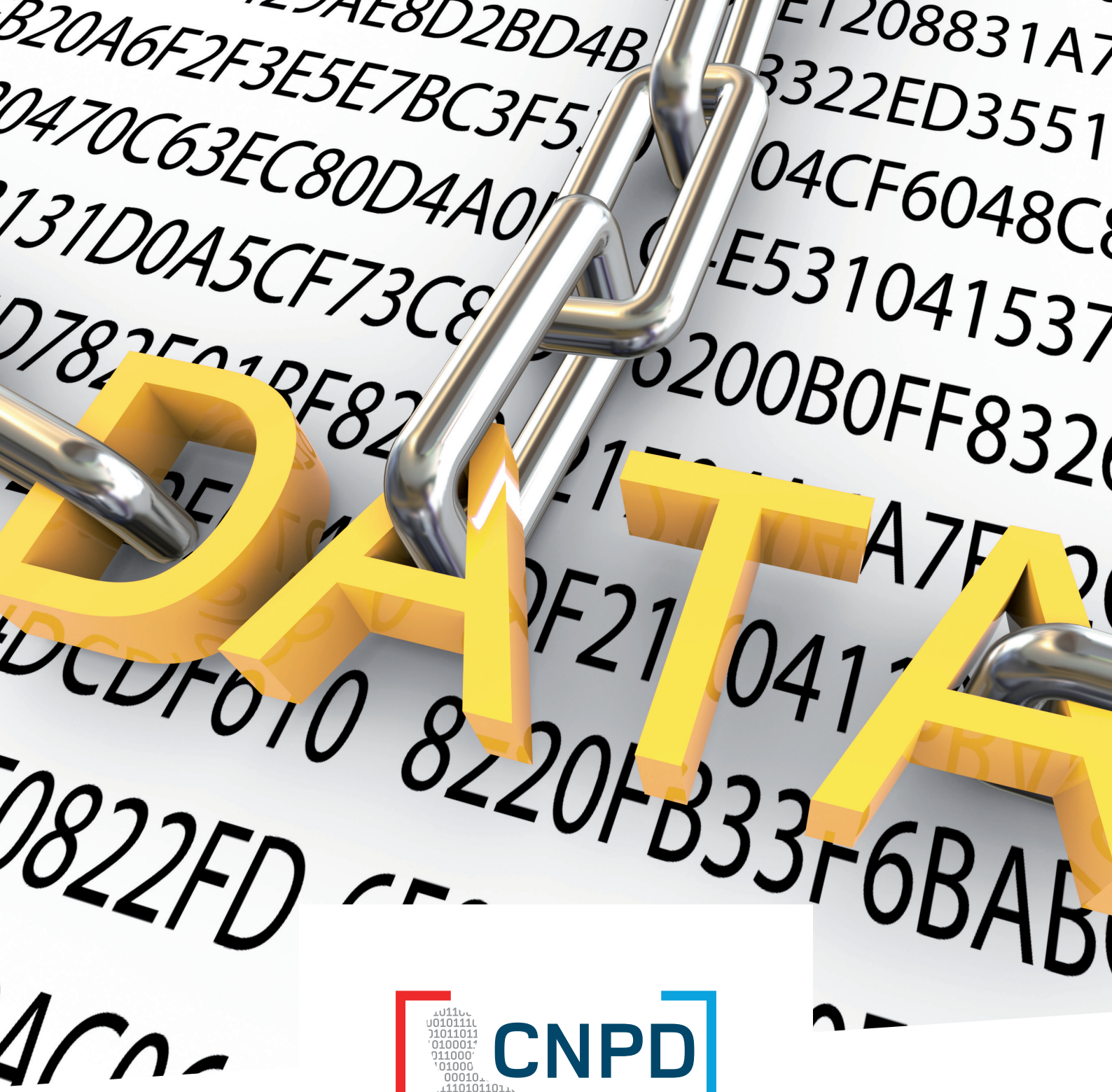


CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2015

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2015

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

Table des matières

1 Avant-propos

Le collège :
Georges Wantz, Tine A. Larsen, Thierry Lallemang

Deux décisions importantes en matière de protection des données ont été prises au niveau européen en 2015. Celles-ci ont eu, ont actuellement et auront encore à l'avenir un impact direct sur le travail et le fonctionnement de la CNPD :

- l'accord de l'Union européenne sur la réforme de la protection des données[1] et
- l'invalidation par la Cour de justice de l'UE des accords « Safe Harbor »[2].

Pour ce qui est de l'accord, les nouvelles règles européennes en matière de vie privée à l'ère numérique seront applicables à partir du 25 mai 2018. Outre le règlement général sur la protection des données, le paquet législatif comprend

[1] La partie 3.1. est consacrée à la réforme sur la protection des données.
[2] La partie 3.2. est consacrée à l'invalidation des accords « Safe Harbor ».

une directive spécifique pour le domaine de la police et de la justice.

Le règlement vise à donner aux citoyens plus de contrôle sur leurs données à caractère personnel, à responsabiliser davantage les entreprises tout en réduisant leurs charges administratives et à renforcer le rôle des autorités de protection des données tel que la CNPD. Les nouvelles règles, qui remplaceront la directive de 1995 régissant actuellement la matière, seront directement applicables dans tous les Etats membres de l'Union européenne y inclus du Luxembourg et à tous les acteurs actifs sur le territoire.

Pour les acteurs traitant des données personnelles, un changement de mentalité s'impose. La question ne se limite plus à savoir s'ils ont bien accompli les formalités administratives nécessaires préalables auprès de la CNPD. Ils devront adopter une approche de « privacy by design » et effectuer un vrai travail de réflexion avant la mise en œuvre d'un traitement afin d'assurer une protection optimale des données à caractère personnel des citoyens.

Tout au long de la durée de vie des données, un contrôle accru de l'application de la réglementation deviendra par ailleurs possible : pour la première fois, des amendes administratives importantes pourront être infligées en cas de traitement illicite ou d'abus constatés dans le cadre de l'utilisation de données personnelles.

À côté de l'accord sur la réforme européenne, une autre décision majeure a été prise en 2015 en matière de protection des données personnelles : le 6 octobre, la Cour de justice de l'Union européenne a déclaré les accords « Safe Harbor » invalides (Arrêt dans l'affaire C-362/14 - Maximillian Schrems/Data Protection Commissioner). Depuis lors, les transferts qui s'exerçaient vers des entreprises établies aux Etats-Unis d'Amérique sur base de ces accords sont illicites.

De plus, les missions et les pouvoirs des autorités de protection des données ont été confortés par cet arrêt « Schrems ». La Cour a conclu que les pouvoirs des autorités nationales n'étaient pas réduits par l'existence d'une décision de 2000, par laquelle la Commission avait considéré que Safe Harbor protégeait suffisamment les citoyens de l'UE. Les autorités de protection des données ont la possibilité d'étudier, en toute indépendance, une plainte alléguant qu'un pays tiers ne permet pas d'assurer un niveau adéquat de protection. La décision a réaffirmé que la protection des données personnelles fait partie intégrante des droits fondamentaux en Europe.

Au niveau national, la forte croissance de l'activité que la CNPD connaît depuis plusieurs années s'est poursuivie.

En 2015, l'autorité luxembourgeoise a participé à 252 réunions (+ 49% par rapport à 2014) et a reçu le plus grand nombre de demandes de renseignement depuis sa création, soit 2.361, ce qui constitue une augmentation de 7% par rapport à l'année précédente. Elle doit fournir des conseils appropriés aux acteurs, tant du secteur public, que du secteur privé qui la consultent pour vérifier la conformité de leurs pratiques ou projets à l'égard des dispositions légales applicables.

Cette évolution est confirmée par le futur règlement qui place la guidance et la sensibilisation de ces acteurs au centre des missions de la CNPD, en réduisant largement les formalités administratives en contrepartie.

1 Avant-propos

Le travail consultatif de la CNPD peut varier de la simple guidance à des renseignements juridiques très poussés, voire des avis sur les projets de loi et règlements grand-ducaux si leur thématique touche à la protection des données. En 2015, la Commission nationale a avisé 13 projets de loi ou mesures réglementaires concernant notamment les radars automatiques, la modernisation du droit de la faillite, le casier judiciaire, l'accord FATCA, l'introduction d'une subvention de loyer ou encore l'organisation du secteur des services de taxis.

La CNPD a reçu 217 plaintes, dont le nombre est d'ailleurs en constante augmentation depuis 2011. Elles concernent les entreprises, mais aussi le secteur public. Majoritairement, ces plaintes proviennent de l'étranger et sont en lien direct avec la présence des sièges européens de nombreuses entreprises multinationales au Luxembourg. Outre les demandes de vérification de licéité de certaines pratiques administratives ou commerciales, il s'agit le plus souvent de demandes d'effacement ou de rectification de données non respectées ou de transmissions déloyales de données à des tiers.

L'autorité de contrôle a, en outre, effectué 35 contrôles et investigations en 2015, que ce soit dans le cadre de la surveillance sur le lieu de travail ou encore lorsqu'elle a pris connaissance d'une attaque informatique, d'une faille de sécurité ou d'une autre violation des dispositions légales en matière de protection des données.

Les 154 demandes d'autorisation en vue du transfert de données vers des pays tiers enregistrées en 2015 représentent le chiffre annuel le plus élevé depuis la création de la CNPD et une hausse significative de 69% par rapport à l'année précédente.

Dans les prochaines années, les services de la CNPD seront réorganisés afin de mieux répondre aux attentes des différents acteurs et de préparer l'entrée en vigueur du règlement européen en 2018. Conscient de l'importance de la mission de la CNPD et de la complexité croissante des questions que soulèvent les traitements de données à caractère personnel à l'ère numérique, le Gouvernement a décidé de renforcer progressivement les effectifs de la CNPD. La CNPD salue cette décision, qui lui permettra de rencontrer les futurs défis avec les ressources nécessaires.

Le siège de la CNPD à Belval

Luxembourg, le 13 juin 2016

La Commission nationale pour
la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

2 Les activités en 2015

L'année 2015 en un coup d'œil

Janvier

21 - La CNPD participe à un panel lors de la conférence internationale « Computers, Privacy and Data Protection » à Bruxelles
27 - La CNPD organise une conférence avec l'APDL et SMILE sur les défis à venir du projet de règlement européen en matière de protection des données
28 - Journée de la protection des données
30 - La CNPD avise le projet de règlement grand-ducal relatif aux cartes de légitimation et lettres de légitimation de certains agents et experts externes de l'Administration des chemins de fer

Février

6 - La CNPD émet un avis à l'égard du projet de loi n°6588 portant organisation du secteur des services de taxis
6 - La CNPD émet un avis relatif au projet de règlement grand-ducal concernant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales
25 - La CNPD émet un avis à l'égard du projet de loi n°6714 portant création du système de contrôle et de sanction automatisé

Mars

6 - La CNPD donne une séance d'information à l'ABBL concernant la protection de la vie privée sur le lieu du travail

Mai

13 - La CNPD donne un avis sur le projet de loi n°6763 concernant l'accord FATCA
13 - La CNPD donne une présentation à l'Association des Secrétaires Communaux de Luxembourg
18 - La CNPD participe à la Conférence de printemps des autorités de protection des données à Manchester
22 - La CNPD participe au premier « Information Security Day »

Juin

8-9 - La CNPD donne des cours de formation à l'Institut National d'Administration Publique
13 - La CNPD participe à la quatrième édition de « Hack4Kids » avec un atelier sur les données à caractère personnel
19 - La CNPD avise le 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 - La CNPD intervient à la conférence de l'ABBL sur l'échange automatique d'informations fiscales
26 - La CNPD participe à une table ronde lors de la conférence de l'OLDE intitulée « Internet : libertés et restrictions »
30 - La CNPD participe au colloque de l'Union Internationale des avocats sur le thème « l'Homme augmenté : de la science-fiction à la réalité »

Juillet

2 - La CNPD avise le projet de loi n°6542 portant introduction d'une subvention de loyer
2 - La CNPD donne son avis sur le projet de loi n°6820 concernant l'organisation du casier judiciaire
30 - La CNPD avise les projets

DELIBERATIONS

755
Délibérations adoptées

13
Avis relatifs à des projets ou propositions de loi ou mesures réglementaires

35
Demandes d'agréments pour les chargés de la protection des données

FORMALITES PREALABLES

724
Notifications reçues
(+18% par rapport à 2014)

1.117
Demandes d'autorisations
(+11% par rapport à 2014)

7.492
Déclarants (depuis 2002)

GUIDANCE

252
Réunions
(+49% par rapport à 2014)

2.361
Demandes de renseignement
(+7% par rapport à 2014)

PLAINTES ET INVESTIGATIONS

217
Plaintes
(+5% par rapport à 2014)

35
Investigations

VIOLATIONS DE DONNEES (COMMUNICATIONS ELECTRONIQUES)

2
Notifications

de loi n°6759 et n°6762 concernant les échanges de données entre les Etats-Unis et le Luxembourg
30 - La CNPD intervient aux journées eHandwierk sur le cloud computing

Septembre

11 - La CNPD donne une formation à l'Ecole supérieure du travail
28 - La CNPD participe au séminaire européen « Case Handling Workshop » à Tirana
30 - La CNPD participe à une conférence de la Chambre des Métiers sur la surveillance sur le lieu du travail

Octobre

1 - La CJUE décide que la réglementation d'un État membre sur la protection des données peut être appliquée à une société étrangère qui exerce dans cet État, au moyen d'une installation stable, une activité réelle et effective (Arrêt « Weltimmo »)
6 - La CJUE invalide les accords « Safe Harbor » (Arrêt « Schrems »)
7-8 - La CNPD participe à l'« Annual Privacy Forum »
16 - La CNPD avise le projet de loi n°6779 portant sur la protection internationale et la protection temporaire
26 - La CNPD participe à la 37ème Conférence internationale des commissaires de la protection des données et de la vie privée à Amsterdam

Novembre

20 - La CNPD émet un avis à l'égard de l'avant-projet de loi portant transposition de la directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen
20 - La CNPD avise le projet de loi n°6539 relatif à la préservation des entreprises et portant modernisation du droit de la faillite

Décembre

1-2 - La CNPD participe à la conférence européenne sur l'administration électronique
3 - La CNPD présente les avancées du G29 lors de la deuxième conférence annuelle sur la protection des données
8 - La CNPD participe à la conférence « The Digital Single Market – What's in it for us ? » à Copenhague
15 - L'UE trouve un accord sur la réforme de la protection des données
17 - La CNPD émet un avis sur le projet de loi n°6893 et le règlement grand-ducal relatif à la reconnaissance des qualifications professionnelles

2 Les activités en 2015

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 2015 était centré 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.

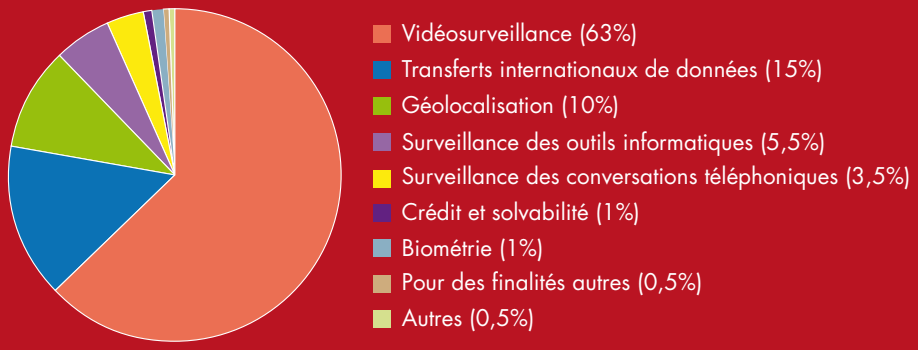
Le nombre total des traitements de données déclarés depuis 2003 s'élève à 24.162. En tout,

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 2015



7.472 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 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.

Il existe deux types de notifications : les notifications ordinaires et les engagements formels de conformité.

Notifications ordinaires

En 2015, la CNPD a reçu 705 notifications ordinaires, ce qui constitue une augmentation de 25% par rapport à l'année précédente. La finalité invoquée le plus souvent était l'administration du personnel. D'autres raisons citées pour traiter des données 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 points aux conditions fixées dans les décisions uniques afférentes, le responsable du traitement

2 Les activités en 2015

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 19 engagements formels de conformité en 2015.

2.1.1.2 Les autorisations préalables

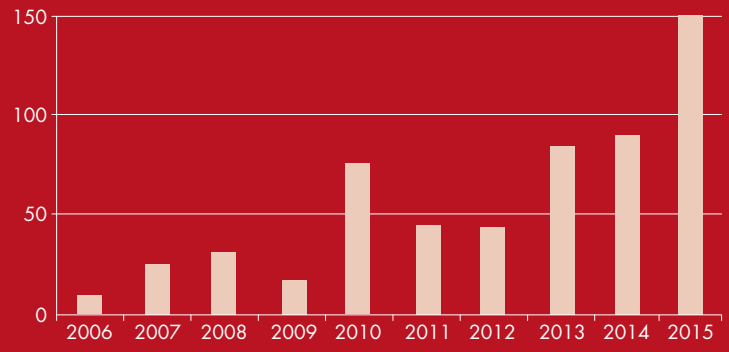
Les traitements présentant un risque particulier au regard de la vie privée des personnes concernées ne sont possibles que moyennant une autorisation de la Commission nationale. Ces dossiers nécessitent toujours une analyse détaillée et une appréciation circonstanciée et pondérée au cas par cas.

Au total, la CNPD a reçu 1.117 demandes (demandes d'autorisation et engagements formels de conformité) en 2015.

Demandes d'autorisation

Le nombre des demandes d'autorisation reçu par la CNPD est en augmentation constante depuis 2011 : 969 demandes lui ont été soumises en 2015 (contre 914 en 2014).

Transferts vers des pays tiers



La grande majorité des demandes en 2015 étaient relatives à la surveillance sur le lieu du travail (83%). 63% concernaient l'exploitation de caméras de surveillance et 10% le contrôle des déplacements de véhicules et de personnes grâce à la géolocalisation. Les demandes concernant les dispositifs de vidéosurveillance ont augmenté en 2015 tandis que celles concernant la géolocalisation ont diminué. Le nombre de requêtes en matière d'enregistrement des conversations téléphoniques et de surveillance des outils informatiques est resté constant.

Engagements formels de conformité

En plus des demandes d'autorisation, la Commission nationale a reçu 148 engagements formels de conformité en 2015 (+74% par rapport à 2014). 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

2.1.2.1 Autorisation en cas de transferts de données vers des pays tiers

En principe, il est interdit de transférer des données à caractère personnel vers des pays situés hors de l'Espace économique européen (Union européenne, Liechtenstein, Norvège et Islande) n'assurant pas une protection adéquate. Si une entreprise souhaite transférer des données personnelles du Luxembourg vers un destinataire établi en dehors de ces pays, elle devra, selon les cas, remplir le formulaire de notification préalable ou demander une autorisation préalable à la CNPD.

Il existe toutefois deux exceptions à ce principe :

- Les accords conventionnels passés entre les exportateurs et destinataires des données ou autres mesures de protection (notamment les « binding corporate rules » ou règles contraignantes d'entreprise) qui constituent des garanties suffisantes. Aux termes de l'article 19 (3), 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 dérogations légales[3] qui ne s'appliquent que dans des cas limités (pour des transferts de données qui ne peuvent être qualifiés de répétés, massifs ou structurels) : consentement de la personne concernée, nécessité pour l'exécution d'un contrat conclu dans l'intérêt de la personne concernée, intérêt public important…

Les transferts de données à caractère personnel à destination des Etats-Unis d'Amérique sur base de la décision d'adéquation 2000/520 de la Commission européenne du 26 juillet 2000 relative aux accords « Safe Harbor » ne sont plus possibles suite à l'arrêt de la Cour de Justice de l'Union européenne du 6 octobre 2015 (« Maximilian Schrems c. Data Protection

[3] Conditions énumérées à l'article 19 (1) de la loi modifiée du 2 août 2002 et également prévues dans la directive.

2 Les activités en 2015

Commissioner ») qui a invalidé cette décision. La CNPD en a informé[4] toutes les entreprises luxembourgeoises concernées par courrier et via son site internet.

En 2015, la Commission nationale a été saisie de 154 demandes d'autorisation en vue du transfert de données vers des pays tiers. Cela correspond à une hausse de 69% 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 lointains 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.

2.1.2.2 Approbation de règles d'entreprise contraignantes

Les règles d'entreprise contraignantes (« Binding Corporate Rules ») constituent

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

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 2015, 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.

2.1.2.3 Contrôle des clauses contractuelles d'Amazon Web Services (AWS)

La CNPD en sa qualité de chef de file - et en collaboration avec d'autres autorités européennes de protection des données concernées (conformément au document de travail 226, adopté par le Groupe de l'Article 29) - a procédé à l'analyse du « Data Processing Addendum » et de l'annexe 2 des clauses contractuelles types d'Amazon Web Services (AWS), Inc.

L'objectif de cette révision par les autorités de protection des données consistait à évaluer si ces documents respectent les exigences en matière de transferts internationaux de données contenues dans les clauses contractuelles types de la Décision 2010/87/UE de la Commission.

Le 6 mars 2015, la CNPD a envoyé une lettre à AWS, confirmant que le « Data Processing Addendum » d'AWS était conforme aux clauses contractuelles types de la Décision 2010/87/UE de la Commission et reconnaissant qu'en utilisant le « Data Processing Addendum » ensemble avec ses annexes, AWS prendrait des engagements contractuels suffisants pour fournir un cadre légal à ses flux internationaux de données conformément à l'article 26 de la Directive 95/46/CE.

2.1.3 Les chargés de la protection des données

Tout responsable du traitement dispose de la faculté de désigner 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 en revanche 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 du traitement et, corrélativement, d'un droit d'informer le responsable du 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 ou 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.

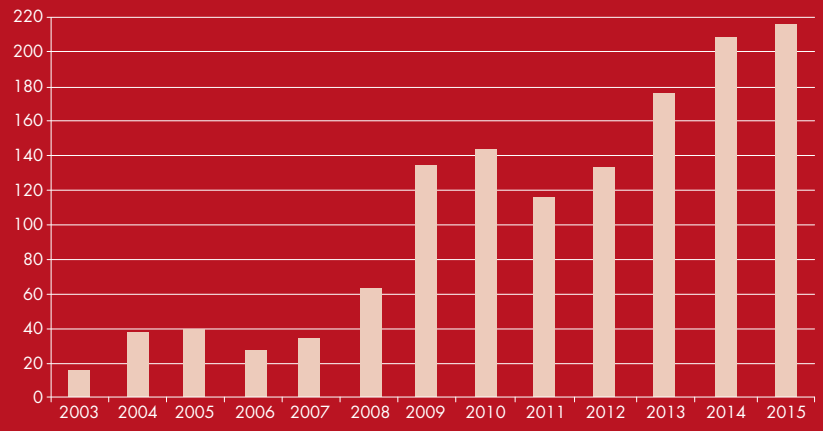
Depuis 2005, 125 entreprises, associations et organismes publics ont désigné un chargé de la protection des données. À la fin de l'année 2015, 149 personnes physiques ou morales étaient agréées pour exercer l'activité de chargé de la protection des données.

2.1.4 Demandes de vérification de licéité et plaintes

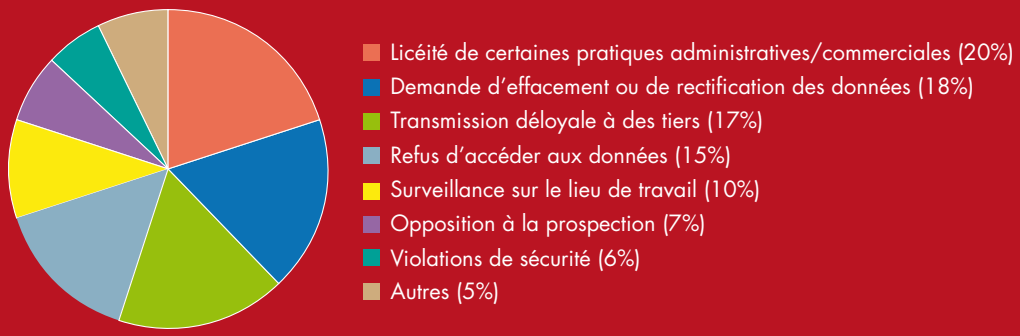
Cette année à nouveau, la CNPD a enregistré un niveau supérieur de plaintes par rapport à l'année précédente : 217 personnes ont fait appel à ses services lorsqu'elles ont estimé qu'il y a eu une violation de la loi ou une entrave à l'exercice de leurs droits. Ce chiffre est en augmentation constante depuis 2011.

70% 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 à Luxembourg. Pour ces acteurs, la CNPD est l'autorité compétente pour assurer le respect de la législation nationale en matière de protection des données.

Evolution du nombre de plaintes



Motif des plaintes



Environ 60% des plaintes visaient des entreprises offrant des services sur Internet.

Dans 20% 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.

Les demandes d'effacement ou de rectification de données non respectées ont représenté 18% des plaintes reçues en 2015. Il s'agissait, entre autres, de :

- demandes de fermetures de comptes auprès de services en ligne ;
- demandes d'effacement d'articles de presse dans lequel les plaignants étaient cités ou
- de boîtes e-mail non effacées après le départ auprès de l'ancien employeur.

Comme tous les ans, la transmission non autorisée de données à des tiers a conduit à un certain nombre de plaintes (17%). Cela inclut par exemple celles concernant l'envoi de courriels confidentiels, mais distribués de façon collective et visible à tous les destinataires (« CC » au lieu de « BCC »).

Les activités en 2015

Un nombre important de plaintes (15%) a par ailleurs 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.

La majorité des requêtes liées à la surveillance sur le lieu du travail (10% des plaintes) concernaient la vidéosurveillance. Toutefois, les plaignants ont également contacté la CNPD lorsqu'ils ont estimé que leur courrier électronique ou les fichiers sur leur ordinateur avaient été consultés illégalement.

Finalement, les plaintes relatives au droit d'opposition à la prospection sont de plus en plus courantes. 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.

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 35 contrôles et investigations en 2015, que ce soit dans le cadre de la surveillance sur le lieu de travail ou encore lorsqu'elle a pris connaissance d'une attaque informatique, d'une faille de sécurité ou d'une autre violation des dispositions légales en matière de protection des données.

Surveillance sur le lieu du travail

La CNPD a contrôlé plusieurs 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 est 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.

Violations de sécurité

L'autorité de protection des données est également intervenue lorsque des violations de données[5] lui ont été signalées.

Elle a notamment contrôlé une entreprise offrant des jeux en ligne suite à un vol de plusieurs milliers de numéros de cartes de crédit. Une autre investigation concernait une société offrant des services en ligne après que certains de ses utilisateurs avaient eu accès aux comptes personnels d'autres utilisateurs.

Dans ces circonstances, il est très important de rapidement mettre en place les mesures de sécurité nécessaires pour protéger les données à caractère personnel des personnes concernées et d'éviter des incidents similaires dans le futur.

Autres investigations

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

- de demandes d'accès ou d'opposition non respectées par le responsable du traitement ;

- de consultations non autorisées de données par des employés ou par l'employeur ;

- de transmissions de données illégales à des tiers.

De plus, elle a entamé une investigation dans le secteur des assurances concernant les nombreuses nouvelles applications en ligne et sur les téléphones mobiles.

Avertissements

La Commission nationale peut prononcer des avertissements si elle estime que la loi sur la protection des données n'est pas respectée.

En 2015, elle a prononcé deux avertissements en application de l'article 33 de la loi modifiée du 2 août 2002 à l'encontre

- d'une administration publique pour avoir violé le principe de la proportionnalité des données et pour ne pas avoir respecté les obligations légales en matière de confidentialité des données à caractère personnel

[5] Il s'agit des violations de données en dehors du secteur des communications électroniques. Celles-ci sont traitées dans la partie 2.1.6.1.

Les activités en 2015

en diffusant une quantité d'informations personnelles disproportionnée au grand public ;

- d'une entreprise offrant des services en ligne n'ayant pas mis en place des mesures de sécurité suffisantes.

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 2015, deux violations de données dans le secteur des

communications électroniques ont été signalées 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 a 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 est 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 est 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.

Les statistiques sur la conservation des données au titre des articles 5 et 9 sont transmises annuellement à la Commission européenne. 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 2015, des informations ont été transmises aux autorités compétentes (Police judiciaire et Justice) dans 1.949 cas (contre 1.430 en 2014). Dans 1.210 cas (contre 457 en 2014), les demandes de données n'ont pas pu être satisfaites. Au total, les autorités compétentes ont fait 3.159 demandes auprès des opérateurs. Ce chiffre a augmenté par rapport à l'année 2014 où 1.887 demandes ont 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*

2 Les activités en 2015

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 ».

En 2015, la Commission nationale a émis 13 avis dans le cadre de projets de loi ou de règlements grand-ducaux :

1. Avis concernant le projet de règlement grand-ducal relatif aux cartes de légitimation et lettres de légitimation de certains agents et experts externes de l'Administration des chemins de fer (Délibération n°4/2015 du 30 janvier 2015) ;

2. Avis à l'égard du projet de loi n°6588 portant a) organisation du secteur des services de taxis et b) modification du Code de la consommation (Délibération n°37/2015 du 6 février 2015) ;

3. 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 (Délibération n°45/2015 du 6 février 2015) ;

4. Avis à l'égard du projet de loi n°6714 portant création du système de contrôle et de sanction automatisé et modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques, et du projet de règlement grand-ducal autorisant la création d'un fichier et le traitement de données à caractère personnel dans le cadre du système de contrôle et de sanction automatisé (Délibération n°74/2015 du 25 février 2015) ;

5. Avis relatif au projet de loi n°6798 portant approbation : - 1. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des États-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et relatif aux dispositions des États-Unis d'Amérique concernant l'échange d'informations communément appelées le « Foreign Account Tax Compliance Act », y compris ses deux annexes ainsi que le « Memorandum of Understanding » y relatif, signés à Luxembourg le 28 mars 2014, - 2.

Les séances de délibération de la Commission nationale

Le collège se réunit en principe une fois par semaine en séance de délibération. Une partie importante de ces séances est consacrée à l'examen des dossiers de demande d'avis ou d'autorisation. Au cours de 39 séances en 2015, la Commission nationale a adopté 755 délibérations, dont notamment :

- 705 autorisations ;
- 13 avis relatifs à des projets ou propositions de loi et mesures réglementaires ;
- 35 décisions concernant les chargés de la protection des données ;
- 2 avertissements

de l'échange de notes y relatives (Délibération n°198/2015 du 13 mai 2015) ;

6. Avis 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 (Délibération n°228/2015 du 19 juin 2015) ;

7. Avis complémentaire à l'égard du 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 et du projet de règlement grand-ducal fixant les conditions et modalités d'octroi de la subvention de loyer prévue par l'article 14quinquies de la loi modifiée du 25 février 1979 concernant l'aide au logement (Délibération n°258/2015 du 2 juillet 2015) ;

8. Avis à l'égard du projet de loi n°6820 portant modification : 1) de la loi du 29 mars 2013 relative à l'organisation du casier et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne, 2) du Code d'instruction criminelle, 3) du Code pénal (Délibération n°259/2015 du 2 juillet 2015) ;

9. Avis relatif au 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 au 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 (Délibération n°366/2015 du 30 juillet 2015) ;

10. Avis relatif au projet de loi n°6779 portant sur la protection internationale et la protection temporaire (Délibération n°476/2015 du 16 octobre 2015) ;

11. Avis à l'égard de l'avant-projet de loi portant transposition de la directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen (Délibération n°651/2015 du 20 novembre 2015) ;

12. Avis à l'égard du projet de loi n°6539 relatif à la préservation des entreprises et portant modernisation du droit de la faillite (Délibération n°652/2015 du 20 novembre 2015) ;

Les activités en 2015

13. Avis à l'égard du projet de loi n°6893 relatif à la reconnaissance des qualifications professionnelles et du projet de règlement grand-ducal relatif à la reconnaissance des qualifications professionnelles (Délibération n°718/2015 du 17 décembre 2015).

2.2.1 Cartes de légitimation de l'Administration des chemins de fers

Suite à la demande du Ministère du Développement durable et des Infrastructures, la Commission nationale s'est prononcée au sujet du projet de règlement grand-ducal relatif aux cartes de légitimation et lettres de légitimation de certains agents et experts externes de l'Administration des chemins de fer.
L'objectif de ce projet consiste à définir les informations figurant sur les cartes de légitimation des agents de l'Administration des chemins de fer (ACF) et les lettres de légitimation des experts externes de l'ACF, de même que leurs modalités de délivrance, d'utilisation et de restitution, ainsi que leur durée de validité.
Il est également créé, à cette occasion, un registre des cartes de légitimation et des lettres de légitimation.

La Commission nationale a limité ses observations aux questions traitant des aspects portant sur la protection des données.

L'article 9 prévoit que le registre « renseigne au moins sur la date d'émission, la durée de validité, les décisions visées à l'article 4, les mesures administratives visées à l'article 7 et les restitutions visées à l'article 8 ». La CNPD a estimé dans son avis que le terme « au moins » apparaît comme trop vague et permettrait de collecter d'autres données supplémentaires que celles indiquées dans le texte.
Aux yeux de la CNPD, cette disposition ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal, et n'est par ailleurs pas conforme à l'article 4 de la loi modifiée du 2 août 2002. La Commission nationale a suggéré d'énumérer dans l'article 9 de façon exhaustive les données qui pourront être traitées dans le registre, et de supprimer le terme « au moins ».

Dans ce contexte, la CNPD s'est demandé si le registre ou un autre fichier informatique séparé, tenu par l'ACF, ne contenait pas en réalité aussi des données personnelles comme par exemple les noms et prénoms, adresses, dates de naissance et photos des demandeurs ou titulaires.
Concernant les photos, la CNPD a rappelé son opposition à un éventuel stockage numérique des photos.

La Commission nationale a par ailleurs noté que le modèle de

demande relative à l'attribution d'une carte de légitimation reproduit la mention « numéro d'identification personnelle (matricule de sécurité sociale) ». A défaut de préciser dans quelle mesure cette information est nécessaire, la CNPD a proposé de supprimer cette mention dans le modèle. En effet, les seuls noms, prénom, lieu et date de naissance de la personne concernée paraissent suffisants afin d'identifier le titulaire de la carte, d'autant plus que c'est l'employeur qui doit introduire la demande et que ce dernier aura préalablement vérifié l'identité de ses agents.

2.2.2 Organisation du secteur des services de taxis

La Commission nationale a présenté ses réflexions et commentaires dans son avis au sujet du projet de loi n°6588 portant a) organisation du secteur des services de taxis et b) modification du Code de la consommation. L'objectif de ce projet de loi est de réformer le secteur des services de taxis au Luxembourg, et ce notamment en instaurant un régime d'autorisation centralisé, en renforçant les conditions d'accès aux activités d'exploitant et de conducteur de taxi, en diversifiant les contrôles et en facilitant les sanctions applicables.

Il est prévu de créer un registre des exploitants et des conducteurs de taxi, tenu auprès du Ministère du Développement durable et des Infrastructures, dans lequel figureraient notamment les données nécessaires à la gestion administrative et au suivi des licences d'exploitation de taxi et des cartes de conducteur de taxi. Ce registre servirait en outre aux membres de la police grand-ducale et aux agents de l'administration des douanes et accises dans l'exercice des missions leurs conférées, notamment en ce qui concerne les contrôles susmentionnés.

La CNPD a noté dans son avis qu'il ne ressortirait pas clairement du texte qui est le responsable du traitement. Pour cette raison, elle a suggéré de préciser dans le projet de loi que le ministre ayant le transport dans ses attributions était à considérer comme responsable du traitement. L'autorité de protection des données a par ailleurs remarqué que le texte ne précisait ni le contenu exact du registre, ni n'expliquait comment ledit registre était alimenté concrètement. La CNPD a suggéré de restructurer l'article 20 en précisant les finalités claires et précises du traitement et d'énumérer de manière exhaustive les catégories de données concernées, avec indication de leur origine.

En ce qui concerne l'accès du ministère à différents autres fichiers étatiques, la CNPD avait considéré que le texte examiné ne respectait pas les principes de proportionnalité et de nécessité au regard de la finalité envisagée. En effet, le nombre de personnes concernées par le dispositif envisagé est limité au nombre des conducteurs de taxis et d'exploitants de taxi. L'article 20 paragraphe (2) du projet de loi analysé permettrait cependant un accès aux données contenues dans des fichiers ou registres concernant l'ensemble de la population. La CNPD a estimé nécessaire la mise en place d'une solution technique permettant de garantir que les agents du ministère puissent seulement accéder aux données concernant les personnes qui ont introduit une demande, à l'exclusion des données relatives au reste de la population.

Quant à l'accès direct du nouveau registre par les forces de l'ordre, la CNPD s'est demandé si cette disposition ne devrait pas être intégrée dans le corps de l'article 34-1 de la loi modifiée du 22 juillet 2008 qui précise notamment les fichiers auxquels les forces de l'ordre peuvent avoir accès. Se posait par ailleurs la question si les membres de la police devaient avoir accès à l'intégralité des données du registre ou s'il ne faudrait pas limiter cet accès aux données effectivement nécessaires.

La CNPD a par ailleurs considéré qu'un accès direct au fichier du casier judiciaire au moyen d'un système informatique tel qu'envisagé par le ministère est difficilement envisageable,

alors que les dispositions de la loi du 29 mars 2013 relative à l'organisation du casier judiciaire prévoient limitativement tous les cas dans lesquels un extrait du casier peut être délivré. Considérant que l'on ne se trouve pas dans l'une de ces hypothèses et que la notion de délivrance du bulletin n°2 du casier judiciaire est à interpréter de manière stricte, notamment au vu de la sensibilité des données qu'il comporte, la Commission nationale a recommandé de biffer le point e) de l'article 20, paragraphe (2) du projet de loi.

La CNPD a également estimé nécessaire de prévoir un système de journalisation des accès aux données et une disposition réglant la durée de conservation des données à caractère personnel.

2.2.3 Accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales

La Commission nationale a donné son avis sur le 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.

Par délibération du 12 juillet 2013, la Commission nationale avait déjà avisé l'avant-projet de règlement grand-ducal en question en relevant certains points qui nécessitaient soit davantage de précisions, soit des modifications. Après examen du projet de règlement grand-ducal, la CNPD a salué les corrections qui y ont été apportées par rapport à l'avant-projet, mais a encore soulevé les points suivants :

La CNPD a suggéré de préciser dans un seul article quelles données à caractère personnel sont collectées et traitées dans le registre ainsi que l'origine de celles-ci.

Elle a conseillé de ne pas recourir à des formulations trop vagues afin d'éviter que le responsable du traitement puisse collecter d'autres données supplémentaires que celles strictement nécessaires au traitement envisagé.

