiquées sur le net sont des renseignements personnels (nom, date de naissance, numéro de carte d'identité) et les moyens de contacts (adresse postale ou email, numéro de téléphone). D'autres informations telles que des photos, des renseignements sur la santé, le revenu, l'emploi ou encore sur la localisation sont moins fréquentes, mais ont néanmoins été dévoilées en ligne par près de 4 internautes sur 10.

L'étude du STATEC décrit également ce que font les internautes pour gérer l'accès à leurs informations personnelles sur Internet :

- 43% déclarent avoir lu les clauses relatives à la politique de confidentialité avant d'avoir fourni des informations personnelles ;
- 63% ont restreint l'accès à leur localisation géographique ;
- 64% ont limité l'accès à leur profil ou contenu sur les réseaux sociaux ;
- 72% n'ont pas autorisé l'utilisation des données personnelles à des fins de publicité ;
- 66% ont vérifié la sécurité du site Internet sur lequel ils ont fourni des informations personnelles (en regardant par exemple s'il s'agit d'un site de type « https ») ;
- 21% ont demandé d'accéder à leurs informations personnelles détenues par des sites Internet ou des moteurs de recherche afin de les actualiser ou de les supprimer.

Selon l'étude, 76% des internautes sont au courant que les cookies (ou témoins de connexion) peuvent être utilisés pour retracer leurs mouvements sur Internet et créer un profil pour chaque utilisateur afin de leur proposer des publicités sur mesure. La majorité (54% des utilisateurs) ont déjà modifié les paramètres de leur navigateur Internet pour empêcher l'enregistrement de cookies. 20% des internautes utilisent même un logiciel anti-traçage limitant la capacité de tracer leurs activités sur Internet.

Cette étude montre que beaucoup d'internautes au Luxembourg sont

[11] Source : STATEC (enquête sur l'utilisation des TIC dans les ménages et par les particuliers 2016).
[12] Idem.

préoccupés par l'enregistrement de leurs activités en ligne et par les publicités sur mesure. Dans les prochaines années, cette prise de conscience devra être encore plus forte dans le monde des objets connectés. De plus en plus de données sont produites, collectées et analysées à travers des objets interconnectés tels que des montres, des jouets, des cafetières, des thermostats, des pèse-personnes, des caméras ou encore des maisons et voitures intelligentes. En même temps, le danger d'une utilisation abusive de la masse des données personnelles qui circulent et de la cybercriminalité augmente. Les annonces de failles de sécurité, fuites de données, attaques informatiques et violations de confidentialité se multiplient.

De nombreux secteurs de l'économie, allant notamment du transport à la santé et de la finance à l'énergie, cherchent à exploiter le potentiel de la collecte de données massives, qui inclut de vastes volumes de données personnelles.

Dans le secteur financier, un des grands thèmes de 2017 sera la transposition et la modification de la « 4ème Directive Anti-Blanchiment »[13] et l'obligation pour les Etats-Membres d'établir un registre des bénéficiaires effectifs. La CNPD suivra également attentivement les travaux de transposition de « MIFID II »[14], notamment en ce qui concerne les obligations en matière de collecte et de conservation des données et des documents. Les changements du régime de secret professionnel dans le secteur financier, proposés par le projet de loi n°7024, notamment en ce qui concerne l'assouplissement des règles relatives à la sous-traitance, revêtent également une importance particulière en 2017. La CNPD rappelle que les responsables du traitement doivent s'assurer de la conformité de leur projet de sous-traitance non seulement avec la législation applicable au secteur financier, mais également avec la loi sur la protection des données.

Dans le domaine de la police et de la justice, le majeur défi sera la transposition pour le 6 mai 2018 de la directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale. Le projet de loi prévoit que la CNPD sera dorénavant compétente pour contrôler et vérifier le respect des dispositions de la loi transposant ladite directive. Ainsi, la majeure partie du domaine de compétence de l'autorité de contrôle « Article 17 », créée par l'actuelle loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, sera repris par la CNPD. De cette manière, la CNPD aura pour mission de superviser les traitements de données personnelles effectuées, entre-autres, par les juridictions de l'ordre judiciaire et de l'ordre administratif, par la Police grand-ducale et les Douanes, par les établissements pénitentiaires, par le Service de renseignement, ainsi que par l'Armée luxembourgeoise, lorsque ces autorités agissent à des fins pénales. De même, les traitements de données personnelles par les fonctionnaires des différentes administrations étatiques ayant la qualité d'officier de police judiciaire seront contrôlés par la CNPD lorsque ces derniers recherchent des infractions pénales.

Dans le domaine du transport, la directive réglementant l'utilisation dans l'UE des données des dossiers passagers (PNR) pour la prévention et la détection d'infractions terroristes et de formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, devra également être transposée en droit national. Elle impose aux transporteurs de fournir aux Etats membres de l'UE les données des passagers de vols internationaux à destination ou en provenance du territoire de l'UE.

Dans le secteur des communications électroniques, la Commission Européenne est en train d'adapter les règles issues de la directive « e-Privacy »[15]. Cette directive encadre le traitement des données de communications

[13] Directive 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme.
[14] Directive 2014/65/UE du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE.
[15] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

électroniques, notamment l'utilisation des cookies. La Commission européenne a proposé de la remplacer par un règlement qui vise à actualiser les règles en vigueur, en étendant leur champ d'application à l'ensemble des fournisseurs de services de communications électroniques, y compris les acteurs tels que Facebook ou Skype. Il vise également à créer de nouvelles possibilités de traiter des données de communication et de renforcer la confiance et la sécurité dans le marché unique numérique. Parallèlement, la proposition vise à harmoniser les règles applicables aux communications électroniques avec les nouvelles normes fixées dans le règlement général sur la protection des données.

Les dossiers mentionnés ci-dessus représentent seulement une sélection des travaux auxquels la CNPD devra faire face dans les prochaines années. Le plus grand chantier reste toutefois la préparation au nouveau règlement général sur la protection des données, le texte qui va encadrer l'utilisation des données à caractère personnel des citoyens européens par les entreprises, administrations et associations à partir du 25 mai 2018. Cette nouvelle législation vise à créer un ensemble de règles uniformes à travers l'UE adaptées à l'ère numérique, à améliorer la sécurité juridique et à renforcer la confiance des citoyens et entreprises dans le marché unique du numérique. En 2017, la CNPD va poursuivre sa politique de sensibilisation des acteurs et des citoyens y compris les plus jeunes pour les informer et les préparer à la prochaine mise en application du nouveau règlement européen sur la protection des données. Pour s'assurer de la plus large diffusion de l'information sur ce sujet, la CNPD utilisera l'ensemble des canaux de diffusion actuellement disponibles.

Pour accompagner cette évolution majeure, la CNPD travaille sur une refonte complète de son site internet afin de proposer à l'ensemble des utilisateurs une expérience de navigation en adéquation avec leurs nouveaux besoins. Ainsi, certaines sections actuelles du site comme celles concernant les notifications sont vouées à disparaître, alors que d'autres activités comme la gestion des déclarations des violations de données augmenteront en importance.

Des brochures d'information pour les professionnels du secteur, ainsi que pour le grand-public sont aussi en cours d'élaboration. La mise en application prochaine des nouveaux principes et règles édictées par le règlement européen constitue l'opportunité pour une remise à jour complète des documents existants.

Fort du succès de la grande conférence en octobre 2016 et des séances d'information

spécifiques du mois de novembre 2016, la CNPD va continuer à proposer et à participer à des séminaires d'information, des débats et workshops sur ce sujet. Ainsi, à l'approche de la date fatidique de la mise en application du règlement européen, un événement dédié à l'information du grand public sera organisé pour s'assurer de la bonne diffusion de l'information relative aux nouveaux droits offerts aux citoyens par ce règlement européen. Une attention particulière sera aussi donnée aux futurs délégués à la protection des données qui sont amenés à assumer un rôle essentiel dans la mise en œuvre par les responsables du traitement ainsi que les sous-traitants de la conformité aux principes du règlement.

Avec la mise en application du nouveau règlement européen, la loi actuelle sera abrogée et remplacée par un nouveau texte légal. En effet, le règlement européen requiert qu'au niveau national, un texte de loi régisse les statuts et le fonctionnement de la CNPD. Ce règlement européen a aussi la particularité d'offrir aux Etats membres de nombreuses possibilités de dérogation dans certains domaines spécifiques comme la recherche ou la liberté d'expression. L'ensemble de ces mesures doivent être promulgués en droit national avant l'entrée en application des dispositions du nouveau règlement en mai 2018.

Conformément aux missions qui lui seront attribuées par la nouvelle loi organique, la CNPD émettra son avis en accord avec la procédure législative nationale. Suite au vote de ce volet national, la CNPD s'appliquera à assister l'ensemble des acteurs dans l'interprétation et la mise en application de ces nouvelles dispositions issues tant de la législation communautaire que de la législation nationale.

Comme déjà évoqué précédemment, l'activité de la CNPD va être profondément transformée par le règlement européen. Dans cet esprit, la CNPD continuera le travail d'adaptation de ses procédures et l'intégration du volet de coopération renforcée avec les autres autorités de contrôle européennes et le futur Comité Européen de la Protection des Données.

5 Ressources, structures et fonctionnement

5.1 Rapport de gestion relatif aux comptes de l'exercice 2016

Dépenses

Le total des frais de fonctionnement de l'établissement public au cours de l'exercice 2016 s'élevait à 2.162.430,24 €.
Ce chiffre constitue une augmentation de 14,18 % par rapport à l'exercice précédent. Bien qu'il ne dépasse pas les prévisions budgétaires originaires, il est tout de même supérieur à la dotation qui avait finalement été accordée en 2016 et qui était de 2.050.922 €.

Ce sont essentiellement les charges relatives au personnel permanent et temporaire qui ont augmentées sensiblement, sans pour autant dépasser les prévisions budgétaires estimées à 2.055.000 €. Cette position avait en effet été revue à la hausse en raison du surcroît permanent de travail, dont la CNPD témoigne depuis un certain moment. En 2016, la CNPD a pu engager un fonctionnaire juriste et un employé juriste à durée indéterminée pour renforcer le service juridique. En début de l'année, la CNPD a également eu recours aux services d'un expert-juriste externe qui assistera la CNPD pendant deux ans dans les travaux de préparation de la mise en application du nouveau Règlement européen sur la protection des données qui produira entièrement ses effets à partir du 25 mai 2018.

Les dépenses d'honoraires et frais d'experts et de prestataires externes s'élevaient à 22.484,95 €, ce qui constituait une nette augmentation par rapport à l'année précédente où les dépenses sur ce poste ne s'élevaient qu'à 10.549,82 €. Ceci est dû au fait que certaines décisions de la CNPD ont été contestées en justice. La CNPD a dû recourir aux services d'avocats externes pour se défendre. Les affaires ont finalement été décidées en faveur de la CNPD. Le restant de cette position avait été transféré sur la position des salaires sur laquelle l'expert-juriste avait également été payé. Parmi ces dépenses figuraient les honoraires d'avocats et de la fiduciaire qui tient la comptabilité et établit le bilan de l'établissement public.

Le montant des charges locatives pour le bâtiment administratif à Belval s'élevait à 13.876,16 €, c'est-à-dire le double du montant de l'année précédente où le montant ne s'élevait qu'à 6.881,74 € en 2015. La régularisation du montant en

2016 avait déjà été annoncée depuis un moment.

Les frais d'entretien des locaux, les frais de port et de télécommunications et autres charges générales d'exploitation ont connu une progression linéaire suivant l'augmentation du nombre de collaborateurs en activité.

Pour ce qui est des équipements et fournitures de bureau, les dépenses ont diminué de 54,55 % par rapport à l'année passée où la CNPD avait renouvelé une partie de ses équipements surannés (ordinateurs, écrans, imprimantes, serveurs et back-up). Les coûts se sont élevés à 25.809,44 € par rapport à 56.789,63 € en 2015.

Les frais de déplacement et de séjour à l'étranger se chiffraient à 39.529,20 €, une augmentation de 31,54 % par rapport à l'année précédente où les dépenses pour ce poste s'élevaient à 30.050,88 € et un dépassement de 12,94 % des prévisions budgétaires. Ce montant s'explique par les engagements de la CNPD à l'étranger. En effet, les frais de voyage, dans une large mesure incompressibles, se rapportent à la participation des membres effectifs et des collaborateurs de la Commission nationale aux réunions, séances de travail et conférences organisées sur le plan européen dans le domaine de la protection des données, où l'autorité luxembourgeoise ne peut pas faire la politique de la chaise vide et se doit d'être représentée. S'y ajoutaient en 2016 par ailleurs un nombre de voyages supplémentaires en raison de la collaboration soutenue de la CNPD à l'élaboration des positions stratégiques au niveau du groupe de travail de l'article 29 dans le cadre de la prochaine entrée en application du nouveau règlement européen sur la protection des données. Les frais de déplacement et de séjour pour les agents en formation externe sont également inclus dans cette somme.

Les frais de formation externe hors frais de déplacement et de séjour pour le personnel s'élevaient à 3.440,80 € en 2016 comparés à 2.828,52 € en 2015 et dépassaient dès lors les prévisions de 240,80 €. Ces frais vont évoluer davantage au cours des années à venir, étant donné que la CNPD apporte beaucoup d'attention à la formation de base, continue et linguistique de ses collaborateurs.

Les dépenses pour l'information du public et la communication s'élevaient à 13.589,30 €, ce qui est largement en-dessous des prévisions budgétaires de 25.000 € et même en-dessous du montant de 15.480,13 € dépensé en 2015. Ce résultat s'explique d'une part par le fait que certains des projets prévus sont restés en suspens et d'autre part, du fait qu'un certain nombre d'activités ont été exécutées en collaboration avec d'autres institutions qui ont pris en charge une partie des frais. Les dépenses pour la maintenance des systèmes et réseaux informatiques s'élevaient à 15.793,28 € ce qui ne correspond qu'à 65,66 % des prévisions budgétaires faites pour pouvoir continuer le renouvellement des équipements et débuter la digitalisation des services informatiques de la CNPD. Or, les projets ont été reportés afin de combler les lacunes de recettes sur les redevances et d'avoir la garantie d'être toujours en mesure de payer les salaires aux collaborateurs.

Les amortissements comptabilisés en 2016 atteignaient un montant total de 3.093,55 €, donc légèrement moins que l'année précédente où le montant s'élevait à 3.118,55 €. Ils concernaient pour l'essentiel le mobilier et les équipements informatiques, ainsi que les investissements relatifs au développement et à la mise en service de l'application informatique spécifique dédiée à l'établissement du registre

public des traitements prévu à l'article 15 de la loi, ainsi qu'à l'optimisation des procédures administratives.

Recettes

Le montant des redevances perçues en application des articles 37 paragraphe (4), 13 paragraphe (3) et 14 paragraphe (4) de la loi s'élevaient à 158.075 €, comparé à 130.075 € en 2015. Ce surplus constitue une augmentation de 17,71 % par rapport à l'année précédente, mais reste 36,77 % en-dessous des prévisions budgétaires tablées à 250.000 €. En outre, des produits financiers (intérêts créditeurs) ont été enregistrés à hauteur de 51,31 €.

S'y ajoute encore exceptionnellement aux recettes le montant de 40.000 € reçu par l'Université de Luxembourg dans le cadre du Partenariat que la CNPD entretient avec le Centre for Security, Liability and Trust de l'Université.

Résultat d'exploitation

Compte tenu de la dotation annuelle de 2.050.922 €, dont la Commission nationale a bénéficié en 2016 de la part de l'Etat en application de l'article 37 paragraphe (4) de la loi, le résultat d'exploitation de l'établissement public s'élève à 86.618,07 € au 31 décembre 2016.

Ressources, structures et fonctionnement

5.2 Personnel et services

Collège
Tine A. LARSEN,
présidente
Thierry LALLEMANG,
membre effectif
Georges WANTZ,
membre effectif

Membres suppléants
Josiane PAULY,
Ministère du Développement durable et des Infrastructures (Département des transports), direction de la circulation et de la sécurité routières
Marc HEMMERLING,
Association des Banques et Banquiers Luxembourg (ABBL), membre du comité de direction
François THILL,
Ministère de l'Économie, direction du commerce électronique et de la sécurité de l'information

Secrétariat, administration générale et finances
Tessy PATER,
rédacteur
Serge FERBER,
employé de l'Etat
Anna MAGI,
employée de l'Etat

Service communication et documentation
Tom KAYSER,
attaché

Service juridique
Georges WEILAND,
attaché
Michel SINNER,
attaché
Christian WELTER,
attaché
Laurent MAGNUS,
employé de l'Etat
Arnaud HABRAN,
employé de l'Etat
Mickaël TOME,
employé de l'Etat
Mathilde STENERSEN,
employée de l'Etat
Danielle JEITZ,
attachée

Tenue du registre public et prise en charge administrative des notifications et demandes d'autorisation
Marc MOSTERT,
rédacteur
Stéphanie MATHIEU,
rédacteur

Service informatique et de la logistique
Alain HERRMANN,
chargé d'études
Michèle FELTZ,
chargée d'études

Experts associés ponctuellement
Andra GIURGIU,
chercheuse SnT
Guillaume BYK,
support Task force Réforme

De gauche à droite : Tessy Pater, Serge Ferber, Arnaud Habran, Anna Magi, Laurent Magnus, Tine A. Larsen, Alain Herrmann, Andra Giurgiu, Christian Welter, Georges Weiland, Thierry Lallemang, Michel Sinner, Georges Wantz, Tom Kayser, Michèle Feltz, Stéphanie Mathieu

5.3 Organigramme de la Commission nationale

Secrétariat
Serge FERBER
Anna MAGI

Collège
Tine A. LARSEN
Thierry LALLEMANG
Georges WANTZ

Administration générale, personnel, budget et finances
Tessy PATER

Communication et documentation
Tom KAYSER

Service juridique
Georges WEILAND, Michel SINNER
Christian WELTER, Laurent MAGNUS
Arnaud HABRAN, Mickaël TOME
Mathilde STENERSEN, Danielle JEITZ

Service informatique et logistique
Alain HERRMANN
Michèle FELTZ

Experts associés ponctuellement
Andra GIURGIU
Guillaume BYK

Notifications et autorisations préalables, chargés de la protection des données
Marc MOSTERT
Stéphanie MATHIEU

Guidance et investigations
(compostion ad hoc
juriste + informaticien)

6 La Commission nationale en chiffres

Formalités préalables

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	
a) Notifications											TOTAL 2003-2016
Notifications ordinaires	760	385	345	295	355	437	421	564	705	975	9.488
Notifications simplifiées	537	-	-	-	-	-	-	-	-	-	3.797
Engagements de conformité	-	942	227	15	46	149	651	45	19	28	2.122
(Total a 2003-2016)	1.297	1.327	572	310	401	586	1.072	609	724	1.003	15.407
b) Autorisations préalables											TOTAL 2003-2016
Demandes d'autorisation	392	606	542	607	604	706	833	914	969	1.338	9.294
Engagements de conformité	151	220	70	92	49	70	149	85	148	111	1.913
(Total b 2003-2016)	543	826	612	699	653	776	982	999	1.117	1.449	11.207
(Total général a + b 2003-2016)	1.840	2.153	1.184	1.009	1.054	1.362	2.054	1.608	1.841	2.452	26.614
Déclarants (responsables ayant accompli des formalités)	3.754	4.357	4.772	5.110	5.399	5.821	6.559	6.993	7.472	8.005	

Demandes de renseignements par écrit

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
(Total a 2003-2016)	148	138	138	213	173	273	274	416	340	430

Plaintes

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Plaintes et demandes de vérification de licéité	34	63	133	145	115	133	177	207	217	185

Séances de délibération

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
	40	40	37	38	35	27	31	20	39	32

Participations aux groupes de travail sur le plan européen

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
	22	22	32	40	37	43	39	40	47	61

Prises de contact et concertations avec des organisations représentatives sectorielles ou acteurs

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Secteur public	56	52	54	56	69	71	102	92	146	125
Secteur privé	40	44	52	54	71	61	75	77	106	73
(Total)	96	96	106	110	140	132	177	169	252	198

Séances d'information, conférences, exposés

	2007	2008	2009	2010	2011	2012	2013	2014	2015	206
	14	11	23	21	15	10	18	22	15	44

7 Annexes

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°6921 portant: 1) modification du Code d'instruction criminelle ; 2) modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; 3) adaptation de la procédure pénale face aux besoins liés à la menace terroriste

Délibération n°147/2016
du 12 février 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 du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après : « la Commission nationale » ou « la CNPD ») a notamment pour mission d'aviser « 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 ». Conformément à l'article 32 paragraphe (3) lettre (e) et (f) 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 du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission de présenter au gouvernement toutes suggestions susceptibles d'améliorer le cadre légal et d'aviser « *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 lettre du 4 décembre 2015, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n°6921 portant 1) modification du Code d'instruction criminelle ; 2) modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; 3) adaptation de la procédure pénale face aux besoins liés à la menace terroriste.

Ces dernières années, la lutte contre le terrorisme est devenue à la fois cruciale et plus difficile. L'émergence et l'évolution rapide des nouvelles technologies permettent l'utilisation de nouveaux outils de détection et de poursuite. Le projet de loi sous examen s'inscrit ainsi parmi des initiatives similaires des pays limitrophes[1], qui ont estimé nécessaire d'introduire de nouvelles mesures de surveillance pour combattre le terrorisme[2].

La Commission nationale constate que les moyens d'investigation

[1] Tels que la Belgique, La France, l'Allemagne et les Pays-Bas.
[2] La Cour européenne des droits de l'homme a également constaté la nécessité de mesures de surveillance secrète. Voir l'arrêt *Klass et autres c. Allemagne,* 6 septembre 1978, § 48, série A n°28.

proposés élargissent les pouvoirs du procureur d'Etat, du juge d'instruction et de la police judiciaire et facilitent la consultation, la conservation et l'utilisation d'une pléthore de données à caractère personnel. Ces mesures ont ainsi un impact considérable sur les droits fondamentaux des citoyens, notamment le droit à la vie privée et le droit à la protection des données à caractère personnel, consacrés dans l'article 8 de la Convention européenne des droits de l'homme et dans les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

Conformément à ces textes, une limitation de ces droits fondamentaux doit être prévue par la loi et les mesures doivent être nécessaires dans une société démocratique pour atteindre un but légitime. Il découle de la jurisprudence de la Cour européenne des droits de l'homme, ainsi que de celle de la Cour de justice de l'Union européenne qu'une telle ingérence doit impérativement être limitée à ce qui est strictement nécessaire dans une société démocratique[3]. Plus particulièrement, elle doit être proportionnée au but légitime poursuivi. Ceci implique que la loi doit établir des critères objectifs encadrant et limitant la collecte et l'utilisation des données à caractère personnel par les autorités répressives[4].

La loi doit en outre être accessible et suffisamment claire et précise pour permettre aux citoyens de savoir en quelles circonstances et sous quelles conditions ces mesures peuvent être mises en œuvre, ainsi que de connaître les conséquences éventuelles pour eux[5]. Il est nécessaire que la loi définisse avec une clarté suffisante l'étendue et les modalités d'exercice des pouvoirs conférés aux autorités compétentes, ainsi que les garanties aptes à protéger efficacement les données à caractère personnel[6].

De plus, l'exercice des pouvoirs doit être soumis à un contrôle par un organe indépendant, telle qu'une juridiction ou une autorité administrative indépendante, afin de limiter le risque d'abus[7]. D'après la Cour européenne des droits de l'homme, dans le cadre des mesures de surveillance, c'est « *en principe souhaitable que le contrôle soit confié à un juge en un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière* »[8].

Finalement, il faut que la loi prévoie des voies de recours pour les personnes ayant fait l'objet d'une mesure de surveillance[9]. En effet, en introduisant des mesures limitant les droits fondamentaux des citoyens, il faut obligatoirement qu'un juste équilibre soit ménagé entre le respect de ces droits et l'intérêt public de détecter et poursuivre les infractions pénales[10].

Dans ce sens, la Commission nationale s'interroge sur les circonstances dans lesquels ces nouveaux outils d'investigation pourront être mis en œuvre. Le projet de loi, qui s'inscrit dans le contexte des menaces et attentats terroristes récents dans nos pays voisins, décrit dans l'introduction de l'exposé des motifs la nécessité de mettre à jour la législation luxembourgeoise afin de pouvoir combattre efficacement le terrorisme. Or, le texte sous examen ne se limite pas à cet objectif unique. Il étend le champ d'application de l'article 24-1 aux « crimes flagrants » et introduit la mesure prévue à l'article 48-27 projeté à la poursuite de tous crimes et délits, peu importe qu'il s'agisse ou non d'actes de terrorisme. La Commission nationale regrette que l'objectif de faciliter, en général, la poursuite de tous crimes et délits n'est pas clairement séparé de l'objectif principal du projet de loi, qui est la mise en place de nouveaux moyens d'investigations pour lutter plus efficacement contre le terrorisme.

La Commission nationale note finalement qu'en décembre 2015, le Parlement européen et le Conseil sont arrivés à un accord informel sur le texte de la Directive relative à la protection des personnes physiques à

---

3 *Klass et autres c. Allemagne*, 6 septembre 1978, § 48, série A n°28 ; *S. et Marper c. Royaume-Uni* [GC], n°30562/04 et 30566/04, § 101, CEDH 2008-V ; *Szabo et Vissy c. Hongrie*, n°37138/14, § 53, 12 janvier 2016.

4 *Arrêt Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, point 39 ; Arrêt *Schrems*, C-362/14, EU:C:2015:650, point 94.

5 Voir entre autres : *Liberty et autres c. Royaume-Uni*, n°58243/00, § 59 - 62, 1 juillet 2008 et les jurisprudences citées ; *Zakharov c. Russie* [GC], n°47413/06, § 228-229, 4 décembre 2015.

6 Voir entre autres : *S. et Marper c. Royaume-Uni* [GC], n°30562/04 et 30566/04, § 95 et 103, CEDH 2008-V ; *Liberty et autres c. Royaume-Uni*, n°58243/00, § 59 - 62, 1 juillet 2008 et les jurisprudences citées ; *Zakharov c. Russie* [GC], n°47413/06, § 230-231, 4 décembre 2015 ; Arrêt *Schrems*, C-362/14, EU:C:2015:650, point 91 et jurisprudences citées.

7 *Klass et autres c. Allemagne*, 6 septembre 1978, § 51 - 57, série A n°28 ; *Szabo et Vissy c. Hongrie*, n°37138/14, § 77, 12 janvier 2016.

8 *Klass et autres c. Allemagne*, 6 septembre 1978, § 56, série A n°28. Voir aussi *Szabo et Vissy c. Hongrie*, n°37138/14, § 77, 12 janvier 2016 ; Arrêt *Schrems*, C-362/14, EU:C:2015:650, point 95.

9 Arrêt *Schrems*, C-362/14, EU:C:2015:650, point 94.

10 Voir notamment *S. et Marper c. Royaume-Uni* [GC], n°30562/04 et 30566/04, § 112, CEDH 2008-V.

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[11].

Le texte de compromis du projet de directive reprend les grands principes en matière de protection des données et y ajoute des obligations pour garantir que les données à caractère personnel soient protégées du début jusqu'à la fin de la procédure pénale. Le texte de compromis du projet de directive dispose que les Etats Membres doivent prévoir des délais pour l'effacement des données ou une révision périodique de la nécessité de conserver celles-ci[12], instaurer des principes de la protection des données dès la conception et de la protection des données par défaut *(data protection by design and data protection by default)*[13] et veiller à ce que des techniques de journalisation soient utilisées pour une série de traitements[14].

Au vu de ce qui précède, la Commission nationale tient à souligner l'importance de la conformité du présent projet de loi avec les principes régissant la protection des données en général et avec le texte de compromis du projet de directive en particulier.

Ci-dessous seront passés en revus les articles que le projet de loi sous avis propose d'ajouter à la législation luxembourgeoise ou de modifier.

1. La terminologie

A titre préliminaire, la Commission nationale constate que les termes utilisés dans le projet de loi ne correspondent pas à ceux figurant dans la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électronique (« loi du 30 mai 2005 »), qui transpose plusieurs directives européennes. En effet, dans le projet de loi, il est question d'« opérateurs et fournisseurs de communications électroniques » alors que la loi du 30 mai 2005 fait état d'opérateurs (de réseau) et de fournisseurs de services (de communications électroniques). De plus, la loi du 30 mai 2005 parle de communications électroniques et non de télécommunications.

La Commission nationale recommande dès lors d'aligner la terminologie du projet de loi (ainsi que celle des articles 24-1 et 67-1 actuels du Code d'instruction criminelle) sur celle d'ores et déjà utilisée dans la législation européenne et nationale.

[11] Directive 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, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de prévention de telles menaces, et à la libre circulation de ces données, 2012/0010 (COD), texte de compromis datant du 15 décembre 2015.
[12] Ibid., Article 4b et considérant 18.
[13] Ibid., Article 19.
[14] Ibid., Article 24.

2. Article 24-1 du Code d'instruction criminelle

Le projet de loi prévoit de permettre le repérage ou la localisation de communications électroniques en cas de crime flagrant avant qu'une instruction préparatoire ne soit ouverte.

Le projet de loi, en son état actuel, appelle les observations suivantes :

2.1. Les infractions visées

A l'avenir, l'article 24-1 du Code d'instruction criminelle permettra le repérage ou la localisation de communications électroniques « *pour les crimes flagrants* ». Il est sous-entendu que ces mesures pourront être ordonnées pour *tous* types de crimes.

Dans ce contexte, il y a lieu de rappeler que l'article 24-1 prévoit un accès aux données de communications conservées en vertu des articles 5 et 9 de la loi du 30 mai 2005.

Ce type de conservation des données de connexion de communications électroniques est au centre de l'arrêt de la Cour de justice de l'Union européenne (ci-après la CJUE) rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12.

Il résulte dudit arrêt[15] que l'accès par les autorités judiciaires à de telles données doit être délimité de manière très précise, notamment pour ce qui est des infractions permettant un tel accès. Il faudrait vérifier en détail quelles sont les infractions pour lesquelles la commission justifie cet accès eu égard à l'ampleur et à la gravité de l'ingérence dans les droits fondamentaux consacrés par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne.

Le projet de loi n°6763[16] a justement comme objectif de mettre la législation luxembourgeoise en conformité aux principes énoncés dans l'arrêt précité de la CJUE et à cette fin notamment d'établir une liste des infractions visées.

Afin que la charte des droits fondamentaux de l'Union européenne et l'arrêt de la CJUE du 8 avril 2014 soient respectés, il conviendrait d'établir d'abord ce catalogue d'infractions avant d'étendre les possibilités de repérage et traçage existantes à tous crimes flagrants.

2.2. La protection des personnes titulaires d'un secret professionnel et des journalistes

Le fait de pouvoir retracer toutes sortes de communications électroniques de quiconque permet de savoir quelles ont été les personnes ayant été en contact avec des personnes titulaires d'un secret professionnel, tels que les avocats, médecins etc., et avec les journalistes qui bénéficient d'une protection légale de leurs sources.

La législation luxembourgeoise ne prévoit aucune exception pour ce qui est des communications soumises au secret professionnel, ni au niveau de la conservation des données de communications (articles 5 et 9 de la loi du 30 mai 2005), ni au niveau de l'accès aux données par les autorités judiciaires (articles 24-1 et 67-1 du Code d'instruction criminelle).

Rappelons dans ce contexte que la directive 2006/24/CE a été déclarée invalide notamment en raison du fait qu'elle ne prévoyait « *aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel* ».

Par ailleurs, il se pose la question de savoir si le secret des sources des journalistes, qui a fait l'objet d'une jurisprudence abondante de la part de la Cour européenne des droits de l'homme, est suffisamment protégé.

Certes, la loi du 8 juin 2004 sur la liberté d'expression dans les médias prévoit la protection des sources des journalistes. On peut cependant se demander si cette protection satisfait aux exigences de la prédite jurisprudence de Strasbourg[17].

---

[15] Cf. notamment le considérant 60 de l'arrêt.

[16] Projet de loi n°6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

[17] Pour un cas de figure postérieur à la loi du 8 juin 2004: voir l'arrêt de la Cour européenne des droits de l'homme (Cinquième section) du 18 avril 2013 rendu dans l'affaire Saint-Paul Luxembourg S.A. c. Luxembourg, requête n°26419/10.

La Commission nationale a d'ailleurs rendu attentif le législateur à ces lacunes de la législation luxembourgeoise dans le contexte du projet de loi n°6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques[18].

En l'état, la Commission nationale estime que le texte du projet de loi ne répond pas aux exigences de la jurisprudence européenne.

2.3. Raison d'être de l'extension du champ d'application de l'article 24-1 alinéas 3 et suivants

Selon le commentaire des articles, l'extension projetée permettra un traçage ou une localisation à un stade très précoce des investigations. A l'heure actuelle, une instruction ne pourrait guère être ouverte, car *« le juge d'instruction ne pourra pas être saisi sur base d'un dossier d'enquête tant soit peu complet. »*

En ordonnant un traçage ou une localisation sur base de l'article 24-1, le juge d'instruction est toujours censé apprécier si la mesure est nécessaire à la manifestation de la vérité et rendre une ordonnance motivée indiquant les circonstances de l'espèce. La Commission nationale présume en effet que les conditions de l'67-1 sont également applicables à une mesure ordonnée sur base de l'article 24-1[19].

Si la Commission nationale a toujours insisté sur la nécessité d'une décision judiciaire en matière d'accès aux données de trafic de communications électroniques, encore faut-il que les conditions soient réunies pour que l'appréciation judiciaire fonctionne bien en pratique[20].

Il est très difficile d'apprécier, si, en l'espèce, les juges saisis seront toujours en mesure de bien apprécier en connaissance de cause, alors qu'ils sont censés trancher à un moment où le dossier de l'enquête est encore peu complet.

En ce qui concerne l'autre motif invoqué dans le commentaire des articles pour l'extension, à savoir la gestion de crise en cas de crime qui se poursuit comme par exemple en cas de prise d'otage, il concerne certainement seulement un petit pourcentage des affaires. Dès lors, une mesure ciblée pour ces cas de figure serait plus justifiée qu'une extension généralisée du champ d'application de l'article 24-1.

2.4. Conclusion

La Commission nationale ne rejette pas, a *priori*, l'idée d'une telle extension si, comme prévu en l'espèce, cette mesure ne se fait que sur ordonnance d'un juge d'instruction, que l'extension

[18] Avis n°214/2014 du 13 mai 2014 (Avis de la Commission nationale pour la protection des données quant à la conformité de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données dans le secteur des communications électroniques et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 pour la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication) ; Avis n°228/2015 du 19 juin 2015 (Avis de la Commission nationale pour la protection des données relatif au projet de loi n°6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques).

[19] L'avis de la Commission nationale n'a d'ailleurs pas été demandé lors de l'introduction des alinéas 3 et suivants de l'article 24-1 du Code d'instruction criminelle en 2014.

[20] Voir à ce sujet : Astrid Ackermann, « *Funktioniert der Richtervorbehalt?* », 26 août 2015. Disponible sur « https://www.datenschutzbeauftragter-info.de/funktioniert-der-richtervorbehalt/ ».

soit précédée par un catalogue d'infraction, limitée à des mesures ciblées et réponde aux exigences de la jurisprudence européenne.

3. Article 39 du Code d'instruction criminelle

La Commission nationale n'a pas d'observations à faire concernant cet article.

4. Article 48-26 du Code d'instruction criminelle

L'article 48-26 nouveau a pour objet d'introduire en droit luxembourgeois l'enquête sous pseudonyme.

4.1. Les personnes surveillées

L'article 48-26 du projet de loi prévoit la possibilité pour les officiers de police judiciaire de procéder à des enquêtes sous pseudonyme dans le but de constater des crimes et délits contre la sûreté de l'Etat ou des actes de terrorisme et de financement de terrorisme. Serait, par exemple, possible a) la participation sous un pseudonyme aux échanges électroniques, b) le contact, sous un pseudonyme, avec les personnes susceptible d'être les auteurs de ces infractions et c) l'extraction, l'acquisition ou la conservation par ce moyen des éléments de preuve et des données sur les personnes susceptibles d'être les auteurs des infractions.
Ces mesures permettraient en conséquence aux officiers de police judiciaire de s'intégrer dans des communautés virtuelles et ainsi recueillir de nombreuses informations sur des personnes présumées être les auteurs des infractions sur lesquelles porte l'enquête.

Par ailleurs, comme l'a souligné un arrêt de la cour constitutionnelle allemande sur la « *cyber-infiltration* » et la captation des données informatiques, non seulement les données de la personne surveillée peuvent être traitées, mais également celles de toutes les personnes avec qui la personne surveillée entre en contact[21]. Par exemple, en s'inscrivant à un forum de discussion, l'officier de police judiciaire pourra consulter les données à caractère personnel de chaque utilisateur du forum.

Rappelons que selon l'article 2 lettre (r) de la loi du 2 août 2002 et l'article 3(3) du texte de compromis du projet de directive, la simple consultation est considérée comme un traitement de données à caractère personnel. La consultation ou l'utilisation des données relatives à n'importe quel membre d'un forum de discussion constituerait dès lors un traitement de données à caractère personnel au sens de la loi et non seulement les données relatives aux personnes susceptibles d'être les auteurs de ces infractions. Or, conformément à l'article 4 paragraphe (1) lettre (b) de la loi du 2 août 2002, les données à caractère personnel doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées …* »[22].

La Commission nationale se rallie au groupe de travail « Article 29 » qui a souligné que le traitement des données à caractère personnel relatives aux personnes non soupçonnées d'avoir commis une infraction « *ne devrait être autorisé que dans certaines conditions spécifiques et pour autant qu'il soit absolument nécessaire à une finalité légitime, clairement définie et particulière* »[23].
Le traitement des données à caractère personnel relatives aux personnes non soupçonnées d'avoir commis une des infractions figurant dans l'article 48-26 du projet de loi devrait en conséquence se limiter à ce qui est strictement nécessaire.

Afin de limiter le traitement de ces données et d'assurer la conformité de l'article à la loi du 2 août 2002, la Commission nationale recommande au législateur de s'inspirer de l'article 48-17 paragraphe (5) du Code d'instruction criminelle relatif à l'infiltration et d'instaurer une obligation expresse pour l'officier de police judiciaire qui a effectué l'enquête de consigner dans son rapport seulement les données strictement nécessaires à la constatation des infractions et d'omettre toutes données à

[21] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. (1-333), § 297 *„Betroffen ist nicht nur derjenige, der den Anlass für die Überwachungsmaßnahme gegeben hat. Der Eingriff kann vielmehr eine gewisse Streubreite aufweisen, wenn Erkenntnisse nicht nur über das Kommunikationsverhalten desjenigen, gegen den sich die Maßnahme richtet, sondern auch über seine Kommunikationspartner gewonnen werden.".*

[22] Cette condition est reprise dans l'article 4 paragraphe (1) lettre (c) du texte de compromis du projet de directive, qui prévoit que « *Member States shall provide that personal data must be … adequate, relevant, and not excessive in relation to the purposes for which they are processed…* ».

[23] GA29, Avis *03/2015*, 1 décembre 2015, p. 7 ; GA29, Avis *01/2013*, 26 février 2013, p. 3.

caractère personnel relatives à des personnes non susceptibles d'être les auteurs des infractions.

4.2. La limitation des personnes pouvant procéder à l'enquête sous pseudonyme

Le projet de loi autorise tout officier de police judiciaire de procéder à des enquêtes sous pseudonyme. En revanche, d'après l'article 706-87-1 du Code de procédure pénale français, dont s'inspire l'article 48-26 du projet de loi, cette mesure ne peut être mise en œuvre que par les officiers ou agents de police judiciaire qui « *sont affectés dans un service spécialisé désigné par arrêté du ministre de l'intérieur et spécialement habilités à cette fin* ».

Conformément à la jurisprudence de la CJUE et de la Cour européenne des droits de l'homme, les dispositions limitant le droit à la protection des données à caractère personnel doivent contenir des garanties aptes à protéger efficacement les données à caractère personnel enregistrées « *contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données* »[24]. Une telle protection pourrait être assurée en limitant « *le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi* »[25].

Au vu de ce qui précède, la Commission nationale considère que le projet de loi sous examen devrait limiter le nombre des personnes pouvant procéder à des enquêtes sous pseudonyme à des officiers de police judiciaire spécialement habilités à cette fin, à l'instar de l'article 706-87-1 du Code de procédure pénale français.

4.3. La nature du pseudonyme utilisé

Par ailleurs, le projet de loi ne contient aucune précision quant aux pseudonymes qui pourront être utilisés par les officiers de police judiciaire, notamment s'il s'agit des identités fictives ou des identités « réelles ». Etant donné que l'utilisation d'une identité « réelle » pourrait causer des graves préjudices aux personnes dont les identités seraient usurpées, la Commission nationale estime nécessaire de préciser que les officiers de police judiciaire ne pourront en aucun cas avoir délibérément recours à des identités « réelles ».

4.4. Conclusion

Dans un souci de limiter la collecte de données et d'assurer la conformité de l'article aux principes fondamentaux du droit des individus à la protection de leurs données, la Commission nationale recommande aux auteurs du projet d'y apporter les limitations développées ci-avant.

---

[24] *S et Marper c. Royaume-Uni* [GC], n°30562/04 et 30566/04, § 99 et 103, CEDH 2008-V ; Affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland e.a.*, ECLI:EU:C:2014:238, considérant 54.

[25] Voir par rapport à la conservation des données à caractère personnel, les affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland e.a.*, ECLI:EU:C:2014:238, considérant 62.

Finalement, d'un point de vu rédactionnel, la Commission nationale suppose que les infractions énumérées dans l'article 48-26 paragraphe (2) alinéa 2 devraient être « *les actes de terrorisme et de financement de terrorisme au sens des articles 135-1 à 135-6, … »*, et non « *les actes de terrorisme et de financement de terrorisme au sens des articles 135-1 à 136-6, … ».*

5. Article 48-27 du Code d'instruction criminelle

Ce nouvel article est appelé à permettre au procureur d'Etat ou au juge d'instruction de requérir les opérateurs de télécommunications et les fournisseurs d'un service de télécommunications d'identifier l'abonné ou l'utilisateur habituel de leurs services ou d'identifier les services auxquels une personne donnée est abonnée ou qu'elle utilise habituellement.

5.1. Articulation de l'article

La disposition est formulée en des termes généraux ce qui pourrait ne pas satisfaire à l'exigence de clarté et de prévisibilité posée par la jurisprudence de la Cour européenne des droits de l'homme. La Commission nationale se pose par ailleurs des questions quant à l'articulation de l'article sous avis par rapport à d'autres dispositions existantes et à adopter.

Si la Commission nationale adopte une lecture restrictive des éléments pouvant être identifiés aux termes de cet article, à savoir l'identité seule de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé d'une part, et celle des services de communication électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée, d'autre part, ce qui selon sa compréhension exclut *expressis verbis* le retracement des données de trafic et de localisation relatives aux communications électroniques, elle s'étonne toutefois du libellé de l'article 41, qui bien que n'étant qu'un biais par lequel l'art 48-27 peut être mise en œuvre, semble néanmoins aller plus loin pour ce qui est de l'étendue des données pouvant être identifiées, alors que leurs libellés diffèrent.

Le projet prévoit en effet que l'accès aux données pourra se faire :

- sur la base de toutes données détenues par le procureur d'Etat ou le juge d'instruction

ou

- au moyen d'un accès aux fichiers de clients du fournisseur de services ou de l'opérateur

ou

- sur base de l'article 41 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

L'accès aux données de trafic des communications étant encadré par l'article 67-1 du Code d'Instruction criminelle et par les dispositions de la loi du 30 mai 2005, on peut en effet exclure que les auteurs du projet de loi ait voulu faire double emploi en prévoyant à nouveau l'accès à cette catégorie de données par le biais de l'article 48-27.

La loi du 30 mai 2005 énumère de manière détaillée en son article 7 paragraphe (5) les données relatives à l'identification.

Ainsi sont visées : « *le numéro de téléphone, nom, prénom(s), domicile ou lieu de résidence habituel, dénomination ou raison sociale, lieu d'établissement de l'abonné et de l'utilisateur, pour autant que ce dernier soit identifié ou identifiable* ».

Dans un souci d'éviter toute confusion quant à la nature des données d'identification visées par l'article 48-27, la Commission nationale estime nécessaire de reprendre cette énumération dans le corps de texte dudit article.

Pour ce qui est de l'identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés

par une personne déterminée, la Commission nationale recommande d'adopter une terminologie identique pour les articles 48-27 et 41.

Il est compréhensible, que le législateur veuille procurer aux autorités répressives un moyen d'accéder aux données d'identification des utilisateurs et des moyens de télécommunications que ce dernier utilise, sans devoir recourir aux dispositions de l'article 5 de la loi du 30 mai 2005.

Il est moins compréhensible que pour ce faire, les autorités publiques aient un accès direct à des fichiers privés des sociétés, ce qui constituerait un précédent. Cette nouvelle mesure très intrusive paraît disproportionnée par rapport au but recherché.

Il y a lieu de se demander si un accès sur la base de toutes données détenues par le procureur d'Etat ou le juge d'instruction ou le recours à l'article 41, tel que prévu par le présent projet de loi, ne suffisent pas pour atteindre le but recherché. La Commission nationale suggère dès lors de supprimer du texte du projet de loi la possibilité d'avoir un accès direct aux fichiers des opérateurs.

Les officiers de police judiciaire peuvent, en cas d'urgence, avoir accès aux données visées par l'article 48-27 par les mêmes moyens.

La Commission nationale regrette que l'exposé des motifs et le commentaire des articles soient muets sur la définition de l'extrême urgence, alors que des explications complémentaires auraient pu éclairer la raison pour laquelle l'officier de policier judiciaire se voit doter de si larges compétences, dont notamment l'accès direct à des fichiers. Comment serait d'ailleurs organisé un tel accès direct ? La Commission nationale réitère ses doutes quant à la proportionnalité et la nécessité de cette mesure en présence des autres moyens d'accès aux données existantes ou prévues, dont notamment l'article 41 qui permet d'atteindre le même but recherché.

5.2. Appréciation et conclusion

Dans ce contexte, il ne faut pas oublier, que les communications électroniques occupent une place tout-à-fait particulière dans notre Etat de droit. En témoignant notamment :

- la jurisprudence de la Cour européenne des droits de l'homme des dernières des dernières décennies et l'arrêt de la CJUE rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, et

- la législation en matière de protection des données qui accorde une place particulière aux communications électroniques : en effet, il s'agit du seul domaine qui bénéficie

NOTES PAGE 81

[26] La loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques transposant la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques.

[27] La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel transposant la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

d'une législation particulière très développée[26] allant au-delà des règles de droit commun[27] existant en matière de protection des données, et

- le Code d'instruction criminelle qui, par son l'article 67-1, soumet l'accès aux données de trafic de communications électroniques à des conditions plus restrictives que celles s'appliquant aux perquisitions (qu'on pourrait, en quelque sorte, qualifier de « droit commun ») :

• L'accès n'est possible que pour des faits qui emportent une peine criminelle ou une peine correctionnelle, dont le maximum est égal ou supérieur à un an d'emprisonnement.

• L'accès est soumis à la condition de l'ordonnance du juge d'instruction, et cela même en cas de crime ou de délit flagrant[28].

Dans l'hypothèse du recours à des données relatives au trafic des communications, les autorités judiciaires ont recours aux données conservées en vertu de l'article 5 de la loi du 30 mai 2005.

Il s'agit là du type de conservation de données qui a fait l'objet de l'arrêt de la Cour de justice de l'Union européenne (ci-après la CJUE) rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12.

Le projet de loi n°6763 a comme objectif de mettre la législation luxembourgeoise en conformité avec l'arrêt précité de la CJUE.

Bien qu'à priori, l'article 48-27 vise beaucoup moins de données (les seules données d'identification) que l'article 5 de la loi du 30 mai 2005 précitée, la Commission nationale constate que le présent projet de loi entend introduire un article qui risque de violer les principes énoncés dans cet arrêt. En effet, l'article projeté est en décalage avec l'arrêt de la Cour sur les points suivants :

- L'accès devrait être réservé aux poursuites concernant les infractions graves clairement déterminées[29]. Or, en l'espèce, il est prévu de permettre l'accès pour tous crimes et délits. Rappelons qu'à l'heure actuelle, l'accès aux données n'est permis que dans le cadre de la poursuite d'infractions dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement et que le projet de loi n°6763 entend remplacer ce seuil de l'article 67-1 du Code d'instruction criminelle par un catalogue d'infractions.

- Selon la Cour, l'accès aux données devrait être soumis *« à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales »*[30]. Or, l'article 48-27 a justement pour objet de supprimer la nécessité d'une ordonnance préalable écrite d'un juge d'instruction pour un certain nombre d'hypothèses.

Par ailleurs, la limite entre le champ d'application de l'article 67-1 (et de l'article 24-1) du Code d'instruction criminelle d'un côté et celui du nouvel article 48-27 de l'autre n'est pas claire.

Des cas de figure continuent d'exister pour lesquels, même après l'introduction de l'article 48-27, les mesures resteront soumises aux conditions de l'article 67 1.

Pour le cas où l'article 48-27 devait être maintenu sous sa forme actuelle, la Commission nationale suggère d'amender l'article en y intégrant une liste détaillée et exhaustive des différents types de données censées être soumises dorénavant au champ d'application de l'article 48-27 afin de les distinguer de celles qui resteront soumises exclusivement au champ

[28] Cour d'appel, cinquième chambre, 26 février 2008, arrêt 106/08 V « *Cette localisation de la provenance de l'appel téléphonique […] constitue un repérage de données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés, au sens de l'article 67-1 du Code d'instruction criminelle. La compétence pour ordonner un tel repérage appartient en principe au seul juge d'instruction, et ce depuis la loi du 21 novembre 2002 ayant introduit au Code d'instruction criminelle ledit article 67-1. Alors qu'auparavant de telles investigations étaient opérées sur base des articles 65 et 66 du Code d'instruction criminelle, et pouvaient donc également être opérées dans le cadre des crimes et délits flagrants par les officiers de police judiciaire agissant sur base des articles 31 et 33 du Code d'instruction criminelle, le repérage est depuis l'entrée en vigueur de l'article 67-1 réservé à la compétence exclusive du juge d'instruction. Le fait que l'article 67-1 continue à figurer sous la section III « Des transports, perquisitions et saisies » du chapitre Ier du titre III du Livre premier du Code d'instruction criminelle a uniquement pour objet de distinguer le repérage des moyens de surveillance spéciale des télécommunications (articles 88-1 à 88-4 du Code d'instruction criminelle), mais n'autorise pas les officiers de police judiciaire, agissant en vertu des pouvoirs qui leur sont spécialement conférés au titre des crimes et des délits flagrants, à opérer un tel repérage au titre des articles 33 et 31 du Code d'instruction criminelle (perquisition et saisie). L'article 33 du Code d'instruction criminelle est le pendant de l'article 66 du même code, il n'inclut pas les pouvoirs que le juge d'instruction tient de l'article 67-1 dudit code.* ».

[29] Voir à ce sujet le considérant 60 de l'arrêt.

[30] Considérant 62 de l'arrêt.

d'application de l'article 67-1 (et de l'article 24-1), plus protecteur que les nouvelles dispositions projetées.

Encore que la Commission nationale ne saisit pas la réelle plus-value de ce nouveau moyen d'investigation pour les autorités répressives, l'approche choisie par les auteurs du projet de loi lui semble a priori respectueuse des droits fondamentaux des individus et proportionnée au but poursuivi, alors que c'est une approche en deux étapes. D'abord, un accès à des données d'identification est rendu possible par le biais de l'article 48-27. Pour des enquêtes plus poussées et détaillées, un accès à des données plus sensibles, à savoir les données de trafic des communications et de localisation, est possible en vertu des articles 5 et 9 de la loi du 30 mai 2005.

Or, si contrairement à la lecture que la Commission nationale fait de ce nouvel article, ce dernier devrait tout de même aussi couvrir les données relatifs au trafic des communications et de localisation, elle estime que l'article 48-27 serait manifestement disproportionné par rapport au but recherché, alors qu'il ne contiendrait pas toutes les garanties prévues dans le cadre des articles 5 et 9 de la loi du 30 mai 2005 et de l'article 67-1 du Code d'Instruction criminelle et qu'il s'appliquerait sans distinction à tous crimes et délits et que dès lors, les exigences de la jurisprudence européenne ne seraient pas respectées[31].

Pour des raisons de sécurité et de cohérence juridique, la Commission nationale estime en tout état de cause qu'il y a lieu de coordonner toutes ces dispositions légales éparses existantes et en projet.

5.3. Observations supplémentaires quant à certaines modalités et conditions de l'article 48 27

5.3.1. Conditions de fond applicables

La Commission nationale estime que l'accès aux données de communications électroniques ne devrait être permis que s'il est *« nécessaire à la manifestation de la vérité »*, tel que c'est également précisé à l'article 67-1.

5.3.2. Protection du secret professionnel

Comme il a déjà été précisé pour l'article 24-1, la Commission nationale estime qu'il conviendrait de prendre des mesures afin de protéger le secret professionnel et le cas échéant le secret des sources des journalistes.

A ce sujet, il est renvoyé aux développements exposés au point 2.2. du présent avis.

[31] Arrêt de la CJUE rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12.

5.3.3. Nullités

La Commission nationale suggère que l'existence de l'ordonnance et les exigences relatives à sa motivation (devant refléter « *le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête ou d'instruction* ») soient prescrites à peine de nullité.

De même, la condition de l'extrême urgence devrait être prescrite à peine de nullité si la possibilité d'une réquisition par décision d'un officier de police judiciaire en cas d'extrême urgence est maintenue.

6. Article 65 du Code d'instruction criminelle

La Commission nationale n'a pas d'observations à faire concernant cet article.

7. Articles 88-1 à 88-4 du Code d'instruction criminelle

Le projet de loi projette de modifier les articles 88-1 à 88-4 du Code d'instruction criminelle relatives au contrôle des communications afin de mieux définir les mesures susceptibles d'être prises. Au lieu de se tenir à la formule générale et assez vague de « *moyens techniques de surveillance et de contrôle de toutes les formes de communication* », il est proposé d'énumérer le type de mesures ainsi visées.

Il y aurait ainsi trois types de mesures susceptibles d'être ordonnées :

- la surveillance et le contrôle des télécommunications ainsi que de la correspondance postale,
- la sonorisation de certains lieux ou véhicules et
- la captation de données informatiques.

7.1. Champ d'application des mesures prévues aux articles 88 - 1 à 88 - 4

Les modifications introduites par les articles sous avis appellent les remarques suivantes :

- La sonorisation de lieux ou de véhicules (et surtout la sonorisation de lieux d'habitation) permet, certes, le contrôle des communications, mais elle va beaucoup plus loin que le simple contrôle des communications, alors qu'elle permet de surveiller tous les gestes et les habitudes de la vie quotidienne des personnes surveillées, (quand elles se lèvent et se couchent, quand elles cuisinent), la musique qu'elles écoutent ou les films qu'elles regardent, etc.

- De même la captation de données informatiques ne se limite pas aux communications : la captation peut concerner les documents que les personnes concernées rédigent sur leur ordinateur ou la saisie sur le clavier[32]. Elle permet aussi de contrôler les photos que les personnes surveillées affichent sur leur écran et enregistrent le cas échéant sur leur ordinateur, des images prises par la webcam, etc.

En ajoutant les sonorisations de lieux ou de véhicules et la captation de données informatiques aux mesures pouvant être prises dans le cadre des articles 88-1 à 88-4, on procède donc à un « saut en qualité » considérable des possibilités de surveillance. Aux mesures de contrôle proprement dites pourront aussi s'ajouter l'intrusion clandestine au domicile des personnes visées avant et après les opérations de contrôle, ainsi que l'introduction de logiciels sur les terminaux des personnes à surveiller.

De telles mesures vont donc largement au-delà de ce que permettent les articles 88-1 à 88-2 en leurs termes actuels. Comme il est précisé à juste titre dans le commentaire des articles, l'utilisation des articles 88-1 à 88-4 actuels à ces fins risquerait aussi de se heurter à l'exigence de précision de la jurisprudence de la Cour européenne des droits de l'homme.

Pour ce qui est du « saut en qualité » susmentionné, il faut également garder à l'esprit que les communications passées au domicile dans le cercle familial et privé peuvent revêtir un caractère

[32] Au moyen d'un « keylogger ».

plus intime que celles échangées par exemple par e-mail ou par courrier.

Vu le caractère extrêmement intrusif des mesures nouvellement introduites, il importe d'assortir les mesures de garanties suffisantes.

Ainsi, la Cour constitutionnelle allemande reconnait dans ce contexte un noyau dur, un « *Kernbereich* » de la vie privée qui doit bénéficier d'une protection particulière. Cette notion de « *Kernbereich* » couvre par exemple les conversations tenues au domicile dans le cercle familial. Ainsi la cour a sanctionné les législations qui ne protègent pas à suffisance ce « *Kernbereich* » en matière de sonorisation[33] et de captation des données informatiques[34].

Suite à l'arrêt de la Cour constitutionnelle allemande du 3 mars 2004[35], la législation allemande applicable en matière de sonorisation[36] prévoit dorénavant une protection du « Kernbereich » à deux niveaux :

- Au niveau de la décision ordonnant la mesure : « *Die Maßnahme darf nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte, insbesondere zu der Art der zu überwachenden Räumlichkeiten und dem Verhältnis der zu überwachenden Personen zueinander, anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden (…)* ».
- Au niveau de l'exécution, qui doit le cas échéant être interrompue : « *Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, soweit sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Aufzeichnungen über solche Äußerungen sind unverzüglich zu löschen. Erkenntnisse über solche Äußerungen dürfen nicht verwertet werden. Die Tatsache der Erfassung der Daten und ihrer Löschung ist zu dokumentieren.* ».

Enfin, le caractère très intrusif des mesures pouvant être ordonnées sur base des articles 88-1 à 88-4 projetés est encore amplifié par le fait que le cercle des personnes visées est particulièrement large : Les mesures ne peuvent viser non seulement la personne suspecte, « *d'avoir commis l'infraction ou d'y avoir participé* », mais également celle susceptible « *de recevoir (le cas échéant contre son gré) ou de transmettre des informations destinées à l'inculpé ou au suspect ou qui proviennent de lui* ».

Une limitation du cadre des personnes visées est nécessaire

[33] Arrêt concernant la législation applicable à la sonorisation ordonnée par les autorités judiciaires : Urteil vom 03. März 2004 - 1 BvR 2378/98. La question du « *Kernbereich* » est abordée aux points 157 à 268 de l'arrêt. Disponible sur « http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.html ».

[34] Arrêt concernant la la législation applicable à la captation de données informatiques opérée par le Landesverfassungsschutz de la Rhénanie-du-Nord-Westphalie : Urteil vom 27. Februar 2008 - 1 BvR 370/07. Voir points 270 à 287 de l'arrêt sur la question du « *Kernbereich* ». Disponible sur « http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html ». .

[35] Arrêt 1 BvR 2378/98 précité

[36] Strafprozeßordnung, § 100c Akustische Wohnraumüberwachung. Disponible sur « http://www.gesetze-im-internet.de/stpo/100c.html ».

afin de garantir la prévisibilité de la mesure et d'arriver à un juste équilibre entre les droits fondamentaux des personnes et les intérêts des autorités répressives dans le cadre de la lutte contre le terrorisme.

