CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2017

CNPD

COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Rapport annuel 2017

Table des matières

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

Table des matières

Table des matières

1 Avant-propos

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

« RGPD[1] » en français, « GDPR[2] » en anglais ou encore « DSGVO[3] » en allemand : ces termes, utilisés pour parler des nouvelles règles en matière de protection des données, sont maintenant omniprésents.

Au cours des derniers mois, ils sont apparus de plus en plus dans les médias nationaux et internationaux et faisaient l'objet de nombreux débats, de conférences et tables rondes. Le « RGPD » ou règlement général sur la protection des données suscite de nombreuses interrogations auprès des entreprises, administrations publiques et associations et il est au cœur des préoccupations de la CNPD.

Une année de transition vers le RGPD

L'année 2017 peut en effet être considérée comme une année charnière vers ce nouveau

[1] Règlement général sur la protection des données
[2] General data protection regulation
[3] Datenschutz-Grundverordnung

régime. Une année pendant laquelle les acteurs de tout bord s'engagent dans la dernière ligne droite de préparation aux règles entrant en application dans les 28 pays de l'Union européenne le 25 mai 2018.

Un des avantages du RGPD est qu'il s'agit d'un règlement et non d'une directive. Les mêmes règles seront donc directement applicables à tous les acteurs actifs sur le territoire de l'Union européenne. Les disparités qui caractérisaient les modalités de mise en œuvre de l'ancienne directive de 1995 sur la protection des données dans les États membres avaient donné lieu à des incohérences.

Le nouveau règlement renforce les droits existants, attribue de nouveaux droits tel que le droit à la portabilité ou le « droit à l'oubli » et octroie aux individus une maîtrise accrue de leurs données personnelles. En cas de violation de données graves, les entreprises et organismes publics doivent envoyer une notification à la CNPD et, le cas échéant, aux personnes concernées, dans un délai de 72 heures, afin que les utilisateurs puissent prendre les précautions qui s'imposent.

Toutefois, le contenu du règlement n'est pas si révolutionnaire qu'il ne paraît. En effet, de nombreux principes fondamentaux, comme par exemple le principe de loyauté, d'exactitude, de sécurité, de minimisation des données et de respect des droits des individus dont les données sont traitées – sont issus de la directive de 1995, le RGPD ne cherchant qu'à construire sur ces fondements.

Mais ce qui change fondamentalement, c'est que les organisations ne devront plus introduire une notification ou une demande d'autorisation préalable pour traiter des données à caractère personnel. Elles devront par contre vérifier elles-mêmes la légalité de leurs traitements et mettre les garanties adéquates en place pour protéger les personnes concernées. L'effectivité des mesures prises sera contrôlée par la CNPD avec la possibilité de prononcer des sanctions lourdes en cas d'infraction. A partir du 25 mai 2018, il revient aux entreprises elles-mêmes de s'intéresser au RGPD et de se mettre en conformité. À tout moment, elles devront être capables de démontrer la pertinence et l'adéquation des mesures techniques et organisationnelles mises en œuvre pour garantir le respect des obligations introduites par le règlement.

Vers plus de guidance et de sensibilisation

Ce changement de paradigme permettra à la CNPD de se concentrer davantage sur sa mission de sensibilisation du grand public et de guidance des responsables de traitement de données.

A l'approche de la date butoir du 25 mai 2018, ces deux missions étaient prioritaires. Ainsi, de nombreuses mesures ont été prises en matière d'information, de sensibilisation et de guidance en 2017, dont notamment :

- l'organisation de sessions d'information sur le RGPD les 18 et 19 octobre ;
- l'élaboration de l'outil « Compliance Support Tool » permettant aux acteurs privés et publics de tester leur conformité au RGPD ;
- la création de la nouvelle brochure « Vos obligations en matière de protection des données » pour les responsables de traitements et leurs sous-traitants ;
- l'organisation d'une conférence sur les droits des consommateurs dans le cadre du RGPD avec l'ULC et Securitymadein.lu ;
- la publication de trois vidéos animées présentant les nouveautés du RGPD ;
- la participation à la campagne « Big Data » de BEE SECURE ;

1 Avant-propos

- la publication d'un guide de préparation au GDPR sur son site Internet ;
- l'organisation de la formation « Introduction à la protection des données » ou encore
- la participation à de nombreuses conférences et formations (Chambre de Commerce, ABBL, administrations étatiques, élus locaux, INAP, etc.).

Une Commission très sollicitée

Parallèlement aux efforts accrus en matière de guidance, la CNPD a continué à assurer ses missions « traditionnelles ».

Ainsi, elle est de plus en plus sollicitée par les entreprises, administrations ainsi que par les associations qui ont besoin de conseils personnalisés pour se conformer à la loi, par les citoyens qui ont un besoin d'information en matière de protection des données.
En 2017, la CNPD a participé à 281 réunions (+83 par rapport à 2016) et répondu à 528 demandes d'information par écrit (+23% par rapport à 2016).

Jusqu'au 25 mai 2018, la CNPD continuera également à recevoir des déclarations préalables d'acteurs publics et privés qui souhaitent traiter des données personnelles. À ce titre, elle a reçu 1.041 notifications et 1.162 demandes d'autorisation en 2017.

L'autorité de contrôle luxembourgeoise a, en outre, participé au processus législatif avec 22 avis sur des projets de loi ou mesures règlementaires en lien avec la protection des données. A titre d'exemple peuvent être cités les avis concernant la mise en œuvre du RGPD et la modification de la loi sur la protection des données, la protection des données en matière pénale et de sécurité nationale, les traitements des données des dossiers passagers, les services financiers et le secret bancaire ou encore la fonction publique.

Au-delà de son rôle consultatif, la CNPD reçoit en moyenne 197 plaintes par an depuis 2013. En 2017, à nouveau 200 personnes ont fait appel à ses services alors qu'elles ont estimé qu'il y a eu une violation de la loi. La moitié des plaintes provenaient de citoyens d'autres Etats membres de l'Union européenne et 48% concernaient des entreprises offrant des services sur Internet.

Parmi ces plaintes, 109 ont conduit à des contrôles et investigations, soit 32 de plus que l'année précédente.
Il s'agissait entre autres

Le siège de la CNPD à Belval

d'entreprises qui surveillaient leurs employés de manière illégale, de demandes d'accès, de rectification ou d'effacement non respectées ou encore de communications de données illégales à des tiers.

L'année a été très productive et ce notamment grâce au recrutement progressif de collaborateurs, la CNPD ayant pu engager 4 personnes en 2017. L'augmentation de la charge de travail, des défis, mais également du nombre de collaborateurs, se prédestine pour l'avenir.

Luxembourg, le 16 mai 2017

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

2 Les activités en 2017

L'année 2017 en un coup d'œil

Janvier

13 - Monsieur Christophe Buschmann est assermenté en tant que membre effectif de la CNPD
26 - La CNPD organise un panel avec l'Université du Luxembourg lors de la Computers, Privacy and Data Protection (CPDP) conférence à Bruxelles
28 - Journée de la protection des données
28 - La CNPD publie 3 vidéos animées sur le futur règlement européen sur la protection des données
28 - La CNPD lance le nouveau formulaire de plainte

Février

14 - La CNPD donne une présentation sur les DPO à la conférence « GDPR : comment organiser sa gouvernance interne ? »
16 - La CNPD donne une formation au Laboratoire National de Santé (LNS) à Dudelange

Mars

2 - La CNPD intervient à la 3e édition du Lëtzebuerger Juristendag

Avril

25 - La CNPD participe à la conférence « Law enforcement challenges in the online context » organisée par l'Université du Luxembourg
27-28 - La CNPD participe à la Conférence de printemps des autorités de protection des données à Chypre
28 - La CNPD participe à la 3e édition de l'Information Security Education Day

Mai

17 - La CNPD intervient à la conférence « GDPR - take control of your risk » de l'American Chamber of Commerce in Luxembourg
19 - La CNPD participe à la 9e Journée Sécurité Santé de la CFL

Juin

16 - La CNPD accueille l'autorité de protection des données du Japon
20-21 - La CNPD participe au séminaire européen « Case Handling Workshop » à Manchester

Juillet

4-7 - La CNPD organise des formations d'introduction à la protection des données

Septembre

25-29 - La CNPD participe à la 39ème Conférence internationale des commissaires de la protection des données et de la vie privée à Hong Kong
27 - La CNPD participe au symposium international sur la liberté d'information à Potsdam
27 - La CNPD intervient à la conférence de l'ABBL intitulée « Protection des données : GDPR, cybersécurité – un défi pour les entreprises »
28 - La CNPD participe à la table ronde « How to

DELIBERATIONS

1.051
Délibérations adoptées

22
Avis relatifs à des projets ou propositions de loi ou mesures réglementaires

36
Demandes d'agréments pour les chargés de la protection des données

FORMALITES PREALABLES

1.041
Notifications reçues

1.162
Demandes d'autorisations

8.786
Déclarants (depuis 2002)

GUIDANCE

281
Réunions
(+42% par rapport à 2016)

528
Demandes de renseignement par écrit
(+23% par rapport à 2016)

PLAINTES ET INVESTIGATIONS

200
Plaintes

109
Investigations

VIOLATIONS DE DONNEES (COMMUNICATIONS ELECTRONIQUES)

3
Notifications

build, explore, analyse, secure, trust your data in the cloud era ? » dans le cadre des IT Days

Octobre

5 - La CNPD participe à la journée de la protection des données auprès de l'administration étatique
10 - La CNPD participe à la conférence « Fit4Data Protection : RGPD » de la Chambre de Commerce
12 - La CNPD lance un outil permettant aux responsables du traitement de tester leur conformité au nouveau règlement
16 - La CNPD organise la conférence « Verbraucherschutz an Dateschutz ginn Hand an Hand » avec l'ULC et Securitymadein.lu
17 - La CNPD donne une formation à l'Institut Luxembourgeois des Actuaires (ILAS)
18-19 - La CNPD organise des séances d'information sur le règlement général sur la protection des données
18 - La CNPD publie sa nouvelle brochure « Vos obligations en matière de protection des données »
20 - La CNPD donne une présentation à l'occasion de la journée de l'accréditation de l'OLAS

Novembre

14 - La CNPD participe à la table ronde « From GDPR compliance to a European Data Market - a Long and Winding Road? » lors des Luxembourg Internet Days
20-21 - La CNPD préside une session lors de l'International Intelligence Oversight Forum 2017, organisé par le Haut-Commissariat aux Droits de l'Homme
28 - La CNPD intervient à ILA's (Institut luxembourgeois des administrateurs) Director's Day

Décembre

8 - La CNPD donne une conférence à l'Association Professionnelle des Courtiers en Assurances au Luxembourg
10 - Journée internationale des Droits de l'Homme
28 - La CNPD avise le projet de loi n°7184 relatif à la création de la CNPD et la mise en œuvre du règlement général sur la protection des données
28 - La CNPD avise le projet de loi n°7168 transposant la directive européenne 2016/680 dans le domaine de la police et de la justice

2 Les activités en 2017

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 2017 était axé sur les activités suivantes :

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

2.1 Supervision de l'application de la loi

2.1.1 Formalités préalables

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

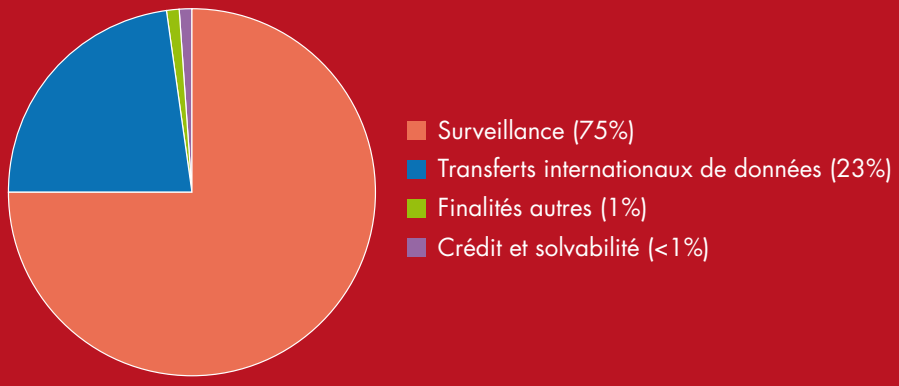
Le nombre total des traitements de données déclarés depuis 2003 s'élève à 28.817. En tout,

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 2017



8.786 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 le 25 mai 2018, certaines démarches administratives seront simplifiées. Les obligations de déclaration pour les organismes qui traitent des données à caractère personnel seront notamment supprimées.

2.1.1.1 Les notifications préalables

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

Au total, la CNPD a reçu 1.041 notifications préalables en 2017, soit 38 de plus que l'année précédente. Il existe deux types de notifications : les notifications ordinaires et les engagements formels de conformité.

Notifications ordinaires

En 2017, la CNPD a reçu 977 notifications ordinaires. La finalité la plus souvent invoquée était l'administration du personnel. D'autres raisons citées pour traiter des données personnelles dans le cadre de notifications étaient la gestion de la clientèle, la comptabilité, la gestion des fournisseurs ou encore la recherche scientifique.

Engagements formels de conformité

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

2 Les activités en 2017

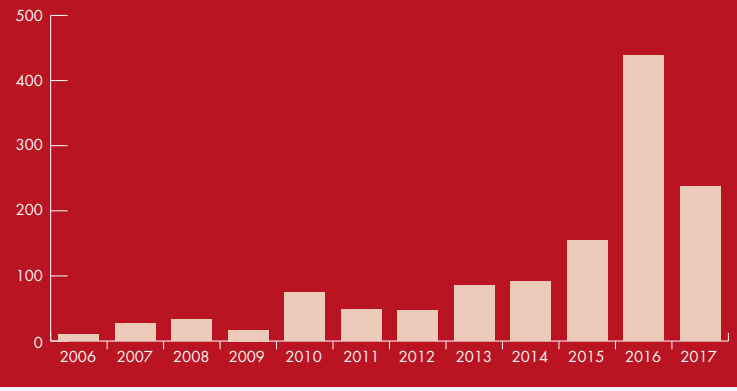
le responsable du traitement adresse à la Commission nationale un engagement formel par lequel il déclare que le traitement est conforme à la description figurant dans la décision unique.

Par sa décision n°108/2007 du 14 septembre 2007, la Commission nationale a défini les modalités des traitements de données que les employeurs (chefs d'entreprise, chefs d'établissement ou leurs délégués) sont amenés à opérer dans le cadre de l'organisation et du déroulement des élections des délégués du personnel, des délégations des jeunes travailleurs et des représentants du personnel dans les comités mixtes d'entreprise et les conseils d'administration des sociétés anonymes. La CNPD a reçu 64 engagements formels de conformité en 2017.

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

Transferts vers des pays tiers



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 1.162 demandes (demandes d'autorisation et engagements formels de conformité) en 2017.

Demandes d'autorisation

Le nombre de demandes d'autorisation reçues par la CNPD se maintient à un niveau élevé : 1.030 demandes lui ont été soumises en 2017 (contre 1.338 en 2016).

75% des demandes en 2017 étaient relatives à la surveillance sur le lieu du travail. 58% de celles-ci concernaient l'exploitation de caméras de surveillance et 10% le contrôle des déplacements de véhicules et de personnes grâce à la géolocalisation.

Engagements formels de conformité

En plus des demandes d'autorisation, la Commission nationale a reçu 132 engagements formels de conformité en 2017. 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 signer un engagement formel par lequel il déclare que le traitement est conforme à la description figurant dans la décision unique de la Commission nationale.

2.1.2 Transferts de données hors Union européenne

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

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

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

La loi prévoit des exceptions à ce principe d'interdiction. D'autres moyens existent pour permettre aux responsables du traitement d'apporter un niveau de protection suffisant pour transférer des données vers des pays tiers.

Les dérogations légales

L'article 19 (1) de la loi modifiée du 2 août 2002 et la directive 95/46/CE prévoient des exceptions au principe d'interdiction de transferts (consentement de la personne concernée, nécessité pour l'exécution d'un contrat conclu dans l'intérêt de la personne concernée, intérêt public important…). Ces dérogations

2 Les activités en 2017

légales ne s'appliquent toutefois que pour des transferts de données qui ne peuvent être qualifiés de répétés, massifs ou structurels.

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

Les clauses contractuelles types

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

Les règles d'entreprise contraignantes

Les règles d'entreprise contraignantes (« Binding Corporate Rules ») constituent un outil susceptible d'assurer une protection adéquate des données à caractère personnel lorsque celles-ci sont transférées

ou traitées en dehors de l'Union européenne.

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

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

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

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

En 2017, le groupe Rakuten a adopté des règles d'entreprise contraignantes. Ces règles visent en premier lieu à garantir que la protection dont bénéficient les employés et clients de Rakuten dans les Etats membres de l'Union européenne continue à s'appliquer lorsque les informations sont transférées en dehors de l'UE. Rakuten Inc. est une entreprise offrant des services sur Internet. Son siège mondial est situé au Japon et son établissement principal en Europe se trouve au Luxembourg. Pendant une année, la CNPD a coopéré avec Rakuten en qualité d'autorité chef de file (« lead authority ») dans le cadre de la procédure de coopération et de reconnaissance mutuelle européenne, en collaboration avec les autorités de protection des données de sept autres pays européens où le groupe est implanté (à savoir l'Allemagne, l'Autriche, l'Espagne, l'Estonie, la France, l'Irlande et le Royaume-Uni). Ces dernières ont validé le résultat atteint par la CNPD.

Le « EU-U.S. Privacy Shield Framework »

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

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

Formalités

De plus en plus d'entreprises collaborent avec des partenaires commerciaux et offrent leurs produits et services sur des

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

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

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

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

Au total, la CNPD a été saisie de 238 demandes de transfert en 2017. La majorité des demandes émanaient d'entreprises du secteur financier. Le pays de destination était le plus souvent les Etats-Unis.

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 par conséquent recourir à un chargé externe inscrit sur la liste des personnes agréées par la CNPD afin d'exercer cette fonction. Depuis 2007, sur suggestion de la CNPD, les salariés peuvent également être désignés comme chargés, à condition que ces derniers bénéficient d'une certaine indépendance vis-à-vis des

responsables du traitement qui les ont désignés et qu'ils disposent du temps approprié pour pouvoir s'acquitter de leurs missions.

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

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

Avec la désignation d'un chargé, l'expertise de la protection des données fait son entrée dans les entreprises et autres organismes. Le nouveau règlement européen, qui entrera en vigueur le 25 mai 2018, prévoit que les autorités publiques et les entreprises qui effectuent certains traitements de données à risques doivent désigner un délégué à la protection des données.

Au total, 136 entreprises, associations et organismes publics ont désigné un chargé de la protection des données.

À la fin de l'année 2017, 150 personnes physiques ou morales étaient agréées pour exercer l'activité de chargé de la protection des données.

2.1.4 Demandes de vérification de licéité et plaintes

En 2017, 200 personnes ont fait appel aux services de la CNPD lorsqu'elles ont estimé qu'il y a eu une violation de la loi ou une entrave à l'exercice de leurs droits. Les 5 dernières années, la CNPD a reçu 197 plaintes en moyenne par an.

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

48% des plaintes visaient des entreprises offrant des services sur Internet.

Motifs des plaintes

Dans presque un tiers 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 :

2 Les activités en 2017

- les conditions générales relatives à des commerces ou des services en ligne ;

- la durée de conservation des données collectées (p.ex. : historique d'achat) ;

- la demande de documents comme la carte d'identité ou le passeport à des fins de vérification d'identité ;

- la publication des données à caractère personnel en ligne ;

- la collecte illicite ou excessive de données ;

- la création d'annuaires sans le consentement des personnes concernées ;

- la prise de photos à l'insu de la personnes concernée ;

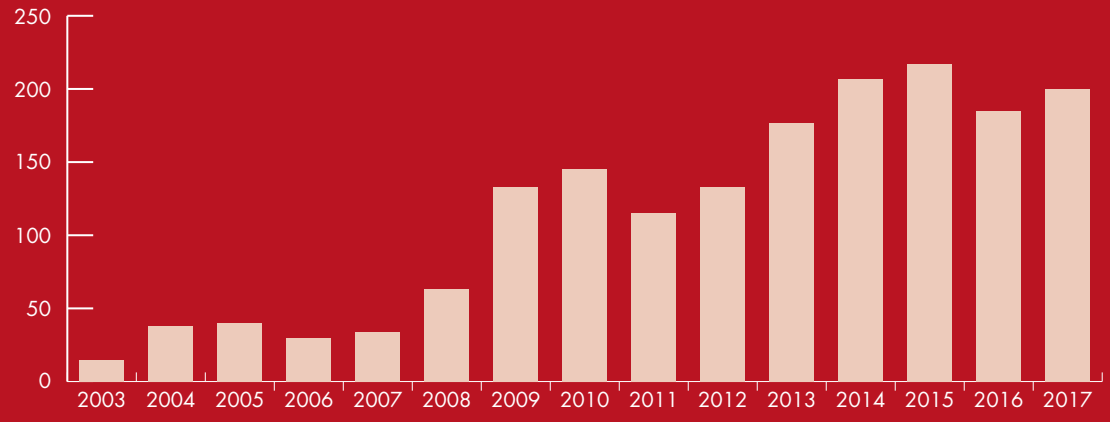
- les décisions individuelles automatisées.

La transmission non autorisée de données à des tiers a également conduit à un certain nombre de plaintes (18,5%). Cela inclut par exemple la publication de données (vidéos, photos, etc.) en ligne sans les protéger suffisamment ou encore l'utilisation de données à des fins autres que celles pour lesquelles elles ont été collectées initialement. Des plaintes récurrentes concernent l'envoi de courriels à des personnes auxquelles ils n'étaient pas destinés ou l'envoi de courriels confidentiels mais distribués de façon collective et visible à tous les destinataires (« CC » au lieu de « BCC »). La CNPD est également saisie de plus en plus de plaintes concernant des consultations non autorisées dans le registre national des personnes physiques par des agents du secteur public.

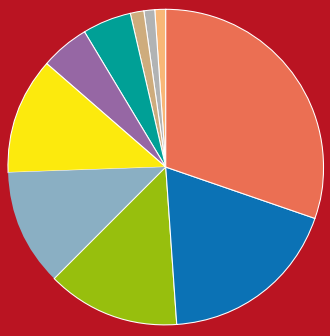
Un nombre important de plaintes (13,5%) a été motivé par le non-respect du droit d'accès par les responsables du traitement. Ceux-ci ont refusé aux citoyens d'accéder à leurs données, ignoré leurs requêtes ou ne leur ont pas donné assez de renseignements par rapport aux obligations légales à respecter en matière de droit à l'information et d'accès. À ce titre, les fermetures, respectivement les suspensions de comptes clients, notamment par les sociétés de commerce en ligne, font l'objet de plaintes récurrentes. Dans de telles situations, les citoyens ne comprennent pas toujours les raisons pour lesquelles le statut de leur compte a changé en raison des informations parfois insuffisantes qui leurs sont fournies par les sociétés. Souvent, ils veulent une confirmation que leurs données ne font plus l'objet d'un traitement.