La CNPD a par ailleurs estimé nécessaire 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 ayant l'Economie dans ses attributions puissent seulement accéder aux données concernant les personnes qui ont introduit une notification préalable ou une demande auprès du ministère précité dans le cadre de l'article 32 de la loi du 2 septembre 2011, à l'exclusion des données

relatives au reste de la population concernée (résidente ou non).

Enfin, elle a proposé d'ajouter un nouvel article relatif à la durée de conservation des données du registre tenu par le ministère ayant l'Economie dans ses attributions.

2.2.4 Radars

La Commission nationale a présenté ses réflexions et commentaires au sujet :

- du projet de loi n°6714 portant création du système de contrôle et de sanction automatisé et modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques,

- et du projet de règlement grand-ducal autorisant la création d'un fichier et le traitement de données à caractère personnel dans le cadre du système de contrôle et de sanction automatisé.

L'objectif est de mettre en place un système de contrôle et de sanction automatisé (« CSA ») visant à automatiser la constatation de certaines infractions routières et la sanction subséquente du contrevenant présumé de l'infraction. Ainsi sera facilitée la constatation, sans interception des véhicules, de certaines infractions au code de la route, et en particulier, mais non exclusivement, du non-respect des vitesses maximales autorisées. Un tel système devrait permettre, d'après le Gouvernement, de réduire le nombre d'infractions et, partant, d'améliorer la sécurité sur les routes luxembourgeoises.

Dans ce contexte, il a été proposé de créer un centre de traitement des infractions routières (« le centre ») qui a pour mission la gestion du système de CSA et qui est exploité par la Police grand-ducale, sous la surveillance du procureur d'Etat. Il ressort des projets de loi règlement grand-ducal que la Police grand-ducale mettra dans ce cadre en œuvre un traitement de données à caractère personnel au sens de l'article 2 lettre (r) de la loi 2 août 2002.

Dans son avis, la CNPD s'était demandé si pratiquement toutes les dispositions figurant actuellement dans le projet de règlement grand-ducal ne devraient pas figurer dans la loi. De façon plus générale, la CNPD s'était posé la question de savoir s'il ne serait pas utile de préciser quelles étaient les données ou catégories de données nécessaires permettant de réaliser chacune des finalités prévues dans l'actuel article 2 du projet de loi. En l'absence d'une telle précision, il serait en effet difficile pour la CNPD d'apprécier le caractère adéquat, pertinent et non excessif de certaines données dans le projet de règlement grand-ducal.

La CNPD a remarqué par ailleurs que la procédure proposée dans le projet de loi, selon laquelle les sociétés de location seront obligées de donner accès à la Police à leurs fichiers respectifs, suppose que les sociétés privées de location soient obligées de tenir un tel fichier. Cette obligation devrait le cas échéant être inscrite dans la loi. En outre, si un tel accès était accordé à la Police, il s'agirait d'un traitement de données à caractère personnel, qui devrait à ce titre également figurer dans le projet de loi, de même que les données auxquelles auraient accès les services de police, et les finalités pour lesquelles il serait réalisé.

Quant au droit d'accès, la CNPD a estimé nécessaire d'adapter le paragraphe (2) de l'article 10 du projet de loi en permettant à la personne pécuniairement responsable ou la personne désignée comme conducteur du véhicule au moment de l'infraction de consulter la photo concernant son véhicule, selon son choix, sur place au Centre, ou de recevoir communication de la photo via une demande écrite préalable adressée au Centre. Concernant l'image du passager, la CNPD s'est demandé s'il ne faudrait pas, dès la prise de photos, masquer automatiquement l'image du passager.

Les activités en 2015

La Commission nationale s'est par ailleurs interrogée sur la question de savoir pourquoi l'article 4 lettre (a) du projet de règlement grand-ducal sous examen prévoyait que la police soit destinataire des données enregistrées dans le cadre du système CSA, alors que c'est justement elle, par l'intermédiaire de son Directeur général, qui a la qualité de responsable du traitement.

En ce qui concerne les radars tronçons, la CNPD a proposé de prévoir un système permettant que les données (y compris les photographies) relatives aux personnes n'ayant pas commis d'infraction soient immédiatement et automatiquement détruites par le système mis en place, de telle sorte qu'aucune donnée à caractère personnel ne puisse plus être réutilisée.

2.2.5 Accord FATCA

La CNPD a avisé le projet de loi n°6798 portant approbation :

1. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des États-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et relatif aux dispositions des États-Unis d'Amérique concernant l'échange d'informations communément appelées le « Foreign Account Tax Compliance Act », y compris ses deux annexes ainsi que le « Memorandum of Understanding » y relatif, signés à Luxembourg le 28 mars 2014 (ci-après désigné « l'accord FATCA »),
2. de l'échange de notes y relatives.

L'accord FATCA a pour objectif d'améliorer le respect des obligations fiscales à l'échelle internationale à travers une assistance mutuelle en matière de fiscalité sur la base d'une infrastructure efficace pour l'échange automatique d'informations entre, d'une part, le Gouvernement du Grand-Duché de Luxembourg, et d'autre part, le Gouvernement des Etats-Unis d'Amérique.

Cet accord s'inscrit dans un contexte européen et international où une importance accrue a été reconnue en matière d'échange automatique d'informations comme moyen de lutte contre la fraude et l'évasion fiscales transfrontières. La CNPD a regretté toutefois qu'elle n'ait pas été consultée lors de la phase de négociation de l'accord FATCA, alors que le projet de loi a pour but d'approuver un accord signé, qui ne peut plus être modifié à moins de le renégocier avec le Gouvernement des Etats-Unis d'Amérique.

Elle a limité ses observations aux questions soulevées par

les dispositions du projet de loi traitant des aspects portant sur la protection des données, dont plus particulièrement les articles 2 et 3.

L'autorité de contrôle a suggéré de préciser les modalités de transmission des données, ainsi que les mesures de sécurité techniques et organisationnelles devant le cas échéant être mises en place à l'occasion de la communication de ces données à l'Administration des contributions directes. A défaut de telles précisions dans le projet de loi ou dans un règlement grand-ducal à adopter, la Commission nationale a indiqué qu'elle ne serait pas en mesure d'apprécier le caractère adéquat et sécurisé de la transmission des données à l'Administration des contributions directes.

Enfin, la Commission nationale s'était demandé si la durée de conservation des données prévue dans le projet de loi ne mériterait pas davantage de précisions.

2.2.6 Communications électroniques

La Commission nationale a avisé le 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.

Dans son avis n°214/2014 du 13 mai 2014, la Commission nationale avait analysé la législation luxembourgeoise existante au regard de l'arrêt de la Cour de justice de l'Union européenne rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12 (Digital Rights Ireland et Seitlinger et autres). Dans ledit avis, la CNPD avait attiré l'attention sur plusieurs points de la législation qui devraient faire l'objet de modifications suite à l'arrêt précité.

Dans son avis de 2015, la CNPD a passé en revue les sujets évoqués dans l'avis précité à la lumière des dispositions afférentes du projet de loi avisé.

La CNPD a noté que le projet de loi examiné n'introduisait aucune exception pour ce qui est des communications soumises au secret professionnel, ni au niveau de la conservation elle-même, ni au niveau de l'accès aux données. Pour cette raison, la Commission nationale a réitéré sa proposition de son avis de 2014 d'aligner le régime de l'accès aux données issues de la conservation à celui existant en matière d'écoutes téléphoniques pour ce qui est des aménagements en matière de communications couvertes par le secret professionnel.

En ce qui concerne la conservation des données qui a été fixée à 6 mois, la CNPD s'était posé la question de savoir si une durée de conservation encore plus courte ne pourrait pas être envisagée étant donné que la directive 2006/24, qui avait prévue une durée minimale de 6 mois, avait été déclarée invalide.

La Commission nationale a noté avec satisfaction que l'article 5-1 de la loi modifiée du 30 mai 2005 imposait désormais que les données soient conservées sur le territoire de l'UE et que les sanctions en matière d'abus, prévues par les articles 5 paragraphe (6) et 9 paragraphe (6), avaient été alourdies. En revanche, la CNPD a regretté que, contrairement à ce qu'elle avait suggéré dans ses avis n°85/2010 du 26 avril 2010 et n°214/2014 du 13 mai 2014, le projet de loi ne prévoyait pas la nullité de la preuve obtenue moyennant une violation de la législation sur la rétention des données de télécommunication.

2.2.7 Introduction d'une subvention de loyer

La CNPD a avisé les amendements gouvernementaux au sujet du 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 et du projet de règlement grand-ducal fixant les conditions et modalités d'octroi de la subvention de loyer prévue par l'article 14quinquies de la loi modifiée du 25 février 1979 concernant l'aide au logement,

approuvés par le Conseil de Gouvernement dans sa séance du 30 avril 2015.

L'autorité de protection des données a émis son premier avis relatif à ce projet de loi en date du 21 juillet 2014. Dans son nouvel avis, elle a limité ses observations aux questions traitant des aspects portant sur la protection des données. De manière générale, la CNPD a salué la démarche des auteurs d'avoir pris en compte et intégré la plupart des recommandations de la CNPD dans les nouveaux projets de loi et de règlement grand-ducal tels qu'amendés. Cependant, il restait certains points sur lesquels elle a émis ses observations.

En ce qui concerne l'amendement 3 du projet de loi, la CNPD a noté avec satisfaction que la nouvelle procédure prévue ne repose plus sur un accès direct du Ministère du logement aux fichiers des administrations concernées, mais bien sur un accès sur demande, ce qui apparaît davantage conforme aux principes de nécessité et proportionnalité. Elle a cependant suggéré d'utiliser la formulation suivante : « L'accès prend la forme d'une communication des données (…) » à la place du mot « échange ». En effet, ce dernier terme laisse penser que la transmission des données s'opérerait dans les deux sens, alors qu'elle ne se fera en réalité que depuis les administrations concernées vers le gestionnaire en charge du dossier au sein du Ministère du Logement.

Dans le même ordre d'idées, la CNPD a proposé de modifier le libellé à l'endroit de l'alinéa 1 du premier paragraphe en utilisant les termes « peuvent recevoir communication des données » à la place de la formulation « peuvent accéder aux données » utilisée à l'alinéa 1 du premier paragraphe.

Le nouvel alinéa 4 prévoyait un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. La CNPD a noté que cette procédure de traçage des accès était également précisée dans le projet de règlement grand-ducal, ce qui peut apparaître quelque peu redondant. Les deux dispositions pourraient dans ce cas être regroupées dans un seul paragraphe de la loi.

Quant à l'amendement 4 du projet de règlement grand-ducal, la CNPD a suggéré de remplacer la formulation du paragraphe (1) suivant laquelle [le ministre] « a la qualité de responsable dudit accès » par la phrase suivante : « Il a la qualité de responsable du traitement » pour des raisons de cohérence avec l'article (2) lettre (n) de la loi du 2 août 2002.

2.2.8 Casier judiciaire

Faisant suite à une demande du Ministère de la Justice, la CNPD a avisé :

- le projet de loi n°6820 portant modification 1) de la loi du 29 mars 2013 relative à l'organisation du casier et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne, 2) du Code d'instruction criminelle, 3) du Code pénal,

- le projet de règlement grand-ducal fixant la liste des administrations et personnes morales de droit public pouvant demander un extrait du casier avec l'accord de la personne concernée.

L'un des objectifs principaux des textes analysés était d'adresser les principales problématiques rencontrées après l'entrée en vigueur de la loi du 29 mars 2013. La suppression du bulletin n°3 résultant de cette loi a eu pour effet une extension des inscriptions des condamnations figurant au bulletin n°2. Cette extension avait fait l'objet de vives critiques, car elle pouvait notamment mener à une discrimination potentielle d'un demandeur d'emploi luxembourgeois vis-à-vis d'un demandeur d'emploi de nos pays voisins. En effet, dans certains cas, le « nouveau » bulletin luxembourgeois n°2 renseignait sur des condamnations qui n'auraient pas figuré au bulletin d'un demandeur d'emploi étranger. Le bulletin de ce dernier, ayant subi les mêmes condamnations, pouvait en effet présenter une mention « néant ».

A part adresser ces problèmes spécifiques, les textes analysés ont également introduit une réforme en profondeur du casier judiciaire. Cette dernière se composait notamment d'une introduction de cinq nouveaux bulletins dont la délivrance était directement liée à leur finalité, des nouvelles modalités de délivrance des bulletins, d'une liste des destinataires des bulletins revue à la baisse, d'un régime d'accès limité, de durées de conservation plus courtes et de l'introduction d'une sanction pénale en cas de non-respect des dispositions de la loi.

La Commission nationale a limité ses observations aux questions traitant des aspects portant sur la protection des données. En ce qui concerne la durée de conservation des inscriptions au casier, la CNPD a estimé qu'il serait plus approprié de tenir compte de la durée de vie effective de la personne concernée au lieu d'effacer les données 100 ans après la naissance. Une telle solution éviterait des dates de conservation le cas échéant longues et présenterait le net avantage d'uniformiser la solution applicable à toutes les personnes concernées.

La CNPD a noté avec satisfaction que :

- la demande formelle du Conseil d'Etat, insistant sur l'introduction de finalités pour lesquelles la délivrance d'un extrait du casier judiciaire pouvait être demandée, a été suivie ;

- les auteurs du texte aient prévu dans la plupart de ces nouveaux bulletins un effacement des inscriptions des condamnations mineures après un délai de cinq ans (ou trois ans pour le bulletin n°4) à partir de certaines dates prédéterminées ;

- la CNPD ait été suivie en ce qui concerne sa recommandation relative à la transparence à adopter envers les personnes concernées dans le contexte des délivrances automatiques des bulletins du casier judiciaire.

Quant au bulletin n°2, la CNPD a estimé que la revue à la baisse du nombre des administrations pouvant demander un extrait du casier ainsi que la limitation stricte des cas de délivrance liés à des finalités bien définies contribuaient à une transparence plus élevée pour toutes les personnes concernées.
Alors que la délivrance des bulletins n°1 et n°2 est limitée aux destinataires se trouvant inscrits sur une liste préétablie, le bulletin n°3 peut être délivré à la personne concernée elle-même ou à un tiers muni d'une procuration valide. Dans le cadre d'une finalité de recrutement, la production du

bulletin n°3 peut être exigée par l'employeur, mais il faut qu'elle soit faite par écrit et il faut qu'elle soit spécialement motivée par rapport aux besoins spécifiques du poste. Dans le cadre de la finalité portant sur la gestion du personnel, l'employeur ne peut demander la remise du bulletin n°3 que lorsque des dispositions légales le prévoient ou en cas de nouvelle affectation justifiant un nouveau contrôle de l'honorabilité par rapport aux besoins spécifiques du poste.
Par ailleurs, pour ce qui concerne les deux finalités pré-mentionnées, la durée de conservation est d'un mois au maximum. Dans son avis, la Commission nationale a félicité les auteurs pour la revue à la baisse du temps de conservation des données, mais avant tout pour l'encadrement strict et très protecteur des droits des personnes concernées. Ces nouvelles dispositions contraignantes devraient contribuer à éliminer significativement toutes les pratiques qui ont vu le jour au cours de ces dernières années en ce qui concerne la production d'extraits du casier judiciaire.
La CNPD a par ailleurs noté que la recommandation de son avis du 25 octobre 2012 avait été intégrée dans le projet de loi analysé. Celle-ci concernait la problématique de la visibilité accrue des condamnations relatives à la sécurité routière au moyen d'un nouveau bulletin, le bulletin n°4. Ce dernier renseigne toutes les décisions inscrites au bulletin n°3, ainsi que toutes les condamnations prononçant une interdiction de conduire. En effet, la CNPD avait suggéré d'introduire des dispositions spécifiques « pour le recrutement du personnel appelé à exercer leur fonction au volant de véhicules automoteurs ».

La Commission nationale a encore noté que l'article 9, qui a introduit une sanction en cas de non-respect des dispositions analysées dans l'avis, permettra de sensibiliser toutes les personnes physiques ou morales recevant des extraits du casier judiciaire à respecter les dispositions du projet de loi analysé. La protection de la vie privée des personnes concernées s'en trouve efficacement augmentée.

2.2.9 Echange de données à caractère personnel entre le Luxembourg et les Etats-Unis

Suite aux demandes du Ministère de la Justice, la CNPD a avisé

- 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.

Les deux projets de loi analysés, amendés le 10 avril 2015 par le gouvernement, portent sur l'approbation d'accords prévoyant des échanges en matière policière et judiciaire de données à caractère personnel du Luxembourg en direction des Etats-Unis d'Amérique et vice versa.

La CNPD a noté dans son avis que tant le memorandum, que l'accord crime grave présentaient beaucoup d'imprécisions sur un bon nombre de questions ayant trait à la protection des données. La CNPD s'est interrogée sur la conformité des traitements de données, visés par les deux accords, à la législation européenne et nationale sur la protection des données.

Le fait que beaucoup de questions seront régies principalement, voire exclusivement par le droit interne des Etats signataires, laissait persister des doutes quant à l'existence de garanties suffisantes en matière de protection des données et de la vie privée des citoyens.

La CNPD a regretté par ailleurs qu'elle n'ait pas été consultée lors de la phase de négociation, respectivement avant la signature des accords, alors que les projets de lois ont pour objet d'approuver deux accords signés qui ne peuvent plus être modifiés à moins de les renégocier avec les Etats-Unis d'Amérique.

2.2.10 Protection internationale et protection temporaire

La CNPD s'est prononcée au sujet du projet de loi n°6779 (1) relatif à la protection internationale et à la protection temporaire, (2) modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat, la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration et la loi du 28 mai 2009 concernant le Centre de Rétention, et (3) abrogeant la loi modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection. Ce projet de loi a pour objectif principal de transposer en droit national la directive 2013/32/UE relative aux procédures d'asile et d'abroger la loi modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection. La directive quant à elle s'inscrit dans le processus de communautarisation de l'asile (Régime d'Asile Européen Commun – « RAEC »).

La Commission nationale a limité ses observations aux questions traitant des aspects portant sur la protection des données. Les procédures d'octroi et de retrait de la protection internationale et de la protection temporaire entraîneront la tenue d'un fichier y afférent auprès de la Direction de l'Immigration du Ministère des Affaires étrangères et européennes. Pour cette raison, le projet de loi a prévu des dispositions qui concernaient spécifiquement le traitement de données à caractère personnel (article 80 du projet de loi). La Commission nationale a également soulevé d'autres points du projet de loi, qui ont trait à la vie privée et au traitement de données des demandeurs de protection internationale et qui suscitaient des commentaires.

La CNPD a recommandé notamment :

- d'encadrer dans un texte légal les dispositions spécifiques ayant trait au traitement de données à caractère personnel ;

- d'adapter le texte de loi afin qu'il définisse les modalités et conditions précises des transmissions de données entre le ministre et d'autres instances ;

- de prévoir une disposition fixant la durée de conservation.

Les activités en 2015

Quant à la surveillance des demandeurs au moyen d'un bracelet électronique, la CNPD a estimé nécessaire de renoncer à toute référence au port d'un tel bracelet dans le projet de loi à défaut d'un cadre législatif qui fixe les conditions et les modalités du recours à une telle mesure.

2.2.11 Espace ferroviaire unique européen

La Commission nationale a avisé l'avant-projet de loi portant transposition de la refonte du 1er paquet ferroviaire et modifiant :

- la loi modifiée du 10 mai 1995 relative à la gestion de l'infrastructure ferroviaire ;
- la loi modifiée du 11 juin 1999 relative à l'accès à l'infrastructure ferroviaire et à son utilisation ;
- la loi modifiée du 22 juillet 2009 relative à la sécurité ferroviaire et
- la loi du 3 août 2010 sur la régulation du marché ferroviaire.

Elle a limité ses observations aux questions traitant des aspects portant sur la protection des données.

Dans son avis, la Commission nationale s'est interrogée sur la nécessité de publier des données à caractère personnel (nom, adresse, date de naissance, coordonnées des personnes de contact) concernant les examinateurs dans un registre national, alors que ni la directive 2012/34/UE n'impose une telle publication, ni aucun élément du texte n'amène à conclure qu'une telle publication serait absolument nécessaire.

La CNPD a par ailleurs noté qu'il ne résultait pas clairement du texte qui est désigné comme responsable du traitement de ce registre et a suggéré de le préciser.

Selon le projet de loi, les données intéressant le bilan d'examen sont conservées pendant dix ans par l'examinateur. La CNPD s'est demandé pourquoi ces données sont conservées par les examinateurs et non par le responsable du traitement. La CNPD a aussi estimé que la durée de conservation paraissait trop longue. Toutefois, en l'absence de justifications plus précises, elle n'était pas en mesure d'apprécier si ce délai respectait le principe de nécessité et de proportionnalité.

2.2.12 Modernisation du droit de la faillite

Dans son avis sur le projet de loi n°6539 relatif à la préservation des entreprises et portant modernisation du droit de la faillite, la CNPD a limité ses observations aux questions traitant des aspects portant sur la

protection des données, soulevées plus particulièrement dans le chapitre 2 du projet de loi.

L'objectif principal du projet de loi est de réformer et de moderniser le droit de la faillite au Luxembourg, notamment par l'introduction de toute une série de mesures aidant à préserver les entreprises en difficulté. Les auteurs ont prévu plusieurs mesures qui incluent notamment (i) la collecte d'informations d'entreprises en difficultés (c'est-à-dire un volet prévisionnel), (ii) la mission de conciliation ainsi que l'accord amiable (c'est-à-dire un volet réorganisationnel sans ouverture de procédure judiciaire) et (iii) les procédures judiciaires de réorganisation.

La CNPD a renoncé dans son avis à se prononcer sur ce troisième volet. Ceci incluait également la nouvelle procédure de dissolution administrative sans liquidation, qui devra être déclenchée par l'intervention du Procureur d'Etat.

Quant à la collecte des données sur les entreprises en difficulté, il ne résultait pas clairement du texte si les auteurs avaient effectivement souhaité conférer la qualité de responsable du traitement au Comité de conjoncture ou non. De plus, il ressortait du texte que certaines données à caractère personnel seraient également transmises à et traitées par la Cellule d'Evaluation des Entreprises en Difficulté (CEvED).

En effet, au vu des ambiguïtés et incertitudes existantes quant au rôle de chacun des différents intervenants cités ci-avant, la Commission nationale a estimé nécessaire de préciser dans le texte les rôles respectifs de chacun avec précision.

La CNPD a noté que l'article 5 du projet de loi ne précisait pas du tout quelles données ou catégories de données pouvaient effectivement être collectées et traitées. Le texte ne précisait pas non plus l'origine des données collectées et traitées, ni les opérations de traitement envisagées. En effet, il faudrait notamment préciser et énumérer (i) à quelles données précises, contenues dans des fichiers étatiques, les responsables du traitement pouvaient avoir accès (p.ex. Centre commun, administrations fiscales), (ii) quelles données proviendraient directement des intéressés et (iii) quelles données proviendraient d'autres sources (tribunaux, greffes, etc.).

En ce qui concerne la création d'une base légale pour la transmission de certains jugements au Comité de conjoncture, la CNPD a recommandé de rajouter une disposition qui précise que le Comité de conjoncture ne pourra pas transmettre ou communiquer ces données à caractère personnel à des tiers non autorisés, c'est-à-dire qui ne sont pas impliqués ou visés dans les procédures prévues par le projet de loi.

La CNPD a finalement commenté la liste des protêts. Dans un souci d'équilibre et de mise en balance des intérêts respectifs en cause, à savoir le risque de divulgation d'informations sensibles relatives aux débiteurs, d'une part, et l'intérêt des personnes morales ou physiques à vouloir se protéger contre des entreprises en difficulté, d'autre part, elle a accueilli favorablement la modalité de publication limitée, dans la mesure où les intéressés devaient se déplacer pour prendre connaissance de la liste des protêts auprès des greffes des tribunaux. Pour cette raison, la CNPD a suggéré de rajouter en fin de phrase du dernier paragraphe de l'article 88 les termes « sur place », pour éviter toute ambiguïté relative aux publications par d'autres moyens. En effet, une telle disposition limiterait la diffusion de ces données au grand public notamment via Internet et permettrait dès lors de réduire sensiblement le risque de stigmatisation de la partie défaillante, tout en maintenant le droit des parties intéressées d'être informées sur les inscriptions récentes de la liste des protêts.

2.2.13 Reconnaissance des qualifications professionnelles

La Commission nationale a avisé le projet de loi n°6893 et le

Les activités en 2015

règlement grand-ducal relatifs à la reconnaissance des qualifications professionnelles. Elle a limité ses observations aux questions traitant des aspects portant sur la protection des données.

La CNPD a suggéré de faire référence à la loi modifiée du 2 août 2002 au lieu de la directive 95/46/CE dans le projet de loi. La référence à cette loi est d'autant plus importante, alors que l'article 56 du projet de loi prévoit entre autres des échanges de données relatives à des sanctions pénales entre autorités. Elle a aussi recommandé de supprimer la référence à la directive 2002/58/CE qui est transposée en droit national par la loi modifiée du 30 mai 2005 relative à la protection de la vie privée dans le secteur des communications électroniques, alors qu'elle ne comprenait pas en quoi le projet de loi examiné touche le champ d'application de ce texte.

Concernant le registre des titres professionnels, la CNPD a estimé qu'il ne résultait pas clairement du texte qui était le responsable du traitement. Pour cette raison, la CNPD a suggéré de désigner comme responsable du traitement le ministre ayant l'Enseignement supérieur dans ses attributions, en précisant que les données étaient fournies par les autorités compétentes des différentes professions réglementées.

L'article 59 prévoit la création du registre des titres professionnels « en vue de l'accès aux professions réglementées… » et fait référence aux informations qui servent de base pour l'émission des cartes professionnelles européennes, telles que prévues par la directive européenne 2013/55/UE. L'article fait donc ressortir deux catégories de finalités. Pour une meilleure lisibilité du texte, la CNPD a recommandé de regrouper ces deux finalités au paragraphe 1er de l'article 59 et d'inverser les paragraphes (2) et (3), afin de préciser d'abord les finalités du traitement des données, ensuite le principe de la création d'un fichier et enfin la provenance des données.

La Commission nationale a par ailleurs suggéré d'avoir recours au terme de « fichier » afin de s'aligner sur la terminologie utilisée dans la loi modifiée du 2 août 2002. Elle a précisé qu'il n'était pas souhaitable d'utiliser deux termes différents, à savoir « registre » et « banque de données ».

En ce qui concerne la publicité et de la transparence, la CNPD a considéré comme excessive et disproportionnée la divulgation au public de la date de naissance ainsi que de l'adresse, au cas où celle-ci renseignerait l'adresse privée. Elle a pourtant estimé nécessaire d'exclure des mesures de publicité la date de naissance, ainsi que l'adresse privée des professionnels, à moins que cette dernière se confonde avec l'adresse professionnelle.

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

Dans le cadre de la journée européenne de la protection des données, la CNPD, en collaboration avec l'APDL (Association pour la protection des données au Luxembourg) et « Security made in Lëtzebuerg », a organisé une conférence sur les défis à venir du projet de règlement européen en matière de protection des données, suivie d'une table ronde sur les questions d'analyse de risque notamment liées au Big Data. Suite aux mots de bienvenue de Mme Tine A. Larsen (Présidente de la CNPD) et de Mme Nathalie Sprauer (Présidente de l'APDL), M. Cédric Nedelec (Administrateur APDL) a donné une présentation intitulée « Nouvelle législation européenne sur la protection des données à caractère personnel : la révolution en matière de gouvernance ». Cette présentation a été suivie par une table ronde avec la participation de Mme Florence Thomas (Inspection générale de la sécurité sociale), M. Thierry Petitgenet (CASES), M. Eric Krier (BEE SECURE), M. Pascal Steichen (CIRCL) et M. Alain Herrmann (CNPD).

Le 28 janvier est la date de la célébration de la Journée de la protection des données, organisée annuellement depuis 2007 par le Conseil de l'Europe avec le soutien de la Commission européenne. L'objectif de cette journée est de sensibiliser les citoyens au sujet de leurs droits et devoirs dans le contexte de la protection de la vie privée et de la protection des données.

Cette date correspond à l'anniversaire de la signature le 28 janvier 1981 de la « Convention 108 » du Conseil de l'Europe, qui a été le premier instrument international juridiquement contraignant en la matière. Depuis plus de 30 ans, la loi vise à protéger tout citoyen contre l'utilisation abusive des données le concernant et à assurer la transparence quant à l'utilisation des fichiers et des traitements effectués à partir de ses données personnelles.

Le 7 février, la CNPD a également participé au « Safer Internet Day », qui a été célébré dans le monde entier sous le slogan « Tous ensemble pour un Internet meilleur » (« Let's create a better Internet together »).

2 Les activités en 2015

Il s'agit d'une initiative de la Commission européenne pour soutenir et connecter les citoyens à travers le monde, dans leur engagement pour une utilisation plus sûre des nouveaux médias. Célébré dans plus de 70 pays dans le monde entier, le « Safer Internet Day » a rapidement dépassé les frontières de l'Europe pour devenir au fil des ans un rendez-vous incontournable en matière d'éducation numérique. Au Luxembourg, BEE SECURE s'occupe de la coordination de cet événement.

L'autorité de protection des données luxembourgeoise a par ailleurs soutenu la campagne « Clever Cloud » de BEE SECURE, qui a choisi le thème du « cloud computing » pour sa campagne annuelle, car il est le reflet de l'évolution des usages des technologies de l'information dans nos sociétés. Toutefois, il est incompris par ses utilisateurs finaux. Pour le grand public, le cloud est une notion abstraite, bien loin de la réalité qu'en en font les acteurs de l'économie. La nouvelle campagne visait à informer le grand public de cette réalité en décryptant tant les aspects économiques, que technologiques et légaux. Cette campagne était aussi l'occasion de mettre en avant des entreprises du Luxembourg particulièrement innovantes dans le domaine. Différentes fiches thématiques (cadre juridique du cloud, partage de fichiers sur le cloud, droit à l'image, etc.) ont été publiées sur le site BEE SECURE.

Le 13 juin, Mme Michèle Feltz a participé à la quatrième édition de « Hack4Kids » au centre culturel de Sandweiler avec un atelier sur les données à caractère personnel. Plus d'une centaine d'enfants âgés de 7 à 12 ans étaient présents. L'événement était composé de quatre modules conçus par SECURITYMADEIN.LU en partenariat avec des professionnels de l'éducation et des experts en sécurité de l'informatique (CIRCL, Code Club Luxembourg, CNPD, POST, LTETT) :

- Création de modèles en 3D : initiation à la manipulation de modèles sur « Sketch-Up » (LTETT).
- Organisation d'un jeu sur le filtrage de données par la POST.
- Organisation d'un atelier sur les données à caractère personnel (CNPD).
- Coding sur Scratch : animation de personnages et création d'un dialogue (Code Club).

En parallèle, les enfants ont également pu découvrir d'autres activités ludiques telles que le light-painting, une technique de prise de vue photographique, ainsi que le makey-makey, une activité animée par BEE SECURE, permettant aux enfants de jouer au piano avec des bananes. A la pause, un « human programming challenge » (une sorte de flashmob) a été organisé et les enfants ont pu « danser » sur un pseudo-code de manière à comprendre la façon dont fonctionne un ordinateur.

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 2015, le collège a accordé 27 interviews aux organes de presse. Parmi les thèmes traités, citons la réforme du cadre juridique européen en matière de protection des données, l'arrêt « Schrems », le dossier de soins partagé, le casier judiciaire, la fuite de données de la société VTECH 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

2 Les activités en 2015

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.).

Quant au grand public, il 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 ou demande de renseignement complémentaire, voire pour déposer une plainte.

La Commission nationale a par ailleurs élaboré des fiches pratiques sur le Privacy by Design[6], sur les webcams et les objets connectés[7] en collaboration avec *Securitymadein.lu*.

[6] http://www.cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/index.html
[7] http://www.cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/webcams-objets-connectes/index.html

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 21 janvier, Mme Tine A. Larsen, présidente de la CNPD, a participé à la conférence « Computers, Privacy and Data Protection » à Bruxelles. Elle a assuré la modération du panel « User's control over their data : is prior consent the best way to monitor ? » auquel ont participé Mme Julie Brill (Federal Trade Commision des Etats-Unis), M. Finn Myrstad (Norwegian Consumer Council), Mme Marie-Charlotte Roques-Bonnet, (Microsoft) et M. Wojciech Rafat Wiewiórowski, (EDPS).

Le 6 mars, M. Thierry Lallemang, membre effectif de la CNPD, et M. Christian Welter du service juridique ont présenté les principes de la protection de la vie privée au travail lors d'une séance d'information auprès de l'ABBL (Association des Banques et Banquiers, Luxembourg).
Le 13 mai, M. Thierry Lallemang a fait un exposé au sujet de la protection des données dans le secteur communal à l'assemblée générale de l'Association des Secrétaires Communaux du Grand-Duché de Luxembourg (ASC).

Le 22 mai, M. Alain Herrmann du service informatique et nouvelles technologies a participé au premier « Information Security Day » (ISED) avec une présentation sur le « privacy by design ». Cet événement a été organisé par l'Université du Luxembourg et le Luxembourg Institute of Science and Technology (LIST).

Le 1er juin, Mme Michèle Feltz du service informatique et nouvelles technologies a fait un exposé sur la protection des données à une classe de 13ème du Lycée technique d'Esch (section technicien informatique) dans le cadre du cours « sécurisation des données ».

Les 8 et 9 juin, M. Thierry Lallemang et M. Alain Herrmann ont donné des cours de formation à l'Institut National d'Administration Publique (INAP)

Le 19 juin, Georges Wantz, membre effectif de la CNPD, est intervenu à la conférence de l'ABBL sur l'échange automatique d'informations fiscales. Sa présentation a porté sur le rôle des banques en tant que responsables du traitement dans le cadre de l'échange automatique de données.

Le 26 juin, l'OLDE (Observatoire Luxembourgeois de Droit Européen) a organisé une conférence intitulée « Internet : libertés et restrictions » dans la cité judiciaire. Le mot de bienvenue de M. Marc Jaeger (Président de l'OLDE) et l'allocution de M. Félix Braz (Ministre de la Justice) ont été suivis par des exposés sur l'état de la jurisprudence au niveau européen et national par :

- M. Dean Spielmann (Président de la Cour Européenne des Droits de l'Homme),
- M. François Biltgen (Juge à la Cour de Justice Européenne) et
- M. Max Braun (Premier substitut du procureur d'Etat à Luxembourg).

La conférence a été clôturée par une table ronde dirigée par M. Jeannot Nies (Membre du comité de l'OLDE) avec la participation de :

- M. Rosario Grasso (Bâtonnier du barreau de Luxembourg),
- M. Mark D. Cole (Professeur à l'Université de Luxembourg),
- Mme Tine A. Larsen (Présidente de la CNPD) et
- M. Laurent Moyse (Journaliste).

Le 30 juin, l'Union Internationale des Avocats (UIA) a organisé un colloque à Luxembourg sur le thème de « l'homme augmenté : de la science-fiction à la réalité ».

2 Les activités en 2015

Un sujet bouleversant qui remet en question la notion même d'humanité et qui soulève des problèmes éthiques, moraux, politiques et philosophiques sans précédent. L'événement a réuni plus de 150 participants dont certains provenaient de l'étranger. Après les mots de bienvenue par Mme Tine A. Larsen et Me Rosario Grasso, Gaspard Koenig, philosophe français et directeur du think-tank GenerationLibre a parlé des problématiques liées aux NBIC (Nanotechnologies, Biotechnologies, Intelligence artificielle et Sciences cognitives). Il a ouvert le débat par une question audacieuse : le transhumanisme est-il un humanisme ? Dans un discours riche en références scientifiques et culturelles, Monsieur Koenig a opposé l'individu 2.0 qui émerge des laboratoires californiens à l'individu 1.0 que nous sommes, nous invitant à ne pas nier la mutation de notre humanité, tout en laissant une place au hasard, qui fait notre humanité. Fabrice Pakin, entrepreneur dans le domaine de l'e-santé et fondateur de la startup Ignilife, est intervenu sur le thème de l'intelligence des algorithmes au service de la prévention médicale. Confiant en l'avenir de l'homme biologique, il a exposé les bienfaits d'une médecine prédictive, participative et personnalisée que la technologie met à disposition de tous.

Les 8 et 9 juillet, M. Alain Herrmann est intervenu aux journées eHandwierk. La Chambre des Métiers en coopération avec le Ministère de l'Economie, la CNPD, Luxinnovation, l'Union européenne de l'artisanat des petites et moyennes entreprises et Entreprise Europe Network ont proposé trois séances sur le sujet « Le cloud computing dans les PME artisanales ».

Le 11 septembre, M. Thierry Lallemang a donné une formation d'une journée à l'Ecole supérieure du travail sur la protection des données.

Le 23 septembre, M. Alain Herrmann a donné un workshop sur le thème « Privacy by Design » à la Fédération des Hôpitaux Luxembourgeois (FHL).

Le 30 septembre, M. Thierry Lallemang a participé à la conférence de la Chambre des Métiers intitulée « Quelle surveillance possible sur le lieu de travail ? Mode d'emploi pour les employeurs. ». Dans le but d'apporter une réponse pratique aux préoccupations légitimes de tout employeur du secteur artisanal d'opérer valablement et dans le respect de la loi une surveillance sur le lieu du travail, M. Lallemang a présenté les règles à connaître dans le domaine et les procédures mises en place par la CNPD afin de faciliter certaines demandes d'autorisation. Le cabinet Arendt&Medernach, représenté par Maître Louis Berns et Maître

Héloïse Bock, a complété le mode d'emploi de l'employeur en déterminant des situations très concrètes où il est possible d'utiliser les outils de surveillance, et notamment pour sanctionner le salarié.

Du 7 au 8 octobre, M. Georges Wantz a participé au panel « Economics of PETs (Privacy enhancing technologies) » lors de l'« Annual Privacy Forum » qui s'est tenu à Luxembourg. Cette conférence a été organisée par l'ENISA (Agence Européenne chargée de la sécurité des réseaux et de l'information), la « DG Connect » de la Commission européenne et l'Universite du Luxembourg.

Le 27 octobre, M. Tine A. Larsen participe à un workshop dans le cadre du projet PHAEDRA II visant à améliorer la coopération entre les autorités de protection des données. Le panel auquel la présidente de la CNPD a participé était intitulé « Costs, languages, human resources – how to overcome practical barriers for efficient cooperation between DPAs ? ».

Les 1 et 2 décembre 2015, M. Mickaël Tome du service juridique de la CNPD a participé au panel « Principe Once Only et protection des données : ennemis ou amis ? » à la Conférence européenne sur l'administration électronique (eGovernment) intitulée « Des services publics simples, sûrs et transparents ». Organisée par le Centre des technologies de l'information de l'Etat (CTIE) à la Maison du Savoir, cette conférence a donné l'occasion à des professionnels du secteur de l'administration électronique d'horizons très divers et provenant de toute l'Europe de partager leurs projets, leurs meilleures pratiques et leurs expériences dans le domaine de l'administration électronique. Les intervenants, des experts reconnus dans leur domaine, ont présenté des sujets-clés de la modernisation administrative en Europe.