7.2. Nécessité d'apporter des précisions quant aux données informatiques à capter

L'article 88-1 du projet de loi prévoit que le juge d'instruction puisse ordonner l'utilisation de moyens techniques de surveillance et de contrôle de toutes les formes de communication qui permettent de capter des données informatiques. La Commission nationale estime qu'il est nécessaire que le Code d'instruction criminelle précise que l'ordonnance du juge d'instruction doit énoncer quel type de données informatiques peuvent être captées (p.ex. copies d'écran, contenus et métadonnées de communications électroniques, fichiers sur le disque dur, enregistrements audio, enregistrements de saisies au clavier, activation et captation de données de la webcam) afin de garantir une meilleure prévisibilité du texte[37]. La captation de données informatiques par les autorités judiciaires devrait donc se limiter aux données spécifiées dans l'ordonnance du juge d'instruction.

L'article 88-1 paragraphe (3) indique que les données informatiques captées peuvent inclure des données « *reçues et émises par des périphériques audiovisuels* » tels que les microphones ou les webcams intégrés au terminal infiltré. Or, ces périphériques peuvent enregistrer les conversations et les images d'autres personnes que du suspect, comme, par exemple, les membres de sa famille (ou toutes autres personnes présentes dans l'entourage du suspect) et permettent aussi de surveiller les locaux (ou les lieux) dans lesquels se trouve le terminal infiltré. La surveillance s'étend donc au-delà de la personne-même à surveiller, ce qui constitue une intrusion dans la vie privée de personnes en partie non-suspectes et est plus attentatoire à la vie privée que d'autres mesures de captation de données informatiques.

Une écoute (par le microphone de l'ordinateur) ou une vidéosurveillance (par la webcam de l'ordinateur) de l'intérieur d'un logement n'est pas toujours nécessaire et proportionnée et une autre forme de captation de données informatiques moins intrusive, comme p. ex. un contrôle des documents rédigés par la personne surveillée ou des images affichées sur son écran, peut suffire.

Dès lors, le texte de loi devrait également prévoir que l'ordonnance décidant de la mesure précise exactement et en détail quelles sont les opérations à effectuer. Il faut en tout cas éviter des ordonnances prescrivant simplement une « captation des données informatiques » sans donner davantage de détails.

7.3. Risques en matière de sécurité concernant la captation de données informatiques

La Commission nationale constate que les dispositifs techniques prévus pour capter des données informatiques risquent d'être exploités par des tiers (p.ex., services de renseignements étrangers[38], cybercriminels[39]). Par exemple, si le dispositif contient des erreurs d'implémentation ou des backdoors, ces lacunes peuvent être exploitées par des tiers afin d'accéder aux données de la machine infiltrée. De plus, les entreprises qui développent les logiciels de surveillance sont souvent la cible d'attaquants et leurs clients, ainsi que le code source des logiciels, risquent d'être publiés sur Internet[40]. L'utilisation de ces dispositifs techniques crée des risques potentiels pour les citoyens.

La Commission nationale estime dès lors qu'il est indispensable de prendre les initiatives et mesures nécessaires pour garantir que a) le dispositif technique soit uniquement exploitable par les officiers de police judiciaire, qualifiés et habilités à cette fin, et b) que des procédures

---

[37] Voir CNIL, *Délibération n°2015-078 du 5 mars 2015 portant avis sur un projet de loi relatif au renseignement*, p. 7 ; Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), 27.02.2013, p. 97.

[38] Sean Gallagher, *NSA secretly hijacked existing malware to spy on N. Korea*, Ars Technica, 19.1.2015. Disponible sur « http://arstechnica.com/information-technology/2015/01/nsa-secretly-hijacked-existing-malware-to-spy-on-n-korea-others/ ».

[39] Federal Trade Commission, *Spyware Workshop : Monitoring Software on your personal computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff*, 7.03.2005.

[40] Martin Steiger, *Sicherheitsesoterik statt Menschenrechte*, Digma 2015 – 4, p. 135.

soient mises en place afin de désinstaller les logiciels pour lesquels des informations ont été révélées lors de cyberattaques.

De plus, la Commission nationale considère qu'il est primordial de soumettre les dispositifs techniques permettant la captation de données informatiques « à distance » via Internet à un contrôle de qualité à effectuer par des auditeurs externes et indépendants. Un tel contrôle de qualité permettrait de clarifier et de détecter, entre autres, si le dispositif peut être aisément exploité par des tiers, comme c'était le cas pour un dispositif développé par DigiTask et utilisé par le Bundeskriminalamt en Allemagne[41].

La Commission nationale constate qu'il n'est pas certain que les finalités poursuivies par la captation de données informatiques à l'aide de dispositifs techniques soient atteintes, ce qui jette des doutes sur l'efficacité de ce type de mesures. Il est, en effet, difficile de garantir qu'il n'existe pas de logiciels de sécurité (p.ex. logiciels open source ou développés par des entreprises) qui détectent ce type de logiciels de surveillance. Citons à ce sujet Eugene Kaspersky, CEO d'une entreprise qui vend des logiciels de sécurité : « *We detect all malware regardless its purpose&origin* »[42]. De plus, si la personne à surveiller se rend compte que sa machine a été infiltrée, il est fort probable qu'elle change de stratégie (et de moyens de communications).

Par ailleurs, la Commission nationale tient à souligner le risque élevé de cyberattaques contre les infrastructures, nécessitant une ouverture sur l'Internet et utilisées par les autorités répressives (p.ex. base de données centralisée) pour transmettre et stocker les données informatiques collectées à l'aide de dispositifs techniques installés sur les terminaux des personnes concernées. Par conséquent, afin de garantir la confidentialité des données captées, il est essentiel de mettre en place des mesures techniques et organisationnelles qui garantissent un haut niveau de sécurité.

La Commission nationale recommande partant de prévoir dans le texte de la loi l'obligation de chiffrer les données captées lors du transfert et lors du stockage, d'établir un système d'habilitations (droits d'accès, rôles, utilisateurs) afin de contrôler l'accès aux données captées et de tracer tous les événements qui ont trait à la captation de données informatiques à l'aide du dispositif technique (à partir de l'installation du dispositif jusqu'à la désinstallation du dispositif). Ceci rejoindrait par ailleurs le texte de compromis du projet de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les

[41] Chaos Computer Club, *Analyse einer Regierungsmalware*, 8.10.2011. Disponible sur « http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf ».
[42] Mathew J. Schwartz, *FinFisher Mobile Spyware Tracking Political Activists*, InformationWeek, 31.08.2012. Disponible sur « http://www.darkreading.com/vulnerabilities-and-threats/finfisher-mobile-spyware-tracking-political-activists/d/d-id/1106086? ».

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, qui dispose dans son article 24 que « *Member States shall ensure that logs are kept for at least the following processing operations in automated processing systems : collection, alteration, consultation, disclosure including transfers, combination or erasure…* »[43].

En outre, la Commission nationale s'interroge sur l'intégrité du système infiltré et des données informatiques captées. Il ne peut être exclu que l'installation du dispositif technique compromette l'intégrité du système et des données. De plus, si le dispositif technique installé sur le terminal d'une personne suspecte serait capable de manipuler (i.e., modifier, supprimer, ajouter) des données sur le terminal infiltré, il y aurait ainsi un risque que la police judiciaire collecterait des preuves falsifiées du terminal en question.

Par conséquent, la Commission nationale estime qu'il est nécessaire de mettre en place des mesures pour garantir l'intégrité des données informatiques collectées tant au niveau de la transmission de données qu'au niveau des données stockées sur le terminal. De telles mesures amélioreraient également la recevabilité et l'irréfutabilité de données captées en tant que preuves devant un juge.

Ainsi, le dispositif technique ne devrait permettre ni la manipulation de données sur le système infiltré, ni l'installation et l'activation de dispositifs techniques supplémentaires, distincts du dispositif technique de surveillance, ni d'ouvrir d'autres vulnérabilités dans le système infiltré[44]. La Commission nationale estime aussi nécessaire que les événements liés à l'installation du dispositif soient journalisés et que l'intégrité du système sur lequel le dispositif technique est installé soit préservée. De plus, le projet de loi devrait préciser les mesures de contrôle prises par le juge d'instruction lors de l'installation du dispositif de surveillance.

L'article 88-2 paragraphe (3) dispose que les mesures de surveillance « *doivent être levées dès qu'elles ne sont plus nécessaires* ». Or, comment peut-on garantir le retrait du dispositif technique d'un terminal infiltré? Quelles procédures techniques et organisationnelles seront appliquées pour désactiver et désinstaller le dispositif ? S'agit-il d'une désinstallation automatique qui aura lieu après un temps défini à compter de la date de l'ordonnance du juge d'instruction ?

Il est nécessaire de préciser les modalités exactes de la désinstallation du dispositif technique de terminaux infiltrés et les modalités de suppression des données informatiques captées de personnes qui ont été surveillées à tort ou qui se révèlent non-suspectes au cours de la surveillance.

Lorsque le dispositif technique a modifié le système du terminal infiltré, le dommage subi par la personne surveillée, mais surtout l'origine du dommage, seront difficile à prouver en cas de recours contre l'Etat.

La Commission nationale s'interroge, en conséquence, sur la proportionnalité des mesures de surveillance envisagées par rapport aux buts recherchées et aux résultats escomptés et recommande de prévoir des garanties supplémentaires afin de mitiger les risques liés à ce traitement de données et de limiter l'intrusion dans la sphère privée des personnes concernées et de leur environnement.

7.4. Secret professionnel et protection des sources du journaliste

Le projet de loi prévoit la protection des personnes liées par le secret professionnel. Pourtant, la protection n'est pas absolue, puisqu'elle ne joue que si les individus détenteurs du secret professionnel ne sont pas « *suspects d'avoir elles-mêmes commis l'infraction ou d'y avoir participé* ».

---

[43] Article 24 du texte de compromis de la Directive 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, d'exécution de sanctions pénales ou de protection contre les menaces pour la sécurité publique et de prévention de telles menaces, et à la libre circulation de ces données, 2012/0010 (COD), texte de compromis datant du 15 décembre 2015.

[44] Voir aussi Chaos Computer Club, *Stellungnahme an das Bundesverfassungsgericht zum BKA-Gesetz und zum Einsatz von Staatstrojanern*, 7.07.2015, p. 5 ; *Nationalratskommission befürwortet Staatstrojaner*, TagesAnzeiger, 17.4.2015. Disponible sur « http://www.tagesanzeiger.ch/schweiz/standard/Nationalratskommission-befuerwortet-Staatstrojaner/story/11016889 ».

7.4.1. Protection prévue par les articles

Les articles 88-2 paragraphe (5) et 88-4 paragraphe (3) reprennent les dispositions déjà contenues dans les articles 88-1 et 88-2 du Code d'instruction criminelle :

- « *Les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes d'avoir elles-mêmes commis l'infraction ou d'y avoir participé ne peuvent être utilisées. Leur enregistrement et leur transcription seront immédiatement détruits par le juge d'instruction.* » *(article 88-2 paragraphe (5) projeté)*

- « *Les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes d'avoir elles-mêmes commis l'infraction ou d'y avoir participé ne peuvent être utilisées. Leur enregistrement et leur transcription sont immédiatement détruits par le juge d'instruction.* » *(article 88-4 paragraphe (3) projeté)*

7.4.2. Protection des sources du journaliste

Seules les personnes liées par le secret professionnel au sens de l'article 458 du Code pénal sont couvertes par cette disposition.

En revanche, les journalistes, qui ne sont pas liés par un secret professionnel, ne sont donc pas protégés par les dispositions susmentionnées. En effet, la protection des sources du journaliste n'est pas à assimiler à un secret professionnel[45].

Comme en matière d'accès aux données de trafic de communications[46], on peut se demander si la protection prévue par la loi du 8 juin 2004 sur la liberté d'expression dans les médias est suffisante[47].

Ne faudrait-il pas prévoir une protection expresse des journalistes dans les articles 88-1 à 88-4 projetés du Code d'instruction criminelle à l'instar notamment de la législation française qui a servi d'exemple pour les modifications projetées des articles 88-1 et suivants ?

Le Code de procédure pénale français prévoit en effet une protection expresse des journalistes, aussi bien en matière de sonorisation[48], qu'en matière de captation des données informatiques[49]. Y sont protégés « *les locaux d'une entreprise de presse, d'une entreprise de communication audiovisuelle, d'une entreprise de communication au public en ligne, d'une agence de presse, dans les véhicules professionnels de ces entreprises ou agences*

---

[45] « *La protection des sources journalistiques ne doit pas être confondue avec le secret professionnel. Celui-ci est une obligation alors que celle-là est une protection. Dans le premier cas, il est interdit de dire ; dans le second, il est permis de ne pas dire.* » Loïc DENIS, La protection des sources journalistiques, dans *LES CAHIERS DU JOURNALISME NO13 – PRINTEMPS 2004*. Disponible sur « www.cahiersdujournalisme.net/cdj/pdf/13/18_Denis.pdf ».

[46] Point 2.2. du présent avis

[47] Pour un cas de figure postérieur à la loi du 8 juin 2004 (non en matière de contrôle des communications mais en matière de perquisition): cf. l'arrêt précité de la Cour européenne des droits de l'homme (Cinquième section), affaire Saint-Paul Luxembourg S.A. c. Luxembourg, requête n° 26419/10 du 18 avril 2013.

[48] Article 706-96 du Code de procédure pénale français renvoyant à la liste des lieux protégés énumérés à l'article 56-2.

[49] Article 706-102-5 du Code de procédure pénale français renvoyant à la liste des lieux protégés énumérés à l'article 56-2.

ou au domicile d'un journaliste lorsque les investigations sont liées à son activité professionnelle ».

7.4.3. Etendue de la protection et incidence de l'introduction des mesures de sonorisations de lieux ou véhicules et de captation de données informatiques

Alors que les articles 88-1 et 88-2 s'appliquent aujourd'hui aux communications électroniques et postales, ce sont les *communications avec* des personnes liées par le secret professionnel qui sont protégées. Vu l'introduction des mesures de sonorisations de lieux ou véhicules et de captation de données informatiques, il se pose la question de savoir s'il ne faudrait pas désormais protéger aussi les *lieux* où travaillent les personnes protégées (contre la sonorisation) et les lieux où se trouvent des systèmes informatiques, voire les systèmes informatiques eux-mêmes utilisés par les personnes protégées (contre la captation des données informatiques).

L'article 706-96 alinéa 3 du code de procédure pénale français sur les sonorisations est formulé de la manière suivante :

« La mise en place du dispositif technique mentionné au premier alinéa ne peut concerner les lieux visés aux articles 56-1,56-2 et 56-3 ni être mise en oeuvre dans le véhicule, le bureau ou le domicile des personnes visées à l'article 100-7. »

En matière de captation des données informatiques, la formulation est la suivante :

« La mise en place du dispositif technique mentionné à l'article 706-102-1 ne peut concerner les systèmes automatisés de traitement des données se trouvant dans les lieux visés aux articles 56-1, 56-2 et 56-3 ni être réalisée dans le véhicule, le bureau ou le domicile des personnes visées à l'article 100-7. »[50].

Au vu des considérations ci-avant, la Commission nationale recommande fortement d'étendre et d'adapter en ce sens la protection dans la législation luxembourgeoise.

7.5. Protection physique des données obtenues

Les données obtenues suite à la captation informatique et, dans une moindre mesure, les enregistrements sonores, sont facilement susceptibles de faire l'objet de manipulations. Dès lors, il faut les protéger de manière adéquate.

Des mesures protectrices efficaces représentent non seulement une garantie indispensable pour le justiciable, mais protègent aussi l'institution judiciaire contre des contestations injustifiées et allégations de manipulations.

Elles s'imposeront en tout état de cause en vertu de l'article 27 du projet de Directive 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[51].

L'article 88-4 paragraphe 2 projeté[52] prévoit ce qui suit :

« Les télécommunications enregistrées et les correspondances, ainsi que les données ou renseignements obtenus par d'autres moyens techniques de surveillance et de contrôle sur la base de l'article 88-1 sont remis sous scellés et contre récépissé au juge d'instruction qui dresse procès-verbal de leur remise. Il fait copier les correspondances pouvant servir à conviction ou à décharge et verse ces copies, les enregistrements ainsi que tous autres données et renseignements reçus au dossier […]. »

L'article ne précise pas par qui, quand et comment les enregistrements sont mis sous scellé.

L'article dispose que les correspondances font l'objet de

[50] Article 706-102-5 alinéa 3 du Code de procédure pénale français.
[51] XXXX
[52] Article 88-2 alinéa 3 actuel.

copies qui sont jointes au dossier. En revanche, à lire l'article, les enregistrements sonores et informatiques seraient joints au dossier sous leur forme « originale » (sous laquelle ils ont été remis au juge d'instruction).

Il semble évident que les enregistrements doivent être maniés et consultés au cours de l'instruction, si ce n'est que pour faire l'objet de copies, à moins qu'ils aient fait l'objet d'un procès-verbal exhaustif avant la mise sous scellé, ce qui parait encore imaginable pour des enregistrements sonores, mais l'est moins pour certains enregistrements issues d'une captation de données informatiques (et en toute état de cause, cette hypothèse devrait être précisée dans le texte).

Il est donc fort probable que les scellés doivent être ouverts. Cependant, rien ne précise que les enregistrements doivent, de nouveau, être remis sous scellé après ouverture.

Or, entre ce moment de l'ouverture des scellés et l'intervention d'un jugement définitif, des années peuvent s'écouler et les données doivent également être soumises protégées pendant cette durée.

Enfin, le sort des enregistrements obtenus en cas d'expertise ordonnée sur base des articles 87 ou 88 du Code d'instruction criminelle n'est pas clair non plus.

L'article 163 du Code de procédure pénale français dispose à ce sujet ce qui suit :

« Pour l'application de leur mission, les experts sont habilités à procéder à l'ouverture ou à la réouverture des scellés et à confectionner de nouveaux scellés après avoir, le cas échéant, procédé au reconditionnement des objets qu'ils étaient chargés d'examiner ; dans ce cas, ils en font mention dans leur rapport, après avoir, s'il y a lieu, dressé inventaire des scellés ;… »

La Commission nationale recommande de compléter les dispositions relatives à la mise sous scellé afin de donner des réponses aux questions et problèmes formulés ci-dessus.

7.6. Information des personnes concernées

Le droit à l'information des personnes concernées est un gage de transparence face à des investigations qui constituent une ingérence grave dans la vie privée de ces personnes.

L'information des personnes concernées est également nécessaire afin que les voies de recours existant en théorie puissent être exercées en pratique.

7.6.1. Personnes visées

L'information est prévue au bénéfice de « *la personne dont les communications ont été surveillées* ». Pour la Commission nationale, il n'est pas clair s'il s'agit uniquement de la personne suspectée ou aussi d'autres personnes concernées comme par exemple des membres de famille cohabitant dans le même logement (faisant l'objet d'une sonorisation) ou utilisant le même ordinateur (faisant l'objet d'une captation de données informatiques) que la personne suspectée, dans l'hypothèse où ces autres personnes concernées sont connues.

Pour ce qui est plus particulièrement de la sonorisation de lieux privés, la Cour constitutionnelle allemande a d'ailleurs décidé ce qui suit :

« *Die Benachrichtigungspflicht dient der Gewährleistung effektiven Schutzes der hier betroffenen Grundrechte. Demzufolge sind all diejenigen von der heimlichen Maßnahme zu unterrichten, in deren Grundrechte durch sie eingegriffen worden ist und denen somit Rechtsschutzmöglichkeiten und Anhörungsrechte offen stehen müssen. Zielperson einer akustischen Wohnraumüberwachung ist zwar allein der Beschuldigte. Der Grundrechtseingriff einer akustischen Wohnraumüberwachung bleibt aber nicht auf diesen begrenzt.*

Als Beteiligte im Sinne des § 101 Abs. 1 StPO sind daher neben dem Beschuldigten die Inhaber und Bewohner einer Wohnung zu benachrichtigen, in denen Abhörmaßnahmen durchgeführt worden sind.

Eine Benachrichtigungspflicht besteht grundsätzlich auch gegenüber solchen Personen, die sich als Gast oder sonst zufällig in einer überwachten Wohnung aufgehalten haben und die in ihrem durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützten Recht am gesprochenen Wort und in ihrem informationellen Selbstbestimmungsrecht betroffen sind. »[53]

La Commission nationale estime dès lors nécessaire de préciser les destinataires de l'information.

7.6.2. Délais et exceptions

L'information a lieu « *au cours même de l'instruction et en tout cas au plus tard dans les douze mois qui suivent la cessation de la prédite mesure.*»

Cependant, dans le cadre des infractions pour lesquelles le juge d'instruction pourrait avoir recours aux mesures de sonorisation de lieux ou véhicules et de captation de données informatiques, la loi prévoit une exception à ce délai de 12 mois. Une telle exception, qui permettrait aux autorités de retarder sans limitation l'information, risque de priver la personne de son droit à l'information.

D'ailleurs, en matière de sonorisation, la Cour constitutionnelle allemande a décidé ce qui suit :

« *Um sicherzustellen, dass die Zurückstellung [der Benachrichtigung] auch im weiteren Verlauf auf das unbedingt Erforderliche begrenzt bleibt, bedarf es in Zeitabständen einer wiederkehrenden gerichtlichen Überprüfung.* »[54].

La Commission nationale fait siennes les réflexions de la Cour constitutionnelle allemande pour recommander de permettre un retardement de l'information que sur décision explicite et pour une période limitée dans le temps, le cas échéant renouvelable, après un contrôle juridictionnel.

7.7. Voies de recours

Il est prévu de supprimer le recours de l'opposition prévu initialement pour le contrôle des communications. Selon le commentaire des articles, il existerait des recours adéquats (y compris pour des tiers) en la forme du recours en nullité prévu par l'article 126 du Code d'instruction criminelle.

A défaut de jurisprudence publiée en matière de contrôle

[53] Points 294 à 296 de l'arrêt précité du 3 mars 2004.
[54] Point 306 de l'arrêt précité du 3 mars 2004.

des communications effectué sur base des articles 88-1 et 88-2 du Code d'instruction criminelle, il est difficile d'apprécier l'efficacité des voies de recours.

On constate cependant que la plupart des conditions des articles 88-1 à 88-4 projetés du Code d'instruction criminelle ne sont pas prescrites à peine de nullité. Tel est notamment le cas pour la nécessité d'une infraction ayant trait au terrorisme pour les mesures de sonorisation de lieux ou véhicules et de captation de données informatiques, la nécessaire inopérance des moyens ordinaires d'investigation, l'exigence d'une décision spécialement motivée, la limitation dans le temps de la mesure, l'approbation par le président de la chambre du conseil de la prolongation de la mesure, ainsi que de l'introduction dans un lieu privé et de l'installation par Internet d'un logiciel d'espionnage, l'interdiction d'appliquer la mesure à l'inculpé et la protection des personnes titulaires d'un secret professionnel.

Pour la Commission nationale, toutes ces conditions devraient être prescrites à peine de nullité afin de garantir au mieux possible leur respect et d'assurer leur sanction en cas de non-respect eu égard à l'intrusion grave dans la vie privée.

Enfin, les personnes concernées, et les tiers en particulier ne peuvent vraiment faire usage des voies de recours que s'ils ont connaissance des mesures ordonnées. A ce sujet, il est renvoyé aux développements exposés ci-dessus relatifs au droit à l'information des personnes surveillées.

7.8. Conclusion

La Commission nationale s'interroge sur la proportionnalité des mesures de surveillance envisagées par rapport aux buts recherchées et aux résultats escomptés et recommande de prévoir des garanties supplémentaires afin de garantir la prévisibilité de la mesure et d'arriver à un juste équilibre entre les droits fondamentaux des personnes et les intérêts des autorités répressives dans le cadre de la lutte contre le terrorisme et de mitiger les risques liés à ce traitement de données, ainsi que de limiter l'intrusion dans la sphère privée des personnes concernées et de leur environnement.

La Commission nationale recommande dès lors de compléter les dispositions des articles sous avis, afin d'apporter des réponses aux problématiques soulevées ci-dessus.

8. Article 41 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

Le présent article vise à réintroduire une disposition abrogée en 2011 en raison essentiellement de difficultés techniques. Selon l'exposé des motifs, l'instrument conçu par la loi de 2002 est, à supposer opérationnel, d'une efficacité indiscutable. Il évite de devoir procéder, comme en l'état actuel du droit, à des perquisitions auprès des opérateurs pour obtenir les informations en question, et après mise en vigueur de l'article 48-27 tel que proposé, de devoir adresser des réquisitions aux opérateurs. L'instrument permet beaucoup plus simplement un accès direct et à distance par voie de communication électronique aux informations en question.

8.1. Insertion dans la loi de 2002

Le projet de loi sous avis prévoit d'insérer les dispositions relatives au nouveau traitement de données à effectuer notamment par l'Institut Luxembourgeois de Régulation (ILR) dans la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Cette loi a pour objet de transposer la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Or, la directive 95/46/CE est sur le point d'être remplacée par le nouveau règlement du Parlement européen et du Conseil 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[55].

Le fait que le règlement soit directement applicable, risque d'avoir comme conséquence que la loi modifiée du 2 août 2002 sous sa forme actuelle disparaisse prochainement[56].

8.2. Manque de précisions concernant les données traitées

L'élément clé de ce traitement de données, à savoir les données traitées, n'est pas déterminé dans le texte et serait fixé dans un règlement grand-ducal. Ainsi, la loi ne s'exprime pas clairement sur la nature des données visées.

Or, l'article 11 paragraphe (3) de la Constitution dispose ce qui suit : « *L'Etat garantit la protection de la vie privée, sauf les exceptions fixées par la loi* ». Selon la jurisprudence de la Cour constitutionnelle, « *dans les matières réservées par la Constitution à la loi, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc* »[57]. L'article 41 projeté ne saurait guère satisfaire à cette exigence.

Par ailleurs, les termes de l'article ne permettent pas d'exclure avec certitude que des données relatives au trafic des communications effectuées ne soient visées[58].

La Commission nationale estime nécessaire que la loi énumère en détail les données d'identification visées, à l'instar de l'article 7 paragraphe (5) ou des articles 5 et 9 (où un règlement grand-ducal prévoit le détail des données) de la loi du 30 mai 2005 et de façon générale, agencer la terminologie employée sur celle de l'article 48-27.

8.3. Nature de l'accès

L'article 41 est une des façons d'accéder aux données prévues par l'article 48-27 et l'accès prévu par le présent texte est subordonné aux conditions dudit article. Alors que l'accès est direct et à distance par voie de communication électronique, il procure selon les auteurs du projet de loi un gain d'efficacité spectaculaire.

La Commission nationale constate que l'accès est soumis aux conditions de l'article 48-27. Les données ne peuvent être accédées que dans des cas spécifiques, pour des recherches

[55] A ce règlement s'ajoutera, en matière répressive, la directive précitée 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.

[56] Même si une loi nationale devra régler un certain nombre de questions institutionnelles et procédurales relatives au nouveau règlement.

[57] Arrêt 117 de la Cour constitutionnelle.

[58] La Commission nationale se demande si les « *données concernant l'identité (…) des utilisateurs* » incluent des données précises relatives à l'identité de la personne ayant passé telle ou telle communication donnée.

déterminées et dans le respect de procédures strictes. Ces garanties indispensables sont toutefois menacées par le paragraphe (4) dudit article en ce qu'il dispose que « *La procédure est entièrement automatisée suite à l'autorisation de la Commission nationale.* »

En effet, une procédure entièrement automatisée laisse peu de place pour le respect de procédures, à moins que ce ne soit que le volet de la transmission des données des opérateurs et des fournisseurs vers l'ILR qui soit visé. La Commission nationale recommande de préciser ce point.

8.4. Durée de conservation

La loi ne précise rien quant à la durée de conservation des données auprès de l'ILR.

Il n'est pas clair si lors de la mise à jour des données qui doit avoir lieu une fois par jour au moins, les données anciennes sont effacées de manière automatique, ou si les données sont empilées jusqu'à l'infini, ou bien si elles sont effacées après un certain délai. Ce sont des questions auxquelles la loi devrait répondre afin de répondre aux exigences de précision et de prévisibilité de jurisprudence de la Cour européenne des droits de l'homme en matière d'ingérence au droit au respect de la vie privée.

Rappelons aussi que, dans son arrêt rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, la Cour de justice de l'Union européenne a fustigé le fait que la directive 2006/24/CE laisse, pour ce qui est de la durée de conservation, une marge s'étendant de 6 mois à 2 ans sans donner davantage de précisions[59]. Or, en l'espèce, aucune durée de conservation du tout n'est fixée.

La durée de conservation ne doit en aucun cas être disproportionnée par rapport aux finalités du traitement.

8.5. Nécessité et proportionnalité du traitement de données envisagé

Le présent projet tend à mettre en place un système qui permet d'accéder aux données concernant l'utilisation de moyens de communication de pratiquement tous les citoyens habitant le pays, accès qui peut être effectué non seulement en cas de suspicion de terrorisme, mais pour tout crime ou délit.

Si le système est indispensable pour assurer la lutte contre la criminalité, celle-ci devrait être moins effective dans les pays ne disposant pas d'un tel système, ce qui n'est pas avéré.

Par ailleurs, des voies alternatives moins attentatoires à la vie privée comme une accélération des procédures sans création d'une

[59] Considérants 63 et 64.

nouvelle banque de données, devraient être explorées avant la mise en place d'un tel système.

Pour le surplus, la Commission nationale renvoie à ses développements au point 5.2.

8.6. Le cas particulier des services de secours

L'article 41 réintroduit également un droit d'accès pour la Centrale des secours d'urgence et la Centrale du service d'incendie et de sauvetage de la Ville de Luxembourg aux mêmes conditions et modalités que les autres autorités visées par cet article.

L'accès à ces données par les services de secours constitue une finalité toute à fait différente de celle poursuivie par les autorités répressives. Ni le projet de loi, ni l'exposé des motifs ou le commentaire des articles fournissent des précisions sur le motif des services de secours qui doit certainement être recherché dans son propre cadre législatif, mais qui vise peu probablement la prévention, la recherche, la constatation ou la poursuite d'infractions. La Commission nationale considère que pour le cas où un recours à un tel mécanisme devrait être nécessaire, l'accès par les services de secours ne devrait pas figurer parmi les dispositions de l'article 41 de la loi du 2 août 2002 réintroduit dans la loi dans un but de renforcer les moyens de lutte contre le terrorisme, mais plutôt dans une loi spéciale règlementant les pouvoirs des services de secours.

Par ailleurs, la Commission nationale estime qu'en présence de l'article 4 paragraphe (3) lettre (c) et surtout de l'article 7 paragraphe (5) lettre (a) de la loi du 30 mai 2005 précitée, les services de secours disposent des accès aux données nécessaires à l'atteinte de leurs finalités et qu'il n'y a pas besoin de prévoir des mécanismes supplémentaires.

En effet, l'article 7 « Identification de la ligne appelante et la ligne connectée » dispose en son paragraphe (5) « *(a) Tout fournisseur ou opérateur de services de téléphonie fixe ou mobile qui fournit un accès au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminées par l'Institut luxembourgeois de régulation transmet (« push ») pour chaque appel à destination d'un de ces numéros d'appel d'urgence les données disponibles concernant l'appelant y compris les données de localisation.* »

Le point (c) rajoute que « *Pour les appels effectués à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminées par l'Institut, l'identification de la igne appelante « et les données de localisation de l'appelant » sont toujours présentées même lorsque l'appelant les a empêchés.* »

L'article 4 paragraphe (3) prévoit une exception à la confidentialité des communications en faveur du numéro d'urgence unique européen 112 et des numéros d'urgence déterminées par l'Institut de Régulation Luxembourgeois en vertu de laquelle les communications peuvent être enregistrées à partir de ces numéros.

Notons que le Règlement 14/182/ILR du 26 août 2014 relatif à la détermination de numéros d'urgence au sens de la loi du 30 mai 2005, considère en plus du numéro d'appel d'urgence unique européen « 112 », comme numéros d'urgence au sens de l'article 4 paragraphe (3) et de l'article 7 paragraphe (5) lettres (a) et (c) le numéro « 113 » de la Police Grand-Ducale et le numéro « 44 22 44 » du Service d'Incendie et de sauvetage de la Ville de Luxembourg.

Les numéros des six Centres d'Intervention Principaux de la Police Grand-Ducale sont considérés comme numéros d'urgence au sens de l'article 4 paragraphe (3) lettre (c) de la loi de 2005.

Pour le cas où le législateur devrait néanmoins décider de maintenir l'accès des données par les services de secours en vertu de l'article 41, la

Commission nationale s'étonne sur les conditions et modalités dans lesquels cet accès devrait s'effectuer. Vu le libellé actuel du texte en projet et en l'absence de précisions à ce sujet, la Commission nationale doit supposer qu'un accord du moins oral du juge d'instruction ou du Procureur d'Etat doit précéder toute consultation, qui elle doit être spécifique. Ceci n'est certainement pas la réelle volonté des auteurs du projet de loi, car adopter les mêmes conditions et modalités pour les besoins des services de secours risquerait d'entraver leur bon fonctionnement. Quoi qu'il en soit retenu, il est évident que l'accès par les services de secours doit être proportionné à leur finalité et entouré des garanties appropriées nécessaires à la protection des droits fondamentaux des individus concernés.

8.7. Absence de règles de sécurité

La loi ne prévoit pas de règles de sécurité particulières afin de protéger au mieux le nouveau traitement de données.

Certes, les articles 22 et 23 de la loi modifiée du 2 août 2002 sont en principe applicables. Cependant, ces articles laissent une marge de manœuvre beaucoup trop grande et ne sont pas suffisantes pour un traitement d'une telle envergure[60].

Rappelons qu'en matière de rétention de données de communications électroniques, la Cour de justice de l'Union européenne a, dans son arrêt précité du 8 avril 2014, déclaré invalide la directive 2006/24/CE notamment parce que celle-ci « *ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles* »[61].

En l'espèce, il faudrait assurer, pour ce qui est du traitement en général et des procédures automatisées de transmission en particulier, un niveau de sécurité particulièrement élevé.

Par ailleurs, il faudrait prévoir dans la loi une conservation, dans un log, des données relatives à l'identité des personnes accédant aux données, au moment et au motif de la consultation (avec, le cas échéant, la référence de la décision du magistrat prise en vertu de par l'article 48-27 projeté du Code d'instruction criminelle), à l'image de ce qui se fait pour les accès des officiers de police judiciaire ou des magistrats aux banques de données d'administrations publiques 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 respectivement de l'article 48-24 du Code d'instruction criminelle.

---

[60] A titre d'exemple, en Allemagne, la loi nationale transposant la directive 2006/24/CE a été déclarée anticonstitutionnelle notamment en raison de l'absence de règles de sécurité spécifiques adaptées à l'ampleur du traitement de données, les règles générales de sécurité applicables en matière de protection des données étant insuffisantes : « *Das Fehlen hinreichender Sicherheitsstandards im Telekommunikationsgesetz kann auch § 9 BDSG in Verbindung mit der zugehörigen Anlage nicht ausgleichen. Unbeschadet ihrer zum Teil abstrakt hohen Standards bleibt diese Norm, die ohnehin nur subsidiär anwendbar ist (vgl. Fetzer, in: Arndt/Fetzer/Scherer, TKG, 2008, vor § 91 Rn. 10; Klesczewski, in: Säcker, Berliner Kommentar zum TKG, 2. Aufl. 2009, § 91 Rn. 15), zu allgemein, um in hinreichend spezifischer und verlässlicher Weise die besonders hohen Sicherheitsstandards bezüglich der nach § 113a TKG zu speichernden Daten sicherzustellen.* » Bundesverfassungsgericht, 1 BvR 256/08 vom 2.3.2010, point 274 de l'arrêt.Le §9 BDSG y mentionné et son « Anlage » correspondent aux articles 22 paragraphe (1) et 23 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

[61] Considérant 67 de l'arrêt.

L'absence de règles de sécurité ne saurait être réparée par l'exigence de l'autorisation à délivrer par la Commission nationale. En effet, une procédure d'autorisation devrait avoir comme objectif plutôt de faire veiller au respect de la loi, que de parer aux carences de celle-ci.

8.8. La procédure d'autorisation

8.8.1. Objet de l'autorisation

A la différence de la plupart des autorisations que la Commission nationale délivre habituellement et qui couvrent tous les aspects d'un traitement de données à caractère personnel, l'autorisation à délivrer en l'espèce est limitée à « *la procédure* » (ou les modalités du caractère automatisé de cette procédure) et exclut bon nombre d'aspects :

- L'existence même du système est prévue par l'article 41 projeté de la loi modifiée du 2 août 2002.

- Les destinataires sont fixés par l'article 41 projeté ainsi que par l'article 48-27 projeté du Code d'instruction criminelle.
- Les données traitées seront fixées par règlement grand-ducal.

- Le « *format et les modalités de mises à disposition des données* » seront également fixées par règlement grand-ducal.

Des questions relatives au champ d'application de la procédure d'autorisation subsistent :

- Est-ce que « *la procédure* » à autoriser en vertu du paragraphe (4) de l'article 41 projeté est uniquement celle relative à l'accès aux données par les destinataires finaux, accès évoqué dans les paragraphes (3) et (4) *in fine* ? Dans l'affirmative, la transmission des données de l'ILR vers les destinataires finaux (magistrats, services de secours) ferait, certes, partie du champ d'application de la procédure d'autorisation. En revanche, la transmission (probablement plus massive) de données des fournisseurs de service et opérateurs vers l'ILR en serait exclue.

- Ou bien « *la procédure* » couvre-t-elle aussi la transmission de données des fournisseurs de service et opérateurs vers l'ILR qui est réglée par le paragraphe (2) de l'article 41. Dans cette hypothèse, il se poserait la question de la limite entre « *le format et les modalités de mises à disposition des données* » à fixer par règlement grand-ducal et « *la procédure* » à autoriser par la Commission nationale.

- Est-ce que les questions relatives au stockage des données indépendantes de la question de la transmission font partie de « *la procédure* » ?

La Commission nationale se demande aussi s'il n'y a pas un risque qu'en l'espèce, un traitement se trouve en quelque sorte labellisé « *autorisé par la Commission nationale* », alors que l'emprise réelle de la Commission nationale dans le cadre de cette procédure d'autorisation est très limitée.

8.8.2. En cas de refus

Que se passerait-t-il en cas de refus par la CNPD ? L'autorisation ne portant pas sur l'existence même du système dans son ensemble, mais uniquement sur la procédure d'accès automatisée, le système devrait être mis en place sans l'accès automatisé. Or, cela n'aurait guère de sens, étant donné que la raison d'être affichée du nouveau système est justement sa rapidité obtenue grâce à l'accès automatisé.

8.9. Conclusion

Pour la Commission nationale, les modalités de mise en œuvre de ce nouveau traitement de données ne sont pas suffisamment claires. Dès lors, elle ne peut se prononcer en pleine connaissance de cause.

Si néanmoins le principe de l'introduction d'un tel traitement

de données devait être retenu, celui-ci devrait répondre aux questions et exigences formulées ci-dessus.

Ainsi décidé à Esch-sur-Alzette en date du 12 février 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°6810 concernant une administration transparente et ouverte et au projet de loi n°6811 modifiant la loi du 4 décembre 2007 concernant la réutilisation des informations du secteur public

Délibération n°196/2016
du 26 février 2016

Introduction

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 » ou « la loi »), 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 en date du 15 juin 2015, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer sur le projet de loi n°6811 modifiant la loi du 4 décembre 2007 sur la réutilisation des informations du secteur public (ci-après « le projet de loi n°6811 »).

Le projet de loi n°6811 a pour objectif de transposer en droit national la directive 2013/37/UE concernant la réutilisation des informations du secteur public, adoptée le 26 juin 2013 et modifiant la directive 2003/98/CE du 17 novembre 2003 qui a le même objet. Cette première directive de 2003, également dénommée « Directive ISP I », avait été transposée en droit luxembourgeois par la loi du 4 décembre 2007 sur la réutilisation des informations du secteur public.

La directive 2013/37/UE (ci-après « directive ISP II ») vise à encourager et à faciliter la réutilisation des informations de nature diverses détenues par le secteur public, qui constituent une source de croissance importante de l'économie numérique et une valeur ajoutée potentiellement forte pour les services offerts aux citoyens et aux entreprises. Elle aura pour effet d'engager le Luxembourg plus avant dans une logique d'ouverture et de partage des informations détenues par les organismes du secteur public.

Il ressort du considérant n°8 de la directive ISP II que le but poursuivi est d'*« imposer aux Etats membres une obligation claire de rendre tous les documents réutilisables, à moins que des règles nationales relatives à l'accès aux documents ne limitent ou n'excluent cet accès et sous réserve des autres exceptions prévues par la présente directive »*.

L'exposé des motifs du projet de loi n°6811 précise par ailleurs que *« le projet de loi ne tend pas à définir, élargir ou modifier les règles d'accès aux informations détenues par le secteur public, mais se greffe sur les dispositions existantes en matière d'accès et se limite à fixer les conditions de leur réutilisation »*. Sans créer d'obligation d'autoriser la réutilisation de documents, le projet de loi n° 6811 vise à faciliter la réutilisation des informations du secteur public accessibles en vertu du droit national.

La Commission nationale relève un lien certain entre le projet de loi n°6811 et le projet de loi n°6810 relative à une administration transparente et ouverte (ci-après « le projet de loi n°6810 ») qui ont fait l'objet d'un dépôt simultané à la Chambre des députés, le 5 mai 2015. En effet, ces deux projets de lois convergent vers un double objectif de transparence et d'ouverture de l'administration.

Elle note que le Conseil d'Etat a souligné dans son avis n°6811/03 du 24 novembre 2015, à propos des projets de lois n°6810 et 6811 que *« ces deux projets de lois n'ont manifestement fait l'objet d'aucune coordination préalable. Les deux textes accusent en effet des divergences de terminologie et de champ d'application importantes »*.

La Commission nationale observe que l'environnement légal et réglementaire, ainsi que les pratiques administratives en matière d'accès aux informations du secteur public sont appelés à évoluer profondément avec l'entrée en vigueur des projets de lois n°6810 et 6811.

Le Gouvernement entend en effet moderniser l'Etat luxembourgeois, notamment à travers l'initiative *Digital Lëtzebuerg*, en le dotant d'une administration numérique performante, transparente et ouverte.

La Commission nationale ne peut que souscrire aux objectifs poursuivis par les deux initiatives législatives précitées, qui concourent toutes deux à rendre plus effectif le droit pour les citoyens de s'informer des affaires publiques. Aux termes des évolutions que les deux projets de textes introduiront en droit luxembourgeois, les citoyens seront en effet plus à même de suivre, de comprendre et de contrôler l'activité de l'administration. La Commission nationale observe que ce mouvement tend en outre à instaurer une confiance accrue et à améliorer la qualité des relations entre l'administration et les citoyens.

Dans le même temps, elle se soucie de parvenir à la définition d'un cadre juridique où l'accès aux documents administratifs, la réutilisation des données

publiques et la protection de la vie privée et des données à caractère personnel trouvent un équilibre. Il lui importe que la protection des données contribue à construire un cadre juridique solide et exigeant pour une meilleure transparence de l'action publique.

Au vu des éléments qui précèdent et compte tenu de la complémentarité des deux projets de lois et de leurs objectifs communs, la Commission nationale a estimé utile de les examiner conjointement dans le cadre du présent avis.

I. Sur le projet de loi n°6810 relative à une administration transparente et ouverte

Le projet de loi n°6810 a pour objectif de définir un cadre pour la mise en œuvre d'une politique d'ouverture aux citoyens des documents qui sont détenus par les administrations et services de l'Etat, les communes, les établissements publics placés sous leur tutelle ainsi que les personnes morales fournissant des services publics, dans la mesure où les documents correspondent à une activité administrative[62].

Ce projet de loi traduit la partie du programme gouvernemental dédiée au développement d'une administration transparente et ouverte.

A. Sur l'objet du projet de loi n°6810

L'article 1er paragraphe (1) du projet de loi n°6810 dispose que « *les documents accessibles en vertu de la présente loi sont d'office rendus publics et diffusés auprès du public* ». Sans définir expressément la notion de « *document accessible* », le projet de loi n°6810 dresse, en son article 4, une liste limitative de restrictions à l'accessibilité et à la communicabilité des documents.

L'article 1er paragraphe (2) du projet de loi instaure quant à lui un droit d'accès général aux documents détenus par l'administration, dans la mesure où ce droit concerne les documents détenus par les administrations et services de l'Etat, les communes, les établissements publics placés sous leur tutelle, ainsi que les personnes morales fournissant des services publics, dès lors que les documents correspondent à une activité administrative. Il concerne en outre les documents détenus par la Chambre des Députés, le Conseil d'Etat, le Médiateur et la Cour des comptes.

Il ressort de la lecture combinée des paragraphes (1) et (2) de l'article 1er précité que la notion de « document accessible » au sens du projet de loi est particulièrement large. Elle s'étend en effet à tout type de document détenu par une administration. Le commentaire des articles précise toutefois, s'agissant de l'article 1er du projet de loi n°6810, que les

[62] Exposé des motifs du projet de loi n°6810 relatif à une administration transparente et ouverte, spéc. p. 2.

documents visés sont ceux « *qui revêtent un caractère administratif* » et qui se « *rapportent donc à la gestion d'une activité administrative* ». Le commentaire de cet article précise en outre que « *les documents étrangers à la gestion administrative d'un service public et que l'administration ou une personne morale est venue à détenir dans le cadre de ces activités ne sont pas accessibles. Ainsi, les documents qui se rapportent à la gestion d'une activité industrielle et commerciale exercée, par exemple, par un établissement public à caractère industriel et commercial tel qu'il est défini par l'instruction du Gouvernement en Conseil du 11 juin 2004 sur la ligne de conduite et les règles générales en matière de création d'établissements publics ne sont pas accessibles* ».

En dépit des précisions apportées dans le commentaire des articles, la Commission nationale estime que la notion de « document accessible » pourrait être encore clarifiée à l'article 1er du projet de loi n°6810, afin de mieux circonscrire le périmètre de l'accessibilité des documents détenus par l'administration.

La Commission nationale est d'autant plus attentive à l'impact et au champ d'application du projet de loi n° 6810 que son exposé des motifs traduit la volonté du Gouvernement de proposer un cadre moins restrictif concernant l'accès aux documents administratifs que celui que prévoyait le projet de loi n°6540 relative à l'accès des citoyens aux documents détenus par l'administration (déposé le 5 février 2013). La Commission nationale note à cet égard que le Gouvernement a retiré du rôle de la Chambre des Députés le projet de loi n°6540 précité.

La Commission nationale constate que le projet de loi n°6810 entend poser le cadre d'une politique de mise à disposition générale des documents administratifs. En effet, aux termes de l'article 1er paragraphe (2) du projet de loi n°6810, l'accès aux documents administratifs sera désormais de droit, sauf dans les cas où le législateur lui-même en a limité la portée. La loi luxembourgeoise se rapprochera ainsi de plusieurs législations étrangères ayant instauré un principe de libre accès aux documents administratifs. Elle dépassera en outre l'objectif atteint par les initiatives législatives ponctuelles ou sectorielles de reconnaissance de la transparence administrative par le législateur jusqu'à ce jour (notamment par la loi du 1er septembre 1978 réglementant la procédure administrative non contentieuse, par les lois successives du 12 juin 1937, du 20 mars 1974 et du 21 mai 1999 dans le domaine de l'aménagement du territoire, par la loi du 16 avril 1979 dans le domaine des établissements classés, par la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, par la loi modifiée du 2 août 2002 en matière de protection des données à caractère personnel, ou encore par les lois du 10 août 1992, puis du 25 novembre 2005 en matière environnementale).

B. Sur la diffusion des documents

Comme énoncé précédemment, l'article 1er paragraphe (1) du projet de loi n°6810 pose un principe de publication et diffusion d'office auprès du public des documents accessibles en vertu de ladite loi en projet.

La Commission nationale note que l'article 2 du projet de loi n°6810 prévoit que les administrations et établissements publics soumis audit projet de loi sont « *tenus de procéder à la publication des documents accessibles en vertu de la présente loi. Ces documents sont diffusés moyennant les nouvelles technologies de l'information et de la communication* ».

Par ailleurs, l'article 3 du projet de loi dispose que « *sans préjudice d'autres dispositions légales qui règlent l'accès des documents détenus par les organismes visés à l'article 1er, ces derniers sont tenus de communiquer les documents qu'ils détiennent, quel que soit*

le support, à toute personne physique ou morale qui en fait la demande, sans que celle-ci ne soit obligée de faire valoir un intérêt ».

Il ressort de la lecture combinée de ces articles que le Gouvernement entend ériger en principe l'obligation de diffusion des documents administratifs et faire de leur communication sur demande une exception.

En ce sens, l'exposé des motifs du projet de loi n°6810 indique que *« le projet de loi pose le principe de l'ouverture et du partage en ligne des documents administratifs. L'administration devra prendre l'initiative de publier en ligne les documents qui ont vocation à être librement accessibles en application des règles inscrites dans le projet de loi »*. L'exposé des motifs poursuit en précisant qu' *« étant donné que l'égal accès aux nouvelles technologies n'est pas toujours assuré, le texte proposé continue à prévoir, à l'instar du projet de loi n°6540, la possibilité pour toute personne physique de prendre l'initiative pour demander l'accès à un document »*.

Le commentaire des articles précise s'agissant de l'article 2 du projet de loi relatif à l'obligation de publication des documents accessibles en vertu de ladite loi qu' *« il s'agit en fait de la généralisation d'une mission que le Service information et presse du Gouvernement (SIP) remplit depuis des années, cela en application de l'article 32 de la loi modifiée du 27 juillet 1991 sur les médias électroniques et qui confère au SIP, entre autres, la mission d'assurer l'information de la presse, mais également du public et des milieux intéressés sur les activités de l'Etat »*.

La Commission nationale observe que ces dispositions sont de nature à accroître la transparence de l'action publique en introduisant une logique de « l'offre » (logique reposant sur un principe de diffusion par les administrations de leur propre initiative des documents administratifs qu'elles détiennent), allant ainsi plus loin que la logique de la « demande » que de nombreuses législations européennes ont adoptée jusqu'à ce jour (logique reposant sur un principe de communication des documents administratifs sur demande des intéressés).

Elle relève que ces dispositions pourraient opérer un changement de paradigme important qui va dans le sens des réflexions récemment menées à l'étranger, notamment en France, afin de rendre effective la transparence administrative au moyen notamment d'une plus grande ouverture des données détenues par les administrations (mouvement plus connu sous le nom d'« Open Data »).

La Commission nationale ne peut donc que souscrire à

l'objectif poursuivi par les dispositions précitées du projet de loi. Elle estime toutefois qu'un temps d'adaptation devra nécessairement être laissée aux administrations pour se conformer à ce nouveau cadre juridique, dans des conditions respectueuses de la loi modifiée du 2 août 2002.

C. Sur les limites au droit d'accès

L'article 4 du projet de loi n° 6810 pose des limites à l'accessibilité et à la communicabilité des documents.

L'article 4 paragraphe (1) du projet de loi dispose notamment que « *ne sont pas accessibles les documents dont la communication porterait atteinte à la sécurité des personnes ou au respect de la vie privée* » ou encore « *à un secret ou une confidentialité protégés par la loi* ».

Par ailleurs, l'article 4 paragraphe (2) du projet de loi dispose que « *ne sont communicables qu'à la personne concernée les documents qui :*

- *comportent des données à caractère personnel ;*
- *comportent une appréciation ou un jugement de valeur sur une personne physique, nommément désignée ou facilement identifiable, à moins que celle-ci n'ait donné son accord ;*
- *comportent une opinion communiquée à titre confidentiel à l'administration, à moins que le caractère confidentiel du document n'ait été levé par la personne qui est à l'origine du document.* »

La Commission nationale salue les efforts mis en œuvre par les auteurs du projet de loi n°6810 en vue d'assurer la protection d'intérêts privés fondamentaux qui peuvent entrer en conflit avec le droit d'accès aux documents administratifs.

Au vu des dispositions précitées de l'article 4 paragraphes (1) et (2), la Commission nationale s'interroge néanmoins sur l'articulation des dispositions de la loi modifiée du 2 août 2002 et de celles qui seront issues du projet de loi n°6810. Elle note que le projet de loi n°6810 est silencieux sur ce point.

Le commentaire des articles du projet de loi n°6810 précise, s'agissant de l'article 4 précité, que « *l'autorité publique sollicitée devra, le cas échéant, mettre en balance l'intérêt de la communication d'un document et l'intérêt protégé par un motif d'exception. Etant donné que l'accès aux documents constitue la règle générale, les motifs d'exception doivent être interprétés de manière restrictive* ».

Sur ce point, la Commission nationale estime que la balance des intérêts réalisée par les autorités publiques concernées devra s'effectuer au terme d'un examen minutieux des risques qu'une telle communication pourrait engendrer pour la vie privée, risques nécessairement plus importants en raison de l'accessibilité accrue des documents administratifs.

Le commentaire des articles poursuit plus loin, s'agissant du paragraphe (2) de l'article 4 précité : « *le respect de la vie privée des personnes explique que les documents qui contiennent des informations d'ordre personnel ou privé ne sont accessibles qu'à la personne concernée. La disposition en question ne fait toutefois pas forcément obstacle à la communication du document dans sa totalité. En effet, il suffit bien souvent d'occulter certaines mentions pour que le document devienne librement accessible* ».

La CNPD tient à souligner que, dès lors que les documents accessibles ou communicables en vertu du projet de loi n°6810 contiendraient des données à caractère personnel, des garanties adéquates au regard de la loi modifiée du 2 août 2002 devraient être prévues. L'obligation de procéder à la publication des documents accessibles en vertu de l'article 2 du projet de loi n°6810 doit s'exercer, en effet, sans préjudice des exigences en matière de protection des données.

Elle relève que l'article 4 paragraphe (5) du projet de loi n°6810 prévoit que « *lorsque la demande porte sur un document comportant des mentions non communicables mais qu'il est possible d'occulter ou de disjoindre, sans charge administrative excessive, le document est communiqué au demandeur après occultation ou disjonction de ces mentions.* »

La Commission nationale accueille favorablement le principe de telles mesures dans une optique de protection des données. Elle relève qu'une disposition similaire existe en droit français, mais que les auteurs du projet de loi y ont ajouté la mention « *sans charge administrative excessive* ». Elle estime que cet ajout pourrait limiter de façon inopportune le recours auxdites mesures d'occultation et de disjonction et suggère, dès lors, de supprimer la mention « *sans charge administrative excessive* » de l'article 4 paragraphe (5) du projet de loi n°6810.

Les administrations doivent faire preuve d'une certaine vigilance en présence de documents administratifs contenant des données à caractère personnel, compte tenu des risques de réidentification qui pourraient exister. La limite posée par l'article 4 paragraphes (1) et (2) du projet de loi n°6810 a en effet pour conséquence que les administrations doivent identifier clairement, préalablement à la publication de documents administratifs, les documents comportant des données à caractère personnel.

A ce jour, la Commission nationale a été saisie à plusieurs reprises de situations dans lesquelles la présence de données à caractère personnel a échappé à une administration qui les a mises en ligne, la technique d'anonymisation utilisée par une administration n'a pas permis une anonymisation irréversible des documents diffusés ou encore de situations dans lesquelles le caractère indirectement identifiant des données n'est pas apparu de prime abord. Or, dans de tels cas de figure, l'impact de la publication de documents sur la vie privée des personnes a pu être considéré comme excédant ce qui est acceptable au nom de l'impératif de transparence (pour une illustration dans le cadre de la publication des aides reçues par les agriculteurs dans le cadre de la politique agricole commune, voir CJUE, 9 novembre 2010, Volker und Markus Schecke GbR et Hartmut Eifert c./ Land Hessen, req. n°C-92/09 et C-93/09).

Dans une optique de « *privacy by design* », la Commission nationale recommande par ailleurs que les bases de données appelées à être développées par les administrations prévoient, dès

leur conception, les modalités d'anonymisation éventuelle des données.

Elle estime en outre, à l'instar des recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL) en France et de l'*Information Commissioner's Office* (ICO) au Royaume-Uni (équivalent britannique de la CNPD et de la future « Commission d'accès aux documents » envisagée à l'article 8 du projet de loi n°6810), que les administrations devraient s'interroger préalablement à la publication et au partage en ligne des documents administratifs sur les risques de réidentification existants.

Ainsi, ces administrations pourront décider d'une accessibilité plus ou moins large des documents qu'elles détiennent, en fonction du risque pour les données en cause , par exemple la diffusion des documents sur Internet auprès du grand public et sans restriction d'accès, la mise en ligne de documents subordonnée à des conditions d'accès restreintes (notamment l'obligation de créer un compte d'utilisateur pour pouvoir accéder aux données), la consultation sur place de documents etc.

D. Sur l'instauration d'une « Commission d'accès aux documents »

L'article 8 du projet de loi n°6810 prévoit l'instauration d'une « Commission d'accès aux documents » chargée de veiller au respect du droit d'accès dans les conditions prévues par ledit projet de loi. La CNPD note que la Commission d'accès aux documents ne sera pas dotée d'un pouvoir décisionnel, mais jouera un rôle consultatif essentiel. Ladite Commission pourra en effet éclairer les intéressés (administrations et administrés) sur l'application du droit d'accès aux documents administratifs, et ce en amont d'éventuels recours contentieux devant le juge administratif.

La CNPD se réjouit de la présence obligatoire de l'un de ses représentants au sein du collège de la Commission d'accès aux documents, afin de garantir une application harmonieuse des dispositions issues du projet de loi n°6810 et de la loi modifiée du 2 août 2002.

E. Sur la combinaison du projet de loi n°6810 et du projet de loi n°6811

A titre subsidiaire, la Commission nationale relève que le projet de loi n°6810 est silencieux quant à son articulation avec d'autres lois en vigueur ou projets de lois visant à encadrer de manière spécifique l'accès aux documents (notamment l'actuel projet de loi sur le régime des archives nationales) et, plus particulièrement, avec le projet de loi n°6811 sur la réutilisation des informations du secteur public. Elle s'interroge sur la mise en cohérence de l'ensemble de ces initiatives législatives concomitantes et sur leur contrariété textuelle.

En définitive, s'agissant du projet de loi n°6810, la Commission nationale accueille favorablement l'introduction d'un droit d'accès général aux documents administratifs en droit interne.

Compte tenu des risques particuliers que la mise en ligne des documents administratifs pourrait constituer pour la protection des données à caractère personnel, elle estime toutefois essentiel de circonscrire le périmètre des informations accessibles, en application du projet de loi n°6810. Cette délimitation est d'autant plus importante que la définition du cadre juridique applicable au droit d'accès aux documents administratifs est une compétence étatique, à la différence de la définition du cadre applicable à la réutilisation des informations du secteur public, qui fait l'objet d'une harmonisation européenne.

II. Sur le projet de loi n°6811 concernant la réutilisation des informations du secteur public

La CNPD est consciente de la marge de manœuvre limitée laissée au législateur, compte tenu du cadre juridique existant

en matière de réutilisation des informations du secteur public (directive 2003/98/CE du 17 novembre 2003 et la loi du 4 décembre 2007 la transposant en droit interne) et des nouvelles obligations introduites par la directive 2013/37/UE. Elle tient à formuler des observations au regard de la loi modifiée du 2 août 2002 dans les situations où des documents ou informations publiques mis à disposition à des fins de réutilisation comporteraient des données à caractère personnel.

A. Sur l'applicabilité de la loi modifiée du 2 août 2002 à la réutilisation d'informations du secteur public comportant des données à caractère personnel

L'article 1er du projet de loi n°6811 pose un principe général selon lequel toutes les informations du secteur public accessibles au public en vertu du droit national et qui ne sont pas couvertes par une des exceptions prévues à l'article 2 du projet de loi sont réutilisables à des fins commerciales et non commerciales.