Les demandes d'effacement ou de rectification de données auxquelles les suites souhaitées n'avaient pas été réservées ont constitué 12% des plaintes reçues en 2017. Il s'agissait,

Evolution du nombre de plaintes



Motif des plaintes



- Licéité de certaines pratiques administratives/commerciales (30,5%)
- Transmission déloyale à des tiers (18,5%)
- Refus d'accéder aux données (13,5%)
- Demande d'effacement ou de rectification des données (12%)
- Surveillance sur le lieu de travail (12%)
- Opposition à la prospection (5%)
- Exercice du droit à l'oubli (5%)
- Violation de sécurité (1,5%)
- Mesure de sécurite (1%)
- Autres (1%)

entre autres, de demandes de fermeture de comptes auprès de services en ligne ou de demandes d'effacement de données personnelles (adresses e-mail, évaluations, etc.) sur des sites Internet.

La majorité des requêtes liées à la surveillance sur le lieu du travail (12% des plaintes) concernaient la vidéosurveillance. Des plaignants ont également contacté la CNPD lorsqu'ils ont estimé que des systèmes de géolocalisation avaient été utilisés illégalement par leur employeur (utilisation sans autorisation de la CNPD ou surveillance en dehors des heures de travail).

5% des plaintes étaient relatives au droit d'opposition et à la prospection. La CNPD a dû intervenir à plusieurs reprises lors d'envois de courriels ou de SMS non sollicités ou encore dans des cas où les plaignants ont voulu connaître l'origine des données utilisées par les organisations/sociétés en vue de les prospecter.

Finalement, les plaintes concernant le droit au déréférencement dans les moteurs de recherche sont de plus en plus courantes (5% des plaintes en 2017).

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. Ce pouvoir d'investigation exclut les locaux d'habitation.

2 Les activités en 2017

Dans la plupart des cas, la CNPD intervient suite à des plaintes dans lesquelles des atteintes à la législation sur la protection des données lui sont signalées. Elle peut toutefois également entamer des investigations sur sa propre initiative, notamment dans un but de prévention.

En 2017, elle a effectué 109 contrôles et investigations, soit 32 de plus que l'année précédente. Cette tendance se poursuivra dans les prochaines années avec le nouveau règlement européen qui renforcera le rôle de supervision de la CNPD et privilégiera le contrôle a posteriori plutôt qu'a priori.

Il y a deux types d'intervention : les contrôles sur place où une intervention rapide de la CNPD est nécessaire ou les investigations par écrit.

Contrôles sur place

Dans presque 20% des cas, les agents de la CNPD sont directement intervenus sur place pour vérifier si les dispositions légales en matière de surveillance sur le lieu du travail ou encore les obligations posées par les autorisations de la CNPD avaient été respectées.

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

Dans d'autres cas, les responsables du traitement disposaient d'une autorisation, mais ne respectaient pas les conditions et exigences posées par celle-ci. Il s'agissait notamment du non-respect de l'obligation d'informer les salariés de l'existence d'un dispositif de surveillance.

Investigations par courrier

La CNPD est par ailleurs intervenue selon une procédure écrite dans des cas :

- de demandes d'accès, de rectification ou d'effacement non respectées par les responsables du traitement (23% des investigations) ;
- de communications de données illégales à des tiers (15% des investigations) ;
- de collectes de données excessives (10% des investigations) ;
- de demandes d'opposition non respectées par le responsable de traitement (5% des investigations) et encore

- de mesures de sécurité insuffisantes pour protéger des données personnelles (3% des investigations).

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 propose un formulaire de notification d'une violation de sécurité disponible sur son site Internet. Ce formulaire reprend toutes les questions pertinentes auxquelles les fournisseurs devront répondre dans une telle situation.

En 2017, 3 violations de données dans le secteur des communications électroniques, ayant eu un impact mineur, 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 avait été transposée au niveau national par la loi du 24 juillet 2010 modifiant la loi du 30 mai 2005 sur la protection de la vie privée dans le secteur des communications électroniques. L'objectif de cette directive était de conserver pendant un certain délai les données que traitent les opérateurs de télécommunications et les fournisseurs d'accès à Internet pour les besoins de la recherche, de la détection et de

2 Les activités en 2017

la poursuite d'infractions.
Un des enjeux majeurs de cette directive était le maintien de l'équilibre entre, d'une part, l'accès aux données traitées par des fournisseurs de communications électroniques dans le cadre de la lutte contre le terrorisme et la criminalité grave, et d'autre part, la protection de la vie privée des citoyens.

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

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

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

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

En 2017, les autorités compétentes ont fait 4.759 demandes auprès des opérateurs. Ce chiffre a augmenté par rapport à l'année 2016 où 4.398 demandes avaient été faites. Sur les 4.759 demandes, 676 demandes n'ont pas pu être satisfaites.

2.2 Avis et recommandations

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

En 2017, la Commission nationale a émis 22 avis dans le cadre de projets de loi ou de règlements grand-ducaux. Une sélection des avis est résumée ci-après. Tous les avis peuvent être consultés sur le site Internet de la CNPD à l'adresse *https://cnpd.public.lu/fr/publications/rapports/index.html.*

Les séances de délibération de la Commission nationale

Le collège se réunit en séance de délibération en principe une fois par semaine. Une partie importante de ces séances est consacrée à l'examen des dossiers de demande d'avis ou d'autorisation. Au cours de 38 séances en 2017, la Commission nationale a adopté 1.051 délibérations, dont notamment :

- 956 autorisations ;
- 22 avis relatifs à des projets ou propositions de loi et mesures réglementaires ;
- 40 décisions concernant les chargés de la protection des données.
- 26 décisions d'ouvrir des enquêtes.

2.2.1 Institut public d'aide à l'enfance et à la jeunesse

Le 10 mars 2017, la Commission nationale a émis un avis relatif à l'avant-projet de loi portant création d'un Institut public d'aide à l'enfance et à la jeunesse. Cette nouvelle structure a pour mission d'offrir un encadrement spécifique ciblé aux besoins des enfants et des jeunes âgés de 0 à 27 ans.

L'article 15 de cet avant-projet de loi prévoit la création d'un « fichier individuel des personnes accueillies par l'Institut », dans lequel figurent les données personnelles nécessaires aux fins de documenter l'hébergement et l'encadrement des personnes accueillies par les différents départements de l'Institut et à des fins d'études historiques et statistiques.

La CNPD a accueilli avec satisfaction le fait que cet article crée un cadre légal détaillé dans lequel des traitements de données à caractère personnel peuvent avoir lieu au sein de l'Institut. Elle a cependant tenu à partager certaines observations relatives au fichier de données à caractère personnel créé, en ce qui concerne plus particulièrement les finalités du traitement, les catégories de données traitées, la détermination du responsable du traitement, l'origine des données, les personnes ayant accès aux données, la durée de conservation des données, ainsi que les mesures de sécurité et le traçage des accès aux données.

2.2.2 Police

En date du 24 mars 2017, la Commission nationale s'est prononcée au sujet des projets de loi :

- n°7044 portant réforme de l'Inspection générale de la Police et modifiant 1) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat 2) la loi modifiée du 25 mars 2015 instituant un régime de pension spécial transitoire pour les fonctionnaires de l'Etat et des communes ainsi que pour les agents de la Société nationale des Chemins de Fer luxembourgeois 3). Le livre Ier du Code de la sécurité sociale et au sujet du projet de règlement y relatif et

- n°7045 portant réforme de la Police grand-ducale et abrogeant la loi du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

L'autorité de contrôle luxembourgeoise a soulevé un certain nombre de lacunes concernant les dispositions relatives à l'accès des agents de la Police grand-ducale et de l'Inspection générale de la Police à certaines bases de données étatiques et a suggéré des améliorations.

Elle a également soulevé le fait que si le projet de loi n°7045 règle l'accès de la Police grand-ducale aux bases de données des administrations, il est muet sur les bases de données opérées par la Police elle-même.

Dans son avis complémentaire du 1er décembre 2017, la CNPD a déploré qu'il n'a pas été suffisamment tenu compte de ses critiques exprimées dans son avis du 24 mars 2017.

2.2.3 Menace terroriste

En 2017, la CNPD a rendu deux avis complémentaires suite à deux séries d'amendements concernant le projet de loi n°6921 portant 1) modification du Code d'instruction criminelle, 2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, 3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques, 4) adaptation de la procédure pénale face aux besoins liés à la menace terroriste.

Pour rappel, la Commission nationale avait rendu un premier avis relatif à ce projet de loi en date du 12 février 2016 (délibération n°147/2016), ainsi qu'un avis relatif à une première série d'amendements gouvernementaux (délibération n°803/2016 du 14 septembre 2016).

Dans son deuxième avis complémentaire du 30 mars 2017, la CNPD a analysé les modifications apportées à l'article 47-27 projeté du Code de procédure pénale et a constaté que les données que les autorités judiciaires peuvent obtenir auprès des fournisseurs de services de télécommunications ne sont toujours pas déterminées avec suffisamment de précision.

En ce qui concerne la captation de données informatiques, elle a suggéré des améliorations notamment inspirées de la législation suisse, en particulier en ce qui concerne la sécurité des traitements de données.

Dans son troisième avis complémentaire du 10 mai 2017, la CNPD a examiné en détail les amendements relatifs à l'enquête sous pseudonyme et a soulevé un certain nombre de questions relatives à la signification du texte.

La CNPD a par ailleurs pris position par rapport à l'amendement introduisant la fixation d'images à l'intérieur de logements ou de véhicules. En particulier, elle a pointé le fait qu'il n'est pas clair si cette mesure peut être utilisée exclusivement dans le contexte d'infractions ayant trait au terrorisme telles qu'énumérées à l'article 88-2 paragraphe (2) lettre a) points 1. et 2. du Code de procédure pénale.

2.2.4 Déclaration de certaines maladies dans le cadre de la santé publique

Le 10 mai 2017, la Commission nationale s'est prononcée sur un projet de loi concernant la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique, ayant pour objectif d'améliorer le système de surveillance des maladies infectieuses au Grand-Duché de Luxembourg et de regrouper les données portant sur les maladies infectieuses dans un système centralisé.

Le système proposé par les rédacteurs du projet de loi vise à centraliser dans une base de données nationale, gérée par la Direction de la Santé, l'ensemble des données concernant les maladies à déclaration obligatoire. Il repose sur un principe de transmission obligatoire de données individuelles au Directeur de la Santé ou à son délégué par les médecins, les médecins-dentistes et les responsables des laboratoires d'analyses de biologie médicale pour une liste de maladies infectieuses présentant un risque particulier pour la santé publique. La CNPD a souligné dans son avis, qu'en qualité de responsable des traitements de données via ce système centralisé et exhaustif, la Direction de la Santé devra garantir un niveau particulièrement élevé de protection de la confidentialité et de la sécurité des données des personnes concernées.

En application du principe de minimisation des données, la CNPD a suggéré de limiter la collecte aux données strictement nécessaires à la surveillance sanitaire et de renoncer à la collecte systématique des nom, prénom, date de naissance entière et adresse des patients telle qu'elle était prévue dans certaines hypothèses par le projet de loi.

Compte tenu de l'extrême sensibilité des données collectées, la Commission nationale a indiqué que la mise en place de mesures d'anonymisation irréversible des données, passé un certain délai, serait de nature à garantir une meilleure protection des personnes à l'égard de leurs données à caractère personnel, à l'instar de la procédure de gestion des données prévues par le code de la santé publique français.

La CNPD a souligné dans son avis que le médecin ou le laboratoire qui signale une maladie à déclaration obligatoire devra en informer les personnes concernées, et ce au moment de l'annonce du diagnostic ou au moment qu'il jugera, en conscience, le plus opportun. Il devra notamment leur préciser quelles données seront transmises à l'autorité sanitaire et le caractère anonyme de la transmission.

Un document d'information individuelle, dont le modèle pourrait être établi par l'autorité sanitaire, pourrait également être remis aux personnes concernées, expliquant notamment à quoi sert le dispositif de déclaration obligatoire et comportant les mentions requises par l'article 26 précité de la loi modifiée du 2 août 2002.

La CNPD a également estimé dans son avis que les personnes concernées devraient pouvoir exercer leur droit d'accès aux données les concernant auprès de la Direction de la Santé pour autant qu'elles ne sont pas anonymisées, et ce par l'intermédiaire des médecins et laboratoires déclarants.

La Commission nationale a recommandé, s'agissant des transmissions par voie électronique, que des mesures de chiffrement à l'état de l'art pour des données sensibles soient mises en œuvre. Elle a également recommandé, s'agissant des transmissions par voie postale, que ces dernières soient effectuées sous pli confidentiel portant la mention « secret médical ».

Enfin, compte tenu de l'extrême sensibilité des données recueillies, la CNPD a insisté sur la nécessité de prévoir des mesures spécifiques de protection de l'identité des patients, tout en permettant une surveillance et un suivi efficace des cas de maladies infectieuses déclarés.

Les activités en 2017

2.2.5 Subvention pour ménage à faible revenu

En date du 10 mai 2017, la CNPD s'est prononcée au sujet du projet de règlement grand-ducal fixant les conditions et modalités d'octroi de la subvention pour ménage à faible revenu et de la subvention du maintien scolaire. Ce projet de règlement grand-ducal a pour objet de fixer les modalités d'octroi et de calcul de la subvention pour ménage à faible revenu d'une part, et de la subvention du maintien scolaire pour les élèves de l'enseignement secondaire d'autre part.

Ces deux subventions devraient être introduites par le nouvel article 2 de la loi du 13 juillet 2006 portant réorganisation du Centre psycho-social et d'accompagnement scolaires, telle que modifiée par le projet de loi N°6787 ayant pour objet l'organisation de la Maison de l'orientation et modifiant des dispositions diverses. La Commission nationale a regretté dans son avis de ne pas avoir été saisie dudit projet de loi.

A l'instar du Conseil d'Etat, la Commission nationale a estimé que les principes et points essentiels sur les modalités de l'octroi, les montants maximums et les conditions d'attribution de l'aide financière sont déterminés à suffisance par le projet de loi. En revanche, elle s'est demandée si une présentation plus précise des fichiers créés et des opérations de traitements effectuées à l'occasion de la gestion et de l'octroi des subventions dans celui-ci ne présenterait pas un avantage de clarté et de prévisibilité juridique pour les personnes concernées.

La CNPD a ensuite émis certaines remarques quant aux catégories de données traitées visées par le projet de règlement grand-ducal. Enfin, elle a abordé la question de l'accès au registre national des personnes physiques par le Centre psycho-social et d'accompagnement scolaire, prévu par le projet règlement grand-ducal.

2.2.6 Exposition aux rayonnements ionisants

Le 14 juillet 2017, la CNPD a publié son avis concernant le projet de loi relatif à i) la protection sanitaire des personnes contre les dangers résultant de l'exposition aux rayonnements ionisants et à la sécurité des sources de rayonnements ionisants contre les actes de malveillance, et ii) à la gestion des déchets radioactifs, du transport de matières radioactives et de l'importation, et iii) portant création d'un carnet radiologique électronique.
Les objectifs principaux du projet de loi sont « de garantir un haut niveau de protection de la population contre les conséquences d'une situation

d'urgence nucléaire» et une « amélioration de la protection sanitaire des personnes contre les dangers résultant de l'exposition aux rayonnements ionisants, y compris contre le radon au moyen d'un plan d'action radon et également un renforcement de la protection des patients soumis à une exposition médicale et la mise en place d'un carnet radiologique électronique ».

Dans son avis, la Commission nationale a limité ses observations aux questions soulevées par les dispositions du projet de loi traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel.

L'autorité de contrôle a analysé le flux d'information à l'égard de la surveillance radiologique individuelle de toutes les catégories de travailleurs exposés et a recommandé, inter alia, d'ajouter un délai déterminé pour la notification de la Direction de la santé (et d'autres acteurs) au cas où les 6/10 des limites de doses pour l'exposition professionnelle sont dépassées au cours d'une année calendaire. La CNPD a aussi constaté que la mise en place d'un système de surveillance individuelle soit justifié sur la base de plusieurs finalités citées par la loi du 2 août 2002 mais qu'au niveau des données concernées, le projet de loi n'était pas suffisamment précis en ce qui concerne les données d'identification exactes qui sont traitées. En outre, la Commission nationale a rappelé i) le principe de la minimisation des données par rapport aux données personnelles transmises aux différents acteurs, ii) les obligations des chefs d'établissement au niveau de l'information des travailleurs exposés et au niveau des droits des personnes concernées, et iii) le principe de la conservation des données personnelles pour une durée limitée.

La CNPD a analysé la création du carnet radiologique électronique, inter alia, par rapport au responsable du traitement et s'est interrogée sur la raison pour laquelle le projet de loi n'a pas envisagé que la responsabilité du traitement soit exercée de manière conjointe par les différents acteurs du carnet radiologique électronique et non pas seulement par l'Agence nationale des informations partagées dans le domaine de la santé.

En outre, la CNPD a constaté que le patient dispose d'un droit d'opposition avant le début du traitement de ses données dans le cadre du carnet radiologique électronique, mais aussi après. Elle s'est toutefois interrogée sur la manière dont le formulaire d'opposition serait rendu accessible en pratique et sur le sort des données enregistrées après une opposition signalée après le début du traitement.

Dans le contexte de la mise à disposition de données à des tiers, la Commission nationale a finalement rappelé que, dans l'esprit du Règlement général sur la protection des données (Règlement (UE) 2016/679), chaque fois que les finalités statistiques ou de recherche scientifique peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes, il convient de procéder de cette manière.

2.2.7 Services financiers et secret bancaire

La Commission nationale a avisé le projet de loi n°7024 portant mise en œuvre du règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte. Alors que le projet de loi vise à modifier plusieurs textes législatifs, la CNPD s'est limitée à commenter les modifications proposées, qui ont trait à la sous-traitance dans le secteur financier et dans le secteur des assurances.

Dans son avis du 16 mars 2017 et dans son avis complémentaire du 27 juillet 2017, la CNPD a rappelé que les professionnels du secteur financier et du secteur des assurances devront structurer

2 Les activités en 2017

leurs projets de sous-traitance de façon à respecter non seulement les obligations découlant de leur secteur propre, mais également les obligations découlant à l'heure actuelle de la loi modifiée du 2 août 2002 et celles découlant du futur règlement européen sur la protection des données, notamment en ce qui concerne le recours au consentement des personnes concernées, l'information des personnes concernées et les transferts de données vers des pays tiers.

La Commission nationale a par ailleurs attiré l'attention des auteurs du projet de loi sur les dispositions du RGPD qui prévoient des obligations pour les responsables du traitement et les sous-traitants en ce qui concerne les mesures de sécurité et l'encadrement de la sous-traitance en cascade.

2.2.8 Agence eSanté

Par courrier du 31 juillet 2017, le Ministre de la Sécurité Sociale a fait parvenir à la Commission nationale une série

d'amendements parlementaires au projet de loi n°7061 modifiant certaines dispositions du Code de la sécurité sociale. Pour rappel, la CNPD avait rendu, le 2 décembre 2016, un premier avis relatif audit projet de loi, dans lequel elle avait formulé diverses observations concernant les adaptations apportées à l'article 60ter du Code de la sécurité sociale concernant les missions et les moyens de l'Agence nationale des informations partagées dans le domaine de la santé (ci-après désignée « l'Agence eSanté »).

Dans son avis complémentaire du 17 novembre 2017, la CNPD a accueilli de manière favorable l'effort des auteurs des amendements tendant à encadrer plus précisément l'accès de l'Agence eSanté aux fichiers du Centre commun de la sécurité sociale et de la Caisse nationale de santé d'un côté, et le renvoi à un règlement grand-ducal spécifique visant à préciser les modalités de gestion de l'identification et les catégories de données contenues dans les annuaires référentiels d'identification d'autre côté. Néanmoins, la Commission nationale a regretté, en dépit des recommandations qu'elle a pu formuler à ce sujet, que les auteurs des amendements n'aient pas saisi l'opportunité pour clarifier les missions de l'Agence eSanté, s'agissant de l'offre d'un service de pseudonymisation en qualité de tiers de confiance.

2.2.9 Traitement des données des dossiers passagers

En date du 23 novembre 2017, la CNPD a publié un avis concernant le projet de loi n°7151 relatif au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave. Ledit projet de loi a pour objet de transposer en droit national la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

L'autorité de contrôle a entre autres suggéré d'identifier et d'énumérer expressément dans le corps du texte du projet de loi les différentes banques de données gérées par les services compétents en la matière ou qui leur sont accessibles dans l'exercice de leurs missions, en vue de réaliser une évaluation des passagers avant leur arrivée ou leur départ prévu du territoire luxembourgeois. Elle a ajouté qu'un règlement grand-ducal pourra alors prévoir une liste exhaustive des critères d'évaluation prédéterminés à compléter ou modifier si nécessaire.

Par ailleurs, la CNPD s'est ralliée à l'avis 1/15 de la Cour de Justice de l'Union européenne du 26 juillet 2017 concernant l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, en recommandant aux auteurs du projet de loi de décrire de manière plus précise et concise la rubrique relative aux informations disponibles sur les « grands voyageurs », ainsi que le champ des « remarques générales ». Ainsi, la CNPD a estimé qu'en l'état actuel, les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal n'ont pas été respectées par le texte du projet de loi qui ne pouvait donc pas être considéré comme étant conforme à l'article 4 de la loi modifiée du 2 août 2002, ni à l'article 8 de la Convention européenne des droits de l'homme, à l'article 52 de la Charte des droits fondamentaux de l'Union européenne, ainsi qu'à l'article 6, paragraphe (3) du RGPD.

2.2.10 Fonction publique

Le 8 septembre 2017, Monsieur le Ministre de la Fonction publique et de la Réforme administrative a déposé à la Chambre des députés le projet de loi n°7182 portant

Les activités en 2017

modification de la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat et de dispositions diverses. Ce projet de loi vise entre autres à insérer un nouveau chapitre 10bis dans la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat, qui porterait sur la « Protection des données nominatives ».

Au vu de la nature des dispositions prévues par ce nouveau chapitre 10bis, et en application de l'article 32, paragraphe (3), lettre (f) de la loi modifiée du 2 août 2002, la Commission nationale a pris la décision de se saisir elle-même pour aviser ce projet de loi.

La Commission nationale a tenu à saluer la décision des auteurs du projet de loi d'insérer un tel chapitre, justifié par la nécessité de mettre le statut général des fonctionnaires de l'Etat en conformité avec les nouvelles règles relatives à la protection des données prévues par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données qui entreront en vigueur le 25 mai 2018 (« RGPD »).

La CNPD n'a pas partagé la recommandation du Conseil d'Etat, selon laquelle ce chapitre 10bis devrait être supprimé alors qu'il appartient au législateur de régler dans le cadre du projet de loi n°7184 portant création de la Commission nationale pour la protection des données et la mise en œuvre du RGPD, la question de la portée du règlement européen précité de manière générale, et plus particulièrement à l'égard de la fonction publique.