Le 3 décembre, Mme Tine A. Larsen a présenté les avancées du groupe de travail européen « Article 29 » lors de la deuxième conférence annuelle sur la protection des données. Meetincs a réuni à sa tribune des experts qui ont fait le tour d'horizon de sujets d'actualité en la matière.

Le 8 décembre, Mme Tine A. Larsen a participé à la conférence « The Digital Single Market – What's in it for us ? » à Copenhague (Danemark). La présidente de la CNPD est intervenue au panel « Data protection, trust and e-privacy » avec M. Marc Hemmerling (ABBL), M. Henning Mortensen (Senior Policy Advisor, DI Digital), Mme Pernille Tranberg (Advisor, Digital Identity) et Mme Rosa Barcelo (Senior Expert, DG Connect).

Le 10 décembre, le Luxembourg Institute of Science and Technology a organisé une conférence sur le thème de la sécurité de l'information dans

Les activités en 2015

le secteur de la santé. Parmi les secteurs les plus impactés par les risques liés à la sécurité de l'information, celui de la santé est particulièrement critique et complexe quant à la nature des données et des échanges en jeu. Pour cette raison, dans la continuité de dix années de travaux communs, le Ministère de l'Economie (son GIE Smile) et le Luxembourg Institute of Science and Technology ont présenté les résultats du projet HEEL (HEalth modELing) de modélisation et d'outillage des bonnes pratiques de sécurité de l'information, mise en œuvre avec quelques services-clés du secteur (analyse biomédicale, radiologie, urgence…). Ces travaux étaient l'occasion d'une réflexion sur les perspectives nationales qui permettront de sensibiliser et d'outiller les acteurs du domaine et ainsi relever le défi national face au nouveau règlement européen en matière de protection des données. Dans sa présentation, M. Alain Herrmann a fait le lien entre ce nouveau règlement et la sécurité de l'information dans le domaine de la santé.

Le 10 décembre, Mme Tine A. Larsen a participé à la conférence organisée par la Commission consultative des Droits de l'Homme avec Dean Spielmann sur le thème : « La Cour européenne des Droits de l'Homme : son importance et ses défis ».

Le 10 décembre, M. Georges Wantz a donné une présentation sur le « privacy by design » à la conférence « Rétrospectives 2015 » de l'Association pour la protection des données au Luxembourg (APDL).

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 2015, la Commission nationale a participé à plus de 146 réunions avec les acteurs du secteur public et à 106 réunions avec ceux du secteur privé. Cela représente une augmentation de plus de 49% par rapport à l'année précédente. Elle était, entre autres, en relation avec les ministères, administrations et organes publics suivants :

- Ministère des Affaires étrangères : conservation des données, SATMED, évaluation Schengen ;
- Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse : Edusphere, chèque-service accueil ;
- Service des Communications et des Médias : réforme du cadre européen sur la protection des données, e-gouvernment, Trusted Third Party ;
- Ministère de la Culture - Archives Nationales : archivage ;
- Ministère du Développement durable et des Infrastructures - Département des Transports : radars automatiques, organisation du secteur des services de taxis, échange d'informations concernant les infractions en matière de sécurité routière ;
- Ministère du Développement durable et des Infrastructures - Administration de l'environnement : subventions ;
- Ministère de l'Enseignement et de la Recherche : interconnexion des banques de données ;
- Ministère de l'Economie : Interpol, International Mass Market Fraud Working Group ;
- Ministère de la Fonction publique et de la Réforme administrative : réformes dans la fonction publique ;
- Ministère de la Justice : rétention des données, whistleblowing ;
- Ministère de la Santé : accès du patient aux données électroniques ;
- Institut luxembourgeois de régulation : protection des données dans le secteur des communications électroniques ;
- Commission de Surveillance du Secteur Financier : impact du futur règlement européen relatif à la protection des données sur le secteur financier, législations européennes dans le domaine financier prévoyant la collecte de données personnelles (EMIR, MiFID, MiFir, ...) ; les systèmes d'informations et surveillance des PSF de support ;
- Centre des technologies de l'information de l'Etat (CTIE) : banques de données de l'Etat, identifiant unique ;
- Fonds National de Solidarité : transfert de certaines données ;
- Institut national d'administration publique (INAP) : plans de formation ;
- Agence pour le développement de l'emploi (ADEM) : mise en œuvre de projets informatiques, réforme de l'ADEM ;
- Parquet de Luxembourg : cybercriminalité ;
- Police Grand-Ducale : vidéosurveillance ;
- Haut-commissariat à la protection nationale, ANSSI : sécurité de l'information ;
- Administration des Contributions directes ;
- Conseil d'Etat : divers dossiers communs relatifs à la protection des données.

Parmi les entreprises multinationales implantées au Luxembourg, la Commission nationale a notamment rencontré Amazon, eBay, Skype 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 continue 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 » (ou PIA – Privacy Impact Assessment) dans le cadre du dossier de soins partagés (DSP). Les objectifs de cette démarche consistent à évaluer le niveau de sécurité du système d'information et le niveau de protection des données à caractère personnel ayant vocation à être traitées par l'intermédiaire du DSP, notamment les données de santé des patients. Elle a également poursuivi sa coopération avec la Fédération des Hôpitaux Luxembourgeois pour promouvoir les bonnes pratiques en matière de protection des données au niveau du fonctionnement quotidien des hôpitaux. Le collège de la CNPD participe par ailleurs aux réunions du comité de pilotage du CNS et a rencontré des représentants du Luxembourg Institute of Health (CRP-Santé) en 2015.

2.4.2 Demandes de renseignements

La Commission nationale a reçu 2.361 demandes de renseignement en 2015. Depuis sa création, l'autorité de protection des données n'a jamais reçu autant de requêtes en une seule année. Dans la majorité des cas, il s'agissait de demandes relatives aux formalités à accomplir pour mettre en œuvre un traitement de données ou de questions juridiques relatives à la législation.

Elle a répondu à 2.021 demandes par téléphone et à 340 par écrit. Presque la moitié des demandes émanaient d'entreprises. Les autres provenaient d'administrations publiques, d'avocats et de citoyens qui s'adressent aussi régulièrement à la Commission nationale.

2.5 Recherche

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.

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 2015 à 47 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 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 » ;

- 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 ;

- du séminaire européen d'échanges d'expériences dans le traitement des cas pratiques (« Case Handling Workshop ») ;

- de la conférence de printemps des commissaires européens à la protection des données ;

- de la conférence internationale des commissaires à la protection des données et de la vie privée.

Par ailleurs, les membres de l'autorité de contrôle de l'article 17 (comprenant deux membres de la CNPD) ont participé 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

Les activités en 2015

des données et de promouvoir une application harmonisée de la directive dans les 28 États membres de l'Union européenne.

Parmi les sujets traités par le groupe de travail en 2015, citons :

- la révision du cadre légal européen de la protection des données ;
- l'arrêt de la Cour de Justice de l'UE reconnaissant un droit à l'oubli (arrêt « Costeja ») ;
- la révision du cadre légal européen de la protection des données ;
- l'invalidation des accords « Safe Harbor » ;
- la rétention des données ;
- la coopération entre les autorités de protection des données ;
- les cookies ;
- le PNR européen ;
- l'échange automatique de données personnelles à des fins fiscales ;
- les conditions d'utilisation de Facebook ;
- les drones ;
- les BCR pour les sous-traitants ;
- le cloud computing ;
- le déréférencement dans les moteurs de recherche ;
- l'indépendance des autorités de protection des données.

Les principaux documents de travail de 2015 du groupe sont résumés ci-dessous et peuvent être téléchargés dans leur version complète sur Internet[8].

2.6.1.1 Le système européen d'échange de données des dossiers passagers (PNR européen)

Après les attaques intervenues à Paris les 7 et 8 janvier 2015, la possibilité de mettre en place un système PNR européen a de nouveau été évoquée dans l'actualité internationale.

Les données des dossiers passagers (ou « PNR » - « Passenger Name Record ») sont des données personnelles collectées auprès des passagers aériens au stade de la réservation commerciale. Elles permettent d'identifier, entre autres : l'itinéraire du déplacement, les vols concernés, le contact à terre du passager (numéro de téléphone au domicile, professionnel, etc.), les tarifs accordés, l'état du paiement effectué, le numéro de carte bancaire du passager, ainsi que les services demandés à bord tels que des préférences alimentaires spécifiques (végétarien, asiatique, cascher, etc.) ou des services liés à l'état de santé du passager.

[8] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/

Le G29, qui n'est, en principe, ni pour ni contre un tel système tant qu'il est conforme aux droits fondamentaux, a considéré dans un communiqué de presse du 5 février 2015 que l'ampleur et la nature indiscriminée du traitement de données dans le projet de PNR européen est susceptible de porter gravement atteinte au droit à la protection de la vie privée et aux données personnelles de tous les voyageurs, tel que défini aux articles 7 et 8 de la Charte des Droits Fondamentaux de l'Union Européenne.

Le groupe a relevé par ailleurs qu'un système PNR ne pourrait être acceptable que dans le cas où la nécessité d'une telle collecte était démontrée et le principe de proportionnalité respecté. Si la nécessité de mettre en place un système PNR européen était démontrée, des garanties suffisantes devraient accompagner ce dispositif afin d'en assurer la proportionnalité.

2.6.1.2 Echange automatique de données à caractère personnel à des fins fiscales

Le 4 février 2015, le G29 a fait une déclaration concernant l'introduction de mécanismes pour l'échange de données à caractère personnel à des fins fiscales et leur impact sur la protection de la vie privée.

L'échange d'informations est considéré comme un outil essentiel dans la lutte contre l'évasion fiscale. Il est nécessaire d'assurer que les conditions préalables à un traitement licite et équitable des données dans ce contexte sont respectées. La prévention de l'évasion fiscale est un objectif d'intérêt général et en même temps une activité qui a un impact sur la sphère privée de tous les citoyens. Les États doivent poursuivre un tel objectif dans le plein respect des droits fondamentaux des individus.

Les points essentiels de la déclaration du groupe de travail, qui s'adresse en premier lieu aux gouvernements nationaux et aux institutions européens, sont les suivants :

1. L'échange automatique des données personnelles à des fins fiscales devrait répondre aux exigences de protection des données, à savoir aux principes de limitation de la finalité et de la nécessité ;

2. Les Etats membres, qui conservent des immenses quantités de données qu'ils transmettent automatiquement à des fins fiscales, doivent être conscients qu'ils doivent faire face à des risques (de sécurité) élevés et que cet échange soulève

d'importantes questions en matière de responsabilité des autorités publiques ;

3. Le G29 confirme son approche qui consiste à continuer à fournir sa guidance afin d'augmenter les garanties en matière de protection des données dans ce domaine.

2.6.1.3 Enquête sur les témoins de connexion (« cookie sweep »)

Le 17 février 2015, le G29 a publié les résultats d'une enquête sur l'utilisation des cookies sur 478 sites web européens. Malgré une amélioration globale des informations fournies par les sites internet, le groupe de travail a constaté que les cookies étaient toujours souvent placés sans le consentement des internautes.

Les cookies permettent à un site web de reconnaître les préférences d'un utilisateur telles que ce dernier les a définies lors d'une précédente visite sur le même site. Ils peuvent faciliter l'utilisation ultérieure d'un site en gardant en mémoire les détails d'un compte, la langue choisie auparavant ou les achats antérieurs. Techniquement, un petit fichier texte au format alphanumérique (souvent chiffré) est déposé sur l'ordinateur de l'internaute par le serveur du site visité ou par un serveur tiers (régie publicitaire, service de web analytique, etc.).

Les autorités de protection des données européennes étaient préoccupées par le nombre élevé de cookies placés par les sites internet et par les dates d'expiration excessives des cookies. Pour cette raison, elles ont demandé aux opérateurs de sites web de poursuivre leurs efforts pour fournir de l'information pertinente aux internautes et pour obtenir un consentement valide pour l'utilisation des cookies.

Au Luxembourg, la loi du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques est applicable en la matière. En vertu de cette loi, qui est une transposition de la directive européenne 2002/58/CE (« ePrivacy »), les sites internet doivent informer les internautes et recueillir leur accord préalable avant de pouvoir placer des cookies sur leur ordinateur. Il existe toutefois quelques exceptions à ce principe d'opt-in. Celles-ci sont analysées en détail dans l'avis 2/02012 du G29.

Quelques résultats intéressants de l'étude :

- Plus de 16.000 cookies ont été placés au total (les sites de médias en ont placés 50 en moyenne).

- 22 sites en ont placés plus que le double de la moyenne (>100).

- 70% des cookies utilisées sont des « cookies tiers », c'est-à-dire des cookies créés par des sites web différents de celui visité par l'utilisateur. Plus de la moitié de ces cookies provient de seulement 25 domaines.

- La durée de vie moyenne d'un cookie était de 1 à 2 ans, 20% des cookies avaient une durée de vie de 2 à 5 ans et 374 avaient une date d'expiration supérieure à 10 ans. Il y en avait même 3 dont la date d'expiration était le 31 décembre 9999.

- 26% des sites n'ont pas du tout informé les internautes sur l'utilisation de cookies. Parmi ceux qui ont notifié les utilisateurs, la visibilité de l'information pourrait être améliorée dans 39% des cas. Dans la moitié des cas, les utilisateurs ont seulement été informés. Leur consentement n'a pas été demandé.

2.6.1.4 Position commune sur la réforme de la protection des données

Le 15 juin 2015, le Conseil de l'Union européenne est parvenu à trouver un accord sur le projet de règlement relatif à la protection des données. Les autorités de protection des données européennes, réunies dans le groupe de travail « Article 29 », ont salué le fait que les trois institutions européennes - la Commission, le Parlement et le Conseil - ont été prêtes à commencer les négociations en trilogue.

Dans ce contexte, le groupe de travail a adopté une position commune sur les points essentiels de la réforme (définitions, champ d'application, principes essentiels, droits des personnes concernées, compétences des autorités de protection des données et modèle de gouvernance) qui devraient être pris en compte par les institutions européennes.

L'avis a été transmis symboliquement aux représentants des trois institutions. Le groupe de travail a espéré que cette contribution aiderait à maintenir un niveau élevé de protection des données personnelles dans l'Union européenne[9].

[9] La partie 3.1. est consacrée à la réforme sur la protection des données.

Les activités en 2015

2.6.1.5 Utilisation de drones

Le 16 juin 2015, le groupe de l'Article 29 a publié un avis dans lequel il analyse le respect de la vie privée et de la protection des données personnelles dans le cadre de l'utilisation de drones.

À la lumière de l'intégration progressive des drones dans l'espace aérien civil européen et l'émergence de nombreuses applications de drones (loisirs, services, photographie, logistique, surveillance des infrastructures), il y a un réel besoin de se concentrer sur les défis qu'un déploiement à grande échelle de cette technologie pourrait avoir sur la vie privée des individus et les libertés civiles et politiques et d'évaluer les mesures nécessaires pour assurer le respect des droits fondamentaux et la protection des données.

En effet, des risques d'entrave à la vie privée peuvent se présenter avec l'utilisation de drones. Un de ces risques est le manque de transparence de ce type de traitement en raison de la difficulté de voir les drones de la terre ou de savoir quelles données sont collectées, à quelles fins et par qui.

En outre, la dextérité des drones et la possibilité d'interconnecter de multiples drones facilite encore plus leur capacité à atteindre des points de vue uniques. Les drones peuvent notamment contourner les obstacles et ne sont pas limitées par des barrières, des murs ou des clôtures. Ils peuvent facilement collecter un large éventail d'informations, même sans la nécessité d'une ligne de vue directe, pendant de longues périodes de temps et à travers une grande surface sans interruption. Les risques pour la vie privée sont encore plus élevés lorsque les drones sont utilisés à des fins répressives.

Afin de répondre à ces préoccupations, le G29 a noté qu'il faut remplir plusieurs obligations avant d'utiliser un drone. Il faut notamment demander une autorisation de l'aviation civile lorsque le droit national permet d'opérer un drone. Lorsque le traitement est légitime, il faut respecter les principes de limitation de la finalité, de minimisation des données et de proportionnalité. Les personnes concernées doivent également être informées du traitement effectué (principe de transparence). De même, il est nécessaire de mettre en oeuvre toutes les mesures de sécurité appropriées et de supprimer ou anonymiser les données personnelles qui ne sont pas strictement nécessaires.

En outre, le groupe de travail a recommandé d'adopter les principes de la protection de la vie privée dès la conception et de la protection de la vie privée

par défaut et d'utiliser l'outil du PIA (Privacy Impact Assessment) pour évaluer l'impact des drones sur la vie privée.

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 2015 à Seoul et à Berlin, le groupe a adopté des documents de travail sur :

- l'informatique vestimentaire (« wearables ») ;
- la responsabilisation des gouvernements lorsqu'ils accèdent à des données personnelles conservées par des entreprises privées ;
- l'analyse vidéo intelligente ;
- la localisation à partir des communications d'appareils mobiles.

Ces documents peuvent être téléchargés sur le site Internet du groupe de travail[10].

2.6.2.1 L'informatique vestimentaire (« wearables »)

Le « wearable computing » est un terme qui désigne des objets quotidiens, des vêtements, des montres ou des lunettes dans lesquelles sont insérés des capteurs pour étendre leurs fonctionnalités. Ces capteurs peuvent collecter en temps réel des données concernant le corps (humeur, habitudes, activités physiques, état de santé, vitesse, mobilité) et l'environnement (images, sons, température, humidité, emplacement, environnement social) de l'utilisateur.

Des caméras sont intégrées dans de nombreux appareils de ce type. Même si une telle caméra ne peut que capter certains éléments énumérés ci-dessus, cette fonction est au centre de nombreuses préoccupations en matière de protection de la vie privée. C'est en effet la capacité de ces dispositifs d'enregistrer des données en permanence et/ou secrètement qui soulève des questions en matière de protection de la vie privée, en particulier des non utilisateurs qui peuvent faire l'objet de ces enregistrements.

[10] 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 2015

Avec ces dispositifs, l'informatique « disparait » en quelque sorte dans les vêtements, les lunettes et les montres et, finalement, sous la peau. Les indices traditionnels, qui permettraient à un individu de savoir que ces dispositifs sont opérationnels, ne sont plus présents. Le résultat est un manque croissant de transparence et la difficulté qui s'ensuit pour les utilisateurs et les autres personnes concernées à faire des choix éclairés.

Dans son avis, le Groupe de Berlin a fait les recommandations suivantes :

- Le traitement des données à caractère personnel dans et par les dispositifs d'informatique vestimentaire devrait être aussi transparent que possible pour les utilisateurs et autres personnes dont les données sont traitées. Dans le cas des dispositifs miniaturisés ou cachés, l'information devrait être fournie par des moyens autres que visuels. Cela inclut la transparence concernant des connexions à d'autres dispositifs auxiliaires tels que les smartphones.

- La personne portant le dispositif devrait avoir - par défaut - le contrôle sur les données traitées. Il ne devrait y avoir aucune obligation de se connecter aux serveurs des fabricants, à d'autres plateformes ou de services de cloud.

- La transmission ou la divulgation de données devrait nécessiter une information claire ainsi que le consentement explicite de l'utilisateur du dispositif.

- Les droits d'accès, de rectification et de suppression de la personne concernée devraient être respectés. Les individus devraient avoir un moyen de vérifier l'exactitude des données générées ou l'analyse qui est faite à l'aide des données recueillies par un dispositif portable.

- Les individus devraient avoir la possibilité de retirer leur consentement à la divulgation de données à tout moment. Ils devraient également avoir la possibilité de stocker leurs données localement (par exemple sur un smartphone ou un autre appareil de l'utilisateur).
- Des moyens pour assurer la portabilité des données devraient être fournis.

- L'utilisation de l'informatique vestimentaire sur le lieu du travail soulève des questions supplémentaires à l'égard de la liberté de choix de l'employé. Les employés qui choisissent de ne pas participer aux programmes basés sur ce type d'appareil ne devraient pas être affectés négativement par leur décision.

- Lorsque les données traitées par ces dispositifs sont

considérées comme données de santé, le traitement ultérieur de ces données ne devrait être autorisé qu'après avoir obtenu le consentement explicite de la personne concernée.

2.6.2.2 *Responsabilisation des gouvernements lorsqu'ils accèdent à des données personnelles conservées par des entreprises privées*

Le groupe de travail a examiné l'utilité pour les entreprises de télécommunications et les fournisseurs de services en ligne d'établir des rapports de transparence en matière de protection des données et de confidentialité. Des rapports sur la transparence sont utiles pour augmenter la confiance dans les organisations qui détiennent de nombreuses données à caractère personnel et permettent à responsabiliser les autorités publiques qui veulent accéder à ces données.

Les rapports de transparence sont des rapports périodiques des responsables du traitement contenant des statistiques et des explications sur les données personnelles qui sont transmises à des tiers à des fins non commerciales. Ce document de travail traite principalement des transmissions à des autorités répressives.

Le Groupe de Berlin a expliqué d'abord pour quelles raisons les acteurs publics ont de plus en plus accès aux données d'entreprises privées et pourquoi il est devenu très intéressant pour les entreprises de détenir ces données. Ensuite, le groupe a décrit les parties qui se trouvent en principe dans un rapport de transparence.

Le groupe de travail a recommandé aux autorités de protection des données d'encourager les entreprises à intégrer les principes suivants dans leurs rapports de transparence :

1. Le principe de responsabilité : les entreprises devraient agir de manière responsable lorsqu'elles communiquent des données aux autorités publiques ;
2. Le principe de transparence : les entreprises devraient communiquer de manière périodique sur la quantité et la nature des demandes des autorités publiques ;
3. Le principe de fiabilité : les rapports devraient être précis et complets ;
4. Le principe que les rapports ne devraient pas induire en erreur (par exemple en publiant des statistiques incomplètes) ;
5. Le principe de la comparabilité : les statistiques devraient être comparables aux statistiques de rapports précédents ou à d'autres rapports de transparence ;
6. Le principe d'accessibilité : les rapports devraient être accessibles au public, aux parties prenantes et aux médias.

2.6.2.3 *Analyse vidéo intelligente*

Le Groupe de Berlin a examiné l'utilisation de technologies intelligentes d'analyse vidéo par des acteurs du secteur privé et du secteur public.

L'analyse vidéo intelligente est utilisée pour détecter et suivre des individus afin de pouvoir leur proposer des publicités personnalisées, une sécurité améliorée ou des solutions de gestion de la clientèle. Cette technologie peut fournir des informations détaillées de mesure d'audience des nouveaux canaux et médias pour communiquer avec des individus. Les technologies analysées dans le document du groupe de travail sont utilisées pour détecter et/ou suivre des personnes et des objets, mais pas pour les identifier.

Le groupe a examiné les implications de ces technologies sur la vie privée et a donné des recommandations pour une mise en œuvre transparente et conforme au cadre légal en matière de protection des données.

Les activités en 2015

Un exemple typique d'un enregistrement dans une base de données dans un magasin équipé de systèmes d'analyse de vidéo intelligent serait :
- date d'entrée : 12.05.2014,
- temps : 12:02 ,
- sexe : masculin,
- estimation de l'âge : 35,
- position : entrée principale.

Ces données peuvent être analysées pour donner au gérant des informations sur le sexe et la distribution d'âge des acheteurs, sur le nombre et la fréquence des visites, sur les sections les plus visitées du magasin et d'autres informations utiles. Des affichages numériques pourraient être utilisés pour diffuser des publicités ciblées (par exemple, des produits de rasage si un visiteur de sexe masculin a été détecté) ou pour inciter les visiteurs à interagir avec l'annonce (par exemple, participer à des jeux pour gagner des crédits ou des réductions en intégrant la reconnaissance des gestes, des écrans tactiles et des smartphones).

Même si les individus ne sont pas identifiés, l'analyse vidéo intelligente peut avoir un impact significatif sur leur vie privée. Ces technologies peuvent par exemple être utilisées par les services répressifs pour détecter une conduite inappropriée ou abusive dans des lieux publics (p.ex. dormir sur des bancs de parc), afin d'émettre des avertissements pour différentes infractions (p.ex. message automatisé pour réprimander le stationnement illégal) ou même pour des décisions basées sur le sexe ou l'appartenance ethnique. Dans le domaine privé, les risques en matière de protection de la vie privée existent aussi, même s'ils sont moins visibles. Les individus ont le droit de savoir ce que les caméras sont capables à faire. Peu de personnes sont au courant qu'il y a des caméras qui peuvent détecter notre sexe et suivre nos mouvements lorsqu'on est en train de faire ses courses.

Afin de mieux protéger la vie privée des personnes concernées par ce type de surveillance, le Groupe de Berlin a fait plusieurs recommandations :

- Le principe de légalité et d'équité devrait être respecté en prévoyant des mécanismes de transparence. Les individus devraient être informés de manière intelligible sur la présence de systèmes d'analyse de vidéo intelligents et de ce que ces technologies font exactement. Dans le secteur public, de tels systèmes devraient être prévues par une loi.

- Le groupe de travail a encouragé les fournisseurs d'affichages électroniques d'intégrer des interfaces permettant aux utilisateurs de se désengager ou de donner

leur consentement de manière simple.

- Le traitement de données sensibles devrait être évité.

- Pour informer les individus de manière adéquate, le groupe a préconisé une approche à plusieurs niveaux. Les informations les plus importantes devraient être communiquées lors de la collecte des données et complétées par des renseignements supplémentaires via différents canaux (posters, brochures, informations sur le site web, etc.).

- Les opérateurs d'analyse de vidéo intelligentes devraient effectuer un PIA (« Privacy Impact Assessment ») afin d'identifier les risques avant la mise en œuvre de la technologie.

2.6.2.4 *Localisation à partir des communications d'appareils mobiles*

Le Groupe de Berlin a examiné les risques en matière de protection des données associés à la collecte de données relatifs à un dispositif mobile et l'obtention de données de localisation à partir de données de communication. Un exemple serait l'utilisation de données concernant la connexion à un réseau wifi pour analyser la fréquentation d'un magasin. Un nombre important de risques pour la vie privée découlent du fait que le suivi de localisation des appareils mobiles se fait de manière cachée. Souvent, il suffit que le wifi d'un appareil mobile soit activé pour que des données soient collectées. Aucune action de l'utilisateur n'est nécessaire et il est fort probable qu'il n'est pas conscient de cette possibilité d'être localisé.

Le groupe de travail a énuméré tous les autres risques potentiels qui peuvent découler de cette collecte et a fait de nombreuses recommandations aux organisations souhaitant localiser des appareils mobiles :

- s'informer sur la législation applicable dans le domaine ;

- faire un PIA (« Privacy Impact Assessment ») ;

- respecter les codes de conduite existants ;

Les activités en 2015

- minimiser la collecte de données, limiter les périodes de conservation des données et choisir des paramètres par défaut qui respectent la vie privée ;

- notifier les individus concernés ;

- anonymiser les données sans délai ;

- demander le consentement si les données sont combinées avec d'autres informations.

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

Depuis 2015, la CNPD fait également partie du groupe de travail international sur l'Education au numérique. Ce groupe compte actuellement 42 autorités de protection des données, membres actifs et observateurs.

Le programme d'action 2014-2015 du groupe de travail définissait 3 axes prioritaires :

1. La création d'une plateforme web de partage de ressources d'éducation au numérique dans le domaine de la protection des données.

2. L'élaboration d'un kit tutoriel destiné à la formation des formateurs sur la protection des données.

3. La promotion des concours nationaux et l'élaboration d'un kit de concours à l'attention des autorités de protection des données.

La CNPD a participé activement aux deux premiers projets. Concernant le premier projet, un espace dédié au groupe de travail a été créé en ligne sur lequel 20 autorités de protection des données se sont inscrites. Quant au deuxième projet, une enquête par questionnaire a été réalisée afin de dresser un état des lieux sur les ressources d'éducation à la protection des données et à la vie privée. Un rapport d'étape sur l'enquête a été établi par la CNIL, la CNPD et l'APDCAT (autorité de Catalogne) avec la participation des autres autorités de protection des données et/ou de leur ministère de l'éducation, de panels d'enseignants et de formateurs. En particulier, l'enquête a permis de déterminer les acteurs qui élaborent des ressources éducatives sur la protection des données et d'identifier des thématiques communes à intégrer dans un futur kit tutoriel.

2.6.4 Le séminaire européen « Case Handling Workshop »

L'autorité de protection des données de l'Albanie a

Conférence de printemps des autorités européennes de la protection des données (Manchester, 19 mai 2015).

organisé le séminaire européen « Case Handling Workshop » à Tirana, les 28 et 29 septembre 2015.

Ce « workshop » a permis aux employés des autorités de protection des données européennes d'échanger leurs expériences pratiques en matière de traitement des plaintes et de promouvoir la coopération entre les différentes autorités européennes.

En 2015, le séminaire a abordé les thèmes suivants au cours de huit sessions et 19 présentations :

- protection des données dans le domaine de la finance ;
- protection des données dans le secteur public ;
- échange de données entre autorités nationales dans des affaires transfrontalières ;
- émergence de nouveaux services et technologies ;
- marketing direct et Internet.

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

L'autorité de protection des données du Royaume-Uni (ICO - Information Commissioner's Office) a organisé la Conférence européenne des autorités de protection des données à Manchester du 18 au 20 mai 2015.

100 experts de 40 différents pays s'étaient réunis pour cette « Spring conference » dont le titre était « Navigating the digital future - let's get practical ».

L'édition de 2015 a commencé par une présentation des priorités de la Commission européenne et du Parlement européen concernant la réforme du cadre légal sur la protection des données, les PNR et la surveillance de masse par les services secrets. Le commissaire du Royaume-Uni, Christopher Graham, a ensuite présenté une nouvelle étude concernant l'attitude des Européens envers le droit relatif à la protection des données.

Ce discours a été suivi de 3 sessions principales sur les sujets suivants :

Les activités en 2015

- Session 1 : « Delivering rights for individuals - individuals' expectations » ;
- Session 2 : « Data protection rights - how organisations can successfully deliver » ;
- Session 3 : « Putting data protection rights at citizens' fingertips - the challenges for DPAs ».

Une résolution concernant les thèmes abordés a été adoptée à la fin de la conférence. Les participants ont demandé aux législateurs de s'assurer que les futures lois soient facilement compréhensibles et ont appelé les gouvernements à s'assurer que les autorités de protection des données aient assez de ressources afin de pouvoir exécuter leurs obligations.

2.6.6 Conférence internationale des commissaires de la protection des données

L'autorité de protection des données néerlandaise a organisé la 37ème Conférence internationale des commissaires de la protection des données et de la vie privée à Amsterdam du 26 au 29 octobre 2015.

Placé sous le thème « Privacy bridges », les commissaires ont discuté de la façon de créer des passerelles entre les différents régimes de protection des données et de la vie privée qui existent à travers le monde.

Des résolutions relatives aux thèmes suivants ont été adoptées :

- déclaration d'Amsterdam sur les données génétiques et de santé et surveillance des services de sécurité et de renseignement ;
- protection de la vie privée dans le domaine de l'action humanitaire internationale ;
- rapports de transparence ;
- coopération avec le rapporteur spécial des Nations unies sur le droit à la protection de la vie privée ;
- direction stratégique de la conférence (2016-2018).

3 Les temps forts de 2015

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 Accord sur la réforme de la législation européenne en matière de protection des données

Le 15 décembre 2015, la Présidence luxembourgeoise du Conseil de l'Union européenne est parvenue à un accord informel en trilogue avec le Parlement européen et la Commission européenne sur le paquet « protection des données » qui définira les nouvelles règles européennes applicables en matière de vie privée à l'ère numérique. Ce paquet législatif comprend un règlement général sur la protection des données et une directive spécifique pour le domaine de la police et de la justice. Le 18 décembre 2015, le Comité des représentants permanents (Coreper) a approuvé ces textes de compromis.

L'accord de principe de l'Union européenne a été approuvé par le Conseil de l'Union européenne et voté par le Parlement européen le 14 avril 2016. Les nouvelles règles issues du règlement seront applicables le 25 mai 2018, deux ans après leurs publications au journal officiel de l'Union européenne. Suite à son adoption, la directive devra être transposée par les Etats membres dans leur législation nationale.

Pourquoi était-il nécessaire de réformer le cadre légal ?

La législation de l'UE relative à la protection des données existe depuis plus de 20 ans. Si la directive de 1995 garantit une protection effective, il est devenu nécessaire de moderniser les règles en vigueur pour tenir compte de la globalisation et l'émergence des nouvelles technologies.

Ces règles ont, en effet, été adoptées à une époque où de nombreux services en ligne actuels - et les défis en découlant pour la protection des données - n'existaient pas encore. Avec les sites de réseaux sociaux, le cloud computing, l'internet des objets, les services utilisant la géolocalisation et les cartes à puce, le traitement des données à caractère personnel a augmenté de manière exponentielle.

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 dans la presse nationale et internationale se multiplient.

Les disparités qui caractérisent les modalités de mise en œuvre de cette législation dans les États membres ont également donné lieu à des incohérences qui créent de la complexité, de l'insécurité juridique et des coûts administratifs. Cette situation a une incidence sur la confiance des individus et sur la compétitivité de l'économie de l'UE.

Un ensemble solide de règles est donc nécessaire pour garantir que le droit des personnes à la protection des données à caractère personnel les concernant, reconnu par l'article 8 de la Charte des droits fondamentaux de l'Union européenne, reste effectif à l'ère numérique.

Le « paquet » protection des données : de quoi s'agit-il ?

La réforme de la protection des données est un ensemble de mesures législatives proposé par la Commission européenne en 2012 pour actualiser et moderniser les règles contenues dans la directive de 1995 sur la protection des données (Directive 95/46/CE) et dans la décision-cadre de 2008 relative à la protection des données traitées dans le cadre de la coopération policière et judiciaire en matière pénale (Décision-cadre 2008/977/JAI).

Le paquet « protection des données » comprend un règlement général sur la protection des données et une directive spécifique pour le domaine de la police et de la justice.

Règlement général sur la protection des données

Deux ans après sa publication, le règlement général sur la protection des données sera directement applicable à tous les acteurs actifs sur le territoire de l'Union européenne. Les nouvelles règles consistent à donner aux citoyens davantage de contrôle sur leurs données personnelles et à responsabiliser davantage les entreprises tout en réduisant leurs charges déclaratives.

Un renforcement des droits des individus

Le nouveau règlement renforce les droits existants et octroie aux individus une maîtrise accrue de leurs données personnelles, grâce à :

- Un droit à l'effacement des données élargi et un « droit à

3 Les temps forts de 2015

l'oubli » : lorsqu'une personne ne souhaite plus que les données qui la concernent soient traitées, et dès lors qu'aucun motif légitime ne justifie leur conservation, ces données doivent être supprimées. Cela permet ainsi, par exemple, à une personne concernée d'exiger le retrait immédiat de données à caractère personnel collectées ou publiées sur un réseau social alors qu'elle n'était encore qu'un enfant.

- Un **accès plus simple à ses propres données personnelles** : les individus disposeront de plus d'informations sur la façon dont leurs données sont traitées, et ces informations devront être formulées de manière claire et compréhensible.

- Un **droit à la portabilité des données** : il sera plus facile de transférer les données personnelles d'un prestataire de services, par exemple un réseau social, à un autre.

- Une **meilleure information sur ce qu'il advient des données à caractère personnel dès qu'elles sont partagées** : les personnes physiques doivent notamment être informées de la politique en vigueur en matière de protection des données, en termes clairs et simples; cela peut également se faire au moyen d'icônes normalisées.

- Des règles plus précises pour autoriser les responsables du traitement des données à traiter des données à caractère personnel, avec notamment **l'obligation d'obtenir le consentement explicite** des personnes physiques concernées.

- Le **droit d'être informé en cas d'accès non autorisé** aux données personnelles : par exemple, les entreprises et organisations doivent notifier à l'autorité nationale de contrôle, dans les plus brefs délais, les violations de données graves, afin que les utilisateurs puissent prendre les mesures appropriées.

- La **« protection des données dès la conception » et la « protection des données par défaut »**. Ces principes sont désormais des éléments essentiels des règles de l'UE en matière de protection des données. Des garanties en la matière seront intégrées aux produits et aux services dès les premiers stades de leur développement, et des paramétrages par défaut respectueux de la vie privée seront la norme, par exemple sur les réseaux sociaux ou les applications mobiles.

- Un **contrôle accru de l'application de la réglementation** : les autorités chargées de la protection des données tel que la CNPD

pourront infliger des amendes lourdes aux entreprises qui ne respectent pas les règles de l'UE allant jusqu'à concurrence de 4 % de leur chiffre d'affaires annuel mondial.

- Une **meilleure protection des jeunes** : si un jeune de moins de 16 ans souhaite utiliser des services en ligne, le fournisseur de services doit s'assurer que les parents ont donné leur accord. Les États membres peuvent abaisser cette limite d'âge sans toutefois descendre en dessous de 13 ans.

Une responsabilité accrue des responsables du traitement

La réforme apporte clarté et cohérence en ce qui concerne les règles à appliquer, et rétablit la confiance du consommateur, ce qui permettra aux entreprises de tirer pleinement parti des possibilités offertes par le marché unique numérique. Pour les entreprises, la réforme apportera de nombreux changements :

- **Un continent, un droit** : le règlement établira un corpus unique de règles: il sera donc plus simple et moins coûteux, selon la Commission européenne, pour les entreprises d'exercer leurs activités dans l'UE.

- **Un guichet unique (« One-stop-shop »)** : les entreprises traiteront avec une seule autorité de contrôle (qui se trouve dans l'Etat membre dans lequel elles ont leur établissement principal), ce qui leur permettra d'économiser quelque 2,3 milliards d'euros par an selon la Commission européenne.

- **L'application des règles européennes sur le sol européen** : les entreprises établies hors de l'UE devront appliquer les mêmes règles que les entreprises européennes lorsqu'elles offrent des biens ou services sur le marché européen ou surveillent le comportement des citoyens européens. Les grands groupes américains comme Facebook, Google ou Apple sont donc directement concernés.

- **Suppression des notifications/ demandes d'autorisation** : les déclarations aux autorités de contrôle constituent une formalité qui représente un coût de 130 millions d'euros par an pour les entreprises selon la Commission européenne. La réforme les limitera au maximum.

Le règlement prévoit une série de mesures pour renforcer la responsabilité des responsables du traitement, l'objectif étant d'assurer un respect absolu des nouvelles règles en matière de protection des données :

- Les responsables du traitement doivent mettre en œuvre un certain nombre de mesures de sécurité. Dans certains cas, ils devront par ailleurs **notifier les violations de données** à caractère personnel à la CNPD dans un délai de 72 heures après en avoir pris connaissance.