Cet article traduit l'objectif de la directive 2013/37/UE d'encourager et de faciliter la réutilisation de données détenues par les administrations et qui représentent un potentiel important pour l'économie numérique. Sont ici visées, comme le souligne l'exposé des motifs du projet de loi n°6811, tant les données géo-spatiales, que les données environnementales, les données routières, les données statistiques diverses, ou encore les données de santé publique.

Au titre des exceptions prévues à l'article 2 figurent « *les documents dont l'accès est exclu ou limité en application des règles d'accès en vigueur pour des motifs de protection des données à caractère personnel, et aux parties de documents accessibles en vertu des règles d'accès en vigueur qui contiennent des données à caractère personnel dont la réutilisation est incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel* ».

Bien que de nombreuses informations publiques visées par le projet de loi n°6811 ne portent pas sur des données à caractère personnel, la Commission nationale estime que les organismes relevant du secteur public détiennent un volume important de données à caractère personnel dont la nature et la sensibilité peuvent varier. Elle estime en outre que des données à caractère personnel pourraient être accidentellement diffusées à l'occasion de la mise à disposition de données au public et que les garanties visant à éviter toute réidentification possible des personnes risquent parfois de ne pas être suffisamment

robustes. Elle relève enfin que la loi impose parfois expressément la publication d'informations personnelles.

La Commission nationale rappelle que la notion de « donnée à caractère personnel » est définie de manière large, en application de l'article 2 lettre (2) de la loi modifiée du 2 août 2002. Il s'agit en effet de *« toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable »*.

Comme indiqué précédemment, la loi modifiée du 2 août 2002 a vocation à s'appliquer aux cas dans lesquels des organismes du secteur public visés par le projet de loi n°6811 communiqueraient à des tiers, volontairement ou non, des documents ou informations publiques comportant des données à caractère personnel. La réutilisation de telles données devrait également s'effectuer dans des conditions respectueuses de la loi modifiée du 2 août 2002.

La Commission nationale relève d'ailleurs que le considérant 11 de la directive ISP II prévoit expressément que cette directive *« devrait être mise en œuvre et appliquée dans le respect total des principes relatifs à la protection des données à caractère personnel, conformément à la directive 95/46/CE […]. Il y a lieu, en particulier, de noter qu'en application de ladite directive, les États membres devraient déterminer les conditions dans lesquelles le traitement de données à caractère personnel est licite. »*

Au vu de ces éléments, elle estime que le projet de loi n°6811 devrait faire référence de manière plus explicite au cadre juridique applicable à la protection des données (notamment par un renvoi à la loi modifiée du 2 août 2002), afin de pallier le fait qu'il accroît l'accessibilité des informations du secteur public contenant des données à caractère personnel et le risque d'usage abusif de telles données.

Ainsi, le projet de loi n°6811 pourrait introduire, après l'article 2 de la loi du 4 décembre 2007 en vigueur, une disposition spécifique indiquant dans quelles conditions la réutilisation d'informations publiques comportant des données à caractère personnel est possible (notamment après une anonymisation préalable des informations en cause, en présence d'une disposition légale ou réglementaire le permettant, ou éventuellement si la personne concernée y a expressément consenti).

Une telle disposition pourrait prévoir également, comme c'est le cas dans la loi de transposition française (article 13 de la loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal), que la réutilisation d'informations publiques comportant des données à caractère personnel est subordonnée au respect des dispositions de la loi modifiée du 2 août 2002.

A cet effet, la Commission nationale propose d'insérer après l'article 2 de la loi du 4 décembre 2007 en vigueur, une disposition dont le libellé pourrait avoir la teneur suivante :

« Les informations du secteur public comportant des données à caractère personnel peuvent faire l'objet d'une réutilisation soit lorsque la personne intéressée y a consenti, soit si l'autorité détentrice est en mesure de les rendre anonymes ou, à défaut d'anonymisation, si une disposition législative ou réglementaire le permet.
La réutilisation d'informations du secteur public comportant des données à caractère personnel est subordonnée au respect des dispositions de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. »

La Commission nationale relève que le Contrôleur européen de la protection des données

(« European Data Protection Supervisor » ou « EDPS ») a émis, le 18 avril 2012, un avis sur le paquet de mesures de la Commission européenne relatif à l'ouverture des données[63]. Le Groupe de travail « Article 29 »[64] a également émis un avis visant à garantir une compréhension commune du cadre juridique issu de la directive ISP II et à fournir des orientations quant à sa mise en application[65]. La Commission nationale tient à souligner qu'elle souscrit entièrement aux recommandations émises par ledit Groupe de travail dans cet avis, dont certains éléments sont repris ou développés ci-après.

B. Sur la responsabilité des organismes du secteur public visés pour le traitement de données à caractère personnel

La Commission nationale considère, en application de l'article 2 lettre (n) de la loi modifiée du 2 août 2002, que les organismes relevant du projet de loi n°6811 qui mettraient des données à caractère personnel à disposition de tiers à des fins de réutilisation, en application de l'article 1er du projet de loi n°6811, doivent être considérés comme des responsables de traitements au sens de ladite loi. Elle note que l'article 1er du projet de loi n°6811 permettra d'étendre le champ d'application de la loi aux documents détenus par les bibliothèques (y compris les bibliothèques universitaires, les musées et les archives).

La CNPD souscrit entièrement à la recommandation du Groupe de travail « Article 29 » selon laquelle « *l'organisme du secteur public concerné (ou le législateur, selon le cas) devrait procéder à une évaluation d'impact sur la protection des données avant de rendre disponibles à des fins de réutilisation des informations du secteur public contenant des données à caractère personnel (ou avant d'adopter une législation permettant la publication de données à caractère personnel et les rendant ainsi potentiellement disponibles à des fins de réutilisation)* »[66].

Elle estime, dans l'esprit de la réforme à venir du cadre législatif européen en matière de protection des données, qu'une analyse d'impact sera particulièrement nécessaire dans les cas où les traitements sont susceptibles d'entraîner un risque élevé pour les droits et libertés des personnes physiques.

Autant que faire se peut, seules des documents ou informations publiques rendues anonymes (notamment par agrégation de données) devraient être mises à disposition à des fins de réutilisation. A défaut, des données à caractère personnel pourraient être rendues disponibles à ces fins, si nécessaire et sous réserve de garanties adéquates. En effet, la

[63] Avis de l'EDPS du 18 avril 2012 sur le paquet de mesures de la Commission européenne relatif à l'ouverture des données. Ce paquet comprenait une proposition de directive modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public (ISP), une communication sur l'ouverture des données et la décision 2011/833/UE de la Commission sur la réutilisation des documents de la Commission européenne.

[64] Ce groupe de travail est institué par l'article 29 de la directive 95/46/CE sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il est composé de représentants des autorités nationales chargées de la protection des données, de l'EDPS et de la Commission européenne. Le Groupe Article 29 a notamment pour mission de promouvoir l'application homogène de la directive 95/46/CE dans tous les Etats membres de l'Union européenne.

[65] Avis 6/2013 du Groupe de travail « Article 29 » sur la réutilisation des informations du secteur public (ISP) et des données ouvertes, 5 juin 2013, WP207.

[66] Avis 6/2013 précité, spéc. p. 9.

Commission nationale rappelle que les organismes du secteur public concernés, en leur qualité de responsables de traitements doivent mettre en place des garanties (juridiques, techniques et organisationnelles) suffisantes pour assurer la protection des personnes à l'égard du traitement de leurs données à caractère personnel notamment au regard de la sécurité et de la confidentialité des données relatives aux administrés.

C. Sur la légitimité de la divulgation publique

Le traitement de données à caractère personnel qui consisterait à divulguer ces données sur demande doit être légitimé par l'une des conditions prévues à l'article 5 de la loi modifiée du 2 août 2002.

Dans un souci de sécurité juridique et de prévisibilité, la CNPD souligne, à l'instar du Groupe de travail « Article 29 », *« l'importance d'établir une base juridique solide pour rendre les données à caractère personnel accessibles au public, qui tienne compte des règles pertinentes en matière de protection des données, y compris des principes de proportionnalité, de minimisation des données et de limitation de la finalité »*[67].

Ainsi, à défaut d'anonymisation préalable des données, la Commission nationale estime que toute réutilisation ultérieure d'informations publiques comportant des données à caractère personnel devrait reposer sur une base juridique appropriée (par exemple, un consentement ou une obligation légale), conformément aux dispositions de l'article 5 précité.

D. Sur la limitation de la finalité

L'article 1 paragraphe (2) du projet de loi n°6811 prévoit, en application de la directive ISP II, d'insérer un principe de réutilisation compatible des données, sans autre précision.

La Commission nationale note toutefois que l'exposé des motifs du projet de loi n°6811 précise que *« l'un des principes de ladite loi [loi modifiée du 2 août 2002] est celui selon lequel les données à caractère personnel ne peuvent pas faire l'objet d'un traitement ultérieur à une collecte qui serait incompatible avec les finalités déterminées, explicites et légitimes pour lesquelles ces données ont fait l'objet d'une collecte. »*

L'application effective du principe de limitation de finalité est particulièrement difficile à mettre en œuvre dans le contexte de la réutilisation des informations du secteur public. A cet égard, la Commission nationale tient à souligner que le seul fait que des informations du secteur public comportant des données à caractère personnel soient accessibles au public pour une finalité spécifique ne signifie pas nécessairement que de telles informations soient susceptibles d'être réutilisées pour toute autre finalité.

Elle rappelle que plusieurs facteurs doivent être pris en considération pour déterminer si un traitement ultérieur de données est ou non compatible avec les finalités pour lesquelles ces données ont été initialement collectées : (i) la relation entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur ; (ii) le contexte dans lequel les données ont été collectées et les attentes raisonnables des personnes concernées à propos de leur utilisation ultérieure ; (iii) la nature des données et l'impact de leur traitement ultérieur sur les personnes concernées ; (iv) les garanties mises en œuvre par le responsable du traitement pour assurer un traitement équitable et éviter tout impact excessif sur les personnes concernées[68].

En outre, la Commission nationale se rallie à l'avis du Groupe de travail « Article 29 » selon lequel la directive ISP II n'exclut pas la possibilité pour

[67] Avis 6/2013 précité, spéc. p. 22.
[68] Pour plus de détails sur ce point, voir Avis 03/2013 du Groupe de travail « Article 29 » sur la limitation de finalité, 2 avril 2013, WP 203.

l'organisme du secteur public concerné (ou pour le législateur) de limiter les finalités de réutilisation possible[69]. A cet égard, elle relève qu'en application de l'article 7 de la loi du 4 décembre 2007 en vigueur, les organismes du secteur public peuvent imposer des conditions à la réutilisation de documents, par le biais de licences. Elle estime que l'introduction de conditions particulières dans des licences de ce type pourrait permettre de garantir que des données à caractère personnel ne seront pas utilisées pour des finalités incompatibles avec celles pour laquelle elles ont été initialement collectées. Elle note que le droit luxembourgeois offre d'ores et déjà la possibilité d'un tel encadrement contractuel, notamment dans le cadre du règlement grand-ducal du 9 mars 2009 portant fixation des conditions et modalités de délivrance de la documentation cadastrale.

E. Sur la proportionnalité

La Commission nationale rappelle que l'article 4 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002 pose un principe de proportionnalité qui devrait être appliqué minutieusement dans le choix des méthodes, des modalités et des degrés de détail envisagés pour rendre les informations publiquement disponibles.

Elle tient notamment à souligner qu'en vertu du régime particulier instauré par la loi modifiée du 2 août 2002 pour le traitement de catégories particulières de données, en cas de demande de réutilisation d'informations publiques comportant de telles données sensibles, l'organisme du secteur public concerné devra examiner minutieusement si l'une des conditions de légitimité pour le traitement de données sensibles, prévues aux articles 6 et 7 de la loi modifiée du 2 août 2002, s'applique.

F. Sur les droits des personnes

La CNPD rappelle que les personnes concernées doivent être informées de la divulgation de leurs données personnelles, dans les conditions prévues par l'article 26 de la loi modifiée du 2 août 2002.

Dès lors, les organismes du secteur public concernés devront informer au préalable les personnes concernées de leur intention de divulgation des données au moment de la collecte initiale desdites données.

La Commission nationale rappelle également que les personnes concernées disposent, en vertu de l'article 28 de la loi modifiée du 2 août 2002 d'un droit d'accès, d'un droit de rectification et d'un droit d'effacement des données les concernant, notamment en raison du caractère incomplet

[69] Avis 6/2013 précité, spéc. p. 13.

ou inexact des données. Les personnes disposent en outre, en application de l'article 30 de la loi modifiée du 2 août 2002 d'un droit de s'opposer au traitement de leurs données, tout particulièrement en cas de réutilisation à des fins commerciales de ces dernières. La Commission nationale est consciente des difficultés particulières de garantir l'exercice des droits des personnes dans un contexte de réutilisation de données. Elle estime toutefois que des garanties peuvent être apportées en encadrant les conditions de réutilisation des informations, comme suit.

G. Sur l'encadrement de la réutilisation

La CNPD estime que des mesures juridiques et techniques particulières devraient être mises en place si nécessaire, afin d'apporter des garanties appropriées pour réduire les risques en matière de protection des données.

A titre d'illustration, et sans prétendre à l'exhaustivité, un certain nombre de bonnes pratiques ont pu être identifiées s'agissant du cas de figure le plus fréquent de réutilisation d'informations du secteur public contenant des données à caractère personnel : la mise à disposition de données statistiques agrégées et anonymes, issues de données à caractère personnel (taux de criminalité, dépenses publiques, réussite scolaire des enfants dans différentes zones géographiques ou types d'établissements scolaires).

Les enjeux principaux dans ce cas de figure sont de parvenir à une agrégation et une anonymisation suffisantes des données et de minimiser le risque de réidentification des personnes à partir de plusieurs jeux de données.

A l'instar des recommandations du Groupe de travail « Article 29 » en la matière[70], la Commission nationale souligne également que les contrats de licence, qui peuvent être mis en place en application de l'article 7 de la loi du 4 décembre 2007 (qui demeure inchangé), devraient rappeler aux réutilisateurs qu'ils sont tenus de respecter, le cas échéant, leurs obligations en matière de protection des données. En outre, de tels contrats devraient poser des conditions de nature à assurer une meilleure protection des données (interdire la réidentification des personnes en présence de données anonymisées, interdiction d'utiliser les données pour prendre des mesures ou des décisions concernant des personnes, avertir le donneur de licence en cas de réidentification avérée ou possible, définir les limites de l'utilisation des données…). En outre une « *clause de protection des données* » dans ces contrats de licence seraient de nature à donner force exécutoire au respect des conditions posées.

Par ailleurs, la Commission nationale rappelle que des mesures techniques adéquates doivent être envisagées en fonction des risques identifiés (anonymisation des données[71], mesures visant à éviter le téléchargement massif de données).

Conclusion

En conclusion, la CNPD ne peut que souscrire aux principes insufflés par les deux projets de lois en vue d'une plus grande transparence de l'information publique et d'une meilleure exploitation des informations détenues par les organismes du secteur public. Elle estime toutefois que les évolutions que ces projets de textes sont censés apporter à la culture administrative et au système juridique luxembourgeois ne sont pas sans risque pour la protection de la vie privée et des données à caractère personnel.

La recherche d'un standard élevé de protection des données en est par conséquent le corollaire nécessaire et indispensable. Il en découlera un juste équilibre qui est de nature à conférer des bases solides aux évolutions que le législateur souhaite apporter à la culture et aux pratiques administratives actuelles.

[70] Avis 6/2013 précité, spéc. p. 29.
[71] Sur ce point, la Commission nationale renvoie aux recommandations du Groupe « Article 29 » dans son avis 05/2014 relatif aux techniques d'anonymisation, 10 avril 2014, WP 216.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 26 février 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis complémentaire de la Commission nationale pour la protection des données à l'égard du projet de loi n°6593 portant modification de la loi du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'Etat et de diverses autres lois

Délibération n°252/2016
du 4 mars 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 du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après : « la Commission nationale » ou « la CNPD ») a notamment pour mission d'aviser *« 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 »*.

Faisant suite à la demande lui adressée par Monsieur le Ministre de l'Education nationale, de l'Enfance et de la Jeunesse en date du 30 décembre 2015, lui demandant d'aviser les amendements gouvernementaux au sujet du projet de loi n°6593, la Commission nationale expose ci-après ses réflexions et commentaires au sujet des amendements en question.

La CNPD a émis son premier avis relatif au projet de loi sous objet en date du 25 juillet 2013[72].

De manière générale, la Commission nationale note avec satisfaction que la plupart des commentaires émis dans son précédent avis, ainsi que les remarques du Conseil d'Etat ayant trait à l'article 1 sous point 10 du projet de loi n°6593 dans son avis du 11 novembre 2014[73], ont été pris en compte lors de la rédaction du nouvel article 1er sous point 11 du projet de loi amendé sous examen (portant création d'un nouvel article 11*bis* dans la loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'Etat).

Il apparaît cependant que la refonte dudit projet de loi opérée à l'occasion des amendements gouvernementaux, ayant notamment pour conséquence la création de trois fichiers de données à caractère personnel, appelle de nouveaux commentaires de la part de la Commission nationale, plus amplement détaillés ci-dessous.

1. Les fichiers de données à caractère personnel créés

Il ressort du commentaire des articles du projet de loi sous objet, ainsi que du texte du projet d'article 11bis paragraphe 1er qui serait inséré dans la loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'Etat, que la refonte de ladite loi, ainsi que l'opérationnalisation de l'unité de sécurité du centre socio-éducatif de l'Etat, rendent nécessaire la création de trois fichiers de données à caractère personnel au sens de l'article 2 lettre (h) de la loi du 2 août 2002.

Dans le projet d'article 11*bis* paragraphe 1er, ces trois fichiers de données à caractère personnel sont dénommés comme suit:

- le « *dossier personnel pour chaque pensionnaire* » ;
- le « *registre de l'unité de sécurité* » ; et
- le « *registre spécial pour les fouilles corporelles* ».

Les paragraphes (2), (3) et (5) du projet d'article 11*bis* paragraphe 1er font référence tantôt à ces fichiers, tantôt à d'autres libellés ou dénominations, à savoir :

- le « *dossier individuel* », les « *dossiers individuels des pensionnaires* », les « *dossiers individuels des pensionnaires du centre* » ou les « *dossiers personnels des pensionnaires placés au centre* » ;
- le « *registre des entrées et sorties journalières des personnes ayant accès à l'unité de sécurité* » ; et
- le « *registre spécial des fouilles corporelles* ».

La Commission nationale comprend cependant que ces dénominations font référence respectivement au « *dossier personnel pour chaque pensionnaire* », au « *registre de l'unité de sécurité* », et au « *registre spécial pour les fouilles corporelles* ».

Dans un souci, d'une part, de cohérence entre les différents paragraphes du projet de loi sous objet, et d'autre part, d'utilisation de la terminologie de la loi du 2 août 2002, à savoir la notion de « *fichier de données à caractère personnel* » de l'article 2 lettre (h) de ladite loi, la CNPD propose de remplacer les diverses dénominations précitées par les termes suivants :

- le « *fichier individuel des pensionnaires* » ;
- le « *fichier de l'unité de sécurité* » ; et
- le « *fichier spécial des fouilles corporelles* ».

2. Les responsables de traitement

Les responsables de traitement des fichiers évoqués ci-avant sont indiqués dans le projet d'article 11*bis* paragraphe (2).

Ce paragraphe prévoit en effet que le Procureur général d'Etat est considéré comme le responsable du traitement en ce qui concerne « *le traitement des données à caractère judiciaire au sens de l'article 8 de la loi du 2 août 2002* », tandis que le directeur du centre est considéré comme le responsable du traitement en ce qui concerne « *le traitement des données à*

[72] Document parlementaire n°6593/01.
[73] Document parlementaire n°6593/07, pp. 12-13.

caractère administratif dans le cadre de l'hébergement et de l'encadrement du pensionnaire ».

Le commentaire des articles du projet de loi sous objet explique en effet que « *de par leur origine les données ont un caractère mixte, dans la mesure où les données saisies dans le cadre de la protection de la jeunesse revêtent un caractère judiciaire, tandis que les données saisies dans le carde de la gestion du centre et celles émanant du pensionnaire lui-même admettent un caractère administratif* »[74].

Comme l'indiquent les auteurs du projet de loi[75], les données relatives à la protection de la jeunesse constituent en effet des données judiciaires au sens de l'article 8 de la loi du 2 août 2002. Les travaux parlementaires de la loi du 2 août 2002 précisent à ce sujet « *qu'aucun traitement de données judiciaires n'est « réservé » à l'Etat, mais que les traitements de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peuvent être effectuées qu'en exécution d'une disposition légale. Cette disposition intègre, bien évidemment, les données relatives à la protection de la jeunesse* »[76]. La CNPD note qu'en l'occurrence, le traitement de données judiciaires serait effectué en exécution de l'article 11*bis* paragraphe (2).

Les auteurs du projet de loi concluent que, « *eu égard à la définition de la notion de responsable de traitement fournie par la loi modifiée du 2 août 2002 (…), on se trouve nécessairement en présence de deux responsables de traitement* »[77], en l'espèce le Procureur général d'Etat et le directeur du centre. Dès lors, la Commission nationale comprend, à la lecture du projet d'article 11*bis* paragraphe (2), que le Procureur général d'Etat d'une part, et le directeur du Centre d'autre part, doivent être considérés comme responsables conjoints de traitement, chacun pour ce qui concerne sa propre compétence.

Or, il est indiqué à trois reprises au paragraphe 1er du même article 11*bis*, que les trois fichiers de données à caractère personnels visés sont créés « *auprès le directeur du centre* ». La CNPD est à se demander si une telle formulation ne pourrait pas prêter à confusion, en laissant penser à la lecture du premier paragraphe que le directeur du centre devrait être considéré comme seul responsable de traitement. Dans ce contexte, les termes « *auprès le directeur du centre* » pourraient être supprimés.

3. Les finalités du traitement

La CNPD note avec satisfaction que les finalités des traitements de données à caractère personnel ont bien été précisées

[74] Commentaire des amendements gouvernementaux au projet de loi n°6593, p.30.
[75] Idem, en particulier la note de bas de page 9.
[76] Document parlementaire 4735/00, p.34.
[77] Commentaire des amendements gouvernementaux au projet de loi n°6593, p.30.

dans le projet d'article 11*bis* paragraphe (1).

Il s'agit des finalités suivantes :
- pour le « dossier personnel pour chaque pensionnaire » (fichier individuel des pensionnaires), *« documenter l'hébergement et l'encadrement de chaque pensionnaire placé dans les unités du centre »* ;
- pour le « registre de l'unité de sécurité » (fichier de l'unité de sécurité), *« aux fins de surveillance et du maintien de la sécurité de l'unité »* ;
- pour le « registre spécial pour les fouilles corporelles » (fichier spécial des fouilles corporelles), *« documenter la fouille corporelle entreprise »*.

Il ressort en outre des commentaires des articles[78] que les données figurant dans le fichier individuel des pensionnaires comprennent *« les données prescrites par les règles des Nations Unies pour la protection des mineurs privés de liberté »*, en particulier par la règle 21.

4. Les catégories de données traitées

La CNPD constate avec satisfaction que le projet d'article 11*bis* paragraphe (1) énumère de façon détaillée les catégories de données traitées.

En ce qui concerne la collecte et l'utilisation des données personnelles dans le cadre du fichier individuel des pensionnaires, la Commission nationale se réfère à son précédent avis relatif au projet de loi sous objet[79].

En particulier, compte tenu de la finalité d'authentification inhérente à la prise de photographie, ainsi que des explications fournies dans le commentaire de la première version du projet de loi, la collecte et le traitement d'une photographie d'identité paraissent légitimes et proportionnés aux yeux de la CNPD.

Par ailleurs, la Commission nationale note que la collecte de la confession du pensionnaire s'opère désormais de façon facultative. Cette précision répond partiellement au problème exprimé dans son précédent avis, selon lequel le traitement des données relatives à la confession n'est légitime et proportionné qu'à la condition que le consentement du pensionnaire soit libre. Afin d'enlever toute ambiguïté à ce sujet, il serait bienvenu de préciser dans le texte de l'article de loi que la collecte de cette donnée ne peut s'opérer que moyennant le consentement exprès de la personne concernée conformément à l'article 6 paragraphe (2) lettre (a) de la loi modifiée du 2 août 2002. En outre, le consentement doit être informé, ce qui implique que par exemple, une notice d'information devra clairement expliquer au pensionnaire quelle est la finalité de la collecte de cette information, que la collecte de données relatives à sa confession est facultative, et que le fait de refuser de répondre à une question relative à ses convictions religieuses ou philosophiques n'entraîne en aucun cas de conséquences négatives.

Enfin, en ce qui concerne les documents relatifs à la santé physique et mentale du pensionnaire, la Commission nationale se réfère à son précédent avis. En particulier, l'accès au dossier médical par le directeur du centre peut constituer une dérogation au secret médical qui serait en l'espèce prévue dans un texte légal, à savoir le projet d'article 11*bis* paragraphe (1).

Les catégories de données traitées dans le cadre du fichier de l'unité de sécurité, ainsi que du fichier spécial des fouilles corporelles, n'appellent quant à elles pas de commentaire particulier.

5. L'origine des données

Tout comme le projet de loi initial, le projet de loi tel qu'amendé ne spécifie pas l'origine des données. Le commentaire des articles précise cependant que *« les données saisies dans le cadre de la protection de la jeunesse revêtent un caractère judiciaire, tandis que les données saisies dans le cadre de la gestion du centre et celles*

[78] *Idem*, p. 28.
[79] Délibération n°386/2013 du 25 juillet 2013, document parlementaire n°6593/01, pp. 2-3.

émanant du pensionnaire lui-même admettent un caractère administratif »[80].

On peut en déduire que les données à caractère personnel figurant dans les trois fichiers précités peuvent présenter des origines différentes, sans que le texte de l'article en projet, ni le commentaire de l'article ne le précisent. En particulier, on ne comprend pas avec exactitude si les données sont transmises au centre par les autorités judiciaires compétentes en matière de droit de la jeunesse, si elles peuvent provenir également d'autres sources, notamment d'autres fichiers publics ou étatiques, et/ou si elles sont collectées directement auprès des pensionnaires par le personnel du centre.

6. Les personnes ayant accès aux données

Le paragraphe (3) du projet d'article 11*bis* prévoit désormais les personnes qui peuvent avoir accès aux fichiers précités. La CNPD se félicite de cette précision.

Il y a cependant lieu de constater qu'à l'exception de l'accès au fichier des fouilles corporelles, le texte de ce paragraphe (3) ne prévoit pas toujours quelles sont précisément les finalités relatives à l'exercice de ces différents accès. Ces finalités ressortent néanmoins du commentaire des articles.

Par ailleurs, le texte ne prévoit pas ce qu'il entend par « accès direct ». Si cela recouvre le cas d'une communication des données, la question de la manière dont cette communication a lieu et comment elle est sécurisée peut également être posée. Quoi qu'il en soit, il pourrait être utile de clarifier ce que l'on doit entendre par « *accès direct* », sinon de supprimer le mot « direct » si cette précision n'apparaît pas nécessaire.

Dans un souci de clarté juridique, sur base du texte du paragraphe (3) ainsi que des finalités ressortant du commentaire des articles[81], et en reprenant les dénominations des fichiers évoquées plus haut, la CNPD propose à titre d'exemple le libellé suivant :

« Peuvent avoir un accès au fichier individuel des pensionnaires, à l'exception des données visées aux alinéas 2 et 3 :

- *les membres du personnel socio-éducatif, du personnel psycho-social et du personnel médical du centre, afin d'assurer l'encadrement des pensionnaires pendant leur placement au centre,*

- *le procureur général d'Etat, le procureur d'Etat, les juges de la jeunesse, le directeur et son délégué, aux fins de décision et de gestion en rapport avec le placement des pensionnaires*

[80] Commentaire des amendements gouvernementaux au projet de loi n°6593, p. 30.
[81] *Idem*, pp. 31-32.

au centre, ainsi que dans l'exercice de leurs missions légales.

Peuvent avoir un accès au dossier médical du pensionnaire, figurant dans le fichier individuel des pensionnaires :
- *le personnel médical du centre, aux fins de médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements,*

- *le directeur du centre auquel est confié la garde du pensionnaire mineur et son délégué afin de pouvoir agir dans l'intérêt de la personne concernée lorsque sa santé est menacée, et afin de préserver le bien-être physique et mental de la personne concernée et des pensionnaires du centre.*

Peuvent avoir un accès aux données figurant au point 8 de la notice individuelle du fichier individuel des pensionnaires, le directeur du centre auquel est confiée la garde du pensionnaire mineur et son délégué afin de pouvoir agir dans l'intérêt de la personne concernée lorsque sa santé est menacée, et afin de préserver le bien-être physique et mental de la personne concernée et des pensionnaires du centre.

Peuvent avoir un accès au fichier de l'unité de sécurité :
- *les membres du personnel de garde de l'unité de sécurité afin de contrôler toutes les entrées et les sorties dans l'unité de sécurité,*

- *le procureur général d'Etat, le procureur d'Etat, les juges de la jeunesse, le directeur et son délégué, aux fins de décision et de gestion en rapport avec le placement des pensionnaires au centre, ainsi que dans l'exercice de leurs missions légales.*

Peuvent avoir un accès au fichier spécial des fouilles corporelles :
- *les membres du personnel de garde de l'unité de sécurité, les membres du personnel du centre autorisés à pratiquer les fouilles corporelles et le médecin requis pour réaliser la fouille intime, pour les seuls besoins de la saisine des données nécessaires pour documenter la fouille corporelle à réaliser,*

- *le procureur général d'Etat, le procureur d'Etat, les juges de la jeunesse, le directeur et son délégué, aux fins de décision et de gestion en rapport avec le placement des pensionnaires au centre, ainsi que dans l'exercice de leurs missions légales.*

Les personnes visées au paragraphe 3 ci-avant ayant reçu connaissance des données à caractère personnel visées par le présent article sont tenues au respect du secret professionnel par rapport à des tiers, sous peine des sanctions prévues par l'article 458 du Code pénal ».

7. Le traçage des accès aux données

La Commission nationale note avec satisfaction que les auteurs du projet de loi sous objet ont tenu compte de sa remarque concernant le traçage des accès aux données dans son avis du 25 juillet 2013, dans le paragraphe (4) du projet d'article 11bis. Ils expliquent s'être inspirés du projet de loi de l'article 4 du règlement grand-ducal du 26 septembre 2008 portant création des traitements de données à caractère personnel nécessaires à l'exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par la loi[82].

8. La durée de conservation des données

Le paragraphe (5) du projet d'article 11bis spécifie les durées de conservation des données figurant dans les différents fichiers précités. Les auteurs du projet de loi expliquent avoir voulu régler par cette disposition la question de la durée de conservation des données, soulevée par la CNPD dans son avis du 25 juillet 2013[83]. En particulier, ils expliquent qu' *« il est veillé à ce que la durée de conservation des données n'excède pas la durée*

[82] *Idem*, p. 33.
[83] *Idem*, p. 34.

qui est nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ».

La Commission nationale constate qu'au regard des explications fournies dans le commentaire des articles, les données seront en effet conservées pour une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées, conformément à l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002.

9. Articulation entre les différents paragraphes : proposition d'une nouvelle structure de l'article 11*bis*

Dans un souci d'une meilleure lisibilité du texte, la Commission nationale est à se demander s'il ne serait pas plus opportun d'adopter une même structure rédactionnelle pour ce qui concerne les trois fichiers créés. Au sein de cette structure, il pourrait être précisé, pour chaque fichier, ses finalités, les catégories de données contenues dans le fichier, le cas échéant l'origine des données, la durée de conservation des données et les personnes ayant accès aux données issues de ce fichier.

On pourrait par exemple prévoir trois paragraphes distincts pour chaque fichier, qui auraient à chaque fois la structure suivante :

« Il est créé un fichier (…) [cf. point 1 de cet avis].
Ce fichier a pour finalité(s) (…) et contient les données à caractère personnel suivantes : (…) [cf. points 3 et 4].
Ces données proviennent de (…) [cf. point 5].
Peuvent avoir accès au fichier (…) [cf. point 6].
La durée de conservation de ces données est de (…) [cf. point 8]».

Ensuite, on pourrait prévoir deux paragraphes séparés qui s'appliqueraient aux trois paragraphes précédents, l'un concernant les responsables de traitement [paragraphe 2 actuel du projet de loi, point 2 de cet avis], et l'autre relatif au traçage des accès aux données [paragraphe 4 du projet de loi, point 7 de cet avis].

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 4 mars 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données à l'égard de l'avant-projet de loi portant organisation d'un registre électronique national des entreprises de transport par route

Délibération n°496/2016
du 23 mai 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 a notamment pour mission d'aviser *« 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 »*.

Faisant suite à la demande lui adressée par Monsieur le Ministre du Développement durable et des Infrastructures en date du 15 février 2016, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi portant création d'un registre électronique national des entreprises de transport par route.

L'objectif général de l'avant-projet de loi sous analyse est la création d'un registre électronique des transporteurs afin de répondre notamment aux exigences des règlements CE suivants :

- Règlement (CE) n°1071/2009 du Parlement européen et du Conseil du 21 octobre 2009 établissant des règles communes sur les conditions à respecter pour exercer la profession de transporteur par route, et abrogeant la directive 96/26/CE du Conseil.

- Règlement (CE) n°1072/2009 établissant des règles communes pour l'accès au marché du transport international de marchandises par route.

- Règlement (CE) n°1073/2009 établissant des règles communes pour l'accès au marché international des services de transport par autocars et autobus, et modifiant le règlement (CE) n°561/2006.

- Règlement (CE) n°1213/2010 du 16 décembre 2010 établissant les règles communes concernant l'interconnexion des registres électroniques nationaux des entreprises de transport routier.

Ce registre électronique servira d'une part à gérer les entreprises de transports routiers ainsi que les autorisations de transports et d'autre part, à vérifier l'honorabilité ainsi que les capacités financières et professionnelles des gestionnaires de transport tel que requis par les dispositions des règlements CE précités. Le législateur européen a par ailleurs établi, au moyen des règlements précités, une liste uniformisée des catégories, types et niveaux de gravité des infractions aboutissant à une perte d'honorabilité des gestionnaires de transport. Les autorités compétentes de chaque Etat membre sont obligées de procéder à divers contrôles afin de vérifier si les entreprises de transport satisfont effectivement aux exigences posées par les règlements précités et surtout à l'obligation d'honorabilité. Une interconnexion des différents registres nationaux au niveau européen permet un échange d'informations rapide et efficace entre Etats membres et permet ainsi une application uniforme des dispositions précitées. Grâce à ce système, des infractions, des condamnations ou des sanctions prises à l'encontre d'une entreprise de transport seront également suivies d'effet (notamment par la perte de l'honorabilité) dans les autres Etat membres.

1. Article 2

Selon les dispositions de l'article 2 de l'avant-projet de loi sous analyse, le ministre ayant les transports dans ses attributions met en œuvre les traitements relatifs aux missions lui dévolues par les textes nationaux relatifs à la gestion des entreprises de transports routiers et par les règlements européens précités.

Dans sa rédaction actuelle, il ne ressort pas clairement du texte que le registre créé sert effectivement à traiter toutes les données nécessaires pour ces objectifs. En effet, ledit registre ne doit pas uniquement servir à satisfaire toutes les obligations imposées par les règlements européens précités, il doit également permettre au ministre d'effectuer toutes les missions lui imposées par la législation nationale[84].

Dès lors, l'article 2 pourrait prendre la teneur suivante :
« Art.2. (1) Le ministre ayant les transports dans ses attributions, désigné ci-après le « Ministre » tient un registre électronique des entreprises de transport par route aux fins de la gestion des entreprises de transports routiers et la délivrance et la gestion des autorisations de transports par route, ainsi que pour la mise en place et l'exploitation du registre électronique national des entreprises de transport par route prévu à l'article 16 du règlement (CE) n°1071/2009 précité.

(2) Dans ce registre figurent toutes les données nécessaires pour les finalités suivantes :

1. *délivrance et gestion des licences communautaires et des copies conformes telle que prévue à l'article 4 du règlement (CE) n°1072/2009 précité et à l'article 4 du règlement (CE) n°1073/2009 précité ;*
2. *délivrance et gestion des attestations de conducteur telle que prévue à l'article 5 du règlement (CE) n°1072/2009 précité ;*
3. *inscriptions des infractions et des retraits de licence communautaire ou de copies conformes telles que prévues à l'article 14 du règlement (CE) n°1072/2009 et l'article 24 du règlement (CE) n°1073/2009 ;*
4. *délivrance et gestion d'autorisations de transports bilatérales ou multilatérales ;*
5. *contrôles des entreprises de transports routiers ;*
6. *vérification de la capacité professionnelle et de l'honorabilité des gestionnaires de transport des entreprises de transports routiers ;*
7. *interconnexion avec les registres électroniques nationaux des autres Etats membres de l'Union européenne telle que prévue à l'article 16, paragraphe 5, du règlement (CE) n°1071/2009 précité ;*
8. *échange d'informations sur les infractions visées à l'article 6, paragraphe 1, point b), du règlement (CE) n°1071/2009 précité. »*

[84] cf. notamment les missions imposées par les dispositions de la loi du 30 juillet 2002 concernant l'établissement de transporteur de voyageurs et de transporteur de marchandises par route et portant transposition de la directive 98/76/CE du Conseil du 1er octobre 1998.

2. Article 3

L'article 3 désigne le ministre ayant les transports dans ses attributions en tant que responsable du traitement. Or, pour des raisons terminologiques, la CNPD propose de modifier cet article. En effet, l'on pourrait comprendre que le ministre obtiendrait la qualité de responsable en vertu des dispositions de la loi modifiée du 2 août 2002, alors que cette loi ne fait que définir la notion de responsable du traitement[85].

Dès lors, la Commission nationale suggère la modification suivante : *« Art. 3. Le Ministre a la qualité de responsable du traitement au sens de l'article 2, lettre (n) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel »*.

3. Article 4

L'article 4 de la loi organise la publicité de certaines données, tel que prévu par l'article 16, paragraphe 2, alinéa 3 du règlement CE n°1071/2009 précité. Les quatre catégories de données reprises à l'article 4 de l'avant-projet de loi font partie des données à minima qui doivent figurer dans les registres électroniques nationaux.

Selon les dispositions de l'article 16 du règlement CE précité, font également partie des données qui doivent figurer dans les registres nationaux le *« nombre, catégorie et type d'infractions graves telles que visées à l'article 6, paragraphe 1, point b) qui ont donné lieu à une condamnation ou à une sanction durant les deux dernières années »* ainsi que le *« nom des personnes déclarées inaptes à assurer la gestion des activités de transport d'une entreprise aussi longtemps que leur honorabilité n'a pas été rétablie, conformément à l'article 6, paragraphe 3, ainsi que les mesures de réhabilitation applicables »*.

Le règlement CE n°1071/2009 prévoit la possibilité pour les Etats membres de choisir de conserver ces deux dernières catégories de données dans des registres distincts. Cette faculté expresse s'explique au vu de la sensibilité des données judiciaires.

Il ressort de l'avant-projet de loi sous analyse que le Luxembourg va opter pour un registre unique, dans le cadre duquel toutes ces données se trouveront dans un même fichier. Dès lors, des mesures de sécurité technique et d'organisation suffisantes doivent être prises par le responsable du traitement ainsi que par son sous-traitant afin de garantir qu'uniquement les données de l'article 4 ne soient rendues publiques, à l'exclusion des données relatives aux infractions et des données relatives aux inaptitudes.

4. Article 5

a. L'énumération des données devant figurer dans le registre

L'article 5 précité établit une liste limitative des finalités pour lesquelles l'accès à certains fichiers tenus auprès d'autres entités étatiques doit être autorisé au responsable du traitement dans le cadre des missions lui dévolues en ce qui concerne le registre des entreprises de transports. La Commission nationale salue le degré de détail avec lequel les auteurs de l'avant-projet de loi précisent les données qui peuvent être accédées.

b. Nécessité d'identifier concrètement les fichiers visés par les accès

Le deuxième paragraphe de l'article 5 semble vouloir introduire un régime d'accès différent pour les données contenues dans le registre des entreprises ainsi que pour les données issues du casier et des fichiers exploités par la Police Grand-Ducale et l'Administration des Douanes et Accises, par rapport aux données visées au 1er paragraphe de l'article 5, points 1, 2 et 3.

La CNPD s'interroge sur la nécessité d'établir une différenciation du régime des accès entre les différents fichiers concernés. En effet, les modalités des accès doivent toujours être configurées de manière à permettre uniquement un accès si

[85] Loi modifiée du 2 août 2002 précitée, article 2, lettre (n).

un dossier a été introduit auprès du ministère précité ou si l'on se trouve dans le cadre de contrôles effectués par les autorités compétentes dans le domaine des transports routiers. A ce titre, la Commission nationale renvoie à son argumentation développée sous le point 4.3 ci-après.

La CNPD propose dès lors de biffer la première phrase du paragraphe 2 de l'article 5 « *De même, le registre…* » et de renuméroter les points 1. et 2. du deuxième paragraphe en conséquence.

Le point 2 du deuxième paragraphe fait état de plusieurs fichiers auxquels le responsable du traitement peut accéder, à savoir le fichier du casier judiciaire ainsi que les fichiers exploités par la Police Grand-Ducale et l'Administration des Douanes et Accises. Le casier judiciaire est réglementé dans la loi du 29 mars 2013 relative à l'organisation du casier judiciaire et aux échanges d'informations extraites du casier judiciaire entre les Etats-membres de l'Union européenne et fait, par ailleurs, actuellement l'objet d'une modification (projet de loi n°6820). Par contre, la simple indication « *des fichiers exploités par la Police Grand-Ducale et l'Administration des Douanes et Accises* » n'est pas précise et ne permet pas de savoir quels fichiers sont concrètement visés par un tel accès. S'agit-il du seul règlement grand-ducal du 21 décembre 2004 « *portant autorisation de la création d'un fichier des personnes ayant subi un avertissement taxé en matière de circulation routière et modification du règlement grand-ducal modifié du 7 juin 1979 déterminant les actes, documents et fichiers autorisés à utiliser le numéro d'identité des personnes physiques et morales* » ? Quels fichiers sont visés en ce qui concerne l'administration des Douanes et Accises ? La Commission nationale recommande dès lors d'énumérer séparément et individuellement tous les fichiers visés.

Par ailleurs, dans l'énumération des données accédées par les autorités précitées, qu'est-ce qu'il faut exactement comprendre par la catégorie « infractions » ? De quelles infractions s'agirait-il exactement? La CNPD propose que des précisions quant aux infractions concrètement visées soient intégrées dans le texte.

c. Prolifération des accès à divers fichiers étatiques et mise en place d'une solution technique

Il ressort de ce qui précède que le ministre ayant les transports dans ses attributions aura accès à une multitude de fichiers étatiques dans le cadre de la gestion des entreprises de transports routiers ainsi que des autres missions lui incombant en vertu des règlements CE précités.

Selon le principe de proportionnalité et de nécessité,

tout traitement de données à caractère personnel doit être proportionné aux finalités à atteindre, compte tenu du risque que le traitement fait peser pour la vie privée des personnes concernées. Dans le cadre de l'analyse des principes de la nécessité et de la proportionnalité d'un traitement de données, la Commission nationale se doit de vérifier s'il n'existe pas de moyens alternatifs, moins intrusifs et moins attentatoires à la vie privée des personnes concernées, mais permettant d'arriver aux mêmes finalités. Cette vérification des moyens alternatifs résulte notamment de la jurisprudence de la Cour de Justice de l'Union Européenne qui exige que « *les moyens mis en œuvre (…) soient aptes à réaliser l'objectif visé et n'aillent pas au-delà de ce qui est nécessaire pour l'atteindre* »[86].

Il s'agit en effet d'éviter une prolifération des accès d'une administration aux fichiers d'une autre administration, si ces accès n'apparaissent pas comme proportionnés et nécessaires par rapport aux intérêts publics distincts qu'elles poursuivent.

Les objectifs de gestion des entreprises de transports routiers et de vérification de l'honorabilité, de la capacité financière et de la capacité professionnelle des gestionnaires de transport doivent être mis en balance avec le droit pour les personnes concernées à la protection de leur vie privée. Ce dernier constitue un droit fondamental consacré notamment par l'article 11 (3) de la Constitution, par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ainsi que par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Il s'agit donc de vérifier si cette balance des intérêts penche en faveur du droit fondamental au respect de la vie privée, qui protège l'intérêt des citoyens, ou en faveur de l'intérêt légitime de l'administration, en tenant compte du critère de proportionnalité et de nécessité.

Un accès à un fichier d'une administration par une administration tierce laisse toujours courir un risque pour la vie privée des personnes concernées. Dans un souci de confidentialité et de sécurité des données au sens des articles 21 à 23 de la loi du 2 août 2002, il convient d'éviter tout risque d'abus ou de détournement de finalité.

Un des critères à prendre en compte en outre dans l'analyse du principe de proportionnalité et de nécessité est la proportion du nombre de personnes concernées par ces accès par rapport au nombre de personnes non concernées, mais dont les données seraient consultables par l'administration via un accès direct aux fichiers d'autres administration en cas d'un réexamen du dossier.

En l'espèce, le nombre de personnes concernées par le dispositif envisagé est limité aux gestionnaires de transport, aux conducteurs et au personnel de bureau indiqué sur les demandes ou aux personnes dont les données seront constatées lors d'un contrôle, donc un nombre assez limité de personnes. L'article 5 de l'avant-projet de loi, dans sa rédaction actuelle, permettrait cependant un accès aux données contenues dans des fichiers ou registres concernant l'ensemble ou la quasi-totalité de la population luxembourgeoise. En effet, tel serait par exemple le cas du registre national des personnes physiques, du fichier renseignant sur les véhicules immatriculés et du fichier du casier judiciaire.

La Commission nationale considère dès lors, pour ce qui concerne la version actuelle du texte sous examen, que le principe de proportionnalité et de nécessité n'est pas respecté au regard de la finalité envisagée.

Au vu de ce qui précède, la Commission nationale estime nécessaire, comme elle l'a déjà soulevé dans ses avis antérieurs relatifs à des textes de loi similaires[87], que soit prévue la mise en place d'une solution technique permettant de garantir, d'un point de vue informatique, que les agents du ministère du Développement durable et des Infrastructures puissent seulement accéder aux données concernant

[86] Arrêt du 9 novembre 2010, *Schecke et al.*, C-92/09 et C-93/09, point 74 et jurisprudence citée.

[87] Voir entre autres :
- Délibération n°69/2014 du 24 mars 2014 relative au projet de loi n°6612 relatif 1) au titre d'artiste, 2) aux mesures sociales au bénéfice des artistes professionnels indépendants et des intermittents du spectacle, 3) à la promotion de la création artistique ;
- Délibération n°339/2014 du 21 juillet 2014 relative au projet de loi n°6542 portant introduction d'une subvention de loyer et modifiant la loi modifiée du 25 février 1979 concernant l'aide au logement.
- Délibération n°37/2015 du 6 février 2015 précitée.

les personnes qui ont soit introduit une demande auprès du ministère précité, soit qui font l'objet d'un contrôle dans le cadre de la gestion des entreprises de transports routiers ou des obligations découlant des règlement européens précités.

Certes, l'article 10 contient certaines précisions à cet effet, mais il n'instaure qu'une limitation des accès pour certaines finalités. En effet, pour les finalités d'inscription des infractions et des retraits de licence communautaire ou dans le cadre d'échange d'informations sur les infractions, l'accès au fichier « *véhicules immatriculés au Luxembourg* », au registre des entreprises ainsi qu'au casier sera possible sans qu'un dossier lié à la personne concernée ne soit ouvert. Ceci permettrait en pratique au responsable du traitement de consulter l'intégralité des données de ces fichiers touchant, pour la plupart, la totalité de la population luxembourgeoise.

Or, il doit être exclu que des données de personnes non-concernées soient consultées. A ce titre, la CNPD rappelle qu'elle n'est pas convaincue de l'argument du contrôle a posteriori qui ne prévient pas les abus. En effet, un contrôle des « *logs d'accès* » ne permet que de détecter des abus, à condition bien entendu que de tels contrôles réguliers soient effectués.

Dans une optique de « *data protection by design* » qui, par ailleurs, est expressément prévue à l'article 25 du nouveau règlement général sur la protection des données[88] du 27 avril 2016, la Commission nationale estime que le texte de l'avant-projet sous analyse devrait être modifié de manière à limiter les accès de telle façon que les données des personnes non-concernées ne puissent pas être consultées.

d. Modifications terminologiques

La Commission nationale recommande de modifier la première phrase de l'article 5 de la manière suivante : « *Dans la poursuite des finalités décrites à l'article 2, paragraphe 2,* ***le responsable du traitement*** *peut accéder…* ». En effet, ce n'est pas le registre qui accède à des traitements de données à caractère personnel, mais le responsable du traitement, tel que défini à l'article 2, lettre (n) de la loi modifiée du 2 août 2002.

Par ailleurs, les points 1 à 3 du premier paragraphe ainsi que les points 1 à 2 du deuxième paragraphe de l'article 5 renvoient à des fichiers de données à caractère personnel au sens de l'article 2, lettre (h) de la loi modifiée du 2 août 2002. Pour des raisons de cohérence, il serait dès lors utile d'utiliser une même terminologie. L'article 5 précité pourrait donc prendre la teneur suivante : « *Dans la poursuite des finalités décrites*

[88] 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 abrogeant la directive 95/46/CE.

à l'article 2, paragraphe 2, le responsable du traitement peut accéder ***aux données issues des fichiers suivants*** *: … ».*

5. Article 6

La Commission nationale recommande de modifier l'article 6 d'un point de vue terminologique de la manière suivante : *« Le responsable du traitement reçoit en outre communication des données relatives aux infractions … Ces données sont enregistrées dans le registre dans le cadre des finalités décrites à l'article 5.».*

6. Article 7

A l'instar de ce qui a été précisé ci-avant à l'endroit de l'article 5, la CNPD propose de remplacer les termes de *« registre »* par *« le responsable du traitement »*, de manière à ce que l'article 7 pourrait prendre la teneur suivante : *« Le responsable du traitement peut communiquer les données contenues dans le registre aux registres électroniques nationaux … ».*

7. Article 9

L'article 9 précise les différents droits[89] des articles 10 à 12 et 14 issus de la directive 95/46/CE[90] et qui ont été transposés en droit national aux articles 26 et suivants de la loi modifiée du 2 août 2002. L'avant-projet de loi aurait simplement pu renvoyer à ces dispositions nationales.

Or, il s'avère que pour ce qui est du droit d'opposition, le règlement (CE) n° 1071/2009 du Parlement européen et du Conseil du 21 octobre 2009 établissant des règles communes sur les conditions à respecter pour exercer la profession de transporteur par route, et abrogeant la directive 96/26/CE du Conseil utilise une terminologie différente de celle de la directive 95/46/CE et de la loi modifiée du 2 août 2002.

8. Article 10

En ce qui concerne l'article 10, il est renvoyé aux arguments développés ci-avant, dans le cadre de l'analyse de l'article 5 (cf. point 4.4 ci-dessus).

9. Article 11

L'article 11 instaure le droit pour le responsable du traitement de communiquer certaines données à caractère personnel au Centre Commun de la Sécurité Sociale ainsi qu'à l'Inspection du Travail et des Mines, notamment afin de faire vérifier l'affiliation à la sécurité sociale ou de faire vérifier l'emploi légal des personnes contrôlées.

La Commission nationale ne s'oppose pas à une telle communication de données, mais considère cependant que les simples références à *« des données à caractère personnel »* relatives aux gestionnaires ou aux conducteurs sont trop vagues.

En effet, cette terminologie ne permet pas de savoir quelles données sont effectivement visées par une telle communication.

La CNPD estime dès lors que ces dispositions ne respectent pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal et ne peut pas être considérée comme conforme à l'article 4 de la loi modifiée du 2 août 2002. Elle estime dès lors nécessaire de préciser quelles données peuvent être communiquées.

10. Articles 12 et 13

La CNPD constate avec satisfaction que les auteurs de l'avant-projet de loi sous analyse ont intégré des dispositions relatives à la sécurité et à la confidentialité des données ainsi que d'avoir prévu des dispositions expresses quant à la mise en place d'un système de gestion des droits d'accès.

11. Article 14

L'article 14 traite du traçage des accès aux données. La Commission nationale tient à féliciter les auteurs d'avoir intégré ces dispositions très importantes, mais propose néanmoins une légère modification du texte proposé. Ainsi, l'article 14 pourrait avoir la teneur suivante :

« Le système informatique par lequel l'accès ou le traitement des données à caractère personnel

[89] Droit à l'information, droit d'accès, droit de rectification et d'effacement, droit d'opposition.
[90] Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données du 24 octobre 1995.

sont opérés doit être aménagé de la manière suivante :

- *L'accès aux fichiers est sécurisé moyennant une authentification forte ;*

- *Tout traitement des données reprises dans les banques et fichiers de données à caractère personnel qui sont gérés par le ministre ayant les transports dans ses attributions ou auxquels le ministre a accès, ainsi que toute consultation de ces données, ne peut avoir lieu que pour un motif précis qui doit être indiqué avec l'identifiant numérique personnel de la personne qui y a procédé. Le motif, la date et l'heure de tout traitement ou consultation ainsi que l'identité de la personne qui y a procédé doivent pouvoir être retracées dans le système informatique mis en place ;*

- *Les données de journalisation doivent être conservées pendant un délai de trois ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle. »*

12. Durée de conservation des données

Le projet de loi est muet sur la question de la durée de conservation des données enregistrées dans le registre électronique des entreprises de transport par route.

Selon l'article 16 paragraphe (3) du règlement 1071/2009 précité, *« Les données concernant une entreprise dont l'autorisation a été suspendue ou retirée sont conservées dans le registre électronique national pendant deux ans à compter de l'expiration de la suspension ou du retrait de la licence et sont ensuite immédiatement supprimées ».*

La CNPD estime dès lors utile de prévoir une disposition réglant la ou les durée(s) de conservation des données à caractère personnel dans le corps du texte national.

Ainsi décidé à Esch-sur-Alzette en date du 23 mai 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°6850 portant mise en place d'un statut spécifique pour certaines données traitées par le Service de Renseignement de l'Etat

Délibération n°566/2016
du 13 juin 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 10 mai 2016, Monsieur le Ministre d'Etat a invité la Commission nationale à se prononcer au sujet des amendements parlementaires au projet de loi n°6850 portant mise en place d'un statut spécifique pour certaines données à caractère personnel traitées par le Service de Renseignement de l'Etat.

La Commission tient à remarquer qu'elle a été saisie pour donner son avis relatif aux amendements parlementaires alors qu'elle n'avait pas été saisie au préalable pour donner son avis relatif au projet de loi originaire. La CNPD saisit donc l'occasion pour aviser l'entièreté du projet de loi pour ce qui est du volet protection des données.

Selon les auteurs du projet, ce dernier consacre une assise légale à la conservation des dossiers composant « les archives historiques » du Service de Renseignement de l'Etat en vue d'en autoriser les exploitations scientifiques à des fins historiques.

En exécution d'une des recommandations soulevées par la Commission d'enquête de *« confier le traitement, l'utilisation et la conservation à l'Institut culturel de Archives nationales de Luxembourg »*, les archives historiques du Service de Renseignement de l'Etat ont été déménagées le 3 octobre 2013 aux Archives nationales qui les a acceptées en vue de leur mise en dépôt au sens de l'article 21 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (dénommée ci-après la « loi CNPD »). Elles y sont déposées dans une pièce sécurisée, compte tenu de la classification des pièces y contenues, à laquelle le Service de Renseignement de l'Etat n'a plus accès sans autorisation des Archives nationales.

La finalité de cette exploitation scientifique objective des archives historiques est d'examiner, si le SRE a, pendant la période visée, effectué un espionnage de la vie et des activités politiques à Luxembourg ou s'il s'est tenu à l'observation des menaces contre l'Etat luxembourgeois telles que les menaces se présentaient pendant la Guerre Froide.

En outre, l'objet du projet de loi est de garantir une objectivité du travail scientifique et historique et de régler certains aspects juridiques touchant notamment à l'accès des pièces classifiées au sens de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité (dénommée ci-après la « Loi ANS ») et au sort à réserver aux données à caractère personnel au sens de la loi CNPD.

La Commission tient tout d'abord à féliciter les auteurs du projet de loi pour les amendements formulés et plus particulièrement le changement de l'intitulé du projet de loi sous avis. La Commission partage l'avis du Conseil d'Etat à ce sujet. Le nouvel intitulé reflète le fait que le projet n'a vocation à s'appliquer qu'à une partie des documents détenus par le SRE, à savoir à la seule *« banque des données tenue par le SRE,*

constituée d'un fichier de données à caractère personnel établi sur support papier, à savoir des cartes nominatives comportant des références qui renvoient à des microfiches,..., ainsi que les doubles de ces documents,... » et cela encore seulement pour les fiches et dossiers établis sur une période délimitée dans le temps, à savoir les années entre 1996 et 2000. La nouvelle définition à l'article 2 en tient parfaitement compte.

La CNPD tient ensuite à formuler des observations relatives au stockage des données traitées à l'article 3 du projet de loi, ainsi qu'au droit d'accès par les personnes concernées tel que règlementé par l'article 5 du projet de loi.

Observations quant à l'article 3

De par leur caractère sui generis, les pièces composant les « *archives historiques* » du SRE sont largement constituées de données à caractère personnel protégées par la loi CNPD.

Selon le § 11 de l'article 3, le directeur du Service de renseignement de l'Etat est désigné responsable du traitement pendant l'exercice de la mission des experts et les Archives nationales sont à considérer comme sous-traitant du Service de renseignement de l'Etat au sens des dispositions de la loi CNPD.

La Commission s'interroge sur les missions de l'équipe des experts au sens de la même loi. Des obligations particulières sont imposées tant au responsable du traitement, qu'à son sous-traitant, notamment pour ce qui est des mesures de sécurité et de confidentialité décrites aux articles 22 et 23 de la loi CNPD. Parmi les obligations qu'incombent aux experts en vue de garantir un traitement légitime des données, ils devraient être soumis aux mêmes règles de sécurité que les sous-traitants.

Ceci est d'autant plus important que les auteurs du projet de loi ont, contrairement à ce qui est le cas tant pour les agents du Service de renseignement de l'Etat, que des membres de l'autorité de contrôle de l'article 17, choisi, par dérogation à l'article 14 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, d'exempter les experts de l'obligation d'être titulaires d'une habilitation de sécurité. La Commission regrette que le projet soit muet à ce sujet et qu'il ne précise pas les conditions et modalités d'utilisation des données par les experts pendant leur mission. Les experts doivent-ils accomplir leur mission au sein d'un local dédié et sécurisé ? Peuvent-ils transposer les dossiers, les copier, les enregistrer sur des supports fixes ou mobiles, etc... ? Ces questions méritent d'être abordées.

Observations quant à l'article 5

La Commission note avec satisfaction que l'accès aux et l'utilisation de certaines données à caractère personnel par le SRE sont encadrés de manière stricte afin de concilier la vie privée des personnes concernées et les besoins de la recherche historique. Une autre manière de procéder aurait risqué de porter atteinte aux droits des personnes concernées. En effet, il est probable que certaines d'entre elles aient déjà été victimes d'une violation de la législation sur la protection des données, puisqu'il semble que des données personnelles les concernant qui n'étaient pas nécessaires ou n'étaient plus nécessaires à partir d'un certain moment aient été conservées pendant une période excessive. Il convient donc désormais de protéger ces personnes contre la curiosité éventuelle de leurs concitoyens afin d'éviter qu'elles ne soient, le cas échéant, « victimes » une seconde fois.