En effet, il découle de l'article 6, paragraphe (3) du RGPD (lu à la lumière du considérant 45 du RGPD, de l'article 8, paragraphe 2 de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52, paragraphes (1) et (2) de la Charte des droits fondamentaux de l'Union européenne), que la création de traitements de données à caractère personnel par les ministres des ressorts respectifs portant sur la gestion de leur personnel doit être prévu au Grand-Duché de Luxembourg dans une base légale contenant des dispositions spécifiques. Or, le nouveau chapitre 10bis vise à créer les conditions nécessaires pour la création et la mise en œuvre de tels traitements.

Outre sa recommandation de maintenir ce nouveau chapitre 10bis, la Commission nationale a également fait connaître ses remarques relatives à l'intitulé du chapitre en question, sur les finalités des traitements concernés, sur la pertinence des données traitées, sur certaines

durées de conservation visées, sur le système de journalisation des accès aux données, sur les mesures de sécurité à mettre en œuvre, sur l'information et les droits des personnes concernées, et enfin sur les éventuels transferts de données en dehors de l'Union européenne.

2.2.11 Mise en œuvre du RGPD et modification de la loi sur la protection des données

En date du 28 décembre 2017, la CNPD a avisé le projet de loi n°7184 relatif à la création de la Commission nationale pour la protection des données et la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Dans son avis, la Commission nationale a rejoint les auteurs du projet de loi, en ce que le cadre législatif actuel relatif à la protection des données qui date de 1995 est dépassé par l'évolution rapide des technologies et la mondialisation qui ont créé de nouveaux enjeux pour la protection des données à caractère personnel, vu l'ampleur de la collecte et du partage de données à caractère personnel qui a augmenté de manière importante.

Il est vrai que ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union européenne, assorti d'une application rigoureuse des règles via des sanctions dissuasives en cas de violation constatée.

Une réforme de la protection des données sous Présidence luxembourgeoise du Conseil de l'Union européenne, a conduit à l'adoption du règlement (UE) 2016/679 (ci-après : « le RGPD »), tenant à harmoniser les règles nationales existantes et à moderniser la directive 1995/46/CE, ayant pour but de renforcer la protection des données à caractère personnel dans une société de plus en plus digitale en redonnant aux citoyens le contrôle des données qui les concernent, que celles-ci soient collectées et utilisées par les acteurs économiques privés ou par les acteurs publics.

Le RGPD sera d'application directe et déterminera la majorité des dispositions de fond désormais applicables en matière de protection des données.

Selon les auteurs du projet de loi n°7184, ce dernier, qui doit se lire conjointement avec le RGPD, se limite à compléter ce cadre européen par les dispositions nationales qui s'imposent, à savoir :

- la mise en place / l'adaptation de la loi organique de la Commission nationale pour la protection des données (actuellement contenue dans la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel qui devra être abrogée), afin d'octroyer à la CNPD les nouveaux pouvoirs qui lui seront nécessaires pour que celle-ci puisse exercer les missions qui lui sont dévolues par le nouveau règlement (UE) 2016/679 ;

- les dispositions spécifiques dans des domaines où le règlement (UE) 2016/679 prévoit qu'une législation nationale complémentaire peut être adoptée.

Les auteurs du projet de loi ont fait le choix d'abroger la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. La Commission nationale a approuvé ce choix qui permet une meilleure articulation entre les dispositions prises en exécution du RGPD et celles visant à transposer la directive

Les activités en 2017

2016/680[4]. D'autant plus que les auteurs du projet de loi visant à transposer la directive 2016/680 vont au-delà du champ d'application de la directive pour y intégrer les traitements de données personnelles effectués en matière de sécurité nationale et de désigner la future CNPD comme successeur de l'autorité de contrôle de l'article 17 de la loi de 2002, actuellement compétente en la matière.

Elle a constaté que de manière générale, le projet de loi avisé remplit globalement l'objectif principal qui lui est assigné, à savoir adapter le droit luxembourgeois au nouveau cadre européen pour en assurer la pleine effectivité pour les citoyens et les responsables de traitement et sous-traitants.

Selon la CNPD, le projet de loi donne corps au RGPD, qui constitue une avancée considérable pour la protection des données à caractère personnel dans l'Union européenne.

Sous réserve des clarifications demandées, omissions relevées ou compléments proposés dans le cadre de l'examen section par section de son avis, la Commission nationale a estimé que le projet de loi dote en effet le régulateur des pouvoirs nécessaires à l'exercice de ses missions.

2.2.12 Protection des données en matière pénale ainsi qu'en matière de sécurité nationale

Le 28 décembre 2017, la Commission nationale s'est prononcée au sujet du projet de loi n°7168 - projet de loi relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification de certaines lois.

Le projet de loi avisé est censé transposer la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Dans son avis, la CNPD a soulevé un manque de précision du texte pour ce qui est de la détermination des conditions sous lesquelles des limitations peuvent être apportées aux droits à l'information, d'accès et de rectification ou d'effacement.

[4] Directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

En matière de transfert de données dans des pays non membres de l'Union européenne, la CNPD a également soulevé que le texte ne précise pas quels sont les cas particuliers dans lesquels des transferts sont possibles en l'absence de décision d'adéquation ou de garanties appropriées. De même, elle a critiqué le fait que ne sont pas déterminés les cas particuliers dans lesquels des transferts sont possibles à destination de responsables du traitement qui ne sont pas des autorités compétentes en matière de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales. Quant aux sanctions administratives, elle a suggéré d'ajouter au texte des précisions permettant de dire quel article de la loi donne lieu, en cas de violation, à une amende administrative de quel montant.

En ce qui concerne les sanctions pénales, elle a suggéré d'ajouter une ou des sanctions pénales afin que puissent être sanctionnés certains abus qui, dans le passé, ont été sanctionnés pénalement notamment sur base des dispositions pénales de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.
Elle a encore pointé des insuffisances et manques de clarté pour ce qui est des dispositions relatives à la procédure de coopération entre le Parquet et la CNPD.

Parallèlement, elle a plaidé en faveur d'une extension du champ d'application de la coopération entre le Parquet et l'autorité de contrôle judiciaire à d'autres infractions et hypothèses que celles prévues dans le texte du projet de loi.

2.3 Information du public

2.3.1 Actions de sensibilisation du grand public

2.3.1.1 Nouvelle brochure « Vos obligations en matière de protection des données »

En octobre, la Commission nationale a publié une nouvelle brochure pour les responsables de traitements et leurs sous-traitants.

Le but de cette publication est d'informer les entreprises, organismes publics et associations sur leurs obligations en matière de protection des données et de servir comme guide dans leurs efforts de mise en conformité. La brochure tient déjà compte des changements introduits par le nouveau règlement général sur la protection des données qui responsabilisera davantage les acteur privés et publics.

La brochure peut être téléchargée sur le site Internet de la CNPD. Elle est disponible en français et en anglais.

2 Les activités en 2017

Discours de Madame Viviane Reding à la conférence „Verbraucherschutz an Dateschutz ginn Hand an Hand".

2.3.1.2 *Conférence « Verbraucherschutz an Dateschutz ginn Hand an Hand »*

Dans le cadre de la Cybersecurity Week, la CNPD, en collaboration avec Securitymadein.lu et l'Union Luxembourgeoise des Consommateurs (ULC), a organisé une conférence sur les droits des consommateurs dans le cadre du nouveau règlement général sur la protection des données.

Après le discours d'introduction de la Présidente de la CNPD, Madame Tine A. Larsen, sur les nouveaux défis auxquels doit faire face la CNPD dans les prochaines années, la Députée européenne, Madame Viviane Reding, a pris la parole. Dans son discours, elle a notamment parlé des obstacles qu'elle avait rencontré lors de la présentation de la réforme en matière de protection des données dans sa fonction de Vice-présidente de la Commission européenne en 2012 et de la réforme en cours de la directive « ePrivacy » en matière de communications électroniques.

Ces présentations ont été suivies par une table ronde avec des représentants des consommateurs, des commerces en ligne, de la protection des données et de la sécurité.

2.3.1.3 *11e journée de la protection des données*

Le Conseil de l'Europe, avec le soutien de la Commission européenne, a proclamé solennellement le 28 janvier de chaque année comme Journée de la protection des données.

En 2017, le 11e anniversaire de cette journée a été célébré. Le but de cette journée est de sensibiliser les citoyens européens à l'importance de la protection de leurs données personnelles et du respect de leurs libertés et droits fondamentaux, en particulier de leur vie privée.

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

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

Dans le cadre de cette journée, la CNPD a publié trois vidéos animées présentant les éléments importants auxquels les citoyens, entreprises, institutions publiques et associations doivent se préparer avec le nouveau règlement sur la protection des données.

2.3.1.4 Campagne « Big Data » de BEE SECURE

La CNPD était le partenaire principal de la campagne « Big Data » de BEE SECURE, lancée en 2017.

Le « Big Data » fait aujourd'hui déjà partie intégrante de notre quotidien. La campagne a essayé de répondre aux questions : Où sont collectées des données sur moi ? Par qui ? Pourquoi ? Et qu'est-ce que cela signifie pour moi et ma vie ?

L'objectif de la campagne était de montrer ce qui se passe « derrière les coulisses des données » et ce qui n'est pas forcément « visible » pour l'utilisateur.

Toutes les personnes intéressées, notamment les enfants et les jeunes, ainsi que les parents et les éducateurs, ont reçu des conseils précieux pour garder le contrôle de leurs données personnelles face aux développements autour du Big Data. Décider où s'inscrire, réfléchir aux informations personnelles que l'on souhaite partager et garder un œil sur les paramètres techniques étaient les points essentiels de la campagne.

Dans le cadre de la campagne, BEE SECURE a publié chaque mois des articles informatifs (dossiers de campagne) sur des sujets sélectionnés. Le thème a, en outre, été traité lors des formations (au total plus de 900) de BEE SECURE.

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 2017, le collège a accordé une trentaine d'interviews à des multiples organes de presse. Parmi les thèmes traités, citons le règlement général sur la protection des données, les vols de données et la cybersécurité, la surveillance sur le lieu de travail, l'Internet des objets, le « Big Data », l'utilisation de bodycams par la police, les droits des citoyens sur Internet, les compteurs intelligents ou encore les drones.

2.3.3 Outil de communication : le site Internet

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

Les responsables du traitement peuvent y accomplir les formalités prescrites par la loi. Afin de les guider de la manière la plus claire possible, la Commission nationale y met à disposition des rubriques et formulaires dédiés (ex : formulaire de demande

d'autorisation en matière de vidéosurveillance et de transferts de données vers des pays tiers, engagements formels de conformité, formulaires de notification, demande d'agrément pour les chargés de la protection des données, etc.).

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

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

En 2017, la CNPD a continué à alimenter le dossier thématique dédié au nouveau règlement européen sur la protection des données. Il contient des explications sur les nouveaux droits et obligations, des recommandations du groupe « Article 29 » et les présentations données lors des conférences et séances d'informations organisées par la CNPD à ce sujet. Un guide de préparation à l'attention des responsables de traitements a également été ajouté.

La Commission nationale a par ailleurs élaboré un nouveau formulaire en ligne destiné à faciliter l'introduction d'une plainte par le citoyen auprès de l'autorité de protection des données luxembourgeoise. Nombreuses personnes font appel aux services de la CNPD lorsqu'elles estiment qu'il y a eu une violation de la loi ou une entrave à l'exercice de leurs droits. L'utilisation de ce formulaire en ligne permettra un traitement accéléré de ces réclamations.

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.

2.3.4.1 Formation « Introduction à la protection des données »

Les 4, 5 et 6 juillet, la CNPD a organisé une formation d'introduction à la protection des données en langue française et anglaise.

Plus de 240 personnes ont participé à ce séminaire destiné à les familiariser avec les notions de base essentielles, les droits

Formation « Introduction à la protection des données » de la CNPD.

des personnes concernées, le rôle de la CNPD, les obligations du responsable du traitement et les nouveautés apportées par le règlement européen sur la protection des données.

Avec la digitalisation progressive de notre société, de plus en plus d'entreprises, administrations publiques, associations et autres professionnels peuvent être amenés à collecter, échanger et traiter des données à caractère personnel.

Or, les organismes qui utilisent ces données sont soumis à des règles strictes. Des traitements tels que la vidéosurveillance, la géolocalisation, la gestion des ressources humaines, la biométrie ou encore le transfert vers des pays tiers doivent se faire dans le respect de ces règles.

Afin de respecter les droits des citoyens et leurs propres obligations, il est important que les acteurs (intéressés, responsables de traitement, sous-traitants, …) comprennent et connaissent la matière de protection des données personnelles.

2.3.4.2 Cycle de conférences « Fit4DataProtection » de la Chambre de Commerce

La CNPD a participé au cycle de conférences « Fit4DataProtection : Règlement relatif à la protection des données (RGPD) : en route vers la mise en conformité » de la Chambre de Commerce du Luxembourg et son Enterprise Europe Network-Luxembourg.

Le 10 octobre, la Chambre de Commerce a accueilli dans ses locaux près de 320 participants pour la première session « Règlement relatif à la protection des données (RGPD): plus que quelques mois avant l'entrée en vigueur des nouvelles règles! ». Ce premier volet avait pour objectif de sensibiliser les entreprises sur la nécessité de se mettre en conformité avec le nouveau cadre européen et de les informer notamment sur les nouvelles obligations qui leur incombent à cet égard.

Mme Tine A. Larsen, Présidente de la CNPD, a présenté les notions élémentaires qui permettent de répondre aux questions telles que : Qu'est-ce qu'une donnée personnelle ? Qu'est-ce qu'un traitement de données à caractère personnel ? Et qui est concerné par cette nouvelle règlementation ? Elle a ensuite présenté les principaux changements de paradigme liés au contrôle a priori et au contrôle a posteriori, à savoir notamment le principe de protection des données dès la conception (ou « privacy by design ») et, d'autre part, les mesures permettant de garantir que, par défaut, seules les données qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées (« privacy by default »).

M. Christophe Buschmann, membre effectif de la CNPD, a animé un des ateliers, intitulé « Testez votre conformité avec le

nouvel outil de la CNPD, le « Compliance Support Tool ! ». L'objectif de cet outil est d'élaborer une solution innovante et intuitive pour permettre aux entreprises utilisatrices de vérifier le niveau de maturité de leurs organisations en matière de protection des données. L'outil permettra non seulement de gérer un registre de traitement, ainsi que tous les autres documents nécessaires à démontrer leur responsabilité, mais également de réaliser un suivi sur l'évolution du niveau de maturité de leurs organisations.

Pour la deuxième session le 27 novembre, la Chambre de Commerce a accueilli près de 220 participants.

A cette occasion, Mme Mathilde Stenersen du service juridique a rappelé qu'il était important que tous les décideurs et personnes clés de l'entreprise soient informés des changements liés au RGPD. Il a été recommandé de commencer d'ores et déjà à établir un inventaire de l'ensemble des traitements de données personnelles mis en œuvre, via notamment la tenue d'un registre des traitements. Une approche permettant de guider les entreprises dans cet exercice pourrait consister pour chaque traitement de données à se poser les questions suivantes : Qui ? Quoi ? Pourquoi ? Jusqu'à quand et comment ?

En poursuivant sur cette lancée, M. Christophe Buschmann a souligné que pour pouvoir garantir un haut niveau de protection des données personnelles, il était judicieux de mettre en place des procédures internes qui garantissent à tout moment la protection des données, en respectant entre autres les trois principes clé du RGPD à savoir la minimisation du traitement des données (en traitant uniquement ce qui est strictement nécessaire), la transparence et la visibilité. « De manière générale, mieux vaut avoir une approche proactive que réactive », a conclu le représentant de la CNPD lors de son intervention.

Dans le but de poursuivre ce travail de sensibilisation et d'accompagnement des entreprises dans le contexte du RGPD, mais aussi afin d'approfondir certaines questions clés, le cycle Fit4DataProtection se prolongera en 2018 avec l'organisation de sessions d'information complémentaires prévues au courant des mois de février et mai.

2.3.4.3 Workshops sur le nouveau règlement avec l'ABBL

La CNPD a participé à de nombreux workshops avec l'Association des Banques et Banquiers du Luxembourg.

Les thèmes de ces séminaires étaient :

- Practical implementation choices of the GDPR;

- The impact of the GDPR on retail banking;
- Defining what is personal data;
- The right to be forgotten and the blockchain;
- Hashing, blockchain and other technologies towards GDPR compliance;
- Consent by the data subject;
- Data portability: standards and formats;
- Data Protection Officer in financial services: job description;
- Privacy by design: technological and organisational approaches.

2.3.4.4 Autres formations et conférences

Le 26 janvier, la CNPD a organisé le panel « Data Protection Certification in the context of the GDPR's new accountability principle » avec l'Université du Luxembourg et l'Interdisciplinary Centre for Security, Reliability and Trust (SnT) lors de la Computers, Privacy and Data Protection (CPDP) conférence à Bruxelles. M. Alain Herrmann du service informatique et nouvelles technologies a participé au panel présidé par M. Mark D. Cole (Institute of European Media Law) et modéré par Mme Andra Giurgiu (SnT).

Le 14 février, M. Thierry Lallemang, membre effectif de la CNPD, a donné une présentation sur « Les dernières évolutions réglementaires auxquelles le DPO doit être attentif » à la conférence « GDPR&Data Protection : comment organiser la gouvernance interne ? » de CREO. Cette conférence a essayé de répondre aux questions liées à la désignation du DPO, la tenue d'un registre de traitement et l'organisation d'une analyse d'impact.

Le 16 février, M. Arnaud Habran du service juridique et M. Alain Herrmann du service informatique et nouvelles technologies ont donné une formation au Laboratoire National de Santé (LNS) à Dudelange. L'objectif était de sensibiliser les employés du LNS à la protection des données personnelles dans le cadre de leur travail.

Le 2 mars, Mme Tine A. Larsen, présidente de la CNPD, est intervenue à la 3e édition du Lëtzebuerger Juristendag « Intelligence artificielle et avenir des professions juridiques ». Mme Larsen a participé au panel « Liberté individuelles et protection des données – quel cadre législatif ? » avec M. Jeannot Nies (procureur général d'Etat adjoint), Mme Sylvie Allegrezza (professeur), Mme Marie-Jeanne Kappweiler (premier avocat général) et Mme Lotty Prussen (présidente de Chambre de la Cour d'Appel).

Les 25 et 26 avril, Mme Larsen a participé à la conférence « Law enforcement challenges in the online context », organisée par l'Université du Luxembourg. Elle est intervenue dans la table ronde « Obtaining Digital Evidence – Challenges for European Policy-Makers and Law Enforcement » avec Mme Vera Jourova (Commissaire européen), M. Koen Geens (Ministre de la Justice, Belgique) et Mme Daniela Buruiana (Eurojust).

Le 28 avril, environ 60 étudiants, académiques et professionnels ont participé à la troisième édition de l'Information Security Education Day (ISED). Les discussions se focalisaient sur l'impact du nouveau règlement sur la recherche. M. Alain Herrmann a participé à une table ronde avec M. Jean Goetzinger (CLUSIL), Jean-Michel Remiche (POST) et David Hagen (CSSF).

Le 17 mai, M. Christophe Buschmann a participé à la conférence « GDPR – take control of your risk », organisée par l'American Chamber of Commerce in Luxembourg.

Le 17 mai, Mme Edith Malhière du service juridique et M. Alain Herrmann ont participé à la 9e Journée Sécurité Santé de la CFL aux Rotondes à Luxembourg-Bonnevoie. Cette journée s'est adressée à tous les salariés de la CFL. La CNPD y était présente avec un stand sur lequel les visiteurs pouvaient répondre à

Les activités en 2017

un quiz sur la protection des données.

Le 27 septembre. M. Thierry Lallemang, a participé au symposium international sur la liberté d'information à Potsdam, organisé par l'autorité de protection des données de Brandenburg. Sa présentation a porté sur le whistleblowing au Luxembourg.

Le 27 septembre, M. Christophe Buschmann est intervenu à la conférence de l'Association des Banques et Banquiers, Luxembourg (ABBL) intitulée « Protection des données : GDPR, cybersécurité – un défi pour les entreprises ».

Le 28 septembre, M. Buschmann a participé à la table ronde « How to build, explore, analyse, secure, trust your data in the cloud era ? » dans le cadre des IT Days 2017 dont le thème était « Shaping your data ».

Le 5 octobre, la CNPD a participé à la journée de la protection des données auprès de l'administration étatique. Après l'allocution de M. Xavier Bettel, Premier Ministre, et le message du Contrôleur européen M. Giovanni Buttarelli, les différents orateurs ont fait des présentations susceptibles d'éclairer et de guider les acteurs publics dans la mise en oeuvre du nouveau cadre légal au sein de leurs services, départements et administrations respectives. Les représentants de l'autorité de protection des données sont intervenus sur les sujets suivants :

- « Guidance, enquêtes et sanctions, le nouveau rôle de l'autorité de supervision indépendante nationale, exercé en étroite liasion avec ses consoeurs européennes » par Mme Tine A. Larsen, Présidente de la CNPD.
- Les principes clés « traitement licite, transparent et loyal, finalités déterminées et légitimes, conservation limitée » par M. Thierry Lallemang, membre effectif de la CNPD.
- « Les droits des personnes concernées et leur facilitation. Comment gérer les demandes d'accès, d'effacement ou oppositions au traitement de leurs données exercées par les administrés ? » par M. Laurent Magnus, service juridique de la CNPD.
- « Protection et sécurité dès la conception et par défaut: documentation des mesures préventives et des incidents constatés, notification des violations de données à caractère personnel » par M. Christophe Buschmann, membre effectif de la CNPD.

Le 12 octobre, M. Christophe Buschmann est intervenu au Reg Tech Summit sur le thème « The changing landscape of regulations: GDPR – role and

approach of the national DPA ». M. Alain Herrmann a animé un workshop pour présenter le GDPR Compliance Support Tool ensemble avec le LIST et eProseedRTC.

Le 17 octobre, M. Buschmann a participé à une demi-journée de formation de l'Institut Luxembourgeois des Actuaires (ILAS) sur les enjeux et opportunités du RGPD pour les entreprises d'assurance et pour leur Data Protection Officer (DPO).

Le 20 octobre, M. Herrmann a donné une présentation générale sur le nouveau règlement sur la protection des données à l'occasion de la journée de l'accréditation de l'OLAS (Office Luxembourgeois d'Accréditation et de Surveillance).

Le 25 octobre, M. Christophe Buschmann et Mme Mathilde Stenersen (service juridique) ont fait une présentation sur l'impact et les opportunités de MIFID II dans le cadre du RGPD lors de la conférence d'IFE Benelux intitulée « Dernier appel pour MIFI II : plus aucun délai – Etes-vous prêt à relever le défi ? ».