- Pour veiller à ce que le règlement soit à l'épreuve du temps, les principes de la **protection des données dès la conception** et de la **protection des données par défaut** sont introduits. Le règlement imposera que des garanties en matière de protection des données soient intégrées aux produits et services dès la phase initiale de leur conception. Des techniques de protection de la vie privée comme la pseudonymisation seront encouragées, en vue de tirer parti des avantages de l'innovation du « Big Data » tout en protégeant la vie privée.

- Les organismes publics et les entreprises qui effectuent certains traitements de données à risques doivent obligatoirement désigner un **délégué à la protection des données** pour garantir le respect des règles.

- Les responsables d'un traitement peuvent s'exposer à des **amendes d'un montant maximal de 20 millions d'euros ou correspondant à 4% de leur chiffre d'affaires annuel mondial.**

3 Les temps forts de 2015

Un rôle plus important pour les autorités de protection des données

Le nouveau règlement prévoit par ailleurs un rôle plus important pour les autorités de protection des données tel que la CNPD.

Comme mentionné plus haut, des amendes administratives dissuasives pourront être infligées en cas de traitement illicite ou d'abus constatés dans le cadre de l'utilisation de données personnelles. Un tel pouvoir renforce l'indépendance des autorités de contrôle et devrait motiver les responsables du traitement à améliorer la sécurité afin d'éviter des violations de données. Il existe également la possibilité pour les Etats membres de prévoir en plus des sanctions pénales.

Les acteurs privés et publics devront adopter une conduite préventive et responsable à l'égard des données à caractère personnel qu'ils collectent. Avec l'abolition des déclarations préalables, ils devront adopter une nouvelle approche moins bureaucratique, mais plus exigeante de «privacy by design».

Pouvoir les conseiller et les orienter dans cette démarche est le rôle de l'autorité de surveillance. C'est donc à un développement de l'activité de guidance que la CNPD entend se préparer dans les prochains mois, tout comme à l'extension de sa capacité d'investigation et de contrôle.

Au niveau européen, une meilleure coopération entre les autorités de protection des données sera nécessaire afin de faire face de manière efficace aux problèmes ayant un impact dans plusieurs Etats membres.

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.

Directive sur la protection des données traitées à des fins répressives

La directive relative à la protection des données à caractère personnel traitées par la police et les autorités judiciaires pénales remplace la décision-cadre 2008/977/JAI qui régit actuellement le traitement des données par les autorités policières et judiciaires. La nouvelle directive s'applique aussi bien au traitement transfrontière des données à caractère personnel qu'au traitement de ce type de données par les autorités policières et judiciaires au niveau strictement national. La décision-cadre ne porte que sur l'échange transfrontière de données.

Outre les activités menées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, le champ d'application de la nouvelle directive a été étendu à la protection contre les menaces pour la sécurité publique et à la prévention de telles menaces.

Une meilleure coopération entre forces de l'ordre

Avec la nouvelle directive, les forces de l'ordre des États membres de l'UE pourront échanger plus efficacement les informations nécessaires pour les enquêtes, ce qui améliorera la coopération en matière de lutte contre le terrorisme et d'autres formes graves de criminalité en Europe.

Une meilleure protection des données des citoyens

Les données personnelles des individus seront mieux protégées lorsqu'elles seront traitées par les forces de l'ordre, y compris dans le cadre de la prévention de la criminalité. Tous seront protégés, que ce soit la victime, l'inculpé ou le témoin. Dans l'Union européenne, tout traitement des données par les forces de l'ordre devra satisfaire aux principes de nécessité, de proportionnalité et de légalité, et prévoir des garanties appropriées pour les individus. Le contrôle sera assuré par des autorités nationales indépendantes, chargées de la protection des données, et un recours juridictionnel effectif devra être prévu.

Le texte énumère les informations que la personne concernée est toujours en droit de recevoir afin de protéger ses droits si elle craint que ses données aient fait l'objet d'une violation.

La nouvelle directive prévoit qu'un délégué à la protection des données soit nommé pour aider les autorités compétentes à faire respecter les règles en matière de protection des données.

L'analyse d'impact constitue un autre outil permettant d'assurer le respect des dispositions. Lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, les autorités compétentes doivent procéder à une analyse de l'impact potentiel dudit traitement, en particulier en cas de recours à une nouvelle technologie.

3.2 La décision de la Commission européenne relative aux accords « Safe Harbor » jugée invalide par la CJUEl

Dans son arrêt du 6 octobre 2015 « Maximilian Schrems c. Data Protection Commissioner », la Cour de Justice de l'Union européenne (CJUE) a invalidé la décision d'adéquation 2000/520 de la Commission européenne du 26 juillet 2000 relative aux accords « Safe Harbor » (communément appelée « décision Safe Harbor »).

En conséquence, il n'est plus possible de transférer des données à caractère personnel vers les Etats-Unis sur base de la décision « Safe Harbor ».

La CNPD examine actuellement les conséquences de cet arrêt ensemble avec les autres autorités de protection des données européennes au sein du Groupe « Article 29 » (ou « G29 »).

La décision « Safe Harbor »

En principe, il est interdit de transférer des données à caractère personnel vers des pays situés hors de l'Union européenne n'assurant pas une protection adéquate. La Commission européenne peut constater qu'un pays n'appartenant pas à l'UE assure un tel niveau de protection (équivalent aux pays ayant transposé la directive européenne 95/46/CE). C'est ce qu'elle a fait avec sa décision du 26 juillet 2000 pour les Etats-Unis.

Les entreprises établies aux Etats-Unis ayant adhéré aux conditions des accords de la sphère de sécurité (« Safe Harbor ») conclus

Les temps forts de 2015

entre la Commission européenne et les autorités américaines figurant sur la liste tenue par la Federal Trade Commission étaient considérées comme assurant un niveau de protection suffisant pour les données personnelles.

Contexte de l'affaire Schrems

M. Maximillian Schrems, un citoyen autrichien, utilise Facebook depuis 2008. Comme pour les autres abonnés résidant dans l'Union, les données fournies par M. Schrems à Facebook sont transférées, en tout ou partie, à partir de la filiale irlandaise de Facebook sur des serveurs situés sur le territoire des États-Unis, où elles font l'objet d'un traitement. M. Schrems avait déposé une plainte auprès de l'autorité de contrôle irlandaise, considérant qu'au vu des révélations faites en 2013 par M. Edward Snowden au sujet des activités des services de renseignement des Etats-Unis (en particulier la National Security Agency ou « NSA »), le droit et les pratiques des Etats-Unis n'offrent pas de protection suffisante contre la surveillance, par les autorités publiques, des données transférées vers ce pays. L'autorité irlandaise avait rejeté la plainte, au motif notamment que, dans sa décision du 26 juillet 2000, la Commission a considéré que, dans le cadre du régime dit de la « sphère de sécurité », les États-Unis assurent un niveau adéquat de protection aux données à caractère personnel transférées.

Saisie de l'affaire, la High Court of Ireland (Haute Cour de justice irlandaise) souhaitait savoir si cette décision de la Commission aurait pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assurait pas un niveau de protection adéquat et, le cas échéant, de suspendre le transfert de données contesté.

Une décision clé : l'arrêt de la CJUE du 6 octobre 2015

Saisie dans le cadre de cette question préjudicielle, la CJUE a estimé que, pour se prononcer sur le niveau de protection assuré par la décision « Safe Harbor », la Commission européenne ne pouvait pas se limiter à l'analyse de ce régime, *mais « était tenue de constater que les États-Unis assurent effectivement, en raison de leur législation interne ou de leurs engagements internationaux, un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive lue à la lumière de la Charte »*[11].

Or, le jugement de la Cour a confirmé qu'en raison en particulier de l'existence d'une surveillance de masse et de l'absence de possibilité pour un individu de pouvoir exercer un recours judiciaire effectif afin de pouvoir avoir accès à ses données et obtenir rectification et suppression de ses données, de sérieuses questions existaient

en ce qui concerne la continuité du niveau de protection des données personnelles lorsque ces données sont transférées vers les Etats-Unis. Depuis plusieurs années, le G29 a étudié l'impact d'une surveillance de masse sur les transferts internationaux de données et a à plusieurs occasions présenté ses observations à ce sujet.

Constatant que la Commission européenne n'avait pas recherché si les Etats-Unis assuraient effectivement une protection suffisante, la CJUE a ainsi prononcé l'invalidation de la décision « Safe Harbor ».

La Cour a également conclu que les pouvoirs des autorités de protection des données ne se trouvaient pas réduits par l'existence de cette décision. En conséquence, les autorités de contrôle devaient toujours avoir la possibilité d'enquêter, en complète indépendance, au sujet d'une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat des données à caractère personnelles transférées.

Conséquences

Lors de la réunion du 15 octobre 2015 du G29, les autorités de protection des données européennes ont analysé les conséquences de la décision de la CJUE et ont adopté une approche commune sur la question.

En premier lieu, le G29 a souligné que la question de la surveillance massive et indiscriminée est au cœur de l'arrêt de la CJUE. Il a rappelé à ce titre qu'il a toujours considéré qu'une telle surveillance était incompatible avec le cadre juridique européen et que les outils de transferts ne pouvaient constituer une solution à ce problème. Par ailleurs, et comme le G29 l'a déjà indiqué, les pays tiers (en dehors de l'Union Européenne) dans lesquels des autorités publiques accèdent aux informations personnelles, ne pouvaient être considérés comme des destinations sûres dans le cadre de transferts. A cet égard, la décision de la CJUE implique que chaque décision d'adéquation résulte d'une analyse approfondie des lois nationales du pays tiers ainsi que des accords internationaux.

[11] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117fr.pdf

Les temps forts de 2015

Par conséquent, le G29 a demandé aux Etats membres et aux institutions européennes d'engager au plus vite les discussions avec les autorités américaines afin de trouver des solutions politiques, juridiques et techniques permettant de transférer des données vers le territoire américain dans le respect des droits fondamentaux. De telles solutions pourraient intervenir dans le cadre de négociations d'un accord intergouvernemental offrant des garanties fortes aux citoyens européens. Les négociations actuelles portant sur un nouvel accord Safe Harbor pourraient constituer une partie de la solution. Dans tous les cas, ces solutions devront s'appuyer sur des mécanismes clairs et contraignants et comporter au minimum des obligations de nature à garantir le contrôle des programmes de surveillance par les autorités publiques, la transparence, la proportionnalité, l'existence de mécanismes de recours et la protection des droits des personnes.

En parallèle, le G29 a poursuivi son analyse de l'impact de la décision de la CJUE sur les autres outils de transfert (BCR, clauses contractuelles types) mais a considéré que durant cette période, ces outils pourraient encore être utilisés par les entreprises. Les autorités de protection des données se réservaient néanmoins la possibilité de contrôler certains transferts, notamment à la suite des plaintes qu'elles pourraient recevoir.

Au regard de la décision de la CJUE, il est apparu très clairement que les transferts de données depuis l'Union Européenne vers les Etats-Unis n'étaient plus possibles sur la base de la décision de Safe Harbor du 26 juillet 2000. En tout état de cause, les transferts qui s'opèreraient encore sur cette base juridique seraient illégaux.

Afin d'informer l'ensemble des parties prenantes, les autorités de protection des données européennes ont lancé des campagnes d'information au niveau national, comprenant une information ciblée auprès des entreprises ayant déjà réalisé des transferts sur la base du Safe Harbor et une information générale sur les sites des autorités.

Enfin, le G29 a insisté sur les responsabilités partagées des autorités de protection, des institutions européennes, des Etats membres et des entreprises pour élaborer des solutions robustes. Dans ce contexte, les entreprises doivent en particulier mettre en œuvre des solutions juridiques et techniques pour limiter les risques éventuels qu'elles prennent en transférant des données à l'étranger quant au respect des droits fondamentaux des personnes.

La situation au Luxembourg

Les 25 et 26 novembre 2015, la CNPD a envoyé une lettre à toutes les entreprises luxembourgeoises qui transféraient des données à caractère personnel à destination des Etats-Unis d'Amérique sur base de la décision « Safe Harbor ».

Aux termes de cette lettre, la CNPD expliquait aux entreprises concernées que les transferts de données personnelles vers les Etats-Unis n'étaient plus possibles sur base de cette décision et évoquait les autres outils juridiques qui permettraient toujours de transférer des données vers les Etats-Unis, pour le cas où ces entreprises désirent poursuivre de tels transferts.

4 Perspectives

Le nouveau règlement européen en matière de protection des données[12] et l'invalidation de la décision « Safe Harbor »[13] ont marqué l'année 2015 et auront également un impact considérable sur le travail et le mode de fonctionnement de la CNPD dans les années à venir.

Des nouvelles règles à l'ère numérique et de la globalisation

L'Union européenne, suite à l'accord politique obtenu en décembre 2015 lors de la présidence luxembourgeoise du Conseil, a adopté un nouveau règlement général sur la protection des données qui entrera en vigueur le 24 mai 2016. Deux ans après sa publication, l'ensemble des intervenants, y compris la CNPD, se doivent de rapidement s'adapter à cette nouvelle législation pour être prêt lors de sa mise en application, soit le 25 mai 2018. Cela constituera le principal défi de la CNPD durant les prochaines années.

Fidèle à ses missions d'information, de supervision et de coopération, la CNPD a constitué des groupes de travail internes pour aborder cette réforme majeure et aussi favoriser le travail de mise en conformité de l'ensemble des acteurs dans ce domaine.

La majeure partie des principes fondamentaux de l'ancienne directive, qui date de 1995, est préservée. Ce nouveau règlement s'appuie sur les anciens concepts et les conforte. Par rapport à la loi nationale actuellement en vigueur au Luxembourg, le nouveau règlement introduit de nouveaux concepts (p. ex. la portabilité), modifie certains éléments (rôle central du délégué à la protection des données) et supprime certaines activités (demandes d'autorisation et notifications des traitements de données à la CNPD). De plus, pour éviter la divergence de transposition de l'ancienne directive dans les lois nationales, le règlement s'attarde longuement sur la mise en place de moyens pour uniformiser son application au sein de l'Union européenne en créant notamment le Comité européen de la protection des données.

Le règlement européen, en vertu de son application directe, a pour effet mécanique de normaliser les règles applicables au sein des États membres. Cependant, il autorise, voire requiert aussi de l'État luxembourgeois de légiférer sur certains aspects comme les statuts, missions et pouvoirs de la CNPD. Par conséquent, la refonte de la législation nationale actuellement en vigueur au Luxembourg est nécessaire. La CNPD apportera son soutien à cette démarche et contribuera, en accord avec ses attributions légales dans ce domaine, à l'adaptation du cadre législatif national à cette

[12] Voir partie 3.1 pour plus de détails.
[13] Voir partie 3.2 pour plus de détails.

nouvelle régulation européenne. Certains aspects du nouveau règlement doivent encore être impérativement votés avant la mise en application le 25 mai 2018.

Le nouveau règlement renforce les droits et responsabilités de l'ensemble des acteurs (responsable de traitement, sous-traitant, délégué à la protection des données, personne concernée…) liés à la protection des données. Attachée à sa mission d'information et de sensibilisation dans son domaine, la CNPD a déjà commencé d'informer des acteurs sur ces principaux changements. Elle a constitué un groupe de travail qui est chargé de mettre en œuvre une politique globale et cohérente de sensibilisation de l'ensemble des acteurs concernés par le nouveau règlement.
Tout nouveau texte juridique engendre des interrogations d'ordre pratique. La CNPD s'efforcera d'y répondre. Ainsi, pour les responsables de traitement et les sous-traitants, cette réforme comporte de nombreux bouleversements. Elle accroît notamment leur responsabilité dans le domaine de la protection des données tout en leur offrant une plus grande liberté dans la mise en œuvre de leur politique de gestion des données personnelles. De plus, les délégués à la protection des données sont amenés à remplacer les actuels chargés de la protection des données.

La CNPD ainsi qu'au niveau européen le groupe « Article 29 » s'appliqueront à communiquer des lignes directrices pour faciliter ce travail de mise en conformité.

Le nouveau règlement modifie aussi les compétences, missions et pouvoirs de la CNPD.
Un groupe de travail interne spécifique est chargé d'apporter des solutions opérationnelles à cette transformation du rôle et de l'activité de la CNPD. De nouvelles procédures internes seront développées pour s'adapter aux impératifs du règlement (supervision, contrôle et sanction) et pour garantir que l'application de ces nouveaux pouvoirs soit respectueuse des droits et recours dont disposent l'ensemble des intervenants.

La dernière évolution majeure introduite par le règlement est la coopération renforcée entre les autorités de contrôle européennes notamment grâce au mécanisme du « One Stop Shop » et au mécanisme de contrôle de la cohérence. Pour coordonner les interventions entre ces différentes autorités et pour éviter les divergences d'application du règlement au sein de l'Union européenne, il est créé le Comité européen de la protection des données. La CNPD sera amenée à coopérer plus étroitement avec les autres autorités de contrôle européennes ainsi qu'avec ce nouveau Comité européen de la protection des données. De nouvelles procédures internes seront développées auprès de la CNPD pour faciliter cette coopération en intégrant les réflexions et les décisions prises sur ce sujet dans le cadre des réunions du groupe « Article 29 ».

Bien entendu, les besoins exprimés par les acteurs de la protection des données ainsi que la population luxembourgeoise seront pris en compte dans l'élaboration de l'ensemble de ces démarches qui sont réalisées pour permettre à la CNPD d'être prête lors de la mise en application du nouveau règlement (le 25 mai 2018) et pour renforcer le rôle de la CNPD comme garant au Luxembourg du respect, par l'ensemble des acteurs dans le domaine de la protection des données, des libertés et droits fondamentaux des personnes physiques et notamment de leur vie privée.

Transferts de données vers les Etats-Unis: le « Privacy Shield » est appelé à remplacer « Safe Harbor »

Dans son arrêt du 6 octobre 2015, la Cour de Justice de l'Union européenne (CJUE) a invalidé la décision « Safe Harbor ». En conséquence, il n'était plus possible de transférer des données à caractère personnel vers les Etats-Unis sur base de cette décision.

En février 2016, la Commission européenne et les Etats-Unis

4 Perspectives

d'Amérique sont toutefois parvenus à un accord sur un nouveau cadre pour les transferts de données transatlantiques : le « EU-U.S. Privacy Shield ». Ce « bouclier de protection des données EU-USA » est appelé à remplacer la décision « Safe Harbor ».

En quoi consiste le « Privacy Shield » ?

Le 29 février, la Commission a publié un projet de décision sur le caractère adéquat du niveau de protection des Etats-Unis d'Amérique, ainsi que les textes qui composeront le « Privacy Shield ». Ce paquet comprend les « Privacy Shield principles », auxquels les entreprises doivent adhérer, ainsi qu'une série d'engagements écrits du gouvernement des États-Unis (à publier au Federal Register, le journal officiel américain) concernant la mise en œuvre du dispositif, y compris des assurances sur les garanties et les conditions d'accès des pouvoirs publics aux données.

Ce mécanisme devra permettre aux entreprises européennes de transférer des données à caractère personnel à destination des Etats-Unis d'Amérique, s'ils respectent les principes définis dans le « Privacy Shield ». Le nouveau cadre répondrait en effet, selon la Commission européenne, aux exigences définies par la Cour de justice de l'Union européenne dans son arrêt du 6 octobre 2015.

Les garanties du « Privacy Shield »

D'après la Commission européenne, les principales garanties prévues par le « Privacy Shield » sont les suivantes :

- Les entreprises adhérant au « Privacy Shield » seront soumises à des obligations fermes, assorties d'une mise à exécution rigoureuse ;

- Un accès par les autorités américaines aux données à caractère personnel sera étroitement encadré et transparent ;

- Une protection effective des droits des citoyens de l'Union et plusieurs possibilités de recours seront prévues ;

- Enfin, un mécanisme de réexamen annuel conjoint permettra de contrôler le fonctionnement du « Privacy Shield », et notamment le respect des engagements et des assurances concernant l'accès aux données à des fins d'ordre public et de sécurité nationale.

Avis du groupe de travail européen « Article 29 » sur la protection des données (G29)

Le G29, au sein duquel participe la CNPD, a émis son avis au sujet du « Privacy Shield » en date du 13 avril 2016. Cet avis a pour objectif de vérifier si un niveau essentiellement équivalent de protection des données existe

lorsque des données personnelles seront transférées vers les Etats-Unis d'Amérique dans le cadre du « Privacy Shield ».

De manière générale, le G29 a souligné que des améliorations significatives ont été apportées au « Privacy Shield », en comparaison avec la décision « Safe Harbor » invalidée. En particulier, l'insertion de définition clés, les mécanismes de contrôle pour une mise en application effective du « Privacy Shield » et les mécanismes de réexamen conjoint décrit ci-dessus constituent autant de points positifs.

Par contre, le groupe a exprimé des préoccupations à la fois sur les aspects commerciaux et sur la question de l'accès par les autorités publiques aux données transférées dans le cadre du « Privacy Shield ». En outre, le G29 a pointé un manque général de clarté. Il a également indiqué qu'une révision des principes devra être effectuée à l'aune du nouveau règlement européen en matière de protection des données, lorsque ce dernier entrera en vigueur dans le courant de l'année 2018.

Concernant les aspects commerciaux du « Privacy Shield », le G29 a considéré que certains principes clés de la protection des données ne se retrouvaient pas dans les documents présentés par la Commission européenne ou ont été inadéquatement substitués par des notions alternatives. De plus, la question des transferts ultérieurs des données n'a pas été clairement réglée. Par ailleurs, les recours prévus pour les personnes concernées pourraient apparaître trop complexes et difficiles à mettre en œuvre en pratique.

En ce qui concerne la question de l'accès par les autorités publiques aux données transférées dans le cadre du « Privacy Shield », le G29 a regretté qu'il n'y ait pas suffisamment de détail quant au fait qu'une collecte massive et indiscriminée de données personnelles provenant de l'Union européenne par les autorités américaines soit exclue. Une telle collecte ne pourrait en effet pas être considérée comme proportionnelle et strictement nécessaire dans une société démocratique, conformément aux principes et à la jurisprudence européenne en matière de droits de l'Homme. Par ailleurs, le G29 a accueilli avec satisfaction la mise en place d'un « ombudsman », mais a émis des doutes quant au caractère suffisamment indépendant de cette nouvelle institution et quant aux pouvoirs en sa possession afin d'exercer effectivement ses missions.

En conclusion, le G29 a noté les améliorations apportées par le « Privacy Shield » en comparaison de la décision « Safe Harbor » invalidée. Mais, compte tenu des préoccupations exprimées ci-dessus, il a appelé la Commission à apporter des réponses à ces éléments, afin d'aboutir à une décision d'adéquation qui permettrait de garantir que le niveau de protection offert par le « Privacy Shield » soit équivalent à celui de l'Union européenne.

Prochaines étapes

La version finale de la décision d'adéquation « Privacy Shield » de la Commission européenne devra être adoptée par le Collège des commissaires européens, après consultation d'un comité composé de représentants des États membres et après l'avis précité du G29.

Une fois que le mécanisme de constatation du caractère adéquat de la protection des données sera définitivement adopté, les entreprises européennes pourront transférer des données à caractère personnel à destination des Etats-Unis d'Amérique en conformité avec cette décision d'adéquation.

Dans l'intervalle, le G29 a rappelé que les autres instruments juridiques permettant de transférer des données à caractère personnel vers des pays tiers (notamment les clauses contractuelles types et les « binding corporate rules ») continuent d'exister.

5 Ressources, structures et fonctionnement

5.1 Rapport de gestion relatif aux comptes de l'exercice 2015

Dépenses

Le total des frais de fonctionnement de l'établissement public au cours de l'exercice 2015 s'élève à 1.893.948,46 €. Ce chiffre représente une augmentation de 10,77% par rapport à l'exercice précédent. Bien qu'il ne dépasse pas les prévisions budgétaires originaires, il est tout de même nettement supérieur à la dotation qui avait finalement été accordée en 2015 et qui était de 1.714.200 €.

Ce sont essentiellement les charges relatives au personnel permanent et temporaire qui ont augmenté sensiblement, sans pour autant dépasser les prévisions budgétaires estimées à 1.733.020 €. 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. Fin 2014, un poste vacant d'un employé B1 pour le secrétariat avait été pourvu. En début de l'année 2015, la CNPD a recouru aux services d'un expert-juriste externe et en fin d'année, elle a engagé un employé juriste à durée indéterminée pour renforcer l'équipe des autorisations préalables. Les frais de formation pour le personnel s'élevaient à 2.828,52 € en 2015 comparés à 0 € en 2014. Ces frais vont probablement évoluer davantage au cours des années à venir étant donné que la CNPD apporte beaucoup d'attention à la formation de base, continue et linguistiques de ses collaborateurs.

Les dépenses d'honoraires et frais d'experts et de prestataires externes ne s'élevaient qu'à 10.549,82 €, ce qui ne constituait que 17,29% du budget prévu. 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 ne s'élevait qu'à 6.881,74 € en 2015. Ce montant va toutefois être régularisé en 2016 pour se situer autour des 30.000 €.

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, la CNPD a renouvelé une partie de ses équipements surannés

(ordinateurs, écrans, imprimantes, serveurs et back-up). Les coûts se sont élevés à 56.789,63 €, ce qui revient à 189,30% de la somme initialement prévue et une augmentation de 390,96% par rapport à l'année 2014. A part équiper les nouveaux membres du personnel, la CNPD ne devrait pas dans l'immédiat être exposée à des nouvelles grandes dépenses de cette catégorie.

Les frais de déplacement et de séjour à l'étranger se chiffrent à 30.050,88 €, ce qui à 15 € près, correspond à la dépense similaire en 2014. La CNPD reste toutefois 14,14% en dessous des prévisions budgétaires, ce qui est un bon résultat compte tenu de tous 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.

Les dépenses pour l'information du public et la communication de 15.480,13 € restent 38,08% en dessous des prévisions budgétaires, étant donné que certains des projets prévus sont restés en suspens.

L'augmentation de la dépense par rapport à l'année 2014 de 56,76% s'explique par une large publication d'annonces de recrutement dans la presse luxembourgeoise.

En raison d'une part, du renouvellement des équipements, et d'autre part, d'une nouvelle imputation des dépenses sur différentes positions budgétaires, les dépenses pour la maintenance des systèmes et réseaux informatiques ont pu être diminuées de 419,29% par rapport à l'année précédente et de 125,51% par rapport aux prévisions budgétaires. Cette dépense est en effet passée de 75.988,38 € en 2014 à 14.633,18 € en 2015.
A noter toutefois, qu'au vu de l'état suranné de certains équipements informatiques, des efforts d'investissement avaient déjà été effectués pour remplacer ces derniers en 2014 et que les dépenses avaient alors été imputées sur la présente position.

Les amortissements comptabilisés en 2015 atteignaient un montant total de 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'élève à 130.075 €, comparé à 115.168 € en 2014. Ce surplus constitue une augmentation de 12,94% par rapport à l'année précédente, mais reste 13,28% en dessous des prévisions budgétaires tablées à 150.000 €. En outre, des produits financiers (intérêts créditeurs) ont été enregistrés à hauteur de 355,76 €.

Etant donné qu'il n'y a actuellement pas d'argument militant en faveur du maintien des provisions exceptionnelles à un niveau particulièrement élevé, la CNPD a opéré une reprise de ces derniers à hauteur de 41.000 €.

Résultat d'exploitation

Compte tenu de la dotation annuelle de 1.714.200 €, dont la Commission nationale a bénéficié en 2015 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 - 8.317,70 € au 31 décembre 2015. Ce déficit a pu être comblé par l'excédent d'exercices antérieurs.

5 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

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

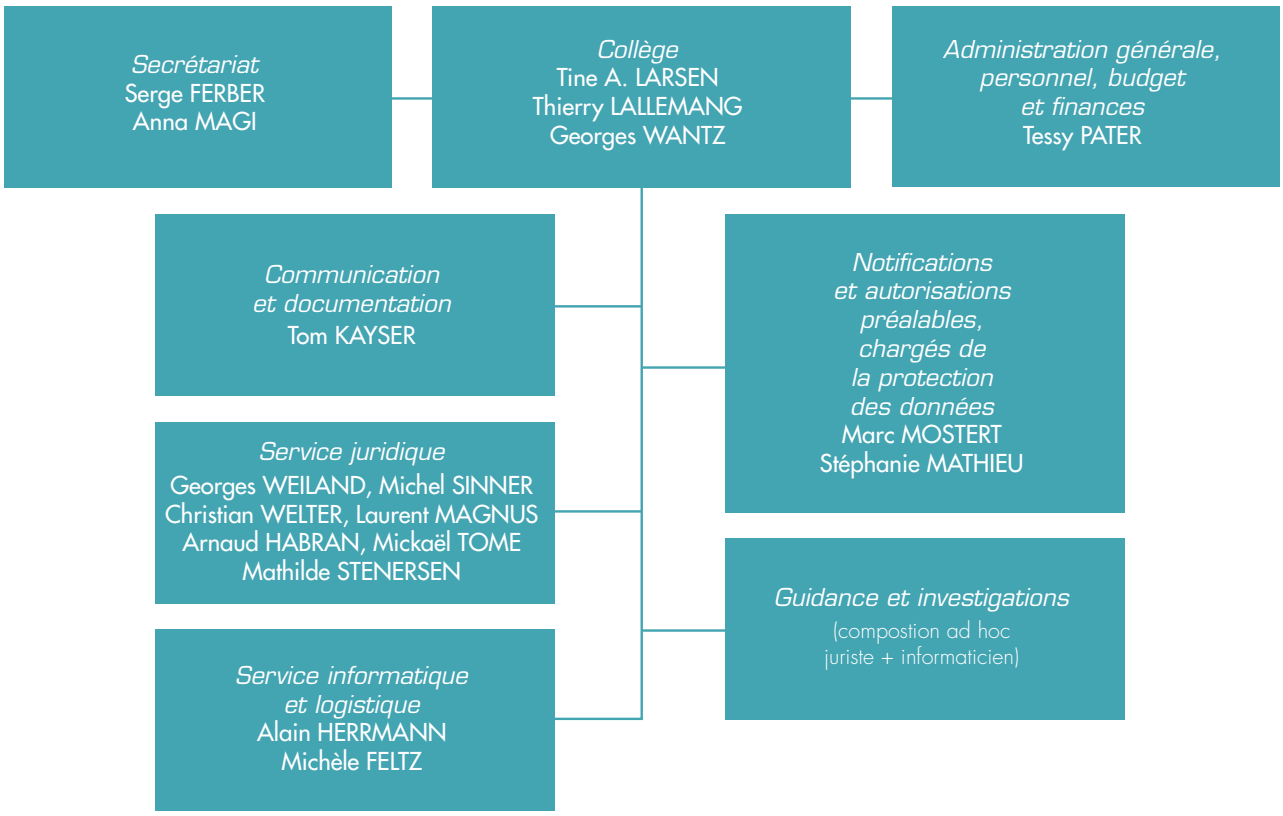
Tenue du registre public et prise en charge administrative des notifications et demandes d'autorisation
Marc MOSTERT,
rédacteur
Stéphanie MATHIEU,
rédacteur

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

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

5.3 Organigramme de la Commission nationale



6 La Commission nationale en chiffres

Formalités préalables

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	
a) Notifications											TOTAL 2003-2015
Notifications ordinaires	250	760	385	345	295	355	437	421	564	705	8.513
Notifications simplifiées	890	537	-	-	-	-	-	-	-	-	3.797
Engagements de conformité	-	-	942	227	15	46	149	651	45	19	2.094
(Total a 2003-2015)	1.140	1.297	1.327	572	310	401	586	1.072	609	724	14.404
b) Autorisations préalables											TOTAL 2003-2015
Demandes d'autorisation	295	392	606	542	607	604	706	833	914	969	7.956
Engagements de conformité	19	151	220	70	92	49	70	149	85	148	1.802
(Total b 2003-2015)	314	543	826	612	699	653	776	982	999	1.117	9.758
(Total général a + b 2003-2015)	1.454	1.840	2.153	1.184	1.009	1.054	1.362	2.054	1.608	1.841	24.162
Déclarants (responsables ayant accompli des formalités)	3.300	3.754	4.357	4.772	5.110	5.399	5.821	6.559	6.993	7.472	

Demandes de renseignements

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
a) Demandes de renseignements par écrit										
(Total a 2003-2015)	150	148	138	138	213	173	273	274	416	340
b) Demandes de renseignements par téléphone										
(Total b 2003-2015)	1.930	1.870	1.586	1.407	1.405	1.634	1.424	1.803	1.776	2.021
(Total général a + b 2003-2015)	2.080	2.018	1.724	1.545	1.618	1.807	1.697	2.077	2.192	2.361

Plaintes

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Plaintes et demandes de vérification de licéité	30	34	63	133	145	115	133	177	207	217

Séances de délibération

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
	39	40	40	37	38	35	27	31	20	39

Participations aux groupes de travail sur le plan européen

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
	23	22	22	32	40	37	43	39	40	47

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

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Secteur public	32	56	52	54	56	69	71	102	92	146
Secteur privé	12	40	44	52	54	71	61	75	77	106
(Total)	**44**	**96**	**96**	**106**	**110**	**140**	**132**	**177**	**169**	**252**

Séances d'information, conférences, exposés

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
	11	14	11	23	21	15	10	18	22	23

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

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Articles et interviews parus dans										
- les quotidiens	67	127	59	104	202	105	94	139	162	148
- les hebdomadaires	4	9	11	10	30	22	12	21	29	22
- les mensuels	5	4	2	1	5	4	1	3	10	25
- les médias audiovisuels	3	3	16	13	21	7	17	24	18	9
- Internet					49	36	51	52	58	59
(Total)	**79**	**143**	**88**	**128**	**307**	**174**	**175**	**239**	**277**	**263**

7 Annexes

Avis relatif au projet de règlement grand-ducal relatif aux cartes de légitimation et lettres de légitimation de certains agents et experts externes de l'Administration des chemins de fer

Délibération n°4/2015
du 30 janvier 2015

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 ».

Par courrier du 6 mai 2014, le Ministère du Développement durable et des Infrastructures a invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif aux cartes de légitimation et lettres de légitimation de certains agents et experts externes de l'Administration des chemins de fer.

L'objectif du projet de règlement grand-ducal consiste à définir les informations figurant sur les cartes de légitimation des agents de l'Administration des chemins de fer (ACF) et les lettres de légitimation des experts externes de l'ACF, de même que leurs modalités de délivrance, d'utilisation et de restitution, ainsi que leur durée de validité. Il est également créé, à cette occasion, un registre des cartes de légitimation et des lettres de légitimation.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données.

Il ressort de l'article 2 du projet de règlement grand-ducal sous objet que les cartes de légitimation comportent des données à caractère personnel au sens de l'article 2 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, à savoir les prénom et nom du titulaire, la date de naissance du titulaire, le numéro d'identification de la carte de légitimation, ainsi que la photographie du titulaire. Les lettres de légitimation comportent, quant à elle, les données à caractère personnel suivantes : les prénom et nom du titulaire, le lieu et la date de naissance du titulaire, le numéro d'identification de la lettre de légitimation, ainsi que la fonction du titulaire en rapport avec la mission.

Selon l'article 5 du projet de règlement grand-ducal sous objet, les cartes de légitimation et lettres de légitimation doivent être présentées par leur titulaire « sur demande de toute personne intéressée pour s'identifier dans l'exercice de la mission pour laquelle il est habilité ». Il ressort de cet article que la finalité pour laquelle sont utilisées les cartes et lettres de légitimation consiste à permettre aux titulaires de ces cartes de s'identifier auprès de toute personne intéressée dans le cadre de leurs missions.

Au vu de ce qui précède, la Commission nationale estime que les données à caractère personnel figurant sur les cartes et lettres de légitimation apparaissent nécessaires et proportionnées par rapport à la finalité poursuivie.

Par ailleurs, l'article 9 du projet de règlement grand-ducal sous examen prévoit que « le directeur de l'ACF est chargé de la création et de la gestion d'un registre des cartes de légitimation et des lettres de légitimation ». Il ressort de cette disposition que la finalité de la tenue de ce registre est la gestion administrative des différentes cartes de légitimation et lettres de légitimation de l'Administration des chemins de fer.

L'article 9 prévoit en outre que le registre « renseigne au moins sur la date d'émission, la durée de validité, les décisions visées à l'article 4, les mesures administratives visées à l'article 7 et les restitutions visées à l'article 8 ». La Commission nationale estime que ces données apparaissent en effet nécessaires à la réalisation de la finalité pour laquelle le registre est créé. Or, le terme « au moins » apparaît comme trop vague et permettrait de collecter d'autres données supplémentaires que celles indiquées dans le texte de l'article 9. Aux yeux de la CNPD, cette disposition ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal, et n'est par ailleurs pas conforme à l'article 4 de la loi modifiée du 2 août 2002. La Commission nationale suggère dès lors d'énumérer dans l'article 9 de façon exhaustive les données qui pourront être traitées dans le registre, et de supprimer les termes « au moins ».

Dans ce contexte, la CNPD est à se demander si le registre ou un autre fichier informatique séparé, tenu par l'ACF, ne contient pas en réalité aussi des données personnelles comme par exemple les noms et prénoms, adresses, dates de naissance et photos des demandeurs ou titulaires. Concernant les photos, la CNPD rappelle son opposition à un éventuel stockage numérique des photos dans un fichier et renvoie à ce sujet à son avis du 15 juin 2012 relatif au projet de loi n° 6284 portant sur l'exploitation d'une base de données à caractère personnel relative aux élèves (délibération n°156/2012).

Enfin, la Commission nationale note que le modèle de demande relative à l'attribution d'une carte de légitimation reproduit à l'annexe 1 du projet de règlement grand-ducal sous objet comporte la mention « numéro d'identification personnelle (matricule de sécurité sociale) ». La Commission nationale se demande en quoi cette donnée apparaît nécessaire afin de confectionner une carte de légitimation. En effet, les seuls noms, prénom, lieu et date de naissance de la personne concernée paraissent suffisants afin d'identifier le titulaire de la carte, d'autant plus que c'est l'employeur qui doit introduire la demande et que ce dernier aura préalablement vérifié l'identité de ses agents. La Commission nationale constate par ailleurs que le numéro d'identification personnelle n'est pas demandé dans le cas d'une lettre de légitimation (telle que reproduite à l'annexe 4). A défaut de préciser dans quelle mesure le numéro d'identification est nécessaire dans la procédure d'octroi d'une carte de légitimation à un agent de l'Administration des chemins de fer par le ministre, la Commission nationale propose donc de supprimer la mention du numéro d'identification personnelle dans le modèle de demande reproduit à l'annexe 1.

7 Annexes

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 30 janvier 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis à l'égard du projet de loi n°6588 portant a) organisation du secteur des services de taxis et b) modification du Code de la consommation

Délibération n° 37/2015
du 6 février 2015

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 l'ancien Ministre du Développement durable et des Infrastructures en date du 19 avril 2013, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n° 6588 portant a) organisation du secteur des services de taxis et b) modification du Code de la consommation, déposé à la Chambre des Députés en date du 21 juillet 2013.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur

la protection des données, soulevées plus particulièrement par l'article 20 du projet de loi sous examen.