L'article 5 permet, sous certaines conditions et réserves, une communication des données à caractère personnel à toute personne concernée qui en fait la demande.

A ce sujet, le Conseil d'Etat observe ce qui suit :

« Les dispositions proposées vont au-delà de la loi précitée du 2 août 2002 en ce que la mission de l'autorité de contrôle visée à l'article 17 de cette loi dépasse celle y inscrite, étant donné que cette autorité pourra autoriser une communication – certes éventuellement limitée conformément aux dis¬positions du projet – du dossier au demandeur, et ne devra pas se borner, ainsi que cela est le cas dans la loi précitée du 2 août 2002, à simplement „informer la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exé¬cution", sans pouvoir accorder un droit d'accès direct. »

Selon le Conseil d'Etat, le projet de loi vise à créer un régime dérogatoire au droit commun quant aux traitements de données personnelles par le SRE pendant la période visée au projet et qui vient se substituer uniquement pour ces traitements et pour cette période de temps en tant que lex specialis à la loi précitée du 2 août 2002, qui reste entièrement applicable pour les autres traitements effectués par le SRE. Il met de même en place un régime dérogatoire à la législation applicable aux archives.

Afin de relever la différence entre le régime spécial instauré par le projet de loi sous avis et la procédure telle que prévue à l'article 17 de la loi CNPD, la Commission propose de remplacer dans l'article 5 paragraphe 2 tel qu'amendé la mention *« conformément à la procédure prévue à l'article 17, paragraphe 2, alinéa 5 de la loi modifiée du 2 août 2002 précitée »* par la mention *« par l'intermédiaire de l'autorité de contrôle prévue à l'article 17, paragraphe 2, alinéa 1 de la loi du 2 août 2002 précitée »*.

En effet, dans sa formulation actuelle, le passage de texte dont le remplacement est proposé, risque de prêter à confusion voire, est contradictoire avec le début de la même phrase de l'article 5 paragraphe 2 projeté, qui prévoit justement des modalités d'accès plus favorables à la personne concernée que celles de la procédure prévue à l'article 17, paragraphe 2, alinéa 5 de la loi modifiée du 2 août 2002. Appliquer la procédure de l'article 17 paragraphe 2, alinéa 5 signifierait que l'autorité prévue à l'article 17 de la loi modifiée du 2 août 2002 du traitement devrait se borner à *« informer la personne concernée que le traitement en question ne contient aucune donnée contraire aux conventions, à la loi et à ses règlements d'exécution »* et ne permettrait pas une communication des données à caractère personnel à la personne concernée telle que prévue au début de la phrase de l'article 5 paragraphe 2 projeté.

En ce qui concerne le champ d'application dans le temps de l'article 5 paragraphes 1 à 3

régissant le droit d'accès des personnes concernées, la CNPD constate que les auteurs du projet distinguent entre les personnes concernées qui introduisent une demande d'accès pendant la mission des experts et ceux qui aux termes du deuxième paragraphe, *« ont déjà »* effectué une telle demande. Faut-il déduire des paragraphes 1 et 2, que le régime spécial ne s'appliquerait explicitement que pour les personnes concernées ayant introduit une demande avant le début de la mission des experts ? Or, à suivre le raisonnement du Conseil d'Etat sur le régime spécial dérogatoire à la procédure originaire prévue à l'article 17 de la loi CNPD pour les personnes concernées, le projet de loi crée une procédure unique applicable aux personnes intéressées pour la durée de la mission des experts. Afin d'éviter tout soupçon de discrimination entre les personnes concernées en raison du moment d'introduction de leur demande, la Commission conseille de préciser la procédure applicable pour les personnes visées au premier paragraphe, voire de fusionner les deux premiers paragraphes.

Le Conseil d'Etat soulève la question du droit d'accès après la fin de la mission des experts. Celui-ci semble être réglé par le régime général instauré par la loi CNPD d'une part, et les règles applicables à l'archivage, d'autre part. Les responsables du traitement et leurs sous-traitants devront le moment venu s'assurer d'exécuter les traitements conformément aux dispositions applicables en matière de protection des données et d'archivage.

Ainsi décidé à Esch-sur-Alzette en date du 13 juin 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données relatif aux « Procédures de mise en œuvre du Protocole d'Accord conclu entre le Gouvernement du Grand-Duché de Luxembourg et les Etats-Unis d'Amérique pour l'échange d'informations de détection du terrorisme »

Délibération n°568/2016 du 20 juin 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 sa délibération n°366/2015 du 30 juillet 2015, la Commission nationale a rendu un avis portant conjointement sur le projet de loi n°6759 portant approbation du „Memorandum of Understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information", signé à Luxembourg le 20 juin 2012 et le projet de loi n°6762 portant approbation de l'Accord entre le Gouvernement de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave, signé à Luxembourg le 3 février 2012.

Dans ce contexte, par courrier du 31 décembre 2015, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du document *« Procédures de mise en œuvre du Protocole d'Accord conclu entre le Gouvernement du Grand-Duché de Luxembourg et les Etats-Unis d'Amérique pour l'échange d'informations de détection du terrorisme »*.

Ledit document est censé faire figure d'*« implementing procedures to be agreed between the Parties arising under this Memorandum of Understanding »* telles que prévues par différentes dispositions du Protocole d'Accord conclu entre le Gouvernement du Grand-Duché de Luxembourg et les Etats-Unis d'Amérique pour l'échange d'informations de détection du terrorisme qui a fait l'objet du projet de loi d'approbation n°6759.

Dans le présent avis, la Commission nationale limite son analyse aux aspects devant faire l'objet de telles *« implementing procedures »* en vertu dudit Protocole d'Accord.

Plus précisément ce sont - outre l'article II paragraphe 1 qui pose le principe même du recours aux accords de mise en œuvre - les articles III paragraphe 1, III paragraphe 2, IV et V paragraphe 11 du Protocole d'Accord qui renvoient aux procédures de mise en œuvre.

L'accord de procédure de mise en œuvre sous avis se réfère, dans son préambule, aux trois dernières des quatre dispositions susmentionnées, mais non à l'article III paragraphe 1.

Cet article III paragraphe 1 renvoie aux procédures de mise en oeuvre pour la détermination des *« points of contact and the individuals responsible for handling encounter, technical, and redress matters »*.
La Commission nationale se demande si cet article fera ultérieurement l'objet d'un accord de mise en œuvre supplémentaire.

Les articles III paragraphe 2 et IV du Protocole d'Accord renvoient aux « implementing procedures » pour ce qui est du déroulement pratique des échanges de données avant, respectivement après une éventuelle « encounter » / « rencontre ».

La Commission nationale constate que sur ce point, les Procédures

de mise en œuvre étoffent les principes contenus dans le Protocole d'accord par un bon nombre de précisions.

L'article V paragraphe 11 du Protocole d'accord renvoie aux « *implementing procedures* » pour ce qui est des procédures de « *complaint* » (ou « *recours* » selon la terminologie en langue française des Procédures de mise en œuvre).

Tout comme le Protocole d'accord, le texte de procédure de mise en œuvre ne précise pas devant qui le recours doit être exercé. S'agirait-il peut-être d'une réclamation auprès de l'institution même qui a traité les données plutôt que d'un recours devant une autorité (administrative ou judiciaire) indépendante ?

Par ailleurs, la portée de ce « recours » risque d'être très limitée. En effet, au regard des textes du Protocole d'accord et des Procédures de mise en œuvre, il semble que le « recours » ne puisse pas porter sur toutes questions de licéité et de conformité aux règles de protection des données mais seulement sur des questions relatives à l'exactitude des données. Si tel est le cas, faut-il comprendre que d'autres règles ou principes sujets à contestations en seraient exclus, telles que la proportionnalité du traitement, la durée de conservation des données ou le respect des finalités du traitement ?

Eventuellement, le recours prévu dans les Procédures de mise en œuvre s'apparente plus au droit de rectification[91] à exercer auprès du responsable du traitement qu'à une véritable voie de recours.

Enfin, pour pouvoir exercer un recours à l'encontre d'un traitement de données, il faut avoir connaissance de l'existence de ce traitement. Ceci peut s'avérer difficile en l'espèce, puisque le Protocole d'accord ne prévoit pas de dispositions relatives au droit à l'information ou au droit d'accès.

Pour le surplus, la Commission nationale renvoie aux développements dans son avis du 30 juillet 2015 (délibération n°366/2015).

La CNPD tient encore à relever qu'un accord-cadre dénommé « EU-U.S. Umbrella Agreement » relatif à la protection des données dans les cas de transferts transatlantiques de données dans le domaine des enquêtes, de la prévention, de la recherche et de la poursuite d'infractions pénales a été signé par les Etats-Unis d'Amérique et l'Union européenne en date du 2 juin 2016 et pourrait bientôt entrer en vigueur en cas de vote favorable du Parlement européen[92]. Les garanties en termes de protection des données y prévues vont au-delà de ce qui est prévu par le Protocole d'accord et les procédures de mise en œuvre précités. La Commission

[91] tel que prévu notamment par l'article 28 paragraphe (4) de a loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.
[92] http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf

nationale se demande quelle sera l'articulation entre les règles relatives à la protection des données du Protocole d'accord et des procédures de mise en œuvre et celles plus favorables aux personnes concernées et donc plus protectrices de l'« Umbrella Agreement » une fois en vigueur. Est-ce que les règles de l'« Umbrella Agreement » primeront sur les accords bilatéraux conclus entre les Etats-Unis d'Amérique et le Grand-Duché de Luxembourg ?

En tout état de cause, il serait largement préférable que le Protocole d'accord et les procédures de mise en œuvre contiennent d'office des garanties au moins aussi protectrices que celles de l'« Umbrella Agreement ».

Elle tient aussi a signaler que depuis le dépôt du projet de loi n°6759, l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire C 362/14 (« arrêt Schrems ») est intervenu. La CNPD doute que les principes résultant dudit arrêt soient respectés par le Protocole d'Accord ainsi que par l'Accord entre le Gouvernement de Luxembourg et le Gouvernement des Etats-Unis d'Amérique aux fins du renforcement de la coopération en matière de prévention et de lutte contre le crime grave, signé à Luxembourg le 3 février 2012 faisant l'objet du projet de loi d'approbation n°6762.

Ainsi décidé à Esch-sur-Alzette en date du 20 juin 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°6708 relative au contrôle de l'exportation, du transfert, du transit et de l'importation des biens de nature strictement civile, des produits liés à la défense et des biens à double usage ; au courtage et à l'assistance technique ; au transfert intangible de technologie ; à la mise en œuvre de résolutions du Conseil de sécurité des Nations unies et d'actes adoptés par l'Union européenne comportant des mesures restrictives en matière commerciale à l'encontre de certains Etats, régimes politiques, personnes, entités et groupes ainsi que sur le projet de règlement grand-ducal portant exécution de la présente loi relative au contrôle des exportations

Délibération n°611/2016 du 6 juillet 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 a notamment pour mission d'aviser *« 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 11 juillet 2014, Monsieur le Ministre de l'Economie a invité la Commission nationale à se prononcer au sujet du projet de loi n°6708 relative au contrôle de l'exportation, du transfert, du transit et de l'importation des biens de nature strictement civile, des produits liés à la défense et des biens à double usage ; au courtage et à l'assistance technique ; au transfert intangible de technologie ; à la mise en œuvre de résolutions du Conseil de sécurité des Nations unies et d'actes adoptés par l'Union européenne comportant des mesures restrictives en matière commerciale à l'encontre de certains Etats, régimes politiques, personnes, entités et groupes (ci-après : « projet de loi ») ainsi que sur le projet de règlement grand-ducal portant exécution de la présente loi relative au contrôle des exportations.

Suivant l'exposé des motifs, le projet de loi « *s'inscrit dans une logique de simplification administrative et de codification réformatrice dans le domaine du contrôle de l'exportation, de l'importation et de transit des marchandises et de certains biens dits sensibles* ».

L'article 37 paragraphe (3) du projet de loi prévoit que *le traitement, par l'Office du contrôle des exportations, importations et du transit, des données à caractère personnel collectées dans le cadre de ses missions, 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 Commission nationale se pose la question de savoir sur quelle base légale exacte de la loi modifiée du 2 août 2002, le législateur entend justifier la nécessité de recourir à un règlement grand-ducal pour encadrer les traitements effectués par l'Office du contrôle des exportations, importations et du transit (ci-après « l'Office »).

La Commission nationale s'interroge dès lors de savoir si le législateur entend prévoir un règlement grand-ducal sur base de l'article 17 de la loi précitée en raison de la nature particulière des produits visés par les opérations d'exportations, d'importations et du transit, à savoir des produits liés à la défense.

En effet, l'article 17 de la loi modifiée du 2 août 2002 dispose que les traitements relatifs à la sûreté de l'Etat à la défense et à la sécurité publique font l'objet d'un règlement grand-ducal.

En raison de l'absence de précisions dans le projet de règlement grand-ducal quant

aux traitements de données effectuées, la Commission nationale n'est, à ce stade, pas en mesure d'apporter un avis éclairé ni sur le contenu du projet de loi lui-même, ni sur le projet de règlement grand-ducal portant exécution. De ce fait, la Commission nationale se limite à quelques observations et plus spécifiquement à l'article 37 du projet de loi qui dispose que :

« (1) L'Office du contrôle des exportations, importations et du transit est habilité à donner accès aux documents conservés dans le cadre de l'exercice de ses attributions à toute administration nationale et internationale, et aux services externes dûment commis par ces dernières pour autant qu'un tel accès soit nécessaire afin de permettre au Grand-Duché de Luxembourg de remplir ses engagements internationaux.

(2) L'Office du contrôle des exportations, importations et du transit est habilité à correspondre avec la Commission européenne et les autres instances d'organisations intergouvernementales auxquelles le Grand-Duché de Luxembourg a adhéré, pour tout ce qui a trait aux attributions de l'office du contrôle des exportations, importations et du transit telles que déterminées par la présente loi et aux engagements du Luxembourg vis-à-vis de ces organisations.

L'Office du contrôle des exportations, importations et du transit est autorisé à consulter, traiter et utiliser les données figurant dans les bases de données constituées dans le cadre de l'Union européenne et des régimes, organismes et traités internationaux de contrôle des exportations tels que définis dans la proposition 2000/401/PESC du Conseil du 22 juin 2000 relative au contrôle de l'assistance technique liée à certaines destinations finales militaires.

(3) Le traitement, par l'Office du contrôle des exportations, importations et du transit, des données à caractère personnel collectées dans le cadre de ses missions, 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 Commission nationale attire l'attention des auteurs du projet de loi et du règlement grand-ducal que la loi modifiée du 2 août 2002 s'applique exclusivement aux données à caractère personnel qui concernent des *personnes physiques identifiées ou identifiables ; une personne physique est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique*[93]. Par conséquent, les traitements de données concernant exclusivement des personnes morales ne tombent pas dans le champ d'application de la présente loi. Autrement dit, la loi modifiée du 2 août 2002 s'applique uniquement aux traitements effectués par l'Office qui comprennent des données relatives à des personnes physiques.

La Commission nationale souhaite également attirer l'attention des auteurs du projet de loi et du règlement grand-ducal sur l'arrêt de la Cour constitutionnelle du 29 novembre 2013, selon lequel *« l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements »*[94]. La CNPD se réfère également à un récent avis du Conseil d'Etat selon lequel *« dans les matières réservées à la loi formelle, l'exercice du pouvoir réglementaire par le Grand-Duc est subordonné à l'existence d'une disposition législative spécifiant les fins, les conditions et les modalités dans lesquelles un règlement grand-ducal peut être pris »*[95]. La Commission nationale estime dès lors que le projet de loi devrait préciser d'une part, qui est le responsable de traitement et d'autre part, quelles sont les finalités des traitements.

[93] Article 2 lettre (e) de la loi modifiée du 2 août 2002.
[94] Cour constitutionnelle, arrêt 108/13 du 29 novembre 2013 (Mém. A n°217 du 13 décembre 2013, p.3886).
[95] Avis du Conseil d'Etat du 9 décembre 2014 à l'égard du projet de loi 6588 portant organisation du secteur des services de taxis et modification du code de la consommation, p.11 (article 5). Voir aussi p.19 (article 20).

Quant au responsable du traitement, il ressort de l'article 36, paragraphe (2) du projet de loi que l'Office est placé sous l'autorité d'un membre du gouvernement qui en assume la responsabilité administrative et politique. Les autorisations pour les opérations portant sur des biens de nature strictement civile, sur les produits liés à la défense, sur les biens susceptibles d'être utilisés en vue d'infliger la peine capitale, la torture ou d'autres peines ou traitements cruels, inhumains ou dégradants, sur les biens à double usage et quant au transfert intangible de technologie sont délivrées par le ministre ayant le Commerce extérieur dans ses attributions. Par conséquent, il y a lieu de considérer le ministre ayant le Commerce extérieur dans ses attributions comme responsable du traitement au sens de l'article 2 lettre (n) de la loi modifiée du 2 août 2002.

Quant aux finalités du traitement, la Commission nationale estime que celles-ci auraient dû être précisées d'ores et déjà dans le projet de loi. L'article 4 paragraphe (1) de la loi modifiée du 2 août 2002 dispose que les données doivent être collectées pour des *finalités déterminées, explicites et légitimes*, et qu'elles ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités. En vertu du principe de finalité, les données à caractère personnel ne peuvent être traitées qu'en vue d'une ou de plusieurs finalités légitimes, ce qui implique qu'il doit toujours y avoir une raison concrète pour laquelle les données à caractère personnel seront traitées, et que cette raison doit être établie précisément avant le début du traitement. Ce principe est un des principes de base de la protection des données. Par conséquent, la CNPD estime que les termes « *collectées dans le cadre de ses missions* » repris à l'article 37 paragraphe (3) du projet de loi définissent de manière trop vague les finalités du traitement. Ainsi, afin d'apporter une meilleure visibilité aux finalités des traitements de données, il y aurait lieu de définir limitativement au sein du projet de loi, les finalités exactes qui justifient la collecte des données à caractère personnel.

Par ailleurs, l'article 37 paragraphe (1) du projet de loi définit de manière trop vague les catégories de destinataires auxquelles les données peuvent être communiquées. Le Conseil d'Etat dans son récent avis du 7 juin 2016 précise également que « *la loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication* »[96]. La Commission nationale estime qu'il aurait été préférable de définir de manière plus précise les différentes administrations nationales et internationales et services externes dûment habilités à accéder aux

[96] Avis du Conseil d'Etat du 7 juin 2016 à l'égard du projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures, p.5 (article 11).

données et que le règlement grand-ducal aurait pu définir les différentes catégories de données auxquelles chaque destinataire aurait droit d'accéder.

Enfin, comme le mentionne l'exposé des motifs du projet de règlement grand-ducal nous soumis ensemble avec le projet de loi relative au contrôle des exportations, un règlement grand-ducal devra être ultérieurement pris, en raison de la considération nécessaire de circonstances non encore connues à ce jour ou d'autres motifs, pour les traitements de données à caractère personnel collectées par l'Office du contrôle des exportations, importations et du transit (ci-après « l'Office »). Etant donné qu'un tel projet de règlement grand-ducal fait actuellement défaut, la CNPD n'est pas en mesure de formuler d'autres observations.

Ainsi décidé à Esch-sur-Alzette en date du 6 juillet 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données à l'égard du projet de règlement grand-ducal fixant les modalités d'application de la législation portant organisation des services de taxis

Délibération n°612/2016 du 6 juillet 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 du 2 août 2002 »),la Commission nationale pour la protection des données a notamment pour mission d'aviser *« 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 6 juin 2016, Monsieur le Ministre du Développement durable et des Infrastructures, a invité la Commission nationale à aviser le projet de règlement grand-ducal

1) fixant les modalités d'application de la législation portant organisation des services de taxis ;
2) modifiant l'arrêté grand-ducal modifié du 23 novembre 1955 portant règlementation de la circulation sur toutes les voies publiques ;
3) modifiant le règlement grand-ducal modifié du 26 août 1993 relatif aux avertissements taxés, aux consignations pour contrevenants non-résidents ainsi qu'aux mesures d'exécution de la législation en matière de mise en fourrière des véhicules et en matière de permis à points ;
4) modifiant le règlement grand-ducal modifié du 19 novembre 2010 portant réglementation de la circulation sur les voies et places ouvertes à la circulation publique aux abords de l'Aérogare de Luxembourg ;
5) modifiant le règlement grand-ducal du 5 novembre 2015 portant réglementation de la circulation sur les voies et places ouvertes à la circulation publique aux abords de la Gare de Luxembourg ;
6) abrogeant le règlement grand-ducal du 9 juillet 2004 fixant les prix maxima pour des courses de taxi et ;
7) abrogeant le règlement grand-ducal modifié du 3 décembre 1997 portant règlementation des services de taxis à l'aéroport.

La Commission nationale observe qu'elle a seulement été saisie à un moment avancé de la procédure d'élaboration du projet de règlement grand-ducal et qu'elle limite ses observations à quelques points du texte intitulé *« Texte coordonné du projet de règlement grand-ducal après amendements gouvernementaux »* tel qu'en l'état en date du 6 juin 2016.

En ce qui concerne l'intitulé du chapitre V du projet de règlement grand-ducal sous analyse, elle suggère de modifier le titre « *Données des fichiers* » par celui de « *Données traitées* ».

A toutes fins utiles, la Commission nationale voudrait relever une erreur matérielle au premier paragraphe de l'article 14 qui devrait comporter le numéro (1) au lieu du numéro (2).

Dans le cadre des trois catégories de données traitées, à savoir celles relatives à « *l'exploitant personne physique* », celles relatives à « *l'exploitant société commerciale* » et celles relatives au « conducteur de taxis », le numéro d'identification est énuméré dans chacune de ces trois catégories. Alors que la Commission nationale comprend que les auteurs du texte sous examen entendent faire référence au numéro d'identification du registre national des personnes physiques introduit par la loi modifiée du 19 juin 2013[97], elle suggère de le préciser dans le texte, afin d'éviter tout risque de confusion. Dès lors, il serait utile de rajouter à chaque mention du numéro d'identification les termes « *du registre national des personnes physiques* ».

En ce qui concerne le traitement des photographies des conducteurs de taxi, la Commission nationale constate avec satisfaction que le texte précise que celles-ci ne peuvent être conservées que pendant une durée de deux mois après la délivrance de la carte de conducteur et qu'à l'expiration de ce délai, elles doivent être supprimées automatiquement et irréversiblement.

En ce qui concerne le paragraphe (2) de l'article 14, la Commission nationale propose la modification suivante : « *Les données qui peuvent être communiquées à la SNCA en vertu du paragraphe 10 de l'article 18 de la loi du XXX portant organisation des services de taxi sont les données suivantes : … ».* Considérant que l'exploitant, le taxi et le taximètre sont énumérés dans la liste qui suit, leur première énumération est redondante.

Ainsi décidé à Esch-sur-Alzette en date du 6 juillet 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

[97] 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.

Avis de la Commission nationale pour la protection des données relatif aux avant-projets de règlements grand-ducaux 1) précisant les données accessibles et les données communiquées en exécution des articles 4 et 6 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves, 2) pris en exécution de l'article 5 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves, et 3) fixant le modèle et les modalités de délivrance, d'utilisation et de retrait de la carte d'élève « myCard »

Délibération n°613/2016 du 6 juillet 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 du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser *« 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 21 octobre 2015, le Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse (ci-après « le ministre ») a invité la Commission nationale à se prononcer au sujet :

- de l'avant-projet de règlement grand-ducal précisant les données accessibles et les données communiquées en exécution des articles 4 et 6 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves,

- de l'avant-projet de règlement grand-ducal pris en exécution de l'article 5 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves, et

- de l'avant-projet de règlement grand-ducal fixant le modèle et les modalités de délivrance, d'utilisation et de retrait de la carte d'élève « myCard ».

Les objectifs de ces avant-projets de règlements grand-ducaux sont de compléter la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves (ci-après la « loi du 18 mars 2013 »), notamment en fixant le détail des données à caractère personnel pouvant être accédées ou communiquées dans le cadre des différents cas de figure énumérés limitativement aux articles 4 et 6 de la loi, de fixer les critères et les conditions d'accès aux données, les modalités d'octroi et de retrait des autorisations d'accès, la périodicité de la révision des accès et la durée de leur validité conformément à l'article 5 de la loi, et d'arrêter le modèle ainsi que les modalités de délivrance, d'utilisation et de retrait de la carte d'élève « myCard » conformément à l'article 3, paragraphe (1), point 5 de la loi.

1) En ce qui concerne l'avant-projet de règlement grand-ducal précisant les données accessibles et les données communiquées en exécution des articles 4 et 6 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves

L'article 1er de cet avant-projet de règlement grand-ducal énumère les données à caractère personnel contenues dans huit fichiers différents gérés par d'autres autorités administratives, auxquelles le ministre peut accéder en vertu de l'article 4 de la loi du 18 mars 2013. L'énumération des données relatives aux différents fichiers inclut chaque fois le « matricule » des élèves. La Commission nationale souligne à ce titre qu'en vertu de l'article 46 de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, toute référence au « matricule » (ou au « numéro d'identité ») doit dorénavant faire référence au « numéro d'identification ».

L'article 2 de l'avant-projet de règlement grand-ducal précise ensuite quelles données seront mises à disposition des autorités et entités en vertu de l'article 6 de la loi du 18 mars 2013.

Cependant, il y a un manque de cohérence entre la liste des autorités et entités figurant à l'article 6 de la loi du 18 mars 2013, qui peuvent recevoir communication des données, et la liste des autorités et entités énumérées à l'article 2 de l'avant-projet de règlement grand-ducal. Ainsi, les autorités et entités ont été regroupées dans l'article 2 de l'avant-projet de règlement grand-ducal au lieu d'avoir été indiquées séparément comme dans la loi. De plus, l'ordre d'énumération de ces tiers à l'article 6 de la loi du 18 mars 2013 ne correspond pas à celui proposé à l'article 2 de l'avant-projet de règlement grand-ducal. La Commission nationale estime dès lors que, pour des raisons de facilité de lecture voire d'application en pratique par les acteurs concernés, il serait utile d'aligner la liste des tiers dans l'article 2 de l'avant-projet de règlement grand-ducal sur celle de l'article 6 de la loi du 18 mars 2013 et, en outre, de suivre le même ordre dans l'énumération des tiers dans le règlement grand-ducal que dans le texte de la loi.

Aux termes de l'article 6, alinéa 1er, point 5 de la loi, « *le ministre est autorisé à communiquer…des données à caractère personnel relatives aux élèves … à l'Institut national pour le développement de la formation professionnelle continue, aux fins de constitution d'un échantillon représentatif de profils et de parcours scolaires d'élèves pour suivre ceux-ci au passage de la formation initiale à la formation continue ou à la vie active* ».Toutefois, l'avant-projet de règlement grand-ducal ne détermine pas quelles données peuvent être communiquées à cet établissement. La Commission nationale recommande donc de préciser dans le règlement grand-ducal la liste des données pouvant faire l'objet d'une communication à l'Institut national pour le développement de la formation professionnelle continue.

L'article 2, point 9 de l'avant-projet prévoit que les chambres professionnelles et les conseillers à l'apprentissage pourront recevoir certaines données à caractère personnel du ministre. Or, l'article 6 de la loi du 18 mars 2013 limite la communication des données aux seuls conseillers à l'apprentissage. Pourtant, en incluant les chambres professionnelles dans les tiers pouvant recevoir communication des données, l'avant-projet de règlement grand-ducal ne maintient pas la même limitation des personnes, établie par la loi, qui peuvent être destinataires des données.

La Commission nationale suggère dès lors que la référence aux

chambres professionnelles soit supprimée du texte de l'article 2, point 9 de l'avant-projet de règlement grand-ducal, ou bien que les auteurs du texte justifient l'inclusion des chambres professionnelles et précisent quelles chambres professionnelles sont visées.

Par ailleurs, en ce qui concerne les données pouvant être communiquées aux conseillers à l'apprentissage, la Commission nationale note que ceux-ci auraient accès aux données à caractère personnel des élèves tant sur base de l'article 2, point 1 que sur base de l'article 2, point 9 de l'avant-projet sous examen. Dans un souci de clarté, la Commission nationale recommande dès lors de regrouper, sous un seul point de l'article 2, toutes les données pouvant être communiquées aux conseillers à l'apprentissage.

2) En ce qui concerne l'avant-projet de règlement grand-ducal pris en exécution de l'article 5 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves

L'article 5 de la loi du 18 mars 2013 dispose que « *l'accès aux données et la possibilité de les traiter sont gérés par un système de gestion des identités et des droits d'accès. Ce système constitue la base de la gestion des droits d'accès, de leur attribution à leur suppression, à l'échelle de toutes les données, pour tous les membres de l'administration de l'Education nationale ainsi que pour les partenaires de l'Ecole appelés à intervenir sur des données en vertu de la législation scolaire* ».

Le présent avant-projet de règlement grand-ducal a donc pour vocation de déterminer « *les critères et conditions d'accès aux données, les modalités d'octroi et de retrait des autorisations d'accès, la périodicité de la révision des accès et la durée de leur validité* ».

L'article 1er dispose que le ministre gère un système d'accès aux données des élèves, « provisionné » de manière automatisée par le biais de son fichier du personnel nommé « SYCLOPE » en ce qui concerne les « *membres du personnel de l'administration de l'Education nationale* ». À ce titre, la Commission nationale relève que la première phrase de l'article 1er de l'avant-projet fait double emploi avec la première phrase de l'article 5 de la loi et pourrait donc être supprimée.

L'article 2 prend soin d'énumérer les différentes catégories du personnel pouvant accéder aux données des élèves, à savoir :

- les « membres du personnel enseignant, éducatif et psycho-social »,
- les « membres du personnel administratif des lycées », et
- les « membres du personnel administratif des services et administrations du ministère ».

Les auteurs du texte projeté renvoient simplement vers un approvisionnement du système de gestion des droits d'accès « de manière automatisée » par le fichier du personnel « SYCLOPE » au lieu de préciser, comme requis par le paragraphe (2) de l'article 5 de la loi du 18 mars 2013, « *les critères et conditions d'accès aux données* » ou de renvoyer au moins vers un descriptif dudit fichier. Un règlement grand-ducal pris en exécution d'une loi n'apporte guère de plus-value et ne présente pas des garanties juridiques suffisantes s'il se contente de renvoyer vers une simple référence (nom d'un logiciel informatique) au lieu de définir lui-même les critères d'accès aux données. En outre, la Commission nationale émet ses réserves quant à l'emploi des termes « *qui en est une source autoritaire* » qui ne remplissent pas non plus les conditions de précision et de sécurité juridique nécessaires.

Contrairement aux alinéas 2 et 3, l'alinéa 1 de l'article 2 ne définit pas explicitement la personne qui est chargée d'octroyer ou de retirer l'accès aux données des élèves par les membres du personnel enseignant, éducatif et psycho-social. La CNPD suggère dès lors de compléter cet article en précisant justement la

personne ou le service qui est en charge d'octroyer et de retirer les accès pour cette catégorie.

Elle estime par ailleurs que les termes « *en fonction de leur profil* » utilisés à l'article 2, alinéas 2 et 3 de l'avant-projet de règlement n'apportent pas de sécurité juridique suffisante étant donné que la notion de « *profil* » est une notion assez vague qui risque d'entraîner la possibilité pour certaines catégories de personnes d'avoir accès aux données alors que leurs missions ne le nécessitent pas. Il est dès lors suggéré de remplacer les termes « *en fonction de leur profil* » par « *en fonction de leurs attributions spécifiques* », ce qui présuppose que chaque membre du personnel accède aux données dans un cadre strictement limité à sa tâche professionnelle, définie si possible au préalable par le directeur, le chef de service ou le chef d'administration.

En ce qui concerne les membres du personnel administratif des lycées, des services et administrations du ministre, l'avant-projet de règlement prévoit à l'article 3, alinéa 2 une durée de validité des droits d'accès correspondant à la « *durée de leur mission* ». Sur ce point, la Commission nationale rend les auteurs de l'avant-projet de règlement grand-ducal particulièrement attentif au fait qu'en cas de changement d'affectation du membre du personnel, le chef de service respectivement le chef d'administration devront veiller à vérifier si les nouvelles attributions du membre du personnel nécessitent de maintenir ou non l'accès aux données des élèves. Par conséquent, il y aurait lieu de préciser, dans le cadre de l'alinéa 2 de l'article 3 de l'avant-projet de règlement grand-ducal, une obligation de révision des accès lors de chaque changement d'affectation d'un membre du personnel.

De plus, elle estime que le terme « *mission* » pourrait être remplacé par les termes « tâches professionnelles ». Elle propose dès lors de modifier l'alinéa 2 de l'article 3 de l'avant-projet de règlement grand-ducal par le libellé suivant : « *Pour les membres du personnel administratif des lycées, des services et administrations du ministère, l'accès aux données des élèves est octroyé pour la durée de leur tâches professionnelles. En cas de changement d'affectation d'un membre du personnel, le chef de service respectivement le chef d'administration est tenu de vérifier s'il y a lieu de maintenir ou de retirer son accès aux données des élèves en fonction de ses nouvelles tâches professionnelles* ».

3) En ce qui concerne l'avant-projet de règlement grand-ducal fixant le modèle et les modalités de délivrance, d'utilisation et de retrait de la carte d'élève « myCard »

L'article 3, paragraphe (1), point 5 de la loi du 18 mars 2013 a instauré l'identification et l'authentification de l'élève moyennant une carte d'élève. L'objet du présent avant-projet de règlement grand-ducal est d'arrêter le modèle ainsi que les modalités de délivrance, d'utilisation et de retrait de cette carte, conformément à l'article précité.

Les auteurs du texte rappellent que depuis son introduction en 2007, la carte « myCard », destinée au départ uniquement à l'authentification et au paiement électronique au restaurant scolaire - a évoluée vers une *« carte d'identité scolaire multiservices »*. À part sa fonction d'identification, la carte peut héberger diverses fonctions d'authentification et de paiement électroniques. Elle peut notamment être utilisée, entre autres, pour :

- l'emprunt de livres à la bibliothèque du lycée,
- l'accès aux salles de classe ou salles didactiques du lycée,
- l'accès aux bâtiments du lycée,
- l'accès aux parkings du lycée,
- l'accès et le paiement auprès du service de photocopies du lycée,
- l'accès et le paiement auprès du service d'impression du lycée,
- l'authentification sur les postes de travail du lycée,
- l'accès au restaurant scolaire et à la cafétéria du lycée,
- le paiement électronique au restaurant scolaire et à la cafétéria du lycée,
- l'accès au transport scolaire pour les élèves.

Le texte de l'avant-projet de règlement grand-ducal définit en effet :

- le modèle de la carte, par le biais de l'article 5 (informations figurant sur la carte),
- les modalités de délivrance, par le biais des articles 3 (délivrance et restitution de la carte) et 4 (personnalisation, renouvellement et remplacement de la carte),
- les modalités d'utilisation, par le biais des articles 8 (vol ou perte de la carte) et 9 (responsabilité de l'utilisation et de la conservation, interdictions),
- les modalités de retrait, par le biais de l'article 10 (droit de retrait par le ministre).

L'article 3, alinéa 3 prévoit que l'élève doit restituer la carte au moment où il quitte l'enseignement luxembourgeois.

Afin d'éviter une utilisation abusive de la carte dans l'hypothèse où l'élève ne la restitue pas, la Commission nationale suggère de compléter cet article par une disposition qui prévoit la désactivation des fonctionnalités électroniques de la carte.

Il résulte de l'article 4 que le traitement relatif à la gestion des cartes (personnalisation, renouvellement et remplacement) s'effectue par le responsable d'école qui peut à son tour désigner des personnes habilitées à personnaliser des cartes.

En ce qui concerne l'article 4, alinéa 4, point 7, la Commission nationale suggère d'en modifier les dispositions pour rendre les obligations du responsable d'école plus contraignantes lorsqu'il est amené à traiter les photographies des élèves pour la personnalisation des cartes. A ce titre, elle souligne la disposition non équivoque de l'article 3, paragraphe 2, dernier alinéa de la loi du 18 mars 2013 qui oblige le responsable du traitement, après une période de conservation de deux mois, de supprimer *« automatiquement et irrévérsiblement »* les photographies. Ainsi, elle propose le libellé suivant pour l'article 4, alinéa 4, point 7 : *« le responsable d'école se charge de la gestion des photos ; il veille à ce que les photos numériques ne soient utilisées que pour la personnalisation des cartes et qu'elles soient supprimées du fichier conformément à l'article 3, paragraphe 2, dernier alinéa de la loi du 18 mars 2013 ».*

En ce qui concerne l'article 10, la Commission nationale recommande de préciser davantage les modalités de retrait de la carte en soulignant qu'il était du vœu exprès du Conseil d'Etat que soient détaillés dans un règlement grand-ducal *« le modèle de la carte et les modalités de délivrance et de retrait »* (doc. parl. 6284/11 – amendement 11). Dans l'état actuel, l'article 10 n'apporte guère de plus-value par rapport à l'article 3, paragraphe 1, point 6 de la loi du 18 mars 2013.

En outre, en ce qui concerne le retrait de la carte par le ministre, la Commission nationale suggère de compléter cet article, à l'instar de sa proposition à l'article 3, alinéa 3, par une disposition qui prévoit la désactivation des fonctionnalités électroniques de la carte en cas d'utilisation frauduleuse.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 6 juillet 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de règlement grand-ducal pris en exécution de la future loi portant réorganisation du Service de Renseignement de l'Etat et au projet de règlement grand-ducal pris en exécution de la loi du 15 juin 2004 relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité

Délibération n°639/2016 du 13 juillet 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 deux courriers du 8 juin 2016, Monsieur le Premier Ministre a invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif aux modalités de traitement des données à

caractère personnel par le Service de renseignement de l'État, règlement à prendre en exécution de la future loi portant réorganisation du Service de Renseignement de l'Etat votée à la Chambre des Députés en date du 9 juin 2016 (projet de loi n°6675) et au sujet du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité, règlement à prendre en exécution de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

La Commission nationale passe en revue les articles qui donnent lieu à observations.

I. Le projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par le Service de renseignement de l'État

Ad article 3

L'article 3 aborde la question des données à caractère personnel que le Service de renseignement est en droit de traiter.

La Commission nationale rappelle dans ce contexte que l'*avant-projet de règlement grand-ducal portant création et fixant les modalités de fonctionnement d'un fichier relatif au traitement de données à caractère personnel par le Service de Renseignement de l'Etat* soumis à la CNPD pour avis en 2013 comportait en son article 5 une longue énumération des catégories de données pouvant être traitées. A ce titre, la CNPD avait formulé un grand nombre d'observations relatives à cette énumération[98] qu'elle souhaite réitérer pour les besoins du présent avis. Elle s'étonne que l'actuel projet de règlement sous avis ne contienne plus cette énumération des catégories de données.

Le règlement grand-ducal à prendre en vertu de l'article 10 paragraphe (1) de la future loi portant réorganisation du Service de Renseignement de l'Etat est pourtant censé donner des précisions relatives aux traitements de données qui peuvent être effectués par le Service de renseignement. Or, la formulation utilisée (« toutes données… ») à l'article 3 est à tel point vague et générale qu'on peut se demander s'il y a des limites quant à l'étendue de la collecte des données ou quelles sont les données qui ne peuvent pas être traitées par le Service de renseignement. La CNPD estime que l'article 3 dans sa teneur actuelle ne satisfait pas à l'article 8 paragraphe 2 de la Convention européenne des droits de l'homme et des libertés fondamentales qui exige que toute ingérence dans la vie privée par une autorité publique doit nécessairement reposer sur une base légale ou réglementaire suffisamment précise (voir aussi les développements à l'article 9 in fine du présent avis).

Pour ce qui est plus précisément des données sensibles mentionnées à la lettre c) de l'article 3, la Commission nationale regrette que le texte sous avis permette leur traitement d'une manière aussi généralisée. Rappelons que sont visés « *les traitements qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions, religieuses ou philosophiques, l'appartenance syndicale, ainsi que les traitements de données relatives à la santé et à la vie sexuelle, y compris le traitement des données génétiques* »[99]. La CNPD s'interroge sur la nécessité du traitement des données relatives à la santé et à la vie sexuelle est excessif. L'avant-projet de règlement soumis à la CNPD pour avis en 2013 excluait expressément le traitement de données relatives à la santé et à la vie sexuelle.

Ad article 4

Selon l'article 4 du projet de règlement sous avis, il « *sera procédé à un réexamen de la nécessité de conserver les données traitées au plus tard tous les dix ans* ».

La Commission nationale considère que ce délai de dix ans est excessivement long, eu égard notamment au caractère en partie très sensible des données et eu égard au fait que

[98] Avis de la Commission nationale pour la protection des données relatif à l'avant-projet de règlement grand-ducal pris en exécution de l'article 4 de la loi modifiée du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat et à l'avant-projet de règlement grand-ducal pris en exécution de l'article 23 de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, délibération n°274/2013 du 28 juin 2013 http://www.cnpd.public.lu/fr/decisions-avis/2013/sre/index.html

[99] article 6 paragraphe (1) la loi modifiée du 2 août 2002.

les personnes concernées ne sauront normalement pas qu'elles font l'objet d'un traitement de données à caractère personnel. Rappelons que l'avant-projet de règlement soumis à la CNPD pour avis en 2013 prévoyait un délai de réexamen de cinq ans seulement et que la CNPD plaidait dans son avis du 28 juin 2013 pour un délai de trois ans.

La CNPD salue cependant que ce délai commence à courir à partir du premier enregistrement d'une donnée à caractère personnel concernant la personne visée en relation avec la finalité ayant donné lieu au traitement des données concernées.

Ad article 7

L'article 7 traite des autorisations d'accès à accorder par le Directeur du Service de renseignement.

Il serait préférable que les agents bénéficiant d'une autorisation d'accès n'aient pas d'office accès à l'intégralité de la partie active, mais qu'il soit précisé dans le règlement que les droits d'accès soient limités aux besoins de chaque agent eu égard à ses missions en fonction de critères objectifs définis dans une procédure interne.

Il serait par ailleurs indiqué de préciser dans le règlement qu'en cas de réaffectation interne d'un agent ou d'un changement de ses missions, les autorisations devront être adaptées ou retirées en fonction du nouveau poste ou des nouvelles missions.

Enfin, même si cela semble aller de soi, il ne serait pas inutile de préciser que toute autorisation devrait être retirée quand un agent quitte le Service de renseignement de manière temporaire ou définitive. A ce titre, la CNPD renvoie au rapport annuel de Autorité de contrôle spécifique « Article 17 » pour les années 2014 et 2015 qui aborde la question des mutations entre les services de police d'un côté et le Service de renseignement de l'autre.[100]

Ad article 8

Selon l'exposé des motifs, *« une attention particulière a été portée à la journalisation des accès aux données à caractère personnel pour un meilleur suivi et contrôle des consultations ou des traitements effectués par les différents agents du SRE »*.

Or, l'article 8 paragraphe (2) ne fait que poser le principe de la conservation des données de journalisation. La Commission nationale estime qu'il est nécessaire de prévoir, dans le texte du règlement grand-ducal, une obligation de contrôler, sur base régulière, les données de journalisation (telles que définies à l'article 9 du projet de règlement grand-ducal), afin de détecter d'éventuels abus.

[100] Rapport annuel de Autorité de contrôle spécifique « Article 17 » pour les années 2014 et 2015, page 10 en bas et page 15
http://www.cnpd.public.lu/fr/publications/rapports/groupe_article17/rapport_1415.pdf
cf aussi : Scéance publique de la Chambre des Députés du 10 mai 2016
http://visilux.chd.lu/ArchivePage/video/1718/sequence/75133.html

En outre, la Commission nationale recommande de préciser la procédure prévue pour enregistrer et traiter les données de journalisation mentionnée dans l'article 8 paragraphe (2) afin de garantir une transparence accrue de la gestion de ces données. Il serait important :

- de mettre en œuvre des mesures (par exemple de type cryptographique) pour garantir l'intégrité du contenu de la journalisation : le contenu ne doit pas pouvoir être manipulé, et plus particulièrement par la possibilité de modification ou de suppression des enregistrements ;
- de garantir la confidentialité (par exemple de type cryptographique) du contenu de la journalisation.

Par ailleurs, la Commission nationale considère qu'il est primordial de conserver des sauvegardes des fichiers contenant les données de journalisation, afin de prévenir la perte de la continuité et de la disponibilité de ces données (par exemple, suite à leur suppression par un attaquant). Enfin, il est important que des protocoles de sécurité répondant à l'état de l'art soient utilisés pour garantir la confidentialité et l'intégrité des données de journalisation lors de leur transfert du système de conservation de ces données vers le système de sauvegarde.

Ad article 9

La Commission note avec satisfaction que sont établis des fichiers de journalisation comprenant, outre les informations relatives à l'agent ayant procédé au traitement, la date, l'heure et aussi les informations relatives au motif de l'accès conformément à l'article 10 du projet de loi n°6675.

Elle estime cependant que le délai de conservation des fichiers de journalisation de 3 ans est insuffisant, eu égard au caractère partiellement sensible des données, mais également eu égard aux antécédents en matière de traitements de données du Service de renseignement non conformes à la loi.

Dès lors, la Commission nationale suggère que ce délai soit porté à 5 ans. Il convient de relever que la prescription des délits, et notamment des infractions à la législation sur la protection des données (par exemple l'accès non autorisé ou abusif à des données), est de 5 ans. Or, une conservation des fichiers de journalisation pendant seulement 3 ans risquerait, dans de nombreux cas, de rendre impossible de fait des poursuites judiciaires au-delà de cette durée de 3 ans.

La Commission nationale note encore que article 12 de l'avant-projet de règlement lui soumis pour avis en 2013 prévoyait la communication de données aux autorités judiciaires, aux autorités de police et aux administrations, ainsi qu'aux organismes de renseignement et de sécurité étrangers. Si le présent projet de règlement sous avis ne contient plus de dispositions à ce sujet, le principe de ces communications a cependant été maintenu au niveau de la loi avec l'article 9 de la future loi portant réorganisation du Service de Renseignement de l'Etat.
La CNPD réitère à ce sujet sa demande formulée en 2013 que les communications de données en question devraient être retraçables et faire l'objet d'une documentation.

Enfin, la CNPD regrette que le gouvernement n'ait pas profité de l'occasion pour inclure, dans le projet de règlement grand-ducal sous avis, des précisions relatives à la question de l'accès par le Service de renseignement à des systèmes informatiques prévu à l'article 8 paragraphe (1) lettre c) de la future loi portant réorganisation du Service de Renseignement de l'Etat. En effet, cette mesure de surveillance pouvant être mis en œuvre par le Service de renseignement porte par nature une atteinte grave au droit au respect de la vie privée et à la protection des données à caractère personnel des personnes en faisant l'objet. Une telle atteinte ne saurait être admise que si elle apparaît strictement nécessaire au but

poursuivi et si des garanties suffisantes sont prévues, de nature à garantir la proportionnalité des dispositifs de surveillance mis en œuvre. En particulier, la Commission nationale rappelle que de tels mesures ou dispositifs de surveillance doivent, conformément à l'article 8 paragraphe 2 de la Convention européenne des droits de l'homme et des libertés fondamentales, ainsi qu'à la jurisprudence de la Cour de Strasbourg en la matière, reposer sur une base légale suffisante et être mis en œuvre dans des conditions permettant d'assurer un juste équilibre entre l'ingérence dans la sphère privée de la personne surveillée à son insu et les troubles à l'ordre public susceptibles de résulter d'activités qui pourraient menacer la sécurité nationale.

La CNPD renvoie à ce sujet à ses développements exhaustifs, exposés au point 7.3. dans son avis (délibération n°147/2016) du 12 février 2016 relatif au projet de loi n°6921 portant adaptation de la procédure pénale face aux besoins liées à la menace terroriste[101].

Il résulte de ce qui précède qu'il est primordial que le gouvernement prévoit dans le projet de règlement grand-ducal sous examen ou dans un projet de règlement grand-ducal séparé des règles précises quant à la question soulevée ci-avant, afin de satisfaire aux exigences de la Convention européenne des droits de l'homme et des libertés fondamentales ainsi qu'à la jurisprudence de la Cour de Strasbourg en la matière.

II. Le projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité

A titre liminaire, la CNPD note que son avis a été demandé sur le projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par l'Autorité nationale de Sécurité, mais qu'elle n'a pas été saisie pour avis en ce qui concerne le projet de loi n°6961 portant modification 1. de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 2. du Code pénal.

Ad article 3

La CNPD regrette que le texte ne donne aucune précision sur l'origine des données. Le texte devrait au moins faire une distinction entre les données que le demandeur d'une habilitation doit fournir lui-même et celles qui sont collectées à partir d'autres fichiers étatiques ou encore par d'autres moyens de recherche.

En ce qui concerne les catégories de données pouvant faire l'objet d'un traitement, l'article

[101] http://www.cnpd.public.lu/fr/decisions-avis/2016/lutte-terrorisme/147-2016-PL6921.pdf

ne contient pas d'énumération explicite des catégories de données à l'image de l'article 5 de l'avant-projet de règlement lui soumis pour avis en 2013, mais ne fait que renvoyer aux critères d'appréciation de l'article 24 bis projeté de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité tel que prévu par le projet de loi n°6961 sans pour autant fournir davantage de détails.

En ce qui concerne par exemple des données relatives à *« la mise en accusation dans des affaires judiciaires, y compris des affaires de mœurs »*, on peut se demander à partir de quel stade (enquête préliminaire, instruction, décision de renvoi de la chambre du conseil) on peut considérer quelqu'un comme « mis en accusation » au sens de l'article en question. On pourrait aussi se poser la question si l'utilisation du terme « accusation » se réfère de manière spécifique aux affaires criminelles ou aux affaires pénales en général. Il semble également étonnant qu'on se réfère de manière expresse aux affaires de mœurs.

Pour ce qui est des données relatives à l'insolvabilité, il se pose également la question de savoir de quelles données il s'agit précisément et quelle est leur source. Fait-on référence à des procédures judiciaires civiles liées au surendettement ? Or, si on accorde à l'ANS un accès aux données relatives à ces procédures, il faudrait le prévoir de manière plus explicite à l'article 22 de la loi du 15 juin 2004 dans sa version du projet de loi n°6961. Le Luxembourg ne dispose pas non plus de banque de données publique contenant des données relatives à la solvabilité à l'image de la Centrale des crédits aux particuliers de la Banque nationale de Belgique ou des Fichiers d'incident bancaire de la Banque de France. Et même si une telle banque de donnée existait dans le futur, elle devrait être citée à l'article 22 de la loi du 15 juin 2004 dans sa version du projet de loi n°6961 afin que l'ANS puisse y avoir accès. Est-ce que les données pourraient provenir par exemple de banques ? Mais dans ce cas, le secret bancaire ne pourrait-il pas être opposé à l'ANS ? Ou ces données seraient-elles simplement fournies par la personne concernée avec tous les risques de fiabilité que cela comporterait.

Ces incertitudes soulèvent encore une fois l'importance de la détermination par voie règlementaire de l'origine des données.

Ad articles 7, 8 et 9

La CNPD renvoie à ses observations faites ci-dessus relatives aux articles 7, 8 et 9 du projet de règlement grand-ducal relatif aux modalités de traitement des données à caractère personnel par le Service de renseignement de l'État.

Enfin, la CNPD tient encore à faire quelques observations relatives au droit d'accès.

A défaut de dispositions spécifiques, les règles de l'article 17 de la loi modifiée du 2 août 2002 s'appliqueront, règles ne permettant qu'un droit d'accès « indirect » extrêmement limité.

Or, la question des habilitations de sécurité ne saurait être traitée sur un pied d'égalité avec des mesures policières ou des mesures de services de renseignements qui visent à élucider respectivement à prévenir des infractions pénales en partie très graves et où un droit d'accès direct risquerait d'anéantir les efforts des autorités en question.

La CNPD est dès lors à se demander s'il ne serait pas plus approprié d'introduire, par voie légale, un droit d'accès direct selon les règles de droit commun de l'article 28 de la loi modifiée du 2 août 2002 à l'instar d'autres pays. En cas d'application du droit d'accès direct de droit commun, les exceptions prévues par l'article 29 de la loi modifiée du 2 août 2002 s'appliqueraient le cas échéant. Alternativement aux exceptions de l'article 29, on pourrait, en cas de besoin, prévoir des exceptions

spécifiques au droit d'accès en matière d'habilitations de sécurité. A titre d'exemple de disposition prévoyant un droit d'accès (direct) assorti d'exceptions, on pourrait se référer à l'article 23 du *Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz - SÜG) allemand*[102].

Quel qu'il en soit, d'éventuelles dispositions relatives à un droit d'accès direct devraient au moins avoir une base légale dans la future loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité (projet de loi n°6961), le règlement grand-ducal d'exécution pouvant tout au plus compléter ou préciser les dispositions de la loi.

Ainsi décidé à Esch-sur-Alzette en date du 13 juillet 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis complémentaire de la Commission nationale pour la protection des données à l'égard du projet de loi n°6893 relative à la reconnaissance des qualifications professionnelles

Délibération n°660/2016 du 20 juillet 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 « la loi du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser *« 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 6 juillet 2016, Monsieur le Ministre délégué à l'Enseignement supérieur et à la Recherche a sollicité la CNPD d'aviser les amendements adoptés par la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace en date du 24 juin 2016[103] concernant le projet de loi n°6893 relative à la reconnaissance des qualifications professionnelles. Ayant avisé le prédit projet de loi n°6893 en date du 17 décembre 2015, la CNPD se limite à formuler

[102] http://www.gesetze-im-internet.de/s_g/__23.html
[103] Cf. doc. parl.n°6893/08 du 24 juin 2016.

quelques observations relatives aux amendements.

Elle note avec satisfaction que les auteurs du projet de loi l'ont suivie en son avis, alors qu'à l'article 56 ont été supprimées les références aux directives 95/46/CE et 2002/58/CE et qu'il est fait référence directement à la loi modifiée du 2 août 2002. Par ailleurs, elle constate que les auteurs ont également suivi la recommandation conjointe du Conseil d'Etat[104] et de la Commission nationale[105] en supprimant les mesures de publicité visées à l'article 59 du projet de loi concernant la date de naissance, ainsi que l'adresse du professionnel concerné. Dans le même article, le terme « *banque de donnée électronique* » a été remplacé par « *fichier électronique* » comme suggéré par le Conseil d'Etat et la Commission nationale dans leurs avis respectifs.

Néanmoins, la CNPD réitère sa recommandation exprimée dans son avis du 17 décembre 2015 (délibération n°718/2015) de désigner clairement dans les articles 59 et 66 qui est le responsable du traitement. Concernant le registre des titres professionnels (article 59), la CNPD rappelle sa proposition de désigner comme responsable du traitement le ministre ayant l'Enseignement supérieur dans ses attributions, en précisant que les données sont fournies par les autorités compétentes des différentes professions réglementées. Pour ce qui est du registre des titres de formation (article 66), la CNPD avait suggéré de désigner, soit le ministre ayant l'Education nationale dans ses attributions ou le ministre ayant l'Enseignement supérieur dans ses attributions comme responsable pour tout traitement effectué sur le registre, soit les deux ministres comme responsables conjoints, chacun pour le traitement de données relevant de son ressort.

Pour le surplus la CNPD n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 20 juillet 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de loi portant modification 1) de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration, 2) de la loi modifiée du 28 mai 2009 concernant le Centre de rétention et 3) de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales

Délibération n°683/2016 du 28 juillet 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 du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser « *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 27 avril 2016, Monsieur le Ministre de l'Immigration et de l'Asile a invité la Commission nationale à se prononcer au sujet du projet de loi portant modification 1) de la loi modifiée du 29 août 2008 sur la libre circulation des

[104] Cf. doc. parl. n°6893/07 du 7 juin 2016.
[105] Cf. délibération n°718/2015 du 17 décembre 2015, doc. parl. n°6893/03 du 17 avril 2016.

personnes et l'immigration, 2) de la loi modifiée du 28 mai 2009 concernant le Centre de rétention et 3) de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales (ci-après le « projet de loi »).

Suivant l'exposé des motifs, le projet de de loi vise à transposer en droit national la directive 2014/36/UE du Parlement européen et du Conseil du 26 février 2014 établissant les conditions d'entrée et de séjour des ressortissants de pays tiers aux fins d'un emploi en tant que travailleurs saisonniers et la directive 2014/66/UE du Parlement européen et du Conseil du 15 mai 2014 établissant les conditions d'entrée et de séjour des ressortissants de pays tiers dans le cadre d'un transfert temporaire intragroupe.

En outre, le projet de loi entend créer dans la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration (ci-après « la loi du 29 août 2008 ») deux autres nouvelles catégories de titres de séjour pour des ressortissants de pays tiers, à savoir pour l'investisseur et pour le travailleur salarié qui assure la continuité d'activité de son employeur au Grand-Duché de Luxembourg.

Le projet de loi prévoit également d'ajouter à l'article 32, paragraphe (2) de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales (ci-après la « loi du 2 septembre 2011 »), un point (i) qui permettra au ministre ayant les autorisations d'établissement dans ses attribution d'avoir un accès direct au fichier des étrangers tenu pour le compte du service des étrangers du ministre ayant l'immigration dans ses attributions, afin de simplifier la procédure d'obtention d'une autorisation d'établissement.

A) Modification de la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration

1) Quant à la situation actuelle

A l'heure actuelle, les traitements de données à caractère personnel mis en œuvre dans le cadre de la loi du 29 août 2008 tombent notamment dans une des deux hypothèses suivantes :

i. La gestion des autorisations et titres de séjour, qui implique le traitement des données à caractère personnel, qui sont conservées dans une base de données, connu sous la dénomination « fichier des étrangers », tenu par le ministre ayant l'immigration dans ses attributions.

ii. Les contrôles pour vérifier si les conditions fixées pour l'entrée et le séjour des étrangers sont

remplies. A ce titre, l'article 138 de la loi du 29 août 2008 prévoit un accès direct du ministre à six différents fichiers tenu par d'autres administrations et services, comme par exemple un accès au « *fichier des autorisations d'établissement exploité pour le compte du ministre ayant les Classes moyennes dans ses attributions* ».

Ensuite, le règlement grand-ducal du 26 septembre 2008 portant création des traitements de données à caractère personnel pris en exécution de la loi du 29 août 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par l'article 138 de cette loi (ci-après le « règlement grand-ducal du 26 septembre 2008 ») règle les modalités d'accès par le ministre aux données traitées par les autres administrations, y compris quelles données peuvent être accédées, ainsi que certaines conditions relatives au traitement des données qui sont directement recueillies auprès du demandeur d'un titre de séjour.

2) Quant à la collecte des données à caractère personnel prévue par le projet de loi

Le projet de loi prévoit la création de quatre nouvelles catégories de titres de séjour, à savoir 1) le titre de séjour en tant que « travailleur salarié » dans le cadre de la continuité d'activité d'une entité agréée (article 44bis nouveau), 2) le « titre de séjour pour une personne faisant l'objet d'un transfert temporaire intragroupe » ou encore dénommé titre de séjour « TIC », (articles 47 - 47-6 nouveaux), 3) le titre de séjour « travailleur saisonnier » (articles 49bis – 49quinquies nouveaux) et 4) le titre de séjour en qualité d'« investisseur » (articles 53bis – 53quater nouveaux).