Le 14 novembre, M. Buschmann a participé à la table ronde « From GDPR compliance to a European Data Market - a Long and Winding Road? » lors des Luxembourg Internet Days 2017.

Le 15 novembre, M. Magnus du service juridique et M. Buschmann ont donné une présentation à la conférence d'EFE intitulée « Assurance vie » : « Protection des données : quelles mesures prendre pour se mettre en conformité ? ».

Les 20 et 21 novembre, Mme Larsen a présidé une session lors de l'International Intelligence Oversight Forum 2017, organisé à Bruxelles par le Haut-commissariat aux Droits de l'Homme. Le thème de cet événement était « The Road Ahead – Dilemmas and Best Practices in Democratic Intelligence Oversight ».

Le 21 novembre, Mme Mathilde Stenersen et M. Georges Weiland du service juridique ont participé à « la Table d'Experts » concernant le nouveau règlement général sur la protection des données. L'objectif de cet événement, organisé par RH Expert, était d'informer les participants de la réforme et de sensibiliser les employeurs à leurs obligations au Luxembourg.

Le 28 novembre, M. Christophe Buschmann est intervenu au « ILA's Director's Day » (Institut luxembourgeois des administrateurs) avec une présentation sur la protection des données et la sécurité des données.

Le 28 novembre, M. Christophe Buschmann et Mme Mathilde Stenersen du service juridique ont donné une présentation à la conférence « Réforme de la protection des données » organisée par Academy and Finance. La présentation a porté sur le contrôle de l'application des règles et la notification des violations de données personnelles.

Le 8 décembre, M. Buschmann et M. Magnus ont donné une conférence à l'Association Professionnelle des Courtiers en Assurances au Luxembourg.

Tout au long de l'année, M. Thierry Lallemang a donné des formations sur la protection des données dans le cadre du cycle de formation pour les élus locaux, organisé par l'Institut national d'administration publique (INAP) et le Syvicol.

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

Les activités en 2017

tournent vers elle pour vérifier la conformité de leurs pratiques ou projets à l'égard des dispositions légales applicables.

La Commission nationale a participé à 281 réunions en 2017, soit 83 de plus qu'en 2016. Parmi ces réunions, 165 étaient avec les acteurs du secteur public et 116 avec ceux du secteur privé.

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

- Service des Communications et des Médias ;
- Ministère de la Justice ;
- Ministère des Finances ;
- Ministère des Affaires étrangères et européennes ;
- Ministère de l'Economie ;
- Ministère de la Fonction publique et de la Réforme administrative ;
- Ministère de l'Education nationale, de l'Enfance et de la Jeunesse ;
- Ministère du Développement durable et des Infrastructures – Département des Transports ;
- Commission de surveillance du secteur financier ;
- Commissariat aux assurances ;
- Institut luxembourgeois de régulation ;
- Centre des technologies de l'information de l'Etat (CTIE) ;
- Institut luxembourgeois de la normalisation (ILNAS) ;
- SECURITYMADEIN.LU ;
- BEE SECURE.

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

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

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

Dans le domaine de la santé, la Commission nationale a continué à participer activement aux travaux de l'agence « e-santé », notamment en ce qui concerne la mise en œuvre depuis 2014 d'un « Data Protection Impact Assessment » dans le cadre du dossier de soins partagés (DSP). Le collège de la CNPD a participé par ailleurs aux réunions du comité de pilotage de la Caisse Nationale de Santé (CNS) et a rencontré des représentants du Luxembourg Institute of Health (LIH) en 2017.

2.4.2 Demandes de renseignements

La Commission nationale a reçu 528 demandes de renseignement par écrit en 2017, soit 98 de plus qu'en 2016.

Presque un quart des requérants avaient des questions concernant la législation sur la protection des données et en particulier sur le nouveau règlement européen. Dans 17% des cas, il s'agissait de requêtes relatives aux formalités à accomplir pour mettre en œuvre un traitement de données. La CNPD a également reçu de nombreuses questions concernant la vidéosurveillance et les chargés de la protection des données.

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

2.5 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 techniques. 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 2017 à 67 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 » ;
  - « Border, Travel and Law Enforcement » ;
  - « Enforcement » ;
- du « Groupe de Berlin », dédié à la protection des données dans le secteur des communications électroniques ;
- du groupe de travail international sur l'Education au numérique ;
- de la conférence de printemps des commissaires européens à la protection des données à Chypre ;
- de la conférence internationale des commissaires à la protection des données et de la vie privée à Hong Kong ;
- du séminaire européen « Case Handling Workshop » à Manchester.

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

2.5.1 Le groupe « Article 29 »

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

2 Les activités en 2017

Le règlement général sur la protection des données et la directive en matière de police et justice vont modifier considérablement la structure actuelle et la manière de travailler du groupe « Article 29 ». Le 25 mai 2018, le Comité européen de la protection des données (« European data protection board ») remplacera le groupe « Article 29 » et deviendra un organe de l'UE qui possèdera la personnalité juridique. Il sera composé des autorités nationales et du Contrôleur européen à la protection des données.

Parmi les sujets traités par le groupe de travail en 2017, citons :

- la préparation au nouveau règlement européen en matière de protection des données ;
- l'« EU-U.S. Privacy Shield Framework » ;
- la refonte de la directive « e-Privacy ».

Les principaux documents de travail de 2017 du groupe de travail sont résumés ci-dessous et peuvent être téléchargés dans leur version complète sur Internet[5].

2.5.1.1 Préparation du règlement général sur la protection des données

En 2017, le groupe de travail de l'article 29 a travaillé sur les outils de mise en œuvre du règlement général sur la protection des données (RGPD).

Après analyse des contributions de la consultation publique, le G29 a adopté les versions définitives de ses lignes directrices à destination des professionnels sur

- le droit à la portabilité des données ;
- les délégués à la protection des données ;
- l'autorité chef de file ;
- les études d'impact sur la vie privée ;
- les notifications des violations de données à caractère personnel ;
- le profilage et
- les amendes administratives.

Le G29 a également poursuivi ses travaux concernant l'organisation et la structure du futur Comité Européen à la Protection des Données (CEPD), afin d'être prêt le 25 mai 2018.

A. Droit à la portabilité des données

L'article 20 du RGPD crée ce nouveau droit, qui est étroitement lié au droit d'accès aux données, tout en différant de celui-ci à de nombreux égards. Il confère

[5] http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

aux personnes concernées le droit de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement. Ce nouveau droit a pour objectif de responsabiliser les personnes concernées et de leur permettre de contrôler davantage les données à caractère personnel les concernant.

Dans la mesure où il permet la transmission directe des données à caractère personnel d'un responsable du traitement à un autre, le droit à la portabilité des données constitue également un instrument important qui facilitera la libre circulation des données à caractère personnel dans l'Union et qui stimulera la concurrence entre les responsables du traitement. Il facilitera le passage d'un prestataire de services à un autre et encouragera dès lors la mise au point de nouveaux services dans le contexte de la stratégie pour un marché unique numérique.

L'avis du G29 fournit des orientations sur la manière d'interpréter et de mettre en œuvre ce droit. Il a pour objet d'examiner la question du droit à la portabilité des données et son champ d'application. Il précise les conditions dans lesquelles ce nouveau droit s'applique compte tenu de la base juridique du traitement des données (soit le consentement de la personne concernée, soit la nécessité d'exécuter un contrat) et du fait que ce droit est limité aux données à caractère personnel fournies par la personne concernée. L'avis fournit également des exemples et des critères concrets pour expliquer les circonstances dans lesquelles ce droit s'applique.

B. Les délégués à la protection des données

Les délégués à la protection des données (DPD) seront au cœur du nouveau cadre juridique pour de nombreux organismes, afin de faciliter la conformité avec les dispositions du RGPD.

En vertu du RGPD, certains responsables du traitement et sous-traitants ont l'obligation de désigner un DPD. Cette obligation s'appliquera à l'ensemble des autorités et organismes publics (indépendamment de la nature des données qu'ils traitent), ainsi qu'à d'autres organismes dont les activités de base consistent en un suivi systématique à grande échelle de personnes ou en un traitement à grande échelle de catégories particulières de données à caractère personnel. Même lorsque le RGPD n'exige pas spécifiquement la désignation d'un DPD, les organismes peuvent parfois juger utile d'en désigner un sur une base volontaire. Le G29 encourage ces efforts déployés sur une base volontaire.

Les DPD agissent comme intermédiaires entre les acteurs concernés (par exemple, les autorités de contrôle, les personnes concernées et les entités économiques au sein d'un organisme). Le RGPD reconnaît le DPD en tant qu'acteur clé dans le nouveau système de gouvernance des données et établit les conditions relatives à sa désignation, à sa fonction et à ses missions.

L'objectif des lignes directrices du G29 est de préciser les dispositions pertinentes du RGPD afin d'aider les responsables du traitement et les sous-traitants à respecter la législation, mais aussi d'assister les DPD dans leur rôle. Les lignes directrices formulent également des recommandations en matière de bonnes pratiques, en s'appuyant sur l'expérience acquise dans certains États membres de l'Union. Le G29 assurera le suivi de la mise en œuvre des lignes directrices et pourrait les compléter avec des précisions supplémentaires si nécessaire.

C. La désignation de l'autorité chef de file

Il n'est pertinent de désigner une autorité de contrôle chef de file que lorsque le traitement transfrontalier de données à caractère personnel est effectué par un responsable du

traitement ou un sous-traitant. Le RGPD définit le « traitement transfrontalier » comme suit :

- un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ; ou

- un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres.

Cela signifie que, si une organisation a des établissements en France et en Roumanie, par exemple, et si le traitement de données à caractère personnel a lieu dans le cadre de l'activité de ceux-ci, ce traitement constituera un traitement transfrontalier. L'organisation peut aussi exercer une activité de traitement dans le seul cadre de son établissement situé en France. Toutefois, si cette activité affecte sensiblement, ou est susceptible d'affecter sensiblement, des personnes concernées en France et en Roumanie, elle sera également considérée comme un traitement transfrontalier.

L'avis du G29 sur la désignation de l'autorité chef de file a comme objectif

- de définir les notions clés comme « autorité chef de file », « traitement transfrontalier » ou « établissement principal » ;

- d'énumérer les étapes de la désignation de l'autorité chef de file et

- de répondre aux autres questions pertinentes concernant le rôle de l' « autorité de contrôle concernée », le traitement local et les sociétés établies en dehors de l'UE.

D. Analyse d'impact relative à la protection des données (AIPD)

Une AIPD est un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face. Les AIPD sont un outil important au regard du principe de responsabilité, compte tenu de leur utilité pour les responsables du traitement non seulement aux fins du respect des exigences

du RGPD, mais également en ce qui concerne leur capacité à démontrer que des mesures appropriées ont été prises pour assurer la conformité au règlement. Autrement dit, une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve.

Conformément à l'approche par les risques préconisée par le RGPD, il n'est pas obligatoire d'effectuer une AIPD pour chaque opération de traitement. Une AIPD n'est requise que lorsque le traitement est «susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques». Afin de garantir une interprétation cohérente des situations dans lesquelles une AIPD est obligatoire, les lignes directrices du G29 s'appliquent en premier lieu à éclaircir cet aspect et fournissent des critères pour les listes que les autorités de protection des données sont tenues d'adopter en vertu de l'article 35, paragraphe 4 du RGPD.

Les lignes directrices du G29 concernant l'AIPD s'efforcent également de promouvoir la mise en place :

- d'une liste commune à l'échelle de l'Union des opérations de traitement pour lesquelles une AIPD est obligatoire ;

- d'une liste commune à l'échelle de l'Union des opérations de traitement pour lesquelles une AIPD n'est pas nécessaire ;

- de critères communs concernant la méthodologie à suivre pour la réalisation d'une AIPD ;

- de critères communs pour la détermination des cas dans lesquels l'autorité de contrôle doit être consultée ;

- de recommandations basées sur l'expérience acquise dans les États membres de l'UE, dans la mesure du possible.

E. Notifications des violations de données

Une violation de données à caractère personnel est une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Les violations de données peuvent être catégorisées selon les trois principes bien connus de la sécurité de l'information :

- Violation de confidentialité : en cas de divulgation ou d'accès non autorisé ou accidentel à des données à caractère personnel ;

Les activités en 2017

- Violation de disponibilité : en cas de perte / destruction accidentelle ou non autorisée de données à caractère personnel ;

- Violation d'intégrité : en cas de modification accidentelle ou non autorisée de données à caractère personnel.

Dans ses lignes directrices, le G29 traite en détail la problématique des violations de données dans plusieurs chapitres :

- définition de la violation de données ;

- étude approfondie de l'article 33 (notification à l'autorité de régulation) ;

- étude approfondie de l'article 34 (communication à la personne concernée) ;

- évaluation du degré de risque de la violation ;

- documentation relative aux violations de données et rôle du DPD en la matière ;

- rappel des autres obligations de notification de faille de sécurité dans le cadre d'autres réglementations.

F. Décisions individuelles automatisées et profilage

Le RGPD définit le profilage comme « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire* » des éléments la concernant.

Le profilage et les décisions individuelles automatisées sont utilisés dans un nombre croissant de secteurs. La finance, la santé, l'assurance, le marketing et la publicité ne sont que quelques domaines dans lesquelles le profilage est utilisé pour faciliter la prise de décision.

Les avancées technologiques et les capacités de l'analyse des données, de l'intelligence artificielle et de l'apprentissage automatique ont facilité la création de profils et la prise de décisions automatisées susceptibles d'avoir un impact significatif sur les droits et libertés des individus.

Le profilage et la prise de décision automatisée peuvent être utiles pour les individus et les organisations lorsqu'ils permettent de gagner en efficacité ou d'économiser des ressources. Ces processus peuvent toutefois également poser des risques importants pour les droits et libertés des individus qui nécessitent des garanties appropriées. En effet, ces procédés peuvent être opaques et les individus ne savent pas toujours qu'ils sont profilés.

L'objectif des lignes directrices du G29 est de définir les termes de profilage et de décisions individuelles automatisées et d'expliquer les dispositions du RGPD les concernant. Le G29 aborde également la question des enfants et du profilage, ainsi que la relation entre le profilage et les analyses d'impact relative à la protection des données. Les annexes fournissent des recommandations sur les meilleures pratiques, en s'appuyant sur l'expérience acquise dans les États membres.

G. L'application et la fixation des amendes administratives

Les responsables du traitement et les sous-traitants sont plus que jamais chargés de veiller à la protection effective des données à caractère personnel des individus. Les autorités de contrôle sont investies de pouvoirs pour garantir que les principes du RGPD ainsi que les droits des personnes concernées sont respectés conformément à l'esprit et à la lettre du règlement.

L'application cohérente des règles relatives à la protection des données est essentielle à un régime harmonisé de protection des données. Les amendes administratives sont au cœur du nouveau régime d'application introduit par le règlement. Elles constituent un élément efficace de la panoplie dont les autorités de contrôle disposent pour faire respecter la réglementation.

Les lignes directrices du G29 concernant l'application et la fixation des amendes administratives visent à aider les autorités de contrôle, auxquelles elles sont destinées, à améliorer l'application du règlement et à mieux le faire respecter.

Le G29 a précisé que les lignes directrices ne sont pas exhaustives et ne fournissent pas d'explications sur les différences entre les systèmes administratifs, civils ou pénaux lors de l'imposition de sanctions administratives en général.

Afin d'assurer une approche cohérente de l'imposition des amendes administratives, qui reflète de manière adéquate l'ensemble des principes énoncés dans les lignes directrices, il a été convenu que le CEPD adopte une définition commune des critères d'évaluation visés à l'article 83, paragraphe 2, du règlement. Le CEPD et chaque autorité de contrôle conviennent donc d'utiliser les lignes directrices dans le cadre d'une approche commune.

2.5.1.2 Le Privacy Shield

En 2017, le G29 a adopté des FAQ (Questions fréquemment posées) concernant le Privacy Shield[6] à l'attention des individus et à l'attention des entreprises.

Dans les FAQ à l'attention des individus, le groupe de travail explique ce qu'est le Privacy Shield, comment les personnes concernées peuvent en bénéficier et la procédure à suivre pour déposer une plainte.

Quant aux FAQ à l'attention des entreprises, le G29 y répond aux questions suivantes :

- Le « Privacy Shield », de quoi s'agit-il ?
- Quelles entreprises des Etats-Unis sont éligibles pour le Privacy Shield ?
- Que faire avant de transférer des données à caractère personnel à une entreprise basée aux Etats-Unis qui est ou prétend être certifiée « Privacy Shield » ?
- Ou peut-on trouver de la guidance concernant l'enregistrement de filiales américaines d'entreprises européennes ?

Le G29 a par ailleurs décidé de la publication, sur son site et sur les sites des autorités de régulation nationales, d'un formulaire spécifique pour les individus pour leur permettre d'exercer, auprès du médiateur américain, leur droit d'accès aux données personnelles qui seraient traitées par les agences américaines de renseignement pour des motifs de sécurité nationale.

[6] Voir partie 2.1.2 pour plus d'informations à ce sujet

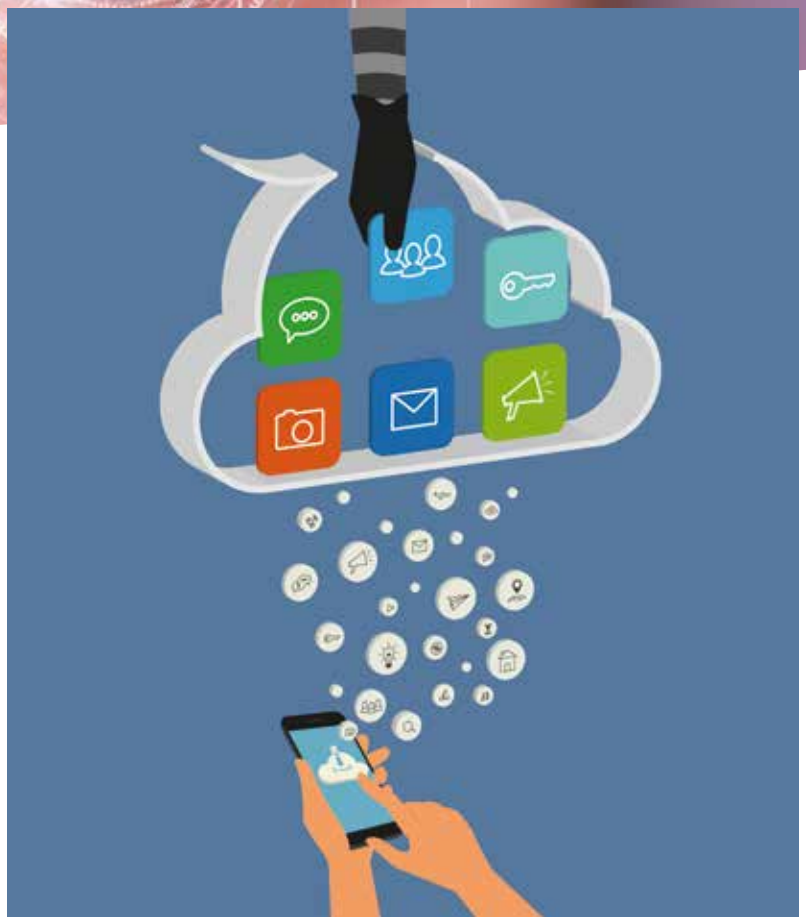
2.5.1.3 *Vie privée dans les communications électroniques*

Dans son avis, le groupe de travail a salué la proposition de règlement relatif au respect de la vie privée dans les communications électroniques présentée par la Commission européenne le 10 janvier 2017. Il s'est félicité que le choix se soit porté sur un règlement comme instrument réglementaire. Un règlement garantit en effet l'uniformité des règles dans toute l'Union européenne et apporte de la clarté aux autorités de contrôle, ainsi qu'aux organisations. Il permet en outre d'assurer la cohérence avec le règlement général sur la protection des données (RGPD). Cette cohérence est en outre appuyée par le choix de confier à l'autorité chargée de surveiller le respect du RGPD la responsabilité du contrôle de l'application des règles relatives au respect de la vie privée dans les communications électroniques.

En même temps, le choix (du maintien) d'un instrument juridique complémentaire est positif. La protection des communications confidentielles et de l'équipement terminal présente des caractéristiques particulières qui ne sont pas couvertes par le RGPD. Des dispositions complémentaires concernant ce type de services s'imposent donc pour garantir une protection adéquate du droit fondamental à la vie privée et à la confidentialité des communications, y compris la confidentialité de l'équipement terminal. À cet égard, le groupe de travail a soutenu fermement l'approche du principe retenu par le règlement proposé, consistant à prévoir des interdictions très vastes et des exceptions limitées et à appliquer la notion de consentement de manière ciblée.

Le groupe de travail s'est félicité de l'extension du champ d'application du règlement proposé pour y inclure les opérateurs offrant des services de communication par contournement (« over-the-top », OTT) ; il s'agit de services qui présentent des fonctions équivalentes aux moyens de communication plus traditionnels et peuvent donc avoir un effet similaire sur le respect de la vie privée et le droit à la confidentialité des communications des citoyens de l'UE. Le groupe a estimé qu'il était également positif que le règlement proposé couvre clairement le contenu et les métadonnées associées et reconnaisse que les métadonnées peuvent révéler des informations très sensibles.

Le groupe de travail a relevé néanmoins quatre sources de



préoccupation majeure.
En ce qui concerne le suivi de la localisation de l'équipement terminal, les conditions dans lesquelles l'analyse du contenu et des métadonnées est autorisée, les paramètres par défaut de l'équipement terminal et des logiciels et l'accès subordonné à l'acceptation du suivi (tracking walls), le règlement proposé abaisserait le niveau de protection octroyé par le RGPD. Dans son avis, le groupe de travail a formulé des suggestions spécifiques pour veiller à ce que le règlement relatif à la vie privée et aux communications électroniques garantisse le même niveau de protection, ou un niveau plus élevé, en adéquation avec le caractère sensible des données de communications (tant pour le contenu que pour les métadonnées).

2.5.2 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 2017 à Washington D.C. et à Paris, le groupe a adopté des documents de travail sur :

- les plateformes d'apprentissage en ligne ;
- les principes régissant la collecte de renseignement par les autorités publiques ;
- les questions de protection de la vie privée dans le cadre de la base de données WHOIS de l'ICANN et
- les méthodes de mise à jour des systèmes intégrés dans les objets connectés.

Ces documents peuvent être téléchargés dans leur intégralité (en anglais et en allemand) sur le site Internet du groupe de travail[7].

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

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

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

[7] https://www.datenschutz-berlin.de/working-paper.html

Les activités en 2017

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

1. Les données personnelles
2. Vie privée, libertés fondamentales et protection des données personnelles
3. Comprendre l'environnement numérique – au plan technique
4. Comprendre l'environnement numérique – au plan économique
5. Appréhender la régulation des données personnelles, connaître la loi
6. Appréhender la régulation des données personnelles : maîtriser l'usage des données personnelles
7. Maîtriser mes données : apprendre à exercer mes droits
8. Maîtriser mes données : apprendre à me protéger en ligne
9. Agir dans le monde numérique : devenir un citoyen numérique

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

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

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

L'autorité de protection des données de Chypre a organisé la « Spring conference » à Limassol les 27 et 28 avril 2017.