L'objectif principal du projet de loi est de réformer le secteur des services de taxis au Luxembourg, et ce notamment en instaurant un régime d'autorisation centralisé, en renforçant les conditions d'accès aux activités d'exploitant et de conducteur de taxi, en diversifiant les contrôles et en facilitant les sanctions applicables. Entre autres, il est prévu de créer un registre des exploitants et des conducteurs de taxi, tenu auprès du Ministère du Développement durable et des Infrastructures, dans lequel figureraient notamment les données nécessaires à la gestion administrative et au suivi des licences d'exploitation de taxi et des cartes de conducteur de taxi. Ce registre servirait en outre aux membres de la police grand-ducale et aux agents de l'administration des douanes et accises dans l'exercice des missions leurs conférées en vertu du projet de loi sous analyse, notamment en ce qui concerne les contrôles susmentionnés.

1. Détermination du responsable du traitement

Il ressort des dispositions de l'article 20, paragraphe (1) du projet de loi sous analyse que le ministre ayant les transports dans ses attributions tient le registre pré-mentionné. Dans sa version actuelle, il ne résulte cependant pas clairement du texte en projet qui est le responsable du traitement. 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 également toutes les questions de responsabilité dépendent directement de cette désignation. Il a ainsi notamment l'obligation de veiller à la confidentialité et à la sécurité des données et il doit mettre en place l'organisation appropriée des mesures techniques.

A la lecture des dispositions pré-mentionnées, la Commission nationale comprend qu'il est dans l'intention des auteurs du texte d'attribuer la responsabilité du traitement au ministre ayant les transports dans ses attributions. Elle suggère dès lors de préciser que ledit ministre est à considérer comme responsable du traitement au sens de l'article 2, lettre (n) de la loi modifiée du 2 août 2002.

2. Finalités du traitement de données à caractère personnel et catégories de données collectées et traitées

L'alinéa 2 du paragraphe (1) de l'article 20 prévoit que le registre contient les données (i) des exploitants de taxis, (ii) des intéressés figurant sur la liste d'attente telle que précisée à l'article 8, paragraphe (3) et (iii) des conducteurs. L'alinéa deux du même article précise en détail toutes les opérations de traitement qui peuvent être effectuées sur ces données.

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* ». *Par ailleurs, les données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ;*[1] ».

Le texte sous analyse ne précise cependant ni le contenu exact du registre, ni n'explique comment ledit registre est alimenté concrètement en données. En effet, le texte sous analyse se limite à énoncer que figurent dans le registre « *toutes les données nécessaires…* » (art. 20 para. (1)), et précise dans son paragraphe 2 que le ministre peut «*…s'entourer de toutes les informations requises…* ». Ces formulations sont cependant trop vagues car elles permettraient au responsable du traitement de collecter d'autres données supplémentaires que celles strictement nécessaires au

[1] Article 4, paragraphe (1), lettre (b) de la loi.

traitement envisagé. Aux yeux de la CNPD, ces dispositions ne respectent pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal, et ne sont par ailleurs pas conformes à l'article 4 précité.

Dans cet ordre d'idées, le texte ne mentionne pas non plus l'origine des données collectées et traitées dans le registre. En effet, il faudrait préciser et énumérer (i) quelles données proviennent d'autres fichiers, ou autrement dit, à quelles données précises, contenues dans d'autres fichiers étatiques, le ministre peut avoir accès et (ii) quelles données proviennent directement des demandeurs et intéressés. En l'état actuel, il ne ressort qu'implicitement du texte sous analyse que le nouveau fichier du « registre des exploitants de taxi, des conducteurs et des inscrits sur la liste d'attente » sera constitué, d'une part, de données transmises par les administrés au ministère et, d'autre part, de données provenant des bases de données telles que décrites dans le paragraphe (2) de l'article 20 [2].

La Commission nationale recommande dès lors de restructurer l'article 20, en précisant :

- le responsable du traitement,
- les finalités claires et précises du traitement, telles que l'octroi et le suivi des licences d'exploitation de taxi, la gestion de la liste d'attente, etc.,
- une énumération exhaustive des catégories de données concernées, avec indication de leur origine.

Tant que les finalités ainsi que les catégories de données destinées à être collectées et traitées n'ont pas été clairement précisées, la Commission nationale se voit dans l'impossibilité d'évaluer le respect des principes de nécessité et de proportionnalité des données au regard des finalités poursuivies.

3. Prolifération des accès à divers fichiers étatiques et mise en place d'une solution technique

Dans le cadre de l'instruction des procédures administratives prévues par le projet de loi, le paragraphe (2) de l'article 20 prévoit que le ministre ayant les transports dans ses attributions *« peut s'entourer de toutes les informations requises… »* et qu'il *« …peut notamment accéder …»* à différents autres fichiers étatiques.

Selon le principe de proportionnalité et de nécessité, tout traitement de données à caractère personnel doit être proportionné aux finalités à

[2] Voir aussi la partie ci-après sur la prolifération des accès aux fichiers étatiques.

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* »[3].

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 administrative des conducteurs et exploitants de services de taxis, le suivi afférent des licences et autorisations, ainsi que la vérification du respect des conditions posées par la loi dans le cadre des contrôles opérés par la police grand-ducale et les douanes 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 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 au nombre des conducteurs de taxis, d'exploitants de taxi ainsi qu'aux gens inscrits sur la liste d'attente de l'article 8 paragraphe (3), donc un nombre assez limité de personnes. L'article 20 paragraphe (2) du projet de loi sous objet, dans sa rédaction actuelle, permettrait cependant un accès aux données contenues dans des fichiers ou registres concernant l'ensemble de la population luxembourgeoise (dans le cas du registre national des personnes physiques).

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[4], que soit prévue la mise en place d'une solution technique permettant de garantir,

---

[3] Arrêt du 9 novembre 2010, Schecke et al., C-92/09 et C-93/09, point 74 et jurisprudence citée.

[4] 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.

d'un point de vue informatique, que les agents du ministère du Développement durable et des Infrastructures puissent seulement accéder aux données concernant les personnes qui ont introduit une demande auprès du ministère précité dans le cadre d'une demande en obtention d'une licence d'exploitation de taxi ou demande en obtention d'une carte de conducteur de taxi, à l'exclusion des données relatives au reste de la population. En d'autres termes, seule l'ouverture d'un dossier administratif à l'occasion de l'introduction de telles demandes ouvrirait aussi le droit pour ledit ministère d'accéder aux fichiers visés à l'article 20 paragraphe (2) et auxquels il n'aurait pas accès en l'absence de dossier. Le texte du projet de loi devrait être adapté en ce sens.

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 ministère précité puisse accéder aux fichiers d'autres administrations.

4. Accès direct au nouveau registre par les forces de l'ordre

Le troisième alinéa du paragraphe (1) de l'article 20 du projet sous analyse accorde un accès direct aux données du registre, au moyen d'un système informatique, aux membres de la police grand-ducale et aux fonctionnaires de l'administration des douanes et accises dans l'exercice des missions qui leur sont conférées par le présent projet de loi. En effet, le nouveau registre ne servira pas uniquement de base pour la gestion des demandes de licences d'exploitation de taxi ou de cartes de conducteur de taxi ainsi qu'à leur confection, mais permettra aussi aux forces de l'ordre de diversifier et de faciliter leurs contrôles par rapport aux potentielles infractions commises par les conducteurs ou les exploitants de taxis. Le registre contiendrait donc un nombre important de données nécessaires aux forces de l'ordre pour vérifier la conformité ou non aux dispositions érigées en infraction pénale.

La CNPD ne s'oppose pas au principe d'un tel accès par les forces de l'ordre aux données contenues dans le registre pour la finalité indiquée. Elle se demande cependant si cette disposition ne devrait pas être intégrée dans le corps de l'article 34-1 la loi modifiée du 22 juillet 2008 qui précise notamment les fichiers auxquels les forces de l'ordre peuvent avoir accès, ainsi que les conditions dans lesquelles de tels accès peuvent être opérés.

Se pose par ailleurs la question si les membres de la police doivent avoir accès à l'intégralité des données du registre ou s'il ne faudrait pas limiter cet accès aux données effectivement nécessaires.

Si ces dispositions relatives aux accès par les forces de l'ordre aux données contenues dans le registre ne seraient pas intégrées dans le corps de la loi du 22 juillet 2008 précitée, la Commission nationale estime néanmoins nécessaire de prévoir un système de journalisation des accès et de rajouter une disposition en ce sens (voir point 6 du présent avis).

5. La problématique supplémentaire de l'accès au fichier du casier judiciaire

Même s'il est envisagé d'obtenir l'accord de la personne concernée pour accéder à son casier judiciaire, la CNPD estime néanmoins qu'un accès direct au fichier du casier judiciaire au moyen d'un système informatique tel qu'envisagé par le ministère est difficilement envisageable, alors que les dispositions de l'article 8 de la loi du 29 mars 2013 relative à l'organisation du casier judiciaire[5] prévoient limitativement tous les cas dans lesquels un extrait du casier peut être délivré. Considérant que l'on ne se trouve pas dans l'une de ces hypothèses et que la notion de délivrance du bulletin n°2 du casier judiciaire est à interpréter de manière stricte, notamment au vu de la sensibilité des données qu'il comporte, la Commission nationale recommande de biffer le point e) de l'article 20, paragraphe (2) du projet de loi.

Etant donné que le ministère de la justice travaille actuellement sur un projet de réforme de ladite loi du 29 mars 2013, la CNPD suggère de régler cette problématique dans le cadre de ce projet de réforme.

A toutes fins utiles, la Commission nationale voudrait relever une erreur matérielle à la fin de l'énumération des différents fichiers auxquels le ministère envisage d'accéder. En effet, elle devrait lire *« L'accès au fichier visé au point e) est conditionné à l'accord préalable de l'administré » et non pas « …visé au point d) … ».*

6. Traçage des accès aux données

Dans le contexte des mesures de sécurité et de confidentialité des traitements dont question aux articles 22 et 23 de la loi modifiée du 2 août 2002, la CNPD estime également nécessaire de prévoir un système de journalisation des accès aux données. Ainsi, à l'instar d'autres textes légaux, il conviendrait de remplacer le paragraphe (3) de l'article 20 par une disposition qui pourrait avoir la teneur suivante :

« Le système informatique par lequel l'accès ou le traitement des données à caractère personnel 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 pour chaque traitement ou consultation avec l'identifiant numérique personnel de la personne qui y a procédé. 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*

[5] 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 modifiant : 1) le code d'instruction criminelle ; 2) le code pénal ; 3) la loi modifiée du 13 juillet 1949 ayant pour objet de majorer certains droits d'enregistrement et de timbre et des taxes diverses ; 4) la loi modifiée du 12 janvier 1955 portant amnistie de certains faits punissables et commutation de certaines peines en matière d'attentat contre la sûreté extérieure de l'état ou de concours à des mesures de dépossession prises par l'ennemi et instituant des mesures de clémence en matière d'épuration administrative ; 5) la loi modifiée du 7 mars 1980 sur l'organisation judiciaire.

7 Annexes

à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle. »

7. Durée de conservation des données

Le projet de loi est muet sur la question de la durée de conservation des données.

Selon l'article 4 paragraphe (1) lettre (d) de la loi du 2 août 2002, celles-ci peuvent en effet seulement être « *conservées 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 (…)* » .

La CNPD estime dès lors nécessaire de prévoir une disposition réglant la durée de conservation des données à caractère personnel.

Ainsi décidé à Esch-sur-Alzette en date du 6 février 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

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

Délibération n°45/2015
du 6 février 2015

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 26 juin 2014, le Ministère de l'Economie a invité la Commission nationale à se prononcer au sujet du 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.

Par délibération du 12 juillet 2013, la Commission nationale avait déjà avisé l'avant-projet de règlement grand-ducal en question en relevant certains points qui nécessitaient soit davantage de précisions, soit des modifications. Après examen du présent projet de règlement grand-ducal, la CNPD salue les corrections qui y ont été apportées par rapport à l'avant-projet, mais se doit également de soulever les points suivants :

1) Ad articles 1 et 2

L'article 1 du projet de règlement grand-ducal indique que le Ministre ayant l'Economie dans ses attributions met en oeuvre les traitements de données à caractère personnel nécessaires à l'exécution de la loi du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales. Cet article précise également un certain nombre de données qui sont traitées dans ce registre.

L'article 2 quant à lui énumère les données (contenues dans d'autres fichiers étatiques) auxquelles le Ministre peut accéder via un système informatique direct afin de contrôler si une personne satisfait aux exigences posées par la loi du 2 septembre 2011.

Dans un souci de clarté, la Commission nationale suggère de restructurer l'article 1 du projet de règlement grand-ducal en y intégrant aussi l'article 2. En effet, cela permettra de préciser dans un seul article quelles données à caractère personnel sont collectées et traitées dans le registre ainsi que l'origine de celles-ci.

La Commission nationale propose ainsi de modifier l'article 1 du projet de règlement grand-ducal qui pourrait avoir la structure suivante :

« Art. 1er. (1) (inchangé)

(2) Le registre visé à 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 contient les données à caractère personnel suivantes :

1. *Les données collectées directement auprès des personnes soumises à une déclaration préalable ou qui sont demandeurs ou titulaires d'une autorisation d'établissement :*

- *Noms, prénoms, coordonnées … (etc.)*
- *(…)*

2. *Les données collectées via un système informatique direct, issues des fichiers visés au paragraphe (2) de l'article 32 de la loi du 2 septembre 2011 :*

- *(a) pour le registre général des personnes physiques (…)*
  - *o – le numéro d'identification national ;*
  - *o – (…)*
- *(b) pour le fichier du Registre de commerce et des sociétés (…)*
  - *o – (…)*
- *(…)*
- *(h) (…)*

3. *Les autres données et informations créées par le ministère dans le cadre de la gestion et du suivi des autorisations d'établissement :*

- *les dates de délivrance, de prolongation, de révocation ou d'annulation des autorisations d'établissement, (…)*
- *(…)*

(3) (inchangé) »

- En ce qui concerne l'article 1 paragraphe (2) dernier tiret du projet de règlement grand-ducal

Dans son avis relatif à la version de l'avant-projet de règlement grand-ducal, la Commission nationale estimait que le dernier tiret de l'article 1 paragraphe (2) *(« toutes autres informations fournies par l'administré ou par d'autres administrations »)* était trop vague et constituait en quelque sorte une catégorie *« fourre-tout »*. Dans le projet

de règlement sous examen, ledit tiret a été complété par les termes « *qui sont requises par la loi du 2 septembre 2011 pour le traitement des dossiers d'autorisation d'établissement* ».

Si le projet de règlement grand-ducal prend ainsi soin de préciser pour quelle finalité ces données sont accédées, la Commission nationale maintient néanmoins son point de vue que la formulation de l'ajout proposé reste trop vague car il permettrait au responsable du traitement de collecter d'autres données supplémentaires que celles strictement nécessaires au traitement envisagé. Aux yeux de la CNPD, une telle disposition ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal et n'est par ailleurs pas conforme à l'article 4 paragraphe (1) de la loi modifiée du 2 août 2002 qui exige que l'utilisation des données traitées doit se limiter aux finalités pour lesquelles elles ont été collectées et que les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées.

En effet, si l'article 32 paragraphe (2) dernier tiret de la loi du 2 septembre 2011 prémentionnée prévoit qu'un règlement grand-ducal doit être pris pour préciser les «conditions, critères et modalités» de l'accès direct aux données, il faudrait alors aussi que les dispositions de celui-ci soient suffisamment détaillées et précises pour ne plus laisser place à interprétation. Dès lors, la Commission nationale propose soit de déterminer avec précision de quelles données il s'agit, soit de supprimer le dernier tiret de l'article 1 paragraphe (2) du règlement grand-ducal dans son intégralité.

- <u>En ce qui concerne l'article 2 lettre (a) du projet de règlement grand-ducal</u>

La Commission nationale avait considéré, lors de son avis relatif à l'avant-projet de règlement grand-ducal, que des précisions relatives à l'article 2 lettre (a) devraient être fournies, afin de clarifier quelles données des « *ascendants et descendants* » de la personne concernée pouvaient être accédées, en partant du principe que seules les données des ascendants et descendants au premier degré étaient concernées (conformément à l'article 5 paragraphe (2) lettres (j) et (k) de la loi du 19 juin 2013 relative à l'identification des personnes physiques).

Dans le texte sous examen, les auteurs ont modifié et précisé le texte en indiquant « *pour les besoins de l'article 36 de*

la loi du 2 septembre 2011, les ascendants et descendants tels que prévus à l'article 5 paragraphe (2) lettre (j) de la loi du 19 juin 2013 précitée ». Or, l'article 5 paragraphe (2) lettre (j) de la loi du 19 juin 2013 faisant uniquement référence aux ascendants, la Commission nationale est à se demander s'il n'y aurait pas lieu de compléter la disposition en faisant également référence aux descendants visés par l'article 5 paragraphe (2) lettre (k) de ladite loi de 2013.

Par ailleurs, l'article 36 de la loi du 2 septembre 2011 relatif à la *« transmission de l'entreprise »* ne fait pas seulement référence aux *« ascendants et descendants »*, mais de façon globale au *« conjoint, à un descendant, à un ascendant ou à un collatéral ou allié jusqu'au troisième degré ».* La Commission nationale s'interroge dès lors sur la nécessité de compléter le projet de règlement grand-ducal en ce sens, afin d'éviter que le texte final du règlement grand-ducal soit incomplet et ne puisse pas répondre à la finalité recherchée par l'article 36.

2) Ad article 3

Cet article prévoit que l'accès aux données et informations figurant dans les différents fichiers étatiques visés à l'article 2 est limité aux seuls agents autorisés et nommément désignés par le ministère en fonction de leurs attributions.

Il convient cependant d'éviter que des *« fishing expeditions »* puissent avoir lieu, c'est-à-dire que les agents du ministère puissent accéder indistinctement aux données contenues dans ces fichiers relatives à des personnes non demandeurs ou titulaires d'une autorisation d'établissement.

La Commission nationale estime dès lors nécessaire, comme elle l'a déjà soulevé dans ses avis antérieurs relatifs à des textes de loi similaires[6], 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 ayant l'Economie dans ses attributions puissent seulement accéder aux données concernant les personnes qui ont introduit une notification préalable ou une demande auprès du ministère précité dans le cadre de l'article 32 de la loi du 2 septembre 2011, à l'exclusion des données relatives au reste de la population concernée (résidente ou non). En d'autres termes, seule l'ouverture d'un dossier administratif à l'occasion de l'introduction d'une notification ou demande ouvrirait aussi le droit pour ledit ministère d'accéder aux fichiers visés à l'article 2 du projet de règlement grand-ducal et auxquels il n'aurait pas accès en l'absence de dossier. Le texte du projet de règlement grand-ducal devrait être adapté en ce sens.

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 ministère précité puisse accéder aux fichiers d'autres administrations.

3) Ad article 4

Cet article instaure les principes de traçabilité et en détermine les modalités.

La Commission nationale propose de rajouter au texte existant les dispositions qui suivent :

« Le système informatique par lequel l'accès ou le traitement des données à caractère personnel 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*

[6] 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 relative au projet de loi n°6588 portant a) organisation du secteur des services de taxis et b) modification du Code de la consommation

Annexes

fichiers de données à caractère personnel qui sont gérés par le ministre ayant l'Economie 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 pour chaque traitement ou consultation avec l'identifiant numérique personnel de la personne qui y a procédé. Lors de chaque traitement de données … (inchangé) … »

4) Durée de conservation des données à caractère personnel

La Commission nationale propose d'ajouter un nouvel article relatif à la durée de conservation des données du registre tenu par le ministère ayant l'Economie dans ses attributions.

En effet, le projet de loi est muet sur la question de la durée de conservation des données.

Selon l'article 4 paragraphe (1) lettre (d) de la loi du 2 août 2002, celles-ci peuvent en effet seulement être « *conservées 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 (…)* ».

La CNPD estime dès lors nécessaire de prévoir une disposition réglant la durée de conservation des données à caractère personnel.

Pour le surplus, la Commission nationale constate avec satisfaction que toutes les autres recommandations formulées dans sa délibération du 12 juillet 2013 ont été suivies, de sorte qu'elle n'a plus d'autres observations à soulever quant aux articles restants.

Ainsi décidé à Esch-sur-Alzette en date du 6 février 2015.
La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis à l'égard du projet de loi n°6714 portant création du système de contrôle et de sanction automatisé et modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques, et du projet de règlement grand-ducal autorisant la création d'un fichier et le traitement de données à caractère personnel dans le cadre du système de contrôle et de sanction automatisé

Délibération n°74/2015
du 25 février 2015

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 du Développement durable et des Infrastructures en date du 14 juillet 2014, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de :

- l'avant-projet (entretemps devenu projet) de loi n°6714 portant création du système de contrôle et de sanction automatisé et modification de la loi modifiée du 14 février 1955 concernant la réglementation de la circulation sur toutes les voies publiques,
- et de l'avant-projet (entretemps devenu projet) de règlement grand-ducal autorisant la création d'un fichier et le traitement de données à caractère personnel dans le cadre du système de contrôle et de sanction automatisé.

Les projets de loi et de règlement grand-ducal sous avis ont pour objectif de mettre en place un système de contrôle et de sanction automatisé (« CSA ») visant à automatiser la constatation de certaines infractions routières et la sanction subséquente du contrevenant présumé de l'infraction. Ainsi sera facilitée la constatation, sans interception des véhicules, de certaines infractions au code de la route, et en particulier, mais non exclusivement, du non-respect des vitesses maximales autorisées. Un tel système devrait permettre, d'après le Gouvernement, de réduire le nombre d'infractions et, partant, d'améliorer la sécurité sur les routes luxembourgeoises.

Dans ce contexte, il est proposé de créer un centre de traitement des infractions routières (« le centre ») qui a pour mission la gestion du système de CSA et qui est exploité par la Police grand-ducale, sous la surveillance du procureur d'Etat. Il ressort des projets de loi et de règlement grand-ducal sous objet que la Police grand-ducale mettra dans ce cadre en œuvre un traitement de données à caractère personnel au sens de l'article 2 lettre (r) de la loi 2 août 2002.

D'emblée, la Commission nationale tient à saluer la référence dans les projets de loi et de règlement grand-ducal sous examen aux termes et concepts de la loi du 2 août 2002. Elle se félicite également de ce que les principes issus de cette loi, et notamment les principes de finalité, de nécessité et proportionnalité, de loyauté et transparence, ou encore le droit d'accès des personnes concernées, ont été de manière générale intégrés dans les projets de loi et règlement grand-ducal sous examen.

La CNPD tient cependant à faire part ci-après de ses observations par rapport à certains articles de ces projets présentant des aspects ayant trait à la protection des données.

1. Remarques préliminaires

La Commission nationale souhaite attirer l'attention des auteurs du projet de loi et de 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* »[7]. 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* »[8].

Or, la CNPD constate que la plupart des conditions et modalités du traitement sont inscrites dans le projet de règlement grand-ducal. Pour des raisons de légistique, la CNPD se demande si pratiquement toutes les dispositions figurant actuellement dans le projet de règlement grand-ducal ne devraient pas figurer dans la loi.

Par ailleurs, la Commission nationale comprend, après communications reçues des services du ministère du développement durable et des infrastructures, et suivant le commentaire de l'article 2 du projet de loi[9], que certaines données figurant dans le fichier dont il est question à l'actuel article 1er paragraphe (1) premier alinéa du projet de règlement grand-ducal (que l'on pourrait appeler « fichier CSA ») se retrouvent dans deux fichiers, à savoir, d'une part, le fichier des personnes ayant subi un avertissement taxé en matière de circulation routière[10] (« fichier avertissement taxé »), et d'autre part, la banque de données nominatives de police générale[11] (« fichier Ingepol »).

La CNPD se demande dès lors si le fichier « CSA » intégrera des données d'autres fichiers, et notamment des fichiers « avertissement taxé » et « Ingepol », et des données auxquelles les personnes visées à l'article 3 du projet de règlement grand-ducal pourront accéder dans le cadre de cet article, pour former un nouveau fichier. Ou s'agit-il, au contraire, de fichiers distincts, entre lesquels il y aurait le cas échéant communication de données ?

En tout état de cause, toutes les opérations de traitement (collecte de données, communication de données, accès de données figurant dans un autre fichier, interconnexions de fichiers[12], etc.) doivent être précisées dans la loi, puisqu'il s'agit de traitements de données à caractère personnel au sens de l'article 2 lettre (r) de la loi du 2 août 2002.

---

7 Cour constitutionnelle, arrêt 108/13 du 29 novembre 2013 (Mém. A n°217 du 13 décembre 2013, p. 3886).
8 Avis du Conseil d'Etat du 9 décembre 2014 à l'égard du projet loi 6588 portant organisation du secteur des services de taxis et modification du Code de la consommation, p. 7 (article 5). Voir aussi p. 19 (article 20).
9 *Cf.* commentaire des articles, pp. 10-11.
10 Créé par le 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.
11 Créée par le règlement grand-ducal modifié du 2 octobre 1992 relatif à la création et l'exploitation d'une banque de données nominatives de police générale.
12 Voir à cet égard la remarque infra de la CNPD relative à l'article 3 paragraphe (3) du projet de règlement grand-ducal, ayant trait à la notion d'interconnexion.

La CNPD relève en outre qu'une des finalités prévues dans l'actuel projet de loi[13] consiste à « *transmettre au ministre ayant les transports dans ses attributions les données nécessaires pour procéder, le cas échéant, à la réduction des points dont est doté le permis de conduire, conformément à l'article 2bis de la loi modifiée du 14 février 1955 précitée* ». Afin que la Commission nationale puisse apprécier le caractère proportionné d'un tel traitement au regard de sa finalité, il serait utile de préciser exactement quelles données ou catégories de données sont visées par cette disposition.

De façon plus générale, elle est à se demander s'il ne serait pas utile de préciser quelles sont les données ou catégories de données nécessaires permettant de réaliser chacune des finalités prévues dans l'actuel article 2 du projet de loi sous examen. En l'absence d'une telle précision, il serait en effet difficile pour la CNPD d'apprécier, conformément à l'article 4 paragraphe (1) lettre (b) de la loi du 2 août 2002, le caractère adéquat, pertinent et non excessif de certaines données envisagées dans le projet de règlement grand-ducal[14].

2. Article 4 du projet de loi

L'article 4 paragraphe (1), quatrième alinéa du projet de loi sous objet dispose que « *lorsque le véhicule à l'aide duquel une infraction est commise est loué à un tiers au moment de l'infraction, la présomption de responsabilité pécuniaire prévue à l'alinéa premier incombe au locataire, sous les réserves prévues au paragraphe (2)* ».

La Commission nationale note à cet égard qu'il est prévu, d'après le commentaire des articles du projet de loi[15], que « *le centre pourra identifier le locataire au moyen de requêtes automatisées dans les fichiers des différentes sociétés de location de véhicules, afin de rechercher l'auteur d'infraction selon la procédure légale prévue dans le cadre du système CSA. La Fédération Luxembourgeoise des Loueurs de Véhicules (FLLV), qui représente 95% des sociétés de location de véhicules, s'est montrée a priori ouverte à l'approche préconisée, de sorte qu'il est proposé que les sociétés de location de véhicules seront obligées de donner accès à la Police grand-ducale à leurs fichiers respectifs* ».

La CNPD tient à remarquer que cette procédure suppose que les sociétés privées de location de voitures soient obligées de tenir un tel fichier. Cette obligation de détenir un fichier devrait le cas échéant être inscrite dans la loi.

En outre, si un tel accès était accordé à la Police grand-ducale, il s'agirait d'un traitement de données à caractère personnel[16], qui devrait à ce titre également figurer dans le projet de loi sous objet, de même que les données auxquelles auraient accès les services de police, et les finalités pour lesquelles il serait réalisé. De plus, la procédure d'accès devrait dans ce cas être accompagnée de garanties appropriées en matière de protection des données, et notamment la garantie que la Police puisse seulement accéder par requête informatique aux données des personnes qui ont déjà commis une infraction, à l'exclusion des personnes non concernées.

3. Article 5 du projet de loi

La CNPD s'interroge sur la pertinence des termes « au moins » apparaissant dans la première phrase de l'article 5 paragraphe (2) du projet de loi sous objet. La liste énumérant les informations devant figurer dans le courrier envoyé à la personne présumée pécuniairement responsable ne devrait-elle pas être exhaustive ?

4. Article 8 du projet de loi

La CNPD se félicite de la décision de ne pas introduire le principe du versement préalable d'une consignation en cas de

---

[13] Plus précisément dans son article 2 paragraphe (1) numéro (6).
[14] La CNPD a déjà eu l'occasion d'expliquer cette position dans son avis 238/2010 du 26 juillet 2010 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.
[15] *Cf.* commentaire des articles, p. 14.
[16] Au sens de l'article 2 lettre (r) de la loi du 2 août 2002.

contestation, comme c'est le cas en France[17].

Par ailleurs, elle comprend que l'exercice du droit de contestation n'interrompt pas mais suspend le délai de prescription, « *en ce sens qu'après la contestation les délais recommencent à courir tout en tenant compte du temps déjà écoulé* »[18]. La formulation du paragraphe (3) pourrait cependant paraître quelque peu équivoque en n'indiquant pas que le délai est dans ce cas suspendu.

5. Article 10 du projet de loi

La Commission nationale prend note du choix du gouvernement « *de ne pas transmettre d'office à tous les contrevenants présumés la photo du véhicule en infraction et d'alourdir par là le système dans son ensemble* »[19]. L'article 10 paragraphe (2) du projet de loi sous examen prévoit en ce sens que « *toute personne présumée pécuniairement responsable ou ayant été désignée comme conducteur du véhicule au moment de l'infraction a le droit de consulter la photo concernant le véhicule en infraction et les données à caractère personnel la concernant traitées dans le cadre de l'exploitation du système CSA* »[20]. Cette consultation « *se fait au Centre et sous le contrôle de la police grand-ducale* »[21].

Toutefois, la CNPD se demande si l'obligation pour la personne pécuniairement responsable ou la personne désignée comme conducteur du véhicule au moment de l'infraction de se déplacer au Centre, dont l'implantation est envisagée à Bertrange[22], ne constitue pas un obstacle injustifié au droit d'accès de cette personne. Cette problématique apparaît d'autant plus importante pour les personnes résidant à une grande distance du Centre, ainsi que pour les non-résidents.

La Commission nationale tient à souligner à cet égard que le droit d'accès doit s'exercer, aux termes de l'article 28 paragraphe (1) de la loi du 2 août 2002, « *sur demande à introduire auprès du responsable du traitement* » et « *sans frais, à des intervalles raisonnables et sans délais excessifs* ». Il ressort en outre des travaux parlementaires de la loi du 2 août 2002[23] qu'« *il est fondamental que le droit d'accès soit garanti et qu'il puisse s'exercer sans contrainte et sans frais (…)* ».

La CNPD estime dès lors nécessaire d'adapter le paragraphe (2) de l'article 10 du projet de loi sous objet en permettant à la personne pécuniairement responsable ou la personne désignée comme

---

[17] *Cf.* commentaire des articles, p. 17.
[18] *Cf.* commentaire des articles, p. 18.
[19] *Cf.* commentaire des articles, p. 19.
[20] Article 10 paragraphe (1) du projet de loi sous examen.
[21] Article 10 paragraphe (2) du projet de loi sous examen.
[22] *Cf.* commentaire des articles, p. 19.
[23] Projet de loi relatif à la protection des personnes à l'égard du traitement des données à caractère personnel, document parlementaire 4735/00 du 7 décembre 2000, commentaires des articles, p. 44.

conducteur du véhicule au moment de l'infraction de consulter la photo concernant son véhicule, selon son choix, sur place au Centre, ou de recevoir communication de la photo via une demande écrite préalable adressée au Centre.

Par ailleurs, le paragraphe (3) du même article prévoit que « *lors de l'exercice du droit d'accès, toute personne autre que le conducteur est masquée sur la photo exhibée, sauf exception dûment justifiée* ». La CNPD se félicite de cette disposition qui garantit le respect de la vie privée des personnes tierces et des conducteurs.

Elle se demande cependant s'il ne faudrait pas, dès la prise de la photo, masquer automatiquement l'image du passager, ce dernier n'ayant en effet pas de lien avec l'infraction. En effet, pourquoi les agents de police du Centre devraient-ils pouvoir visionner et le cas échéant identifier les passagers ? Ce n'est qu'à l'occasion d'une éventuelle procédure judiciaire que l'image du passager pourrait, au besoin, être rendue visible.

6. Article 2 du projet de règlement grand-ducal

La Commission nationale se réfère à ses explications développées ci-dessus sous le point 1, concernant le besoin, pour des raisons de légistique, d'intégrer certaines dispositions figurant actuellement dans le projet de règlement grand-ducal dans la loi.

Par ailleurs, elle suggère de rajouter aux termes « *les informations* » de la première phrase de l'article 2 les mots « *et les données* », pour aligner la terminologie sur celle utilisée dans la loi du 2 août 2002[24].

Enfin, elle se demande si les termes utilisés dans les numéros (6) second alinéa[25], (7)[26] et (8)[27] n'apparaissent pas trop vagues, et ne mériteraient pas davantage de précisions.

7. Article 3 du projet de règlement grand-ducal

La CNPD relève tout d'abord que le titre de l'article, à savoir « *Consultation des données* », n'apparaît pas tout-à-fait approprié à l'hypothèse prévue dans ce projet d'article, et préférerait une formulation telle que « *Accès aux données figurant dans d'autres fichiers étatiques* ».

Le paragraphe (2) de l'article 3 du projet de règlement grand-ducal sous objet, quant à lui, prévoit dans sa rédaction actuelle que « *seules les données à caractère personnel strictement nécessaires, dans le respect du principe de proportionnalité, peuvent être consultées* ». Les termes « strictement nécessaires » apparaissent très vagues et ne permettent pas à la Commission nationale d'apprécier le caractère adéquat, pertinent et non excessif des données qui peuvent être consultées. Aux yeux de la CNPD, cette disposition ne respecte donc pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal, et n'est guère conforme à l'article 4 de la loi modifiée du 2 août 2002. La CNPD estime indispensable d'indiquer quelles sont les données ou catégories de données nécessaires parmi celles visées dans le paragraphe (1) que les personnes habilitées pourraient consulter afin de réaliser les finalités à préciser.

Enfin, le paragraphe (3) du même article prévoit que les données contenus dans le fichier créé en vertu de l'article 1 paragraphe (1) peuvent faire l'objet d'une « *interconnexion, mise en relation ou rapprochement* ». La Commission nationale comprend cependant qu'il ne s'agit pas d'une interconnexion de données au sens de l'article 16 de la loi du 2 août 2002, mais bien d'un accès aux données visées dans

[24] Et définie dans l'article 2 lettre (e) de cette loi.
[25] « *Les données relatives aux contestations* ».
[26] « *Les données relatives aux avertissements taxés, dont le paiement des avertissement taxés* ».
[27] « *Les données relatives aux procès-verbaux* ».

Annexes

l'article 2 par communication aux personnes visées dans l'article 3 du projet de règlement grand-ducal. La CNPD suggère d'adapter la formulation du paragraphe (3) en conséquence.

8. Article 4 du projet de règlement grand-ducal

La Commission nationale s'interroge pourquoi l'article 4 lettre (a) du projet de règlement grand-ducal sous examen prévoit que la police grand-ducale soit destinataire des données enregistrées dans le cadre du système de CSA, alors que c'est justement elle, par l'intermédiaire de son Directeur général, qui a la qualité de responsable du traitement[28].

Serait-ce pour permettre à la police grand-ducale de poursuivre d'autres infractions de droit commun ? Dans ce cas, il ne s'agirait pas d'une transmission des données mais bien d'un traitement ultérieur ou d'un traitement visé le cas échéant par l'actuel article 2 paragraphe (3) du projet de loi.

Par ailleurs, l'article en question ne précise pas quelles catégories de données sont susceptibles d'être transmises aux destinataires visés aux lettres a), b) et c). La CNPD comprend que du fait de leurs missions légales, l'intégralité des données figurant dans le fichier sont susceptibles d'être communiquées à la police grand-ducale et aux autorités judiciaires luxembourgeoises (lettres a) et b)). Il y aurait par contre lieu de préciser quelles données sont transmises au ministre ayant dans ses attributions les Transports (lettre c)).

9. Article 5 du projet de règlement grand-ducal

La CNPD note que le projet de règlement grand-ducal prévoit plusieurs durées de conservation dans son article 5, à savoir deux semaines après l'acquittement de l'avertissement taxé pour les photos enregistrées respectivement deux mois après leur enregistrement si elles ne sont pas exploitables[29], trois ans après le paiement de l'avertissement taxé pour les autres données[30], et après l'expiration du délai de prescription de l'action publique au cas où une infraction constatée ne donne lieu à établissement ni d'un avertissement taxé, ni d'un procès-verbal[31].

Elle rappelle que les données doivent être de manière générale « *conservées 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* »[32].

---

[28] Aux termes de l'article 1er paragraphe (3) du projet de règlement grand-ducal sous analyse.
[29] Article 5, paragraphe (1) du projet de règlement grand-ducal sous objet.
[30] Article 5, paragraphe (2) du projet de règlement grand-ducal sous objet.
[31] Article 5, paragraphe (4) du projet de règlement grand-ducal sous objet.
[32] Article 4, paragraphe (1), lettre (d) de la loi du 2 août 2002.

A défaut de précisions et d'explications quant aux différentes durées de conservation des données susmentionnées dans le commentaire des articles, la Commission nationale n'est pas en mesure d'apprécier le caractère proportionné ou non des durées de conservation indiquées.

10. Article 6 du projet de règlement grand-ducal

La Commission nationale suggère de remplacer les termes « l'accès aux traitements de données » par « les traitements de données » au début de l'article 6 du projet de règlement grand-ducal sous analyse, étant donné que c'est bien l'ensemble du traitement de données qui est soumis à la surveillance de l'autorité de contrôle visée à l'article 17 paragraphe (2) de la loi du 2 août 2002, et non pas seulement les accès.

Le deuxième alinéa du même article du projet de règlement grand-ducal prévoit une mesure 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 du 2 août 2002, comme elle a déjà eu l'occasion de le souligner dans plusieurs avis portant sur des projets de loi ou de règlement grand-ducal récents[33].

Cependant, la CNPD suggère de préciser davantage ce que recouvrent les termes « identifiant numérique personnel » de la lettre (a) de ce deuxième alinéa. En tout état de cause, la CNPD suggère que l'accès aux fichiers soit sécurisé moyennant une authentification forte (par exemple via le système d'authentification « LuxTrust »). Par ailleurs, la Commission nationale se demande s'il ne serait pas opportun d'ajouter l'information selon laquelle les personnes habilitées ne puissent consulter les fichiers auxquels ils ont accès que pour un motif précis qui doit être indiqué pour chaque traitement ou consultation.