Ces modifications envisagées par le projet de loi entraîneront une augmentation des données à caractère personnel traitées par le ministre dans sa base de données appelée le « fichier des étrangers », sans qu'il soit spécifié exactement quelles données seraient collectées et traitées. A titre d'exemple, il semble que le demandeur devra soumettre plusieurs documents relatifs à son projet financier pour obtenir un titre de séjour en qualité d' « investisseur »,, y compris les données qui sont nécessaires afin de satisfaire aux exigences de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (article 53bis, paragraphe (6) projeté).

Ainsi, malgré l'énumération des données pouvant être accédées par le ministre auprès d'autres instances dans le règlement grand-ducal du 26 septembre 2008, ni le projet de loi, ni un projet de règlement grand-ducal ne prévoient des dispositions relatives aux données qui seront collectées directement auprès des demandeurs d'un titre de séjour.

Or, conformément à l'article 4, paragraphe (1) de la loi du 2 août 2002, l'utilisation des données traitées doit se limiter aux finalités pour lesquelles elles ont été collectées et les données doivent être adéquates, pertinents et non excessives au regard des finalités pour lesquelles elles ont été collectées. Afin que la Commission nationale puisse s'assurer du caractère adéquat, pertinent et non excessif de ces données, elles devraient être spécifiées dans un texte légal ou règlementaire.

Dès lors, en considération de ce qui précède, du nombre croissant de catégories de données à caractère personnel qui sont collectées et traitées dans la base de données appelée le « fichier des étrangers » et en considération du caractère sensible de certaines de ces données, la Commission nationale réitère sa recommandation déjà formulée dans son avis du 18 juillet 2008 (délibération n°202/2008)[106] de prévoir dans le règlement grand-ducal du 26 septembre 2008 une disposition listant les données qui seront directement recueillies auprès des demandeurs d'un titre de séjour par le ministre ayant

[106] Avis relatif au règlement grand-ducal du 26 septembre 2008 portant création des traitements de données à caractère personnel nécessaires à l'exécution de la loi du 29 aout 2008 sur la libre circulation des personnes et l'immigration et déterminant les données à caractère personnel auxquelles le ministre ayant l'immigration dans ses attributions peut accéder aux fins d'effectuer les contrôles prévus par la loi (http://www.cnpd.public.lu/fr/decisions-avis/2008/libre-circ-pers/202_2008.pdf).

l'immigration dans ses attributions et ce pour toutes les catégories d'autorisation de séjour.

3) Quant à la création du nouveau « registre des entités agrées »

En ce qui concerne le titre de séjour du « travailleur salarié » dans le cadre de la continuité d'activité d'une entité agréée (article 44bis nouveau), le projet de loi envisage de créer un registre des entités agréées, qui serait tenu par le ministre ayant les affaires étrangères dans ses attributions. Afin d'être inscrite au registre, l'entité doit faire une demande qui inclut, entre autres, une preuve de l'honorabilité de l'entité sur base des antécédents judiciaires. En cas de survenance d'un incident majeur empêchant l'exercice normal des activités de l'entité, l'entité agréée pourra demander un titre de séjour pour les salariés venant travailler au Luxembourg, ceci afin d'assurer la continuité de ses activités.

En considération du fait que l'article 44bis, paragraphe (1) nouveau prévoit que le registre des entités agréées serait tenu par le ministre ayant les affaires étrangères dans ses attributions et non par le ministre ayant l'immigration dans ses attributions, et que l'article 44bis, paragraphe (9) nouveau prévoit qu'une transmission de la demande aura lieu entre les deux ministres, la Commission nationale en conclut que le registre des entités agréées sera un registre distinct du « fichier des étrangers ».

Or, ni les conditions d'accès aux données ou de transmission des données, ni l'utilisation et l'obtention de ces données dans ce registre ne sont précisées dans le projet de loi.

Dans son avis du 7 juin 2016 sur le projet de loi n°6975 portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'État pour études supérieures (doc. parl. n°6975/5), le Conseil d'Etat s'est prononcé sur cette question en rappelant « … *que l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, est une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.*

La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication. En cas d'accès direct et, le cas échéant, d'interconnexion, la loi doit encore préciser que le système informatique par lequel l'accès est opéré doit être aménagé de sorte que l'accès est sécurisé

moyennant une authentification forte (…) »[107].

Afin de satisfaire aux exigences posées par la Constitution, la CNPD estime nécessaire d'adapter le projet de loi et d'établir les modalités de l'obtention de l'utilisation des données, ainsi que les conditions d'accès aux données et de transmission des données.

4) Quant à la transmission de données entre le ministre et les autres instances

Le projet de loi fait état de plusieurs transmissions de données, dont notamment la transmission des données aux autorités nationales d'autres Etats-membres conformément aux deux directives citées ci-avant, la transmission du dossier entre le ministre ayant l'immigration dans ses attributions et le ministre ayant les affaires étrangères dans ses attributions dans le cadre du titre de séjour du « travailleur salarié » en cas de continuité d'activité d'une entité agréée ou encore la transmission entre le ministre ayant l'immigration dans ses attributions et, selon le cas, le ministre ayant les finances dans ses attributions ou le ministre ayant l'économie dans ses attributions, pour les demandes d'autorisation de séjour « investisseur ». Dans aucun de ces cas, il est précisé les modalités de la transmission entres ces entités.

De plus, l'article 51, paragraphe (3) du projet de loi établit une exemption pour la procédure de vérification des demandes de titre de séjour pour le travailleur indépendant, si les activités visées ont déjà reçu un agrément par la Commission de surveillance du secteur financier. Ceci étant, le projet de loi reste muet sur la transmission de cet agrément au ministre.

Une telle précision fait également défaut dans le cadre de la coopération envisagée entre les ministres et la commission consultative prévue à l'article 149 nouveau.

Dès lors et en se référant à ses observations formulées au point 3) du présent avis, la Commission nationale estime nécessaire d'adapter en ce sens le texte du projet de loi sous examen afin d'y prévoir les modalités et conditions précises des transmissions des données entre le ministre ayant l'immigration dans ses attributions et les autres instances.

5) Quant à la durée de conservation des données

Après examen, la Commission nationale note que la durée de conservation des données recueillies n'est pas indiquée dans le projet de loi, ni d'ailleurs dans un projet de règlement grand-ducal.

Or, selon l'article 4, paragraphe (1), lettre (d) de la loi du 2 août 2002, les données peuvent seulement être « *conservée sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées…* ». Afin de satisfaire à cette exigence légale, la Commission nationale propose dès lors de modifier le règlement du 26 septembre 2008 afin d'y prévoir une disposition qui règlera la question de la durée de conservation de toutes les données à caractère personnel recueillies et traitées par le ministre.

B) Modification de l'article 32 de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales.

Le projet de loi entend modifier l'article 32 de la loi du 2 septembre 2011. Cet article précise une liste de huit fichiers tenus par d'autres administrations et services auxquels le ministre ayant les autorisations d'établissement dans ses attributions peut accéder afin d'apprécier si une entreprise sollicitant une autorisation d'établissement satisfait aux exigences prévues par la loi prédite et ses règlements d'exécution.

[107] Voir aussi l'avis du Conseil d'Etat du 9 décembre 2014 à l'égard du projet de loi 6588 portant organisation du secteur des services de taxis et modification du code de la consommation (doc. parl. n°6588/8).

L'article 2 du règlement grand-ducal du 28 avril 2015 portant création des traitements de données à caractère pris en exécution de l'article 32 de la loi du 2 septembre 2011 énumère les données pouvant être accédées en vertu de l'article 32, paragraphe 2 de loi du 2 septembre 2011.

Dans ce contexte, le projet de loi sous examen entend rajouter à la liste existante de l'article 32, paragraphe 2 de la loi du 2 septembre 2011 un nouveau fichier (point (i)), à savoir le « fichier des étrangers tenu pour le compte du service des étrangers du ministre ayant l'immigration dans ses attributions ». Cet accès serait conditionné à l'accord préalable du demandeur.

La Commission nationale note cependant que le prédit règlement grand-ducal du 28 avril 2015, dans sa version actuelle, n'énumère pas les données figurant dans le « fichier des étrangers » auxquelles le ministre ayant dans ses attributions les autorisations d'établissement pourrait accéder.

En l'absence d'une telle précision, le ministre ayant les autorisations d'établissement dans ses attributions aurait vocation à accéder à toutes les données figurant dans le « fichier des étrangers ».

Dès lors, afin de pouvoir analyser la proportionnalité de l'accès aux données du « fichier des étrangers », le CNPD estime nécessaire que le règlement grand-ducal du 28 avril 2015 soit modifié et adapté en ce sens, c.à.d. que le texte devrait énumérer les données auxquelles le ministre ayant les autorisations d'établissement dans ses attributions pourra accéder.

Par ailleurs, en vue d'augmenter le niveau de protection des données traitées par le ministre, la Commission nationale profite de l'occasion pour réitérer ses recommandations faites dans son avis du 6 février 2015[108] (délibération n°45/2015), à savoir qu'un règlement grand-ducal devrait fixer la durée de conservation des données et, en plus, préciser la condition que les données ne pourront être consultées que dans le cadre de l'ouverture ou du suivi d'un dossier administratif.

Pour le surplus, la Commission nationale n'a pas d'autres observations à soulever.

Ainsi décidé à Esch-sur-Alzette en date du 28 juillet 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

[108] Avis relatif au projet de règlement grand-ducal 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'industriel ainsi qu'à certaines professions libérales (http://www.cnpd.public.lu/fr/decisions-avis/2015/acces-artisan-etc/45_2015_Deliberation_Ministere-de-l_Economie_avis-acces-professions-d_artisan_-de-commercant.pdf).

Avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°6921 portant : 1) modification du Code d'instruction criminelle ; 2) modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; 3) adaptation de la procédure pénale face aux besoins liés à la menace terroriste

Délibération n°803/2016 du 14 septembre 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 « la loi du 2 août 2002 »),la Commission nationale pour la protection des données a notamment pour mission d'aviser « *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 5 août 2016, Monsieur le Ministre de la Justice a fait parvenir à la CNPD les amendements adoptés par la Commission juridique[109] concernant le projet de loi n°6921 portant 1) modification du Code d'instruction criminelle ; 2) modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; 3) adaptation de la procédure pénale face aux besoins liés à la menace terroriste.

La Commission nationale se limite à formuler seulement quelques observations mineures relatives aux amendements, alors qu'elle a déjà été consultée par le ministère de la Justice à un stade préliminaire au dépôt des amendements en question.

La CNPD note avec satisfaction que les auteurs du projet de loi ont renoncé à réinsérer un article 41 dans la loi du 2 août 2002 (article abrogé par la loi du 28 juillet 2011[110]), mais qu'ils envisagent dorénavant d'ajouter un article 10bis à la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques à sa place.

Néanmoins, la CNPD réitère ses commentaires exprimés dans son avis du 12 février 2016 (délibération n°147/2016) concernant l'inclusion des services de secours parmi les organismes pouvant accéder aux données contenues dans le fichier centralisé auprès de l'Institut, en vertu de l'article 10bis paragraphe (4) du projet de loi, alors que les services de secours devraient actuellement être en mesure d'accéder aux données d'identification et de localisation en vertu de l'article 7 paragraphe (5) de la loi modifiée du 30 mai 2005.

D'un point de vue rédactionnel, la Commission nationale suppose qu'à l'article 10bis paragraphe (4), les auteurs ont voulu faire référence à l'article 48-27 (1) du Code d'instruction criminelle, et non pas à l'article 48-27(7) du Code d'instruction criminelle.

La Commission nationale propose par ailleurs d'aligner la terminologie de l'amendement 5 rajoutant le nouveau paragraphe (3) à l'article 73 de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques sur celle de l'article 10bis paragraphe (2) projeté, en rajoutant le mot « luxembourgeoises » derrière les mots « ressources de numérotation ». Cette précision assurerait également une harmonisation entre la terminologie du projet de loi n°6921 et celle du projet de loi n°7052 portant modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques[111], notamment en ce qui concerne

[109] Cf. doc. parl. n°6921/03 du 8 août 2016.
[110] Loi du 28 juillet 2011 portant modification 1) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; 2) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personne l ; 3) de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat ; 4) du Code de la consommation.
[111] Cf. doc. parl.n°7052/00 du 2 septembre 2016.

la définition de « service à prépaiement » au point 8bis de l'article 2.

Pour le surplus la CNPD n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 14 septembre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7052 portant modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques

Délibération n°804/2016 du 14 septembre 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 « la loi du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser *« 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 23 août 2016, Monsieur le Ministre des Communications et des Médias a invité la Commission nationale à se prononcer au sujet du projet de loi n°7052 portant modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques.

Selon l'exposé des motifs, le projet de loi sous examen a pour objet de modifier la loi du 27 février 2011 sur les réseaux et les services de communications électroniques, afin de créer une

base légale d'après laquelle les entreprises fournissant des services de communications électroniques accessibles au public sous la forme d'un service à prépaiement devraient saisir certaines données à caractère personnel relatives à l'identification de leurs clients avant l'activation du service. Une telle récolte de données serait devenue nécessaire, afin de minimiser le risque d'utilisation des cartes à prépaiement à des fins criminelles et pour faciliter la lutte contre la criminalité, y compris la lutte contre le terrorisme.

La Commission nationale se limite à formuler seulement quelques observations mineures relatives au projet de loi, alors qu'elle a déjà été consultée par le ministère des Communications et des Médias à un stade préliminaire au dépôt du projet de loi en question.

Aux termes de l'article 74*bis* paragraphe (1) lettre (a) point 2 du projet de loi, les données que l'entreprise fournissant des services à prépaiement doit collecter sont : *« le type, le pays de délivrance et le numéro de la pièce d'identité ou de l'attestation de dépôt d'une demande de protection internationale de la personne, ainsi qu'une copie de cette pièce »*. D'après le commentaire des articles, cette collecte peut se faire soit sur place dans un magasin, soit via un enregistrement en ligne. Pour le cas où le client procéderait à un enregistrement en ligne, un scan de la pièce pourrait être utilisé.

Tenant compte de ces explications, la Commission nationale estime qu'il n'est pas clair si l'article 74*bis* paragraphe (1) lettre (a) point 2 du projet de loi obligerait les entreprises à conserver uniquement une copie de la demande de protection internationale ou également une copie de la pièce d'identité. Dans un souci de clarté du texte, la Commission nationale suggère dès lors de clarifier si l'obligation de conservation concerne uniquement la demande de protection internationale ou également la pièce d'identité.

Pour le surplus la CNPD n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 14 septembre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7064 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse et portant modification de la loi du 18 mars 2013 relative aux traitements des données à caractère personnel concernant les élèves

Délibération n°829/2016 du 14 octobre 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 du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser *« 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 10 août 2016, le Ministère de l'Education nationale, de l'Enfance et de la Jeunesse a invité la Commission nationale à aviser le projet de loi n°7064 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse et portant modification de la loi du 18 mars 2013 relative aux traitements des données à caractère personnel concernant les élèves.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par les articles 8 et 16 du projet de loi sous objet.

Ces articles ont notamment pour objet de permettre l'accès au Ministre ayant l'Enfance et la Jeunesse dans ses attributions à certaines données rendues nécessaires à l'administration des aides accordées par l'Etat suite à l'introduction de l'éducation plurilingue dans les structures d'accueil agréées.

Ad article 8

La Commission nationale souhaite tout d'abord se référer à son avis 338/2014 du 21 juillet 2014 relatif au projet de loi no 6410 portant modification de la loi du 4 juillet 2008 sur la jeunesse (document parlementaire n°6410/12). Alors que certaines de ses recommandations ont été intégrées dans la loi du 24 avril 2016, et par conséquent dans l'actuel article 29 de la loi modifiée du 4 juillet 2008 (appelé à être de nouveau modifié par l'article 8 du projet de loi sous examen), d'autres sont restées sans suite.

La CNPD se permet de rappeler certains commentaires déjà évoqués dans cet avis, qui demeurent pertinents au regard de la version coordonnée de l'article 29 de la loi. Ainsi, il serait utile d'expliquer la nécessité pour le ministère de connaître la présence réelle de l'enfant bénéficiaire dans la structure (paragraphe (2) lettre (e)), ainsi que la nécessité d'une publication des données visées au paragraphe (2) lettres (h) à (j) (anciennement lettres (f) à (h)) sur un portail édité par le Ministre. Par ailleurs, la Commission nationale ne comprend pas la raison d'être de la transmission des données dans le cadre du paragraphe (5), alinéa 3 (ancien paragraphe (4) alinéa 3) sans en préciser la finalité, alors que de manière générale, les données ne peuvent pas être communiquées à des tiers ou accédées par des tiers. Enfin, la durée de conservation des données indiquée dans le paragraphe (6) (ancien paragraphe (5)) demeure relativement longue par rapport aux finalités des traitements des données concernées.

En ce qui concerne l'ajout des lettres (f) et (g) dans le paragraphe (2), la Commission nationale comprend, au regard du commentaire des articles, que ces données apparaissent nécessaires aux fins d'assurer la gestion, le suivi administratif, le contrôle et l'étude voire l'évaluation des aides liées au programme d'éducation plurilingue. Dans ce cadre, la proposition d'ajout à deux reprises des termes *« et du programme d'éducation plurilingue »* au paragraphe (1) paraît également appropriée.

A la lecture du dernier alinéa du paragraphe (2), la CNPD ne comprend pas si les données visées aux lettres (a) à (j) sont collectées auprès des personnes concernées (ou de leurs représentants légaux), et que parmi celles-ci, celles indiquées aux lettres (f) et (g) peuvent être communiquées par la suite aux autorités communales? Ou si seules les données relevant des lettres (a), (b), (c), (d), (e), (h), (i) et (j) sont collectées auprès des personnes concernées (ou de leurs représentants légaux), tandis que les données visées aux lettres (f) et (g) proviennent des fichiers des différentes autorités communales ? En tout état de cause, le terme « échange » devrait être précisé : s'agit-il d'une communication des données, d'un accès sur demande, d'une interconnexion, etc. ?

Le paragraphe (3) s'inscrit, selon le commentaire des articles, dans le cadre de mesures de simplification administrative. Sans remettre en cause le bien fondé de telles mesures, la Commission nationale se doit de mettre en balance cet objectif avec le droit pour les personnes concernées à la protection de leur vie privée. Ce dernier élément constitue un droit fondamental consacré notamment par l'article 11 (3) de la Constitution, par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ainsi que par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Il s'agit donc de vérifier si cette balance des intérêts penche en faveur du droit fondamental au respect de la vie privée, qui protège l'intérêt des citoyens, ou en faveur de l'intérêt légitime de l'administration à la simplification de ses procédures, en tenant compte du critère de proportionnalité et de nécessité.

En l'espèce, les auteurs du projet de loi ont souhaité maintenir la faculté pour les personnes concernées de délivrer elles-mêmes un certificat de paiement des allocations familiales auprès de l'agent communal chargé de l'instruction de la demande d'adhésion au chèque-service accueil. L'accès par l'agent communal aux données est en effet uniquement permis sur base du consentement spécifique de la personne concernée (paragraphe (3), alinéa 2). Dans ce cadre, la Commission nationale estime que les droits fondamentaux de la personne concernée ne prévalent pas sur l'intérêt de l'administration à la simplification administrative, qui s'opère dans l'intérêt du citoyen et avec son accord préalable.

Cependant, il ne ressort pas du paragraphe (3) de quelles administrations ou institutions de sécurité sociale l'agent communal pourra recevoir communication des données, ni à quelles catégories exactes de données il peut avoir accès. La Commission nationale souhaite attirer l'attention des auteurs du projet de loi sur l'arrêt de la Cour constitutionnelle du 29 novembre 2013, selon lequel *« l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc »*[112]. La CNPD se réfère également à un récent avis du Conseil d'Etat selon lequel *« pour autant qu'il s'agisse de renvoyer à un règlement grand-ducal le soin de spécifier les conditions légales, la loi doit fixer, en application des dispositions de l'article 32(3) de la Constitution, la finalité, les conditions et les modalités du règlement grand-ducal en question »*[113].

Dans ce cadre, il est indispensable de prévoir dans le texte de loi de quelles administrations ou institutions de sécurité sociale l'agent communal pourra recevoir communication des données. En ce qui concerne les catégories de données visées, il pourrait être fait référence à l'article 2 du futur règlement grand-ducal précisant les données accessibles et les données communiquées en exécution des articles 4 et 6 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves.

Enfin, c'est à bon escient que les auteurs du projet de loi ont

[112] Cour constitutionnelle, arrêt 108/13 du 29 novembre 2013 (Mém. A n°217 du 13 décembre 2013, p. 3886).
[113] Avis du Conseil d'Etat du 15 juillet 2016, document parlementaire 6708/05.

prévu à l'alinéa 4 des mesures de sécurisation de l'accès aux données, ainsi qu'une procédure de traçage des accès, ce qui permet d'éviter tout risque d'abus ou de détournement de finalité. Ces mesures participent au souci de confidentialité et répondent à l'obligation pour le responsable du traitement de garantir la sécurité des données au sens des articles 21 à 23 de la loi du 2 août 2002.

Ad article 16

L'article 16 a pour objet de compléter l'article 6 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves. La Commission nationale a déjà eu l'occasion d'émettre ses commentaires relatifs ou liés à cette loi (cf. avis 238/2010 du 26 juillet 2010, 126/2011 du 15 avril 2011 et 156/2012 du 15 juin 2012, et plus récemment son avis 613/2016 du 6 juillet 2016).

L'article 6 de la loi du 18 mars 2013 indique les autorités ou entités auxquelles le Ministre ayant l'éducation nationale dans ses attributions est autorisé à communiquer des données à caractère personnel relative aux élèves. L'article 16 du projet de loi sous examen y ajoute un point 14. Le commentaire des articles révèle que cet ajout apparaît nécessaire pour faire fonctionner le système d'aides mise en place par la loi modifiée du 4 juillet 2008 sur la jeunesse, et est à lire avec l'article 8 du projet de loi sous examen.

Dans ce cadre, la Commission nationale peut admettre qu'une telle communication de données à caractère personnel puisse s'avérer nécessaire au regard de l'article 29 paragraphe (2) lettres (f) et (g) de la loi modifiée du 4 juillet 2008, telle que modifiée par le présent projet de loi.

Par ailleurs, comme elle l'avait déjà évoqué dans son avis 238/2010 du 26 juillet 2010, la Commission nationale estime nécessaire que les catégories de données qui feront l'objet d'une communication (dans ce cas au Ministre ayant l'enfance et la jeunesse dans ses attributions) soient énumérées au sein d'un règlement grand-ducal, en vue de pouvoir apprécier la compatibilité des finalités de la base de données relative aux élèves avec celles du traitement opéré par le Ministre. En l'espèce, la CNPD comprend que les catégories de données concernées sont celles visées aux lettres (f) et (g) de la loi modifiée du 4 juillet 2008 sur la jeunesse (telle que modifiée par le projet de loi sous examen).

Dans ce contexte, il est utile de relever que l'avant-projet de règlement grand-ducal précisant les données accessibles et les données communiquées en exécution des articles 4 et 6 de la loi du 18 mars 2013 relative aux traitements de données à

caractère personnel concernant les élèves, entend déjà préciser les catégories de données visées aux points (1) à (13) de l'article 6 de la loi du 18 mars 2013. La Commission nationale a émis dans son avis 613/2016 du 6 juillet 2016 ses remarques à ce sujet. Il serait utile d'intégrer à l'occasion de l'adoption de cet avant-projet de règlement grand-ducal les catégories de données visées aux lettres (f) et (g) du futur article 29 paragraphe (2) de la loi modifiée du 4 juillet 2008, au regard du point (14) de l'article 6 de la loi du 18 mars 2013.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 14 octobre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Avis de la Commission nationale pour la protection des données à l'égard du projet de loi n°6977 sur la nationalité luxembourgeoise et portant abrogation de : 1. la loi du 23 octobre 2008 sur la nationalité luxembourgeoise ; 2. la loi du 7 juin 1989 relative à la transposition des noms et prénoms des personnes qui acquièrent ou recouvrent la nationalité luxembourgeoise

Délibération n°837/2016 du 14 octobre 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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après : « la CNPD ») a notamment pour mission d'aviser *« 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 »*.

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Justice en date du 22 mars 2016, la CNPD entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n°6977 sur la nationalité luxembourgeoise et portant abrogation de la loi du 23 octobre 2008 sur la nationalité luxembourgeoise et de la loi du 7 juin 1989 relative à la transposition des noms et prénoms des personnes qui acquièrent ou recouvrent la nationalité luxembourgeoise.

La CNPD limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement dans le chapitre 12, aux articles 96 à 106 du projet de loi sous examen.

Remarque préliminaire

De manière générale, la Commission nationale salue que la plupart des principes essentiels issus de la loi modifiée du 2 août 2002 aient été intégrés dans les articles sous rubrique. Certains articles suscitent cependant quelques remarques, développées ci-après.

Afin de s'aligner sur la terminologie utilisée dans la loi modifiée du 2 août 2002, la CNPD suggère de remplacer dans tous les articles concernés (ainsi que dans le titre du chapitre) les termes *« banque de données »* par « fichier » ou *« traitements de données »*.

Article 96

La CNPD s'interroge sur la portée exacte de la finalité visée à l'article 96 point 3° du projet de loi, à savoir *« la préservation de l'historique des données à des fins administratives »*.

Si l'intention était de conserver des données dans le cadre des finalités évoquées aux paragraphes (1) et (2) du même article, il conviendrait de supprimer ces termes et de prévoir tout simplement une durée de conservation pour ces données[114]. En effet, la conservation des données ne peut pas être considérée comme une finalité en soi.

Si, au contraire, une finalité spécifique est visée, la Commission nationale estime nécessaire de préciser plus en détail cette disposition, de manière à clarifier quelles sont exactement les « *fins administratives* » visées par les auteurs du projet de loi.

En effet, conformément à l'article 4, paragraphe (1), lettre (a) de la loi modifiée du 2 août 2002, les données traitées par un responsable du traitement doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités* ».

Pour autant qu'il ne s'agisse pas de données anonymes[115] (telles que visées par la deuxième hypothèse du point 3 de l'article 96), le libellé de l'article 96 point 3° doit être considéré comme étant trop vague.

Article 97

Les données figurant dans le fichier relatif à la nationalité luxembourgeoise telles qu'énumérées à l'article 97, apparaissent nécessaires et non excessives. Le catalogue des données est clairement circonscrit.

Pour ce qui est du « *numéro d'identification* » visé à l'article 97 paragraphe (1) numéros 2, 11, 12 et 13, la Commission nationale suggère de préciser qu'il s'agit du numéro d'identification des personnes physiques, tel que défini par l'article 1er de la loi du 19 juin 2013 relative à l'identification des personnes physiques.

L'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002 impose au responsable de traitement de veiller à ce que les données qu'il traite ne soient pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées. Or, le projet de loi sous avis ne contient aucune disposition relative à la durée de conservation des données.

La CNPD estime donc nécessaire de préciser le texte du projet de loi en ce sens.

Article 98

Alors qu'il ressort implicitement du texte du projet de loi, ainsi que du commentaire relatif à l'article 98, que le Ministre de la Justice est à considérer comme responsable du traitement, la CNPD propose de le préciser dans le corps du texte et suggère

[114] Voir les commentaires développés sous l'article 97 ci-après.
[115] La loi modifiée du 2 août 2002 n'a pas vocation à s'appliquer aux données anonymes.

le libellé suivant : « *Le ministre*[116] *a la qualité de responsable du traitement au sens de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Il désigne les agents qui sont en charge, sous son autorité, des opérations relatives à la gestion et à la tenue du fichier relatif à la nationalité luxembourgeoise.*»

Article 99

Dans le cadre des mesures de sécurité et de confidentialité visées à l'article 99 point 4°, la CNPD estime nécessaire de prévoir un système de traçage des accès aux données, ce qui constitue une garantie en matière de protection des données à caractère personnel des personnes concernées dans le cadre des articles 22 et 23 de la loi du 2 août 2002. Ainsi, il conviendrait de rajouter une disposition, à l'instar d'autres lois ou règlements grand-ducaux, qui pourrait avoir la teneur suivante : « *Le système informatique par lequel l'accès au fichier est opéré doit être aménagé de sorte que l'accès aux fichiers soit sécurisé moyennant une authentification forte, que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.* »

Article 102

Cet article est inspiré des dispositions de l'article 38 de la loi du 19 juin 2013 relative à l'identification des personnes physiques[117].

Il est vrai qu'un nombre important d'administrations ou services relevant de l'Etat ou des communes ont accès au registre national des personnes physiques. Or, en l'espèce, pour ce qui est du fichier relatif à la nationalité luxembourgeoise, la CNPD est à se demander quelles administrations ou services relevant de l'Etat ou des communes autres que ceux énumérés aux points 1° et 2° de l'article 102 pourraient accéder à ce fichier et pour quelles finalités ? Si aucune autre entité n'a accès audit fichier, quelle serait la raison d'être de cette disposition ?

Article 103

L'article 103 du projet de loi semble contenir une erreur matérielle. En effet, la référence à l'article 101 (1) relatif au droit de rectification semble être erronée. Ne devrait-elle pas plutôt se référer à l'article 100 (1) du projet de loi ?

Article 104

La CNPD fait sienne l'argumentation développée par le Conseil d'Etat dans son avis du 21 juin 2016 en ce qui concerne l'article 104 paragraphe (2) du projet de loi. Le Conseil d'Etat a à juste titre soulevé qu'« *alors que l'article 41 de la loi précitée du 19 juin 2013 dispose que l'interdiction de communiquer des données figurant au registre national ou communal ne vise pas les autorités, administrations, services, institutions ou organismes qui sont habilités à obtenir de telles données par ou en vertu de la loi, l'article 104, paragraphe 2, prévoit l'adoption de règlements grand-ducaux pour déterminer les entités qui peuvent recevoir communication de ces listes. 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.* »[118]

Article 105

Cette disposition autorise le ministre à délivrer des statistiques à des tiers, à condition que les statistiques « *ne permettent pas l'identification des personnes inscrites dans cette banque [de*

[116] Le projet de loi définit la notion de « ministre » dans son article 9.
[117] Loi 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 et portant modification de 1) l'article 104 du Code civil; 2) la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales; 3) la loi communale modifiée du 13 décembre 1988; 4) la loi électorale modifiée du 18 février 2003 et abrogeant 1) la loi modifiée du 22 décembre 1886 concernant les recensements de population à faire en exécution de la loi électorale et 2) l'arrêté grand-ducal du 30 août 1939 portant introduction de la carte d'identité obligatoire, telle que modifiée.
[118] Avis du Conseil d'Etat n°51.599 du 21 juin 2016 ; p. 23.

données] ». La CNPD comprend par là que seules des données anonymisées peuvent être communiquées à des tiers à des fins statistiques. A ce titre, elle s'interroge sur la pertinence des paragraphes (2) à (4) de l'article 105 en projet. Ne suffirait-il pas de préciser tout simplement que la délivrance des statistiques ne peut se faire que moyennant des données préalablement anonymisées, à l'instar de ce qui est prévu à l'article 96 point 3° du projet de loi sous examen ?

Article 106

Selon l'article 106 du projet de loi sous avis, le ministre et les officiers de l'état civil ont le droit d'accéder aux banques de données relatives à l'autorisation de séjour et à la protection internationale.

A ce titre, la Commission nationale se rallie à l'avis du Conseil d'Etat du 21 juin 2016 précité. En effet, il s'avère nécessaire d'identifier avec précision les fichiers de données à caractère personnel relatifs à l'autorisation de séjour et à la protection internationale qui sont visés par cet article. Il faudrait également préciser quelles données sont strictement nécessaires pour accomplir les missions découlant des finalités précisées à l'article 96 sous analyse.

Nonobstant ce qui précède, la CNPD estime nécessaire, d'un point de vue informatique, que soit prévu la mise en place d'une solution technique permettant de garantir que les agents du ministère et les officiers de l'état civil puissent seulement accéder aux données des personnes qui ont introduit une demande d'obtention de la nationalité luxembourgeoise, à l'exclusion des données relatives aux autres personnes se trouvant dans les fichiers relatifs à l'autorisation de séjour et à la protection internationale. En d'autres termes, seule l'ouverture d'un dossier administratif à l'occasion de l'introduction d'une demande d'obtention de la nationalité luxembourgeoise ouvrirait aussi le droit pour ledit ministère et les officiers de l'état civil d'accéder aux fichiers visés à l'article 106 du projet de loi et auxquels ils n'auraient pas accès en l'absence d'un dossier administratif relatif à une demande d'obtention de la nationalité luxembourgeoise.

Par ailleurs, le système de traçage des accès, tel que décrit dans le cadre de l'article 99 du projet de loi, devrait également être implémenté.

Ainsi décidé à Esch-sur-Alzette en date du 14 octobre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Deuxième avis complémentaire de la Commission nationale pour la protection des données à l'égard du projet de loi n°6893 relative à la reconnaissance des qualifications professionnelles

Délibération n°838/2016 du 14 octobre 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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser *« 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 27 septembre 2016, Monsieur le Ministre délégué à l'Enseignement supérieur et à la Recherche a sollicité la CNPD d'aviser les amendements adoptés par la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace en date du 21 septembre 2016[119] concernant le projet de loi n°6893 relative à la reconnaissance des qualifications professionnelles. Ayant avisé le prédit projet de loi n°6893 en date du 17 décembre 2015[120] et du 20 juillet 2016[121], la CNPD se limite à formuler quelques observations relatives aux derniers amendements adoptés.

Elle note avec satisfaction que les auteurs du projet de loi l'ont suivie en ses recommandations formulées dans ses deux avis précités, quant à la désignation non-équivoque des responsables du traitement. En effet, les amendements adoptés introduisent une désignation claire du ou des responsable(s) du traitement aux articles 59 et 66 du projet de loi sous analyse.

A ce titre, la Commission nationale constate que les auteurs ont opté, à l'article 66 relatif au registre des titres de formation, pour une désignation non-équivoque de plusieurs responsables de traitement conjoints. Ainsi, le ministre ayant l'Education nationale dans ses attributions et le ministre ayant la Formation professionnelle dans ses attributions sont désignés responsables du traitement (au sens de l'article 2, lettre (n) de la loi modifiée du 2 août 2002) pour la partie du registre qui relève de la section de l'enseignement secondaire. Le ministre ayant l'Enseignement supérieur dans ses attributions est désigné comme responsable du traitement pour la partie du registre relevant de la section des données relatives à l'enseignement supérieur.

Les autres amendements ne relevant pas de son domaine de compétence, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 14 octobre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

[119] Cf. doc. parl. n°6893/14 du 21 septembre 2016.
[120] Délibération n°718/2015 du 17 décembre 2015.
[121] Délibération n°660/2016 du 20 juillet 2016.

7 Annexes

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°6913 sur l'archivage

Délibération n°839/2016 du 14 octobre 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 » ou « la loi »), 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 en date du 4 décembre 2015, le Ministre de la Culture a invité la Commission nationale à se prononcer sur le projet de loi n°6913 sur l'archivage (ci-après « le projet de loi »). Il est accompagné de quatre projets de règlements grand-ducaux[122].

Le projet de loi a pour objectif de *« régler l'archivage dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits et obligations des producteurs ou détenteurs d'archives que pour assurer, par le biais de la sauvegarde d'un patrimoine archivistique national et dans un esprit de transparence démocratique, l'accès à la documentation d'intérêt historique, scientifique, culturel, économique ou sociétal du Grand-Duché de Luxembourg »* (art. 1er dudit projet).

Il entend renouveler le cadre juridique en vigueur, qui repose actuellement sur une réglementation fragmentée et ancienne[123], afin de mettre en œuvre une politique publique cohérente en matière d'archives et de répondre aux défis actuels. Les technologies de l'information et de la communication jouent, en effet, un rôle essentiel dans la mise en œuvre de la politique archivistique du Luxembourg. Il convient tout particulièrement de prendre en considération la multiplicité des supports sur lesquels les archives peuvent désormais être créées et conservées (papier, numérique, audiovisuel…).

Une bonne gestion de l'information et des archives au niveau national est essentielle à plusieurs égards : elle permet de préserver la mémoire collective du Luxembourg et pose les conditions d'une organisation publique crédible et d'une transparence nécessaire au bon fonctionnement de la démocratie.

---

[122] Les quatre projets de règlements grand-ducaux ayant vocation à accompagner le projet de loi sous examen concerne 1) le fonctionnement interne du Conseil des archives ; 2) la communication, la reproduction et la publication des archives ; 3) l'exercice du droit de surveillance des archives publiques par les Archives nationales ; 4) les modalités d'établissement des tableaux de tri, de destruction d'archives, de versement et de transfert d'archives aux Archives nationales. Le projet de règlement grand-ducal relatif à la communication, à la reproduction et à la publication des archives a vocation à abroger et à remplacer le règlement grand-ducal du 15 janvier 2001 sur la consultation des fonds d'archives aux Archives nationales.

[123] Le cadre juridique actuel se compose de l'arrêté royal grand-ducal du 8 février 1878 portant règlement sur l'organisation et le service des bureaux du Gouvernement, la loi du 9 décembre 1976 relative à l'organisation du notariat, la loi du 20 mars 1990 relative aux doubles des registres de l'état civil, la loi électorale modifiée du 18 février 2003 s'agissant des élections communales, le règlement grand-ducal du 15 janvier 2001 sur la consultation des fonds d'archives aux Archives nationales et la loi du 25 juin 2004 portant réorganisation des instituts culturels.

De manière générale, la Commission nationale ne peut que saluer la présente démarche visant à doter l'Etat luxembourgeois d'une politique publique en matière d'archives et du cadre juridique nécessaire à sa mise en œuvre. La légitimité de constituer et d'exploiter, dans l'intérêt public, des documents d'archives contenant des données à caractère personnel ne fait aucun doute.

Elle relève à cet égard que la Déclaration universelle sur les archives adoptée par l'Organisation des Nations Unies pour l'éducation, la science et la culture (« UNESCO ») reconnaît *« le caractère unique des archives, à la fois témoignage authentique des activités administratives, culturelles et intellectuelles et reflet de l'évolution des sociétés ».*

Comme le souligne l'exposé des motifs du projet de loi, *« les archives forment un élément intrinsèque de notre identité et constituent un trésor irremplaçable ; elles contribuent à documenter l'activité des institutions publiques, à assurer la continuité et le contrôle de leur gestion, ainsi que la sécurité du droit. Elles permettent de sauvegarder les intérêts légitimes de personnes touchées ou de tiers, ainsi que ceux de la science et de la recherche ».*

Si l'apport des projets de textes dépasse le strict champ de la protection des données à caractère personnel, le régime juridique qui en découle s'agissant, notamment, du versement de documents d'intérêt public aux Archives Nationales, de leur tri, de leur conservation, de leur destruction et de leur communication au grand public ou aux chercheurs appellent des observations au regard de la loi modifiée du 2 août 2002.

Pour sa part, la Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de loi et des projets de règlements grand-ducaux sous examen traitant des aspects liés au respect de la vie privée à la protection des données à caractère personnel.

III. L'applicabilité de la loi modifiée du 2 août 2002 aux archives

Bien que de nombreux documents d'archives ne comportent aucune donnée à caractère personnel, la Commission nationale considère que de tels documents peuvent tomber sous l'application de la loi modifiée du 2 août 2002, dès lors qu'ils se rapportent à des personnes physiques potentiellement encore vivantes ou à des personnes décédées dont la publication de données à caractère personnel a des conséquences sur la vie privée de leurs ayants droit.

En effet, la Commission nationale estime que la divulgation de documents d'archives anciens pourrait avoir des conséquences néfastes sur la personne directement concernée, mais également sur ses descendants ou plus largement sur les membres de sa famille. A titre d'illustration, la divulgation du contenu d'un casier judiciaire d'une personne, la révélation d'informations concernant le passé intime d'une personne (maladie mentale, maladie héréditaire…) pourraient avoir des conséquences négatives pour la famille d'une personne, notamment pour son conjoint survivant, ses enfants ou d'autres descendants.

Comme le souligne l'exposé des motifs du projet de loi, la mémoire individuelle et collective que le projet de loi entend sauvegarder *« se base en grande partie sur des données nominatives et sur l'accès à ces données ».*

L'applicabilité de la loi de 2002 ne soulève pas de difficulté particulière dans des situations où le contenu concret des documents en cause leur confère un caractère privé par nature. Tel peut être le cas, en particulier, des archives notariales, des fonds issus des cours et tribunaux, ou encore des fonds de personnes et de familles ayant confié certains de leurs documents aux Archives nationales.

Dans certaines circonstances, il peut s'avérer difficile de déterminer *in abstracto* si des données contenues dans des documents d'archives entrent dans le champ d'application de l'article 2 lettre (e) de la loi définissant la notion de « données à caractère personnel ». En effet, la nature des documents en cause ne révèle pas toujours de manière évidente le caractère personnel ou non des données qui y figurent, ce d'autant que la définition des archives posée l'article 2 (1) du projet de loi est particulièrement large[124]. Un examen détaillé du contenu des documents en cause s'avère alors nécessaire pour déterminer la nature des données au regard de l'article 2 lettre (e) de la loi modifiée du 2 août 2002.

La Commission nationale relève dans le projet de loi plusieurs références expresses à la loi modifiée du 2 août de 2002[125]. Ces références attestent d'une volonté du législateur de prendre pleinement en considération, à juste titre, le cadre juridique applicable à la protection des données, dans l'hypothèse où les documents en cause comporteraient des données à caractère personnel.

L'exposé des motifs précise en outre que « *la présente loi doit être compatible avec les lois existantes dans des domaines connexes dont notamment la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, dont l'objectif principal est de protéger le citoyen contre un fichage systématique et de veiller à ce que chaque citoyen puisse faire valoir, s'il le souhaite, le droit à l'oubli* ».

Ainsi, les objectifs poursuivis par le projet de loi soumis à examen et ceux de la loi modifiée du 2 août 2002 doivent être articulés, afin de parvenir à un juste équilibre entre le droit au respect de la vie privée, d'une part, et la gestion et l'exploitation des archives dans l'intérêt du public, d'autre part. Pour ce faire, la Commission nationale estime nécessaire d'instaurer des mécanismes permettant d'apprécier les intérêts en jeu et de garantir l'accès de certains documents d'archives contenant des données à caractère personnel, tout en limitant la divulgation d'informations pouvant porter atteinte à la vie privée des personnes.

S'il peut être difficile d'anticiper, dès aujourd'hui, quelles archives auront une utilité pour l'avenir, la Commission nationale considère que la recherche d'un juste équilibre est essentielle dans un domaine où le droit à la mémoire et le droit à l'oubli entrent souvent en conflit.

IV. La responsabilité des traitements

La Commission nationale relève que les Archives nationales jouent

[124] L'article 2 (1) du projet de loi définit les archives comme « *les documents - quels que soient leur date, leur stade d'élaboration, leur forme matérielle et leur support - produits ou reçus par une personne physique ou morale de droit public ou privé dans l'exercice de son activité, ainsi que les instruments de recherche et les données complémentaires qui sont nécessaires à la compréhension et à l'utilisation de ces documents. Constituent également des archives, les documents entrés dans la propriété de l'Etat du Grand-Duché de Luxembourg et de ses prédécesseurs en droit par voie de cession à titre gratuit ou onéreux, incorporation, sécularisation, nationalisation, confiscation, dévolution, don ou legs* ».

[125] Un renvoi exprès aux dispositions de la loi modifiée du 2 août 2002 s'observe notamment dans le chapitre V intitulé « Sous-traitance », le chapitre VII intitulé « Protection des archives publiques » et le chapitre X intitulé « Renseignements donnés aux personnes concernées et contestation » du projet de loi.

actuellement un rôle essentiel et sont l'institution de référence pour l'orientation de la politique archivistique du Grand-Duché du Luxembourg.

En effet, en application de l'article 7 de la loi du 25 juin 2004 portant réorganisation des instituts culturels, « *les Archives nationales ont pour mission de réunir tous les documents d'intérêt historique national leur soumis. Elles classent, inventorient et conservent les archives publiques en vue de leur utilisation à des fins historiques et administratives* ».

En application de cette obligation légale, les Archives nationales collectent, conservent, évaluent, inventorient, organisent, communiquent et mettent en valeur les archives.

La Commission nationale observe par ailleurs que l'article 3 paragraphe (1) du projet de loi prévoit que « *sauf dispositions contraires dans la présente loi ou dans d'autres textes législatifs et sans préjudice des missions spécifiques attribuées aux autres instituts culturels par la loi modifiée du 25 juin 2004 portant réorganisation des instituts culturels de l'Etat, les producteurs ou détenteurs d'archives publiques doivent proposer aux Archives nationales le versement de leurs archives publiques ne présentant plus d'utilité administrative. […]* ».

A ce titre et en application de l'article 2 lettres (n) de la loi modifiée du 2 août 2002, les Archives nationales doivent en principe être considérées comme responsable des traitements susmentionnés mis en œuvre à des fins archivistiques.

Toutefois, la Commission nationale note que les articles 4 et 5 du projet de loi visent à instaurer des régimes dérogatoires de gestion des archives.

En premier lieu, l'article 4 du projet de loi prévoit que la Chambre des Députés, le Conseil d'Etat et les juridictions luxembourgeoises (art. 4 paragraphe (2)) du projet de loi) et les établissements publics (art. 4 paragraphe (3)) sont responsables de leurs traitements d'archives au sens de l'article 2 lettre (n) de la loi modifiée du 2 août 2002[126]. Ils remplissent ce rôle sous la surveillance des Archives nationales, dans un souci de cohérence de la politique archivistique.

Dans l'hypothèse où la Chambre des Députés, le Conseil d'Etat et les juridictions luxembourgeoises ne seraient pas en mesure de conserver elles-mêmes leurs propres archives, l'article 4 paragraphe (2) du projet de loi autorise ces institutions à solliciter des Archives nationales qu'elles assurent la conservation de leurs archives.

Par ailleurs, certains producteurs ou détenteurs d'archives publiques autres que les organismes susmentionnés peuvent se voir accorder un régime dérogatoire d'archivage autonome, c'est-à-dire par leurs propres soins, de leurs documents d'archives, dans les conditions définies à l'article 5 du projet de loi.

Dans un souci de cohérence de la politique archivistique, l'article 4 paragraphe (2) du projet de loi prévoit en outre que les Archives nationales surveillent la conservation et la gestion de leurs archives par la Chambre des Députés, le Conseil d'Etat et les juridictions luxembourgeoises.

Il ressort de la lecture combinée des articles 3, 4 et 5 du projet de loi que, dans certaines situations, les parties en jeu peuvent être amenées à se répartir certaines des responsabilités dans le cadre de la gestion d'archives publiques. En application de l'article 2 lettres (n) et (o) de la loi modifiée du 2 août 2002, la Commission nationale observe que les Archives nationales sont susceptibles d'intervenir en qualité de sous-traitant d'un traitement d'archives dont la responsabilité restera celle de l'organisme déposant. Elle estime que, dans ce cas de figure, les Archives nationales n'auront pas la responsabilité de l'intégralité des décisions relatives au traitement de données (y compris

[126] Dans un souci de cohérence de la politique archivistique, l'article 4 paragraphe (2) du projet de loi prévoit en outre que les Archives nationales surveillent la conservation et la gestion de leurs archives par la Chambre des Députés, le Conseil d'Etat et les juridictions luxembourgeoises.

la fourniture des accès aux données des personnes).

La Commission nationale rappelle que, quelle que soit la nature des organismes concernés, la qualité de responsables de traitements les assujettit à une obligation de prévoir les garanties suffisantes (juridiques, techniques et organisationnelles) pour assurer la protection des personnes à l'égard du traitement de leurs données à caractère personnel, à charge pour ces organismes de transférer contractuellement une partie de leurs obligations sur leur sous-traitant.

A cet égard, une formalisation dans un contrat de la répartition des rôles et responsabilités des déposants d'archives et des Archives nationales devrait avoir lieu, de manière systématique et préalablement à l'accession aux documents d'archives, conformément à l'article 22 paragraphe (3) de la loi modifiée du 2 août 2002.

V. Les finalités des traitements de données à caractère personnel

Les traitements envisagés à des fins d'archivage dans l'intérêt public poursuivent les finalités détaillées à l'article 1er précité du projet de loi. Il s'agit de répondre aux besoins de la gestion et de la justification des droits et obligations des institutions publiques, de sauvegarder un patrimoine archivistique national et dans un esprit de transparence démocratique, l'accès à la documentation d'intérêt historique, scientifique, culturel, économique ou sociétal du Grand-Duché de Luxembourg

L'exposé des motifs précise en outre que « *l'archivage contribue à documenter l'activité des institutions publiques, à assurer la continuité et le contrôle de leur gestion, ainsi que la sécurité du droit. Il sauvegarde les intérêts légitimes de personnes touchées ou de tiers, ainsi que ceux de la science et de la recherche. Il crée ainsi les conditions nécessaires à la compréhension de l'histoire* ».

Il en ressort une volonté expresse du législateur d'élargir le champ de compétences des Archives nationales, en ne le limitant plus uniquement à la réunion des documents d'intérêt historique national[127]. Ainsi, les Archives nationales disposeront de la base légale nécessaire pour pouvoir procéder à la publication numérique de documents, à leur valorisation lors d'expositions ou d'ateliers pédagogiques.

La Commission nationale regrette toutefois que l'article 1er du projet de loi ne reprenne pas certains éléments de rédaction de l'article L. 211-2 du code du patrimoine français[128], dont il s'inspire pourtant. A la différence de l'article 1er du projet de loi (qui ne vise que la gestion de la justification des droits et obligations des seuls producteurs

[127] L'article 7 de la loi du 25 juin 2004 portant réorganisation des instituts culturels dispose que « *les Archives nationales ont pour mission de réunir tous les documents d'intérêt historique national* ».
[128] L'article L. 211-2 du code du patrimoine français dispose que « *la conservation des archives est organisée dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de la recherche* ».

ou détenteurs d'archives), l'article L. 211-2 du code du patrimoine français inclut parmi les finalités de l'archivage la justification des droits des personnes physiques ou morales, publiques ou privées. Comme le souligne le Conseil d'Etat dans son avis du 21 juillet 2016 relatif au projet de loi sur l'archivage[129], *« les documents des archives publiques peuvent évidemment servir à documenter les droits d'autres personnes que ceux des personnes qui ont produit ou qui détiennent les documents afférents. »*

Sous réserve de l'observation qui précède, la Commission nationale estime que les données traitées à des fins archivistiques dans l'intérêt public répondent à des finalités déterminées, explicites et légitimes, conformément à l'article 4 paragraphe (1) lettre (a) de la loi modifiée du 2 août 2002.

Ces traitements, certes mis en œuvre pour des finalités autres que celles pour lesquelles les données ont été collectées initialement, doivent être considérés comme des traitements ultérieurs a priori compatibles et licites.

Dans le contexte particulier de la mise à disposition de documents d'archives à des fins de réutilisation, la Commission nationale estime primordial d'évaluer l'impact potentiel qu'une telle mise à disposition pourrait avoir sur les droits et libertés des personnes.

A cet égard, la CNPD souscrit entièrement à l'opinion du Groupe de travail « Article 29 » dont elle fait partie sur la réutilisation des informations du secteur public[130] selon laquelle *« une évaluation minutieuse de l'impact sur la protection des données devrait garantir qu'aucune collection d'archives ne soit rendue disponible à des fins de réutilisation avant que soit exclu tout impact négatif potentiel sur les personnes concernées ou que les éventuels risques aient été réduits à un minimum acceptable. Le secteur des archives pourrait également envisager de rédiger des codes de conduite ou de modifier les codes existants afin d'expliquer les bonnes pratiques »*.

VI. Les données traitées

Le projet de loi n'énumère pas les catégories de données traitées dans le cadre de l'archivage. A l'issue de plusieurs échanges avec les Archives nationales, la Commission nationale a noté toutefois, sans prétendre à l'exhaustivité, que les catégories de données à caractère personnel ont vocation à être traitées :

- des données relatives à l'identité civile (nom de famille, nom d'usage, prénoms, surnom, alias, pseudonyme…) et aux coordonnées des personnes concernées ;
- des photographies ;
- des données relatives à la naissance (date et lieu de naissance) ;
- des données relatives à la nationalité (acquisition, perte, naturalisation…) ;
- des données relatives au décès (date, lieu et cause du décès) ;
- des données relatives aux unions et désunions (date et lieu du mariage, du partenariat, du divorce, de la rupture de partenariat) ;
- des données relatives à la filiation biologique ou adoptive (noms, prénoms, date et lieu de naissance des parents, conséquences de la filiation) ;
- parmi les données précitées, certaines relèvent des catégories particulières de données, données communément appelées « données sensibles », définies à l'article 6 de la loi, à savoir des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données relatives à la santé, à la vie sexuelle et les données génétiques (données issues des fonds de l'Inspection Générale de la sécurité sociale, des Soldbücher, etc) ;
- des données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté relevant de l'article 8 de la loi modifiée du 2 août 2002 (données issues des fonds de la police ou de la gendarmerie, ou encore des juridictions comportant des dossiers criminels et pénaux ;
- des données relatives à la vie économique et professionnelle

[129] Avis du Conseil d'Etat n°51.437 du 21 juillet 2016 portant sur le projet de loi sur l'archivage (doc. parl. n°6913), spéc. p. 6.
[130] Avis 6/2013 du Groupe de travail « Article 29 » sur la réutilisation des informations du secteur public (ISP) et des données ouvertes, 5 juin 2013, WP207.

(fonds « ADEM », fonds « Ministère de la Fonction publique »…)
- des données relatives au patrimoine (données issues des registres de l'enregistrement, des hypothèques, des déclarations de succession).

Les données traitées concernent les citoyens luxembourgeois ou étrangers ayant été en contact avec une institution ou un organisme producteur ou détenteur d'archives au Luxembourg (ministère, administration, juridiction, notaires…).

La Commission nationale estime qu'il est de la responsabilité de l'autorité déposant des documents d'archives auprès des Archives nationales de déterminer la nature des données qui y figurent. Elle est toutefois consciente que, pour des raisons pratiques (liées notamment au volume de documents généré), cet examen préalable peut s'avérer difficile dans certaines circonstances.

Elle rappelle en outre que l'article 4 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002 pose un principe de proportionnalité qui devrait être appliqué minutieusement dans le choix des méthodes, des modalités et des degrés de détail envisagés pour rendre les données issues de documents d'archives publiquement disponibles. En effet, les traitements à des fins archivistiques dans l'intérêt public devraient se limiter aux données adéquates, pertinentes et non excessives au regard des finalités poursuivies (conservation, inventorisation, mise à disposition des chercheurs, mise à disposition du public…).

En particulier, la CNPD estime que les catégories particulières de données au sens de l'article 6 de la loi modifiée du 2 août 2002 ne doivent pas être publiées pour répondre à la seule finalité de valorisation du patrimoine auprès du grand public. Elle considère en effet que seule la finalité de mise en valeur à des fins historiques, statistiques ou scientifiques justifie en principe leur publication, sous réserve toutefois que cette publication s'effectue dans des conditions respectueuses de la vie privée des personnes[131].

VII. La durée de conservation des données

L'article 6 paragraphe (1) du projet de loi instaure une procédure selon laquelle les Archives nationales doivent sélectionner en concertation avec les producteurs ou détenteurs d'archives publiques les documents destinés à être archivés de façon définitive. Pour ce faire, des « tableaux de tri » consigneront, pour chaque type de document, la durée durant laquelle ces documents doivent être conservés par l'administration concernée pour des raisons

[131] A l'instar de la position adoptée par la Commission nationale de l'informatique et des libertés française (CNIL) dans sa délibération n°2012-113 du 12 avril 2012 portant autorisation unique de traitements de données à caractère personnel contenues dans des informations publiques aux fins de communication et de publication par les services d'archives publiques (AU-029).

administratives (délai dit « d'utilité administrative »[132]) et le sort finalement réservé à chaque type de document à l'issue dudit délai d'utilité administrative.

La CNPD constate avec satisfaction qu'en application du régime susmentionné, les documents d'archives comportant des données à caractère personnel ne seront en principe conservés que s'ils présentent une utilité administrative ou un intérêt archivistique, scientifique.

Toutefois, en application de l'article 4 paragraphe (1) lettre (d) de la loi du 2 août 2002, les données à caractère personnel contenues dans des documents destinés à l'archivage devraient être en principe conservées sous une forme permettant l'identification des personnes concernées pendant une période n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles les données ont été collectées.

Comme énoncé précédemment, les documents d'archives comportent bien souvent des données à caractère personnel dont la conservation à long terme peut s'avérer nécessaire à des fins historiques, statistiques ou scientifiques. Dans de tels cas de figure, il devrait pouvoir être fait exception à la durée de conservation limitée prévue à l'article 4 paragraphe (1) lettre (d) de la loi du 2 août 2002, ce que prévoit certaines législations étrangères[133].

La CNPD estime donc, pour davantage de clarté, que l'article 6 du projet de loi pourrait être complété d'un paragraphe (3), rédigé sur le modèle de l'article L. 212-3 du Code du patrimoine français :
« (3) Lorsque les archives publiques comportent des données à caractère personnel collectées dans le cadre de traitements régis par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, ces données font l'objet, à l'expiration de la durée prévue à l'article 4 paragraphe (1) lettre (d) de ladite loi, d'une sélection pour déterminer les données destinées à être conservées et celles, dépourvues d'utilité administrative ou d'intérêt scientifique, statistique ou historique, destinées à être éliminées ».

Cette recommandation va dans le sens des évolutions à venir avec l'entrée en vigueur du Règlement général sur la protection des données[134] dont le considérant 156 prévoit que « *le traitement ultérieur de données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques doit être effectué lorsque que le responsable du traitement a évalué s'il est possible d'atteindre ces finalités grâce à un traitement de données à caractère personnel qui ne permettent pas ou plus d'identifier les personnes concernées, pour autant que des garanties appropriées existent (comme par exemple la pseudonymisation des données) (…) ».*

VIII. L'information et les droits des personnes

La Commission nationale observe que les auteurs du projet de loi ont souhaité aménager la protection des droits des personnes telle que prévue par la loi modifiée du 2 août 2002 en prévoyant des dispositions spécifiques dans le projet de loi sous examen.

Elle note à cet égard que l'article 89 du Règlement général sur la protection des données laisse aux Etats membres la possibilité de prévoir des dérogations aux droits reconnus aux personnes concernées (droit d'accès, droit de rectification, droit à l'effacement, droit à la limitation du traitement, droit à la portabilité des données), afin de tenir compte des finalités et des contraintes particulières de l'archivage dans l'intérêt public[135].

A. Le droit d'accès

L'article 19 du projet de loi aménage les conditions et les modalités d'exercice du droit d'accès des personnes, prévu par l'article 28 de la loi modifiée du 2 août 2002.

---

[132] L'article 2 paragraphe 6 du projet de loi définit le délai d'utilité administrative comme *la période pendant laquelle les archives publiques doivent être conservées par le producteur ou détenteur d'archives publiques ou par son successeur en droit en raison notamment de l'utilité administrative qu'elles présentent et des obligations juridiques qui incombent aux producteurs ou détenteurs des archives ».*

[133] En France, une disposition législative spécifique en ce sens, l'article 36 de la loi n°78-17 du 7 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, prévoit que *« Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; le choix des données ainsi conservées est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine ».*

[134] Règlement (UE) 206/679 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 abrogeant la directive 95/46/CE, spéc. considérant 156.

[135] L'article 89 alinéa 3 du Règlement général sur la protection des données prévoit en effet que *« Lorsque des données à caractère personnel sont traitées à des fins archivistiques dans l'intérêt public, le droit de l'Union ou le droit d'un Etat membre peut prévoir des dérogations aux droits visés aux articles 15, 16, 18, 19, 20 et 21, sous réserve des conditions et des garanties visées au paragraphe 1 du présent article, dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités ».*

En application du paragraphe (1) de l'article 19 du projet de loi, les personnes concernées pourront demander communication des données les concernant aux Archives nationales, par écrit et sous réserve de fournir les renseignements nécessaires et suffisants pour qu'une telle demande soit traitée.