De nombreux experts européens s'étaient réunis pour cette conférence intitulée « New horizons » dont le sujet principal était les réformes en cours en matière de protection des données au niveau de l'Union européenne et du Conseil de l'Europe.

La présidente de l'autorité chypriote, Madame Irene

Participants à la conférence de printemps des autorités européennes à la protection des données.

Loizidou Nikolaidou, a tenu le discours d'ouverture, suivi de sessions sur les sujets suivants :

- Panel 1 : « The dawn of new data protection regimes »
- Panel 2 : « Raising awareness – bringing DPAs closer to people and enterprises »
- Panel 3 : « Transparency and accountability in the Cloud »
- Panel 4 : « LEAs access to data – large scale systems, interoperability and transborder data flows »
- Panel 5 : « Genomes and DNA databases – challenges for privacy »
- Panel 6 : « Expanding our horizons – the Spring conference in the new regime »

Des résolutions sur la modernisation de la Convention 108 du Conseil de l'Europe et sur les règles et procédures concernant la conférence de printemps ont été adoptées.

2.5.5 Conférence internationale des commissaires de la protection des données

L'autorité de protection des données de Hong Kong a organisé la 39ème Conférence internationale des commissaires de la protection des données et de la vie privée du 25 au 29 septembre 2017.

La conférence internationale a eu lieu pour la première fois en 1979. Elle est constituée d'une séance ouverte à tous les experts dans le domaine de la protection des données, d'une session fermée réservée aux autorités de protection des données ainsi que de plusieurs événements parallèles organisés par les organisations internationales et les ONG.

Lors de la première journée, les commissaires ont eu des discussions approfondies sur les échanges d'informations entre les gouvernements en mettant un accent particulier sur la protection des données sensibles, la prévention de la discrimination et la gestion des risques.

Pendant la deuxième journée, le Rapporteur spécial des Nations Unies sur le droit à la vie privée, Joseph Cannataci, a présenté les progrès réalisés dans son mandat et ses objectifs pour l'année à venir.

Après cette intervention, les groupes de travail en matière

d'éducation au numérique, de « data protection metrics », d'action humanitaire, de télécommunications et de coopération en matière d'application des lois ont fourni une mise à jour sur leurs activités.

Des résolutions relatives aux thèmes suivants ont été adoptées :

- la protection des données dans les véhicules connectés et automatisés ;
- la collaboration entre les autorités de protection des données et de protection des consommateurs pour une meilleure protection des citoyens et consommateurs dans l'économie numérique ;
- l'exploration des possibilités futures en matière de coopération transfrontière dans l'application des lois.

Les prochaines conférences internationales auront lieu en Belgique et en Bulgarie en octobre 2018 et en Albanie en 2019.

2.5.6 Le séminaire européen « Case Handling Workshop »

L'autorité de protection des données du Royaume-Uni a organisé le séminaire européen « Case Handling Workshop » à Manchester les 20 et 21 juin 2017.

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.

Les thèmes suivants ont été abordés au cours de 10 sessions:

- la portabilité des données ;
- la coopération entre les autorités dans le cadre du nouveau règlement sur la protection des données (RGPD) ;
- les notifications des violations de données ;
- la gestion des plaintes dans le cadre du RGPD ;
- l'impact des nouvelles technologies sur la protection de la vie privée des individus ;
- la protection des données dans le secteur de la police et de la justice ;
- la protection des données dans le domaine de la santé.

3 Les temps forts de 2017

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 Séances d'information sur le nouveau règlement général sur la protection des données

Les 18 et 19 octobre 2017, la CNPD a organisé deux sessions d'information (en français et en anglais) sur le nouveau règlement général sur la protection des données dans la Halle des poches à fonte à Esch/Belval.

Presque 500 représentants d'entreprises, d'administrations publiques, d'associations et d'indépendants ont été sensibilisés lors de ces deux journées.

Le but était d'informer les acteurs privés et publics sur les nouveautés apportées par le RGPD afin qu'ils puissent évaluer les conséquences que le nouveau cadre légal aurait sur leur organisation et se préparer à son arrivée.

Les thèmes suivants ont été traitées :

- La conformité au nouveau règlement : comment se préparer ?
- Le rôle du futur délégué à la protection des données
- Le nouveau droit à la portabilité des données
- Le consentement « renforcé »
- Les nouvelles dispositions sur le profilage
- Les violations de données à caractère personnel
- Les analyses d'impact sur la protection des données
- Le contrôle de la conformité par la CNPD
- Les codes de conduite et certifications
- Démonstration du « Compliance Support Tool » de la CNPD et du LIST

Discours de Tine A. Larsen, présidente de la CNPD, à la séance d'information sur le nouveau règlement général sur la protection des données.

Séance d'information sur le nouveau règlement général sur la protection des données dans la Halle des poches à fonte à Esch/Belval.

3.2 GDPR Compliance Support Tool : lancement de l'outil d'aide à la conformité au nouveau régime de protection des données

Se préparer au 25 mai 2018

L'application, à partir du 25 mai 2018, du nouveau régime relatif à la protection des données confronte d'ores et déjà tous les acteurs à l'obligation de s'y conformer le plus rapidement possible.

Afin de les aider dans leur tâche d'intégration des dispositions du règlement général sur la protection des données dans leur politique interne, la CNPD a développé, avec le soutien de Digital Luxembourg, ensemble avec le Luxembourg Institute of Science and Technology (LIST), un « GDPR Compliance Support Tool ».

Cet outil contribue à l'objectif du Luxembourg de digitaliser et de simplifier les procédures, notamment celles de mise en conformité avec le cadre réglementaire en vigueur et à venir.

Un outil permettant d'évaluer la conformité d'une organisation

L'objectif de l'outil est d'offrir une solution innovante et intuitive aux utilisateurs permettant de vérifier le niveau de maturité de leurs organisations en matière de protection des données. L'outil permettra aux utilisateurs non seulement de gérer un registre de traitement, ainsi que tous les autres documents nécessaires à démontrer leur responsabilité, mais également de réaliser un suivi sur l'évolution du niveau de maturité de leurs organisations. L'outil contient une base de données exhaustive et détaillée avec plus de 350 critères d'exigences réglementaires. Le « GDPR Compliance Support Tool » sera mis à disposition des organisations gratuitement et son contenu sera mis à jour régulièrement par la suite.

Evolution de l'outil

La première phase d'élaboration du « GDPR Compliance Support Tool » consistait dans le développement d'une version de test. Afin d'être proche des besoins des différents secteurs, cette première version a été élaborée conjointement avec des acteurs actifs dans les domaines de la santé et de la finance.

La deuxième phase consistait en une utilisation en conditions réelles de cette première version de l'outil par 28 sociétés. Cette phase de test a été conduite pour confronter l'outil le plus tôt possible aux réalités des organisations et procéder aux ajustements nécessaires pour en assurer la pertinence.

Pour la phase d'industrialisation de l'outil, eProseedRTC a été choisie comme partenaire.

Le « GDPR Compliance Support Tool » est disponible à l'adresse suivante : https://cst.cnpd.lu.

Représentants de la CNPD, du LIST, d'eProseed et de Digital Luxembourg.

4 Perspectives

Le cadre législatif actuel qui date de 1995 est dépassé par l'évolution rapide des technologies et la mondialisation qui ont créé de nouveaux enjeux pour la protection des données à caractère personnel, vu l'ampleur de la collecte et du partage de données à caractère personnel qui a augmenté de manière importante.

La mise en œuvre du « paquet sur la protection des données »

Le RGPD ou règlement (UE) 2016/679, tenant à harmoniser les règles nationales existantes et à moderniser l'ancienne directive 1995/46/CE, a pour but de renforcer la protection des données à caractère personnel dans une société de plus en plus digitale en redonnant aux citoyens le contrôle des données qui les concernent, que celles-ci soient collectées et utilisées par les acteurs économiques privés ou par les acteurs du service public.

Deux autres instruments européens s'ajoutent au RGPD pour constituer le « paquet sur la protection des données », réformant en profondeur le droit de la protection des données au niveau de l'Union européenne. Ainsi, le Parlement européen et le Conseil ont adopté parallèlement en date du 27 avril 2016 :

- la directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil et

- la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

Au niveau national, l'implémentation de ces différentes mesures est en cours avec plusieurs projets de loi qui ont été déposés à la Chambre des députés en 2017 dont :

- le projet de loi n°7184 portant création de la CNPD et relatif à la mise en œuvre du RGPD ;

- le projet de loi n°7168 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et

- le projet de loi n°7151 relatif au traitement des données des dossiers passagers dans le

cadre de la prévention et de la répression du terrorisme et de la criminalité grave.

Une évolution des missions de la CNPD

Le RGPD uniformise et simplifie les règles auxquelles les organismes traitant des données personnelles sont soumises en renforçant les garanties d'ores et déjà offertes par la directive 95/46 (CE). Il prévoit en particulier la réduction des formalités préalables pour la mise en œuvre des traitements comportant moins de risques, avec le passage d'un système de contrôle a priori par la CNPD, par le biais de notifications et d'autorisations, à un contrôle *a posteriori* plus adapté aux réalités du terrain.

Un tel changement de paradigme nécessite une évolution des missions et pouvoirs de l'ensemble des autorités de protection des données de l'Union européenne, dont la CNPD.

Ainsi, la CNPD voit ses pouvoirs de contrôle et de sanctions renforcés avec la possibilité d'infliger des amendes pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial de l'organisme concerné. Des amendes lourdes pour des violations sévères reflètent l'importance de la protection des données au 21e siècle. Il est toutefois alarmiste de suggérer que la CNPD va marquer des premiers exemples avec des institutions pour des violations mineures ou que les amendes maximales deviendront la règle.

Le RGPD exige que les sanctions soient « effectives, proportionnées et dissuasives » - ceci implique que la taille de l'entreprise, la gravité des faits, l'ampleur de la violation, des dommages, du nombre de personnes touchées, ainsi que le niveau de risque et les moyens d'une entreprise pour se mettre en conformité soient pris en compte. Il est clair que l'autorité de contrôle sera moins tolérante avec les grands organismes disposant d'amples ressources qu'avec des petites entreprises avec des moyens plus limités.

Dans ce nouvel environnement juridique, la CNPD devra notamment guider, conseiller et éduquer encore plus les acteurs, notamment les petites et moyennes entreprises qui doivent s'adapter aux nouvelles obligations en matière de protection des données.

La CNPD continuera son approche générale qui consiste à assurer un équilibre entre guidance et contrôle. Elle cherche aussi à sensibiliser au fait que les contrôles n'ont pas comme objectif unique de sanctionner. Ils devront également lui permettre d'identifier les zones d'erreur récurrentes sur base desquelles elle pourra élaborer une guidance qui aidera les entreprises à s'améliorer.

Afin de faire face à toutes ces missions, la CNPD est en train de recruter du personnel additionnel. L'autorité de protection des données sera prévisiblement à 35 personnes à la fin de l'année 2018 et à 49 en 2020.

Un renforcement de la coopération au niveau européen

Les autorités de contrôle européennes devront également coopérer étroitement dans le cadre du « guichet unique » instauré par le RGPD, un mécanisme de coopération renforcé entre les autorités de protection des données qui devront dorénavant adopter des décisions communes lorsque les traitements de données seront transnationaux, ainsi que pour parvenir à une position commune unique pour toute l'Union européenne au sein du nouveau Comité européen pour la protection des données (CEPD ou EDPB pour « European Data Protection Board »).

L'EDPB sera un organe de l'Union européenne possédant la personnalité juridique et aura des pouvoir plus étendus que le groupe de travail « Article 29 ». Le RGPD lui confie notamment la mission d'adopter des décisions contraignantes envers les autorités de contrôle nationales afin de garantir une application

4 Perspectives

cohérente de ses dispositions. Les décisions prises par cet organe constitueront le gage d'une plus grande sécurité juridique pour les responsables de traitement et d'une application uniforme de la législation européenne en matière de protection des données.

L'EDPB peut aussi adopter des documents d'orientations générales afin de clarifier les dispositions des actes législatifs européens en matière de protection des données et, de cette manière, fournir aux acteurs concernés une interprétation cohérente de leurs droits et obligations.

Le Comité peut également :

- conseiller la Commission européenne sur toute question liée à la protection des données à caractère personnel et sur les nouvelles propositions de législation dans l'Union européenne ;
- adopter des conclusions relatives à la cohérence sur des questions de protection de données transfrontalières ; et
- promouvoir la coopération, ainsi que l'échange efficace d'informations et de bonnes pratiques entre les autorités de contrôle nationales.

5 Ressources, structures et fonctionnement

5.1 Rapport de gestion relatif aux comptes de l'exercice 2017

Pour la CNPD l'année 2017 a été laborieuse et marquée par l'approche de la date butoir du 25 mai 2018, date de l'entrée en application du nouveau règlement européen pour la protection des données (RGPD), qui marquera pour l'avenir sa façon de fonctionner.

Déjà pour l'année 2017, le budget de la CNPD laissait percevoir des changements alors que la dotation autorisée de 2 386 726 € était de l'ordre d'environ 16% supérieure à celle autorisée en 2016, qui était de 2 050 922 €. Les fonds supplémentaires étaient essentiellement destinés au recrutement d'effectifs supplémentaires et à couvrir les frais de fonctionnement occasionnés par une commission en expansion.

Le total des frais de fonctionnement de l'établissement public au cours de l'exercice 2017 s'élevait à 2 531 584,32 € ce qui constitue une augmentation de 17% par rapport à l'exercice précédent qui s'élevait à 2 162 430,24 €. Le total des frais de fonctionnement ne dépasse donc que légèrement le montant des prévisions budgétaires originaires estimées à 2 517 926 €. Ce chiffre dépasse certes celui de la dotation autorisée, mais est repris par les recettes sur les redevances qui servent essentiellement à payer les traitements des collaborateurs de la CNPD bien qu'elles ne les couvrent nullement entièrement et qu'elles ont vocation à disparaître avec la réforme qui abolira les formalités préalables et par conséquent les redevances.

Ce sont essentiellement les charges relatives au personnel permanent et temporaire qui ont augmenté sensiblement, pour atteindre 2 257 695,91€ en 2017 comparés à 2 086 622 € en 2016. Les dépenses réelles dépassaient ainsi les prévisions budgétaires estimées à 2 055 000 € d'environ 10%.

Ainsi, la CNPD a engagé en début d'année une juriste employée de l'Etat et une deuxième en automne, suite au départ d'un collaborateur. De même, un chargé d'études informaticien a rejoint les effectifs de la CNPD. Par ailleurs, deux experts externes associés aux travaux de la CNPD en début d'année, ont été intégrés aux effectifs du personnel de la CNPD en cours d'année dont une juriste et un chargé d'études informaticien. Il ne va pas sans dire que la CNPD s'est

également doté d'un nouveau commissaire-informaticien avec effet au 1er janvier 2017 alors que le précédent avait démissionné avec effet au 1er septembre 2016. En fin de compte, la CNPD a donc terminé l'année avec un effectif comportant quatre postes à temps plein supplémentaires, tous de la carrière de l'employé public. La dépense pour ces quatre postes a été en partie compensée par une dotation supplémentaire de 85 321 € pour deux postes pour employés publics de la carrière A1 pour chaque fois 6 mois. Reste à mentionner, qu'un fonctionnaire de la carrière B1 s'était vu accorder un congé pour travail à mi-temps pour des raisons médicales dont la CNPD a dû supporter les coûts. Pour pouvoir assurer le bon fonctionnement de son service, la CNPD s'est vu contrainte de recourir aux services d'un employé public de la carrière B1. Une dotation supplémentaire d'une hauteur de 27 255 € avait été autorisée pour couvrir 5 mois de ce congé en 2017, alors que la CNPD ne peut pas profiter de la provision globale de l'Etat pour remplacements.

Concernant les autres charges, les frais d'honoraires, qui se composent essentiellement des frais de la fiduciaire qui tient la comptabilité et établit le bilan de l'établissement public, sont restés largement en-dessous des prévisions avec 9 479,33 €. En effet, la CNPD craignant l'affluence d'affaires en justice avait prévu une provision substantielle sur cet article. Après une augmentation au double de la moyenne en 2016 suite au recours à des avocats externes, les frais sont donc retournés au niveau de 2015.

Le montant des charges locatives pour le bâtiment administratif à Belval s'élevait à 12 262,33 € montant légèrement inférieur au montant de l'année précédente qui s'élevait à 13 876,16 €, et ce en raison d'épargnes faites au niveau de la consommation d'énergie et de frais de nettoyage.

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

Pour ce qui est des équipements et fournitures de bureau, les dépenses ont augmenté à nouveau de presque 100% par rapport à 2016, année pendant laquelle les frais avaient diminué par rapport à 2015, année pendant laquelle la CNPD avait renouvelé une partie de ses équipements surannés (ordinateurs, écrans, imprimantes, serveurs et back-up). Avec 34 978,61 € elles sont certes supérieures aux coûts de 25 809,44 € de 2016, mais nettement inférieures à ceux de 56 789,63 € en 2015.

Les frais de déplacement et de séjour à l'étranger se chiffraient à 29 255,66 € ce qui constitue une nette baisse par rapport à l'année précédente pendant laquelle les coûts s'élevaient à 39 529,20 €. Or, les dépenses restent inférieures aux prévisions budgétaires. La différence s'explique par le fait que bien que le nombre de voyages de service augmente, les collaborateurs préfèrent commencer leur séjour tôt le matin que la veille et qu'un nombre de réunions a été réduit dans la durée. Le chiffre n'a toutefois aucunement tendance à diminuer dans le futur. Au contraire, les engagements de la CNPD à l'étranger ne feront qu'augmenter à l'avenir alors que non seulement le nombre de groupes de travail que la CNPD devra couvrir à l'étranger a tendance à augmenter. La cadence des réunions du groupe de l'article 29 et prochainement du Comité européen pour la protection des données va augmenter aussi. 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

5 Ressources, structures et fonctionnement

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 frais de déplacement et de séjour pour les agents en formation externe sont également inclus dans cette somme.

Les frais de formation externe hors frais de déplacement et de séjour pour le personnel ont fortement augmenté pour atteindre 9 282,43 € en 2017, comparés à 3 440,80 € en 2016, ce qui constitue le triple des prévisions budgétaires sur cette position. Ces dépenses s'expliquent d'une part par des cours de langue luxembourgeoise organisés pour les nouveaux collaborateurs francophones en interne, et d'autre part par la formation spécialisée en matière de protection des données personnelles. Il est en effet à l'heure actuelle très difficile de trouver des collaborateurs qui maîtrisent tant les trois langues officielles du pays, que la matière de la protection des données personnelles. Afin de pouvoir s'associer du nouveau personnel et avancer dans les préparations pour l'entrée en vigueur du RGPD, il y a lieu de se décider pour une partie des compétences et enseigner l'autre. Les frais de formation vont évoluer davantage au cours des années à venir, étant donné que la CNPD apporte beaucoup d'attention à la formation de base, continue et linguistique de ses collaborateurs.

Les dépenses pour l'information du public et la communication s'élevaient à 23 846,85 € en 2017. Bien que ce montant dépassait de plus de 10 000 € celui de l'année précédente avec 13 589,30 €, il reste à nouveau en-dessous des prévisions budgétaires de 40 000 €, alors que la CNPD n'a pas réussi de finir une partie de ses nouvelles brochures de sensibilisation avant la fin de l'année. Celles-ci figureront donc sur le budget de l'année 2018, année qui sera très chargée en termes de sensibilisation en vue de l'entrée en application des nouvelles règles en matière de protection des données personnelles.

En 2017 à nouveau, les dépenses pour la maintenance des systèmes et réseaux informatiques ont dépassé les prévisions du triple. Les dépenses s'élevaient à 76 657,81 € par rapport à 28 000 € prévues dans les prévisions budgétaires. Cette augmentation s'explique par deux facteurs. D'un côté, la CNPD, en prévision de l'adoption d'une nouvelle structure de contrôle a posteriori sous le RGPD et par conséquent des nouvelles procédures de travail, a procédé à la modélisation de

ses futures structures et processus internes et la mise en place subséquente de nouveaux outils de travail internes en vue de la digitalisation de la CNPD. D'autre part, elle a développé un outil d'appréciation du niveau de maturité des responsables de traitement en termes de protection des données personnelles ensemble avec le LIST. Les dépenses supplémentaires sur cette position proviennent essentiellement du développement des applications informatiques de part et d'autre. Alors qu'il a été décidé de basculer l'informatique entière de la CNPD vers le CTIE, le renouvellement des équipements informatiques a été effectué par le CTIE et ne figurera au budget qu'en 2018.

Les amortissements comptabilisés en 2017 atteignaient un montant total de 6 888,22 €, c'est-à-dire une somme équivalente à deux fois le montant de l'année précédente qui était de 3 093,55 €. Cette augmentation est essentiellement due à l'acquisition de nouveau mobilier destiné à accueillir les nouveaux membres du personnel de la CNPD en 2018.

Recettes

Le montant des redevances perçues en application des articles 37 paragraphe (4), 13 paragraphe (3) et 14 paragraphe (4) de la loi s'élevait à 178 318,51 € comparé à 158 075 € en 2016. Ce surplus constitue une augmentation de 12,80% par rapport à l'année précédente et dépasse les prévisions budgétaires de 33,84%. Par rapport à l'année précédente, les prévisions budgétaires avaient été ramenées au niveau de ce à quoi la CNPD pouvait légitimement s'attendre comparé aux recettes des années précédentes. Or, en prévision de l'entrée en application du RGPD, la CNPD témoigne un afflux des formalités préalables et par conséquent, d'une augmentation correspondante des recettes, qui ont toutefois vocation à disparaître à partir de mai 2018.

Aucune recette de produits financiers (intérêts créditeurs) n'a pu être enregistrée pour l'année 2017.

Résultat d'exploitation

Compte tenu de la dotation annuelle de 2 499 338 €, dont la Commission nationale a bénéficié en 2017 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 146 082,19 € au 31 décembre 2017.