11. La question des décisions automatisées

L'article 31 de la loi du 2 août 2002 précise qu'*« une personne peut être soumise à une décision individuelle automatisée produisant des effets juridiques à son égard, si cette décision (…) est autorisée par la loi, qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée »*.

Dans cette optique, il est important que ce soit un agent de police ou membre du parquet qui prenne la décision finale quant à la constatation d'une infraction au moyen du système de CSA, et non que cette décision découle de façon complètement automatisée du système sans intervention humaine.

A défaut de précisions ou d'explications sur le rôle des agents de police dans la mise en œuvre du système de CSA, la Commission nationale n'est pas en mesure d'apprécier si les personnes concernées peuvent être soumises à des décisions individuelles automatisées dans le cadre des projets de loi et de règlement grand-ducal sous objet, et dans l'affirmative, si des mesures de sauvegarde de l'intérêt des personnes existent.

12. La question des radars tronçons

La Commission nationale comprend que le gouvernement envisage la mise en place de radars dits « tronçons » ou de type « section control ». Il s'agit d'un système qui permet de contrôler la vitesse moyenne d'un véhicule entre deux points, au moyen de deux radars placés à ces deux points. Le projet de loi sous examen y fait indirectement référence, notamment à l'article 3 paragraphe (3), deuxième alinéa du projet de loi sous objet. Si tel est bien le cas, il est nécessaire de prévoir le principe

[33] Voir entre autres :
- Délibération n°37/2015 du 6 février 2015 à l'égard du projet de loi n°6588 portant a) organisation du secteur des services de taxis et b) modification du Code de la consommation ;
- Délibération n°45/2015 du 6 février 2015 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.

Annexes

de l'utilisation des radars tronçons dans la loi.

En tout état de cause, il faudra prévoir un système permettant que les données (y compris les photographies) relatives aux personnes n'ayant pas commis d'infraction soient immédiatement et automatiquement détruites par le système mis en place, de telle sorte qu'aucune donnée à caractère personnel ne puisse plus être réutilisée. En effet, un système qui enregistrerait indistinctement des données relatives à des personnes n'ayant pas commis d'infraction ne serait guère conforme au droit européen eu égard à la jurisprudence de la Cour de Justice de l'Union européenne « Digital Rights » du 8 avril 2014[34].

A cet égard, la CNPD voudrait relever qu'en Suisse, le législateur a prévu pour le cas des radars tronçons que « *tous les véhicules sont certes photographiés aussi bien au début qu'à la fin du tronçon, mais uniquement depuis l'arrière; de plus, les données concernant les véhicules respectant la vitesse maximale autorisée sont ensuite détruites et ne sont pas transmises à des tiers ou comparées avec celles d'autres systèmes d'information. Les véhicules qui dépassent la vitesse prescrite sont par contre automatiquement photographiés depuis l'avant. Seules ces données sont ensuite transmises au service de police cantonale compétent pour sanctionner l'infraction* »[35]. Le gouvernement pourrait s'inspirer d'un tel système qui présente, aux yeux de la Commission nationale, des garanties solides du point de vue de la protection des données, puisqu'il n'est possible à aucun moment, ni pour la Police ni pour d'autres personnes, d'identifier un conducteur n'ayant pas commis d'infraction.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 25 février 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

---

[34] C.J.U.E., Grande Chambre, *Digital Rights Ireland Ltd et Seitlinger e.a. c. Irlande e.a.*, arrêts C-293/12 et C-594/12 du 8 avril 2014.

[35] Préposé fédéral à la protection des données et à la transparence (PFPDT), 18ème rapport d'activité, 2010/2011, p. 22, disponible à l'adresse suivante : http://www.edoeb.admin.ch/dokumentation/00153/00184/index.html?lang=fr.

Avis relatif au projet de loi n°6798 portant approbation :
- *1. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des États-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et relatif aux dispositions des États-Unis d'Amérique concernant l'échange d'informations communément appelées le « Foreign Account Tax Compliance Act », y compris ses deux annexes ainsi que le « Memorandum of Understanding » y relatif, signés à Luxembourg le 28 mars 2014,*
- *2. de l'échange de notes y relatives.*

Délibération n°198/2015
du 13 mai 2015

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 du 26 mars 2015, Monsieur le Ministre des Finances a invité la Commission nationale à se prononcer au sujet du projet de loi n°6798 portant approbation : - 1. de l'Accord entre le Gouvernement du Grand-Duché de Luxembourg et le Gouvernement des États-Unis d'Amérique en vue d'améliorer le respect des obligations fiscales à l'échelle internationale et relatif aux dispositions des États-Unis d'Amérique concernant l'échange d'informations communément appelées le « Foreign Account Tax Compliance Act », y compris ses deux annexes ainsi que le « Memorandum of Understanding » y relatif, signés à Luxembourg le 28 mars 2014 (ci-après désigné « l'accord FATCA »), - 2. de l'échange de notes y relatives.

L'accord FATCA a pour objectif d'améliorer le respect des obligations fiscales à l'échelle internationale à travers une assistance mutuelle en matière de fiscalité sur la base d'une infrastructure efficace pour l'échange automatique d'informations entre, d'une part, le Gouvernement du Grand-Duché de Luxembourg, et d'autre part, le Gouvernement des Etats-Unis d'Amérique.

La Commission nationale comprend que cet accord s'inscrit dans un contexte européen et international où une importance accrue a été reconnue en matière d'échange automatique d'informations comme moyen de lutte contre la fraude et l'évasion fiscales transfrontières[36].

La CNPD regrette toutefois qu'elle n'ait pas été consultée lors de la phase de négociation de l'accord FATCA, alors que le projet de loi sous examen a pour but d'approuver un accord signé, qui ne peut plus être modifié à moins de le renégocier avec le Gouvernement des Etats-Unis d'Amérique.

A l'occasion des discussions entre les Etats-Unis d'Amérique et la Commission européenne portant sur les modalités de mises en œuvre de la loi américaine FATCA au sein des Etats membres, le groupe de travail « article 29 » sur la protection des données[37] s'est penché sur la question de la compatibilité entre les obligations résultant de la loi américaine FATCA d'une part, et le droit européen de la protection des données d'autre part, en adressant deux courriers contenant des recommandations à la Commission européenne les 21 juin et 1er octobre 2012[38].

---

[36] Cf. notamment le considérant (2) de la directive 2014/107/UE.
[37] Regroupant les autorités de protection des données de l'ensemble des Etats membres de l'Union européenne.
[38] Disponibles aux adresses suivantes : http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120621_letter_to_taxud_fatca_en.pdf et http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121001_letter_to_taxud_fatca_en.pdf.

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 portant sur la protection des données, dont plus particulièrement les articles 2 et 3.

Ad article 2 du projet de loi

Le paragraphe (1) de l'article 2 du projet de loi sous avis prévoit que les institutions financières déclarantes luxembourgeoises doivent transmettre à l'Administration des contributions directes les informations relatives aux comptes financiers à échanger en vertu de l'accord FATCA. Cependant, il ne précise pas les modalités de transmission des données (communication sur requête, communication d'office, accès direct de l'Administration aux données concernées, etc. ?). Il semblerait, d'après communications obtenues de la part de l'Administration des contributions directes, que cette transmission de données s'opère au moyen d'un courrier à envoyer à intervalles réguliers à l'Administration des contributions directes. La CNPD estime que le moyen de transmission des données pourrait être précisé dans le texte de l'article.

En outre, il n'est pas fait mention des mesures de sécurité techniques et organisationnelles devant le cas échéant être mises en place à l'occasion de la communication de ces données à l'Administration des contributions directes, conformément aux articles 22 et 23 de la loi modifiée du 2 août 2002. A défaut de telles précisions dans le projet de loi, la Commission nationale n'est pas en mesure d'apprécier le caractère adéquat et sécurisé de la transmission des données à l'Administration des contributions directes. Eu égard au caractère sensible des données traitées, la CNPD suggère de préciser le texte du projet de loi en ce sens, ou à défaut, de l'indiquer dans un règlement grand-ducal à adopter.

Ad article 3 du projet de loi

La CNPD note avec satisfaction que, conformément au paragraphe (2) de l'article 3 du projet de loi sous avis, les personnes concernées seront informées de tout manquement à la sécurité des données susceptible de porter atteinte à leurs données à caractère personnel ou à leur vie privée. Cette obligation d'information pèse, aux termes du texte du projet de loi sous objet, sur « *l'Administration des contributions directes et les Institutions financières déclarantes luxembourgeoises* ». Faut-il comprendre que lorsqu'un manquement aux obligations en matière de sécurité visées aux articles 22 et 23 de la loi modifiée est constaté, l'institution ou l'administration auquel ce

manquement peut être reproché est tenu d'en informer sans délai les personnes concernées ? Si tel est bien le cas, la CNPD se demande si l'emploi du terme *« ou »* ne serait pas plus opportun que le mot *« et »*.

Le premier alinéa du paragraphe (4) de l'article 3 énonce que *« l'institution financière déclarante luxembourgeoise doit faire savoir à chaque personne physique concernée (…) que les informations la concernant seront recueillies et transférées conformément à l'Accord »*. Dans ce contexte, la CNPD voudrait rappeler le considérant 38 de la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques, selon lequel *« le traitement loyal des données suppose que les personnes concernées puissent (…) bénéficier, lorsque des données sont collectées auprès d'elles, d'une information effective et complète au regard des circonstances de cette collecte »*.

Le second alinéa du même paragraphe précise que *« l'institution financière déclarante luxembourgeoise doit communiquer à cette personne toutes les informations qu'elle est autorisée à communiquer conformément à l'article 26 de la loi modifiée du 2 août 2002 »*. L'article 26 de la loi énumère à cet égard les informations devant être obligatoirement fournies à la personne concernée, à savoir l'identité du responsable du traitement et, le cas échéant, de son représentant (lettre a), et la ou les finalités déterminées du traitement auquel les données sont destinées (lettre b). En outre, certaines informations supplémentaires facultatives, à savoir les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées (lettre c, premier tiret), le fait de savoir si la réponse aux questions est obligatoire ou facultative (formulaire ou questionnaire par lequel l'institution financière collectera les données auprès des personnes concernées) ainsi que les conséquences éventuelles d'un défaut de réponse (lettre c, deuxième tiret), et l'existence d'un droit d'accès aux données concernant la personne et de rectification de ces données (lettre c, troisième tiret), peuvent également être fournies *« dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données »*. Dans le cas du projet de loi sous examen, la CNPD est d'avis que ces « circonstances particulières » sont réunies, de telle sorte que l'information concernant ces trois catégories d'information devraient obligatoirement être fournies par l'institution financière, alors qu'elles apparaissent *« nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données »* aux termes de l'article 26 paragraphe (1) lettre (c) de la loi modifiée du 2 août 2002, et qu'il y a lieu de le préciser dans le projet de loi.

Pour plus de clarté et afin de respecter pleinement les obligations de l'article 26 de la loi, le second alinéa du paragraphe (4) de l'article 3 pourrait en conséquence prendre par exemple la forme suivante :

« L'institution financière déclarante luxembourgeoise doit communiquer à cette personne les informations suivant lesquelles :

- *l'institution financière luxembourgeoise est responsable d'un traitement de données à caractère personnel la concernant ;*
- *les données à caractère personnel sont destinées aux finalités prévues dans l'Accord ;*
- *les données seront susceptibles d'être communiquées à l'Administration des contributions directes, ainsi qu'à l'Administration fiscale des Etats-Unis d'Amérique en vertu de cet Accord ;*
- *la réponse aux questions est obligatoire, ainsi que les conséquences éventuelles d'un défaut de réponse ;*
- *la personne concernée dispose d'un droit d'accès aux données communiquées à l'Administration des contributions directes et de rectification de ces données ».*

7 Annexes

Enfin, la Commission nationale se demande si la durée de conservation des données prévues au paragraphe (5) du projet de loi sous objet ne mériterait pas davantage de précisions. En particulier, il n'est pas aisé de déterminer à quelles durées concrètes le Gouvernement a voulu faire référence à travers des termes suivants : « *conformément aux dispositions légales applicables au responsable du traitement des données concernant le régime de prescription* ». La CNPD se réfère à cet égard à la position du groupe de travail « article 29 », qui estime dans son courrier du 21 juin 2012 précité, que dans le contexte de FATCA, « *all data controllers should be clear about how long they will keep and update personal data in line with Articles 6 (c) and (d)* »[39] . Ni le texte du projet de loi, ni le commentaire des articles ne contiennent de précisions à cet égard. En l'absence de telles précisions, la CNPD n'est pas en mesure d'apprécier le caractère proportionné et adéquat de la durée de conservation des données conformément à l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002. Aux yeux de la Commission nationale, cette disposition ne respecte donc pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal, et n'est guère conforme à l'article 4 de la loi modifiée du 2 août 2002.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 13 mai 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

[34] C.J.U.E., Grande Chambre, *Digital Rights Ireland Ltd et Seitlinger e.a. c. Irlande e.a.*, arrêts C-293/12 et C-594/12 du 8 avril 2014.

[35] Préposé fédéral à la protection des données et à la transparence (PFPDT), 18ème rapport d'activité, 2010/2011, p. 22, disponible à l'adresse suivante : http://www.edoeb.admin.ch/dokumentation/00153/00184/index.html?lang=fr.

Avis 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

Délibération n°228/2015 du 19 juin 2015

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 5 janvier 2015, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet 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.

Dans son avis n°214/2014 du 13 mai 2014[40], la Commission nationale avait analysé la législation luxembourgeoise existante au regard de l'arrêt de la Cour de justice de l'Union européenne rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12. Dans ledit avis, la CNPD avait attiré l'attention sur plusieurs points de la législation qui devraient faire l'objet de modifications suite à l'arrêt précité.

Ci-dessous seront passés en revus les sujets évoqués dans l'avis précité à la lumière des dispositions afférentes du projet de loi sous avis.

1) Défaut d'exceptions pour les personnes dont les communications sont soumises au secret professionnel

Dans le considérant (58) de son arrêt du 8 avril 2014, la Cour de justice de l'Union européenne a relevé le fait que la directive 2006/24/CE *« ne prévoit 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 »*.

Le projet de loi sous avis n'introduit aucune exception pour ce qui est des communications soumises au secret professionnel, ni au niveau de la conservation elle-même (articles 5 et 9 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), ni au niveau de l'accès aux données (article 67-1 du Code d'instruction criminelle).

Dans son avis n°214/2014 du 13 mai 2014, la CNPD avait suggéré d'aligner le régime de l'accès aux données issues de la conservation à celui existant en matière d'écoutes téléphoniques pour ce qui est des aménagements en matière de communications couvertes par le secret professionnel, en estimant que *« cette voie […] reviendrait à réduire de façon équivalente les conséquences pour la vie privée résultant de l'ingérence dans le secret de leurs communications électroniques des personnes visées par la CJUE au regard de la protection spéciale dont ils bénéficient dans les activités considérées. »* Par ailleurs, elle avait plaidé pour une exception en faveur des journalistes.

La CNPD réitère dès lors sa proposition et estime nécessaire d'introduire ces exceptions dans

[40] 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.

le projet de loi conformément à l'arrêt de la CJUE.

Si une telle exception est prévue au niveau de l'accès aux données, la disposition y afférente devrait être insérée, outre à l'article 67-1 du Code d'instruction criminelle, également le cas échéant à l'article 24-1 alinéa 3 du Code d'instruction criminelle et à l'article 10 paragraphe (2) du *projet de loi n°6675 1) portant organisation du Service de Renseignement de l'Etat ; 2) modifiant la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat, la loi du 31 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, le Code d'Instruction criminelle, la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, et la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ; 3) abrogeant la loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat. Ledit projet de loi a été déposé à la Chambre des Députés comme projet de loi n°6675 en date du 2 avril 2014.*

2) Durée de conservation et obligation de destruction à l'expiration de la durée de conservation légale

Dans son avis n°214/2014, la CNPD a rendu attentif au fait que l'arrêt de la CJUE mentionne l'exigence que la législation impose la destruction irrémédiable des données à caractère personnel à la fin de la période de conservation obligatoire.

La Commission nationale salue la nouvelle formulation de l'article 5 paragraphe 1er lettre (b) et de l'article 9 paragraphe 1er lettre (b), articles qui prescrivent désormais, sans équivoque possible, la destruction des données, une fois la fin de la durée de conservation de 6 mois atteinte.

Pour ce qui est de la durée de conservation elle-même, la démarche du législateur luxembourgeois était exemplaire dans la mesure où, en 2010, la durée de conservation a été réduite à la durée minimale prévue par la directive 2006/24/CE, à savoir 6 mois. Cependant ladite directive ayant été déclarée invalide, il se pose désormais la question de savoir si une durée de conservation encore plus courte ne pourrait pas être envisagée, par exemple à l'instar des propositions actuelles du gouvernement allemand en la matière.

3) Obligation de conserver les données sur le territoire de l'Union européenne

Dans son avis n 214/2014, en se référant à l'arrêt de la Cour, la CNPD avait plaidé pour l'obligation de conserver les données sur le territoire de l'Union européenne en raison de *« la nécessité de voir soumettre le traitement et la conservation de ces vastes quantités de données sensibles par une autorité de contrôle indépendante mettant en œuvre le droit européen de protection des libertés et droits fondamentaux »*.

La Commission nationale note avec satisfaction que l'article 5-1 de la loi modifiée du 30 mai 2005 impose désormais que les données soient conservées sur le territoire de l'Union européenne.

4) Mesures techniques et d'organisation destinées à assurer la confidentialité et la sécurité des données conservées

Dans ses avis n°85/2010 du 26 avril 2010[41] et n°214/2014 du 13 mai 2014, la CNPD avait suggéré de prévoir des mesures spécifiques en matière de sécurité des données pour la conservation des données de télécommunications. Comme l'a relevé la Cour de justice de l'Union européenne dans son arrêt du 8 avril 2014, le simple renvoi aux règles générales applicables en matière de sécurité des données *« ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles »* (considérant 67).

Le projet de loi sous avis prévoit la fixation des règles en question par voie de règlement grand-ducal.

Selon l'arrêt susmentionné, une directive européenne, en l'espèce la directive 2006/24/CE, qui prescrit la conservation des données de télécommunication sans mesures de sécurité adaptées, viole le droit communautaire, et plus précisément les articles 7, 8 et 52 paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne.

En toute logique, une loi nationale légiférant dans le champ d'application du droit de l'Union européenne[42] qui prescrit le même type de rétention des données sans prévoir les mesures de sécurité adéquates devrait tout autant violer la Charte.

Par ailleurs, 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 constante 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 »*[43]. L'article 5-1 paragraphe (2) projeté de la loi modifiée du 30 mai 2005 ne saurait guère satisfaire à cette exigence.

Dans ces circonstances, la CNPD estime que les dispositions essentielles en matière de sécurité doivent être comprises dans la loi.

Dans l'hypothèse où l'article 5-1 paragraphe (2) projeté était maintenu en ses termes actuels, la CNPD aurait préféré qu'un projet de règlement grand-ducal aurait été soumis pour avis ensemble avec le projet de loi.

5) Sanction des abus

La Commission nationale note avec satisfaction que les sanctions en matière d'abus prévues par les articles 5 paragraphe (6) et 9 paragraphe (6) ont été alourdies.

---

[41] Avis de la Commission nationale pour la protection des données concernant le projet de loi n°6113 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle et le projet de règlement grand-ducal 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.

[42] Plus précisément dans le champ d'application de l'article 15 paragraphe (1) de 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.

[43] Arrêt 117 de la Cour constitutionnelle.

En revanche, la CNPD regrette que, contrairement à ce qu'elle avait suggéré dans ses avis n°85/2010 du 26 avril 2010 et n°214/2014 du 13 mai 2014, le projet de loi ne prévoit pas la nullité de la preuve obtenue moyennant une violation de la législation sur la rétention des données de télécommunication et réitère sa recommandation d'*« inscrire en outre expressément dans le Code d'instruction criminelle la nullité de la preuve obtenue moyennant un accès illicite ou un abus des données en question »*.

6) Les infractions visées

Conformément aux recommandations de la CNPD exprimées dans ses avis n°85/2010 du 26 avril 2010 et n°214/2014 du 13 mai 2014, le projet de loi prévoit une liste limitative d'infractions qui permettent un accès aux données par les autorités.

Selon le commentaire des articles, le catalogue des infractions s'inspire en principe de la liste des infractions prévues à l'annexe D de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale. Vu la difficulté de l'exercice de l'établissement d'une telle liste, il est compréhensible que l'on s'inspire d'une liste existante en droit européen. Il se pose cependant la question de savoir si l'amélioration de la lutte contre la criminalité grave, but recherché lors de la mise en place de la conservation des données par la directive 2006/24/CE (certes invalidée par la CJUE), et la coopération judiciaire en matière pénale traitée par la directive 2014/41/UE sont censées concerner les mêmes infractions.

Par ailleurs, selon le même commentaire d'articles, cette liste est amendée en la précisant par des renvois à des articles déterminés du Code pénal et de certaines lois spéciales afin de l'adapter aux spécificités du droit pénal luxembourgeois.

La rétention des données de télécommunication avait été rendue obligatoire par la directive 2006/24/CE en réaction aux attentats terroristes et pour pouvoir prévenir et sanctionner de tels attentats à l'avenir[44], mais son champ d'application avait été étendu à la criminalité grave de manière générale.

On peut se demander si, effectivement, toutes les infractions énumérées au projet sous avis relèvent de la criminalité grave et si certaines d'entre elles ne s'éloignent pas des actes initialement visées par l'esprit de la directive déclarée invalide.

[44] Cf. considérants 8 et 10 du préambule de la directive 2006/24/CE.

Les mesures de conservation de données prévues constituant une limitation à l'exercice de droits fondamentaux, leur champ d'application devrait être défini de manière aussi limitative que possible.

Enfin, la CNPD suggère d'insérer, à l'article 24-1 alinéa 3 du Code d'instruction criminelle, qui permet un recours aux données de télécommunication en dehors d'une instruction préparatoire, un renvoi vers la liste des infractions de l'article 67-1.

Ainsi décidé à Esch-sur-Alzette en date du 19 juin 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis complémentaire à l'égard du 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 et du projet de règlement grand-ducal fixant les conditions et modalités d'octroi de la subvention de loyer prévue par l'article 14quinquies de la loi modifiée du 25 février 1979 concernant l'aide au logement

Délibération n°258/2015 du 2 juillet 2015

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* ».

Faisant suite à la demande lui adressée par Madame la Ministre du Logement en date du 11 mai 2015, lui demandant d'aviser les amendements gouvernementaux au sujet du projet de loi n°6542 et du projet de règlement grand-ducal susvisé, approuvés par le Conseil de Gouvernement dans sa séance du 30 avril 2015, 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 21 juillet 2014. Elle limite dans le présent avis ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'amendement 3 du projet de loi portant sur l'article 14sexies de la loi modifiée du 25 février 1979 concernant l'aide au logement, ainsi que par l'amendement 4 du projet de règlement grand-ducal introduisant un nouvel article 9 dans ledit projet.

De manière générale, la Commission nationale salue la démarche des auteurs des projets de loi et de règlement grand-ducal d'avoir pris en compte et intégré la plupart des recommandations de la CNPD dans les nouveaux projets de loi et de règlement grand-ducal tels qu'amendés. Cependant, il demeure certains points sur lesquels elle tient à émettre ses observations.

7 Annexes

Amendement 3 du projet de loi (article 14sexies de la loi modifiée du 25 février 1979 concernant l'aide au logement)

L'article 14sexies paragraphe (1), tel qu'amendé, se réfère à la notion de « *données à caractère personnel* », et non plus à celle de « traitements de données à caractère personnel ». Toutefois, les lettres (a) à (c) renvoient à des fichiers de données à caractère personnel au sens de l'article 2 lettre (h) la loi du 2 août 2002. Pour des raisons de cohérence avec cette loi, il serait utile de préciser les catégories de données concernées aux lettres (a) à (c), ou à défaut d'utiliser les termes suivants : « *données à caractère personnel issues des fichiers suivants* » à la place de « *données à caractère personnel suivants* ».

Le nouvel alinéa 3 du premier paragraphe du même article prévoit la forme selon laquelle s'opère l'accès aux fichiers visés à l'alinéa 1. La CNPD note avec satisfaction que la nouvelle procédure prévue par cet alinéa ne repose plus sur un accès direct du Ministère du logement aux fichiers des administrations concernées, mais bien sur un accès sur demande, ce qui apparaît davantage conforme aux principes de nécessité et proportionnalité, tels que développés dans son avis précité du 21 juillet 2014 (délibération 339/2014). Elle suggère cependant d'utiliser la formulation suivante : « *L'accès prend la forme d'une communication des données (…)* » à la place du mot « *échange* ». En effet, ce dernier terme laisse penser que la transmission des données s'opérerait dans les deux sens, alors qu'elle ne se fera en réalité que depuis les administrations concernées vers le gestionnaire en charge du dossier au sein du ministère du Logement.

Dans le même ordre d'idées, la CNPD propose de modifier le libellé à l'endroit de l'alinéa 1 du premier paragraphe en utilisant les termes « *peuvent recevoir communication des données* » à la place de la formulation « *peuvent accéder aux données* » utilisée à l'alinéa 1 du premier paragraphe.

Le nouvel alinéa 4 prévoit maintenant un système de journalisation des accès, ce qui constitue une garantie appropriée contre les risques d'abus. Notons que cette procédure de traçage des accès est également précisée dans le projet de règlement grand-ducal (paragraphe (4)), ce qui peut apparaître quelque peu redondant. Les deux dispositions pourraient dans ce cas être regroupées dans un seul paragraphe de la loi, par le libellé suivant :

« *Le système informatique par lequel l'accès ou le traitement des données à caractère personnel 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 fichiers de données à caractère personnel qui sont gérés par le ministre ayant le Logement 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 pour chaque traitement ou consultation avec l'identifiant numérique personnel de la personne qui y a procédé. 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. »*

<u>Amendement 4 du projet de règlement grand-ducal (article 9 du projet de règlement grand-ducal)</u>

Pour des raisons de cohérence avec l'article (2) lettre (n) de la loi du 2 août 2002, la formulation du paragraphe (1) suivant laquelle [le ministre] *« a la qualité de responsable dudit accès »* pourrait être remplacée par la phrase suivante : *« Il a la qualité de responsable du traitement ».*

Par ailleurs, les données précises indiquées sous les lettres (a) à (c) du paragraphe (2) paraissent a priori nécessaires et proportionnées dans la mesure où elles peuvent se justifier au regard des finalités indiquées dans ce même paragraphe. Il ressort également du texte de ce paragraphe *(« les données (…) concernant le demandeur respectivement le bénéficiaire »)* que le Ministère du logement ne peut recevoir communication que des seules données de la personne concernée, à l'exclusion des données relatives au reste de la population, ce qui constitue également une garantie contre les risques d'abus.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 2 juillet 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis à l'égard du projet de loi n°6820 portant modification : 1) de la loi du 29 mars 2013 relative à l'organisation du casier et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne, 2) du Code d'instruction criminelle, 3) du Code pénal

Délibération n°259/2015
du 2 juillet 2015

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 de la Justice en date du 15 mai 2015, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet :

- du projet de loi n°6820 portant modification 1) de la loi du 29 mars 2013 relative à l'organisation du casier et aux échanges d'informations extraites du casier judiciaire

entre les Etats membres de l'Union européenne, 2) du Code d'instruction criminelle, 3) du Code pénal,

- du projet de règlement grand-ducal fixant la liste des administrations et personnes morales de droit public pouvant demander un extrait du casier avec l'accord de la personne concernée.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données.

L'un des objectifs principaux du projet de loi et de règlement grand-ducal sous analyse est d'adresser les principales problématiques rencontrées après l'entrée en vigueur de 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. La suppression du bulletin n°3 résultant de cette loi a eu pour effet une extension des inscriptions des condamnations figurant au bulletin n°2. Cette extension a fait l'objet de vives critiques, car elle pouvait notamment mener à une discrimination potentielle d'un demandeur d'emploi luxembourgeois vis-à-vis d'un demandeur d'emploi de nos pays voisins. En effet, dans certains cas, le « nouveau » bulletin luxembourgeois n°2 renseignait sur des condamnations qui n'auraient pas figuré au bulletin d'un demandeur d'emploi étranger. Le bulletin de ce dernier, ayant subi les mêmes condamnations, pouvait en effet présenter une mention « néant ».

A part d'adresser ces problèmes spécifiques, les textes sous analyse introduisent également une réforme en profondeur du casier judiciaire. Cette dernière se compose notamment d'une introduction de cinq nouveaux bulletins dont la délivrance est directement liée à leur finalité, des nouvelles modalités de délivrance des bulletins, d'une liste des destinataires des bulletins revue à la baisse, d'un régime d'accès limité, de durées de conservation plus courtes et de l'introduction d'une sanction pénale en cas de non-respect des dispositions de la loi.

1. Introduction d'une durée de conservation limitée des inscriptions au casier

Il ressort des dispositions de l'article 1er, point 5 du projet de loi que « *les inscriptions relatives à une personne physique sont effacées 100 ans après la naissance de la personne concernée* ». La Commission nationale accueille favorablement la volonté de tenir compte de

la notion du droit à l'oubli dans le texte du projet de loi sous analyse. La CNPD s'interroge néanmoins sur l'opportunité de prendre comme point de départ la date de naissance pour calculer la durée de conservation.

En effet, avec cette règle, la durée de conservation effective des données le cas échéant inscrites au casier pour une personne décédée par exemple à l'âge de 30 ans serait de 70 ans, alors que pour une personne décédée à l'âge de 95, la durée ne serait que de 5 ans.

Une disposition qui limiterait la durée de conservation des données inscrites au casier en fonction de la durée de vie effective de la personne concernée serait plus appropriée. Une telle solution éviterait des dates de conservation le cas échéant longues et présenterait le net avantage d'uniformiser la solution applicable à toutes les personnes concernées. Ainsi, la CNPD recommande de supprimer les inscriptions contenues dans le casier après le décès de la personne concernée. Uniquement dans l'hypothèse où la date de décès de la personne concernée ne serait pas connue par les services du casier, il pourrait être recouru à la solution telle que proposée actuellement.

2. Introduction du concept de finalités à indiquer pour la délivrance du casier

La CNPD note avec satisfaction que la demande formelle du Conseil d'Etat (et à laquelle elle s'était ralliée dans sa délibération n°304/2012 du 25 octobre 2012), insistant sur l'introduction de finalités pour lesquelles la délivrance d'un extrait du casier judiciaire peut être demandée, a été suivie[45]. En effet, le projet de loi introduit cinq nouveaux bulletins qui se différencient fortement des deux bulletins actuels. Pour chacun de ces cinq bulletins, le projet de loi introduit des finalités de délivrance précises et prévoit une liste limitative de destinataires auxquels les bulletins peuvent être délivrés.

La Commission nationale estime que ces modifications importantes augmentent la sécurité juridique. En effet, en limitant, au moyen de ces finalités, les cas de figure dans lesquels des extraits du casier peuvent être demandés et en précisant les destinataires, les risques potentiels d'abus sont réduits.

3. Limitation de la durée d'inscription relative aux condamnations mineures

La CNPD félicite les auteurs du texte d'avoir également prévu dans la plupart de ces nouveaux bulletins un effacement des inscriptions des condamnations mineures après un délai de cinq ans (ou trois ans pour le bulletin n°4) à partir de certaines dates prédéterminées (p.ex. le jour où la condamnation a acquis force de chose jugée[46], la fin de l'exécution de l'interdiction de conduire dans le cadre du bulletin n°4). En effet, la Commission nationale avait recommandé dans son avis précité[47] qu'il est « *dans l'intérêt des intéressés que les mentions de l'extrait qui leur est délivré ne mentionne pas les éventuelles condamnations pour faits mineurs…* ».

4. Augmentation de la transparence dans la délivrance des extraits du casier

La Commission nationale note également avec satisfaction qu'elle a été suivie en ce qui concerne sa recommandation relative à la transparence à adopter envers les personnes concernées dans le contexte des délivrances automatiques des bulletins du casier judiciaire[48]. En effet, afin de prévenir et de détecter des éventuels abus dans le cadre de telles délivrances automatiques d'extraits du casier aux autorités, administrations et organismes publics, la CNPD avait notamment recommandé la

[45] Cf. délibération n°304/2012 du 25 octobre 2012 relative au projet de loi n°6418 (avis relatif à l'organisation du casier judiciaire et aux échanges d'informations extraites du casier judiciaire entre les Etats membres de l'Union européenne et modifiant le Code d'instruction criminelle).
[46] Cf. article 1er, point 7 du projet de loi (modification de l'article 7, lettre (b)).
[47] Cf. délibération n°304/2012, point II-1), p.3.
[48] Cf. délibération n°304/2012, point IV, p.5.

mise en place d'un minimum de mesures de sauvegarde destinées à détecter et à prévenir de tels abus. Elle avait par ailleurs recommandé, en accord avec l'article 26 de la loi modifiée du 2 août 2002, d'instaurer une « *information systématique et obligatoire des personnes concernées de toute demande de délivrance d'un extrait les concernant*[49]*…* ».

Dans le projet de loi sous analyse, les auteurs vont même au-delà de ces recommandations. A l'exception du bulletin n°1 (dont la délivrance est strictement limitée aux autorités judiciaires), chaque bulletin susceptible d'être délivré directement à une entité publique doit obligatoirement être précédé par le recueil de l'accord de la personne concernée. Cet accord peut être donné de manière écrite ou électronique. Ce n'est qu'après avoir obtenu ledit accord que l'administration ou l'entité publique concernée peut effectivement demander délivrance du bulletin de casier concerné. La Commission nationale se réjouit de cet ajout important qui va indubitablement renforcer le droit à l'information de la personne concernée ainsi que son droit au respect de sa vie privée.

Toutefois, le projet de texte ne précise rien sur les conséquences d'un éventuel refus d'une personne concernée de donner son accord. En matière de protection des données à caractère personnel, le consentement donné par une personne doit toujours être libre. La notion de liberté implique que la personne doit toujours disposer de la faculté de refuser son consentement, mais sans que ce refus ne puisse lui porter préjudice. La personne concernée devrait donc, dans l'hypothèse où elle refuse de consentir à la délivrance directe du bulletin à l'administration qui lui en fait la demande, toujours disposer de la faculté de demander elle-même ledit bulletin (dans les cas où elle dispose du droit d'en obtenir copie) et de le transmettre par la suite à l'administration concernée. En effet, la personne concernée doit avoir la possibilité de prendre connaissance des inscriptions de son casier avant de marquer son accord pour une transmission automatique dudit bulletin aux administrations concernées. Ceci permet à la personne concernée de décider au préalable, dans l'hypothèse d'inscriptions de condamnations mineures, de retirer sa demande d'emploi auprès de l'administration concernée ou de décider de ne pas soumettre une telle demande d'emploi par exemple. Cette faculté de refuser une délivrance directe ne doit en aucun lieu avoir des

[49] Cf. délibération n°304/2012, point IV, p.6.

conséquences négatives pour le dossier de la personne concernée auprès de l'administration concernée. La Commission nationale suggère dès lors de préciser le texte en ce sens dans le cadre des bulletins n°3, 4 et 5.

Dans un souci de sécurité juridique, il aurait également été souhaitable que le projet de loi précise les modalités concrètes du recueil du consentement.

5. Observations quant au bulletin n°2

La liste des administrations et personnes morales de droit public ayant droit à obtenir un extrait du bulletin n°2 ainsi que les motifs d'une demande de délivrance sont désormais fixées par règlement grand-ducal. Le projet de règlement grand-ducal qui a été soumis, ensemble avec le projet de loi, à l'avis de la CNPD énumère limitativement dix (pour le bulletin n°2), respectivement sept (pour le bulletin n°3) entités publiques ainsi que les motifs précis pour lesquelles une telle délivrance peut avoir lieu. Par exemple, un extrait du bulletin n°2 ne peut être délivré qu'au Ministère de la Fonction Publique « *pour les demandes d'emplois pour des postes liés à la souveraineté nationale* », alors que l'extrait du bulletin n°3 peut être délivré au même ministère pour tous les autres postes. La CNPD estime qu'une telle revue à la baisse du nombre des administrations pouvant demander un extrait du casier ainsi que la limitation stricte des cas de délivrance liés à des finalités bien définies contribuent à une transparence plus parfaite pour toutes les personnes concernées.

La Commission nationale souhaite cependant relever à l'endroit de l'article 1er, point 7 une divergence substantielle entre les textes du projet de loi n°6820 sous examen et du projet de loi n°6675 portant organisation du Service de Renseignement de l'Etat. En effet, selon les dispositions de l'article 5, paragraphe 2 du projet de loi n°6675, « *dans le cadre de l'exercice de sa mission, le SRE a* ***accès direct****, par un système informatique, aux traitements de données à caractère personnel suivants :*
… j) le bulletin n°2 du casier judiciaire ».

Le projet de loi sous analyse prévoit quant à lui un accès **sur demande**[50] du SRE au bulletin n°2 du casier et non pas un accès direct et automatisé. Par ailleurs, le projet de loi instaure également un contrôle régulier de ces accès, alors que le SRE sera obligé de transmettre trimestriellement « *la liste de ses demandes de délivrance et les motifs de ces demandes à l'autorité de contrôle spécifique prévue à l'article 17 de la loi modifiée du 2 août 2002…* ».

La Commission nationale estime que la solution retenue dans le projet de loi sous analyse est beaucoup plus protectrice des droits et libertés des personnes concernées et, au vu de la sensibilité des données en question, elle recommande que le législateur la retienne. Bien entendu, le texte du projet de loi n°6675 devra être adapté en conséquence.

6. Observations quant au bulletin n°3

Alors que la délivrance des bulletins n°1 et n°2 est limitée aux destinataires se trouvant inscrits sur une liste préétablie, le bulletin n°3 peut être délivré à la personne concernée elle-même ou à un tiers muni d'une procuration valide. Il s'agit ici notamment du bulletin que le salarié peut se voir délivrer, afin de le remettre à son futur employeur dans le cadre d'une procédure d'embauche.
Dans ce contexte, la CNPD se réfère à ses réflexions relatives au recueil du consentement de la personne concernée développées ci-avant dans le cadre du bulletin n°2.

[50] Cf. article 1er, point 7, paragraphe (3) : « *Le bulletin n°2 d'une personne physique ou morale est délivré sur demande : 2) au Service de renseignement de l'Etat sur demande de ce dernier* ».

Annexes

L'article 8 relatif au bulletin n°3 du projet de loi doit cependant être lu ensemble avec les dispositions de l'article 8-3, paragraphe (2). En effet, cet article introduit une nouvelle limitation des cas de figure dans lesquels un bulletin n°3 peut être effectivement demandé par un employeur.

L'un des points principaux dans son avis précité portait sur la problématique du manque de base légale pour le traitement des données résultant du casier judiciaire par un employeur, sauf dans quelques cas exceptionnels[51]. A ce titre, la CNPD avait suggéré d'introduire une disposition servant de base légale légitimant ces données pour les finalités « *d'évaluation des candidatures dans le cadre d'une procédure de recrutement*[52]». Par ailleurs, elle avait suggéré d'introduire une durée de conservation maximale de 2 ans.