La Commission nationale observe que le paragraphe (1) de l'article 19 précité confère également aux Archives nationales la possibilité de restreindre la communication de documents lorsque cette dernière est incompatible avec une « *gestion administrative rationnelle* ». A l'instar des observations du Conseil d'Etat en ce sens[136], elle estime que le critère imprécis de « *gestion administrative rationnelle* » est source d'insécurité juridique.

La CNPD tient en effet à souligner qu'en principe les restrictions au droit d'accès des personnes concernées sont limitativement énumérées par l'article 29 de la loi modifiée du 2 août 2002[137] et l'article 23 du Règlement général sur la protection des données. Elle admet que, compte tenu du volume documentaire qu'elles gèrent, les Archives nationales doivent disposer d'informations précises, afin de pouvoir identifier les données et faire droit aux demandes d'accès des personnes concernées. A cet égard, elle souscrit à la recommandation du Conseil d'Etat de revoir la rédaction de l'alinéa 1er du paragraphe (1) de l'article 19 du projet de loi afin de clarifier son objectif[138]. Elle se demande s'il faut comprendre de la disposition précitée une volonté des auteurs du projet de loi de ne pas faire peser sur les Archives nationales une obligation de fournir des documents dans des cas où la communication de tels documents à la personne concernée se révèlerait impossible ou exigerait des efforts disproportionnés. En outre, la Commission nationale admet que les Archives nationales ne sauraient être tenues de donner suite à des demandes d'accès abusives, en particulier par leur nombre ou leur caractère répétitif ou systématique.

En revanche, elle saurait difficilement admettre une restriction du droit d'obtenir communication d'archives publiques contenant des données à caractère personnel fondée sur le caractère incompatible d'une telle demande avec une « *gestion administrative rationnelle* ». Elle considère en effet que les restrictions au droit d'accès dans le contexte des archives doivent répondre à des critères objectifs et clairement identifiables, ce qui n'est pas le cas en l'occurrence de la notion de « *gestion administrative rationnelle* ». Rappelons dans ce contexte que le droit de la protection des données est un droit à valeur constitutionnelle et que l'article 8.2 de la Charte européenne des droits

[136] Avis du Conseil d'Etat n°51.437 précité, spéc. p. 36.

[137] En application de l'article 29 de la loi modifiée du 2 août 2002, le responsable du traitement peut limiter ou différer l'exercice du droit d'accès pour l'un des motifs suivants : sûreté de l'Etat, défense, sécurité publique, police et justice, sauvegarde de l'intérêt économique ou financier important de l'Etat ou de l'Union européenne, protection de la personne concernée ou des droits et libertés d'autrui.

[138] Le Conseil d'Etat suggère en effet d'indiquer à l'alinéa 1er du paragraphe (1) de l'article 19 que la communication doit se faire « *dans la mesure où les personnes concernées peuvent fournir des renseignements précis en vue de l'identification des données les concernant* ». cf. Avis du Conseil d'Etat n°51.437 précité, spéc. p. 36.

fondamentaux fait expressément référence au droit d'accès des personnes concernées.

S'agissant des modalités d'exercice du droit d'accès, la CNPD relève que le droit d'accès peut s'exercer par « *consultation des archives par la personne concernée elle-même, si l'état de conservation des archives le permet et si des intérêts de tiers ne sont pas affectés* » (paragraphe (2) de l'article 19 du projet de loi).

Elle s'interroge sur la possibilité pour la personne concernée d'obtenir également, au titre de son droit d'accès, une copie au format papier d'un document comportant des données la concernant ou d'en obtenir une copie sous forme électronique par courriel. Le cas échéant et si telle est la volonté du législateur, le paragraphe (2) de l'article 19 du projet de loi devrait être complété en ce sens.

En définitive, la Commission nationale ne peut que soutenir la recommandation formulée par le Conseil d'Etat de « *remettre l'ensemble du texte proposé sur le métier, et cela à la lumière du règlement européen* »[139]. Elle s'inquiète en effet de la création d'un droit d'accès au rabais à travers l'article 19 paragraphe (1) du projet de loi sous examen, dès lors que les données en cause sont issues de documents d'archives publiques. Elle est d'avis que des dérogations au droit d'accès peuvent être admises, conformément d'ailleurs à ce que prévoit l'article 89 précité du Règlement général sur la protection des données, sous réserve de garanties appropriées à fixer par le législateur que la Commission nationale n'est pas en mesure d'apprécier en l'occurrence, faute de précisions suffisantes. Elle considère, à l'instar du Conseil d'Etat, que le droit d'accès en matière d'archives publiques comportant des données à caractère personnel pourrait s'exercer selon des modalités particulières encadrées par le projet de loi sous examen[140], mais dans les conditions prévues par l'article 28 de la loi précitée du 2 août 2002, quitte à y introduire quelques retouches.

B. Rectification et retrait

Le paragraphe (3) de l'article 19 du projet de loi prévoit que « *les personnes concernées ne peuvent pas exiger la destruction ni la rectification de données. Si les personnes concernées sont en mesure de fournir des renseignements prouvant que les archives comportent des affirmations litigieuses ou inexactes, elles peuvent exiger qu'une déclaration contradictoire soit ajoutée aux archives* »[141].

La CNPD admet que les personnes concernées ne peuvent exiger la destruction de données traitées à des fins d'archivage dans l'intérêt public, sans que cela ne rende impossible ou compromette gravement la réalisation des objectifs de l'archivage.

En outre, tout en reconnaissant que les archives doivent être gérées et conservées dans des conditions qui en assurent l'authenticité et l'intégrité, la Commission nationale juge excessive l'affirmation selon laquelle les personnes concernées ne peuvent pas exiger la rectification de données.

Compte tenu des finalités de l'archivage, elle estime satisfaisante la possibilité laissée aux personnes concernées d'exercer une maîtrise sur leurs données en ajoutant à un document contenant des informations qu'elles jugent incomplètes, contestables ou inexactes une déclaration complémentaire s'appuyant sur des preuves suffisantes. Dès lors, la CNPD propose de remplacer l'actuelle rédaction du paragraphe (3) de l'article 19 du projet de loi par les dispositions suivantes :

« *Les personnes concernées ne peuvent pas exiger la destruction ou l'effacement de leurs données figurant dans des documents sélectionnés pour être conservées à long terme. Si les personnes concernées sont en mesure de fournir des renseignements prouvant que les archives comportent des affirmations inexactes ou incomplètes, elles*

[139] Avis du Conseil d'Etat n°51.437 précité, spéc. p. 36.
[140] Avis du Conseil d'Etat n°51.437 précité, spéc. p. 36.
[141] Le paragraphe (3) de l'article 19 du projet de loi précise en outre que « *la déclaration contradictoire doit se limiter à l'affirmation des faits et doit énumérer les preuves, sur lesquelles se base la déclaration contradictoire. Une déclaration contradictoire n'est pas possible pour des dossiers où existe un jugement rendu par les juridictions judiciaires ou administratives.* »

peuvent toutefois exiger qu'une déclaration contradictoire ou complémentaire soit ajoutée aux archives ».

Par ailleurs, s'agissant des traitements ultérieurs de publication, diffusion ou indexation sur internet d'archives publiques, la CNPD considère que toute personne dont des données figureraient dans de tels traitements a le droit d'obtenir sans condition le retrait de cette publication en ligne[142].

C. L'exercice des droits de la personne concernée après son décès

Le paragraphe (5) de l'article 19 du projet de loi prévoit qu'*« après le décès de la personne concernée les droits selon les paragraphes 1 à 3 reviennent à ses héritiers légaux »*. Le commentaire des articles justifie cette extension des droits aux héritiers légaux de la personne concernée par le contexte particulier des archives *« où les déclarations contradictoires avec preuves, fournies par un apparenté, peuvent fournir des informations supplémentaires utiles à la recherche historique »*. Il précise en outre qu'en pratique, les Archives nationales ont déjà été confronté à une demande d'un fils de rectifier les données dans un dossier de son père décédé.

La CNPD est particulièrement sensible à ces considérations et accueille favorablement cette disposition.

D. Le droit à l'information

A défaut de précisions dans le projet de loi, la Commission nationale préconise, en cas de publication de documents d'archives sur Internet, que le responsable de traitement procède à une information générale, claire et complète sur le(s) site(s) internet proposant la consultation de documents d'archives.

IX. Sur les destinataires

Peuvent être destinataires des données :
- les agents habilités à collecter, à conserver et à gérer les archives en application du projet de loi ;
- toute personne intéressée à des fins de consultation ou à des fins historiques, scientifiques ou statistiques.

S'agissant des agents en charge de la collecte, de la conservation et de la gestion des archives, la Commission nationale note qu'en application de l'article 17 du projet de loi les personnes chargées de la collecte ou de la conservation d'archives sont assujetties à une obligation de secret professionnel, *« en ce qui concerne les informations contenues dans les archives qui ne peuvent pas ou ne pas encore être légalement communiquées au public »*. Elle relève en outre

[142] A l'instar de la position adoptée par la Commission nationale de l'informatique et des libertés française (CNIL) dans sa délibération n°2012-113 du 12 avril 2012 précitée.

que cette disposition vise les employés privés, stagiaires et étudiants, ainsi que les sous-traitants chargés de la gestion d'archives publiques[143]. La CNPD estime que la disposition précitée de l'article 17 est de nature à assurer une meilleure confidentialité des données, compte tenu des informations parfois sensibles qui figurent dans les documents d'archives. Elle s'interroge toutefois sur les catégories de personnel visées par les auteurs du projet de loi, compte tenu de la mention dans le commentaire des articles de personnes autres que les employés privés, stagiaires et étudiants, ainsi que les sous-traitants qui seraient assujettis au secret professionnel. L'intention des auteurs du projet de loi gagnerait à être clarifiée sur ce point.

S'agissant du grand public, la Commission nationale note tout particulièrement l'intérêt des catégories de destinataires suivants pour les documents d'archives : les généalogistes, les académiques/universitaires, les journalistes, le milieu du théâtre, le milieu du film, le milieu de la publicité, les administrations publiques, les avocats, les architectes/entrepreneurs, les représentants diplomatiques autorisés, les cultes, etc.

X. Sur l'encadrement de la communication des archives

L'article 16 paragraphe (1) du projet de loi entend poser un principe de communication gratuite à des fins de consultation des archives publiques, sauf dispositions particulières plus restrictives. Elle salue cette démarche tendant à rendre accessible plus rapidement la documentation archivistique d'intérêt public.

Compte tenu du développement croissant de services d'archives digitaux et de la mise à disposition de documents d'archives en ligne, elle invite néanmoins à une certaine prudence et à la mise en place de mesures juridiques et techniques adéquates, afin de minimiser les risques pour la vie privée des personnes et le respect de leurs données à caractère personnel.

A. Les délais de communication des archives

Dans un souci de protection de certains intérêts publics ou privés essentiels, l'article 16 paragraphe (2) du projet de loi assujettit la communication de certains documents d'archives publiques à l'écoulement de délais prolongés, en raison de la nature sensible des informations qu'ils contiennent[144] (article 16 paragraphe (2) du projet de loi).

La Commission nationale note que les intérêts publics ou privés visés par l'article 16 paragraphe (2) du projet de loi *« sont essentiellement ceux qui figurent dans les législations étrangères ainsi que les intérêts repris à l'article 4 de l'avant-projet de loi relative à une administration transparente et ouverte »*[145].

L'article 16 paragraphe (2) du projet de loi renvoie à un règlement grand-ducal le soin de déterminer quels documents d'archives publiques sont soumis à des délais de communication prolongés.

A titre préliminaire, la CNPD ne peut que soutenir la recommandation du Conseil d'Etat selon laquelle les restrictions à la communication de certains documents d'archives publiques devraient être déterminées par voie législative et non réglementaire[146].

Elle observe que le principe de tels délais de communication prolongés était déjà inscrit dans le règlement grand-ducal du 15 janvier 2001 précité. La Commission nationale note toutefois l'instauration de délais mobiles. En effet, l'article 3 paragraphe (1) du projet de règlement grand-ducal précité dispose que :

« (1) Les archives qui contiennent des renseignements individuels relatifs à la vie privée, familiale et professionnelle ou à la situation financière d'une personne physique, qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ainsi

[143] Selon les précisions apportées par l'exposé des motifs.
[144] Figurent au titre des intérêts publics ou privés protégés par un délai de communication prolongé : 1) la défense nationale, la sécurité et l'ordre public ; 2) les affaires portées devant les juridictions luxembourgeoises ; 3) la prévention, la recherche ou la poursuite de faits punissables et de l'auteur de ces faits ; 4) les documents déclassifiés ; 5) le secret des affaires ; 6) les données à caractère personnel.
[145] *cf.* Commentaire des articles du projet de loi sous examen, spéc. *Ad article 16.*
[146] *« Le Conseil d'Etat pour sa part recommande que ce soit le législateur qui, du moins dans leurs grandes lignes, définisse ces restrictions à l'accès aux archives publiques et règle cette matière particulièrement importante » cf.* Avis du Conseil d'Etat n°51.437 précité, spéc. 33.

que le traitement de données relatives à la santé et à la vie sexuelle, y compris le traitement des données génétiques ne peuvent être communiquées que :

- *10 ans après le décès de la personne concernée, au cas où la date de décès est connue ;*
- *50 ans à compter de la date du document le plus récent inclus dans le dossier au cas où la date de décès n'est pas connue ou la recherche de la date de décès entraînerait un effort administratif démesuré. »*

Elle note que ces délais mobiles « *s'expliquent par le désir de rendre les archives plus rapidement accessibles. En effet, il semble peu utile de protéger des informations d'ordre privé par un délai fixe allant au-delà des 10 ans après la mort de la personne concernée. Ce principe est inspiré e. a. de la nouvelle loi sur l'archivage de la Hesse (Allemagne) du 26 novembre 2012* »[147].

Par ailleurs, la CNPD se réjouit de ce que le paragraphe (2) de l'article 3 du projet de règlement grand-ducal prévoit que « *ces délais de communication valent également pour les inventaires nominatifs relatifs aux archives énumérées au précédent paragraphe* », tenant ainsi compte du caractère privé de certaines informations figurant dans lesdits inventaires.

Elle s'étonne en revanche que le délai de communication en vigueur pour les documents comportant des renseignements individuels à caractère médical[148] particulièrement sensibles ne figure plus dans le projet de règlement grand-ducal sous examen. Elle s'interroge sur un éventuel souhait des auteurs du projet de loi de réduire le délai de communication de ces documents, dont la communication pourrait porter atteinte au secret médical, aux délais mobiles précités figurant à l'article 3 paragraphe (1) du projet de règlement grand-ducal sur la communication des archives.

Sur ce point, la Commission nationale est d'avis que le raccourcissement des délais qui en résulterait serait en contradiction avec le droit à la protection des données et au respect de la vie privée. Elle estime, en outre, que ce raccourcissement serait en contradiction avec l'allongement de la durée de l'espérance de vie des personnes.

Selon les statistiques du STATEC, la dernière table de mortalité, calculée pour la période 2012 à 2014, indique que l'espérance de vie à la naissance est de 84.8 ans pour les femmes et de 80.2 ans pour les hommes[149].

Par ailleurs, l'espérance de vie moyenne des Luxembourgeois est en continuelle progression,

[147] *cf.* Commentaire des articles du projet de règlement grand-ducal sur la communication, la reproduction et la publication des archives, spéc. *Ad article 3*.
[148] Actuellement, l'article 5 paragraphe 1 du règlement grand-ducal du 15 janvier 2001 fixe à 150 ans, à compter de la date de naissance de la personne concernée, pour les documents comportant des renseignements individuels à caractère médical.
[149] Institut national de la statistique et des études économiques (STATEC), Regards sur la mortalité, n°13/2015, 24 novembre 2015.

quel que soit le sexe. A titre d'illustration, depuis la période 2005/2007, le gain est de 2,6 ans pour les hommes et de 2,1 ans pour les femmes. Actuellement, les espérances de vie à la naissance des hommes et des femmes résidant au Luxembourg sont parmi les plus élevées en Europe

La Commission nationale estime qu'un délai de 10 ans après le décès (si la date de décès est connue) ou de 50 ans à compter de la date du document le plus récent inclus dans le dossier (si la date de décès est inconnue ou extrêmement difficile à trouver) ne suffit pas à garantir, dans toutes les hypothèses, une protection réelle de la vie privée. L'accessibilité des documents d'archives comportent dans certains cas un risque accru d'atteinte à la vie privée et à la protection des données personnelles des individus ou de leurs proches, et ce, même après 10 ans après le décès.

Elle considère qu'un délai plus long pour les documents dont la communication risque de porter atteinte au secret médical serait de nature à assurer une meilleure protection des personnes. Ce délai pourrait être de 25 ans à compter de la date du décès de l'intéressé (si celle-ci est connue) ou de 120 ans à compter de la date de naissance de la personne concernée (si la date du décès n'est pas connue).

En outre, la Commission nationale note qu'en application des paragraphes (1) et (2) de l'article 11 du projet de règlement grand-ducal, la communication de documents d'archives publiques peut être accordée de manière dérogatoire, avant l'expiration des délais de communications prolongés susmentionnés, en présence d'un « *intérêt public motivé* » par le demandeur ou sur autorisation écrite de la personne concernée de son vivant (sur autorisation de ses héritiers légaux en cas de décès). La décision d'autoriser ces accès dérogatoires reviendrait alors au directeur des Archives nationales en accord avec le producteur des archives publiques concernées (art. 12 du projet de règlement grand-ducal).

Occasionnellement saisie de demande d'accès dérogatoire aux archives, la Commission nationale se réjouit de ce que l'article 12 du projet de règlement grand-ducal prévoit un tel cadre pour la consultation, avant l'expiration des délais prolongés, de documents dont la consultation pourrait présenter un intérêt public.

Si ces accès dérogatoires sont de nature à ménager des conditions favorables au développement de la recherche scientifique et historique au Luxembourg, la Commission nationale estime qu'en toute hypothèse que les conditions de traitement de ces données doivent demeurer loyales et licites. En particulier, les données issues des archives consultées ne devraient pas être utilisées pour venir appuyer des mesures ou décisions à l'égard d'un individu en particulier. De même, les données ne devraient pas être utilisées de sorte qu'elles causent ou puissent causer un dommage à l'encontre des personnes concernées[150].

A titre subsidiaire, s'agissant des minutes et répertoires des notaires, le paragraphe 3 de l'article 16 du projet de loi dispose que les documents en question ne peuvent être communiqués à des fins de consultation à des tiers (c'est-à-dire à des personnes autres que les personnes intéressées en nom direct ou leurs héritiers et ayants droit) qu'après l'expiration des délais de communication prolongés à fixer par voie de règlement grand-ducal.

En l'absence de précisions dans le projet de texte, la Commission nationale estime que le projet de règlement grand-ducal précité devrait être complété, afin de mentionner explicitement quels délais de communication prolongés s'appliquent aux minutes et répertoires des notaires.

De manière plus générale, la CNPD appelle les rédacteurs des projets de texte sous examen à harmoniser les notions utilisées pour justifier des délais

[150] La Commission nationale note toutefois que les délais de communication prolongés ne valent pas pour les documents contenant des informations ayant trait à la vie privée de personnalités jouant un rôle dans la vie publique, dans l'hypothèse où la communication, la reproduction et/ou la publication d'archives publiques serait nécessaire à la réalisation d'une recherche ou d'un travail scientifique effectués dans l'intérêt public (art. 11 et 16 du projet de règlement grand-ducal).

de communication prolongés avec les motifs pouvant justifier une limitation de l'accès à des documents au titre du projet de loi n° 6810 relatif à une administration transparente et ouverte, initiative législative en instance devant la Chambre des députés et à propos de laquelle la Commission nationale a déjà eu l'occasion de se prononcer dans son avis du 26 février 2016[151].

B. L'encadrement de la publication des archives sur internet

1. Des délais plus longs

La Commission nationale observe que la publication sur internet de certaines archives contenant des données à caractère personnel sera subordonnée à l'expiration d'un délai plus long que le délai de non-communicabilité desdites archives.

Ainsi de tels documents pourront être mis en ligne à l'expiration d'un délai de 75 ans à compter de la date du document, en application de l'article 4 du projet de règlement grand-ducal sur la communication, la reproduction et la publication des archives.

L'exposé des motifs précise à juste titre qu' *« en matière de protection des données à caractère personnel, il importe en effet de différencier entre la communication d'un dossier physique, accessible sur demande à une personne à la fois et ceci dans un endroit précis, et la mise à disposition en ligne, accessible librement et simultanément à tout internaute peu importe son lieu de consultation ».*

La Commission nationale se félicite de cet encadrement prévu par les auteurs du projet de loi, compte tenu du risque d'atteinte disproportionnée pour la vie privée qui pourrait résulter d'une publication sur Internet de certaines informations ayant trait à la vie privée des personnes (unions, désunions, naturalisations, changements de nom, adoptions, reconnaissances, légitimations, abandons…).

Elle relève en outre qu'en application de l'article 5 du projet de règlement grand-ducal précité, *« pour toute communication d'archives pour lesquelles au moins deux des délais visés aux articles 2 à 4 du présent règlement grand-ducal s'appliquent, le plus long des délais l'emporte ».*

Toutefois la CNPD estime que l'écoulement d'un délai de 100 ans à compter de la date du document avant la publication de documents d'archives sur Internet serait de nature à assurer une meilleure protection de la vie privée et des données des personnes concernées, en conformité avec les recommandations de la CNIL en la matière.

[151] Sur ce point, la Commission nationale renvoie à sa délibération n°196/2016 du 26 février 2016 portant conjointement sur le projet de loi n°6810 relatif à une administration transparente et ouverte et sur le projet de loi n°6811 modifiant la loi du 4 décembre 2007 concernant la réutilisation des informations du secteur public.

2. Prévoir des restrictions d'accès lors de la mise en ligne de données sensibles

Par principe, la publication sur internet d'archives contenant des catégories particulières de données au sens de l'article 6 de la loi devraient faire l'objet de restrictions d'accès.

La CNPD est soucieuse de trouver un équilibre entre l'intérêt des chercheurs et la protection des données. Elle admet que, du fait de leur intérêt pour la recherche historique, scientifique ou statistique, une occultation définitive des données sensibles ne serait pas conforme à l'intérêt public.

Sans imposer de ligne directrice trop rigide en la matière, la CNPD tient à souligner que certains pays voisins[152] ont encadré les traitements de leurs services d'archives en se prononçant en faveur d'une publication des archives sur Internet avec occultation des données sensibles durant un certain délai ou en faveur d'une publication sans occultation des données sensibles mais avec des mécanismes visant à restreindre l'accès aux données : création d'un compte utilisateur pour l'accès à certains fonds, accès restreint à certaines catégories de personnes (chercheurs) ou organismes (instituts de recherche), limitation du nombre de documents consultables….

C. L'encadrement de la réutilisation des archives

La Commission nationale considère que toute réutilisation d'archives publiques contenant des données à caractère personnel ne peut intervenir que dans les conditions prévues, d'une part par la loi modifiée du 2 août 2002 et, d'autre part, par la loi du 23 mai 2016 modifiant la loi du 4 décembre 2007 sur la réutilisation des informations du secteur public.

Sans revenir dans le détail sur cette problématique de la réutilisation des informations du secteur public[153], la CNPD relève que l'article 14 du projet de règlement grand-ducal sur la communication, la reproduction et la publication des archives en reprend le principe, ce dont elle se félicite. L'article 14 précité dispose en effet que *« les documents numériques ou numérisés mis à disposition par les Archives nationales sur leur propre site internet ou sur les sites internet de leurs partenaires peuvent être utilisés en fonction des modalités fixées par le type de licence ou de marque auxquels lesdits documents sont soumis ».*

Comme elle l'a souligné dans son avis du 26 février 2016 sur les projets de loi n°6810 concernant une administration transparente et ouverte et n°6811 sur la réutilisation des informations du secteur public, la CNPD estime que, dans le contexte des archives, l'instauration d'un régime de licence rigoureux est de nature à garantir que des données à caractère personnel ne soient pas utilisées pour des finalités incompatibles avec celles pour laquelle elles ont été initialement collectées. Elle avait en outre observé que les contrats de licence devraient rappeler aux réutilisateurs qu'ils sont tenus de respecter leurs obligations en matière de protection des données.

XI. Les transferts

La CNPD observe que toute exportation d'archives publiques vers un pays situé hors de l'Union européenne doit nécessairement respecter les conditions prévues par la loi modifiée du 2 août 2002. Elle estime dès lors, comme le préconise le Conseil d'Etat[154], que la précision selon laquelle l'exportation des archives publiques peut s'effectuer, *« sans préjudice de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel »* peut être supprimée du paragraphe 3 de l'article 12 du projet de loi.

Elle rappelle à cet égard qu'il est possible de réaliser des transferts de données hors de l'Union européenne, sous réserve du respect des dispositions des articles 18 et 19 de la loi modifiée

[152] Notamment la France, à l'issue d'une procédure de consultation des services d'archives concernés.
[153] Pour plus détails voir la Délibération n°196/2016 du 26 février 2016.
[154] Avis du Conseil d'Etat n°51.437 précité, spéc. p. 26.

du 2 août 2002 concernant les principes et dérogations applicables en matière de transferts de données vers des pays tiers. Elle souligne que le recours aux exceptions prévues par l'article 19 paragraphe (1) de la loi modifiée du 2 août 2002 n'est pas possible pour les transferts répétitifs, massifs ou structurels de données qui doivent quant à eux faire l'objet d'un encadrement spécifique.

XII. La sécurité

En application des articles 22 et 23 de la loi modifiée du 2 août 2002, des mesures techniques et organisationnelles adéquates doivent être envisagées en fonction des risques identifiés, notamment l'anonymisation ou la pseudonymisation des données, des mesures visant à éviter le téléchargement massif ou répété de documents (notamment la limitation du nombre de documents accessibles depuis une même adresse IP). La CNPD recommande également que des mesures techniques soient mises en œuvre par les organismes responsables de la mise à disposition de documents d'archives au public, afin d'empêcher l'indexation desdits documents par les moteurs de recherche externes à leur site internet. Elle observe en effet que le respect des durées de conservation prévues par les textes et l'exercice de leurs droits par les personnes concernées sont rendus plus difficiles, après l'indexation d'informations par les grands moteurs de recherche sur internet. La Commission nationale estime qu'un équilibre entre l'objectif de transparence et la protection des données à caractère personnel peut être atteint en recourant à des mesures de restriction techniques concernant les capacités de recherche de documents d'archives sur internet (« CAPTCHA », « robots.txt »).

La CNPD souligne en effet que les données à caractère personnel contenues dans les archives doivent être stockées et traitées en toute sécurité, afin d'en garantir la confidentialité à tout moment. Elle relève en outre que la nécessité de prévoir des garanties adéquates en matière de traitement d'archives a été pleinement reconnue par le Règlement général sur la protection des données, adopté le 27 avril 2016 et dont les dispositions seront applicables à partir du 28 avril 2018[155].

La Commission nationale note qu'en application de l'article 8 du projet de loi un sous-traitant devra remplir les conditions suivantes : *1)* il devra être spécialisé dans l'archivage de documents, d'une part, et *2)* il devra apporter des garanties suffisantes au regard de la loi modifiée du 2 août 2002, d'autre part.

Dans son avis du 21 juillet 2016, le Conseil d'Etat a souligné au sujet de l'article 8 du projet de

[155] Règlement (UE) 206/679 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 abrogeant la directive 95/46/CE, voir notamment les considérants 156 et 158 et l'article. 9 paragraphe (2), lettre j) et l'article 89 paragraphe (1).

loi que la « *condition essentielle, à savoir celle de la fourniture de garanties suffisantes par le sous-traitant dans le domaine de la protection des données à caractère personnel n'est pas formulée de façon suffisamment précise. S'agissant d'un domaine particulièrement sensible, qui ne tolère pas la moindre insécurité juridique, le Conseil d'Etat insiste à ce que ces garanties soient formulées avec plus de précision au niveau de la loi en projet.* »

La CNPD ne peut que souscrire à cette recommandation et rappelle qu'en cas de recours à un sous-traitant, le responsable du traitement doit en particulier imposer à ce sous-traitant, au moyen d'un contrat, de n'utilliser les données qu'aux fins prévues, de s'assurer de leur confidentialité et de procéder à la destruction ou à la restitution de tous les supports manuels ou informatisés de données à caractère personnel au terme de sa prestation. Elle estime dès lors que les dispositions de l'article 8 du projet de loi devraient être complétées afin de détailler les garanties auxquelles un sous-traitant en matière d'archivage devra être assujetti.

XIII. Sur l'articulation du projet de loi n°6913 avec d'autres initiatives législatives récentes

A titre subsidiaire, la Commission nationale relève que le projet de loi sous examen est silencieux quant à son articulation avec plusieurs initiatives législatives récentes. Elle s'interroge sur la mise en cohérence de ces différents textes ou projets de texte et sur le régime juridique qui résultera de leur entrée en vigueur respective.

A titre d'illustration, la notion d'« *atteinte à un secret ou une confidentialité protégés par la loi* » prévue dans le projet de loi n°6810 relatif à une administration transparente et ouverte, traitant selon une approche globale de l'accès aux documents administratifs, n'a pas son pendant exact dans le projet de loi sous examen, qui se réfère uniquement aux notions de secret fiscal et de secret des affaires (sans mentionner notamment le secret médical). En outre, les notions de « *document détenu par une administration et correspondant à une activité administrative* » (visée par le projet de loi n°6810) et d'« *archive publique* » se recoupent parfois sans se confondre, de sorte qu'il est permis de s'interroger sur le régime précis qui s'appliquera aux documents détenus par l'administration (au sens du projet de loi n° 6810) et qui constituent des archives publiques (au sens du présent projet de loi), sur une éventuelle compétence de la future « *Commission d'accès aux documents* » au regard de certains documents d'archives publiques… La Commission nationale estime que l'intention des auteurs du projet de loi devrait être clarifiée sur ce point.

Plus particulièrement, la CNPD s'interroge sur la manière dont interagiront les dispositions du projet de loi sous examen et de celles de 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'Etat. Dans son avis n°51.266 du 2 février 2016 concernant le projet de loi régissant les archives historiques du Service de Renseignement de l'Etat (projet de loi n°6850), le Conseil d'Etat se posait en effet « *la question de savoir si le projet de loi sous examen (ledit projet de loi n°6913) n'a pas perdu de son utilité suite au dépôt du projet de loi n°6913 sur l'archivage, alors que celui-ci est appelé à régir l'ensemble des fonds d'archives publiques, y compris dès lors ceux du SRE pris dans leur ensemble et donc également les données visées au projet sous examen* ». La Commission nationale estime qu'en dépit de l'adoption récente de la loi du 23 juillet 2016 par la Chambre des députés, la question de l'interaction entre les deux textes précités demeure entièrement ouverte et que le législateur devra porter une attention particulière à leur concordance.

La Commission nationale se demande, en outre, si l'accès et l'exploitation, dans des conditions dérogatoires au droit

commun, de fonds d'archives publiques appelant un régime juridique particulier (tels que l'accès aux archives du SREL) ne devrait pas plutôt être régi par des dispositions législatives ou réglementaires spécifiques dérogeant au droit commun relatif à l'accès aux documents d'archives publiques, tel qu'issu du projet de loi sous examen.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 14 octobre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7049 portant modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

Délibération n°850/2016
du 14 octobre 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 a notamment pour mission d'aviser « *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* ».

Faisant suite à la demande lui adressée par le Ministre des Communications et des Médias en date du 18 août 2016, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de ce projet de loi de modification 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 « le projet de loi »).

Selon l'exposé des motifs, ce projet de loi a deux objectifs principaux : « *la simplification substantielle des formalités obligatoires qui se traduit par un allègement du régime d'autorisation préalable sans pour autant diminuer la protection des citoyens* » ainsi que « *la transition du régime actuel vers le régime du règlement européen relatif à la protection des données* ». En effet, le régime actuel est amené à être remplacé par le règlement européen 2016/679 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 (ci-après « le règlement général sur la protection des données »). Ce règlement abroge la directive 95/46/CE transposée en droit national par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et sera applicable à partir du 25 mai 2018.

Dès son début, la Commission nationale a régulièrement constaté que les responsables de fichiers et de traitements de données sont plus attentifs à l'accomplissement des formalités préalables qu'au respect des principes édictés par la loi. Comme évoqué dans ses rapports annuels d'activité, la Commission nationale a toujours œuvré pour un allègement des formalités administratives pour privilégier les contrôles et mieux préserver la protection des personnes concernées. Cette volonté a été mainte fois réitérée y compris lors de la dernière simplification substantielle de la loi modifiée du 2 août 2002 opérée en 2007[156]. Comme déjà indiqué dans son avis relatif à cette loi modificative du 27 juillet 2007, elle a expliqué que « *l'important est que cela rentre dans les mentalités, pas seulement sur les formulaires* »[157]. Elle avait clairement indiqué le caractère très restrictif de la loi luxembourgeoise par rapport à ses voisins européens. Il ressortait d'un tableau comparatif inclus dans ce même avis que l'obligation d'autoriser ces traitements était rarement requise dans le reste de l'Europe. Pour ce qui est du Luxembourg, il est difficile de constater une plus-value tangible en matière de protection des droits par rapport à d'autres pays dans lesquelles le même régime d'autorisation préalable n'existe pas.

Pour garantir une application effective de la loi et assurer une bonne protection des droits des personnes concernées, il est essentiel que la Commission nationale puisse effectuer régulièrement des contrôles de conformité. Or, actuellement, son activité est principalement accaparée par le traitement des demandes d'autorisations dans le domaine de la surveillance qui représente annuellement entre 85% et 90% des demandes d'autorisation traitées. Avec la simplification proposée par ce projet de loi, la procédure d'autorisation préalable plus lourde sera remplacée par la procédure de notification prévue à l'article 12 de la loi et la Commission nationale pourra plus facilement effectuer des visites de contrôle qui sont plus efficaces et peuvent être mieux ciblées que les autorisations pour s'assurer du respect de la loi par les responsables de traitement de données. La Commission nationale demeure soucieuse de fournir de l'aide et de l'assistance aux responsables de traitement pour les aider à se conformer avec les dispositions légales applicables en publiant notamment sur son site internet des lignes directrices sur ce sujet. Ainsi, en collaboration avec la Chambre des salariés, la Commission nationale a publié en 2014 une brochure très détaillée dédiée à la question de la surveillance.

Dès lors, la Commission nationale ne peut qu'accueillir très favorablement les simplifications des démarches administratives proposées dans ce projet de loi en particulier en ce qui concerne le régime de formalités applicables aux traitements mis en œuvre à des fins de surveillance.

Cette simplification contribue aussi à uniformiser le régime en vigueur au Luxembourg par

[156] *Loi du 27 juillet 2007 portant modification - de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; - des articles 4 paragraphe (3) lettre d) ; 5 paragraphe (1) lettre a) ; 9 paragraphe (1) lettre a) et 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et - de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expression dans les médias.*

[157] *Page 2 de l'avis de la Commission Nationale pour la Protection des Données du 5 décembre 2005 pour le projet de loi portant modification - de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ; - des articles 4 paragraphe (3) lettre d) ; 5 paragraphe (1) lettre a) ; 9 paragraphe (1) lettre a) et 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et - de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expression dans les médias.*

rapport à ses voisins européens. C'est une étape importante avant l'application du nouveau règlement européen dans ce domaine qui sera applicable dans toute l'Union Européenne.

Le nouveau règlement général sur la protection des données privilégie le contrôle a posteriori au lieu du contrôle a priori. De plus, les responsables de traitement se devront de tenir un registre de leurs traitements de données[158]. La Commission nationale est d'avis que la suppression du régime de la demande d'autorisation et le maintien de celui de la notification pour les traitements de données concernés par cette simplification sont de nature à préparer les responsables de traitement à assumer ces nouvelles responsabilités. Pour la Commission nationale, cela impliquera un renforcement de son activité de guidance et de contrôle. Et pour les responsables de traitement de données, cela nécessitera une prise de conscience de leur responsabilité par rapport au traitement de données qu'ils effectuent.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 14 octobre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

[158] *Article 30 du règlement européen 2016/679 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.*

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°6995 portant modification de l'article 23 du Code d'instruction criminelle et de la loi du 7 août 2012 portant création de l'établissement public « Laboratoire national de santé »

Délibération n°856/2016 du 14 octobre 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 » ou « la loi »), 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 en date du 25 mai 2016, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer sur le projet de loi portant modification de l'article 23 du Code d'instruction criminelle et de la loi du 7 août 2012 portant création de l'établissement public « Laboratoire national de santé » (ci-après « le projet de loi »)

Le projet de loi a pour objectif d'adapter certaines dispositions du droit luxembourgeois afin d'instaurer une *« unité de documentation médico-légale des violences »* (projet dénommé *« Opferambulanz »*)[159] dont la gestion sera confiée à l'établissement public « Laboratoire National de Santé » (ci-après « le LNS »). Cette unité a vocation à documenter d'un point de vue médico-légal les blessures physiques subies par des personnes physiques victimes d'infractions pénales intentionnelles ou non intentionnelles.

La Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de loi sous examen traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel.

XIV. La responsabilité du traitement

L'article 2 du projet de loi complète les missions du LNS en introduisant un article 2-1 nouveau à la loi du 7 août 2012 portant création de l'établissement public « Laboratoire national de santé », en confiant à ce dernier la gestion de l'unité de documentation médico-légale des violences.

Il ressort plus précisément du dossier que la documentation médico-légale des violences sera constituée par une équipe dédiée du personnel du LNS relevant du département de médecine légale. Cette équipe constituera « l'unité de documentation médico-légale des violences ».

XV. La finalité du traitement de données à caractère personnel

L'article 2-1 nouveau précité précise que l'unité de documentation médico-légale des violences, *« a comme mission de fournir sans frais à toute personne majeure une documentation médico-légale des blessures physiques subies suite à la commission d'une infraction pénale, ainsi que toute trace en relation avec les blessures documentées. Cette documentation est réalisée indépendamment de toute plainte ou action judiciaire pénale ou civile. »*.

Il ressort de l'exposé des motifs du projet de loi que l'unité de documentation médico-légale des violences sera en charge de constituer et de conserver un *« fichier de données à caractère personnel »* au sens de l'article 2 lettre (h) de la loi, afin de *« documenter d'un point de vue purement médico-légal les blessures physiques d'une personne ayant été causées par la commission d'une infraction pénale, peu importe s'il s'agit*

[159] *cf.* Exposé des motifs du projet de loi, spéc. p. 2.

d'une infraction intentionnelle ou non intentionnelle. »[160].

Afin de mieux circonscrire le champ d'application du projet de loi sous examen, la Commission nationale suggère de modifier la formulation du paragraphe (1) de l'article 2-1 nouveau précité :

« (1) L'établissement gère en outre l'unité de documentation médico-légale des violences qui a comme mission de fournir sans frais à toute personne majeure ***ayant subi des blessures physiques suite à la commission d'une infraction pénale*** *une documentation médico-légale de leurs blessures, ainsi que toute trace en relation avec les blessures documentées. Cette documentation est réalisée indépendamment de toute plainte ou action judiciaire pénale ou civile.*

La CNPD suggère en outre d'apporter les précisions suivantes au paragraphe (2) de l'article 2-1 nouveau précité :

« (2) L'unité de documentation médico-légale des violences prend en charge la conservation de la documentation réalisée conformément aux dispositions de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Sans préjudice des dispositions applicables du Code d'instruction criminelle, seule la personne ***ayant subi les blessures documentées*** *suite à la commission d'une infraction pénale a le droit de disposer de la documentation réalisée à son égard ».*

Il précise en outre que *« l'objectif de cette documentation est son utilisation ultérieure éventuelle dans le cadre d'une procédure pénale concernant les faits ayant causé les blessures physiques. Les services de l'unité médico-légale des violences se limitent à la documentation et à la conservation des preuves et, à ce stade, les prélèvements nécessaires, en fonction des blessures et de leurs causes, sont faits sans qu'il soit procédé dans l'immédiat à leur analyse médico-légale. Ces missions sont le cas échéant ordonnées par le Parquet ou le juge d'instruction au moment où les faits en cause font l'objet d'une enquête ou d'une instruction préparatoire »*[161].

La Commission nationale note que le concept d'unité de documentation médico-légale présente un intérêt tout particulier dans le contexte de violences domestiques ou d'agressions, suite auxquelles les victimes hésitent souvent à déposer plainte auprès des autorités de police ou judiciaires.

Sous réserve des précédentes observations, elle estime que le traitement de données envisagé dans le cadre du fonctionnement de l'unité de documentation médico-légale des

[160] *cf.* Exposé des motifs du projet de loi, spéc. p. 2.
[161] *cf.* Exposé des motifs du projet de loi, spéc. p. 3.

violences répond à une finalité déterminée, explicite et légitime, conformément à l'article 4 paragraphe (1) de la loi.

XVI. Les données traitées

Le projet de loi est silencieux sur ce point.

La Commission nationale note toutefois que l'unité de documentation médico-légale des violences permettra de renseigner, dans la perspective d'enquêtes ou de poursuites judiciaires ultérieures, des éléments qui ne sont pas systématiquement recueillis dans une optique thérapeutique. La CNPD s'interroge toutefois, en l'absence de précisions dans l'exposé des motifs ou du commentaire des articles du projet de loi, quant à la teneur exacte des informations collectées. Elle rappelle à ce titre qu'en application de l'article 4.(1).b) de la loi modifiée du 2 août 2002 les principes de nécessité et de minimisation des données doivent être respectés lors du traitement des données.

Il ressort du dossier que certaines catégories de données à caractère personnel seront systématiquement collectées par les membres de l'unité de documentation médico-légale des violences, notamment les données d'identification des victimes (données nominatives et coordonnées, pseudonymes), des informations concernant les violences constatées sur ces dernières, parmi lesquelles pourraient figurer des catégories particulières de données définies à l'article 6 de la loi modifiée du 2 août 2002 (données relatives à la santé et à la vie sexuelle), ainsi que des prélèvements biologiques.

La CNPD s'interroge sur l'éventuelle collecte de l'image des personnes (photographies) et sur les conditions de collecte de ces images.

Par ailleurs, il ressort du dossier qu'un procédé de pseudonymisation réversible sera mis en œuvre, afin de permettre un retour vers l'identité des personnes concernées et une prise de contact avec ces dernières. L'exposé des motifs précise en effet que « *l'identité de la victime est pseudonymisée, c.-à-dire que l'identité est constatée lors du premier contact, mais tout traitement ultérieur de la documentation et des données personnelles de la victime se fait à l'aide d'un système ne révélant pas l'identité de la victime, comme un système de code barre par exemple. Il est en effet indispensable que l'identité de la victime ait été constatée, notamment afin de permettre au Laboratoire National de Santé lors de tout contact ultérieur de s'assurer qu'il s'agit effectivement de la victime en cause.* »[162].

En l'absence de précisions dans le dossier, la CNPD n'est pas en mesure d'apprécier les modalités de pseudonymisation des données et de réidentification des personnes (établissement éventuel d'une table de correspondance, utilisation d'un algorithme de chiffrement ou d'une fonction de hachage…) attestant de garanties appropriées pour le respect de la vie privée.

Elle recommande, en présence de données sensibles figurant dans le fichier de l'unité de documentation médico-légale des violences, la mise en place d'une gestion séparée entre les données d'identification nécessaires pour recontacter les personnes concernées, d'une part, et les données détaillées concernant les violences, d'autre part, reposant notamment sur la création de deux bases de données distinctes respectant un principe de cloisonnement et sur la définition d'habilitations d'accès différenciées selon le profil et les missions du personnel du LNS.

XVII. La durée de conservation des données

En application de l'article 4 paragraphe (1) lettre (d) de la loi du 2 août 2002, les données à caractère personnel traités au sein de l'unité de documentation médico-légale des violences devraient être en principe conservées sous une forme permettant l'identification des personnes concernées pendant une période n'excédant pas

[162] *cf.* Exposé des motifs du projet de loi, spéc. p. 3.

celle nécessaire à la réalisation des finalités pour lesquelles les données ont été collectées.

Il ressort du dossier que *« la documentation sera conservée par le Laboratoire National de Santé pour une durée maximale de dix ans, ce qui correspond à la durée de prescription de l'action publique pour crimes »*[163]. Le point de départ du délai précité n'est cependant pas précisé.

Une durée de conservation limitée de données à caractère personnel constitue une garantie supplémentaire pour éviter d'éventuels détournements de finalité.

La Commission nationale estime que, passé le délai susmentionné de dix ans à compter de la date de commission des violences, les données conservées au sein de l'unité de documentation médico-légale des violences devront être supprimées. Elle considère, s'agissant d'une matière dont l'essentiel du cadrage normatif doit figurer dans la loi[164], que le délai précité devrait être mentionné dans le projet de loi sous examen.

XVIII. L'information et les droits des personnes

E. Le droit à l'information

A défaut de précisions dans le projet de loi, la Commission nationale préconise que le responsable de traitement procède à une information générale, claire et complète, conformément à l'article 26 de la loi modifiée du 2 août 2002. Elle recommande notamment, outre l'information par publication du projet de loi, une information des personnes dans les livrets d'accueil des hôpitaux ou de l'unité de documentation médico-légale des violences. Elle estime que cette information devrait porter notamment sur les droits dont disposent les personnes concernées.

F. Le droit d'accès

L'article 2 paragraphe 2 du projet de loi dispose que :

« Sans préjudice des dispositions applicables du Code d'instruction criminelle, seule la personne concernée a le droit de disposer de la documentation réalisée à son égard ».

A cet égard, la CNPD relève les précisions utiles de l'exposé des motifs selon lequel :

« La documentation est conservée par le Laboratoire National de Santé mais la victime garde le contrôle et la maîtrise sur la documentation. Ce pouvoir de contrôle de la victime s'entend bien sûr sans préjudice des pouvoirs des autorités répressives si les faits en cause font finalement l'objet d'une enquête ou d'une instruction préparatoire »[165].

---

[163] *cf.* Exposé des motifs du projet de loi, spéc. p. 4.
[164] Avis du Conseil d'Etat du 7 juin 2016 concernant le projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures, avis 6975/5.
[165] *cf.* Exposé des motifs, spéc. p. 3.

Elle note en outre que *« le droit de la victime de disposer de la documentation qui la concerne est bien sûr conditionné par une enquête ou une instruction préparatoire en cours. Dans ce cas, les dispositions du Code d'instruction criminelle relatives par exemple aux perquisitions et saisies prévalent. Si donc, par exemple, les autorités judiciaires prennent connaissance de la commission d'une infraction par un autre biais que la victime elle-même et un juge d'instruction décerne un mandat de perquisition-saisie, la documentation relative à cette infraction sera saisie et la victime ne saurait s'y opposer sur base de son droit de disposer de cette documentation »*[166].

La Commission nationale prend acte de ces modalités d'exercice du droit d'accès. Elle estime ces dernières compatibles avec les exceptions au droit d'accès prévu par l'article 29 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002. Cet article prévoit en effet, pour ce qui concerne certains traitements mis en œuvre pour des besoins de sécurité publique ou de prévention, de recherche, de constatation et de poursuite d'infractions pénales, que le responsable du traitement peut limiter ou différer l'exercice du droit d'accès d'une personne concernée.

XIX. Sur les destinataires

Peuvent être destinataires des données :

- les médecins légistes de l'unité de documentation médico-légale des violences au sein du LNS ;
- les médecins et autres professionnels de santé consultés par les médecins légistes dans le cadre de l'unité de documentation médico-légale des violences ;
- le Parquet ou le juge d'instruction en cas d'enquête ou d'instruction préparatoire.

La Commission nationale en prend acte. Elle note que le législateur entend autoriser, dans certaines situations, un partage d'informations entre professionnels de santé participant à la constitution de la documentation médico-légale des violences, ainsi qu'une communication de ces informations par les médecins aux autorités de police et aux autorités judiciaires.

a) L'échange d'informations entre professionnels de santé participant à la constitution de la documentation médico-légale des violences : le « secret partagé »

La CNPD note que l'unité de documentation médico-légale des violences est censée fonctionner selon un mode décentralisé, reposant sur une collaboration étroite entre ladite unité et les hôpitaux.

En effet, l'exposé des motifs précise qu'*« il est ainsi prévu que les médecin-légistes de l'unité de documentation médico-légale des violences se rendent en principe à l'hôpital pour éviter la disparition de preuves médico-légales dans le cadre des soins médicaux, et également afin d'éviter aux victimes de devoir d'abord se déplacer à l'hôpital pour éviter la disparition de preuves médico-légale des violences dans le cadre de soins médicaux, et également afin d'éviter aux victimes de devoir d'abord se déplacer à l'hôpital pour les soins médicaux et ensuite au Laboratoire National de Santé pour la documentation de leurs blessures. En outre, ce fonctionnement décentralisé vise à favoriser, si nécessaire, une consultation mutuelle entre les médecins et les médecin-légistes afin que chacun puisse accomplir sa mission dans son domaine de compétence qui lui est propre. Néanmoins, rien n'empêche une victime n'ayant par exemple subi que des blessures légères de se rendre directement au Laboratoire National de Santé à Dudelange sans passer auparavant par un hôpital. »*

Pour ce faire, l'article 2 du projet de loi ajoute un article 2-1 nouveau à la loi du 7 août 2012 portant création du LNS

[166] *cf.* Commentaire des articles, spéc. p. 7.

qui pose les conditions d'un partage d'informations entre les médecins hospitaliers et les médecins-légistes de l'unité de documentation médico-légale des violences, en aménageant les conditions applicables au secret professionnel, selon le concept du « secret médical partagé ». Cet article dispose en effet que :

« Le secret professionnel prévu à l'article 458 du Code pénal ne s'oppose pas à l'échange d'informations effectué entre, d'une part, le personnel employé au sein de l'unité de documentation médico-légale des violences et, d'autre part, les médecins et autres professionnels de santé qui sont consultés par les médecins légistes dans le cadre de cette unité ».

La Commission nationale relève en outre que « L'approche générale est celle d'une coopération entre les médecin-légistes de l'unité de documentation médico-légale des violences et d'autres médecins généralistes ou spécialistes. Dans le cadre de lésions corporelles qui pourraient par exemple provenir d'un viol, il est très bien imaginable que le gynécologue et le médecin-légiste sont appelés, dans l'intérêt de la victime, à se consulter mutuellement afin que chacun puisse accomplir sa mission dans le domaine de compétence qui est le sien. Afin d'assurer que cela est possible malgré les secrets professionnels tant du gynécologue que du médecin-légiste, le paragraphe sous examen propose de préciser que l'article 458 du Code pénal ne s'oppose pas à un échange d'informations à cette fin. Il ne s'agit donc nullement d'une obligation d'échanger des informations mais d'une possibilité, et il appartiendra aux différents médecins et aux médecins-légistes d'apprécier en âme et conscience si un échange d'informations sur la patiente/victime est dans l'intérêt de cette dernière »[167].

Sur le principe, la CNPD estime que l'article 2-1 nouveau de la loi du 7 août 2012 portant création du LNS est de nature à permettre un échange bilatéral de données nécessaires entre professionnels de santé intervenant dans la prise en charge des victimes de violences tout en assurant la confidentialité des données contenues dans la documentation médico-légale des violences.

La Commission nationale souligne que les échanges d'informations doivent être opérés dans certaines limites. Elle note avec satisfaction les précisions du commentaire des articles selon lequel *« il est clair que, lorsqu'un échange d'informations a eu lieu, le secret professionnel auquel est tenu le destinataire des informations s'applique également à ces informations »*[168]. A cet égard, il convient de rappeler que les faits couverts par le secret

[167] *cf.* Commentaire des articles, spéc. p. 7.
[168] *Idem.*

professionnel sont non seulement les faits confiés au médecin, mais également ceux découverts par ce dernier dans l'exercice de la profession[169].

En définitive, la CNPD souligne qu'une certaine vigilance devra être mise en œuvre par les professionnels de santé concernés quant aux informations à partager, quant au but de l'échange et surtout quant aux limites de l'échange.

b) La communication d'informations au Parquet rendue « facultative »

L'article 1er du projet de loi, qui vise à modifier le paragraphe 6 de l'article 23 du code d'instruction criminelle, tend à créer, au profit des médecins contribuant à la constitution de la documentation médico-légale des violences, une dispense d'obligation de dénoncer des faits constitutifs d'infractions au Parquet. Le législateur assure ainsi une certaine effectivité au concept d'unité de documentation médico-légale des violences en laissant la possibilité aux victimes de « *faire documenter leurs blessures sans pour autant mettre en marche nécessairement la machine répressive judicaire* »[170].

Plus précisément l'article 1er du projet de loi entend ajouter à l'article 23 du Code d'instruction criminelle un paragraphe 6 nouveau visant à dispenser, d'une part, les membres du personnel du LNS travaillant dans l'unité de documentation médico-légale des violences d'informer le Procureur d'Etat lorsqu'ils acquièrent la connaissance d'une infraction pénale et, d'autre part, de dispenser également les médecins et autres professionnels de santé consultés dans le cadre de l'unité de documentation médico-légale des violences de la même obligation d'information.

Le paragraphe 6 nouveau précité précise en outre expressément que la dispense d'obligation d'information ne s'applique pas aux faits commis à l'égard de mineurs, compte tenu de la protection particulière dont ces personnes particulièrement vulnérables font habituellement l'objet.

Il ressort du commentaire des articles que, sans être obligés de dénoncer, les professionnels visés au paragraphe 6 nouveau de l'article 23 du Code d'instruction criminelle conservent un « droit de dénoncer » des faits susceptibles d'être qualifiés d' « infraction pénale » dans des circonstances qu'ils jugeraient particulièrement graves.

La Commission nationale note avec satisfaction le rappel souligné par les rédacteurs du projet de loi dans le Commentaire des articles selon lequel le droit susmentionné des professionnels de santé de dénoncer des faits au Parquet s'exerce « *sans préjudice quant à leurs obligations découlant du secret professionnel ou médical en application notamment de l'article 458 du Code pénal* »[171]. Il appartiendra ainsi aux médecins concernés d'apprécier si une communication d'informations au Parquet est ou non dans l'intérêt de la victime.

XX. La sécurité

L'article 2 paragraphe (2) précité du projet de loi dispose que « *l'unité de documentation médico-légale des violences prend en charge la conservation de la documentation réalisée conformément aux dispositions de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.* »

Il en résulte, en application des articles 22 et 23 de la loi modifiée du 2 août 2002, une obligation pour le LNS d'adopter les mesures techniques et organisationnelles nécessaires afin d'assurer la sécurité des données, notamment un système de traçage des accès aux données. Elle estime qu'il conviendrait de rajouter une disposition, à l'instar d'autres lois ou règlements grand-ducaux, qui pourrait avoir la teneur suivante : « *Le système informatique par lequel l'accès au fichier est opéré doit être aménagé de sorte que l'accès aux fichiers soit sécurisé moyennant une authentification*

[169] Dean SPIELMANN et Alphonse SPIELMANN in Droit pénal général luxembourgeois, éd. Bruylant, 2002, p. 210.
[170] *cf.* Commentaire des articles, spéc. p. 5.
[171] *cf.* Commentaire des articles, spéc. p. 5.

forte, que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle. ».

La Commission nationale recommande en outre que des mesures de sécurité à l'état de l'art soient mises en œuvre, afin de garantir la confidentialité des données particulièrement « sensibles » contenues dans le traitement de l'unité de documentation médico-légale des violences.

En dernier lieu, la CNPD note avec satisfaction qu'une gestion stricte des habilitations d'accès aux données est mise en place au sein du LNS, afin de limiter l'accès à la documentation médico-légale des violences aux membres du personnel du LNS strictement habilités et nommément désignés par le chef du département de médecine légale du LNS[172].

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 14octobre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

[172] *cf.* Exposé des motifs du projet de loi, spéc. p. 4.

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7079 portant modification de la loi modifiée du 4 septembre 1990 portant réforme de l'enseignement secondaire technique et de la formation professionnelle continue, d'autres dispositions légales, et au projet de règlement grand-ducal modifiant le règlement grand-ducal modifié du 9 janvier 2009 sur la jeunesse

Délibération n°864/2016 du 28 octobre 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 a notamment pour mission d'aviser *« 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 30 septembre 2016, le Ministère de l'Education nationale, de l'Enfance et de la Jeunesse a invité la Commission nationale à aviser :

I. le projet de loi n°7079 portant modification :

1. de la loi modifiée du 4 septembre 1990 portant réforme de l'enseignement secondaire technique et de la formation professionnelle continue ;

2. de la loi du 13 juillet 2006 portant réorganisation du centre de psychologie et d'orientation scolaire (CPOS) ;

3. de la loi du 16 mars 2007 portant 1. organisation des cours de formation professionnelle au Centre national de formation professionnelle continue 2. création d'une aide à la formation, d'une prime de formation et d'une indemnité de formation ;

4. de la loi modifiée du 4 juillet 2008 sur la jeunesse ;

5. de la loi modifiée du 19 décembre 2008 portant réforme de la formation professionnelle ;

6. de la loi modifiée du 12 mai 2009 portant création d'une école de la 2ème chance ;

7. de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves ;

8. du Code de la Sécurité sociale ;

II. le projet de règlement grand-ducal modifiant le règlement grand-ducal modifié du 9 janvier 2009 sur la jeunesse.

Ces projets de loi et de règlement grand-ducal ont pour objet de séparer l'Action locale pour les Jeunes (« ALJ ») du Service de la formation professionnelle, et de l'intégrer au sein du Service nationale de la jeunesse (« SNJ »), respectivement aux lycées.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'article 7 du projet de loi précité.

Cet article 7 rajoute un point 14 à l'article 6, alinéa 1er, de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves. Cet ajout a plus précisément pour objet d'autoriser le Service national de la jeunesse à recevoir des données à caractère personnel relatives aux élèves du Ministre ayant l'Education nationale dans ses attributions *« aux fins de permettre un accompagnement individuel des jeunes désirant renouer avec l'école ou la formation professionnelle ».*

Il ressort de l'exposé des motifs qu'un tel ajout s'avère nécessaire suite à l'intégration de l'ALJ dans le SNJ. En effet, les auteurs

du projet de loi sous examen précisent qu' *« actuellement, l'ALJ en tant que service du ministre ayant dans ses attributions l'Education nationale, a accès à la banque de données concernant les élèves afin de pouvoir retracer le parcours scolaire d'un jeune qui s'adresse à elle pour un soutien individuel. Cet accès est garanti par la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves ».*

« Or la loi modifiée du 4 juillet 2008 sur la jeunesse place le Service National de la Jeunesse sous l'autorité du ministre ayant dans ses attributions la jeunesse. Actuellement le même ministre a dans ses attributions à la fois la jeunesse et à la fois l'éducation nationale. Si cela n'était plus le cas à l'avenir, l'accès à la banque de données des élèves ne serait plus garanti pour le Service national de la Jeunesse ».