Esch-sur-Alzette, le 25 avril 2018

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

5 Ressources, structures et fonctionnement

5.2 Personnel et services

Collège
Tine A. LARSEN,
présidente
Thierry LALLEMANG,
membre effectif
Christophe BUSCHMANN,
membre effectif

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

Secrétariat, administration générale et finances
Serge FERBER,
employé de l'Etat (†)
Tessy PATER,
rédacteur
Anna MAGI,
employée de l'Etat
Pol GOERGEN,
employé

Service communication et documentation
Tom KAYSER,
attaché

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

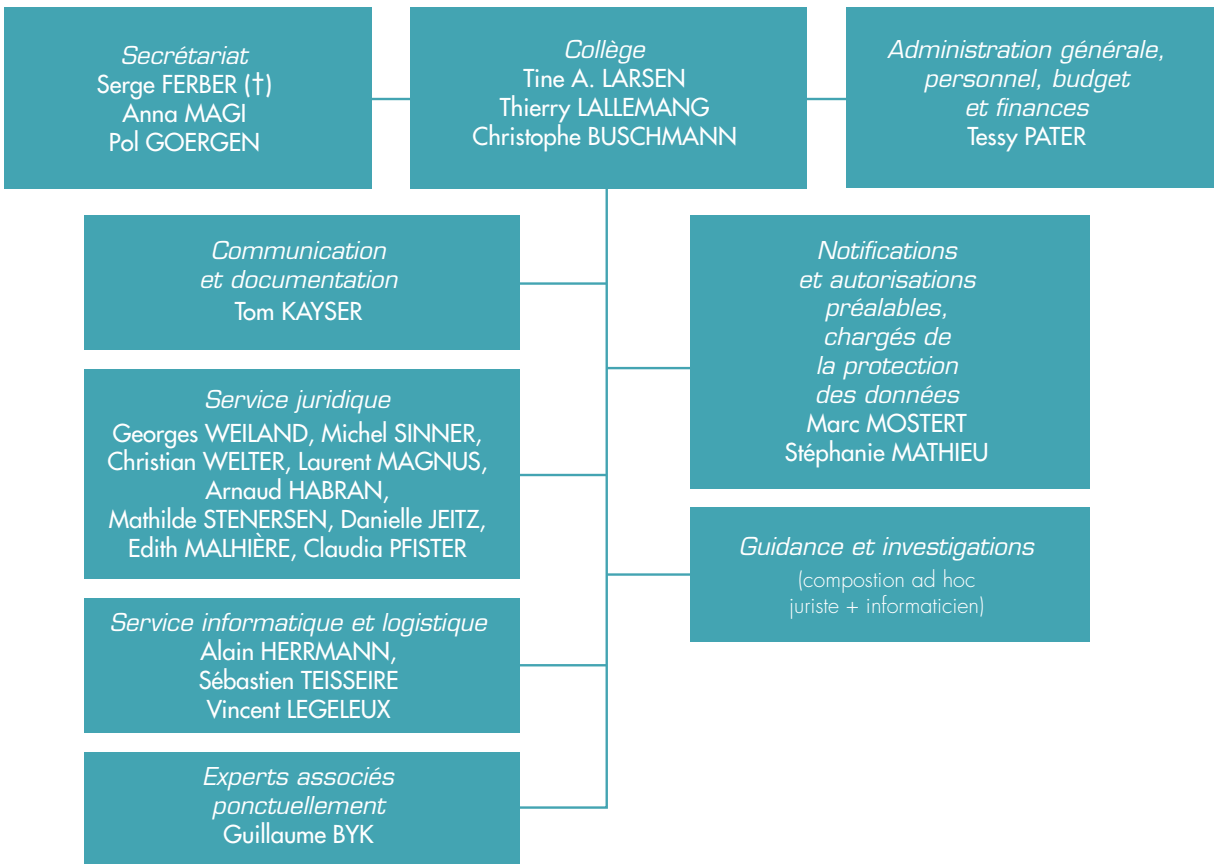
Tenue du registre public et prise en charge administrative des notifications et demandes d'autorisation
Marc MOSTERT,
rédacteur
Stéphanie MATHIEU,
rédactrice

Service informatique et de la logistique
Alain HERRMANN,
chargé d'études
Vincent LEGELEUX,
chargé d'études
Sébastien TEISSEIRE,
employé de l'Etat

Expert associé ponctuellement
Guillaume BYK,
support Task force Réforme

De gauche à droite : Marc Mostert, Dani Jeitz, Claudia Pfister, Guillaume Byk, Georges Weiland, Edith Malhière, Mickaël Tome, Laurent Magnus, Tom Kayser, Thierry Lallemang, Alain Herrmann, Tine A. Larsen, Sébastien Teisseire, Christophe Buschmann, Christian Welter, Vincent Legeleux, Michel Sinner, Mathilde Stenersen, Stéphanie Mathieu, Arnaud Habran, Anna Magi et Tessy Pater.

5.3 Organigramme de la Commission nationale



6 La Commission nationale en chiffres

Formalités préalables

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	
a) Notifications											TOTAL 2003-2017
Notifications ordinaires	385	345	295	355	437	421	564	705	975	977	10.465
Notifications simplifiées	-	-	-	-	-	-	-	-	-	-	3.797
Engagements de conformité	942	227	15	46	149	651	45	19	28	64	2.186
(Total a 2003-2017)	1.327	572	310	401	586	1.072	609	724	1.003	1.041	16.448
b) Autorisations préalables											TOTAL 2003-2017
Demandes d'autorisation	606	542	607	604	706	833	914	969	1.338	1.030	10.324
Engagements de conformité	220	70	92	49	70	149	85	148	111	132	2.045
(Total b 2003-2017)	826	612	699	653	776	982	999	1.117	1.449	1.162	12.369
(Total général a + b 2003-2017)	2.153	1.184	1.009	1.054	1.362	2.054	1.608	1.841	2.452	2.203	28.817
Déclarants (responsables ayant accompli des formalités)	4.357	4.772	5.110	5.399	5.821	6.559	6.993	7.472	8.005	8.786	

Demandes de renseignements par écrit

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
(Total a 2003-2017)	138	138	213	173	273	274	416	340	430	528

Plaintes

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Plaintes et demandes de vérification de licéité	63	133	145	115	133	177	207	217	185	200

Séances de délibération

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
	40	37	38	35	27	31	20	39	32	38

Participations aux groupes de travail sur le plan européen

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
	22	32	40	37	43	39	40	47	61	67

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

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Secteur public	52	54	56	69	71	102	92	146	125	116
Secteur privé	44	52	54	71	61	75	77	106	73	165
(Total)	**96**	**106**	**110**	**140**	**132**	**177**	**169**	**252**	**198**	**281**

Séances d'information, conférences, exposés

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
	11	23	21	15	10	18	22	15	44	40

7 Annexes

Avis relatif à l'avant-projet de loi portant création d'un Institut public d'aide à l'enfance et à la jeunesse

Délibération n°214/2017
du 10 mars 2017

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 : « 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 30 septembre 2016, le Ministère de l'Education nationale, de l'Enfance et de la Jeunesse a invité la Commission nationale à aviser l'avant-projet de loi portant création d'un Institut public d'aide à l'enfance et à la jeunesse.

Cet avant-projet de loi a pour objet d'abroger la loi du 18 avril 2004 portant organisation des maisons d'Enfants de l'Etat et de créer un Institut public d'aide à l'enfance et à la jeunesse (ci-après : « l'Institut ») à dimensions éducative, sociale, soignante et thérapeutique. Cette nouvelle structure a pour mission d'offrir un encadrement spécifique ciblé aux besoins des enfants et des jeunes âgés de 0 à 27 ans.

La Commission nationale limite ses observations aux questions traitant des aspects portant sur la protection des données, soulevées plus particulièrement par l'article 15 de l'avant-projet de loi.

Cet article 15 prévoit la création d'un « fichier individuel des personnes accueillies par l'Institut », dans lequel figurent les données personnelles nécessaires aux fins de documenter l'hébergement et l'encadrement des personnes accueillies par les différents départements de l'Institut et à des fins d'études historiques et statistiques.

De manière générale, la Commission nationale accueille avec satisfaction le fait que la rédaction actuelle de l'article 15 de l'avant-projet de loi sous objet détaille le fichier de données à caractère personnel créé, les finalités du traitement, les catégories de données traitées, l'origine des données, le responsable du traitement, les personnes ayant accès aux données, ainsi que la durée de conservation des données. Ces informations créent en effet un cadre légal détaillé dans le cadre duquel des traitements de données à caractère personnel peuvent avoir lieu au sein

de l'Institut. La CNPD tient cependant à souligner ci-après certaines observations relatives audit article 15.

1. Le fichier de données à caractère personnel créé

Le paragraphe (1) prévoit la création d'un fichier de données à caractère personnel appelé « fichier individuel des personnes accueillies à l'Institut », composé de quatre « pièces » différentes. Parmi ces pièces, la « fiche personnelle », figure notamment pour les enfants et les jeunes adultes admis dans le département hébergement les données suivantes : « *les prénom, nom et qualité des visiteurs et la date des visites* ». Par ailleurs, le paragraphe (5) prévoit la tenue d'un registre dans lequel figure les présences des enfants, des adolescents et des jeunes adultes, ainsi que les visites, les rencontres et les réunions avec les parents, représentants légaux et autres personnes concernées. Or, il ne ressort pas clairement de la rédaction actuelle de l'article 15 si le registre prévu par le paragraphe (5) comporte exclusivement les données appelées à figurer dans le fichier créé par le paragraphe (1), auquel cas ce paragraphe (5) apparaît superflu, où s'il s'agit d'un autre fichier de données à caractère personnel, qu'il conviendrait de décrire au paragraphe (1) pour des raisons de cohérence.

Par ailleurs, les paragraphes (2), (3) et (4) du même article 15 font référence au « *dossier personnel* », au « *dossier individuel* » et au « *fichier individuel* ». Il ne ressort pas clairement du texte de l'avant-projet de loi si ces termes font référence au fichier individuel des personnes accueillies à l'Institut, ou à la fiche personnelle telle que décrite dans le paragraphe (1), alinéa 1, point 1. Pour des raisons de cohérence entre les différents paragraphes de cet article, il serait opportun d'emprunter une même terminologie.

2. Les finalités du traitement

Les finalités des traitements de données à caractère personnel effectués au sein de l'Institut sont décrites au paragraphe (1). Elles consistent, d'une part, à « *documenter l'hébergement et l'encadrement des personnes accueillies par les différents départements de l'Institut* », et d'autre part, à des fins d' « *études, historiques et statistiques, de la population cible* ».

La Commission nationale relève cependant que certaines données appelées à figurer dans ce fichier, telles que « *toute documentation sur [l'] état de santé [de la personne accueillie à l'Institut]* », ou encore « *son numéro de compte bancaire* », n'apparaissent a priori pas nécessaire à la réalisation de telles finalités. Dès lors, la Commission nationale recommande de détailler avec plus de précisions dans le texte de l'avant-projet de loi l'ensemble des finalités pour lesquelles les données énumérées dans l'article 15 seront traitées (telles par exemple, « *à des fins de gestion administrative et financière* », ou encore « *aux fins de préserver le bien-être physique et mental des personnes concernées et des autres personnes accueillies à l'Institut qui les côtoient* » pour ce qui concerne le traitement des données de santé).

3. Les catégories de données traitées

Les données visées aux points (6) et (7) du paragraphe (1), alinéa 2 constituent des catégories particulières de données au sens de l'article 6 de la loi modifiée du 2 août 2002 (données dites « sensibles »).

En ce qui concerne la collecte de toute documentation sur l'état de santé de la personne accueillie par l'Institut (paragraphe (1), alinéa 2, point 6), la Commission nationale comprend sur base du paragraphe (3), alinéa 2 que l'accès à ces données ne pourra être octroyé qu'au directeur et directeur adjoint de l'Institut, ainsi qu'aux responsables des départements concernés, pour les seules finalités de pouvoir agir dans l'intérêt de la personne concernée lorsque sa santé est menacée, et afin de préserver le

bien-être physique et mental de la personne concernée et des autres personnes accueillies à l'Institut.

L'accès au dossier médical par ces personnes est susceptible de constituer une violation au secret médical. Or, les auteurs de l'avant-projet de loi justifient cette entorse en précisant que *« cette exception est justifiée par la nécessité de préserver le bien-être physique et mental des personnes concernées et des autres personnes accueillies à l'Institut qui les côtoient »*. La CNPD peut partager cette analyse pour justifier la nécessité de l'accès au dossier médical par un nombre limité de personnes au sein de l'Institut. Les dérogations au secret médical doivent obligatoirement être prévues dans un texte légal, ce que les auteurs de l'avant-projet de loi se proposent de faire en l'espèce.

En ce qui concerne la collecte des données relatives à la confession (paragraphe (1), alinéa 2, point 7), la Commission nationale se pose la question de la nécessité de disposer de cette information.

De manière générale, l'article 6 de la loi modifiée du 2 août 2002 interdit le traitement des données dites sensibles parmi lesquelles figurent les données relatives aux convictions religieuses, sauf dans les cas d'exception limitativement énumérés à l'article 6 paragraphe (2) de la loi (article 8 paragraphe 2 de la Directive 95/46/CE). Parmi les exceptions qui auraient vocation à s'appliquer en l'espèce figurent notamment le consentement de la personne concernée (article 6 paragraphe (2) lettre (a)) ou la collecte des données dans le cadre d'un traitement de données judiciaires au sens de l'article 8 de la loi modifiée du 2 août 2002 (article 6 paragraphe (2) lettre (i)), lorsque cette donnée provient des autorités judiciaires en cas d'admission sur décision judiciaire.

L'avant-projet de loi précise que l'indication de la confession de la personne accueillie à l'Institut se fera *« à titre facultatif pour la personne concernée »*. Afin d'enlever toute ambiguïté à ce sujet, il serait bienvenu de préciser dans le texte de l'article de l'avant-projet de loi que la collecte de cette donnée ne peut s'opérer que moyennant le consentement exprès de la personne concernée conformément à l'article 6 paragraphe (2) lettre (a) de la loi modifiée du 2 août 2002. En outre, le consentement doit être informé, ce qui implique que par exemple, une notice d'information ou une information orale devra clairement expliquer à la personne accueillie à l'Institut quelle est la finalité de la collecte de cette information, que la collecte de données relatives à sa confession est facultative, et que le fait de refuser de répondre à une question relative

à ses convictions religieuses ou philosophiques n'entraîne en aucun cas de conséquences négatives.

Enfin, la CNPD tient à souligner que les données visées aux points (1) et (2) du paragraphe (1), alinéa 4 constituent des données judiciaires au sens de l'article 8 de la loi modifiée du 2 août 2002. Le traitement de telles données doit être 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. En ce qui concerne le point (2), à savoir « *toute documentation de blessures visibles et d'allégation de mauvais traitements antérieurs* », les remarques exposées ci-dessus concernant le traitement de données de santé restent également valables.

4. Le responsable du traitement

Selon le paragraphe (3), « *le directeur de l'institut est considéré, en ce qui concerne le traitement des données à caractère administratif dans le cadre de l'hébergement des personnes accueillies à l'Institut, comme responsable de traitement au sens de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* ».

La notion de « *données à caractère administratif* » apparaît superflue, à moins que les auteurs de l'avant-projet aient souhaité opérer une distinction entre les « *données à caractère administratif* » et les données de santé visées au paragraphe (3) alinéa 2, voire les données judiciaires visées au paragraphe (1) alinéa 4. Dans ce cas, il conviendrait de le préciser dans le texte de l'avant-projet de loi. La Commission nationale tient à souligner qu'en tout état de cause, toutes ces catégories de données doivent être considérées comme des données à caractère personnel au sens de l'article 2 lettre (r) de la loi modifiée du 2 août 2002.

Enfin, il conviendrait de remplacer les termes de « *responsable de traitement* » par « *responsable du traitement* », afin de s'aligner sur la terminologie de l'article 2 lettre (n) de loi modifiée du 2 août 2002.

5. L'origine des données

Le dernier alinéa du paragraphe (1) précise que les données figurant dans le fichier individuel des personnes accueillies à l'Institut « *proviennent de la personne concernée elle-même, de la personne l'ayant encadrée ou de ses parents ou de son représentant légal, ou des autorités judiciaires en cas d'admission sur décision judiciaire* ».

Cet alinéa n'appelle pas de commentaire particulier.

6. Les personnes ayant accès aux données

Le paragraphe (3) prévoit que le directeur de l'Institut « *peut autoriser l'accès aux données et informations visées au paragraphe (1) de l'article 16 aux membres du personnel de l'Institut nommément désignés par lui, en fonction de leurs attributions* ». La Commission nationale suggère de remplacer « *article 16* » par « *article 15* », afin de corriger une erreur matérielle.

7. La durée de conservation des données

Le paragraphe (4) prévoit notamment que « *les données relatives au fichier individuel sont conservées jusqu'à l'âge de 30 ans de la personne concernée* ». Les auteurs de l'avant-projet de loi justifie une telle durée dans le commentaire des articles en précisant qu' « *il arrive, en effet, qu'une même personne soit admise à plusieurs reprises dans l'une ou l'autre structure de l'Institut. En cas de réadmission, le dossier individuel peut être reproduit et continué. De même, il arrive régulièrement que des personnes ayant été anciennement admises à l'Institut viennent demander des certificats et pièces relatives à leur séjour ou leur encadrement à l'Institut, d'où l'intérêt de conserver ces*

Annexes

données jusqu'à 3 ans à compter du dernier départ possible ».

Alors que la CNPD peut en partie comprendre cette justification, elle tient cependant à rappeler que, conformément à l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002, « *le responsable du traitement doit s'assurer que les données qu'il traite (…) sont 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 sans préjudice du paragraphe (2) ci-après* ». Or, la finalité indiquée au paragraphe (1), consistant à « *documenter l'hébergement et l'encadrement de chaque personne accueillie dans les différents départements de l'Institut* », ne justifie a priori pas la nécessité de conserver les données au-delà du départ de la personne de l'Institut. Si la Commission nationale peut admettre une période limitée de conservation ultérieure des données pour les cas de réadmissions ou de demande de certificats et de pièces, la limite prévue par les auteurs de l'avant-projet de loi (à savoir « *jusqu'à l'âge de 30 ans* ») apparaît excessive d'une part, et peu objective d'autre part, dans la mesure où la durée de conservation effective des données pourrait dans ce cas varier de façon très importante en fonction de l'âge du départ de la personne de l'Institut. La Commission nationale propose donc une durée de conservation de cinq ans après le départ de la personne de l'Institut, durée qui paraît à ses yeux suffisante dans la plupart des cas de demandes de certificats ou de pièces, voire d'éventuelles réadmissions.

Par ailleurs, le paragraphe (4) prévoit également que « *lorsque le délai de conservation des données relatives au dossier individuel du pensionnaire est écoulé, les données sont anonymisées à des fins statistiques ou historiques* ». Il est précisé à cet égard dans le commentaire des articles que « *l'anonymisation des données vise la protection des personnes concernées, mais permet l'utilisation de ces données à des fins de documentation statistique et historique* ». Des données anonymisées ne constituent plus des données à caractère personnel au sens de l'article 2 lettre (e) de la loi modifiée du 2 août 2002. Dès lors, la Commission nationale ne voit pas de problème à ce que de telles données soient conservées pour une durée ultérieure. Cependant, elle tient à souligner que ces données doivent être irrémédiablement anonymisées, ce qui suppose notamment qu'il ne sera plus possible, ni pour l'Institut public d'aide à l'enfance et à la jeunesse, ni pour un tiers, de réidentifier même indirectement les personnes concernées.

8. Les mesures de sécurité et le traçage des accès aux données

La Commission nationale note avec satisfaction que le paragraphe (6) prévoit que les personnes ayant accès aux données à caractère personnel visées à l'article 15 soient tenues au respect du secret professionnel. Afin de corriger une erreur matérielle, il conviendrait de rajouter le mot *« article »* entre les termes *« visées par le présent »* et *« sont tenues au respect du secret professionnel »*.

De manière plus générale, l'avant-projet de loi sous examen ne prévoit pas de dispositions relatives aux mesures de sécurité et de confidentialité des données, à l'exception du paragraphe (4) qui ne s'applique qu'en cas de départ de la personne de l'Institut. Certes, les articles 22 et 23 de la loi modifiée du 2 août 2002 relatifs à la sécurité des traitements de données à caractère personnel sont applicables aux traitements de données envisagés. Cependant, vu l'ampleur de la collecte de données à caractère personnel en cause, il conviendrait de prévoir des mesures de sécurité spécifiques dans le texte du règlement grand-ducal et plus particulièrement en ce qui concerne le contrôle de l'utilisation, de l'accès et de la transmission des données.

Ces mesures devraient notamment englober des restrictions physiques précises à l'accès aux données stockées sur papier et un système de traçage des accès aux dossiers personnels des personnes accueillies à l'Institut, dans l'hypothèse où ils sont établis sur support informatique comme indiqué au paragraphe (2) de l'article 15. La Commission nationale suggère dès lors de rajouter une disposition, à l'instar d'autres lois ou règlements grand-ducaux, qui pourrait avoir la teneur suivante : *« Le système informatique par lequel l'accès au fichier individuel des personnes accueillies à l'Institut est opéré doit être aménagé de sorte que l'accès aux fichiers soit sécurisé moyennant une authentification forte, que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle. »*.

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

Ainsi décidé à Esch-sur-Alzette en date du 10 mars 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre suppléant

7 Annexes

Avis relatif au projet de loi n°7083 relatif à la mise en application du Règlement (UE) N°655/2014 du Parlement européen et du Conseil du 15 mai 2014 portant création d'une procédure d'ordonnance européenne de saisie conservatoire des comptes bancaires, destinée à faciliter le recouvrement transfrontière de créances en matière civile et commerciale, modifiant le Nouveau Code de procédure civile et la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier

Délibération n°216/2017
du 10 mars 2017

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

Par courrier du 21 décembre 2016, Monsieur le Ministre de la Justice a fait parvenir à la CNPD des amendements concernant le projet de loi n°7083 relatif à la mise en application du Règlement (UE) N°655/2014 du Parlement européen et du Conseil du 15 mai 2014 portant création d'une procédure d'ordonnance européenne de saisie conservatoire des comptes bancaires, destinée à faciliter le recouvrement transfrontière de créances en matière civile et commerciale, modifiant le Nouveau Code de procédure civile et la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier

Le Règlement (UE) N°655/2014 met en place des procédures censées faciliter les saisies conservatoires des comptes bancaires dans des litiges à caractère transfrontalier.

Dans ce cadre, il instaure un mécanisme permettant au créancier de demander que les informations nécessaires pour identifier le compte du débiteur soient obtenues par la juridiction compétente pour ordonner la saisie auprès d'une autorité chargée de l'obtention d'informations désignée de l'État membre dans lequel le créancier croit que le débiteur détient un compte.

Le règlement européen qui est d'application directe ne laisse aux Etats-membres aucune marge de manœuvre quant au principe même de cette information, ni quant à la règle selon laquelle, sous certaines conditions, cette

information peut avoir lieu déjà avant même que le créancier ne dispose d'une décision judiciaire ou d'un autre acte exécutoire[1].

En revanche, le règlement laisse aux législateurs nationaux le choix quant à la méthode utilisée pour l'obtention des informations relatives aux comptes.

Les auteurs du projet de loi optent pour la méthode prévue à l'article 14 paragraphe 5. lettre a) du règlement, c'est-à-dire l'obligation pour toutes les banques se trouvant sur son territoire de déclarer, à la demande de l'autorité chargée de l'obtention d'informations - en l'espèce la CSSF -, si le débiteur détient un compte auprès d'elles.