Ces recommandations avaient été suivies par le législateur dans le cadre du projet de loi n°6418 précité, mais la portée de cette recommandation avait été sensiblement élargie par l'introduction d'une finalité relative à la « *gestion du personnel* ». Ainsi, l'actuel article 8, paragraphe (2) dispose que « *L'employeur peut demander dans le cadre de la gestion du personnel et du recrutement du personnel la production par la personne concernée d'un extrait du casier judiciaire et traiter les données afférentes pour les besoins des ressources humaines sous réserve des limitations prévues au paragraphe (3)* ». Ledit paragraphe (3) limite la durée de conservation des données issues du casier à 24 mois.

L'ajout de cette nouvelle finalité dans la loi du 29 mars 2013 a cependant créé certains problèmes, alors que certains employeurs ont estimé pouvoir demander la production répétée d'extraits du casier de tous leurs employés après l'écoulement de ce délai de 24 mois. La Commission nationale avait, dans son avis précité, limité spécifiquement la finalité à celle de l'évaluation des candidatures afin d'éviter de telles pratiques impliquant des données judiciaires.

Elle accueille donc favorablement les nouvelles dispositions contenues dans le projet de loi à l'article 8-3, paragraphe (2) précité. Dans le cadre d'une finalité de recrutement, la production du bulletin n°3 peut être exigée par l'employeur, mais il faut qu'elle soit faite par écrit et il faut qu'elle soit spécialement motivée par rapport aux besoins spécifiques du poste. Dans le

[51] Cf. délibération n°304/2012, point II), p.1-2.
[52] Cf. délibération n°304/2012, point II), p.2.

cadre de la finalité portant sur la gestion du personnel, l'employeur ne peut demander la remise du bulletin n°3 que lorsque des dispositions légales le prévoient ou en cas de nouvelle affectation justifiant un nouveau contrôle de l'honorabilité par rapport aux besoins spécifiques du poste. Par ailleurs, pour ce qui concerne les deux finalités pré-mentionnées, la durée de conservation est d'un mois au maximum.

La Commission nationale félicite les auteurs pour la revue à la baisse du temps de conservation des données, mais avant tout pour l'encadrement strict et très protecteur des droits des personnes concernées. Ces nouvelles dispositions contraignantes devraient contribuer à éliminer significativement toutes les pratiques qui ont vu le jour au cours de ces dernières années en ce qui concerne la production d'extraits du casier judiciaire.

7. Observations quant au bulletin n°4

La Commission nationale avait notamment soulevé la problématique de la visibilité accrue des condamnations relatives à la circulation routière[53] dans son avis du 25 octobre 2012 et avait recommandé d'introduire des dispositions spécifiques « *pour le recrutement du personnel appelé à exercer leur fonction au volant de véhicules automoteurs* ». Or, à l'époque, la recommandation de la CNPD n'avait pas été suivie. Le projet de loi sous examen suit cette recommandation de la CNPD au moyen d'un nouveau bulletin, le bulletin n°4. Ce dernier renseigne toutes les décisions inscrites au bulletin n°3, ainsi que toutes les condamnations prononçant une interdiction de conduire.

A l'instar des remarques développées ci-avant, il faut également lire les dispositions relatives au bulletin n°4 ensemble avec celles de l'article 8-3, paragraphe 3. Ainsi, un employeur ne peut demander au candidat intéressé de lui remettre un bulletin n°4 que « *lorsque la détention d'un permis de conduire valable constitue une condition indispensable pour l'exercice de l'activité professionnelle du salarié et est exigée dans le contrat de travail* ». Par ailleurs, le bulletin n°4 ne peut être conservé au-delà d'un mois si un contrat de travail est conclu. La destruction immédiate de l'extrait est requise de la part de l'employeur si le candidat n'est pas retenu.

La Commission nationale estime que ces limitations très précises sont dans l'intérêt des personnes concernées, car elles contribuent à limiter des dérives potentielles. Ce nouveau cadre légal restrictif augmente la transparence quant aux droits et obligations des employeurs en la matière.

8. Observations quant au bulletin n°5

Le bulletin n°5 reprend en grandes lignes l'idée introduite par l'article 9 de la loi du 29 mars 2013 précitée et permet à un employeur de vérifier les antécédents judiciaires relatifs aux faits commis à l'égard d'un mineur d'un candidat à l'embauche.

La Commission nationale constate avec satisfaction que toutes les hypothèses de délivrance sur demande de la part d'une administration sont également soumises à l'accord préalable de la personne concernée. Faute d'accord, il reste loisible à la personne concernée de se faire délivrer un tel extrait en mains propres, afin de vérifier préalablement à un entretien d'embauche si, le cas échéant, des condamnations mineures figurent encore au bulletin.

9. Observations générales quant à la durée de conservation des extraits du casier

Les dispositions de l'article 8-3, paragraphe (1) introduisent un

[53] Cf. délibération n°304/2012, point II) 2), p.3.

délai de conservation d'un mois en ce qui concerne les bulletins du casier judiciaire délivrés à un employeur public. Dans l'hypothèse où le candidat n'est pas retenu, cet article introduit également une obligation de destruction sans délai.

Suivant le dernier alinéa de l'article précité, « *le bulletin délivré à une administration saisie d'une demande ne peut pas être au-delà d'un délai de un mois après l'expiration du délai pour un recours contentieux* ». Alors que la Commission nationale approuve le délai proposé, elle souhaite néanmoins relever qu'il peut être difficile, pour le citoyen normal, de déterminer à partir de quand exactement ce délai commence à courir. Des précisions à ce titre seraient utiles.

En ce qui concerne les paragraphes (2) et (3) de l'article 8-3, la Commission nationale renvoie aux développements ci-avant, relatifs aux bulletins n°2 et n°3.

Par ailleurs, la CNPD accueille favorablement les précisions contenues dans le paragraphe (4) de l'article 8-3, qui retiennent indubitablement qu'aucun bulletin du casier ne peut être conservé, après l'écoulement des délais susmentionnés.

10. Introduction d'une sanction pénale

Désormais l'article 9 introduit une sanction pénale en cas de non-respect des dispositions analysées ci-avant. La Commission nationale estime que cette sanction permettra de sensibiliser toutes les personnes physiques ou morales recevant des extraits du casier judiciaire à respecter les dispositions du projet de loi sous analyse. La protection de la vie privée des personnes concernées s'en trouve plus efficacement augmentée.

Ainsi décidé à Esch-sur-Alzette en date du 2 juillet 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis relatif au 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 au 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

Délibération n°366/2015
du 30 juillet 2015

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 ») 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 5 janvier 2015, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du 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.

Par courrier du 6 janvier 2015, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du 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.

Les deux projets de loi sous avis, amendés le 10 avril 2015 par le gouvernement, portent sur l'approbation d'accords prévoyant des échanges, en matière policière et judiciaire, de données à caractère personnel du Luxembourg en direction des Etats-Unis d'Amérique et vice versa.

1. 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.

Considérations d'ordre général

Les deux accords ont comme objectif de combattre le terrorisme. Mais alors que le *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* (ci-après le « Mémorandum ») se limite à la lutte contre le terrorisme, 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* (ci-après l' « accord crime grave ») englobe la lutte contre la criminalité de manière générale, même si un accent particulier semble être mis sur le terrorisme (préambule, article 11).

L'accord crime grave prévoit une utilisation à la fois préventive et répressive des données, le Mémorandum semble, à la lecture du préambule, avoir un caractère essentiellement préventif. L'utilisation des données à des fins répressives n'y est pas exclue, mais soumise à des restrictions (article V point 2.).

Annexes

Les finalités des deux accords se chevauchent donc en grande partie.

La CNPD déplore que l'exposé des motifs ne donne pas davantage d'informations sur les raisons pour lesquelles il est recouru à deux accords séparés, ainsi que sur les liens exacts entre les deux accords.

Les infractions visées

Pour ce qui est du Mémorandum, il vise les infractions terroristes. La CNPD se demande si le mot « terrorisme » a la même signification aux Etats-Unis d'Amérique qu'au Luxembourg ? Ni le Mémorandum lui-même, ni le projet de loi d'approbation ne contient de définition ni une quelconque référence à des infractions précises en droit luxembourgeois ou en droit américain ou à des textes supranationaux auxquelles il faudra se référer en cas de difficulté d'interprétation.

Pour ce qui est de l'accord crime grave, celui-ci s'applique à toutes les infractions qualifiées de crimes graves par l'accord. L'expression « crime grave» désigne, en vertu de l'article 1er de l'accord, *« un agissement constitutif d'une infraction passible d'un emprisonnement maximum de plus d'un an, ou d'une sanction plus lourde »*. Il s'agirait donc le cas échéant d'infractions graves et pas forcément de crimes graves selon la terminologie du droit pénal luxembourgeois.

L'accord ne précise pas si cette condition de peine doit être remplie dans le chef de la législation de l'Etat requérant, de l'Etat requis ou des deux.

Rappelons que la Cour de justice de l'Union européenne a déclaré invalide la *directive 2006/24/CE du Parlement 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* en épinglant notamment le fait que la notion de l'« infraction grave » permettant un accès par les autorités répressives aux données n'y était pas délimitée de manière assez précise, alors que seulement les infractions suffisamment graves justifient une ingérence aux droits fondamentaux telle que celle résultant de la directive[54]. Le Luxembourg (dont la législation prévoit que toute infraction pénale, qui emporte une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, est

[54] Considérant 60 de l'arrêt rendu par la Cour de justice de l'Union européenne le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12.
http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130deb6f91fca9baf400aaa56cdd0274c2f3b.e34KaxiLc3eQc40LaxqMbN4ObxaMe0?text=&docid=150642&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=224005

à considérer comme infraction grave au sens de cette directive précitée) est justement en train de remplacer ce seuil d'un an par un catalogue précis des infractions visées (projet de loi n°6763) pour tenir compte dudit arrêt.

Force est de constater qu'en l'espèce, on a de nouveau recours à un seuil de peine général pour déterminer les infractions ayant une gravité suffisante pour justifier certains traitements de données très délicats, au lieu d'analyser de manière précise quelles sont les infractions nécessitant un recours aux traitements en question.

On peut d'ailleurs signaler que des accords similaires signés par la France[55] et la Belgique[56] comportent en annexe un catalogue des infractions à considérer comme crimes graves au sens de l'accord.

Pour ce qui est de l'article 11 de l'accord crime grave, il s'applique, selon l'intitulé de l'article, aux « infractions criminelles et terroristes graves ». Faut-il comprendre par-là les infractions *criminelles* graves *et* les infractions *terroristes* graves ? Apparemment oui, puisque le paragraphe 1. lettre c. vise de manière expresse les infractions criminelles graves en plus des infractions terroristes visées à la lettre a. du paragraphe premier.

Contrairement à ce qui est affirmé dans le commentaire des articles, le champ d'application de l'article 11 semble donc englober toutes les infractions auxquelles s'appliquent les autres dispositions de l'accord et ne pas se limiter aux infractions terroristes. Par ailleurs, l'article 11 ne prévoit aucune différence de régime entre les infractions terroristes et les autres infractions graves.

Il y a lieu de noter qu'un accord similaire conclu par l'Allemagne contient un article semblable à l'article 11. Cependant, il n'y est question que d'infractions terroristes (et de l'entrainement en vue de la commission de ces infractions terroristes) et non d'infractions graves de manière générale.[57] Par ailleurs, une procédure de notifications entre Etats signataires y est prévue pour déterminer les infractions concernées par l'article en question.[58] La CNPD se demande pourquoi le gouvernement luxembourgeois n'a pas insisté sur la mise en place de garanties similaires.

<u>L'utilisation des données pour d'autres finalités</u>

L'article 13 paragraphe 1 de l'accord crime grave dispose que chaque Partie peut traiter les données obtenues en vertu de l'accord « *pour toute autre finalité, mais uniquement avec le consentement préalable de la Partie ayant transmis les données.* »

Une telle utilisation pour d'autres finalités se heurterait au principe de finalité énoncé ci-dessus.

Elle nécessite certes le consentement de la Partie ayant transmis les données, mais n'exige pas celui des personnes concernées et se ferait, le cas échéant, même à l'insu de celles-ci.

D'ailleurs, le commentaire des articles ne donne aucun exemple d'une telle utilisation pour une autre finalité.

Dans ces conditions, et étant donné que l'article 13 précité prévoit que l'utilisation à d'autres fins ne peut se faire qu'avec avec le consentement préalable de la Partie ayant transmis les données, c'est-à-dire ne peut pas se faire contre le gré de la Partie requise, il se pose la question si on ne pourrait pas déjà exclure, au niveau de la loi d'approbation, une telle utilisation pour ce qui est des transferts du Luxembourg vers les Etats-Unis d'Amérique.

Si une telle utilisation à des finalités autres ne peut pas être exclue à ce stade, elle devrait au moins être entourée de conditions très strictes, comme

---

[55] Accord sous forme d'échange de lettres entre le Gouvernement de la République française et le Gouvernement des États-Unis d'Amérique relatif au renforcement de la coopération en matière d'enquêtes judiciaires en vue de prévenir et de lutter contre la criminalité grave et le terrorisme. http://www.senat.fr/leg/pjl14-048.pdf

[56] Accord entre le Royaume de Belgique et les Etats-Unis d'Amérique sur le renforcement de la coopération dans la prévention et la lutte contre la criminalité grave, établi à Bruxelles le 20 septembre 2011
http://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&caller=summary&pub_date=14-10-15&numac=2014015140

[57] Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität, Article 10 paragraphe (1)
http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id='bgbl209s1010.pdf'%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl209s1010.pdf%27%5D__1431526476000

[58] Article 10 paragraphe (3) : *« (3) Mit der Notifikation nach Artikel 24 Satz 1 können die Vertragsparteien einander in einer gesonderten Erklärung die Straftaten notifizieren, die nach ihrem innerstaatlichen Recht als Straftaten im Sinne des Absatzes 1 gelten. Diese Erklärung kann jederzeit durch eine Notifikation gegenüber der anderen Vertragspartei geändert werden. »*

celles proposées par *Commission de la protection de la vie privée* belge[59] :

« 41. Le fait de pouvoir utiliser ces données « pour toute autre finalité, moyennant l'accord préalable de l'autre Etat » (article 14, §1er d)) n'est pas, en l'état actuel du libellé, de nature à rassurer la Commission. Ce traitement ultérieur pour toute autre finalité devrait être assorti de garanties, telles qu'au minimum :
- *cette faculté ne s'applique qu'au cas par cas,*
- *pour une autre finalité spécifiée et motivée au moment de la demande,*
- *moyennant l'accord préalable, spécifique et au cas par cas de l'Etat (un accord de principe général ne serait pas admissible), et*
- *avec une journalisation non seulement des transferts internationaux de données, mais aussi des transferts au sein même de l'Etat (entre autorités nationales habilitées), de sorte qu'un contrôle effectif, notamment par la Commission, soit rendu possible (voir infra point 45).*
- *l'accord préalable de l'Etat et la décision de transmission doivent pouvoir faire l'objet d'un contrôle juridictionnel,*
- *si les cinq conditions ci-dessus ne sont pas rencontrées dans le corps même du texte de l'Accord PCSC, la Commission émet un avis défavorable sur cette transmission « pour toute autre finalité » et recommande la suppression pure et simple d'une telle possibilité dans l'Accord PCSC. »*

Enfin, on peut se demander quelles sont les hypothèses dans lesquelles une communication des données à des personnes privées (avec l'accord de la Partie requise), telle qu'évoquée par l'article 13 paragraphe 2 de l'accord crime grave et l'article V paragraphe 2 lettre d du Mémorandum serait possible et si une telle communication respecterait le principe de finalité.

2. Les catégories de données

Le Mémorandum évoque d'une part la « terrorism screening information » et d'autre part la « background information ».

Par terrorism screening information, il faut comprendre les données d'identification telles que définies à l'article II point 2. du Mémorandum.

La définition de la « *background information* » du Mémorandum est très vague. Peut-il s'agir de données à caractère sensible telle que des informations sur les opinions politiques ou les convictions religieuses des personnes concernées ? Le

[59] Avis n°27/2010 du 24 novembre 2010, Objet : Projet d'accord bilatéral entre la Belgique et les Etats-Unis sur le renforcement de la coopération dans la prévention et la lutte contre les crimes graves (draft agreement on enhancing cooperation in Preventing and Combating Serious Crime – « Accord PCSC ») (CO-A-2010-025), point 41.
http://www.privacycommission.be/sites/privacycommission/files/documents/avis_27_2010_0.pdf

Mémorandum définit d'ailleurs cette notion sans, par la suite, expliquer de manière spécifique quelles seront précisément les communications de données ou autres traitements effectués concernant les données en question. On peut donc se demander pourquoi on définit la « background information » sans y attacher un régime particulier.

De même, les « données complémentaires » des articles 5 et 8 de l'accord crime grave ne sont pas précisées davantage. Ici encore, il se pose notamment la question de savoir s'il peut s'agir de données sensibles comme les données sur les opinions politiques ou les convictions religieuses des personnes concernées.

3. L'origine des données

Plusieurs questions relatives à l'origine des données et la manière dont sont transmises les données (accès direct ou indirect à des bases de données nationales, communication sur demande etc…) se posent.

Les deux accords à approuver permettent-ils aux autorités américaines d'accéder indirectement via des bases de données luxembourgeoises à un certain nombre de systèmes d'information européens, comme les banques de données SIS II, EUROPOL ou VIS qui sont alimentées par des données nationales provenant des autorités répressives respectives des Etats membres de l'Union européenne?

Il se pose aussi la question de savoir si les échanges de données en direction des Etats-Unis d'Amérique peuvent porter sur des personnes sur lesquelles il n'existe - au moment de la demande effectuée par des autorités américaines - pas d'informations policières ou judiciaires au Luxembourg. Il y a lieu de relever qu'en droit interne luxembourgeois, les autorités policières et judiciaires peuvent accéder, sous certaines conditions, à des informations concernant n'importe quel habitant du pays, informations contenues dans une série de banques de données d'autorités publiques. Lesdits accès sont effectués en vertu l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection Générale de la Police respectivement l'article 48-24 du Code d'instruction criminelle. Est-ce que, en application des deux accords à approuver, les autorités américaines peuvent, de manière indirecte, voire directe, avoir accès aux mêmes bases de données d'autorités publiques luxembourgeoises même pour des personnes jusqu'alors inconnues des autorités policières et judiciaires luxembourgeoises ? En effet, les amendements gouvernementaux évoquent de manière expresse des *« traitements de données à caractère personnel visés par l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police »*.

Enfin, lors de la mise en œuvre des accords sous avis, on aura recours à la base de données créée par 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 »).

La CNPD voudrait rappeler[60] dans ce contexte que le règlement Ingepol qui date de 1992 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 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* et qu'il devrait être remplacé par un nouveau règlement grand-ducal en exécution de l'article 17 paragraphe (1) lettre (a) de la articles 22 et 23 de la loi modifiée du 2 août 2002 relative

[60] La CNPD a déjà épinglé ce problème dans son avis relatif au projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière, délibération n°385/2013 du 25 juillet 2013, http://www.cnpd.public.lu/fr/decisions-avis/2013/securite-routiere/385_2013_Deliberation_Ministre-du-Developpement-durable-et-des-infrastructures_avis_PL_6566_securite_routiere.pdf

à la protection des personnes à l'égard du traitement des données à caractère personnel. 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 nouveau règlement grand-ducal.

4. La transmission des données

L'initiative de la transmission

Le Mémorandum ne donne aucune précision relative à l'initiative de la transmission. Il ne permet donc pas de savoir si les données sont transmises par le biais d'un accès direct accordé à l'autre Partie, sur demande de la part de la partie qui veut obtenir des données ou de manière spontanée par la Partie donnant les informations.

Il est seulement précisé dans le projet de loi d'approbation que, pour une partie des données, l'accès se fera après autorisation du Procureur général d'Etat. La même disposition se retrouve dans le projet de loi d'approbation de l'accord crime grave.

Les amendements gouvernementaux (aux deux textes sous avis) donnent davantage de précisions pour ce qui est des transmissions soumises à l'accord du Procureur d'Etat.

Cependant cet accord n'est pas requis pour les « *traitements de données à caractère personnel visés par l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la police* ». Cette exclusion est problématique tant au regard du grand nombre de catégories de données concernées que des personnes concernées – en fait potentiellement toute la population du Luxembourg.

L'accord crime grave prévoit que la consultation des données dactyloscopiques et des profils ADN se fait par accès direct accordé à la Partie qui reçoit les informations, par le biais du point de contact (articles 4 et 7), des précisions supplémentaires devant être données par des ententes ou des accords de mise en oeuvre (articles 6 point 2. et 9 point 2.). Un tel accès direct est en principe problématique, car l'Etat détenant les données en perd, en quelque sorte, la maîtrise.

Il est dès lors important de veiller à ce que cet accès direct se limite à l'information s'il y a une correspondance entre un profil dactyloscopique ou génétique américain et un profil correspondant luxembourgeois sans communication d'autres informations par le biais de cet accès direct (strict limitation au système « hit, no hit »).

Pour ce qui est de la communication des données complémentaires prévue par

les articles 5 et 8, il faudra apparemment complètement se référer à des ententes ou des accords de mise en œuvre. Or, ces textes font défaut et il aurait été utile de pouvoir les apprécier ensemble avec les textes de base.

Enfin, l'article 11 prévoit, du moins partiellement, une communication spontanée par l'Etat qui détient les informations.

Il se pose la question de savoir quand une telle communication a lieu et sur base de quel motif. Seulement chaque fois qu'une personne suspectée d'actes terroristes a un quelconque lien avec l'autre Partie signataire ? Malheureusement l'accord ne donne pas de réponse à cette question.

Dans ces circonstances, et vu la quantité considérable des données le cas échéant transmises (article 11 paragraphe 2.), il est d'autant plus important de délimiter de manière plus précise les infractions auxquelles s'applique l'article 11 (cf. partie « finalités » du présent avis).

Conservation des traces des transmissions et accès

Pour pouvoir sanctionner des abus et des accès non autorisés, il est primordial que les transmissions et accès puissent être retracés.

En vertu de l'article V paragraphe (8) du Mémorandum, chaque Partie doit déterminer les personnes ayant accès aux données de l'autre Partie. Il n'y est cependant pas précisé si on devra pouvoir retracer chaque accès individuel aux données qui est effectué.

L'article 15 de l'accord crime grave prévoit un système de conservation des traces. Il prévoit notamment que des informations sur les données transmises et la date de la transmission seront conservées. Il serait primordial qu'une information - serait-elle minime - sur le motif de la transmission soit également conservée, comme c'est le cas en droit interne luxembourgeois pour les accès des officiers de police judiciaire ou les magistrats aux banques de données d'administrations publiques en vertu l'article 34-1 de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection Générale de la Police respectivement l'article 48-24 du Code d'instruction criminelle.

Pour ce qui est des personnes ou institutions recevant les données après leur transmission, une conservation des traces est prévue concernant *« le destinataire des données au cas où ces dernières sont transmises à d'autres entités »*.

Cette disposition laisse présumer que les traces des destinataires primaires recevant des données à travers le point de contact c'est-à-dire les institutions policières ou judiciaires ne seraient pas conservées contrairement aux traces des autres destinataires.

Cependant, les destinataires primaires, c'est-à-dire les institutions policières ou judiciaires recevant les données en premier devraient également pouvoir être retracées. Il se pose aussi la question de savoir si le système devra seulement permettre de retracer les institutions recevant les informations ou également l'agent individuel qui a accès aux données.

5. La sécurité des traitements

L'article V paragraphe 5 du Mémorandum ne pose que le principe de base du respect de la sécurité des données et renvoie pour l'essentiel aux droits nationaux applicables.

Est-ce que les règles des Etats-Unis d'Amérique sont satisfaisantes, sachant que les Etats-Unis d'Amérique ne constituent pas un pays ayant un niveau adéquat de protection des données au sens de la législation européenne et luxembourgeoise ?

Mais même du côté luxembourgeois, il n'est pas sûr que le droit applicable soit satisfaisant. Le projet de loi d'approbation ne prévoit pas de dispositions particulières relatives à la sécurité des données. Ce seraient donc les règles de droit commun qui s'appliqueraient,

c'est-à-dire celles des articles 22 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 qui s'appliquent. Or, ces règles, qui s'appliquent à tous types de traitements, laissent au responsable du traitement une marge de manœuvre importante – peut-être trop importante au regard des traitements effectués en vertu du Mémorandum. D'ailleurs, la Cour de justice de l'Union européenne a déclaré invalide la directive sur la rétention des données de télécommunications en partie parce qu'elle ne prévoyait pas assez de dispositions précises en matière de sécurité adaptées aux caractéristiques particulières des traitements effectués et renvoyait en partie aux règles générales applicable en matière de protection des données[61].

Du moins pour les traitements de données opérés par la Police Grand-Ducale, un règlement grand-ducal pris en exécution de l'article 17 de la loi modifiée du 2 août 2002 aurait dû prévoir ces mesures. Or, comme déjà expliqué ci-avant, ce règlement n'a jamais été pris (cf. point 3 dernier paragraphe, page 6 du présent avis)

En ce qui concerne l'accord crime grave, l'article 16 pose certes quelques principes de base mais renvoie encore aux Etats signataires pour préciser les détails.

6. Les droits des personnes concernées

Les accords ne règlent pas les droits des personnes concernées. Par exemple, il n'y a pas de dispositions relatives au droit d'accès ou au droit de rectification.

De même, les accords ne prévoient pas de voies de recours pour les justiciables.

Certes, l'article V paragraphe 11 du Mémorandum par exemple prévoit l'obligation pour les parties de prévoir des possibilités pour les individus d'introduire des « complaint », mais ne précise pas s'il s'agit d'un recours devant une instance judiciaire, une instance administrative (indépendante du gouvernement et de l'autorité qui traite les données ?) ou simplement d'une possibilité offerte d'introduire une réclamation auprès de l'autorité qui traite les données.

Aucun des deux accords ne prévoit le contrôle du respect de la protection des données par une autorité de supervision indépendante.

Sur toutes ces questions, ce sera en fin de compte le droit national

[61] Considérants 66 à 68 de l'arrêt rendu par la Cour de justice de l'Union européenne le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130deb6f91fca9baf400aaa56cdd0274c2f3b.e34KaxiLc3eQc40LaxqMbN4ObxaMe0?text=&docid=150642&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=224005

des Parties signataires qui déterminera seul les règles du jeu avec toutes les incertitudes que cela comporte.

A ces incertitudes d'ordre juridique s'ajoutent les difficultés pratiques pour les personnes concernées de s'adresser à des institutions situées de l'autre côté de l'Atlantique.

7. Conclusion

Tant le Memorandum que l'accord crime grave présentent beaucoup d'imprécisions sur un bon nombre de questions ayant trait à la protection des données. La CNPD s'interroge dès lors sur la conformité des traitements de données, visés par les deux accords, à la législation européenne et nationale sur la protection des données.

Le fait que beaucoup de questions seront régies principalement, voire exclusivement par le droit interne des Etats signataires, laisse persister des doutes quant à l'existence de garanties suffisantes en matière de protection des données et de la vie privée des citoyens.

La CNPD regrette par ailleurs qu'elle n'ait pas été consultée lors de la phase de négociation, respectivement avant la signature des accords, alors que les projets de lois sous examen ont pour objet d'approuver les deux accords signés qui ne peuvent plus être modifiés à moins de les renégocier avec les Etats-Unis d'Amérique.

La CNPD espère donc qu'elle sera consultée préalablement à la conclusion d'ententes ou accords conclus en vertu des deux accords[62] et à la mise en œuvre pratique et technique des deux accords.

Ainsi décidé à Esch-sur-Alzette en date du 30 juillet 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis relatif au projet de loi n°6779 portant sur la protection internationale et la protection temporaire

Délibération n°476/2015
du 16 octobre 2015

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 28 janvier 2015, Monsieur le Ministre de l'Immigration et de l'Asile a invité la Commission nationale à se prononcer au sujet du projet de loi n°6779 (1) relative à la protection internationale et à la protection temporaire, (2) modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat, la loi modifiée du 29 août 2008 sur la libre circulation des personnes et l'immigration et la loi du 28 mai 2009 concernant le Centre de Rétention, et (3) abrogeant la loi

[62] Par exemple ceux prévus par les articles 6 et 9 de l'accord crime grave.

modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection (ci-après : « projet de loi »).

Suivant l'exposé des motifs, le projet de loi a pour objectif principal de transposer en droit national la directive 2013/32/UE relative aux procédures d'asile et d'abroger la loi modifiée du 5 mai 2006 relative au droit d'asile et à des formes complémentaires de protection. La directive quant à elle s'inscrit dans le processus de communautarisation de l'asile (Régime d'Asile Européen Commun – « RAEC »).

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données. Les procédures d'octroi et de retrait de la protection internationale et de la protection temporaire entraîneront la tenue d'un fichier afférent auprès de la Direction de l'Immigration du Ministère des Affaires étrangères et européennes. Pour cette raison, le projet de loi prévoit des dispositions qui concernent spécifiquement le traitement de données à caractère personnel (article 80 du projet de loi). La Commission nationale tient également à soulever d'autres points du projet de loi, qui ont attrait à la vie privée et au traitement de données des demandeurs de protection internationale et qui suscitent des commentaires.

1) Quant à la nécessité d'encadrer dans un texte légal des dispositions spécifiques ayant trait au traitement de données à caractère personnel

Dans son avis du 17 juillet 2015[63], le Conseil d'Etat suggère de renoncer à l'article 80 du projet de loi et invite le ministre ayant l'asile dans ses attributions (ci-après « le ministre ») de suivre plutôt les procédures de droit commun résultant de la loi modifiée du 2 août 2002 et de la loi du 19 juin 2013 relative à l'identification des personnes physiques.

Cette manière de procéder peut être envisageable, par le biais d'une notification préalabe à introduire par le ministre auprès de la CNPD. La Commission nationale relève toutefois que le ministre, dans le cadre des missions prévues par le projet de loi, ne sera pas seulement amené à traiter un nombre important de données à caractère personnel pour les besoins du suivi administratif et de la gestion des dossiers des demandeurs de protection internationale, mais sera aussi amené à traiter des données dites « sensibles », à savoir des données relatives à la santé et

[63] Doc. Parl. 6779/3, p. 13.

à la vie sexuelle (par exemple lors des examens médicaux ou lorsqu'il s'agit d'évaluer les motifs de la persécution ou les garanties procédurales spéciales), des données relatives à l'origine raciale ou ethnique, les opinions politiques ou encore les convictions religieuses. Le fichier du ministre contiendra dès lors des « catégories particulières » de données au sens de l'article 8 paragraphe 1 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, transposé en droit national à l'article 6 de la loi modifiée du 2 août 2002.

Il y a lieu de souligner que pour le traitement de ces données dites « sensibles », le législateur européen et luxembourgeois ont prévu un régime plus strict que pour les autres types de données. En effet, ces textes posent une interdiction générale de traiter les données « sensibles », interdiction qui est assortie de dérogations qui sont limitées, exhaustives et qui doivent être interprétées strictement[64].

Ainsi, la création d'un fichier contenant des données de santé et autres données « sensibles » par le ministre pourrait être basée sur le consentement (dérogation prévu à l'article 6(2)(a) de la loi). Or, la Commission nationale rappelle que lorsqu'un traitement de données de santé est basé sur le consentement, le consentement implicite ne suffit pas, la loi modifiée du 2 août 2002 (tout comme la directive 95/46/CE) exigeant le consentement exprès préalable.

Ceci étant, la directive 95/46/CE et la loi modifiée du 2 août 2002 prévoient encore d'autres critères de légitimation que celle du consentement exprès. Etant donné que par la force des choses (le demandeur de protection étant obligé de suivre la procédure prévue par la loi) il est invraisemblable que le consentement exprès sera systématiquement recueilli auprès des demandeurs de protection internationale avant chaque mesure impliquant le traitement de données (de santé ou qui impliquent le traitement de données se rapportant à l'origine raciale ou ethnique, aux opinions politiques ou encore aux convictions religieuses), le traitement répondra plutôt au critère posé à l'article 6(2)(g) de la loi, à savoir que le traitement sera légitime lorsque celui-ci s'avère nécessaire pour un motif d'intérêt public. Il va sans dire que la transposition de la directive 2013/32/UE en droit national et la création d'un fichier y afférent répond bien à un motif d'intérêt public.

L'article 6(2)(g) précité a transposé en droit national l'article 8 paragraphe 4 de la directive 95/46/CE qui pose comme conditions que la dérogation du motif d'intérêt public soit inscrite dans une disposition légale ou une décision de l'autorité de contrôle de l'Etat membre et que des garanties spécifiques et appropriées soient prévues afin de protéger les droits fondamentaux et la vie privée des personnes.

La Commission nationale a de fortes raisons de douter que pour la mise en place du fichier qui sera tenu par le ministre, et dont certaines catégories de données particulièrement sensibles vont vraisemblablement faire l'objet de transmissions vers d'autres acteurs impliqués dans l'application de la loi, une notification préalable auprès de la CNPD suffirait à apporter au traitement les précisions et garanties nécessaires exigées par la directive 95/46/CE et par la loi modifée du 2 août 2002.

La Commission nationale est dès lors à se demander si « l'essentiel du cadrage normatif »[65] du traitement de données prévu par le projet de loi ne devrait pas figurer dans un texte légal, afin

[64] PP. 9 du document de travail WP131 du Groupe de travail « Article 29 ».
[65] Cit. Arrêt 108/13 de la Cour constitutionnelle du 29 novembre 2013.

qu'il réponde au critère posé à l'article 8 paragraphe 4 de la directive 95/46/CE et, par ailleurs, à celui posé à l'article 8 de la Convention européenne des Droits de l'Homme, dont il importe de rappeler la teneur :

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

L'article 80 du projet de loi concerne spécifiquement le traitement de données à caractère personnel des demandeurs d'une protection internationale ou d'une protection temporaire. Dans sa version actuelle, le paragraphe (1) autorise le ministre ayant l'asile dans ses attributions à effectuer un traitement de données à caractère personnel des demandeurs de protection internationale ou temporaire.

Le paragraphe (2) autorise le ministre à accéder au registre national des personnes physiques. Finalement, le paragraphe (3) dispose qu'un règlement grand-ducal déterminera les catégores de données qui pourront être accédées par le ministre et prévoit aussi les règles de retraçage applicables.

La Commission nationale note que le commentaire des articles (p.47 paragraphe 4 du document 6779/00) précise *« que le ministre est autorisé à collecter et à traiter les données à caractère personnel des demandeurs de protection internationale selon les modalités de la loi modifiée du 2 août 2002 »* et *« qu'un règlement grand-ducal détaillera le contenu et les modalités du fichier »*. La question se pose cependant de savoir si le règlement grand-ducal à adopter se rapporte au paragraphe (1) ou bien au paragraphe (3) du projet de loi. La Commission nationale relève enfin que l'ancienne législation[66] précisait bien les données que le ministre ayant l'asile dans ses attributions était autorisé à collecter et traiter.

2) Quant à la transmission de données entre le ministre et d'autres instances

La Commission nationale souligne que le texte du projet

[66] L'article 59 de la loi modifiée du 5 mai 2006.

de loi n'encadre pas certaines communications ou transmissions de données. Tel est le cas par exemple des examens médicaux prévus à l'article 16 du projet de loi, qui sont effectués par des professionnels de santé et qui communiquent « les résultats » au ministre. Dans ce contexte, la Commission nationale se demande si le traitement de ces données ne pose pas de problème quant au respect du secret médical, alors qu'il n'est pas clair si le professionnel de santé communiquera un rapport médical exhaustif, contenant en détail les données de santé, au ministre ou s'il se limitera à communiquer un certificat qui sert à vérifier les allégations du demandeur de protection internationale.

Dans le cadre des évaluations des garanties procédurales spéciales qui « *peuvent s'avérer nécessaires pour certains demandeurs du fait notamment de leur âge, de leur sexe, de leur orientation sexuelle ou de leur identité de genre, d'un handicap, d'une maladie grave, de troubles mentaux, ou de conséquences de tortures, de viols ou d'autres formes graves de violence psychologique, physique ou sexuelle* », prévues à l'article 19 du projet de loi, celles-ci sont effectuées soit par l'OLAI, soit par un professionnel de santé, soit encore par « *un autre expert* ».

Ensuite, et sans préjudice des échanges de données relatifs aux demandeurs de protection internationale qui sont déjà mis en place par des instruments communautaires (comme par exemple pour « Eurodac » ou dans le cadre d'une transmission du dossier du demandeur vers l'Etat responsable de la demande d'asile), la Commission nationale note que le projet de loi laisse par ailleurs sous-entendre certaines transmissions de données sans pour autant en préciser les détails, par exemple en ce qui concerne la transmission du dossier entre le ministre et les agents de police, les agents de l'aéroport, les agents du centre de rétention ou encore les agents du centre pénitentiaire lors de la présentation d'une demande de protection internationale (article 4 paragraphe (1) du projet de loi), lorsqu'il s'agit de procéder à un regroupement familial en coopération avec d'autres Etats membres (article 75 paragraphe (10) du projet de loi) ou encore lorsque le Haut Commissariat des Nations Unies pour les réfugiés, les membres du Comité luxembourgeois des droits de l'enfant ainsi que « *toute organisation disposant d'un agrément* » sont autorisés à « *avoir accès aux informations concernant chaque demande de protection internationale* » en vertu de l'article 24 paragraphe (1) du projet de loi.

Considérant la nature sensible des données que le ministre est amené à traiter, la Commission nationale suggère d'adapter en ce sens le texte de loi afin qu'il définisse les modalités et conditions précises des transmissions de données.

3) Quant à la conservation des données

Le projet de loi ne prévoit pas de durée de conservation des données.

Selon l'article 4 paragraphe (1) lettre (d) de la loi du 2 août 2002, celles-ci peuvent en effet seulement être « *conservées 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 (…)* ».

La CNPD estime dès lors nécessaire de prévoir une disposition fixant la durée de conservation des données à caractère personnel dans le fichier opérationnel ou dans les archives en tenant compte du fait que le ministre est amené à traiter non seulement des données dites « sensibles », mais également des photos, ainsi que des fichiers audio et audiovisuels des demandeurs de protection internationale.