Sur base de ces éléments, la Commission nationale peut admettre que les finalités d'une telle communication de données à caractère personnel relatives aux élèves (à savoir *« de permettre un accompagnement individuel des jeunes désirant renouer avec l'école ou la formation professionnelle »*) corresponde aux nouvelles missions du SNJ, telles que définies à l'article 7, alinéa 1er de la loi modifiée du 4 juillet 2008 sur la jeunesse (modifié par l'article 4, 3° du projet de loi sous objet), et en particulier à sa lettre (c), c'est-à-dire à *« [sa mission] de soutenir la transition des jeunes vers la vie active ».*

Cependant, cet objectif doit être mis en balance avec le droit pour les personnes concernées (c'est-à-dire l'ensemble des élèves) à la protection de leur vie privée. Ce dernier élément constitue un droit fondamental consacré notamment par l'article 11 (3) de la Constitution, par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne ainsi que par l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. Il s'agit donc de vérifier si cette balance des intérêts penche en faveur du droit fondamental au respect de la vie privée, qui protège l'intérêt des citoyens et dans ce cas des élèves, ou en faveur de l'intérêt légitime du SNJ consistant à permettre un accompagnement individuel des jeunes désirant renouer avec l'école ou la formation professionnelle, en tenant compte du critère de nécessité et de proportionnalité.

Selon ce principe de nécessité et de proportionnalité, qui ressort de l'article 4 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002, les données à caractère personnel relatives aux élèves qui seront transmises au SNJ doivent être adéquates, pertinentes et non excessives au regard de la

finalité indiquée dans le projet de loi sous examen.

Un des critères à prendre en compte dans l'analyse du principe de proportionnalité et de nécessité est la proportion du nombre de personnes concernées par la mesure (à savoir les jeunes désirant renouer avec l'école ou la formation professionnelle) par rapport au nombre de personnes non concernées, mais dont les données seraient consultables par le SNJ via une communication des données à caractère personnel relatives aux élèves.

En l'espèce, le nombre de jeunes qui pourraient être pris en charge par le SNJ demeure relativement restreint par rapport à l'ensemble de la population scolaire. En effet, selon l'exposé des motifs du projet de loi sous examen, le public-cible est constitué des décrocheurs potentiels identifiés par les lycées, des décrocheurs identifiés par le ministère, et enfin des jeunes inactifs de longue durée pouvant être qualifiés par l'acronyme « NEET », c'est-à-dire « not in employment, education or training ».

L'article 7 du projet de loi sous objet, dans sa rédaction actuelle, permettrait une communication de données à caractère personnel concernant au contraire une partie très importante de la population, à savoir l'ensemble des élèves (au sens de l'article 1er, point 1 de la loi précitée du 18 mars 2013).

Dès lors, la Commission nationale estime nécessaire, à l'instar d'autres textes légaux pour lesquels son avis a été demandé, que soit prévue la mise en place d'une solution technique permettant de garantir, d'un point de vue informatique, que les agents du SNJ puissent seulement recevoir communication des données concernant les personnes qui font l'objet d'une mesure d'accompagnement individuel, à l'exclusion des données relatives au reste de la population scolaire. En d'autres termes, seule l'ouverture d'un dossier administratif à l'occasion de l'accompagnement d'un jeune en difficulté ouvrirait aussi le droit pour le Ministère ayant l'Education nationale dans ses attributions de communiquer au SNJ des données à caractère personnel concernant ces élèves, et auquel ce dernier n'aurait pas accès en l'absence de dossier.

Ce n'est que sous cette condition que la Commission nationale estime que le principe de proportionnalité et de nécessité serait respecté, et qu'elle ne verrait pas d'objection à ce que le SNJ puisse recevoir communication de données à caractère personnel relatives aux élèves.

Par ailleurs, comme elle l'avait déjà évoqué dans ses avis 238/2010 du 26 juillet 2010[173] et 829/2016 du 14 octobre 2016[174], la Commission nationale estime nécessaire que les catégories de données qui feront l'objet d'une communication (dans ce cas au SNJ) soient énumérées au sein d'un règlement grand-ducal. En effet, en l'absence d'une telle précision concernant les catégories des données qui pourraient être communiquées au SNJ, la Commission nationale n'est pas en mesure d'apprécier la nécessité et proportionnalité de cette transmission de données relatives aux élèves au regard de la finalité consistant à permettre un accompagnement individuel des jeunes désirant renouer avec l'école ou la formation professionnelle.

Or, l'avant-projet de règlement grand-ducal précisant les données accessibles et les données communiquées en exécution des articles 4 et 6 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves, entend déjà préciser les catégories de données visées aux points (1) à (13) de l'article 6 de la loi du 18 mars 2013. La Commission nationale a émis dans son avis 613/2016 du 6 juillet 2016[175] ses remarques à ce sujet. Il serait utile d'intégrer à l'occasion de l'adoption de cet avant-projet de règlement grand-ducal les catégories de données qui pourraient être transmises au SNJ, au regard du futur point (14) de l'article 6 de la loi du 18 mars 2013.

[173] Avis 238/2010 du 26 juillet 2010 de la Commission nationale pour la protection des données concernant l'avant-projet de règlement grand-ducal déterminant les conditions, les critères et les modalités de l'échange de données à caractère personnel entre l'administration de l'éducation nationale et les établissements scolaires, les autorités communales et des tiers.

[174] Avis 829/2016 du 14 octobre 2016 de la Commission nationale pour la protection des données relatif au projet de loi no7064 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse et portant modification de la loi du 18 mars 2013 relative aux traitements des données à caractère personnel concernant les élèves.

[175] Avis 613/2016 du 6 juillet 2016 de la Commission nationale pour la protection des données relatif aux avant-projets de règlements grand-ducaux 1) précisant les données accessibles et les données communiquées en exécution des articles 4 et 6 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves, 2) pris en exécution de l'article 5 de la loi du 18 mars 2013 relative aux traitements de données à caractère personnel concernant les élèves, et 3) fixant le modèle et les modalités de délivrance, d'utilisation et de retrait de la carte d'élève « myCard ».

Enfin, il peut être utile de relever que le projet de loi no7064 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse et portant modification de la loi du 18 mars 2013 relative aux traitements des données à caractère personnel concernant les élèves entend, dans son article 16, ajouter lui aussi un point 14 à l'article 6 de la loi du 18 mars 2013. Il conviendra de prendre ce projet en considération afin d'éviter une numérotation redondante dans cette loi.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 28 octobre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

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[176] et/ou[177] de recours juridictionnels[178].

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 claires. La CNPD partage aussi les soucis du Parquet général[179] et de la Commission consultative des Droits de l'Homme[180] 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.

[176] 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.
[177] 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.
[178] 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.
[179] Avis du 28 avril 2016, page 5.
[180] Avis du 7 juillet 2016, pages 5 et 7.

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

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)[181].

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-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*

[181] 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).

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.

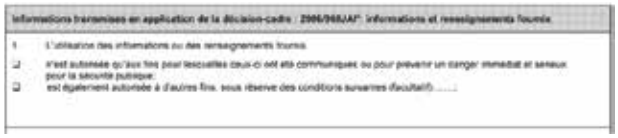
Si la décision - cadre 2006/960/JAI et la décision 2008/615/JAI ne prohibent pas cette utilisation, elles l'encadrent néanmoins (dans les échanges de données entre pays membres de l'Union européenne).

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[182].

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.

[182] Extrait du formulaire « Annexe A » :



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.[183]

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

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

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

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 ingé¬rence 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[184].

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 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[185].

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

[184] En vertu de l'article 5 paragraphe (3) renvoyant à l'article 20 paragraphe (3) et de article 7.
[185] 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).

Annexes

Avis de la Commission nationale pour la protection des données relatif aux projets de loi n°7054 et 7055 (Paquet législatif « Klimabank an nohalteg Wunnen »)

Délibération n°980/2016 du 25 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 » ou « la loi »), 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 en date du 27 octobre 2016, Monsieur le Ministre du Logement a invité la Commission nationale à se prononcer sur plusieurs projets de lois et de règlements grand-ducaux afférents au paquet législatif *« Klimabank an nohalteg Wunnen »*. La CNPD a été saisie plus précisément des projets de textes suivants :

- le projet de loi n°7054 concernant la collecte et la saisie des dossiers d'aides relatives au logement et le projet de règlement grand-ducal y afférent ;
- le projet de loi n°7055 relatif à un régime d'aides à des prêts climatiques et le projet de règlement grand-ducal y afférent ;
- le projet de loi portant introduction d'une certification de la durabilité des logements et modifiant la loi modifiée du 25 février 1979 concernant l'aide au logement, ainsi que le projet de règlement grand-ducal y afférent.

Le paquet législatif *« Klimabank an nohalteg Wunnen »*, dont l'entrée en vigueur est prévue pour le 1er janvier 2017, comprend également les projets de loi et de règlement grand-ducal relatif à un régime d'aides pour la promotion de la durabilité, de l'utilisation rationnelle de l'énergie et des énergies renouvelables dans le domaine du logement (PRIMe House).

La Commission nationale tient à souligner qu'à la demande du ministère du Logement, elle a pu faire part d'un certain nombre d'observations préliminaires durant la phase de réflexion préalable à la rédaction du projet de loi n°7054 susmentionné.

De manière générale, la Commission nationale salue

la démarche des auteurs dudit projet de loi qui ont pris en compte et intégré en amont, durant la phase d'élaboration du projet de loi n°7054, la plupart des recommandations de la CNPD. Elle regrette toutefois que la saisine officielle concernant le paquet « *Klimabank an nohalteg Wunnen* » soit intervenue tardivement[186] et n'ai pas permis que le Conseil d'Etat dispose en temps utile de l'avis de la CNPD, ce que relève d'ailleurs le Conseil d'Etat dans son avis du 15 novembre 2016[187].

La CNPD entend donc limiter ses observations aux dispositions dudit projet de loi appelant des remarques complémentaires à ce stade. Elle estime par ailleurs que les autres projets de textes soumis à son examen n'appellent pas d'observations particulières au regard de la loi modifiée du 2 août 2002.

La CNPD observe que le projet de loi n°7054 vise à encadrer le traitement de données à caractère personnel par les ministères du Logement et de l'Environnement dans le cadre d'un « *guichet unique des aides relatives au logement* » (ci-après « le Guichet Unique »), dont la finalité est de faciliter et de simplifier les démarches des administrés, notamment au stade de l'introduction de leur(s) demande(s) et du suivi administratif de leur(s) dossier(s) de demande d'aides au logement.

L'exposé des motifs du projet de loi précise ainsi qu'« *il suffira à l'administré de s'adresser à un seul bureau pour l'ensemble des aides relatives au logement, à savoir les aides socio-économiques relevant de la compétence du ministre ayant le Logement dans ses attributions, couramment dénommées « aides individuelles au logement, et les aides énergétiques et écologiques relevant de la compétence du ministre ayant l'Environnement dans ses attributions, couramment dénommées « PRIMe House » »*.

La Commission nationale observe avec satisfaction que le système envisagé par les responsables de traitements pour la collecte et la saisie communes des demandes d'aides relatives au logement répond aux conditions de licéité et de légitimité de l'article 4 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Elle note par ailleurs avec satisfaction que le projet de loi précise tant les finalités du traitement (article 1er du projet de loi n°7054), que les catégories de données à caractère personnel traitées (article 2 du projet de loi n°7054), les destinataires habilités à recevoir communication des données et les fichiers externes auxquels les responsables de traitements auront accès pour les besoins de leurs missions respectives (article 4 du projet de loi n°7054), les modalités d'accès et de journalisation des accès aux données (article 5 du projet de loi n°7054).

Tout en indiquant les catégories de données traitées (à savoir les données relatives à l'identification, les données socio-économiques et les données relatives au logement pour lequel une aide est demandée), l'article 2 paragraphe (2) du projet de loi n°7054 renvoie à un règlement grand-ducal le soin de déterminer plus précisément lesdites données. La CNPD s'interroge sur le caractère opportun de cette précision par voie de règlement grand-ducal, alors que les détails suffisants pourraient être apportés directement à l'article 2 du projet de loi sous examen. Elle reconnaît toutefois que la possibilité de procéder par voie de règlement grand-ducal faciliterait d'éventuelles initiatives de faire évoluer la liste des données traitées à moyen terme.

S'agissant de la collecte et de la saisie des données par le ministère du Logement pour le compte du ministère de l'Environnement, la CNPD ne saurait partager l'avis du Conseil d'Etat selon lequel « *il n'est pas nécessaire de régler dans la loi en projet quel ministre effectue la collecte et la saisie des demandes d'aides dans le contexte du guichet unique* »[188]. En effet, en

[186] La CNPD a reçu la demande d'avis officielle concernant le paquet « *Klimabank an nohalteg Wunnen* » le 27 octobre 2016, alors que le Conseil d'Etat en a été saisie le 29 juillet 2016.
[187] *cf.* Conseil d'Etat, Avis n°51.779 du 15 novembre 2016 relatif au projet de loi concernant la collecte et la saisie des dossiers d'aides relatives au logement.
[188] Conseil d'Etat, Avis n°51.779 du 15 novembre 2016 précité, spéc. p. 2.

application de l'article 2 (n) de la loi modifiée du 2 août 2002, *« lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales »*. Les dispositions de l'article 3 précité conservent en réalité tout leur intérêt dans le projet de loi sous examen, en ce qu'elles clarifient la répartition des rôles de responsable du traitement et de sous-traitant entre les deux ministères en cause.

De plus, la Commission nationale rappelle qu'en application de l'article 22 paragraphe (3) de la loi modifiée du 2 août 2002, un tel traitement doit être régi par un contrat ou un acte juridique consigné par écrit et qui prévoit notamment que les agents du ministère du Logement agissent sur la seule instruction du ministère de l'Environnement et que les obligations de sécurité résultant de l'article 22 précité incombent au ministère du Logement. Elle recommande en outre qu'une formation soit dispensée auprès des agents du ministère du Logement affectés au Guichet Unique, afin de les sensibiliser aux principes de protection des données à caractère personnel.

Le Conseil d'Etat précise dans son avis relatif au projet de loi n°7054 qu'au regard de la loi modifiée du 2 août 2002 et en présence d'un consentement des personnes concernées, il n'est plus nécessaire de régler spécifiquement dans la loi l'accès des ministres aux différents fichiers dont la consultation est nécessaire à l'instruction des demandes d'aides au logement[189]. La Commission nationale ne peut pas non plus partager cette analyse, qui par ailleurs, aux yeux de la CNPD, n'est pas en concordance avec la position prise dans d'autres avis antérieurs par le Conseil d'Etat sur la même problématique. Elle se félicite, au contraire, de ce que la liste des fichiers auxquels les responsables de traitement auront accès pour l'exercice de leurs missions a été précisée à l'article 4 du projet de loi, ainsi que les finalités pour lesquelles ces fichiers seront consultés.

En l'absence de consentement de la personne concernée à ce que les ministres compétents vérifient directement dans les fichiers détenus par d'autres administrations les informations nécessaires à l'instruction des demandes d'aides au logement, les personnes concernées disposent en principe d'une alternative consistant à fournir elles-mêmes des pièces justificatives comportant des informations issues desdits fichiers et documentant leur situation administrative. Il en résulte une nécessité d'encadrer, au-delà de l'hypothèse d'un consentement préalable des personnes concernées, les

[189] Conseil d'Etat, Avis n°51.779 du 15 novembre 2016 précité, spéc. p. 3.

cas où les ministres concernés seraient rendus destinataires de données issues de bases de données administratives gérées par d'autres administrations. La CNPD estime essentiel que l'encadrement normatif sur ce point figure dans la loi.

La CNPD estime qu'un tel encadrement législatif irait par ailleurs dans le sens d'autres initiatives législatives récentes[190] à propos desquelles elle s'est prononcée et serait davantage compatible avec la position adoptée par le Conseil d'Etat dans un avis récent relatif à l'aide financière de l'Etat[191] aux termes duquel les principes suivants ont été rappelés :

« (…) l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.
La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication. (…) »

Par ailleurs, la CNPD estime que le règlement grand-ducal du 7 juin 1979 déterminant les actes, documents et fichiers autorisés à utiliser le numéro d'identité des personnes physiques et morales, pris en exécution de l'article 5 de la loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales est devenu caduc pour ce qui est des personnes physiques, par suite de l'entrée en vigueur de la loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité et aux registres communaux des personnes physiques[192]. Dès lors, l'accès des ministres au répertoire général devrait s'effectuer conformément à la procédure prévue par l'article 11 de la loi du 19 juin 2013 précitée. La CNPD tient à souligner que cette observation n'appelle pas à son sens de modification du projet de loi n°7054 sous examen.

S'agissant des droits des personnes, la CNPD rappelle qu'en application de l'article 26 de la loi modifiée du 2 août 2002, l'existence des droits d'accès et de rectification doit être clairement indiquée aux personnes concernées. Elle considère que l'exercice effectif de ces droits devrait être facilité en pratique par l'existence du Guichet Unique auprès duquel les personnes concernées pourront facilement s'adresser.

L'article 5 paragraphe (3) point 3 du projet de loi n°7054 prévoit une journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. A cet égard, la CNPD recommande que la durée de conservation des données de journalisation des accès aux données, précisée à l'article 5 paragraphe (3) point 3 du projet de loi n°7054, soit portée à cinq ans à partir de leur enregistrement (délai de prescription des délits sanctionnés par la loi modifiée du 2 août 2002), délai après lequel elles devraient être effacées, à moins qu'elles ne fassent pas l'objet d'une procédure de contrôle. Par souci de clarté et tenant compte de l'observation qui précède, la CNPD suggère de simplifier la rédaction du paragraphe (3) de l'article 5 précité du projet de loi n°7054 comme suit :

« Le système informatique par lequel l'accès au fichier est opéré doit être aménagé de sorte que l'accès aux fichiers soit sécurisé moyennant une authentification forte, que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle. »

---

[190] A titre d'illustration, voir la loi du 9 décembre 2015 portant introduction d'une subvention de loyer.
[191] Conseil d'Etat, Avis n°6975/5 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.
[192] L'article 45 de la loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité et aux registres communaux des personnes physiques dispose en effet que : *« La loi modifiée du 30 mars 1979 organisant l'identification numérique des personnes physiques et morales ne s'applique plus aux personnes physiques. »*

Le paragraphe (4) de l'article 5 précité du projet de loi renvoie à un règlement grand-ducal le soin de déterminer les modalités de l'accès et les personnes auxquelles l'accès aux fichiers est réservé. La Commission nationale observe que l'article 2 du projet de règlement grand-ducal fixant les mesures d'exécution de la loi concernant la collecte et la saisie des dossiers d'aides relatives au logement apporte peu de précisions à cet égard, cet article se cantonnant à prévoir une gestion stricte des habilitations d'accès aux données. En effet, l'article 2 précité du projet de règlement grand-ducal dispose simplement que seuls les agents des ministères responsables du traitement ou de l'administration placée sous leur autorité, nommément désignés par eux et en fonction de leurs attributions, pourront accéder aux données collectées par le Guichet Unique. La CNPD se demande si cette disposition ne pourrait pas plus simplement être intégrée au premier paragraphe de l'article 5 du projet de loi n°7054.

En dernier lieu, la Commission nationale recommande que des mesures de sécurité à l'état de l'art soient mises en œuvre, afin de garantir la confidentialité des données traitées par l'intermédiaire du Guichet Unique.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 25 novembre 2016.

La Commission nationale pour la protection des données,

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7020 portant mise en œuvre de la réforme fiscale

Délibération n°981/2016 du 25 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 » ou « la loi »), 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 en date du 26 octobre 2016, Monsieur le Ministre des Finances a invité la Commission nationale à se prononcer sur le projet de loi n°7020 du 2016 portant mise en œuvre de la réforme fiscale 2017 (ci-après « le projet de loi »).

Le projet de loi a pour objet de moderniser le système redistributif luxembourgeois en réformant la fiscalité applicable aux personnes physiques et aux personnes morales.

La CNPD entend limiter ses observations aux dispositions dudit projet de loi appelant des observations particulières au regard de la loi modifiée du 2 août 2002. L'attention de la CNPD a été portée plus particulièrement sur le Chapitre 9 (coopération interadministrative et judiciaire), le Chapitre 16 (protection des données inscrites sur le registre national) et le Chapitre 17 (accès à la documentation relative aux actions au porteur) du projet de loi sous examen.

I. La coopération interadministrative et judiciaire et le renforcement des moyens de administrations fiscales

Le chapitre 9 du projet de loi se compose d'un article 10 unique qui entend apporter des modifications aux articles 14 et 16 de la loi du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines et de l'Administration des douanes et accises.

Selon le Commentaire des articles, l'ajout des termes *« à la demande de cette dernière au cas par cas »* à l'article 14 de la loi du 19 décembre 2008 précitée vise à permettre à l'Administration des contributions directes *« d'avoir accès, au même titre que les autres administrations fiscales, de façon directe et illimitée aux données visées, à savoir les informations relatives à la détention des véhicules automoteurs fournies par le ministère des transports en vue notamment d'appliquer correctement le nouvelle article 129d L.IR. ayant pour objet d'introduire l'abattement pour mobilité durable »* (article 10, 1° du projet de loi)[193].

La Commission nationale estime que cet ajout n'appelle pas d'observation particulière de sa part.

L'article 10, 2° du projet de loi entend ensuite modifier l'article 16 du projet de loi à deux égards.

Tout d'abord, l'article 16 de la loi du 19 décembre 2008 précitée serait complété d'un deuxième alinéa libellé comme suit :

« L'Administration des contributions directes et l'Administration de l'enregistrement et des domaines transmettent à la cellule de renseignement financier, à sa demande, les informations susceptibles d'être utiles dans le cadre d'une analyse pour blanchiment ou financement du terrorisme. »

[193] *Cf.* Commentaire des articles, spéc. *Ad article 10, 1°*, p. 64.

Tenant compte de l'extension de l'infraction de blanchiment au droit pénal fiscal par le projet de loi sous examen, l'ajout de ce deuxième alinéa vise à permettre à la cellule de renseignement financier de demander aux administrations fiscales les informations susceptibles de lui être utiles dans l'exercice de sa mission d'analyse d'un cas de blanchiment ou de financement du terrorisme[194].

La Commission nationale estime que cette modification de l'article 16 paragraphe 1er de la loi du 19 décembre 2008 précitée n'appelle pas d'observation particulière de sa part.

Ensuite, le projet de loi prévoit d'insérer un nouveau paragraphe (3) à l'article 16 de la loi du 19 décembre 2008 précitée comme suit :

« (3) Les autorités judiciaires transmettent à l'Administration des contributions directes ainsi qu'à l'Administration de l'enregistrement et des domaines toute information susceptible d'être utile dans le cadre de l'établissement correct et du recouvrement des impôts, droits, taxes et cotisations dont la perception leur est attribuée. »

Sur ce point, la CNPD se rallie à l'avis du Conseil d'Etat[195]. La transmission d'informations des autorités judiciaires vers les autorités administratives présenterait en effet un caractère inédit dans le système juridique luxembourgeois qui ne lui paraît pas compatible avec certains principes issus de la loi modifiée du 2 août 2002.

La Commission nationale rappelle en effet qu'en application de l'article 4 paragraphe (1) lettre (a) de la loi modifiée du 2 août 2002, le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement et notamment que ces données sont collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités.

Or, en l'occurrence, la CNPD estime que le traitement ultérieur à des fins fiscales des données en cause n'apparaît pas a priori compatible avec leur collecte initiale à des fins judiciaires.

Par ailleurs, la CNPD ne peut que soutenir la recommandation formulée par le Conseil d'Etat de modifier la rédaction particulièrement large du projet de paragraphe (3) de l'article 16 précité, afin de rappeler le principe du secret de l'instruction, de limiter la portée de cette nouvelle disposition et d'éviter ainsi que des informations excessives par les instances judiciaires (notamment celles obtenues de manière fortuite à l'occasion d'une enquête judiciaire) ne soient transmises aux administrations fiscales.

---

[194] *cf.* Exposé des motifs, spéc. *Ad article 10, 2°*, p. 64.
[195] Conseil d'Etat, avis n° , spéc. p. 40.

Elle estime en outre que la nouvelle rédaction proposée par le Conseil d'Etat[196] rendrait le projet de loi davantage compatible avec les principes de pertinence et de minimisation des données inscrits à l'article 4 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002.

II. La modification de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques

Le chapitre 16 du projet de loi se compose d'un article 21 unique qui vise à modifier la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques en insérant, entre les termes « *de la sécurité publique,* » et « *de la prévention,* » de l'article 38 de ladite loi, les termes « *de l'établissement ou du recouvrement des taxes, impôts et droits perçus par ou pour le compte de l'Etat,* », dans une perspective de renforcement de l'efficacité du recouvrement de l'impôt.

Ainsi, la nouvelle rédaction de l'article 38 de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques se présenterait comme suit :

« *Art. 38. Toute personne, dont les données font l'objet d'une inscription sur le registre national, a le droit d'obtenir la liste des autorités, administrations, services, institutions ou organismes qui ont, au cours des six mois précédant sa demande, consulté ou mis à jour ses données au registre national ou qui en ont reçu communication, sauf si une consultation ou une communication a été faite par ou à une autorité chargée de la sécurité de l'Etat, de la défense, de la sécurité publique, de l'établissement ou du recouvrement des taxes, impôts et droits perçus par ou pour le compte de l'Etat, de la prévention, de la recherche, de la constatation et de la poursuite d'infractions pénales, y compris de la lutte contre le blanchiment d'argent, ou du déroulement d'autres procédures judiciaires. La procédure prévue à l'article 36 s'applique.* »

Il résulterait de la modification textuelle précitée une extension du champ des dérogations possibles au droit d'accès des personnes afférents aux données les concernant contenues dans le registre national des personnes physiques.

Selon les précisions de l'exposé des motifs et du commentaire des articles du projet de loi[197], cette modification vise en effet à « *parer aux risques d'entraver des procédures et enquêtes administratives et/ou judiciaires tant nationales qu'internationales* » en évitant « *que les contribuables ne soient informés de manière anticipative des recherches entreprises par les administrations fiscales en vue de l'identification des infractions à la loi fiscale ou des moyens déployés et nécessaires au recouvrement (forcé) des impôts au profit de l'Etat.* »

Si la Commission nationale comprend la démarche des auteurs du projet de loi, elle ne peut s'empêcher de souligner que la dérogation au droit d'accès envisagée semble excessive et disproportionnée au regard de la loi modifiée du 2 août 2002. Elle estime que les personnes concernées devraient pouvoir accéder au motif de la consultation de leurs données par les administrations fiscales dans le registre national.

Les possibilités pour un responsable de traitement de limiter ou différer l'exercice du droit d'accès d'une personne concernée sont strictement encadrées par l'article 29 de la loi modifiée du 2 août 2002. Ainsi, en application dudit article 29 paragraphe (1), il peut être dérogé au droit d'accès lorsqu'une telle mesure est nécessaire pour sauvegarder (a) la sûreté de l'Etat, (b) la défense, (c) la sécurité publique, (d) la prévention, la recherche, la constatation et la poursuite d'infractions pénales, y compris celles à la lutte contre le blanchiment, ou le déroulement d'autres procédures judiciaires, (e) un intérêt économique ou financier important de l'Etat ou de l'Union européenne, y

[196] Le Conseil d'Etat propose de formuler le nouveau paragraphe (3) que le projet de loi envisage d'insérer à l'article 16 de la loi du 19 décembre 2008 : « *Sans préjudice de l'article 8 du Code d'instruction criminelle, les autorités judiciaires transmettent à l'Administration des contributions directes ainsi qu'à l'Administration de l'enregistrement et des domaines, à leur demande, les informations susceptibles d'être utiles dans le cadre de l'établissement correct et du recouvrement des impôts, droits, taxes et cotisations dont la perception leur est attribuée.* »

[197] *cf.* Exposé des motifs, spéc. p. 34 et Commentaire des articles, spéc. *Ad article 21*, p. 71.

compris dans les domaines monétaire, budgétaire et fiscal et (f) la protection de la personne concernée ou des droits et libertés d'autrui.

La Commission nationale est d'avis que les cas de dérogation précités sont d'interprétation stricte et qu'aucun d'entre eux n'est applicable dans le contexte du projet de loi sous examen, pas même les (d) et (e) de l'article 29 paragraphe (1) de la loi modifiée du 2 août 2002. En effet, il lui apparaît que le recouvrement de l'impôt ne relève pas stricto sensu du champ de la prévention et de la répression pénale et judiciaire. Elle estime en outre qu'au stade du recouvrement de l'impôt, il apparaît prématuré de considérer que l'intérêt économique ou financier important de l'Etat est en cause.

En toute hypothèse, une dérogation générale au profit de l'ensemble des agents des administrations fiscales, telle qu'elle ressort de l'article 21 du projet de loi apparaît disproportionnée. Si cette dérogation venait à être étendue à d'autres administrations qui mènent aussi des enquêtes administratives, l'article 38 de la loi modifiée du 19 juin 2013 serait vidé de sa substance et perdrait sa raison d'être. La Commission nationale ne peut par ailleurs s'empêcher de souligner que, depuis l'entrée en vigueur de la loi modifiée du 19 juin 2013, elle a malheureusement constaté un nombre important de cas d'abus de consultation des données du registre national.

Dès lors que des faits ayant fait l'objet d'une enquête administrative menée aux fins de recouvrement de l'impôt seraient transmis au parquet, la Commission nationale estime que l'exception judiciaire, déjà prévue à l'article 38 de la loi modifiée du 19 juin 2013 et par ailleurs conforme à l'article 29 paragraphe 1 lettre (d) de la loi modifiée du 2 août 2002, a vocation à s'appliquer.

La CNPD est dès lors d'avis que l'article 21 du projet de loi sous examen devrait être supprimé.

III. L'accès de l'Administration des contributions directes aux documents relatifs aux actions au porteur

Le chapitre 17 du projet de loi se compose d'un article 22 unique qui, selon les précisions de l'exposé des motifs « *vise à vérifier que les sociétés soumises à la loi du 28 juillet 2014 concernant l'immobilisation des actions et parts au porteur se sont conformées à ladite loi. Elle permet en outre un échange d'informations entre l'ACD et la Caisse de consignation visant à assurer que les actions ou parts au porteur non immobilisées dans les délais légaux sont consignées auprès de la Caisse de consignation.* »

La Commission nationale estime que cette disposition du projet de loi n'appelle pas d'observation particulière de sa part.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 25 novembre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Avis de la Commission nationale pour la protection des données à l'égard de l'avant-projet de loi modifiant la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés, et d'autres dispositions légales

Délibération n°983/2016 du 25 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 du 2 modifiée août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser *« 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 ».*

Faisant suite à la demande lui adressée par Monsieur le Ministre du Développement durable et des Infrastructures en date du 17 novembre 2016, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi modifiant :

1) la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés,

2) la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques,

3) la loi modifiée du 23 février 2010 relative à l'application du principe de reconnaissance mutuelle aux sanctions pécuniaires,

4) la loi du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines et de l'Administration des douanes et accises,

5) la loi du 5-15 septembre 1807 relative au Mode de recouvrement des frais de justice au profit du Trésor public, en matière criminelle, correctionnelles et de police.

Cet avant-projet de loi vise entre autres à permettre à l'Administration de l'Enregistrement et des Domaines de procéder au recouvrement de la somme due dans le cadre du système de contrôle et de sanction automatisés sur base d'un titre rendu exécutoire par un officier de police judiciaire, agissant sur délégation du Procureur général d'Etat, tout en lui permettant de procéder à des sommations à tiers détenteur à l'instar de ses attributions déjà exercées en matière de recouvrement fiscal.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'article 11 de l'avant-projet de loi sous examen.

Cet article prévoit l'insertion d'un nouvel article 11*bis* dans la loi du 19 décembre 2008 ayant pour objet la coopération interadministrative et judiciaire et le renforcement des moyens de l'Administration des contributions directes, de l'Administration de l'enregistrement et des domaines et de l'Administration des douanes et accises.

Selon le commentaire de l'article, cette nouvelle disposition *« permettra à l'Administration de l'Enregistrement et des Domaines d'obtenir du Centre Commun de la Sécurité Sociale les informations nécessaires à l'exercice de ses missions d'exécution et de recouvrement »*.

D'après les auteurs de l'avant-projet de loi, cette transmission de données à caractère personnel permettrait à l'Administration de l'Enregistrement et des Domaines de savoir si le contrevenant touche un salaire ou une pension au Luxembourg, afin de pratiquer des sommations à tiers détenteur. Il ressort des termes de l'article 11 de l'avant-projet de loi sous objet que cette transmission restera circonscrite aux seuls nom, prénom, adresse et matricule de l'employeur du débiteur des créances respectives ou de l'organisme débiteur de sa pension ou de sa rente. De plus, la transmission ne pourra avoir lieu que pour la finalité consistant pour l'Administration de l'Enregistrement et des Domaines à procéder au recouvrement des amendes et frais de justice en matière répressive visés à l'article 1er (3) de la loi modifiée du 20 mars 1970 portant réorganisation de l'administration de l'enregistrement et des domaines, des amendes forfaitaires visées à l'article 6, paragraphe 2, de la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés, des sanctions pécuniaires visées à l'article 3 de la loi modifiée du 23 février 2010 relative à l'application du principe de reconnaissance mutuelle aux sanctions pécuniaires, ainsi que de tous autres montants ou avoirs dont le recouvrement, la saisie ou la confiscation sont requis sur base des articles 197,403,668 du Code d'instruction criminelle.

Aux yeux de la CNPD, les données énumérées limitativement dans l'article 11 de l'avant-projet de loi apparaissent nécessaires et proportionnelles au regard de la poursuite de la finalité précitée. Il en aurait été autrement si le montant du salaire ou de la pension des personnes concernées était également transmis à l'Administration de l'Enregistrement et des Domaines,

ce qui aurait dû être considéré comme excessif.

Par ailleurs, le paragraphe (2) du nouvel article 11bis qui serait inséré dans la loi précitée du 19 décembre 2008 prévoit que ce transfert de données *« se fait sous garantie d'un accès sécurisé, limité et contrôlé »*. La Commission nationale comprend par là que les mesures de sécurité techniques et organisationnelles appropriées seront prises à l'occasion de cette transmission de données, que seules les données énumérées au paragraphe (1) seront transmises à l'Administration de l'Enregistrement et des Domaines, et qu'une procédure de traçage des accès sera mise en place afin de pouvoir le cas échéant déceler d'éventuels abus.

Dans ces conditions, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 25 novembre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7022 relative aux abus de marché et portant : 1. mise en œuvre du règlement (UE) n°596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission; 2. transposition de: a) la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché (directive relative aux abus de marché); b) la directive d'exécution (UE) 2015/2392 de la Commission du 17 décembre 2015 relative au règlement (UE) n°596/2014 du Parlement européen et du Conseil en ce qui concerne le signalement aux autorités compétentes des violations potentielles ou réelles dudit règlement; 3. modification de la loi modifiée du 11 janvier 2008 relative aux obligations de transparence des émetteurs; et 4. abrogation de la loi modifiée du 9 mai 2006 relative aux abus de marché

Délibération n°1003/2016 du 2 décembre 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 » ou « la loi »), 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 en date du 7 octobre 2016, Monsieur le Ministre des Finances a invité la Commission nationale à se prononcer sur le projet de loi n°7022 relative aux abus de marché (ci-après « le projet de loi »). La Commission nationale regrette qu'elle n'ait pas été saisie plus tôt dans la procédure législative, alors que le Conseil d'Etat a été saisi pour avis déjà à la date du 2 août 2016.

Le projet de loi a pour objectif d'adapter la législation luxembourgeoise en matière d'abus de marché afin de garantir l'application intégrale et cohérente des nouvelles règles découlant du règlement (UE) n°596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (ci-après « le règlement n°596/2014 » ou « le règlement

européen »), de la directive 2014/57/UE du Parlement européen et du Conseil du 16 avril 2014 relative aux sanctions pénales applicables aux abus de marché et de la directive d'exécution (UE) 2015/2392 de la Commission du 17 décembre 2015 relative au règlement (UE) n°596/2014 du Parlement européen et du Conseil en ce qui concerne le signalement aux autorités compétentes des violations potentielles ou réelles dudit règlement (ci-après « la directive d'exécution 2015/2392 »). Plusieurs des dispositions des mesures touchent au domaine de la protection des données à caractère personnel et la CNPD note que le législateur européen a intégré la législation applicable dans ce domaine dans le paquet législatif, notamment par le biais de l'article 26 du règlement n°596/2014, qui énonce explicitement qu'« *[e]n ce qui concerne le traitement de données à caractère personnel dans le cadre du présent règlement, les autorités compétentes exécutent leurs tâches aux fins du présent règlement conformément aux dispositions législatives, réglementaires et administratives nationales transposant la directive 95/46/CE* ».

Pour sa part, la Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de loi sous examen traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel.

XXI. Quant à la qualité des données traitées par la CSSF et échangées entre la CSSF et le Procureur d'Etat

Le projet de loi fait état d'une coopération entre la Commission de Surveillance du Secteur Financier (ci-après désignée « la CSSF ») et le Procureur d'Etat. La CNPD prend acte de la précision dans le commentaire des articles qu'une disposition similaire figure déjà dans la loi modifiée du 9 mai 2006 relative aux abus de marché (ci-après désignée « la loi modifiée du 9 mai 2006 »)[198].

En effet, conformément à l'article 7 du projet de loi, la CSSF pourrait échanger avec le Procureur d'Etat et le Service de Police Judicaire « *toute information qu'ils jugent utile ou nécessaire* ». L'article détaille ensuite la procédure de coopération entre la CSSF et le Procureur d'Etat dans le cadre de la répression administrative ou pénale des violations ou infractions en matière d'abus de marché. D'après cet article, un dossier d'enquête tenu par le Procureur d'Etat pourrait, sous certaines conditions, être transmis à la CSSF afin que cette dernière puisse poursuivre la procédure.

La Commission nationale rappelle que le traitement de données à caractère personnel par le

[198] Voir le commentaire des articles, p. 25.

Procureur d'Etat tombe dans le champ d'application de l'article 8 de la loi modifiée du 2 août 2002, d'après lequel « *[l]e traitement des données dans le cadre d'enquêtes pénales et de procédures judiciaires est opéré dans le respect des dispositions du Code d'instruction criminelle, du Code de procédure civile, de la loi portant règlement de procédure devant les juridictions administratives ou d'autres lois* ». Il y a lieu de noter que ces Codes-loi ne contiennent pas de dispositions spécifiques relatives à la protection des données et à la vie privée.

Vu la possibilité pour le Procureur d'Etat de transmettre un dossier à la CSSF, la Commission nationale estime nécessaire de préciser si l'article 8 précité continuerait à s'appliquer aux données traitées par la CSSF lors de la poursuite de la procédure, dans la mesure où des données à caractère personnel judiciaires issues de l'enquête du Procureur d'Etat auront été transmises à la CSSF.

La même question se pose dans le cadre des autorisations judiciaires prévues par les paragraphes (4) et (7) de l'article 4 ainsi que par l'article 5 du projet de loi. En effet, les données à caractère personnel traitées par la CSSF, qui est une autorité administrative, lors de sa procédure administrative, tombent dans le champ d'application du régime dit « ordinaire » de la loi modifiée du 2 août 2002, alors que les données à caractère personnel sont à qualifier comme données judiciaires tombant dans le champ d'application de l'article 8 de la loi, du moment que le juge d'instruction émet l'autorisation judiciaire demandée par la CSSF.

Nonobstant ses commentaires relatifs à l'article 4, paragraphe (1), point (7) du projet de loi[199], la Commission nationale estime nécessaire de préciser en détail dans le projet de loi les règles applicables à ces genres d'enquêtes mixtes.

XXII. Quant aux pouvoirs de la CSSF d'exiger la communication des enregistrements téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic

A. Les données traitées par les entités surveillées, les émetteurs, les réviseurs d'entreprises agréés et les cabinets de révision agréés

L'article 4, paragraphe (1), point (6) du projet de loi, qui met en œuvre l'article 23, paragraphe (2), lettre (g) du règlement n°596/2014, confère à la CSSF le pouvoir d'obtenir la communication des enregistrements téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic détenues par les entités soumises à sa surveillance prudentielle, les émetteurs, les réviseurs d'entreprises agréés et les cabinets de révision agréés. Le commentaire des articles précise que la CSSF n'aurait accès qu'aux données existantes et que la disposition n'obligerait de toute façon pas les entités visées d'enregistrer ou de conserver les communications[200]. Il est également expliqué que l'article 29, paragraphe (1) de la loi modifiée du 9 mai 2006 donne actuellement à la CSSF le pouvoir « *d'exiger la communication des enregistrements téléphoniques et des données échangées existants* »[201].

A ce titre, la Commission nationale note qu'à l'époque de l'élaboration de la loi modifiée du 9 mai 2006, le Conseil d'Etat s'était interrogé sur la base légale de cette communication[202]. Par l'adoption du règlement n°596/2014, cette base légale est dès lors en principe créée.

Cependant, alors que le règlement européen oblige les Etats membres de doter l'autorité compétente du pouvoir de « *se faire remettre les enregistrements des conversations téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic détenus par des entreprises d'investissement, des établissements de crédit ou*

[199] Voir le point II.B. du présent avis.
[200] Voir le commentaire des articles, p. 23.
[201] Ibid, p. 22.
[202] « *[L]e Conseil d'Etat se demande tout d'abord quelle est la base légale pour cette communication ? Est-ce la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ? Dans l'affirmative, quelle disposition précise est à appliquer ? Quant à la loi organique de la CSSF (loi du 23 décembre 1998), elle ne fournit probablement pas de base juridique satisfaisante. A supposer que ces deux textes ne fournissent pas de base juridique suffisante, il faudrait, selon le Conseil d'Etat, en créer une dans le cadre du projet sous avis. En effet, la solution alternative consistant à soumettre tout transfert à une procédure d'autorisation ou de notification ne serait guère praticable* ». Avis du Conseil d'Etat du 15 novembre 2005, doc. parl. n°5415/2, p. 7.

des institutions financières »[203], le projet de loi inclut également les émetteurs, les réviseurs d'entreprises agréés et les cabinets de révision agréés dans le champ d'application de cette disposition.

A l'instar de l'avis du 15 novembre 2005 du Conseil d'Etat et vu le fait que les émetteurs, les réviseurs d'entreprises agréés et les cabinets de révision agréés ne figurent pas parmi les entités listées à l'article 23 du règlement européen, la Commission nationale estime que le projet de loi va au-delà du champ d'application défini par le règlement européen en ajoutant ces trois dernières catégories d'organismes.

B. Les données traitées par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics

L'article 4, paragraphe (1), point (7) du projet de loi complèterait, selon le commentaire des articles[204], l'article 4, paragraphe (1), point (6) en prévoyant que la CSSF, sous réserve de l'autorisation judiciaire du juge d'instruction prévue à l'article 5 du projet de loi, pourrait *« exiger la communication des enregistrements de données relatives au trafic détenus par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics lorsqu'il existe des raisons de suspecter une violation et que de tels enregistrements peuvent se révéler utiles à la manifestation de la vérité dans le cadre d'une enquête relative à la violation de l'article 14 ou 15, du règlement (UE) n°596/2014 »*. Cet article met en œuvre l'article 23, paragraphe (2), lettre (h) du règlement n°596/2014, qui dispose qu'*« [a]fin de mener à bien leurs missions au titre du présent règlement, les autorités compétentes sont dotées,* ***conformément au droit national****, au moins des pouvoirs de surveillance et d'enquête suivants : … se faire remettre,* ***dans la mesure où le droit national l'autorise****, les enregistrements existants de données relatives au trafic détenus par un opérateur de télécommunications, lorsqu'il existe des raisons de suspecter une violation et que de tels enregistrements peuvent se révéler pertinents pour l'enquête relative à la violation de l'article 14, point a) ou b), ou de l'article 15 »*.

Or, en l'état actuel du droit luxembourgeois, la CNPD estime que ce pouvoir est prohibé par l'article 5 de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications

[203] Les notions d' « *entreprise d'investissement* » et d' « *établissement de crédit* » sont définies à l'article 4, paragraphe (1), point (2) et (3) du règlement n°596/2014. Une définition du terme « *institution financière* » ne figure pas dans cet article. En revanche, tant l'article 23 de la version allemande que l'article 23 de la version anglaise utilise un terme défini à l'article 4, paragraphe (1), point (4) du règlement, à savoir « Finanzinstitut » et « financial institution ». Sur cette base, la Commission nationale part du postulat que le terme « *établissement financier* », tel que défini à l'article 4, paragraphe (1), point (4) de la version française dudit règlement, devrait figurer à la place d'« institution financière » dans l'article 23, paragraphe (2), lettre (g).

[204] Voir le commentaire des articles, p. 22-23.

électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle (ci-après « la loi modifiée du 30 mai 2005 »).

En premier lieu, bien que le règlement européen ne fournisse pas de définition du terme « opérateur de télécommunication », les auteurs du projet de loi ont opté pour l'inclusion des opérateurs figurant dans la loi modifiée du 30 mai 2005, à savoir les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics.

Ainsi, en ce qui concerne les données relatives au trafic détenues par les entités visées, l'article 3, paragraphe (1), point 27 du règlement n°596/2014 précise que la notion d'« *enregistrements de données relatives au trafic* » doit être interprétée comme étant les enregistrements de données relatives au trafic tels qu'ils sont définis à l'article 2, deuxième alinéa, point b), de la directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[205]. Bien que l'article de la directive, ainsi que l'article 2, lettre (e) de la loi modifiée du 30 mai 2005 qui le transpose, ne définissent pas la notion « d'enregistrements de données relatives au trafic », les « données relatives au trafic » y sont définies comme « *toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation* ».

Le projet de loi ne contient pas de précisions additionnelles quant aux données auxquelles la CSSF aurait accès avec l'autorisation judiciaire, indiquant seulement qu'il s'agit des données « *détenues* » par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics.

Pourtant, en droit luxembourgeois, l'utilisation de ces données n'est possible que dans des conditions très restrictives, notamment à des fins de facturation ou à des fins de recherche, de constatation et de poursuite d'infractions pénales. En vertu du paragraphe (3) de l'article 5 de la loi modifiée du 30 mai 2005, « *les données relatives au trafic qui sont nécessaires en vue d'établir les factures des abonnés et aux fins des paiements d'interconnexion peuvent être traitées* ». Pour ce qui est du traitement à des fins autres que la facturation, le paragraphe 1er de l'article 5 prévoit un régime restrictif qui limite la conservation des données relatives au trafic « *[p]our les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations … ».*

A cet égard, la Commission nationale soulève que le législateur luxembourgeois n'a pas encore précisé quelles données doivent être conservées par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics à des fins de facturation. En revanche, pour ce qui est de la conservation des données relatives au trafic dans le cadre de la répression pénale, le règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics énonce les données qui doivent être conservées.

Il s'avère dès lors que les données qui sont actuellement détenues par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics sont celles qui sont énumérées dans ce règlement grand-ducal et conservées afin de les mettre à disposition aux

[205] Telle que modifiée par la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n°2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs.

autorités judiciaires pour la recherche, la constatation et la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement.

Les auteurs du projet de loi soulignent dans le commentaire de l'article 4, que les données relatives au trafic ont un caractère particulièrement sensible[206]. Un point qu'a également soulevé le Contrôleur européen de la protection des données dans son avis du 10 février 2012 sur le projet de règlement européen dans lequel il avait remarqué que « *[l]es données relatives à l'utilisation de moyens de communications électroniques peuvent contenir un vaste ensemble d'informations personnelles, telles que l'identité des personnes émettant et recevant l'appel, l'heure et la durée de l'appel, le réseau utilisé, la localisation géographique de l'utilisateur en cas de téléphone portable, etc. Certaines données relatives au trafic concernant l'utilisation de l'internet et du courrier électronique (par exemple la liste des sites internet visités) peuvent en outre révéler d'importants détails sur le contenu de la communication. Par ailleurs, le traitement de données relatives au trafic est contraire au secret de la correspondance* »[207].

Compte tenu du caractère sensible des données, l'accès par la CSSF aux données relatives au trafic détenues par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics prévu par le projet de loi constituerait un changement fondamental du régime de l'utilisation des données relatives au trafic.

Ce pouvoir constitue une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données et doit être conforme à l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales. La base légale doit également être suffisamment accessible et prévoir, avec une précision suffisante, dans quelles circonstances et sous quelles conditions la mesure peut être mise en œuvre.

La Commission nationale souligne que le règlement n° 596/2014 a été adopté le 16 avril 2014, soit huit jours après que la Cour de justice de l'Union européenne (ci-après « la CJUE ») ne rende un arrêt dans les affaires jointes C-293/12 et C-594/12 *Digital Rights* Ireland et autres (ci-après « *l'arrêt Digital Rights* ») le 8 avril 2014[208]. Cet arrêt traite précisément de la question de l'accès aux données relatives au trafic détenues par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics. Dans cet arrêt, la CJUE a invalidé la Directive 2006/24/CE du Parlement

[206] Voir le commentaire des articles, p. 23.
[207] Avis du Contrôleur européen de la protection des données du 10 février 2012 sur les propositions de la Commission de règlement du Parlement européen et du Conseil sur les opérations d'initiés et les manipulations de marché, et de directive du Parlement européen et du Conseil relative aux sanctions pénales applicables aux opérations d'initiés et aux manipulations de marché, JO C 177 du 20.6.2012, p. 1–11, paragraphe 24.
[208] Arrêt du 8 avril 2014, *Digital Rights* Ireland et autres, C-293/12 and C-594/12, EU:C:2014:238.

européen et du conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (ci-après « la Directive 2006/24/CE »), en jugeant qu'elle ne respectait pas le principe de proportionnalité et, plus précisément, que la mesure n'était pas limitée à ce qui était strictement nécessaire afin d'atteindre l'objectif légitime de la directive, tel que requis par la Charte des droits fondamentaux de l'Union européenne (ci-après désignée « la Charte »).

Alors que l'annulation de la Directive 2006/24/CE n'entrainait pas la caducité automatique de la législation nationale luxembourgeoise la transposant, à savoir l'article 5 de la loi modifiée du 30 mai 2005, le gouvernement luxembourgeois a pris l'initiative de proposer une modification de la législation nationale afin de la rendre conforme à l'arrêt *Digital Rights*, en déposant le projet de loi n°6763. La Commission nationale a eu l'occasion de se prononcer tant sur la conformité de la législation luxembourgeoise avec l'arrêt Digital Rights avant le dépôt du projet de loi n°6763 que sur le contenu dudit projet de loi dans ses avis du 13 mai 2014[209] et du 19 juin 2015[210].

Sans vouloir reprendre le contenu de ses avis, la Commission nationale relève que la CJUE dans l'affaire Digital Rights critiquait plus particulièrement l'absence d'un « *critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence* »[211].

En ce qui concerne la détermination claire des infractions permettant le recours aux données relatives au trafic, le projet de loi n°6763 prévoit de remplacer la condition actuelle prévue à l'article 5 de la loi modifiée du 30 mai 2005 par le critère que l'infraction pénale doit figurer sur une liste exhaustive d'infractions considérées comme étant suffisamment graves. A cet égard, la CNPD note que les sanctions pénales prévues à l'article 32 de la loi du 9 mai 2006 figurent sur la liste proposée par le projet de loi n°6763, tout comme elles sont par ailleurs implicitement visées par l'article 5 de la loi modifiée du 30 mai 2005 actuellement applicable. N'y figurent pas, les sanctions administratives que peut infliger la CSSF en fonction de l'article 33 de la loi du 9 mai 2006.

En implémentant la nouvelle législation européenne en matière d'abus de marché, le projet de loi sous examen prévoit, comme la loi du 9 mai 2006, tant des sanctions administratives que pourrait infliger la CSSF que des infractions pénales pour les comportements considérés comme étant graves. Sans aborder la question de la problématique du principe non bis in idem, la Commission nationale note que le commentaire des articles précise qu'afin de ne pas violer ce principe, les auteurs du projet de loi ont décidé de « *reprendre le mécanisme prévu par la loi modifiée du 9 mai 2006, mécanisme qui repose sur deux volets, à savoir, d'une part, l'exigence d'un dol spécial pour les infractions pénales et, d'autre part, l'attribution d'une compétence exclusive et alternative soit aux juridictions judiciaires, soit à la CSSF pour sanctionner les abus de marché* » afin de délimiter « *le champ des comportements considérées comme graves et justifiant une répression pénale, par opposition aux manquements administratifs* »[212]. Il s'ensuit donc que les auteurs du projet de loi n'estiment pas qu'une infraction sanctionnée par une « répression administrative » par la CSSF aux termes de l'article 33 de la loi du 9 mai 2006 doit s'entendre comme un

[209] Avis de la Commission nationale pour la protection des données du 13 mai 2014 quant à la conformité de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection des personnes à l'égard du traitement des données dans le secteur des communications électroniques et des articles 67-1, 88-2 et 88-4 du Code d'instruction criminelle avec les exigences posées par l'arrêt du 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 pour la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication (http://www.cnpd.public.lu/fr/decisions-avis/2014/Vorratsdatenspeicherung/214_2014_Deliberation_Ministere-Justice_avis-loi-modifiee-30-mai-2005-arret-CJUE-8-avril-2014-affaires-jointes-C-293-12-et-C-594-12-conservation-donnees.pdf).

[210] Avis de la Commission nationale pour la protection des données du 19 juin 2015 relatif au projet de loi n°6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, doc. parl. n°6763/2.

[211] Arrêt du 8 avril 2014, *Digital Rights Ireland et autres*, C-293/12 and C-594/12, EU:C:2014:238, point 60.

[212] Voir le commentaire des articles, p. 31.

manquement grave. En d'autres mots, les comportements et infractions « graves » relèvent de la compétence des juridictions judiciaires.

Il y a lieu de constater que le projet de loi contourne les sauvegardes et restrictions imposées par la loi, qui sont nécessaires afin de rendre l'utilisation des données relatives au trafic légitime. En effet, pour le cas où les comportements sur lesquels portent l'enquête de la CSSF seraient suffisamment graves, il incomberait au Procureur d'Etat, et non à la CSSF, de poursuivre l'enquête.

En revanche, si les manquements n'étaient pas considérés comme étant suffisamment graves pour justifier l'intervention du Procureur d'Etat, la CSSF pourrait enquêter et pourrait, en vertu de l'article sous examen et à condition d'avoir obtenu l'autorisation judiciaire du juge d'instruction, se faire communiquer les données relatives au trafic détenues par les fournisseurs de services de communications électroniques et les opérateurs de réseaux de communications publics.

Il s'ensuit que les données en question pourraient être accédées dans le cadre de la répression administrative des manquements administratifs, un seuil nettement inférieur aux conditions posées par l'article 5 de la loi modifiée du 30 mai 2005, par l'arrêt Digital Rights et par le projet de loi n°6763, que les autorités judiciaires doivent remplir pour pouvoir se faire communiquer les données.

La CNPD souligne d'ailleurs que la Suède, l'Allemagne et l'Autriche ont, lors de l'annonce de l'adoption du règlement n°596/2014 par le Conseil de l'Union européenne, déclaré qu'ils présumaient que l'accès par les autorités administratives compétentes ne concerne pas les données conservées en vertu de la Directive 2006/24/CE (la directive sur la conservation des données), car « *cela enfreindrait l'exigence prévue par cette directive de ne conserver des données qu'à des fins de recherche, de détection et de poursuite d'infractions graves. Toute extension de l'accès aux données relatives au trafic en dehors de procédures judiciaires créerait un dangereux précédent pour d'autres dossiers de l'UE* »[213].

Il est à noter que la CJUE reprochait également à la directive de ne pas avoir prévu une durée de conservation précise des données, une différenciation dans la durée de conservation en fonction de la catégorie des données conservées ou encore des exceptions pour les personnes dont les communications sont soumises au secret professionnel. Ces critiques se trouvent également applicables dans le cas d'espèce étant donné que de

[213] Conseil de l'Union européenne, Projet de Procès-verbal du 3309e session du Conseil de l'Union européenne (AFFAIRES ÉTRANGÈRES), tenue à Luxembourg les 14 et 15 avril 2014, doc. n°8947/14, p. 8.

telles précisions font défauts dans le projet de loi sous examen.

Au vu de ce qui précède, la CNPD estime que l'article 4, paragraphe (1), point 7 du projet de loi n'est ni compatible avec la jurisprudence européenne, à savoir l'arrêt *Digital Rights*, ni avec le projet de loi n°6763, de sorte qu'elle est d'avis qu'il convient de supprimer cette disposition du projet de loi sous avis.

XXIII. Quant à la tenue de registres des signalements reçus

L'article 8, paragraphe 1er et l'annexe du projet de loi mettent en œuvre l'article 32 du règlement n°596/2014 et transposent la directive d'exécution 2015/2392. Ces dispositions imposent aux autorités de contrôle l'obligation de mettre en place des mécanismes efficaces pour permettre le signalement des violations par des « informateurs », à savoir des mécanismes de « *whistleblowing* », ainsi que les procédures à suivre par la CSSF lors de la réception et le suivi des signalements.

S'il est vrai que les principes de la protection des données à caractère personnel ont été intégrés dans la directive d'exécution 2015/2392 et que l'annexe constitue une transposition fidèle de cette directive, la Commission souhaite néanmoins apporter quelques précisions quant au texte de l'annexe.

A. Les données traitées

Il ressort du 1er paragraphe de la section VII de l'annexe du projet de loi que « *[l]a CSSF tient un registre de tous les signalements de violations reçus conformément au règlement (UE) n°596/2014 et à la présente loi* ».

A cet égard, la CNPD s'interroge sur les données qui figureraient dans cette base de données. S'agit-il seulement des données relatives aux signalements, ou également des données issues des investigations. Est-ce que les informations reçues d'autres autorités seraient également conservées dans cette base de données ?

Conformément à l'article 4, paragraphe (1) de la loi du 2 août 2002, l'utilisation des données traitées doit se limiter aux finalités pour lesquelles elles ont été collectées et les données doivent être adéquates, pertinents et non excessives au regard des finalités pour lesquelles elles ont été collectées. La Commission nationale recommande dès lors de préciser dans le projet de la loi quelles données seront traitées dans ce registre.

B. L'enregistrement des appels effectués par les informateurs

En vertu des sections VI et VII de l'annexe, la CSSF aurait l'option d'enregistrer les appels des informateurs. La CNPD s'interroge sur la mise en œuvre pratique de ces enregistrements, notamment si l'informateur laisserait un message sur un répondeur ou si un des membres du personnel spécialisés entretiendrait une conversation téléphonique avec l'informateur.

La Commission nationale rappelle que l'article 4 de la loi modifiée du 30 mai 2005 énonce le principe de la confidentialité des communications effectuées au moyen d'un réseau de communications public et de services de communications électroniques accessibles au public ainsi que l'interdiction de stocker les communications. Un tel stockage ou enregistrement ne peut se faire qu'avec le consentement de l'utilisateur concerné ou si une des exceptions du paragraphe (3) de l'article 4 s'applique.

Pour le cas où les communications tant des informateurs, que des membres du personnel de la CSSF spécialisés seraient enregistrées, les informateurs pourraient consentir à l'enregistrement de leurs appels. En revanche, pour ce qui est des membres du personnel spécialisés de la CSSF, qui se trouvent dans une situation de subordination par rapport à leur employeur, le consentement ne serait pas considéré comme

étant légitime et est d'ailleurs exclu par l'article L. 261-1 du Code du Travail. Par ailleurs, la CNPD estime qu'aucune des exceptions actuellement prévues au paragraphe (3) de l'article 4 ne pourraient permettre à la CSSF d'enregistrer les communications de ses salariés dans le cadre du présent projet de loi.

Dès lors, si les communications des salariés de la CSSF serait enregistrées, une modification du paragraphe (3) de l'article 4 de la loi modifiée du 30 mai 2005 serait nécessaire afin d'y prévoir une exception supplémentaire.

C. L'anonymat des appelants

Il ressort du texte de l'annexe que les informateurs auraient la possibilité de faire des signalements de manière anonyme. A ce sujet, la Commission nationale se rallie cependant à l'avis n°1/2006 du Groupe de travail « Article 29 » relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière[214], qui estime qu'il ne convient pas d'encourager les signalement anonymes, mais au contraire de promouvoir l'identification des informateurs. En effet, l'identification de l'informateur permet de limiter les risques engendrés par des signalements anonymes, comme p.ex. les dénonciations calomnieuses.