La CNPD peut approuver ce choix eu égard aux exigences du règlement et à l'objectif affiché de l'article 14 du Règlement N°655/2014, à savoir de concilier l'efficacité des procédures de recouvrement et la protection des données[2].

Enfin, il convient de relever que les données sont traitées dans de cadre de procédures judiciaires, de sorte qu'il s'agit de données judiciaires auxquelles s'appliquent l'article 8 de la loi modifiée du 2 août 2002 aux termes duquel « *le traitement des données dans le cadre […] 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.*»

Pour le surplus la CNPD n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 10 mars 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis relatif au projet de loi n°7024 portant mise en œuvre du règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, et portant modification : 1. de la loi modifiée du 5 avril 1993 relative au secteur financier ; 2. de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; 3. de la loi modifiée du 5 août 2005 sur les contrats de garantie financière ; 4. de la loi modifiée du 11 janvier 2008 relative aux obligations de transparence des émetteurs ; 5. de la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif ; 6. de la loi modifiée du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs ; et 7. de la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement

Délibération n°243/2017
du 16 mars 2017

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

[1] Article 14 paragraphe 1. alinéa 2 du Règlement (UE) N°655/2014
[2] Considérants 20 et 21 du Règlement (UE) N°655/2014

Annexes

« la loi de 2002 »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Le 29 juillet 2016, Monsieur le Ministre des Finances a déposé à la Chambre des députés le projet de loi n°7024 relative aux commissions d'interchange et modifiant différentes lois relatives aux services financiers secteur financier (ci-après désigné « le projet de loi »). Au vu des changements apportés par le projet de loi sur les traitements des données à caractère personnel mis en œuvre par les entités tombant dans le champ d'application du projet de loi, la Commission nationale regrette de ne pas avoir été saisie formellement dudit projet de loi par Monsieur le Ministre des Finances, alors même que le Conseil d'Etat, dans son avis du 13 décembre 2016 a souligné *« que la Commission nationale pour la protection des données devrait être entendue en son avis, vu les enjeux, en l'occurrence, au niveau de la protection des données à caractère personnel »*[3].

Dès lors et en application de l'article 32, paragraphe (3), lettre (f) de la loi modifiée du 2 août 2002, la Commission nationale a pris la décision de se saisir elle-même pour aviser le présent projet de loi.

Selon l'exposé des motifs, le projet de loi a un double objectif, à savoir la mise en œuvre du règlement (UE) n°2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, ainsi que la modification de plusieurs lois applicables au secteur financier dont, notamment, la loi modifiée du 5 avril 1993 relative au secteur financier (ci-après « la loi modifiée du 5 avril 1993 »).

Plus particulièrement, le projet de loi vise à faciliter l'externalisation, autrement appelée la sous-traitance, des services par une personne physique ou morale soumise à la surveillance prudentielle de la Commission de Surveillance du Secteur Financier (ci-après désignée « la CSSF ») en vertu de la loi modifiée du 5 avril 1993 ou établie au Luxembourg et soumise à la surveillance de la Banque centrale européenne (ci-après désignée « l'entité surveillée »).

Pour atteindre cet objectif, le projet de loi remplace l'exception au secret professionnel relative à la sous-traitance actuellement prévue à l'article 41, paragraphe

[3] Avis du Conseil d'Etat du 13 décembre 2016, doc. parl. n°7024/02, p. 4.

(5) de la loi modifiée du 5 avril 1993 par trois nouvelles exceptions, à savoir une exception pour la sous-traitance des activités à une entité établie au Luxembourg et surveillée par la CSSF, la Banque Centrale Européenne (ci-après la « BCE ») ou le Commissariat aux assurances (ci-après le « CAA ») (ci-après désignée « la sous-traitance surveillée »), une exception pour la sous-traitance à une entité du groupe auquel l'entité surveillée appartient (ci-après désignée « la sous-traitance intragroupe »), ainsi qu'une exception pour la sous-traitance « dans tous les autres cas » (ci-après désignée « la sous-traitance extragroupe »).

L'externalisation des activités par une entité surveillée implique dans la plupart des cas des traitements de données à caractère personnel et, comme l'a souligné le Conseil d'Etat dans son avis du 13 décembre 2016[4], une augmentation du risque de divulgation des données. Il est dès lors primordial d'entourer la sous-traitance d'un niveau élevé de garanties pour assurer la protection et la confidentialité des données à caractère personnel du début à la fin de la sous-traitance.

La Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de loi sous examen traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel, à savoir l'article 41 de la loi modifiée du 5 avril 1993.

Elle rappelle que le règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD ») sera applicable à partir du 25 mai 2018. Il convient ainsi d'analyser le projet de loi à la lumière de la loi modifiée du 2 août 2002 qui est la législation actuellement en vigueur, d'une part, et du nouveau Règlement européen d'autre part.

I. Quant à la terminologie

Alors que le RGPD consacre la notion de « groupe d'entreprises »[5], la CNPD s'interroge sur la précision que les services doivent être sous-traités « *intégralement* » à l'intérieur du groupe. « *[L]es auteurs du projet de loi ont-ils voulu dire que l'externalisation portera sur la totalité d'un service déterminé ? Quel régime s'appliquera dans ce cas en présence d'une externalisation partielle d'un service ? Le régime défini par la CSSF dans ses circulaires sera-t-il d'application ? Ou est-ce que les auteurs du projet de loi ont visé l'hypothèse d'une externalisation exclusivement effectuée au sein du groupe auquel appartient l'établissement concerné ?* »[6].

Le commentaire des articles précise uniquement que la sous-traitance en cascade à l'intérieur du groupe serait permise en vertu de l'alinéa en question[7].

Il pourrait en être déduit que la disposition relative à la sous-traitance intragroupe vise l'hypothèse où la totalité des services sous-traités sera fournie par une entité du groupe auquel appartient l'entité surveillée et qu'afin que ce dernier puisse bénéficier de l'exception au secret professionnel établie par la disposition, un sous-traitant n'appartenant pas au même groupe que l'entité surveillée ne pourra pas être recruté.

Pour autant, cette disposition en elle-même ne précise pas avec une clarté suffisante les conditions sous lesquelles les entités surveillées seront exemptées de l'obligation au secret professionnel. La Commission nationale estime dès lors nécessaire de modifier le projet de loi afin d'y définir davantage les conditions dans lesquelles la sous-traitance intragroupe pourrait avoir lieu et, notamment, la spécification qu'elle doit avoir lieu « *intégralement à l'intérieur du groupe* ».

---

[4] Avis du Conseil d'Etat du 13 décembre 2016, doc. parl. N°7024/02, p. 4.
[5] Par exemple, voir l'article 4, paragraphe (19).
[6] Avis du Conseil d'Etat du 13 décembre 2016, doc. parl. N°7024/02, p. 7.
[7] Commentaire des articles, p. 15.

Annexes

II. Quant à la relation contractuelle entre le responsable du traitement et le sous-traitant

La loi modifiée du 2 août 2002 et le RGPD soumettent le recours par un responsable du traitement à un sous-traitant à la conclusion d'un contrat ou d'un autre acte juridique écrit, qui doit comporter au moins les clauses obligatoires figurant dans les deux textes législatifs[8]. Le pays d'établissement du sous-traitant n'a pas d'incidence sur la nécessité de conclure un tel contrat, la conclusion étant obligatoire dans tous les cas de sous-traitance.

S'agissant de la sous-traitance surveillée, l'alinéa 1er de l'article 41, paragraphe (2bis), tel qu'ajouté par le projet de loi sous examen, subordonne le recours par une entité surveillée à un sous-traitant à la conclusion d'un contrat de service entre les deux parties.

S'agissant de la sous-traitance intragroupe et extragroupe, cette exigence ne ressort pas clairement des alinéas 2 et 3 de l'article sous examen. En effet, ces dispositions ne soumettent pas la transmission des données confidentielles dans le cadre d'une sous-traitance à la conclusion d'un contrat de service. Le projet de loi fait uniquement mention d'un « accord de confidentialité » que les entités surveillées pourraient mettre en place avec les sous-traitants afin de leur transmettre des données confidentielles.

Ni le projet de loi, ni le commentaire des articles ne fournissent de définition ou d'explications quant à la forme ou au contenu dudit « accord de confidentialité ». En l'absence de précisions à cet égard, la Commission nationale part du postulat que, contrairement à la sous-traitance surveillée, les auteurs du projet de loi n'entendent pas subordonner la sous-traitance intragroupe ou la sous-traitance extragroupe à la conclusion d'un contrat de service.

Alors que la Commission nationale constate que des circulaires de la CSSF prévoient que la sous-traitance doit faire l'objet d'un contrat[9], elle estime qu'afin d'écarter tout risque d'insécurité juridique et pour créer une base légale unique qui garantirait pour toutes les relations de sous-traitance la protection et la confidentialité des données, il est nécessaire de spécifier dans le projet de loi que la sous-traitance doit être encadrée par un contrat de service, quelles que soient les modalités de la sous-traitance.

III. Quant à la sous-traitance en cascade

Comme soulevé au point I., le commentaire des articles relatif

[8] Les clauses obligatoires sont prévues à l'article 22, paragraphe (2) de la loi modifiée du 2 août 2002 et à l'article 28, paragraphes (2) et (3) du RGPD.

[9] Circulaire CSSF 12/552, telle que modifiée, point 207 « *Tout accord de sous-traitance fait l'objet d'un contrat officiel et détaillé (cahier des charges inclus).* » ; la Circulaire CSSF 05/178, p. 3 « *Toute sous-traitance doit être formalisée par un contrat de services avec un cahier des charges qui tient compte des conditions énumérées ci-dessous.* ».

à la sous-traitance intragroupe précise que la sous-traitance en cascade serait permise en vertu du nouvel alinéa 2 du paragraphe (2bis) de l'article 41[10]. Alors que le projet de loi n'y fait aucune référence dans le cadre de la sous-traitance surveillée ou la sous-traitance extragroupe, il est envisageable que la sous-traitance en cascade puisse également être mise en œuvre dans ces deux cas.

En l'absence d'obligation de conclure un contrat de service, l'article 14 du projet de loi sous examen ne prévoit pas de base juridique contraignante en vertu de laquelle la sous-traitance en cascade par les entités surveillées doit fait l'objet d'un contrat et établissant des critères de contrôle que les entités surveillées devraient adopter dans le cadre de la sous-traitance en cascade.

S'il est vrai que la loi modifiée du 2 août 2002 ne comporte pas d'indications spécifiques concernant la sous-traitance en cascade, le RGPD subordonne, en revanche, expressément le recours à la sous-traitance en cascade à l'autorisation écrite préalable du responsable du traitement[11]. Le sous-traitant doit ainsi obtenir soit une autorisation préalable spécifique, soit une autorisation préalable générale pour pouvoir recruter d'autres sous-traitants. Dans le cas où le responsable du traitement accorderait une autorisation générale, le sous-traitant sera obligé d'informer le responsable de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants afin de donner la possibilité à ce dernier de s'opposer à de tels changements.

La Commission nationale relève d'ailleurs que l'importance de maîtriser la sous-traitance informatique en cascade a été soulevée dans des circulaires de la CSSF[12].

Compte tenu de l'importance de maîtriser la sous-traitance en cascade et afin d'établir une base légale uniforme imposant un contrat de service pour la sous-traitance en cascade, la CNPD recommande de modifier l'article 14 du projet de loi pour imposer que l'obligation de conclure un contrat de service s'étend à la sous-traitance en cascade et que ce contrat doit indiquer les conditions dans lesquelles le sous-traitant peut avoir recours à d'autres sous-traitants.

IV. Quant aux transferts de données vers des pays tiers

En vertu de l'article 41, paragraphe *(2bis)*, alinéas 2 et 3, tel qu'ajouté par le projet de loi, les entités régulées pourraient transmettre des données confidentielles, y compris l'historique des transactions des clients, à des sous-traitants établis hors du Luxembourg dans le cadre de la sous-traitance intragroupe et extragroupe. Par ailleurs, le texte actuel ne s'oppose, en principe, pas à ce qu'un sous-traitant recruté sur base de l'alinéa 1er sous-traite des services à un sous-traitant sur base de l'alinéa 2, donc faisant parti du même groupe que le sous-traitant, établi dans un pays tiers.

a. Les règles en matière de protection des données

Dans la législation applicable en matière de protection des données, les transferts de données vers des pays tiers sont strictement encadrés par la loi.

Conformément à la loi modifiée du 2 août 2002, les transferts vers des pays tiers ne sont possibles que si la Commission Européenne a désigné le pays tiers en question comme assurant un niveau de protection adéquat aux termes d'une « décision d'adéquation ». A l'heure actuelle, l'Islande, le Liechtenstein, la Norvège, la Suisse, l'Andorre, les îles de Guernesey, Jersey, Man et Féroé, l'Argentine, l'Uruguay, la Nouvelle Zélande et l'Israël et les sociétés tombant dans le champ d'application de la « *Canadian Personal Information Protection and Electronic Documents Act* » au Canada font l'objet d'une décision d'adéquation. Aux Etats-Unis, seules les entreprises qui ont volontairement adhérés au « *EU-U.S. Privacy Shield Framework* » peuvent directement recevoir des

[10] Commentaire des articles, p. 15.
[11] RGPD, art. 28, paragraphe (2).
[12] Circulaire CSSF 12/552, telle que modifiée, point 186 ; Circulaire CSSF 05/178, p. 3.

données provenant de l'Union européenne.

Le RGPD reprend le régime des décisions d'adéquation et vise à maintenir les décisions rendues sur base 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 (ci-après « la Directive 95/46/CE »), qui a été transposée en droit luxembourgeois par la loi modifiée du 2 août 2002.

A défaut de décision d'adéquation, un responsable du traitement peut mettre en place des garanties appropriées pour pourvoir effectuer des transferts vers des pays tiers, conformément à l'article 19 de la loi de 2002. Ces garanties appropriées peuvent actuellement résulter des clauses contractuelles types adoptées par la Commission européenne en application de l'article 26, paragraphe (4) de la Directive 95/46/CE ou des règles contraignantes d'entreprise approuvées par les autorités de protection des données des États membres concernés. Le recours à ces types de transfert de données nécessite actuellement l'autorisation préalable de la CNPD[13].

La possibilité d'effectuer des transferts sur base de garanties appropriées a été maintenue dans les articles 46 et 47 du RGPD. Contrairement à la loi actuellement en vigueur, le RGPD liste les garanties appropriées qui ne nécessiteront, en principe, plus d'autorisation préalable de la part de la CNPD à l'avenir, tel que des règles d'entreprises contraignantes approuvées conformément à la procédure prévue par le RGPD.

En l'absence d'une décision d'adéquation ou des garanties appropriées, la loi de 2002 et le RGPD permettent aux responsables du traitement de fonder le transfert de données vers des pays tiers sur des dérogations pour des situations spécifiques limitativement prévues par ces textes, par exemples, avec le consentement de la personne concernée ou si le transfert est nécessaire à l'exécution d'un contrat auquel la personne concernée et le responsable du traitement sont parties ou à l'exécution des mesures précontractuelles prises à la demande de la personne concernée[14].

b. La sous-traitance intragroupe et extragroupe

Le projet de loi, quant à lui, pose une double condition que les entités régulées doivent remplir afin de recourir à la sous-traitance intragroupe et à la sous-traitance extragroupe. D'une part, les entités surveillées doivent s'assurer que la sous-traitance est entourée d'une obligation de confidentialité. Les personnes au service des sous-

[13] Cependant, le projet de loi n°7049 portant modification de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel envisage d'abolir l'obligation pour le responsable du traitement d'obtenir une autorisation préalable, pour le cas où il aurait recours à ces mesures.

[14] Loi modifiée du 2 août 2002, art. 19, paragraphe (1) et RGPD, art. 49.

traitants doivent ainsi soit être soumises à une obligation de secret professionnel, soit être liées par un accord de confidentialité. D'autre part, les clients des entités régulées doivent être informés de la sous-traitance intragroupe et doivent donner leur accord préalable par écrit à la sous-traitance extragroupe.

Dans l'optique de la CNPD, la double condition prévue par le projet de loi ne suffit pas pour assurer que les données à caractère personnel soient protégées lors du transfert vers et le traitement par le sous-traitant dans un pays tiers.

En l'absence d'une obligation de secret professionnel, la seule garantie serait l'accord de confidentialité. Compte tenu de l'absence des précisions dans le projet de loi quant au format et au contenu de l'« accord de confidentialité », il n'y a aucune certitude qu'un tel accord mettrait en place des garanties suffisantes pour protéger les données.

En ce qui concerne la sous-traitance intragroupe, la CNPD note qu'en matière de protection des données, la simple information préalable de la personne concernée n'est pas une base légale pour effectuer un transfert de données vers un pays tiers.

Pour ce qui est de la sous-traitance extragroupe, le client doit, selon l'article 41, paragraphe *(2bis)*, alinéa 3, tel qu'ajouté par le projet de loi, donner son accord préalable par écrit à « *la sous-traitance des services sous-traités, [au] type de renseignements transmis dans le cadre de la sous-traitance et [au] pays d'établissement des entités prestataires des services sous-traités* ». Dans l'optique de la CNPD, l'accord donné sur base de ces informations ne saurait pas être considéré comme étant éclairé. En effet, comme soulevé par le Conseil d'Etat dans son avis du 13 décembre 2016[15], les informations qui devraient être fournies en vertu du projet de loi ne sont pas aussi complètes que les informations devant être fournies au client en vertu du point 193 de la Circulaire CSSF 12/552 pour que ce dernier puisse donner son accord à la levée du secret professionnel.

De plus, en matière de protection des données à caractère personnel, l'article 19 de la loi modifiée du 2 août 2002 énonce les dérogations au principe d'interdiction des transferts vers des pays tiers, sur base desquelles un responsable du traitement peut transférer des données vers un pays tiers. Une de ces dérogations est le consentement de la personne concernée[16].

Le consentement figure également à l'article correspondant dans le RGPD relatif aux « dérogations pour des situations particulières »[17], qui précise qu'afin de constituer une base légale pour le transfert de données, le consentement de la personne concernée doit être explicite et le responsable du traitement doit avoir informé la personne concernée « *des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées* »[18].

Aux termes de l'article 2, lettre (c) de la loi de 2002, le consentement de la personne concernée doit être libre, spécifique et informé. Le RGPD reprend ces exigences dans son article 4, numéro (11) et ajoute qu'en plus d'être libre, spécifique et éclairé, il faut encore que le consentement soit univoque et qu'il résulte d'une déclaration ou d'un acte positif clair. Il en résulte que la transparence est un aspect fondamental du consentement[19]. La personne concernée doit recevoir toutes les informations nécessaires à la bonne compréhension des traitements mis en œuvre par le responsable du traitement.

A cet égard, le Groupe de Travail « Article 29 » a précisé qu'afin d'être informé ou éclairé, le consentement doit « *être fondé sur l'appréciation et la compréhension des faits et des conséquences d'une action* »[20]. Dans le cadre des transferts des données vers des pays tiers, cela implique que la personne concernée doit avoir été informée des circonstances particulières

[15] Avis du Conseil d'Etat du 13 décembre 2016, doc. parl. n°7024/02, p. 8.
[16] Loi modifiée du 2 août 2002, art. 19, paragraphe (1), lettre (a).
[17] RGPD, art. 49.
[18] RGPD, art. 49, paragraphe (1), lettre (a).
[19] Avis 15/2011 du Groupe de Travail « Article 29 » sur la définition du consentement (WP 187), p. 10.
[20] Ibid, p. 21.

du transfert, afin de permettre à cette dernière de « *donner son consentement en pleine connaissance de cause* »[21].

Au vu ce qui précède et du fait que les entités surveillées ne seraient tenues, en vertu du projet de loi sous avis, de fournir que des informations très générales sur la sous-traitance, l'accord du client, dans le format prévu par le projet de loi, ne saurait pas remplir les exigences établies par la loi de 2002 et par le RGPD et ne saurait dès lors pas être considéré comme étant suffisamment informé et éclairé.

En tout état de cause, comme soulevé ci-avant, le consentement de la personne concernée constitue une dérogation au principe érigé par la loi de 2002 selon lequel le transfert des données à caractère personnel ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat. A cet égard, le Groupe de Travail « Article 29 » a précisé que ces dérogations ne devraient pas être utilisées pour les transferts qui puissent être qualifiés de répétitifs, massifs ou structurels[22]. Il est évident que le recours à un sous-traitant entrainerait dans la plupart des cas des transferts répétitifs, massifs et/ou structurels. Dans le même ordre d'idée, le RGPD précise que le consentement fait partie des « *dérogations pour des situations particulières* ».

Vu les volumes substantiels des données à caractère personnel qui seraient transmises entre le responsable du traitement et le sous-traitant[23], il serait plus opportun de recourir à des garanties appropriées, telles que des règles d'entreprises contraignantes ou des clauses contractuelles types, prévues par l'article 19 de la loi de 2002 et les articles 46 et 47 du RGPD, si des données sont transférées vers un pays, qui ne fait pas l'objet d'une décision d'adéquation.

La CNPD relève qu'une dérogation à une règle doit être interprétée de façon stricte[24]. En prévoyant que le transfert des données pourrait avoir lieu avec le consentement de la personne concernée, le projet de loi créerait en effet une application généralisée de la dérogation relative au consentement, ce qui va à l'encontre de l'esprit de la loi de 2002 et du RGPD.

Dès lors, en ce qui concerne la protection des données à caractère personnel, la CNPD estime que la dérogation généralisée relative au consentement prévue par le projet de loi ne correspond pas aux critères établis par la loi de 2002 et par le RGPD et ne peut pas à lui seul servir de base légale pour le transfert de données vers des pays tiers.

c. Conclusion

Vu l'absence d'une définition d' « accord de confidentialité », la

[21] Document de travail du Groupe de Travail « Article 29 » relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (WP 114), p. 14.
[22] Document de travail du Groupe de Travail « Article 29 » relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 (WP 114), p. 11 et 13.
[23] Avis du Conseil d'Etat du 13 décembre 2016, doc. parl. N°7024/02, p. 10.
[24] Arrêt de la Cour de Justice de l'Union européenne du 22 novembre 2012, Probst, C-119/12, EU:C:2012:748, point 23; Arrêt de la Cour de Justice de l'Union européenne du 21 décembre 2016, Tele2 Sverige AB, C-203/15 et C-698/15, ECLI:EU:C:2016:970, point 89.

Commission nationale estime que le projet de loi dans son état actuel n'entoure pas le transfert de données vers des pays tiers des garanties suffisantes.

Par ailleurs, la CNPD tient à souligner que l'accord du client, tel que prévu par le projet de loi, ne saurait pas être considéré comme étant informé et éclairé au sens de la loi de 2002 et du RGPD. Finalement, en tout état de cause, dans le cadre de la sous-traitance intragroupe et la sous-traitance extragroupe, telles que prévues par le projet de loi, le consentement généralisé ne pourra pas servir de base légale pour les entités régulées pour effectuer des transferts des données vers des pays tiers.