7 Annexes

4) Quant aux mesures de sécurité et de confidentialité

Dans le contexte des mesures de sécurité et de confidentialité des traitements dont il est question aux articles 22 et 23 de la loi modifiée du 2 août 2002, la CNPD félicite les auteurs du texte d'avoir notamment prévu un système de journalisation des accès aux données, ce qui constitue une garantie appropriée contre les risques d'abus. Toutefois, afin de s'aligner sur d'autres textes légaux récemment adoptés, la CNPD suggère de remplacer le paragraphe (3) de l'article 80 par la disposition suivante :

« Le système informatique par lequel l'accès ou le traitement des données à caractère personnel 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 l'asile 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 pour chaque traitement ou consultation avec l'identifiant numérique personnel de la personne qui y a procédé. 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.* »

5) Quant à la surveillance des demandeurs au moyen d'un bracelet électronique

L'article 22 paragraphe (3) du projet de loi prévoit l'usage du bracelet électronique en tant que mesure « moins coercitive » par rapport à une mesure de rétention à l'égard des demandeurs de protection internationale. La Commission nationale s'aligne sur les conclusions du Conseil d'Etat dans son avis du 17 juillet 2015[67], dans lesquelles celui-ci met en garde contre une éventuelle introduction « généralisée » du bracelet électronique d'une part, et estime que cette mesure est intrusive, attentatoire à la vie privée et à la liberté individuelle, et risque

[67] Doc. Parl. 6779/3, p. 11.

de créer une stigmatisation des demandeurs de protection d'autre part.

L'article 8 paragraphe (4) de la directive 2013/33/UE du 26 juin 2013 établissant des normes pour l'accueil des personnes demandant la protection internationale prévoit en effet la mise en place de mesures moins coercitives par rapport à la rétention : « *les États membres veillent à ce que leur droit national fixe les règles relatives aux alternatives au placement en rétention, telles que l'obligation de se présenter régulièrement aux autorités, le dépôt d'une garantie financière ou l'obligation de demeurer dans un lieu déterminé* ».

La possibilité pour le ministre de prendre une décision d'assignation à résidence à l'égard de demandeurs de protection était par ailleurs déjà prévue à l'article 125 paragraphe (1) de la loi modifiée du 29 août 2008 portant sur la libre circulation des personnes et de l'immigration. Ce texte ne prévoyait cependant pas de mesure de surveillance électronique à l'égard des demandeurs de protection afin de parer au risque de fuite.

A l'époque où une mesure de surveillance électronique, par port d'un bracelet électronique, a été introduite au Luxembourg en 2007 à titre expérimental de deux ans, il s'agissait d'une mesure d'exécution d'une peine privative de liberté ayant comme finalité d'améliorer et de soulager le régime pénitentiaire au Luxembourg. Or, il n'existe, à ce jour, pas de texte légal qui encadre (qui « *fixe les règles* » conformément aux exigences de la directive 2013/33/UE) le recours au bracelet électronique. Si le projet de texte est adopté en l'état, il risque d'assimiler les demandeurs de protection internationale à des délinquants.

Par ailleurs, la Commission nationale renvoie au point 1 de la présente pour rappeler qu'aux termes de l'article 8 de la Convention européenne des Droits de l'Homme, il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée d'une personne que si cette ingérence est prévue par la loi.

Au vu de l'atteinte non négligeable à la liberté de circulation d'un demandeur d'une protection internationale par le port d'un bracelet électronique, la Commission nationale se réfère par ailleurs au protocole 4 de l'article 2 de la CEDH (liberté de circulation), dont la teneur est la suivante :

1) « Quiconque se trouve régulièrement sur le territoire d'un Etat a le droit d'y circuler librement et d'y choisir librement sa résidence.
2) Toute personne est libre de quitter n'importe quel pays, y compris le sien.
3) L'exercice de ces droits ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à la sûreté publique, au maintien de l'ordre public, à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

A ce titre, Amnesty International a publié une prise de position[68] relative à plusieurs problèmes liés aux droits fondamentaux des migrants, des demandeurs d'asile et des réfugiés. Ce document, qui évoque des solutions pour éviter la détention des migrants en situation irrégulière et demandeurs d'asile, retient que « *les mesures de substitution à la détention doivent, dans la manière dont elles sont appliquées, être conformes aux principes de la légalité, de la stricte nécessité, de la proportionnalité et de la non-discrimination* ». En outre, selon Amnesty International, « *toute restriction doit être prévue par la*

[68] Migrants en situations irrégulière et demandeurs d'asile : des solutions pour éviter la détention, POL 33/001/2009.

loi et appliquée conformément à celle-ci, et de solides garanties procédurales doivent exister. Cela signifie que toute limitation de la liberté d'un individu ou de son droit de se déplacer librement doit être exclusivement fondée sur des motifs et des conditions définis par la législation. Les gens doivent pouvoir raisonnablement savoir quand et dans quelles circonstances de telles restrictions sont susceptibles d'être imposées. La loi doit définir chaque mesure applicable, en précisant les critères régissant son application, tout en désignant les autorités responsables de sa mise en oeuvre et les éventuelles délégations d'autorité à des tiers ».

A défaut d'un cadre législatif qui fixe les conditions et les modalités du recours à une surveillance par bracelet électronique, la CNPD estime nécessaire de renoncer à toute référence au port d'un bracelet électronique dans le projet de loi sous examen.

Si, malgré tout, le texte de loi en projet devait retenir la possibilité pour le ministre de recourir à une telle mesure et afin d'éviter que le contrôle d'une telle mesure puisse être confiée à une personne de droit privée, la Commission nationale recommande de modifier le libellé de l'article 22 paragraphe (3) point (b) comme suit : « La mise en œuvre du dispositif technique permettant le contrôle à distance peut être **sous-traitée** à une personne de droit privée », afin d'être en conformité avec la loi modifiée du 2 août 2002 et avec la directive 95/46/CE.

Le même commentaire s'applique bien évidemment aussi à l'article 82 paragraphe (3) lettre (b) du projet de loi.

Pour le surplus, la Commission nationale n'a pas d'observation à formuler au regard de la protection des données à caractère personnel.

Ainsi décidé à Esch-sur-Alzette en date du 16 octobre 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis à l'égard de l'avant-projet de loi portant transposition de la directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen

Délibération n°651/2015
du 20 novembre 2015

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 28 mai 2015, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi portant transposition de la refonte du 1er paquet ferroviaire et modifiant:

- la loi modifiée du 10 mai 1995 relative à la gestion de l'infrastructure ferroviaire ;
- la loi modifiée du 11 juin 1999 relative à l'accès à l'infrastructure ferroviaire et à son utilisation ;
- la loi modifiée du 22 juillet 2009 relative à la sécurité ferroviaire et
- la loi du 3 août 2010 sur la régulation du marché ferroviaire.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données.

L'article 19*undecies* du texte sous analyse prévoit la mise en place et la publication d'un registre national des examinateurs qui disposent de la *« reconnaissance »*, donc d'une déclaration formelle attestant les compétences d'un demandeur à faire passer et à noter des examens en matière de sécurité ferroviaire.

Selon le paragraphe (2) dudit article, sont traités dans ce registre entre autres (i) le nom, l'adresse et la date de naissance des examinateurs ainsi que (ii) les coordonnées des personnes de contact.

La Commission nationale pour la protection des données s'interroge sur la nécessité de publier ces données à caractère personnel, alors que ni la directive 2012/34/UE n'impose une telle publication, ni aucun élément du texte sous analyse n'amène à conclure qu'une telle publication serait absolument nécessaire. Pour les besoins de la transposition de la directive en question en droit national, la CNPD est à s'interroger s'il n'y a pas lieu de suivre l'adage *« la directive et rien que la directive »*. Dans l'hypothèse où une personne souhaiterait vérifier la reconnaissance d'un examinateur spécifique, il suffirait que les agents du ministère gérant ledit registre fournissent sur demande les renseignements y afférents.

Subsidiairement, dans l'hypothèse où une telle publication s'avérerait néanmoins nécessaire, la CNPD estime, en tout état de cause, que l'*« adresse »* ne devrait renseigner que l'adresse professionnelle de l'examinateur. Il en va de même en ce qui concerne les *« coordonnées de personnes de contact »*. Par ailleurs, la *« date de naissance »* ne devrait pas faire l'objet d'une publication, alors que cette information doit être considérée comme excessive. Le traitement de ces données à caractère personnel par le ministère est bien entendu légitime pour des besoins administratifs internes, mais leur publication dans un registre accessible au public doit également être considérée comme disproportionnée.

Il ne résulte pas clairement du texte en projet qui est désigné comme responsable du traitement de ce registre. En effet, il est simplement précisé que l'Administration des chemins de

Annexes

fer « *veille à l'établissement, à la mise à jour et à la publication d'un registre national des examinateurs disposant de la reconnaissance* ». 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 également toutes les questions de responsabilité dépendent directement de cette désignation. Il a ainsi notamment l'obligation de veiller à la confidentialité et à la sécurité des données et il doit mettre en place l'organisation appropriée des mesures techniques.

A la lecture des dispositions pré-mentionnées, la Commission nationale comprend qu'il est dans l'intention des auteurs du texte d'attribuer la responsabilité du traitement au membre du gouvernement ayant les chemins de fer dans ses attributions. Elle suggère dès lors de le préciser dans le texte sous examen.

Suivant les dispositions de l'article 19duodecies, paragraphe (4), « *les examens font l'objet d'un bilan d'examen à délivrer au candidat. Les données intéressant le bilan d'examen sont conservées pendant dix ans par l'examinateur par tous moyens et consultables à tout moment par l'Administration, sans préjudice des dispositions de la législation relative à la protection des personnes à l'égard du traitement des données à caractère personnel.* »

La Commission nationale est à s'interroger pourquoi ces données sont conservées par les examinateurs et non par le responsable du traitement. En effet, il serait plus judicieux que lesdites données soient conservées auprès du responsable du traitement qui est, en plus, soumis à l'obligation de respecter la confidentialité desdites données.

La durée de conservation des données relatives au bilan d'examen de dix ans paraît longue. Or, en l'absence de justifications plus précises, la CNPD n'est pas en mesure d'apprécier si ce délai respecte le principe de nécessité et de proportionnalité au regard des finalités poursuivies.

Ainsi décidé à Esch-sur-Alzette en date du 20 novembre 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis à l'égard du projet de loi n°6539 relatif à la préservation des entreprises et portant modernisation du droit de la faillite

Délibération n°652/2015
du 20 novembre 2015

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 de la Justice en date du 7 février 2013, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n° 6539 relatif à la préservation des entreprises et portant modernisation du droit de la faillite et modifiant

(1) le livre III du Code de commerce,
(2) l'article 489 du Code pénal,
(3) la loi modifiée du 8 janvier 1962 concernant la lettre de gage et le billet à ordre,
(4) la loi du 19 décembre 2002 concernant le registre de commerce et des sociétés ainsi que la comptabilité et les comptes annuels des entreprises,
(5) la loi du 23 juillet 1991 ayant pour objet de réglementer les activités de sous-traitance,
(6) la loi du 5 août 2005 sur les contrats de garantie financière,
(7) la loi modifiée du 10 août 1915 concernant les sociétés commerciales, et
(8) la loi générale des impôts („Abgabenordnung").

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement dans le chapitre 2 du projet de loi sous examen.

L'objectif principal du projet de loi est de réformer et de moderniser le droit de la faillite au Luxembourg, notamment par l'introduction de toute une série de mesures aidant à préserver les entreprises en difficulté. Selon les auteurs, les procédures d'insolvabilité actuelles ne contribuent que très limitativement à la sauvegarde effective d'une entreprise en difficulté, car elles tendent pour la plupart vers une liquidation et donc vers une disparition de l'entité concernée. Le projet de loi sous analyse se fixe le but ambitieux de changer cet état de choses. Pour y parvenir, les auteurs prévoient plusieurs grands axes autour desquels ces modifications se déclinent. Ainsi, ces nouvelles mesures incluent notamment (i) la collecte d'informations d'entreprises en difficultés (c'est-à-dire un volet prévisionnel), (ii) la mission de conciliation ainsi que l'accord amiable (c'est-à-dire un volet réorganisationnel sans ouverture de procédure judiciaire) et (iii) les procédures judiciaires de réorganisation.

1. La problématique des « données judiciaires »

Avant de commenter les dispositions des deux premiers volets précités, la CNPD voudrait aborder la problématique des données judiciaires visées dans le troisième volet relatif aux procédures judiciaires de réorganisation.

Suivant l'article 8, paragraphe (1) de la loi modifiée du 2 août 2002, *« le 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 ressort clairement de cette disposition ainsi que des travaux parlementaires qu'il était l'intention du législateur de ne pas faire appliquer le régime de droit commun de la loi modifiée du 2 août 2002

Annexes

au traitement de données dites « *judiciaires* », en estimant que ces données « *traitées dans le cadre d'enquêtes pénales ou de procédures judiciaires civiles ou administratives* » devaient être soumises aux « *conditions du droit commun de la procédure pénale, civile ou administrative*[69] » prévues dans les Codes et lois spéciales.

Dans le cadre des travaux parlementaires du projet de loi portant modification de la loi du 2 août 2002[70], le Conseil d'Etat a rappelé que les dispositions de l'article 8 signifient « *que le régime de traitement des données dites judiciaires, y compris et notamment les droits des personnes concernées, doit être déterminé dans les différentes lois organisant les procédures devant les juridictions* » et qu'il n'y a pas lieu de prévoir « *…positivement l'application de certaines dispositions…* », ni de consacrer « *…des dérogations ou exemptions à certaines obligations légales* ».

Cette intention ressort également du texte initial du projet de loi n°4735/00 qui précise que « *les traitements de données mis en œuvre conformément aux règles de procédures judiciaires ne doivent pas être notifiés. Cela s'impose afin de ne pas perturber le bon déroulement de la justice et alors que le principe du contradictoire, celui du procès équitable remplissent la plupart des fonctions attribuées à la protection des données* »[71].

La Commission des Médias et des Communications a, par ailleurs, retenue dans son avis[72] que « *cette disposition vise à permettre aux autorités judiciaires, sur la base d'une disposition légale expresse, d'effectuer des traitements de données en relation avec des enquêtes ou procédures judiciaires en cours. Plutôt que de réglementer ce type de traitement dans la présente loi, il paraît préférable d'effectuer un renvoi au droit commun en matière de procédure (pénale, civile ou administrative). La formulation de ce paragraphe du présent article est suffisamment contraignante pour indiquer que le juge ne saurait procéder à des traitements en dehors de tout mécanisme de contrôle. Il s'agira toutefois d'un contrôle interne qui est seul admissible dans la logique de la séparation des pouvoirs. Il s'exercera au titre des règles procédurales de droit commun, notamment du Code d'instruction criminelle* ».

Il ressort de ce qui précède, que les traitements de données à caractère personnel effectués dans le cadre de procédures judiciaires échappent à la mission de contrôle confiée par le législateur à la Commission nationale pour la protection des

[69] Doc. parl. n°4735/13, page 15.
[70] Doc. parl. n°5554/04, page 10.
[71] Doc. parl. n°4735/00, page 100.
[72] Doc. parl. n°4735/08, page 9.

données et suivent les règles prévues dans les Codes et lois spéciales visés à l'article 8 précité. Il y a lieu de relever que ces textes légaux ne contiennent pas de dispositions spécifiques qui tiendraient compte ou intégreraient les principes de protection des données contenus dans la 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, ce que la CNPD déplore.

Dès lors, elle renonce à se prononcer sur les dispositions du projet de loi sous examen portant sur des traitements de données opérés dès l'ouverture d'une procédure judiciaire de réorganisation (c'est-à-dire le volet trois précité). Ceci inclut également la nouvelle procédure de dissolution administrative sans liquidation, qui devra être déclenchée par l'intervention du Procureur d'Etat.

2. La collecte des données sur les entreprises en difficulté

Suivant les dispositions de l'article 5, paragraphe 1er du chapitre 2 du projet de loi, les *« renseignements et données utiles concernant les débiteurs qui sont en difficultés financières telles que la continuité de leur entreprise peut être mise en péril … sont tenus à jour au secrétariat du Comité de conjoncture ».*

a. La détermination du ou des responsable(s) du traitement

Il ne résulte pas clairement de l'article précité si les auteurs ont effectivement souhaité conférer la qualité de responsable du traitement au Comité de conjoncture ou non. Il ressort cependant de l'analyse des traitements de données envisagés (voir point b. ci-après) que telle semble avoir été l'intention des auteurs. Dès lors, la CNPD recommande de clarifier et de préciser le texte en ce sens.

La Commission nationale souhaite par ailleurs relever un passage spécifique contenu dans le commentaire des articles qui prête à confusion en ce qui concerne la détermination du responsable du traitement. En effet, il y est effectué une distinction formelle entre les missions et rôles du secrétariat du Comité de conjoncture et ceux du Comité de conjoncture lui-même en précisant que le secrétariat du Comité de conjoncture *« … par sa participation en tant que membre de la cellule d'évaluation des entreprises … aura également accès à des informations de source administrative, sans toutefois que ces informations puissent par la suite être transmises au comité de conjoncture en raison des contraintes existantes en matière de protection des données …»*[73]. La Commission nationale ne comprend pas cette distinction au sein d'un même organisme. Elle est d'avis qu'un secrétariat, qui est au service d'une entité ou d'un organisme, ne peut pas être considéré comme responsable du traitement au sens de la loi modifiée du 2 août 2002. Par conséquent, le Comité de conjoncture devrait être désigné comme responsable du traitement dans le texte du projet de loi.

Par ailleurs, il ressort indirectement de l'article 8 du projet de loi que certaines données à caractère personnel seront également transmises à et traitées par la Cellule d'Evaluation des Entreprises en Difficulté (CEvED). En effet, ladite cellule, qui est institutionnalisée au moyen du texte sous examen, aura notamment pour rôle d'apprécier l'opportunité ou non d'une assignation en faillite d'une entreprise, au vu de sa situation à un moment précis. Cette appréciation se fera sur base de différentes données, dont des données à caractère personnel. La CNPD renvoie à ce titre au point b. ci-après, mais estime néanmoins nécessaire de préciser le rôle de la CEvED dans le texte.

[73] Doc. parl. n°6539/00, page 51.

En effet, au vu des ambiguïtés et incertitudes existantes quant au rôle de chacun des différents intervenants cités ci-avant, la Commission nationale estime nécessaire de préciser dans le texte les rôles respectifs de chacun avec précision.

A ce titre, elle souhaite relever que le rôle du responsable du traitement ne se cantonne pas uniquement à la simple « tenue à jour » des données qu'il traite, telle que décrite à l'article 5. Bien au contraire, le concept de responsable du traitement constitue une notion-clé pour tout traitement de données à caractère personnel. Il ne détermine pas uniquement les finalités et les moyens des traitements effectués, mais également toutes les questions de responsabilité dépendent directement de cette désignation. Le responsable du traitement a ainsi notamment l'obligation de veiller à la confidentialité et à la sécurité des données et il doit mettre en place l'organisation appropriée des mesures techniques. Le texte sous analyse devrait donc être adapté en ce sens.

b. Finalités du traitement de données à caractère personnel et nature et catégories de données traitées

- Remarques liminaires

Alors que les dispositions de l'article 5 précité visent une multitude de données, il y a lieu de relever que celles-ci ne tombent pas toutes dans le champ d'application de la loi modifiée du 2 août 2002. En effet, depuis l'entrée en vigueur de l'article 1er de la loi du 27 juillet 2007[74] modifiant la loi du 2 août 2002, les dispositions de celle-ci ne s'appliquent plus aux personnes morales. En effet, le législateur, dans un souci de transposer plus fidèlement la directive 95/46/CE précitée, a soustrait les personnes morales du champ de protection de la loi précitée. Les données et informations relatives aux personnes morales ne tombent donc plus dans le champ d'application de la loi modifiée du 2 août 2002.

Bien entendu, les données relatives à des personnes physiques (p.ex. représentants, dirigeants, salariés, clients, etc.) traitées par les personnes morales restent toujours soumises au régime protecteur de la loi modifiée du 2 août 2002.

De même, les données des commerçants exerçant en nom personnel tombent dans le champ d'application de la loi modifiée du 2 août 2002.

- Catégories de données collectées nécessaires aux finalités envisagées

[74] 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.

L'article 5 du projet de loi ne précise pas du tout quelles données ou catégories de données peuvent effectivement être collectées et traitées. Le commentaire des articles est également muet sur cette question. Ce n'est que dans l'exposé des motifs du projet de loi sous analyse où l'on peut retrouver certaines indications sur les catégories de données concernées[75]. En effet, les informations qui semblent être visées par l'article 5 sont : i) des données financières, notamment celles concernant le crédit et la solvabilité (données collectées dans la centrale des bilans), ii) les jugements contre les commerçants, iii) la liste des protêts, iv) les notifications de licenciement pour raison économique et v) les dettes accumulées auprès du Centre commun de la sécurité sociale et des administrations fiscales. Par ailleurs, il ressort du commentaire des articles que le secrétariat du Comité de conjoncture aura accès *« à des informations de source administrative… »*[76], sans pour autant préciser de quelles informations il s'agit concrètement.

Faute de précisions dans le texte, la Commission nationale n'est pas en mesure de déterminer quelles données relèvent en fin de compte de son domaine de compétence ou non. Pour celles qui rentreraient dans sa sphère de compétence, elle se trouve dans l'impossibilité d'apprécier la nécessité et la proportionnalité des données traitées au regard des finalités envisagées.

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 »*. Par ailleurs, les **données doivent être** *« **adéquates, pertinentes et non excessives au regard des finalités** pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement[77]»*.

Le texte sous examen ne précise cependant ni les finalités exactes poursuivies par le ou les responsables du traitement, ni les données concernées par le(s) traitement(s), ni n'explique comment le nouveau fichier tenu auprès du comité de conjoncture (et, le cas échéant, auprès de la Cellule d'Evaluation des Entreprises en Difficulté) est alimenté en données (origine des données). En effet, il se limite à énoncer que les *« renseignements et données utiles concernant les débiteurs qui sont en difficultés financières … sont tenus à jour au secrétariat du Comité de conjoncture »*. Ce libellé est cependant beaucoup trop vague. En effet, les termes « obtenir toute information » ne répondent pas aux exigences de précision et de prévisibilité auxquelles doit répondre un texte légal et ne sont, par ailleurs, pas conformes à l'article 4 précité et constituent un blanc-seing pour le responsable du traitement à collecter des données sans la moindre limitation.

Le texte de l'article 5 ne précise pas non plus l'origine des données collectées et traitées, ni ne précise les opérations de traitement envisagées. En effet, il faudrait notamment préciser et énumérer (i) à quelles données précises, contenues dans des fichiers étatiques, les responsables du traitement peuvent avoir accès (p.ex. Centre commun, administrations fiscales), (ii) quelles données proviennent directement des intéressés et (iii) quelles données proviennent d'autres sources (tribunaux, greffes, etc.).

A ce titre, 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*

[75] Doc. parl. n°6539/00, page 8.
[76] Doc. parl. n°6539/00, page 51.
[77] Article 4, paragraphe (1), lettre (b) de la loi.

essentiels peuvent être réglés par des règlements »[78]. Selon cette jurisprudence, il faudrait donc créer un cadre normatif législatif précis, qui retient au moins les finalités, les conditions et les modalités du ou des traitements envisagés.

Au vu de ce qui précède, la Commission nationale estime nécessaire de préciser à l'article 5 :

- le ou les responsable(s) du traitement,
- les finalités claires et précises du ou des traitement(s),
- l'adoption d'un règlement grand-ducal qui précisera les données ou catégories de données qui peuvent être collectées ou traitées au regard des finalités envisagées.

Pour ce qui est de la collecte de données par l'accès à d'autres banques de données étatiques (cf. doc. parl. n°6539/00, page 51), que ce soit par communication ou interconnexion, le texte de loi en projet devra nécessairement préciser les données qui pourront être communiquées au Comité de conjoncture via un accès à d'autres fichiers étatiques.

En effet, le Conseil d'Etat insiste régulièrement dans ses avis « *que la communication de données à caractère personnel à des tiers, de même que l'interconnexion de fichiers de données sont des opérations très délicates qui doivent être entourées d'un maximum de garanties*[79] ».

Tant que les finalités ainsi que les catégories de données destinées à être collectées et traitées n'ont pas été clairement précisées, la Commission nationale se voit dans l'impossibilité d'évaluer le respect des principes de nécessité et de proportionnalité des données au regard des finalités poursuivies.

3. Droit d'accès

L'article 5, paragraphe (2) du projet de loi introduit un droit d'accès et un droit de rectification au profit des débiteurs concernés. Il ressort implicitement du commentaire des articles[80] que ce droit d'accès spécifique ne porte que sur les données et informations relatives à des personnes morales. Le texte crée donc en quelque sorte un droit d'accès reconnu aux personnes morales dont les informations ne tombent cependant pas dans le champ d'application de la loi modifiée du 2 août 2002, droit qui ne doit pas être confondu avec le droit d'accès prévu à l'article à l'article 28 de la loi modifiée du 2 août 2002 et lequel ne peut être exercé qu'en ce qui concerne les données relatives à une personne physique.

[78] Cour constitutionnelle, arrêt 108/13 du 29 novembre 2013 (Mém. A n°217 du 13 décembre 2013, p. 3886).
[79] Voir par exemple le doc. parl. n°6284/5.
[80] Doc. parl. n°6539/00, page 51.

4. Création d'une base légale pour la transmission de certains jugements au (secrétariat du) Comité de conjoncture

L'article 6 du projet de loi sous examen introduit une base légale expresse pour la transmission de certains jugements par les greffes des tribunaux au (secrétariat du) Comité de conjoncture.

La transmission d'un jugement, dans la mesure où il n'est pas anonymisé, rentre dans le cadre de la définition d'un traitement de données à caractère personnel au sens de l'article 2, lettre (r) de la loi modifiée du 2 août 2002. En effet, les décisions prononcées par les cours et tribunaux contiennent des données à caractère personnel.

La CNPD recommande de rajouter une disposition qui précise que le Comité de conjoncture ne pourra pas transmettre ou communiquer ces données à caractère personnel à des tiers non autorisés, c'est-à-dire qui ne sont pas impliqués ou visés dans les procédures prévues par le projet de loi sous examen.

5. Demande de communication d'informations de la part du (secrétariat du) Comité de conjoncture

L'article 7, paragraphe (1), deuxième alinéa du projet de loi dispose que « *lorsqu'il (le secrétariat du Comité de conjoncture) estime que la continuité de l'entreprise d'un débiteur est menacée, il peut inviter le débiteur afin d'obtenir toute information relative à l'état de ses affaires et au sujet des mesures de réorganisation éventuelles* ».

A ce titre, la Commission nationale renvoit à ses observations faites sous le point 2, lettre b), 2e tiret.

Le paragraphe (2) du même article introduit un droit de communication des données recueillies par le secrétariat du Comité de conjoncture au profit du débiteur (personne morale ou physique). A ce titre, il est renvoyé au point 3 ci-avant.

6. La problématique de la liste des protêts

L'article 88 du texte sous examen vise à remanier le texte actuel de l'article 97 de la loi modifiée du 8 janvier 1962 concernant la lettre de change et le billet à ordre. Ledit article 97 prévoit notamment que les receveurs de l'Administration de l'enregistrement dressent chaque mois un tableau des protêts des lettres de change et des billets à ordre, tableau qui contiendra notamment les nom, prénoms, profession et domicile du souscripteur/accepteur et de sa contrepartie, donc des données à caractère personnel. Ce tableau est envoyé au président du tribunal de commerce dans le ressort duquel le protêt a été fait et est déposé aux greffes de ces tribunaux. Il y est également précisé que ce tableau est accessible au greffe à toute personne qui en fait la demande. Or, avec l'entrée en vigueur de la loi modifiée du 2 août 2002, les greffes ont cessé de diffuser cette liste, « *car cette pratique ne trouvait pas de base légale si ce n'est une référence à l'article 97 … qui prévoit pour le public la possibilité de consulter la liste auprès du greffe des tribunaux d'arrondissement*[81] ».

L'article 88 envisage de rajouter à la liste des destinataires du tableau des protêts (i) le secrétariat du Comité de conjoncture, (ii) la Chambre de commerce ainsi que (iii) la Chambre des métiers. A ce titre, la Commission nationale note que le conseil d'Etat, dans le cadre du projet de loi n°5157[82], avait déjà adressé cette problématique et avait approuvé « *le fait de donner une base légale certaine à cette distribution de données sensibles*[83] ».
Le projet de loi n°5157 a cependant été retiré du rôle de la Chambre.

---

[81] Doc. parl. n°6539/00, page 77.
[82] Projet de loi n°5157 portant des mesures ponctuelles en matière de prévention des faillites et de lutte contre les faillites organisées.
[83] Doc. parl. n°5157/03, page 8.

7 Annexes

La CNPD fait sienne les remarques du Conseil d'Etat précités, qui peuvent être transposées telles quelles à l'article 88 du projet de loi. En effet, cet article reprend quasi intégralement le texte tel qu'il avait été proposé dans le projet de loi n°5157. L'introduction de cette base légale va effectivement augmenter la sécurité juridique pour toutes les parties impliquées.

Elle comprend cependant aussi le risque de stigmatisation ou de mise au pilori des débiteurs et plus particulièrement des commerçants exerçant en leur nom personnel.

Dans un souci d'équilibre et de mise en balance des intérêts respectifs en cause, à savoir le risque de divulgation d'informations sensibles relatives aux débiteurs, d'une part, et l'intérêt des personnes morales ou physiques à vouloir se protéger contre des entreprises en difficulté, d'autre part, la Commission nationale accueille favorablement la modalité de publication limitée, dans la mesure où les intéressés doivent se déplacer pour prendre connaissance de la liste des protêts auprès des greffes des tribunaux. Dès lors, la CNPD suggère de rajouter en fin de phrase du dernier paragraphe de l'article 88 les termes « *sur place* », pour éviter toute ambiguïté relative aux publications par d'autres moyens.

En effet, une telle disposition limite la diffusion de ces données au grand public notamment via Internet et permet dès lors de réduire sensiblement le risque de stigmatisation de la partie défaillante, tout en maintenant le droit des parties intéressées d'être informées sur les inscriptions récentes de la liste des protêts.

Pour le surplus, la Commission nationale n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 20 novembre 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Avis à l'égard du projet de loi n°6893 relative à la reconnaissance des qualifications professionnelles et du projet de règlement grand-ducal relatif à la reconnaissance des qualifications professionnelles

Délibération n°718/2015
du 17 décembre 2015

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 de l'Enseignement supérieur et de la Recherche en date du 12 octobre 2015, la Commission nationale entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n°6893 relative à la reconnaissance des qualifications professionnelles. Par courrier du 30 novembre 2015, le Ministre de l'Enseignement supérieur et de la Recherche a invité la CNPD de se prononcer également au sujet du projet de règlement grand-ducal relatif à la reconnaissance des qualifications professionnelles.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données.

1. Art. 56. Autorités compétentes :

Suivant les dispositions de l'article 56, paragraphe (2) du projet de loi sous analyse, il est prévu que les autorités compétentes luxembourgeoises échangent avec leurs homologues européens des *« informations sur les sanctions disciplinaires ou pénales qui ont été prises ou sur des faits graves et précis susceptibles d'avoir des conséquences sur l'exercice d'activités au titre de la présente loi. Ce faisant, elles respectent les règles sur la protection des données à caractère personnel prévues dans les directives 95/46/CE et 2002/58/CE ».*

Le texte du projet de loi fait référence aux directives 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 et 2005/58/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, à l'instar de l'article 56 paragraphe 4 de la directive 2013/55/UE modifiant la directive 2005/36/CE relative à la reconnaissance des qualifications professionnelles et le règlement (UE) n°1024/2012 concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur, qui fait l'objet de la transposition en droit national par le projet de loi sous avis. La deuxième phrase de l'article 56, paragraphe (2) du projet de loi ne reprend cependant pas fidèlement le libellé de l'article 56 paragraphe 4 de la directive 2013/55/UE et modifie même la portée de ce dernier. La CNPD estime par ailleurs que le projet de loi devrait se référer à la législation nationale, à savoir la loi modifiée du 2 août 2002 qui a transposé en droit la directive 95/46/CE. Elle suggère dès lors de modifier la 2ème phrase de l'article 56, paragraphe (2) comme suit : *« Les traitements de données à caractère personnel aux fins d'échange d'informations doivent être conformes à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ».*

Aussi recommande-t-elle de supprimer la référence à la directive 2002/58/CE qui est transposé en droit national par 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 et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle, alors qu'elle ne comprend pas en quoi le projet de loi sous examen touche le champ d'application de ces textes.

La référence à la loi modifiée du 2 août 2002 est d'autant plus importante, alors que l'article 56 du projet de loi prévoit entre autres des échanges de données relatives à des sanctions pénales entre autorités. En effet, suivant les dispositions de l'article 8, paragraphe (2) de la loi modifiée du 2 août 2002, « *le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être mis en œuvre qu'en exécution d'une disposition légale* », alors que la directive 95/46/CE a laissé une certaine marge de manœuvre aux Etats-membres dans sa transposition. Ainsi, l'article 8[84] de la directive permet de traiter des données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté « *sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national* ». Considérant que le législateur luxembourgeois a choisi que seule une disposition légale peut autoriser le traitement de données relatives à des sanctions pénales, la référence à la loi modifiée du 2 août 2002 à l'article 56 du projet de loi est donc nécessaire afin de clarifier le régime applicable en droit national.

2. Art. 59. Registre des titres professionnels :

a. Responsable du traitement, finalités et origine des données

L'article 58 du projet de loi créé auprès du ministre ayant l'Enseignement supérieur dans ses attributions un centre d'assistance qui a notamment pour mission de gérer le registre des titres professionnels créé à l'article 59 et le registre des titres de formation créé à l'article 66. Il ne résulte cependant pas clairement du texte en projet qui est le responsable du traitement. Le fait que les autorités compétentes des diverses professions réglementées ont également accès audit registre[85] et qu'elles y procèdent notamment à des inscriptions ne facilite pas l'analyse. Les divers intervenants doivent-ils, le cas échéant, être considérés comme responsables conjoints ?

La Commission nationale suggère de désigner comme responsable du traitement le ministre ayant

[84] V. not. article 8 « Traitements portant sur des catégories particulières de données », point 5 de la directive 95/46/CE 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

[85] V. article 59, paragraphe (2).

l'Enseignement supérieur dans ses attributions, en précisant que les données sont fournies par les autorités compétentes des différentes professions réglementées (quitte à ce que le centre d'assistance précité assure la gestion du registre).

Le premier paragraphe de l'article 59 prévoit la création du registre des titres professionnels *« en vue de l'accès aux professions réglementées… »* et le paragraphe 3 du même article fait référence aux informations qui servent de base pour l'émission des cartes professionnelles européennes, telles que prévues par la directive européenne 2013/55/UE.

L'article fait donc ressortir deux catégories de finalités. Pour une meilleure lisibilité du texte, la CNPD recommande de regrouper ces deux finalités au paragraphe 1er de l'article 59 et d'inverser les paragraphes (2) et (3), afin de préciser d'abord les finalités du traitement des données, ensuite le principe de la création d'un fichier et enfin la provenance des données.

Il n'est par ailleurs pas souhaitable que le texte de l'article 59 du projet de loi utilise deux termes différents, à savoir *« registre »* et *« banque de données »*. La Commission nationale suggère d'avoir recours au terme de *« fichier »* afin de s'aligner sur la terminologie utilisée dans la loi modifiée du 2 août 2002.

b. Publicité du registre des titres professionnels

L'article 59, paragraphe (3) prévoit que les informations traitées dans le registre professionnel sont accessibles au public de manière électronique.

La Commission nationale s'interroge quant à l'étendue de cette mesure de publicité qui ne semble pas être prévue ni par la directive 2005/36/CE relative à la reconnaissance des qualifications professionnelles, ni par sa directive modificative 2013/55/CE. Seul l'article 9 de la directive 2005/36/CE qui a trait à l'information des destinataires du service prévoit certaines mesures d'information au profit de tout destinataire du service presté par un professionnel. Or, il est difficilement concevable que par *« des moyens équivalents d'identification*[86] *»* aient été visés la date de naissance ainsi que l'adresse du demandeur.

La collecte et le traitement des données figurant au fichier (« registre professionnel ») sont certes nécessaires et légitimes pour des besoins administratifs internes dans le cadre des finalités poursuivies par le projet de loi. Or, dans le cadre de la publicité et de la transparence, la CNPD considère comme excessive et disproportionnée la divulgation au public de la date de naissance ainsi que l'adresse, au cas où celle-ci renseignerait l'adresse privée. Elle estime dès lors nécessaire d'exclure des mesures de publicité la date de naissance ainsi que l'adresse privée des professionnels, à moins que cette dernière se confonde avec l'adresse professionnelle.

3. Art. 66. Registre des titres de formation :

a. Responsable du traitement

A l'instar des remarques formulées à l'endroit de l'article 59 ci-avant, il ne résulte pas clairement du texte de l'article 66 qui est le responsable du traitement du registre des titres de formation. Le paragraphe (2) dudit article opère une distinction dudit registre en deux sections différentes, à savoir la section de l'enseignement secondaire et celle de l'enseignement supérieur, le ministre ayant l'Education nationale dans ses attributions étant compétent pour la première, alors que le ministre ayant l'Enseignement supérieur dans ses attributions est compétent pour la deuxième.

[86] Article 9, lettre a) de la directive 2005/36/CE.

7 Annexes

La Commission nationale comprend qu'il est dans l'intention des auteurs du texte d'attribuer la responsabilité du traitement à chaque ministre en ce qui concerne son domaine de compétence.

Cependant, dans sa version actuelle, l'article 66 ne permet que de conclure que les deux ministres assument une responsabilité conjointe en ce qui concerne les traitements effectués dans ledit registre. En effet, suivant l'article 2 lettre (n) de la loi modifiée du 2 août 2002, le responsable du traitement est défini comme *« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel… »*.

Au vu de cette définition, il n'existe que trois possibilités en ce qui concerne l'attribution de la responsabilité des traitements effectués dans le registre des titres de formation. Soit le ministre ayant l'Education nationale dans ses attributions est responsable pour le registre, soit le ministre ayant l'Enseignement supérieur dans ses attributions est désigné responsable pour tout traitement effectué sur le registre, soit les deux ministres sont conjointement responsables, chacun pour le traitement de données relevant de son ressort.

En ce qui concerne le projet de règlement grand-ducal relatif à la reconnaissance des qualifications professionnelles, la Commission nationale pour la protection des données n'a pas d'observations particulières à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 17 décembre 2015.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Georges Wantz
Membre effectif

Participations aux travaux européens

Documents adoptés par le groupe de travail « Article 29 » en 2014

Document	Date d'adoption	Référence
Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain	16.12.2015	WP 179
Guidelines for Member States on the criteria to ensure compliance with data protection requirements in the context of the automatic exchange of personal data for tax purposes	16.12.2015	WP 234
Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data	01.12.2015	WP 233
Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing	22.09.2015	WP 232
Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones	16.06.2015	WP 231
Explanatory Document on the Processor Binding Corporate Rules	22.05.2015	WP 204
Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes	04.02.2015	WP 230
Cookie sweep combined analysis	03.02.2015	WP 229

Tous les documents de travail du groupe de travail « Article 29 » peuvent être téléchargés sur Internet[87].

[87] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/

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