D. L'information et les droits des personnes

A l'instar de l'avis n°1/2006 du Groupe de travail « Article 29 » précité[215], la CNPD rappelle que non seulement les droits des personnes effectuant des signalements doivent être garantis, mais également ceux des personnes faisant l'objet d'un signalement, le cas échéant.

(i). Le droit à l'information

L'article 26 de la loi modifiée du 2 août 2002 donne à chaque personne concernée le droit d'obtenir certaines informations relatives au traitement mis en œuvre par le responsable du traitement.

En fonction de la section IV de l'annexe, la CSSF fournit les informations contenues dans les sections IV et V de l'annexe par le biais de son site Internet. De plus, il est prévu dans la section VI que l'informateur reçoit les informations contenues dans les sections IV et V « *avant réception du signalement de violation, ou au plus tard au moment de la réception* »[216].

Comme soulevé par le Groupe de travail « Article 29 » dans son avis n°1/2006, les personnes concernées ont le droit d'obtenir les informations énoncées à

[214] Groupe de travail « Article 29 », Avis n°1/2006 du 1er février 2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière (WP 117), p. 11.
[215] Ibid, p. 14-15.
[216] Voir la section VI, para. (4) de l'annexe.

l'article 26, paragraphe (2) de la loi modifiée du 2 août 2002 lorsque leurs données personnelles sont collectées auprès d'un tiers et non directement auprès d'elles[217]. Cette disposition s'applique lorsqu'un informateur effectue un signalement concernant une tierce personne et fournit des données à caractère personnel relatives à cette dernière. La personne faisant l'objet d'un signalement devrait dès lors être informée dans les plus brefs délais après l'enregistrement des données la concernant. Vu les exceptions établies à l'article 27 de la loi modifiée du 2 août 2002, la CNPD se rallie à la recommandation du Groupe de travail « Article 29 », selon laquelle cette notification peut être retardée s'il existe un risque sérieux qui compromettrait la capacité de l'organisme, dans le cas d'espèce la CSSF, d'enquêter efficacement sur les faits allégués[218].

En ce qui concerne les informations fournies aux personnes concernées par le biais du site Internet de la CSSF, le projet de loi indique dans les sections IV et V de l'annexe que seraient fournies notamment des informations relatives aux procédures applicables aux signalements, aux règles de confidentialité applicables aux signalements ainsi que les procédures de protection des salariés.

Or, l'article 26 précité de la loi précise que la personne concernée a le droit d'obtenir des informations relatives au responsable du traitement, les finalités du traitement, les destinataires auxquels les données sont susceptibles d'être communiquées, le fait de savoir si la réponse aux questions est obligatoire et les conséquences d'un défaut de réponse, ainsi que l'existence d'un droit d'accès. Il ne résulte pas clairement du projet de loi que ces informations seraient fournies à l'informateur et à la personne faisant l'objet d'un signalement.

A cet égard, la Commission nationale renvoie à l'arrêt « *Smaranda Bara* » de la CJUE du 1er octobre 2015[219], selon lequel « *les articles 10, 11 et 13 de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, doivent être interprétés en ce sens qu'ils s'opposent à des mesures nationales, telles que celles en cause au principal, qui permettent à une administration publique d'un État membre de transmettre des données personnelles à une autre administration publique et leur traitement subséquent, sans que les personnes concernées n'aient été informées de cette transmission ou de ce traitement* ». La Commission nationale souligne dès lors l'importance d'assurer que les personnes concernées, tant les informateurs que les personnes faisant l'objet d'un signalement, obtiennent toutes les informations requises en vertu de l'article 26 de la loi du 2 août 2002.

Sous réserve des observations sous le point III.B. du présent avis et en considération du fait que la CSSF pourrait enregistrer les communications avec les personnes effectuant des signalements, la CNPD souligne que l'information doit être suffisamment claire pour permettre à la personne concernée de savoir si les communications sur la ligne téléphonique sur laquelle elle appelle sont enregistrées, à l'instar de l'article 4 de la loi modifiée du 30 mai 2005.

(ii). Le droit d'accès

A défaut de précisions dans le projet de loi, la Commission rappelle que chaque personne concernée dispose d'un droit d'accès aux données la concernant, tel que défini à l'article 28 de la loi modifiée du 2 août 2002. Sous réserve des dérogations admises au titre de l'article 29 de la loi, les personnes concernées pourraient exercer leur droit d'accès auprès de la CSSF pendant la procédure administrative dans les conditions établies par l'article 28 de la loi.

En ce qui concerne les données traitées par le Procureur d'Etat et

[217] Groupe de travail « Article 29 », Avis n°1/2006 du 1er février 2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière (WP 117), p. 14.
[218] Ibid.
[219] Arrêt du 1er octobre 2015, Smaranda Bara et autres, C 201/14, EU:C:2015:638, point 46.

le Service de Police Judiciaire, la Commission nationale réitère ses remarques ci-dessus selon lesquelles de tels traitements tomberaient dans le champ d'application de l'article 8 de la loi modifiée du 2 août 2002 et que l'article 28 ne s'appliquerait pas à ces données.

Afin de permettre aux personnes concernées de savoir quelle disposition s'applique au traitement de leurs données, il conviendrait de préciser quel régime est applicable aux données échangées entre la CSSF, le Procureur d'Etat et, le cas échéant, le juge d'instruction[220], échanges mélangeant des données administratives avec des données judiciaires.

E. La sécurité des données

La section IX (« Procédures de protection des données à caractère personnel ») de l'annexe entend transposer l'article 9 de la directive d'exécution 2015/2392 et dispose que « *(1) La CSSF conserve les registres visés à la section VII au sein d'un système sécurisé et confidentiel. (2) L'accès au système visé au paragraphe 1er est soumis à des restrictions afin de garantir que les données qui y sont conservées soient uniquement accessibles aux membres du personnel de la CSSF qui ont besoin de ces données dans l'exercice de leurs fonctions.* »

En application des articles 22 et 23 de la loi modifiée du 2 août 2002, la CSSF est obligée d'adopter les mesures techniques et organisationnelles nécessaires afin d'assurer la sécurité des données, notamment par un système de traçage des accès aux données. La Commission nationale estime dès lors qu'il conviendrait de modifier l'article afin de l'aligner sur les dispositions contenues dans d'autres lois ou règlements grand-ducaux, et qu'il pourrait avoir la teneur suivante : « *Le système informatique par lequel l'accès au registre est opéré doit être aménagé de sorte que l'accès aux fichiers soit sécurisé moyennant une authentification forte, que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle.*»

F. La durée de conservation des données

En application de l'article 4, paragraphe (1), lettre (d) de la loi modifiée du 2 août 2002, les données à caractère personnel

[220] Voir ci-avant point I du présent avis.

traitées par la CSSF devraient en principe être conservées, sous une forme permettant l'identification des personnes concernées, pendant une période n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles les données ont été collectées.

A ce titre, l'article 28 du règlement n°596/2014 prévoit que « *les données à caractère personnel doivent être conservées pendant une durée maximale de cinq ans* ».

A défaut de précision ultérieure dans le règlement n°596/2014, la Commission nationale recommande de spécifier que la date de départ serait la date de la réception du signalement. Dans l'hypothèse d'une constatation par la CSSF d'une violation de la loi, les données pourraient toutefois être conservées au-delà du délai susmentionné dans le cadre de la procédure administrative ou de la transmission des données aux autorités judiciaires compétentes.

XXIV. Quant aux destinataires

Le cadre législatif sous examen impose à la CSSF une obligation de coopération avec d'autres autorités, notamment le Procureur d'Etat et le Service de Police Judiciaire, l'Inspection du Travail et des Mines, ainsi que les autorités compétentes d'autres Etats membres et des pays tiers.

Pour ce qui est de la transmission de données à caractère personnel au sein et en dehors de la CSSF, la section X de l'annexe prévoit que « *[l]a CSSF dispose de procédures adéquates pour la transmission, en son sein et à des tiers, des données à caractère personnel de l'informateur et de la personne faisant l'objet d'un signalement.* ». Or, comme l'a déjà soulevé le Conseil d'Etat à plusieurs reprises « *…l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, est une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.*

La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication. En cas d'accès direct et, le cas échéant, d'interconnexion, la loi doit encore préciser que le système informatique par lequel l'accès est opéré doit être aménagé de sorte que l'accès est sécurisé moyennant une authentification forte (…) »[221].

La Commission nationale estime dès lors que la disposition en question devrait être précisée afin d'assurer que les modalités de transmission soient prévues et que les données à caractère personnel soient protégées pendant toute les étapes du traitement.

A. Le Procureur d'Etat et le Service de Police Judiciaire

En ce qui concerne la coopération entre la CSSF, le Procureur d'Etat et le Service de Police Judiciaire, la CNPD réitère ses commentaires faits au point I du présent avis concernant l'incertitude du régime applicable aux données échangées entre la CSSF et le Procureur d'Etat et y ajoute que la transmission de données entre tous les intervenants doit être ménagée de façon à assurer pendant toutes les étapes du traitement la confidentialité et la sécurité des données.

B. l'Inspection du Travail et des Mines

En application de la section VIII de l'annexe, une coopération entre la CSSF et l'ITM est prévue afin de protéger les salariées qui signalent des violations du règlement n°596/2014. Il ressort de ces dispositions, que la CSSF et l'ITM « *se dotent de procédures communes précisant l'échange d'informations et la coopération visés…* ».

Or, s'agissant d'une matière dont l'essentiel du cadrage normatif doit figurer dans la loi[222], les modalités d'accès et

[221] Avis du Conseil d'Etat du 7 juin 2016 concernant le projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures, doc. parl. n°6975/5, p. 4. Voir aussi l'avis du Conseil d'Etat du 9 décembre 2014 à l'égard du projet de loi 6588 portant organisation du secteur des services de taxis et modification du code de la consommation, doc. parl. n°6588/8, p. 7.
[222] Voir le point IV du présent avis.

de transmission de données à caractère personnel devraient figurer dans la loi.

Dès lors, la Commission nationale estime nécessaire d'adapter le texte du projet de loi sous examen afin d'y prévoir les modalités et conditions précises des transmissions et échanges de données entre la CSSF et l'ITM.

C. Les destinataires dans les autres Etats membres de l'Union européenne et dans les pays tiers

Les articles 25 et 26 du règlement n°596/2014 obligent, sous certaines conditions, la CSSF de coopérer avec les autorités compétentes d'autres Etats membres, avec l'Autorité européenne des marchés financiers ainsi qu'avec des autorités de surveillance des pays tiers. Pour ce faire, les articles 10 et 11 du projet de loi établissent les conditions de l'échange d'informations entre la CSSF et les autres autorités.

Les transferts des données à caractère personnel éventuels pouvant avoir lieu dans le cadre de cette coopération sont entourés de garanties, non seulement en vertu du règlement n°596/2014[223], mais également en vertu de la directive d'exécution 2015/2392 et du projet de loi. La Commission nationale se limite dès lors à formuler quelques observations ponctuelles.

La CNPD constate que le projet de loi prévoit la possibilité pour la CSSF d'utiliser les données qui lui sont transmises tant par des autorités compétentes d'autres Etats membres que par des autorités de surveillance des pays tiers à des fins autres que « *l'exercice de ses fonctions telles que définies dans la présente loi et dans le cadre de procédures administratives ou judiciaires spécifiquement liées à cet exercice* » ou de les transmettre à une autorité compétente étrangère, si l'autorité communiquant les données y a consenti[224]. La Commission nationale rappelle que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités[225]. La CSSF doit dès lors s'assurer du respect de ce principe lors de chaque traitement effectué, y compris lors d'une éventuelle transmission de données à des autorités compétentes européennes, à l'Autorité européenne des marchés financiers ou à des autorités de surveillance des pays tiers.

En vertu de l'article 25, paragraphe (1), alinéa (4) du règlement n°596/2014, la CSSF pourra transmettre « *des informations spécifiques liées aux enquêtes ou aux procédures pénales engagées concernant d'éventuelles violations du présent règlement* » à d'autres autorités

[223] Notamment les articles 27-29.
[224] Voir les articles 10, paragraphe (3) et 11, paragraphe (4) du projet de loi.
[225] Voir l'article 4, paragraphe (1), lettre (a) de la loi modifiée du 2 août 2002 et l'article 5, paragraphe (1), lettre (b) du règlement (UE) n°2016/640.

compétentes des Etats membres et à l'Autorité européenne des marchés financiers « *afin de satisfaire à leur obligation de coopérer entre elles et avec l'AEMF aux fins du présent règlement* ». Pour le cas où un tel échange nécessiterait un traitement de données judiciaires, la Commission nationale rappelle que ceci doit se faire dans le respect de l'article 8 de la loi modifiée du 2 août 2002.

XXV. Quant à la publication des décisions de la CSSF

Selon l'article 34 du règlement n°596/2014, la CSSF publie sur son site Internet « *toute décision infligeant une sanction administrative ou toute autre mesure administrative pour cause de violation du présent règlement sur leur site internet immédiatement après que la personne faisant l'objet de cette décision a été informée de cette décision* ». Aux termes du règlement européen, la publication doit mentionner, au minimum, le type et la nature de la violation et l'identité de la personne faisant l'objet de la décision.

L'article 14 du projet de loi met cette disposition en œuvre en précisant que les décisions publiées par la CSSF figureront sur son site Internet pendant une durée de cinq ans et que les données à caractère personnel figurant dans les décisions ne seront maintenues sur son site que pendant une période maximale de 12 mois.

Comme l'a soulevé le Contrôleur européen de la protection des données dans son avis du 10 février 2012 cité ci-haut[226], une telle publication constitue une ingérence dans la vie privée et les droits fondamentaux de la personne faisant objet de la décision. Elle doit dès lors, même en se conformant au règlement n°596/2014, être limitée à ce qui est strictement nécessaire.

Ainsi, la CNPD souhaite préciser que, par l'indication de l'identité de la personne faisant l'objet de la décision, elle comprend que sont visés exclusivement le nom et le prénom de la personne concernée et estime qu'aucune autre donnée à caractère personnel ne devrait figurer dans la décision publiée sur le site de la CSSF.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 2 décembre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Avis de la Commission nationale pour la protection des données relatif au projet de loi n°7061 modifiant certaines dispositions du Code de la sécurité sociale

Délibération n°1005/2016 du 2 décembre 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 » ou « la loi »), 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 en date du 24 octobre 2016, Monsieur le Ministre de la Sécurité Sociale a invité la Commission nationale à se prononcer sur le projet de loi n°7061 modifiant certaines dispositions du Code de la sécurité sociale (ci-après « le projet de loi »).

Le projet de loi a pour objectif principal « *d'opérer le redressement d'oublis et des changements purement*

[226] Contrôleur européen de la protection des données, op. cit. section 2.6.

techniques en adaptant les différents livres du Code de la sécurité sociale aux modifications législatives intervenues »[227] (exposé des motifs).

La Commission nationale entend limiter ses observations aux dispositions du projet de loi ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel, en particulier aux adaptations apportées par le projet de loi à l'article 60ter du Code de la sécurité sociale concernant les missions et les moyens de l'Agence nationale des informations partagées dans le domaine de la santé (ci-après désignée « l'Agence eSanté »).

La CNPD regrette, à l'instar de la Chambre des fonctionnaires et employés publics[228], que le projet de loi sous examen n'ait pas été accompagné des projets de règlements grands-ducaux y afférents, ce qui aurait mis la Commission nationale en mesure d'apprécier plus concrètement les mesures d'exécution des dispositions législatives en projet et d'éviter ainsi d'éventuelles lacunes législatives.

I. Le recours par l'Agence eSanté aux services, informations et registres permettant l'identification des patients et des prestataires de soins

La Commission nationale observe que l'article 60*ter* en vigueur du Code de la sécurité sociale[229] comporte une certaine ambiguïté quant à la possibilité pour l'Agence eSanté d'accéder à certaines données détenues par le Centre commun de la sécurité sociale (CCSS) et de la Caisse nationale de santé (CNS), afin d'identifier de manière fiable et pérenne les patients et les prestataires de soins du système de santé luxembourgeois.

La Commission nationale estime que seule une interprétation souple et extensive de l'article 60*ter* (2) du Code de la sécurité sociale en vigueur permet, à l'heure actuelle, de considérer que l'Agence eSanté peut accéder aux informations détenues par le CCSS et la CNS concernant les personnes assurées et les prestataires de soins et permettant leur identification.

De plus, la CNPD estime que la banque de données de la sécurité sociale, dont le CCSS est gestionnaire, a été conçue pour répondre aux besoins spécifiques des « *institutions et administrations énumérées à l'article 413 du Code de la sécurité sociale* », au titre desquelles l'Agence eSanté n'est pas expressément mentionnée.

Aux termes d'une interprétation stricte de l'article 60*ter* paragraphe (2) alinéa 2 du CSS, la Commission nationale est d'avis que l'accès de l'Agence eSanté aux données du CCSS doit être considéré comme

[227] *cf.* Exposé des motifs, spéc. 1.
[228] Avis de la Chambre des fonctionnaires et employés publics concernant le projet de loi n°7061 modifiant certaines dispositions du Code de la sécurité sociale, 11 octobre 2016.
[229] L'article 60*ter* paragraphe (2) alinéa 2 du Code de la sécurité sociale dispose que « *L'Agence peut recourir aux services du Centre commun de la sécurité sociale pour la gestion des droits d'accès des personnes assurées et des prestataires de soins* ».

limité à la finalité de gestion des droits d'accès des assurés sociaux et des prestataires de soins expressément visée par ledit article 60ter paragraphe (2) alinéa 2. L'utilisation des données du CCSS à des fins autres que la finalité précitée constituerait, aux yeux de la CNPD, un traitement de données ultérieur dont la compatibilité avec la collecte initiale des données du CCSS reste à démontrer.

Dès lors, la Commission nationale accueille favorablement la démarche des auteurs du projet de loi tendant à clarifier, *« sur demande de l'Agence eSanté »*, la base légale au titre de laquelle l'Agence eSanté entend accéder à certains services et informations gérés par le CCSS et par la CNS. Elle considère en effet que seule une adaptation législative est de nature à lever les ambiguïtés et les limites résultant de la rédaction actuelle de l'article 60*ter* du Code de la sécurité sociale.

Elle note ainsi que l'article 1, 3° lettre a) du projet de loi entend modifier l'article 60*ter* paragraphe 2 alinéa 2 du Code de la sécurité sociale, afin de permettre à l'Agence eSanté de recourir, dans le cadre de ses missions légales, *« aux services et à certaines informations à préciser par règlement grand-ducal du Centre commun de la sécurité sociale et de la Caisse nationale de santé ainsi qu'aux registres professionnels des personnes exerçant légalement une profession réglementée du domaine de la santé tenus par le ministre ayant la Santé dans ses attributions. »*.

Le commentaire des articles fait état de plusieurs missions résultant de la loi du 17 décembre 2010 portant réforme du système de soins de santé, au titre desquelles l'Agence eSanté doit pouvoir solliciter, en tant que de besoin, les services ou informations du Centre commun de la sécurité sociale et de la Caisse nationale de santé, en particulier la contribution de l'Agence eSanté à l'interopérabilité des systèmes d'information de santé, d'une part, et la mise en place de la sécurité et dela communication entre systèmes d'information des différents acteurs du secteur de la santé et des soins, d'autre part. Le commentaire des articles précise en outre le type de services visés : *« en fonction des projets en cours et de ceux à développer encore, les services peuvent par exemple consister dans un support administratif, opérationnel, technique, informatique ou logistique »*[230]. La Commission nationale en prend acte.

En revanche, elle observe que le projet de loi reste peu explicite quant aux informations dont l'Agence eSanté a besoin pour l'exercice de ses missions, en dépit des précisions du commentaire des articles, selon lesquelles : *« dans le cadre de certains projets ou services comme par exemple le récent déploiement du dispositif du médecin référent en relation avec le dossier de soins partagé ou le futur développement de systèmes d'ePrescription et d'e-Facturation, l'Agence doit aussi pouvoir recourir à certaines informations de la part de la Caisse nationale de santé et du Centre commun de la sécurité sociale. »* Les auteurs du projet de loi ajoutent en effet dans le commentaire des articles que *« Comme les informations nécessitées dans le cadre de ces projets ne sont actuellement pas connues et que les projets évoluent, il est prévu de les préciser par règlement grand-ducal »* [231] La CNPD restera donc particulièrement attentive aux futurs développements à cet égard.

Par ailleurs, alors que le texte en vigueur précise la finalité pour laquelle l'Agence eSanté est habilitée à recourir aux services du Centre commun de la sécurité sociale, à savoir la *« gestion des droits d'accès des personnes assurées et des prestataires de soins »*, la Commission nationale note que cette précision est appelé à disparaître avec le projet de loi en projet pour donner place à une rédaction plus large habilitant l'Agence eSanté à recourir aux services d'autres institutions sans précision quant aux finalités poursuivies.

[230] *cf.* Commentaire des articles spéc. p. 8.
[231] *cf.* Commentaire des articles spéc. p. 8.

Si la Commission nationale peut tout à fait comprendre le souci de prévoir une rédaction suffisamment large pour englober l'ensemble des activités en cours de l'Agence eSanté, elle ne peut s'abstenir de relever que le recours à une rédaction moins explicite que le texte en vigueur quant aux finalités poursuivies pourrait soulever, à nouveau, des interrogations sur la compatibilité de traitements ultérieurs des données issues du CCSS ou de la CNS par l'Agence eSanté dans le cadre de futurs projets.

En outre, la CNPD est à se demander si l'absence de précisions quant aux finalités poursuivies dans le cadre de l'accès aux données des fichiers du CCSS et de la CNS est compatible avec les principes dégagés par la Cour constitutionnelle et la position constante du Conseil d'Etat[232] concernant l'encadrement normatif devant résulter de la loi. En effet, l'arrêt du 11 mars 2016 de la Cour constitutionnelle retient que *« d'après l'article 32, paragraphe 3, de la Constitution, tel que résultant de la loi du 19 novembre 2004, dans les matières réservées par la loi fondamentale à la loi, l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements et arrêtés pris par le Grand-Duc. »*[233].

Par ailleurs, le Conseil d'Etat rappelle régulièrement que :

« (…) l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication. (…) »[234].

II. La mise en place d'un système d'identitovigilance et d'annuaires référentiels d'identification des patients et des prestataires

L'article 1er, 3° lettre b) du projet de loi prévoit de compléter le paragraphe 2 de l'article 60*ter* du Code de la sécurité sociale de trois nouveaux alinéas, afin de conférer une base légale à certains outils développés par l'Agence eSanté dans le cadre de la mise en œuvre de la plateforme et des services eSanté. Les trois nouveaux alinéas du paragraphe 2 de l'article 60*ter* du Code de la sécurité sociale tel que modifié par le projet de loi sont libellés comme suit :

[232] *cf.* Conseil d'Etat, Avis n°51.599 du 21 juin 2016 sur le projet de loi sur la nationalité luxembourgeoise ; Avis n°51.091 du 1er décembre 2015 sur le projet de loi concernant la modernisation du droit des faillites ; Avis n°50.724 du 15 juillet 2016 sur le projet de loi concernant le contrôle des exportations ; Avis n°50.250 du 9 décembre 2014 sur le projet de loi concernant les taxis ; Avis n°51.586 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.

[233] *cf.* Cour constitutionnelle, Arrêt n°121/16 du 11 mars 2016.

[234] *cf.* Conseil d'Etat, Avis n°51.586 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.

« Afin d'assurer la sécurité de la plateforme et la qualité des informations traitées dans le cadre de ses missions, l'Agence met en place un système de surveillance et de gestion des risques et erreurs liés à l'identification des personnes ainsi que des annuaires référentiels d'identification des patients et des prestataires.

L'annuaire référentiel d'identification des patients comprend les données d'identification, les caractéristiques personnelles et la situation de famille du patient ainsi que les données d'identification des représentants légaux des mineurs d'âge non émancipés et des personnes majeures protégées par la loi. L'annuaire référentiel d'identification des prestataires de soins comprend les données d'identification, les données en relation avec la profession et l'emploi du prestataire.

Le règlement grand-ducal visé à l'article 60quater, paragraphe 6 précise les modalités de gestion de l'identification et les catégories de données contenues dans les annuaires référentiels d'identification ».

Il ressort des dispositions qui précèdent une volonté des auteurs du projet de loi de conférer une base légale au dispositif d'identitovigilance développé par l'Agence eSanté, d'une part, et aux annuaires référentiels d'identification des patients et des prestataires de soins, d'autre part.

La Commission nationale ne peut que souscrire aux objectifs de sécurité et de qualité de l'information qui sous-tendent la mise en place de ces outils et que l'Agence eSanté doit nécessairement garantir en sa qualité de responsable de traitement[235]. Elle se demande toutefois si le libellé de « caractéristiques personnelles » mentionné au sein des trois nouveaux alinéas précités au titre des données appelées à figurer dans l'annuaire référentiel d'identification des patients n'est pas trop vague. Elle relève en outre que les auteurs du projet de loi renvoient au règlement grand-ducal visé à l'article 60quater, paragraphe 6 du Code de la sécurité sociale le soin de préciser les catégories de données appelées à figurer dans les annuaires référentiels d'identification, ainsi que les modalités de gestion de l'identification seront précisées dans le règlement grand-ducal visé à l'article 60 quater du Code de la sécurité sociale. La Commission nationale observe à cet égard que le règlement grand-ducal visé à l'article 60quater, paragraphe 6 du Code de la sécurité sociale, en cours d'élaboration, est destiné à encadrer spécifiquement les modalités d'établissement et la forme des informations et des documents à verser au « Dossier de soins partagé ». Elle s'interroge dès lors sur la pertinence de recourir à ce projet de texte pour encadrer des outils et services eSanté dont le champ ne se limite pas au seul DSP (ePrescription, eFacturation…). La CNPD propose ainsi de modifier la rédaction du dernier des trois nouveaux alinéas du paragraphe 2 de l'article 60ter du Code de la sécurité sociale comme suit :

« Les modalités de gestion de l'identification et les catégories de données contenues dans les annuaires référentiels d'identification sont précisées par voie de règlement grand-ducal ».

En définitive, la Commission nationale accueille favorablement l'effort des auteurs du projet de loi visant à clarifier le cadre légal et réglementaire applicable à certains traitements de données de l'Agence eSanté. Compte tenu de la sensibilité des données traitées par l'intermédiaire de la plateforme et des services eSanté, il lui importe en effet que les services eSanté se développent dans un environnement juridique sûr et dans la plus grande transparence vis-à-vis des patients et des prestataires de soins.

Elle regrette toutefois que les auteurs du projet de loi n'aient pas saisi l'opportunité du projet de loi sous examen pour clarifier les missions de l'Agence eSanté, s'agissant plus particulièrement du cadre applicable à l'offre

[235] Le commentaire des articles précise, s'agissant de l'article 1er, 3° du projet de loi qu' *« En sa qualité de responsable du traitement de données à caractère personnel au sens de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, l'Agence doit par ailleurs garantir la qualité des informations traitées et un niveau de sécurité élevé dans toutes ses missions tendant à faciliter l'échange et une meilleure utilisation des données relatives à la santé »*, p. 9.

d'un service de pseudonymisation en qualité de tiers de confiance. La CNPD tient à souligner qu'un encadrement général de l'activité de tiers de confiance fournissant ce type de services serait préférable et permettrait d'accompagner le développement de services innovants en matière de pseudonymisation et d'anonymisation au Luxembourg. Elle considère en outre que de tels services devraient être réservés à des acteurs présentant des garanties d'indépendance, de compétence et ne se trouvant pas en situation de conflit d'intérêts au regard des données qu'ils traitent dans le cadre de leurs diverses activités. Pour autant, dans l'attente d'un encadrement général de l'activité de tiers de confiance et compte tenu des fortes attentes en la matière dans le secteur de la santé, la Commission nationale estime qu'une précision textuelle, prenant la forme d'un alinéa supplémentaire à l'article 60ter paragraphe (1), 1) du Code de la sécurité sociale aurait permis d'apporter une meilleure sécurité juridique au service de pseudonymisation développé par l'Agence eSanté, dont la mise en œuvre à vocation à accompagner des projets nationaux importants du point de vue de la santé publique.

III. Le remplacement des termes « données nominatives » par les termes « données à caractère personnel »

Le projet de loi prévoit de remplacer les termes « *données nominatives* » par les termes « *données à caractère personnel* » au sein de plusieurs articles du Code de la sécurité sociale : l'article 165 figurant au sein du Livre II « Assurance Accident » du Code de la sécurité sociale (art. 2 du projet de loi), d'une part, et l'article 426 alinéa 3 et l'article 427 alinéa 2 figurant au sein du Livre IV « Dispositions communes » du Code de la sécurité sociale (art. 4 du projet de loi), d'autre part.

La Commission nationale ne peut qu'accueillir favorablement cette harmonisation de la terminologie du Code de la sécurité sociale avec celle de la loi modifiée du 2 août 2002, qui a abrogé la loi modifiée du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 2 décembre 2016.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Avis de la Commission nationale pour la protection des données à l'égard du projet de règlement grand-ducal concernant les subsides accordés aux clubs sportifs affiliés auprès d'une fédération sportive agréée

Délibération n°1027/2016 du 22 décembre 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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après : « la CNPD ») a notamment pour mission d'aviser « *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* ».

Faisant suite à la demande lui adressée par Monsieur le Ministre des Sports en date du 5 octobre 2016, la CNPD entend présenter ci-après ses réflexions et commentaires au sujet du projet de règlement grand-ducal concernant les subsides accordés aux clubs sportifs affiliés auprès d'une fédération sportive agréée (ci-après : « le projet de règlement grand-ducal »).

La CNPD limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement aux articles 8 et 10 du projet de règlement grand-ducal.

Suivant l'exposé des motifs, le projet de règlement grand-ducal vise à introduire une aide financière pour les clubs sportifs affiliés auprès d'une fédération agréée se composant de deux parties :

1. un subside de base pour lequel le projet de règlement grand-ducal reprend les critères fixés jusqu'à cette date par un règlement interne du Conseil supérieur des sports ;

2. un subside complémentaire visant à combler la suppression par la loi du 24 avril 2016 portant modification de la loi modifiée du 4 juillet 2008 sur la jeunesse de l'aide financière accordée dans le contexte des activités sportives par les chèques-services accueil.

De manière générale, la CNPD salue que la plupart des principes essentiels issus de la loi modifiée du 2 août 2002 aient été intégrés au projet de règlement grand-ducal. Certains points suscitent cependant quelques remarques, développés ci-après.

1. Les données traitées

L'article 8 du projet de règlement grand-ducal instaure le droit pour le Ministre de « *demander toute pièce supplémentaire nécessaire au contrôle des données introduites par le club ou de faire vérifier les données en question directement auprès d'une fédération concernée ou d'autres instances compétentes […]* ».

La Commission nationale ne met pas en doute cette prérogative, mais considère cependant que les simples références à « *toute pièce supplémentaire* » et à « *d'autres instances compétentes* » sont trop vagues. En effet, cette terminologie ne permet pas de savoir quelles données peuvent effectivement être demandées par le Ministre et à quelles instances spécifiques.

La CNPD estime dès lors que ces dispositions ne respectent pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal et ne peuvent pas être considérées comme conformes à l'article 4 de la loi modifiée du 2 août 2002. Elle estime dès lors nécessaire de préciser quelles données peuvent être demandées par le Ministre des Sports et à quelles instances.

En ce qui concerne les données à figurer dans le fichier relatif aux demandes de subsides énumérées à l'article 10, elles apparaissent nécessaires et non excessives. Le catalogue des données est clairement circonscrit.

Pour ce qui est du terme « matricule » visé au paragraphe (2), lettre (a) de l'article 10, ainsi que celui de « numéro d'identification » au même paragraphe, lettre (i), la CNPD suggère de remplacer le mot « matricule » par « numéro d'identification » par référence à la loi du 19 juin 2013 relative à l'identification des personnes physiques.

2. L'accès aux données

Le paragraphe (6) de l'article 10 prévoit que *« toute personne, qui à quelque titre que ce soit, participe à la gestion ou à la tenue de la banque de données est tenu de respecter son caractère confidentiel. »* Néanmoins, la CNPD recommande aux auteurs du projet de règlement grand-ducal de préciser davantage qui aura accès aux données présentes dans le fichier, ainsi que les modalités d'accès aux données contenues dans le fichier relatif aux demandes de subsides.

En particulier, il est important que seules les personnes qui en ont besoin dans l'exercice de leur fonction et de leurs tâches professionnelles soient habilitées à y avoir accès.

3. La sécurité

La CNPD estime nécessaire de prévoir un système de traçage des accès, ce qui constitue une garantie en matière de protection des données à caractère personnel des personnes concernées dans le cadre des articles 22 et 23 de la loi modifiée du 2 août 2002. Ainsi, à l'instar d'autres lois ou règlements grand-ducaux, il conviendrait de rajouter une disposition qui pourrait avoir la teneur suivante :

« Le système informatique par lequel l'accès au fichier est opéré doit être aménagé de la manière suivante :

- *L'accès au fichier est sécurisé moyennant une authentification forte ;*

- *Les informations relatives aux personnes ayant procédées à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation peuvent être retracés ;*

- *Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle ».*

4. Détermination du responsable du traitement

Alors qu'il ressort implicitement de l'article 10 du projet de règlement grand-ducal, ainsi

que du commentaire relatif audit article, que le Ministre des Sports est à considérer comme responsable du traitement, la CNPD propose de le préciser dans le corps du texte et suggère le libellé suivant : « *Le ministre*[236] *a la qualité de responsable du traitement au sens de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Il désigne les agents qui sont en charge, sous son autorité, des opérations relatives à la gestion et à la tenue du fichier relatif aux demandes de subsides.* »

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 22 décembre 2016.

La Commission nationale pour la protection des données,

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Avis de la Commission nationale pour la protection des données à l'égard du projet de règlement grand-ducal concernant le contrôle médico-sportif obligatoire des membres licenciés actifs des fédérations sportives agréées.

Délibération n°1028/2016 du 22 décembre 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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données (ci-après : « la Commission nationale ou « *la CNPD* ») *a notamment pour mission d'aviser « 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 en date du 12 octobre 2016, Monsieur le Ministre des Sports a invité la Commission nationale à se prononcer sur le projet de règlement grand-ducal concernant le contrôle médico-sportif obligatoire des membres licenciés actifs des fédérations sportives agréées (ci-après : « le projet de règlement grand-ducal »).

La CNPD limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'article 17 du projet de règlement grand-ducal créant un registre électronique des personnes ayant passé un contrôle médico sportif (ci-après : « le registre électronique »).

Suivant l'exposé des motifs, le projet de règlement grand-ducal vise à réduire les coûts de fonctionnement du service médico-sportif par une simplification administrative et par des recettes à recevoir.

De manière générale, la CNPD salue que la plupart des principes essentiels issus de la loi modifiée du 2 août 2002 aient été intégrés au projet de règlement grand-ducal. Certains points suscitent cependant quelques remarques, développés ci-après.

I. Les données traitées

Les données à figurer dans le registre électronique apparaissent nécessaires et non excessives. Le catalogue des données est clairement circonscrit. Par ailleurs, il est précisé dans le commentaire de l'article 17 que les données contenues dans le registre électronique ne sont pas « *de données médicales proprement dites mais ne reflètent que l'identité de la personne examinée ainsi que le résultat de l'examen tel qu'il est*

[236] Le projet de règlement grand-ducal définit la notion de « ministre » dans son article 2.

communiqué également aux fédérations et clubs concernés. »

En ce qui concerne le terme « numéro de sécurité sociale luxembourgeois », la CNPD suggère aux auteurs du projet de règlement grand-ducal de le remplacer par « numéro d'identification des personnes physiques » par référence à la loi du 19 juin 2013 relative à l'identification des personnes physiques.

II. L'origine des données et les finalités poursuivies

– Suivant l'article 9 du projet de règlement grand-ducal, l'attestation du sportif examiné par le centre médico-sportif est communiquée aux clubs et fédérations sportives concernées. La Commission nationale se demande si cette attestation sera aussi transmise via le registre électronique crée à l'article 17 ou, le cas échéant, par la voie postale ? Elle recommande dès lors de préciser à l'article 9 par quel moyen les attestations sont communiquées.

Par ailleurs, la CNPD s'interroge quant à la portée de la phrase suivante : *« Les données à caractère personnel sont reprises directement du répertoire nationale des personnes physiques pour chaque consultation et ne sont pas conservées ».*

Selon l'article 7, alinéa 2 de la loi du 19 juin 2013 relative à l'identification des personnes physiques, le ministre ayant le Centre des technologies de l'information de l'Etat dans ses attributions accorde, le cas échéant, l'accès au registre national après avoir demandé l'avis de la Commission du registre national. Le règlement grand-ducal du 28 novembre 2013 fixant les modalités d'application de la loi du 19 juin 2013 relative à l'identification des personnes physiques précise en son article 5, alinéa 2, que le ministre du ressort qui souhaite accéder au registre national doit introduire une demande motivée sur base de laquelle le ministre ayant le Centre des technologies de l'information de l'Etat dans ses attributions détermine *« par type de mission les données et fonctionnalités accessibles par accès directe ou par interfaçage d'applications informatiques. »*

Suivant l'article 5, alinéa 3 du règlement grand-ducal précité, il revient au chef d'administration d'accorder les accès individuels de ses agents dans les limites des accès accordés par type de mission, ainsi que de notifier ces accès au Centre des technologies de l'information de l'Etat.

La Commission nationale souhaite relever par ailleurs que, même si le ministre des sports a reçu ou recevra l'autorisation d'accéder au registre national, le fait que les données personnelles sont

reprises dudit registre « *pour chaque consultation et ne sont pas conservées* » prête à confusion. La CNPD ne comprend pas très bien l'utilité de créer le registre électronique si les données personnelles des sportifs, telles leurs noms, dates de naissance et adresses ne sont pas conservées dans ledit registre. Enfin, l'échéance ou le résultat du contrôle médical ne sont certainement pas reprises du registre national des personnes physiques ?

– Conformément à l'article 4, paragraphe (1), lettre (a) de la loi modifiée du 2 août 2002, les données traitées par un responsable du traitement doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités*».

La Commission nationale comprend qu'il est dans l'intention des auteurs du texte de créer un registre électronique à des fins de gestion administrative des examens obligatoires du contrôle médico-sportif. En effet, il ressort de l'exposé des motifs que la consultation du registre électronique est « *essentielle pour garantir le respect rigoureux des rythmes d'examens obligatoires et constitue une simplification administrative aussi bien pour les personnes elles-mêmes que pour les fédérations et se traduit par un soulagement du central téléphonique du service médico-sportif du ministère des sports.* »

La CNPD suggère d'insérer les finalités poursuivies par les auteurs du projet de règlement grand-ducal dans le corps du texte.

III. L'accès aux données et leur durée de conservation

L'article 17 du projet de règlement grand-ducal prévoit que les données en cause peuvent être communiquées, soit par accès direct, soit par voie informatique aux destinataires suivants :

1. les différents centres médico-sportifs ;
2. les personnes concernées ;
3. les fédérations pour les seules personnes y affiliées.

Tout d'abord, la Commission nationale constate que selon la dernière phrase de l'article 9 du projet de règlement grand-ducal, le sportif examiné n'est informé par décision du médecin chef de service du service médico sportif que s'il a été déclaré inapte, mais ledit article ne précise pas si le sportif est aussi informé d'un résultat positif. Ainsi, la CNPD se demande si les personnes concernées auront aussi un accès direct au registre électronique, et de ce fait à leurs résultats négatifs ou positifs, ainsi qu'aux autres données les concernant et figurant dans le fichier.

Par ailleurs, la CNPD recommande aux auteurs du projet de règlement grand-ducal de préciser davantage qui aura accès au sein des centres médico-sportifs et des fédérations aux données présentes dans le registre électronique. En particulier, il est important que seules les personnes qui en ont besoin dans l'exercice de leur fonction et de leurs tâches professionnelles soient habilitées à y avoir accès.

De plus, l'article 17 ne définit pas explicitement la personne qui est chargée d'octroyer ou de retirer l'accès aux données du registre électronique. La CNPD suggère dès lors de compléter cet article en précisant justement la personne ou le service qui est en charge d'octroyer et de retirer les accès au registre électronique.

Concernant la durée de conservation des données personnelles, l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002 impose au responsable de traitement de veiller à ce que les données qu'il traite ne soient pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

En l'espèce, la CNPD note que le projet de règlement grand-ducal prévoit que les données

sont conservées jusqu'à ce que le titulaire de la licence ait atteint l'âge de 50 ans. Pour justifier cette durée, les auteurs du texte se basent sur l'article 4 du projet de règlement grand-ducal relatif à la périodicité des examens obligatoires où le dernier est fixé à l'année calendrier au cours de laquelle le sportif atteint ses 50 ans.

Néanmoins, la Commission nationale est d'avis que les termes *« jusqu'à l'âge de 50 ans du titulaire d'une licence »* sont susceptibles de porter à confusion. En effet, il ne ressort pas clairement de la disposition si les données sont conservées d'office jusqu'à l'âge de 50 ans d'un sportif qui s'est une fois soumis à un examen médico-sportif, même s'il a arrêté par après d'exercer une activité sportive par exemple à l'âge de 20 ans, ou si ce ne sont que les données des sportifs qui sont actuellement encore membres d'une fédération qui sont conservées jusqu'à l'âge de 50 ans. Qu'en est-il des données des sportifs qui sont titulaires d'une licence et qui ont dépassé leur 50ième anniversaire ?

Ainsi, pour de raisons de clarté et de sécurité juridique, la Commission nationale propose de préciser en ce sens l'article 17 du projet de règlement grand-ducal en y insérant une phrase selon laquelle les donnes personnelles seront conservées aussi longtemps que le sportif est un membre licencié actif auprès d'une des fédérations sportives agréées. Dès qu'une personne n'est plus membre d'une fédération sportive, ses données devraient en principe être supprimées ou éventuellement être anonymisées à des fins statistiques.

IV. La sécurité

La CNPD félicite les auteurs du projet de loi d'avoir prévu des mesures de sécurisation de l'accès aux données, ainsi qu'une procédure de traçage des accès, ce qui permet d'éviter tout risque d'abus ou de détournement de finalité. Ces mesures participent au souci de confidentialité et répondent à l'obligation pour le responsable du traitement de garantir la sécurité des données au sens des articles 21 à 23 de la loi du 2 août 2002.

De plus, il ressort de l'exposé des motifs que la connexion au registre électronique se fait exclusivement par l'intermédiaire d'une carte Luxtrust, c'est-à-dire par une authentification forte.

Néanmoins, la Commission nationale suggère de préciser davantage le système de traçage des accès à l'instar d'autres lois ou règlements grand-ducaux et de rajouter une disposition qui pourrait avoir la teneur suivante:

« Le système informatique par lequel l'accès au registre électronique est opéré doit être

aménagé de la manière suivante :

- *L'accès au registre est sécurisé moyennant une authentification forte ;*

- *Les informations relatives aux personnes ayant procédées à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation peuvent être retracés ;*
- *Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle ».*

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 22 décembre 2016.

La Commission nationale pour la protection des données,

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Avis de la Commission nationale pour la protection des données à l'égard de l'avant-projet de loi relatif au revenu d'inclusion sociale

Délibération n°1029/2016 du 22 décembre 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 « la loi modifiée du 2 août 2002 »), la Commission nationale pour la protection des données a notamment pour mission d'aviser *« 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 6 juillet 2016, Madame la Ministre de la Famille et de l'Intégration a sollicité la CNPD d'aviser l'avant-projet de loi relatif au revenu d'inclusion sociale. La CNPD limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par les articles 25, 26, 40 et 49 de l'avant-projet de loi sous examen.

Suite aux discussions et échanges avec les représentants du Ministère de la Famille, une version actualisée du projet de loi, comprenant un exposé des motifs et un commentaire des articles, a été transmise à la CNPD. Le présent avis se base donc sur la version actualisée du texte du 16 novembre 2016.

1. Détermination du responsable du traitement et l'articulation entre l'article 25 et l'article 40

1.1. Article 25

Selon les dispositions de l'article 25 de l'avant-projet de loi, le ministre ayant la lutte contre la pauvreté dans ses attributions tient le registre des demandeurs et bénéficiaires du revenu d'inclusion sociale (ci-après « Revis »). Alors que l'article 25 introduit le principe de la création dudit fichier, il ne résulte cependant pas clairement du texte qui en est le responsable du traitement.

En effet, le premier paragraphe de l'article 25 fait référence à l'Office national d'inclusion sociale (qui fait partie intégrante des services placés sous l'autorité du ministre ayant la lutte contre la pauvreté dans ses attributions, ci-après « l'ONIS), alors que le paragraphe (4) fait également référence au « Fonds[237] » ainsi qu'à l'Agence pour le développement de l'emploi (ci-après l'ADEM). Par ailleurs, le paragraphe 3 précise que des *« agents régionaux »* auront également accès au fichier. Il ne ressort cependant pas clairement des dispositions précitées quel est

[237] Le Fonds national de solidarité (« le Fonds »), tel que défini à l'article 3, lettre (f) de l'avant-projet de loi.

le rôle concret de chacune de ces parties.

En matière de protection des données, le concept de responsable du traitement constitue une notion-clé pour tout traitement de données à caractère personnel. En effet, le responsable du traitement ne détermine pas uniquement les finalités et les moyens des traitements effectués, mais il répond également de toutes les obligations lui imposées par la loi comme par exemple l'obligation de mise en place des mesures de sécurité et d'organisation appropriées pour garantir la confidentialité et la sécurité des données, l'obligation d'information des personnes concernées, etc.

A la lecture de l'avant-projet de loi et suivant l'économie de l'article 25, la Commission nationale comprend, qu'il est dans l'intention des auteurs du texte d'attribuer la responsabilité du traitement au ministre ayant la lutte contre la pauvreté dans ses attributions. Par ailleurs, elle comprend que certains agents affectés au service de l'Office national d'inclusion sociale se verront attribuer, par le responsable pré-mentionné, la charge d'effectuer les opérations relatives à la gestion et à la tenue du fichier du Revis. La CNPD suggère dès lors de préciser cela dans le corps du texte et propose le libellé suivant : « *Le ministre ayant la lutte contre la pauvreté dans ses attributions a la qualité de responsable du traitement au sens de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Il désigne les agents qui sont en charge, sous son autorité, des opérations relatives à la gestion età la tenue du fichier du Revis* ».

1.2. Article 40

L'article 40 crée, sous l'autorité du ministre précité, un fichier commun entre le Fonds, l'ONIS et l'ADEM qui ne semble pas se différencier sensiblement du fichier crée dans le cadre de l'article 25. Faut-il comprendre que deux fichiers poursuivant des finalités similaires seraient créés ? N'y aurait-il pas double emploi ? A première vue, l'article 40, en employant les termes de « *fichier commun* » semble traduire la volonté d'instaurer une responsabilité conjointe entre les trois acteurs. Ou, est-ce qu'au contraire, il était l'intention des auteurs du texte de rendre le Fonds seul responsable du traitement ? Cette intention semble notamment ressortir du texte de l'exposé des motifs. En effet, l'un des objectifs principaux de l'avant-projet de loi est la simplification administrative et l'exposé des motifs précise que le Fonds « *…devient le seul organisme compétent en matière d'instruction, d'octroi et de gestion des demandes et de paiement du Revis*[238] *…* ». Une

[238] Exposé des motifs, p. 10.

telle solution serait tout à fait envisageable, quitte à instaurer un système d'accès, de partage ou d'échange des données entre les trois administrations.

Au vu de ce qui précède, il est nécessaire de préciser davantage le texte de l'avant-projet de loi, de manière à clarifier le rôle de chaque intervenant dans le processus d'octroi et de gestion du Revis.

Ainsi, à moins qu'on opte pour un système de responsabilité conjointe entre les trois acteurs, on pourrait imaginer un système avec une répartition des rôles suivants : le Fonds serait le responsable du traitement du fichier ; l'ONIS et l'ADEM seraient des fournisseurs de données et seraient amenés à partager/échanger des données avec le premier et devraient à ce titre pouvoir accéder au fichier.

2. Finalités du traitement de données à caractère personnel et catégories de données collectées et traitées

2.1. Article 25

Selon l'article 25, le fichier de l'Office est créé pour la finalité *« d'exécuter les missions de l'Office prévues à l'article 12 paragraphe 2 »* qui se résument comme suit : (i) *« assurer l'exécution des dispositions prévues au chapitre 3 »*, (ii) *« coordonner à cet effet l'action et l'apport des instances et organismes concernés »* et (iii) *« recueillir les données statistiques nécessaires relatives au Revis accordé aux bénéficiaires »*.

Nonobstant la référence explicite aux missions assumées par l'ONIS, la CNPD estime que l'article 25 ne fournit pas d'indications précises sur les finalités poursuivies par le responsable du traitement en ce qui concerne le fichier créé et est donc très vague. En effet, une simple référence aux missions légales attribuées à un responsable du traitement ne correspond pas nécessairement à une finalité ou des finalités précise(s) d'un traitement de données.

L'article 25, paragraphe (4), alinéa 2 qui précise que *« les données à caractère personnel demandées doivent avoir un lien direct avec la finalité ayant motivé la requête »* ne font que rajouter à l'imprécision et l'incertitude.

Conformément à l'article 4, paragraphe (1), lettre (a) de la loi modifiée du 2 août 2002, les données traitées par un responsable du traitement doivent être *« collectées pour des finalités* ***déterminées, explicites*** *et légitimes, et ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités*[239]*»*.

L'obligation de déterminer et de préciser les finalités d'un traitement de données constitue la pierre angulaire en matière de protection des données à caractère personnel et a notamment été précisée dans le cadre des travaux du groupe de travail de l'article 29, dans son avis WP 203[240]. Il ressort notamment de ce document que les données doivent être collectées pour certains buts (ou finalités) et que ces finalités constituent la raison d'être des opérations de traitement.

Ainsi, par *« finalité déterminée »* on comprend une finalité qui est définie de manière suffisamment précise, de manière à délimiter le champ ou l'étendue de l'opération de traitement de données et à permettre la mise en œuvre des mesures de protection suffisantes par rapport à ce traitement de données. Ceci présuppose que le responsable du traitement considère pour quelle finalité(s) les données seront utilisées et traitées. Le corollaire logique de cette obligation est que le responsable ne doit traiter que des données adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées

Pour pouvoir considérer une finalité comme *« explicite »*, il faut que la finalité poursuivie soit exprimée clairement et non pas de manière ambiguë, vague ou générale. La *« finalité explicite »* contribue dès lors au principe de transparence et de prévisibilité

[239] Article 4, paragraphe (1), lettre (a) de la loi modifiée du 2 août 2002.
[240] Article 29 Working party – Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013.

et permet notamment une identification précise des limites d'utilisation des données par les responsables du traitement.

Au vu de ce qui précède, la Commission nationale estime nécessaire de préciser de manière plus claire à l'article 25 les finalités poursuivies par le fichier.

En ce qui concerne les données traitées dans le cadre du fichier créée par l'article 25, le paragraphe (2) se limite à énoncer, dans 14 tirets, que le registre comprend « *des éléments de l'avis de l'Agence pour le développement de l'emploi* », « *des éléments de la déclaration de collaboration* », « *des indications relatives aux dispenses* », « *des déclarations de l'Office* », etc. Ces formulations sont très vagues et ne contiennent même pas des catégories de données. Aux yeux de la CNPD, ces dispositions ne respectent donc pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal.

A ce titre, la Commission nationale se réfère à l'arrêt de la Cour constitutionnelle du 29 novembre 2013, selon lequel « *l'essentiel du cadrage normatif doit résulter de la loi, y compris les fins, les conditions et les modalités suivant lesquelles des éléments moins essentiels peuvent être réglés par des règlements* »[241].

Au vu de ce qui précède, la Commission nationale recommande de restructurer l'article 25 (en y intégrant, le cas échéant l'article 40) en précisant :

- le ou les responsable(s) du traitement,
- les finalités claires et précises du traitement,
- une énumération exhaustive des catégories de données concernées, avec indication de leur origine (données provenant de la personne concernée elle-même, données provenant d'autres fichiers administratifs), sinon dans un projet de règlement grand-ducal.

L'article 9 du projet de règlement grand-ducal, transmis ensemble avec l'avant-projet de loi sous avis, reste tout aussi imprécis et vague, alors qu'il se limite à reprendre exactement les mêmes données que celles utilisées à l'article 25 de l'avant-projet de loi.

2.2. Article 40

L'article 40 quant à lui contient des finalités plus précises et énumère également les données traitées dans le cadre dudit fichier. Si l'article 40 devait être intégré dans l'article 25, la CNPD renvoit à ses observations ci-dessous.

[241] Cour constitutionnelle, arrêt 108/13 du 29 novembre 2013 (Mém. A n°217 du 13 décembre 2013, p. 3886).

3. Opérations de traitement envisagées et nécessité d'identifier concrètement les fichiers visés par les accès

3.1. Article 25

Le paragraphe 4 de l'article 25 fait état de plusieurs fichiers auxquels l'Office peut accéder dans le cadre de ses missions, à savoir le fichier relatif au Revis géré par le Fonds national de solidarité, le registre national des personnes physiques, le fichier relatif aux bénéficiaires du Revis géré par l'Agence pour le développement de l'emploi et le fichier relatif aux affiliations géré par le Centre commun de la sécurité sociale.

Alors que les fichiers repris sous les numéros (b) et (d) sont bien identifiables car réglementés en détail dans des textes légaux spécifiques, l'indication relative aux fichiers du Revis gérés par le Fonds ou l'ADEM est imprécise et ne permet pas de savoir quels fichiers sont concrètement visés. Par ailleurs, le paragraphe 4 sous analyse ne mentionne, pour aucun des quatre fichiers pré-mentionnés, à quelles données de ces fichiers l'Office peut avoir concrètement accès.

En l'absence de précision quant aux données qui seront accédées ou transmises la CNPD n'est pas en mesure d'apprécier si les données accédées et traitées correspondent aux exigences de l'article 4, paragraphe (1), lettre (a) de la loi modifiée du 2 août 2002, c'est-à-dire si elles sont *« adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées… »*.

Le terme « interconnexion » au sens de la loi modifiée du 2 août 2002 vise l'hypothèse de deux ou plusieurs responsables du traitement qui mettent en corrélation des fichiers. Or, le texte de l'avant-projet de loi sous-entend que les différentes administrations prévues au paragraphe (4) communiquent (en sens unique) des données à l'Office, mais que ce dernier ne communique pas à son tour de données aux autres administrations, c'est-à-dire qu'elles n'ont pas accès aux données du fichier de l'Office. Ainsi, la CNPD propose de remplacer le libellé *« l'Office peut accéder par la voie d'interconnexions aux données »* par le libellé *« l'Office peut recevoir communication des données »*.

3.2. Article 40

Contrairement à l'article 25, l'article 40 ne fournit aucune précision sur l'origine des données. Ainsi, on peut se poser la question si les données traitées dans le cadre de l'article 40 proviennent du Fonds, de l'ONIS et de l'ADEM, voire de la personne concernée elle-même ou est-ce qu'à l'instar de l'article 25, des accès à d'autres fichiers étatiques sont nécessaires afin d'alimenter le fichier ?

4. Durée de conservation des données

L'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002 impose au responsable de traitement de veiller à ce que les données qu'il traite ne soient pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées. Or, le projet de loi sous avis ne contient aucune disposition relative à la durée de conservation des données.

La CNPD estime donc nécessaire de préciser le texte du projet de loi en ce sens.

5. Traçage des données

La Commission nationale salue les dispositions de l'article 25, paragraphe (4), alinéa 3 qui prévoit un traçage des accès aux données, mais propose néanmoins une légère modification du texte. Ainsi, la mention suivante serait à rajouter à la fin dudit dit article : *« Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle. »*

6. Articles 26 et 49

Selon l'article 26, l'Office communique sur autorisation du Ministre de la Famille et de l'Intégration des données pseudonymisées à l'Inspection générale de la sécurité sociale qui peut en disposer dans le cadre de sa mission de recueillir des données statistiques nécessaires sur le plan national et international « *suivant un plan statistique et comptable uniforme pour toutes les institutions sociales* » (article 423, point (4) du Code de la sécurité sociale).

Dans ce contexte, la CNPD attire l'attention sur la différence entre données pseudonymisées et anonymisées. Selon le groupe de travail « article 29 » sur la protection des données « *l'anonymisation est le résultat du traitement des données personnelles afin d'empêcher, de façon irréversible, toute identification* » alors que « *la pseudonymisation n'est pas une méthode d'anonymisation. Elle réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée et constitue par conséquent une mesure de sécurité utile.* »[242]

Contrairement aux données anonymes, les données simplement pseudonymisées tombent toujours sous le champ d'application de la loi modifiée du 2 août 2002.

Dès lors, la CNPD se pose la question si l'établissement de statistiques nationales et internationales, justifie la communication des données pseudonymisées? Une communication de données anonymes ne serait-elle pas suffisante ?

Selon l'article 26 « *L'Office, sur autorisation du ministre, communique, par des procédés informatisés ou non,* ***des données*** *pseudonymisées contenues dans ses fichiers de données collectées dans le cadre de ses missions à l'Inspection générale de la sécurité sociale qui peut en disposer aux fins de l'exécution de ses missions telles que décrites à l'article 423, point 4 du Code de la sécurité sociale* ».

Ce texte n'est pas assez précis pour pouvoir déterminer quelles données devraient, le cas échéant, être communiquées, sous forme pseudonymisée, à des fins statistiques à l'IGSS. Dans sa rédaction actuelle, l'ONIS, devrait, sur demande de l'IGSS, communiquer l'intégralité de ses données (sous forme pseudonymisée) à l'IGSS. Se pose dès lors la question de la nécessité et de la proportionnalité des données communiquées.

Les mêmes observations ci-dessus sont également valables pour ce qui est de l'article 49 qui introduit aussi une communication sur autorisation des données pseudonymisées contenues dans les fichiers des offices sociaux à l'IGSS.

[242] Groupe de travail « article 29 » sur la protection des données, avis 05/2014 sur les Techniques d'anonymisation adopté le 10 avril 2014, p.

7. Remarques finales

A l'article 25, paragraphe (2), lettre d), tiret 4, le texte fait référence au « *rapport social prévu à l'article 14* », alors que ledit article ne fait pas état d'un tel rapport.

Le tiret 13 fait référence aux « *éléments de l'information préalable prévue à l'article 31* », alors que ledit article ne contient aucune disposition relative à une information préalable.

Ainsi décidé à Esch-sur-Alzette
en date du 22 décembre 2016.

La Commission nationale pour
la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

François Thill
Membre suppléant

Participations aux travaux européens

Documents adoptés par le groupe de travail « Article 29 » en 2016

Document	Date d'adoption	Référence
Opinion 03/2016 on the evaluation and review of the ePrivacy Directive	19.07.2016	WP 240
Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector	08.06.2016	WP 239
Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision	13.04.2016	WP 238
Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)	13.04.2016	WP 237
Statement on the 2016 action plan for the implementation of the General Data Protection Regulation (GDPR)	02.02.2016	WP 236
Work Programme 2016-2018	02.02.2016	WP 235

Tous les documents de travail du groupe de travail « Article 29 » peuvent être téléchargés sur Internet[243].

[243] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/

brain&more

CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES

1, avenue du Rock'n'Roll - L-4361 Esch-sur-Alzette
Téléphone : +352 26 10 60-1 - Fax : +352 26 10 60-29
www.cnpd.lu