La CNPD estime donc que le projet de loi n'offre pas dans son état actuel un cadre juridique suffisant pour assurer que les données à caractère personnel des clients des entités régulées soient protégées lors d'un transfert vers un pays tiers.

Elle suggère dès lors de modifier le projet de loi afin d'y indiquer les conditions dans lesquelles ces transferts pourront avoir lieu, notamment en ce qui concerne des garanties à mettre en place entre l'entité régulée et les sous-traitants pour assurer la protection des données lors des transferts vers des pays tiers.

V. Quant à l'information de la personne concernée

Le droit à l'information de la personne concernée, bien que lié étroitement, est distinct de l'obligation du responsable du traitement de s'assurer que le consentement est informé et éclairé[25], est prévu à l'article 26 de la loi modifiée du 2 août 2002. En vertu de cet article, la personne concernée a le droit d'obtenir des informations relatives au responsable du traitement, les finalités du traitement, les destinataires auxquels les données sont susceptibles d'être communiquées, le fait de savoir si la réponse aux questions est obligatoire et les conséquences d'un défaut de réponse, ainsi que l'existence d'un droit d'accès.

La liste des informations qui devront être fournies à la personne concernée sera étendue par le RGPD. Cette dernière doit ainsi être informée non seulement des finalités des traitements, mais également de leur base juridique[26]. En sus des informations qui sont obligatoires à l'heure actuelle, les personnes concernées recevront, entre autres, communication des intérêts légitimes poursuivis par le responsable du traitement lorsque le traitement est fondé sur cette base légale, la durée de conservation des données, le fait que le responsable du traitement a l'intention de transférer des données vers un pays tiers et l'existence d'une décision d'adéquation ou, le cas échéant, les garanties appropriées sur base desquelles le transfert aurait lieu, y compris comment avoir accès à ces garanties appropriées[27].

L'article 14, 2°, du projet de loi précise que le client de l'entité régulée devrait être informé au préalable par écrit « *des services sous-traités, du type de renseignements transmis dans le cadre de la sous-traitance et du pays d'établissement des entités prestataires des services sous-traités* » dans le cadre de la sous-traitance intragroupe.

S'agissant de la sous-traitance extragroupe, l'article 14, 3° du projet de loi obligerait l'entité régulée d'informer ses clients de « *la sous-traitance des services sous-traités, [au] type de renseignements transmis dans le cadre de la sous-traitance et [au] pays d'établissement des entités prestataires des services sous-traités* ».

Conformément à ses remarques relatives au consentement de la personne concernée, la CNPD estime que le projet de loi dans son état actuel ne permet au client ni de clairement prendre connaissance des conditions sous lesquelles la sous-traitance aurait lieu, ni de maîtriser ses données.

En effet, en vertu des règles actuelles établis par la CSSF

[25] Avis 15/2011 du Groupe de Travail « Article 29 » sur la définition du consentement (WP 187), p. 21.
[26] RGPD, art. 13, paragraphe (1).
[27] Ibidem, art. 13, paragraphe (1), lettre (d) et paragraphe (2).

dans la Circulaire CSSF 12/552, les clients doivent être informés de « *l'intérêt de [la] sous-traitance, de la spécificité de la finalité recherchée, du contenu de l'information transmise, du destinataire et de la localisation, ainsi que de la durée dans le temps* »[28], avant de donner leur accord à la levée du secret professionnel.

Ces informations sont davantage appropriées pour assurer que les clients soient clairement informés de la sous-traitance et les risques y associés. La CNPD estime nécessaire de modifier le projet de loi afin d'y prévoir que les clients doivent recevoir au moins les informations indiquées au point 193 de la Circulaire CSSF 12/552, sinon celles énumérées à l'article 14 du RGPD.

VI. Quant aux mesures de sécurité

Les banques et professionnels du secteur financier collectent et traitent une pléthore de données à caractères personnel relatives à leurs clients, y compris des données sensibles telles que des copies des pièces d'identité ou l'historique des transactions. Le traitement de ces données implique des risques non-négligeables, dans la mesure où la divulgation des données pourrait causer un préjudice grave aux clients. Ces risques augmentent avec l'utilisation accrue de nouveaux systèmes informatiques et de structures de sous-traitance de plus en plus complexes. En effet, en confiant leurs données à des sous-traitants, les entités surveillées « *pourraient perdre le contrôle exclusif de ces données …* »[29].

En permettant aux entités surveillées de recourir à la sous-traitance « simple » et à la sous-traitance en cascade, les nouvelles exceptions créées par le projet de loi engendrent dès lors des risques supplémentaires non-négligeables pour les entités surveillées et pour les clients.

Par ailleurs, les modifications apportées par le projet de loi sous avis ne se limitent pas à des exceptions au secret professionnel dans le cadre de la sous-traitance. Les paragraphes (3) et (4) de l'article 41 projeté reformulent les paragraphes (3) et (4) de l'article 41 actuellement en vigueur. Ils précisent que, dans certains cas, des renseignements pourraient être transmis à des autorités nationales, européennes et étrangères chargées de la surveillance prudentielle du secteur financier ou de résolution, ainsi qu'à des actionnaires ou associés. Ces transferts impliquent également des risques, dans la mesure où des données à caractère personnel pourraient être communiquées à des tiers.

Tenant compte de ces risques, la CNPD s'interroge sur l'absence dans l'article du projet de loi sous examen des indications relatives à des mesures de sécurité devant

[28] Circulaire CSSF 12/552, telle que modifiée, point 193.
[29] Avis 05/2012 du Groupe de Travail « Article 29 » sur l'informatique en nuage (WP 196), p. 6.

être mises en place par les entités régulées pour assurer la sécurité et la confidentialité des données.

En matière de la protection des données à caractère personnel, les articles 22 et 23 de la loi modifiée du 2 août 2002 obligent le responsable du traitement de mettre en place des mesures techniques et organisationnelles nécessaires afin d'assurer la protection des données à caractère personnel. Cette obligation est reprise à l'article 32 du RGPD, en application duquel le responsable du traitement doit mettre en œuvre les mesures appropriées afin de garantir un niveau de sécurité adapté au risque.

Eu égard au caractère sensible des données traitées, la CNPD suggère de préciser le texte du projet de loi en prévoyant que des mesures de sécurité doivent être mises en place par les entités surveillées lors de la sous-traitance et pour assurer la protection des données lors de la communication des données aux autorités, aux actionnaires et aux associés.

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

Ainsi décidé à Esch-sur-Alzette en date du 16 mars 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis relatif au projet de loi n°7044 portant réforme de l'Inspection générale de la Police, du projet de règlement de règlement grand-ducal relatif au fonctionnement de l'Inspection générale de la Police et au projet de loi n°7045 portant réforme de la Police grand-ducale

Délibération n°264/2017
du 24 mars 2017

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

Par courrier du 26 août 2016, Monsieur le Ministre de la Sécurité intérieure a invité la Commission nationale à se prononcer au sujet du projet de loi n°7044 portant réforme de l'Inspection générale de la Police et modifiant 1) la loi modifiée du 25 mars 2015 fixant le régime des traitements

et les conditions et modalités d'avancement des fonctionnaires de l'Etat 2) la loi modifiée du 25 mars 2015 instituant un régime de pension spécial transitoire pour les fonctionnaires de l'Etat et des communes ainsi que pour les agents de la Société nationale des Chemins de Fer luxembourgeois 3) Le livre Ier du Code de la sécurité sociale et au sujet du projet de règlement y relatif.

Par courrier du 26 août 2016, Monsieur le Ministre de la Sécurité intérieure a invité la Commission nationale à se prononcer également au sujet du projet de loi n°7045 portant réforme de la Police grand-ducale et abrogeant la loi du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

1) L'article 54 du projet de loi n°7045 est censé remplacer l'article 34-1 de la loi du 31 mai 1999 sur la Police et l'Inspection générale de la Police qui règle l'accès par la Police grand-ducale à un certain nombre de bases de données étatiques.

   En énumérant de manière limitative les bases de données auxquelles la Police grand-ducale a accès, l'article 54 satisfait à l'exigence constitutionnelle selon laquelle *« 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 »*[30].

   En application de ce principe, le Conseil d'Etat rappelle régulièrement dans ses avis que *« (…) l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.*

   La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication. (…) »[31].

2) En ce qui concerne l'article 54 du projet de loi n°7045 portant réforme de la Police grand-ducale, la Commission nationale se demande toutefois s'il est justifié que les bases de données auxquelles la Police grand-ducale a accès dans le cadre des missions de police administrative soient identiques à celles auxquelles elle a accès dans le cadre des

[30] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015.
[31] Voir par exemple : Conseil d'Etat, Avis n°6975/5 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.

missions de police judiciaire. En effet, les deux missions étant différentes à la base, on peut présumer que les bases de données auxquelles un officier de police judiciaire doit avoir accès ne sont pas tout-à-fait identiques à celles auxquelles un officier de police administrative doit avoir accès.

De manière générale, il faut retenir que plus le nombre de personnes accédant aux différents fichiers augmente, plus les risques en termes de protection des données augmentent aussi.

3) L'alinéa 3 de l'article 54 du projet de loi n°7045 prévoit que « *les données à caractère personnel des fichiers accessibles en vertu des alinéas 1 et 2 sont déterminées par règlement grand-ducal.* » Il aurait été judicieux de joindre en même temps un projet de projet de règlement grand-ducal au projet de loi sous examen, notamment au regard de l'extension du champ d'application de l'article 54 aux agents et officiers de police administrative. En l'absence d'un projet de texte, la CNPD n'est pas en mesure d'apprécier la nécessité et la proportionnalité des données accédées.

4) Si l'article 54 précité règle l'accès de la Police grand-ducale aux bases de données des administrations, le projet de loi n°7045 est muet sur les bases de données opérées par la Police elle-même.

Certes, l'article 17 de la loi modifiée du 2 août 2002 prévoit que font l'objet d'un règlement grand-ducal « *les traitements d'ordre général nécessaires à la prévention, à la recherche et à la constatation des infractions pénales qui sont réservés, conformément à leurs missions légales et réglementaires respectives, aux organes du corps de la police grand-ducale, de l'Inspection générale de la police et de l'administration des douanes et accises.* »

On peut cependant se poser la question de savoir si les éléments les plus essentiels des bases de données opérées par la Police ne devraient pas être déterminées par une loi, eu égard notamment à la jurisprudence précitée de la Cour constitutionnelle relative au cadrage normatif.

Par ailleurs, la question des traitements de données à caractère personnel effectuées par la Police est actuellement régie en grande partie 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 »). A ce titre, la CNPD réitère ses observations formulées maintes fois à cet égard dans ses avis antérieurs[32], à savoir que ce règlement ne répond plus aux exigences contemporaines en matière de protection des données et n'a pas été remplacé par un nouveau règlement sur base de l'article 17 de la loi modifiée du 2 août 2002 comme cela aurait dû être le cas.

Enfin, la loi modifiée du 2 août 2002 est vouée à disparaitre prochainement avec la mise en conformité de la législation luxembourgeoise au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

5) Parallèlement à l'article 54 du projet de loi n°7045, l'article 16 du projet de loi n°7044 portant réforme de l'Inspection générale de la Police devra remplacer l'article 77-1 de la loi du 31 mai 1999 sur la Police et l'Inspection générale de la Police qui règle l'accès par les agents de l'Inspection générale de la Police à un

[32] Par exemple :
- point 1.1. de l'avis du 17 novembre 2016 relatif au projet de loi n°6976 relatif à l'échange de données à caractère personnel et d'informations en matière policière https://cnpd.public.lu/fr/decisions-avis/2016/Echange-de-donnees-en-matiere-policiere/966-2016-echange-donnees-police.pdf
- point 3 de l'avis du 30 juillet 2015 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 https://cnpd.public.lu/fr/decisions-avis/2015/echange-usa-lux/366_2015_Deliberation_Ministere-Justice_avis-PL-6759_6762.pdf
- avis du 25 juillet 2013 relatif au projet de loi n°6566 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière https://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

certain nombre de bases de données étatiques, qui sont énumérées de manière limitative au paragraphe 1er de l'article 16.

L'article 16 ne précise cependant pas quelles sont les données (des bases de données y énumérées) auxquelles les agents de l'Inspection générale de la Police ont accès. A défaut de précisions, il faut admettre que l'accès couvre toutes les données, et cela même dans les cas où, en vertu de règlements grand-ducaux pris sur base de l'article 54 projeté de la future loi sur la Police, la Police grand-ducale n'aura accès qu'à une partie des données d'une des bases de données en question. La CNPD estime qu'un règlement grand-ducal devrait préciser les données des fichiers auxquelles les agents de l'Inspection générale de la Police auront accès, à l'instar de ce que prévoit le projet de loi n°7045.

6) L'article 16 paragraphe (3) du projet de projet de loi n°7044 permet à certains agents de l'Inspection générale de la Police d'avoir « *accès aux traitements des données à caractère personnel autorisés sur base de l'article 17 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et dont le responsable du traitement est le Directeur général de la Police, de même qu'aux fichiers de la Police autorisés sur base de l'article 12 de la même loi.*»

Eu égard aux principes énoncés au point 1) du présent avis, il conviendrait de déterminer de manière plus précise les bases de données de la Police grand-ducale auxquelles l'Inspection générale de la Police aura accès sur base de cette disposition.

Par ailleurs, comme cela a déjà été mentionné au point 4) du présent avis, la loi modifiée du 2 août 2002 à laquelle il est fait référence dans l'article 16 paragraphe (3) est vouée à disparaitre prochainement avec la mise en conformité de la législation luxembourgeoise au règlement (UE) 2016/679.

Enfin, comme relevé au même point 4), les traitements de données effectués à l'heure actuelle par la Police sont régis en partie 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 ») qui n'a pas été remplacé par un nouveau règlement sur base de l'article 17 de la loi modifiée du 2 août 2002.

7) En ce qui concerne la terminologie utilisée, l'article 16 paragraphe (3) du projet de loi n°7044 évoque l'accès « *aux fichiers de la Police autorisés sur base de l'article 12* » de la loi modifiée du 2 août 2002.

La Commission nationale tient à remarquer que l'article 12 de la loi modifiée du 2 août 2002 ne prévoit pas l'autorisation de traitements de données à caractère personnel par la CNPD, mais la notification de traitements de données par le responsable du traitement à la CNPD (et la détermination des traitements concernées), les traitements soumis à autorisation quant à eux étant réglés par l'article 14 de la même loi.

Rappelons à ce titre que les traitements soumis à notification en vertu de l'article 12 précité font l'objet d'une publication par la CNPD[33], mais - à la différence des traitements soumis à autorisation préalable en vertu de l'article 14 – ne font pas l'objet d'un contrôle de licéité préalable par la CNPD. Il n'est dès lors pas approprié d'utiliser le terme « autorisés » lorsqu'il est fait référence à l'article 12 de la loi modifiée du 2 août 2002.

8) L'article 54 alinéa 4 lettre (b) du projet de loi n°7045 et l'article 16 paragraphe (4) lettre (b) du projet de projet de loi n°7044 régissent les fichiers de journalisation des accès des agents de la Police grand-ducale, respectivement de l'Inspection générale de la Police aux bases de données des administrations.

La CNPD estime que le motif de la consultation devrait également être indiqué par l'agent au moment de la consultation et conservé, alors que les informations relatives aux agents ayant procédé à la consultation et les informations consultées, la date et l'heure de la consultation seules ne permettent pas forcément de retracer le motif de la consultation.

En ce qui concerne le délai de conservation, la CNPD est d'avis qu'il devrait être porté de trois ans à cinq ans. En effet, la prescription des infractions à la législation sur la protection des données (qui sont de nature correctionnelle) est de cinq ans. Or l'effacement des fichiers de journalisation après trois ans risque de rendre impossibles les poursuites judiciaires relatives à des infractions qui ne seraient pas encore prescrites.

La CNPD n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 24 mars 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

[33] Dans le régistre prévu à l'article 15 de la loi modifiée du 2 août 2002, registre consultable sur internet https://cnpd.public.lu/fr/registre/index.html

7 Annexes

Deuxième avis complémentaire relatif au projet de loi n°6921 portant :
1) modification du Code d'instruction criminelle,
2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques,
3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques,
4) adaptation de la procédure pénale face aux besoins liés à la menace terroriste

Délibération n°279/2017
du 30 mars 2017

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

Par courrier du 7 décembre 2016, Monsieur le Ministre de la Justice a fait parvenir à la CNPD des amendements concernant le projet de loi n°6921 portant 1) modification du Code d'instruction criminelle, 2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, 3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques,4) adaptation de la procédure pénale face aux besoins liés à la menace terroriste.

Pour rappel, la Commission nationale a rendu un premier avis relatif au projet de loi n°6921 en date du 12 février 2016 (délibération n°147/2016), ainsi qu'un avis relatif à une première série d'amendements gouvernementaux (délibération n°803/2016 du 14 septembre 2016).

1) article 24-1 du Code d'instruction criminelle (amendement 1)

La CNPD note avec satisfaction que la modification projetée de l'article 24-1 du Code d'instruction criminelle a été retirée du projet de loi pour être traitée dans le cadre du projet de loi n°6763.

Ledit projet n°6763 devrait d'ailleurs faire l'objet de profondes modifications substantielles, voire être remplacé ou complété par un nouveau projet de loi en raison de l'arrêt rendu par la Cour de justice de l'Union européenne dans les affaires jointes C-203/15 et C-698/15 en date du 21 décembre 2016.

2) article 39 du Code d'instruction criminelle (amendement 2)

La CNPD n'a pas d'observations à formuler concernant cet amendement.

3) article 48-26 projeté du Code d'instruction criminelle (amendement 3)

La CNPD salue que le texte modifié prévoit que l'enquête sous pseudonyme sera réservée aux officiers de police judiciaire spécialement habilités à cette fin par le Procureur Général d'Etat. Il est d'ailleurs fortement recommandé que les officiers de police judiciaire en question bénéficient d'une formation adaptée.

La CNPD partage la position du Conseil d'Etat qui estime que l'enquête sous pseudonyme devrait être réservée aux officiers de police judiciaire de la Police grand-ducale et ne devrait pas pouvoir être effectuée par des officiers de police judiciaire autres que ceux restrictivement énumérés à l'article 10 du code d'instruction criminelle.

De même, elle se rallie au Conseil d'Etat en ce qui concerne l'exigence d'une ordonnance judiciaire pour pouvoir effectuer une enquête sous pseudonyme.

La CNPD regrette cependant que – contrairement à ses suggestions faites au point 4.3. de son avis du 12 février 2016 - il ne soit pas expressément exclu qu'on ait recours, de manière délibérée, aux noms de personnes réellement existantes pour ce qui est des pseudonymes à utiliser.

4) article 48-27 projeté du Code d'instruction criminelle (amendement 4)

4.1.) Types de recherches pouvant être effectuées sur base de l'article 48-27 projeté

Suite aux amendements sous avis, l'accès aux données relatives aux abonnés ou utilisateurs de services de télécommunications et relatives à utilisation de ces services pourra se faire par les deux voies suivantes:

- en requérant le concours d'un opérateur de télécommunications ou d'un fournisseur d'un service de télécommunications

- au moyen d'un accès au fichier créé auprès de l'ILR en vertu de l'article 10bis projeté de la loi modifiée du 30 mai 2005

Dans son avis du 12 février 2016, la CNPD avait rendu attentif au caractère flou du texte en ce qui concerne les recherches pouvant être effectuées sur base de l'article 48-27 projeté.

Suite aux amendements gouvernementaux déposés en date du 8 août 2016, les choses semblent claires pour ce qui est des données pouvant être obtenues par le biais de l'accès au fichier créé auprès de l'ILR. En effet, les données détenues au départ par le magistrat ou officier de police judiciaire (fournies pour effectuer la recherche) et celles obtenues par le biais du fichier créé auprès de l'ILR doivent forcément faire partie de celles contenues dans la base de données et énumérées au deuxième paragraphe de l'article 10bis projeté de la loi modifiée du 30 mai 2005.

En revanche, la nature des recherches pouvant être effectuées auprès des opérateurs de télécommunications ou fournisseurs d'un service de télécommunications demeure floue.

Il pourrait s'agir en partie de recherches du même type que celles pouvant être effectuées par le biais de l'accès au fichier créé auprès de l'ILR, comme par exemple :

- la recherche du nom et de l'adresse de la personne [données recherchées] à partir du numéro de téléphone x [donnée de départ]

- la recherche de tous les numéros de téléphone [données recherchées] dont est titulaire une personne dénommée x habitant à une adresse y [données de départ]

Il pourrait cependant aussi s'agir de cas de figure dans lesquelles le lien entre l'information de départ et l'information recherchée ne peut se faire qu'au moyen de données de trafic de communications[34]. A titre d'exemple, on peut mentionner les hypothèses suivantes :

- la recherche du numéro de téléphone, du nom et de l'adresse d'une personne [données recherchées] ayant appelée le numéro de téléphone x [connu, donnée de départ] à telle ou telle heure précise [données de départ].

- la recherche du numéro IMEI de l'appareil [donnée recherchée] à l'origine de l'appel vers le numéro de téléphone x [connu, donnée de départ] à telle ou telle heure précise [données de départ].

- la recherche du numéro de téléphone, du nom et de l'adresse de personnes [données recherchées] ayant effectué des appels téléphoniques à partir du téléphone mobile doté du numéro IMEI x [données de départ]. (Les recherches via le numéro IMEI sont d'ailleurs citées comme exemple de l'utilisation déjà existante de l'article 46bis du Code d'instruction criminelle belge [ayant inspiré l'article 48-27 sous avis] dans les travaux parlementaires relatifs à sa modification en 2007.)[35]

- la recherche de l'adresse IP de l'ordinateur [donnée recherchée] s'étant connectée à messagerie électronique dotée de l'adresse e-mail x à un moment donné [données de départ]. D'ailleurs l'article 46bis du Code d'instruction criminelle belge a justement été modifié en 2007 et a eu la teneur reprise partiellement par l'article 48-27 projeté afin d'inclure les recherches d'adresses IP à partir des temps de connexions exacts[36].

Or, au regard de la jurisprudence récente de la Cour de justice de l'Union européenne en matière de rétention des données de trafic de communications, il semble qu'un tel recours aux données de trafic ne soit possible qu'après un contrôle préalable par une juridiction ou une autorité administrative indépendante[37]. Par ailleurs, il n'est guère justifiable qu'on utilise les données de trafic pour des enquêtes concernant tous crimes et délits et non seulement des crimes graves.

4.2.) Les cas d'extrême urgence

Dans son avis du 12 février 2016, la CNPD avait pointé le caractère imprécis de la notion d'extrême urgence alors que c'est la situation d'extrême urgence qui permet à un officier de police judiciaire de recourir aux mesures de l'article 48-27 projeté (avec l'accord oral d'un magistrat).

---

[34] A l'heure actuelle, les articles 24-1 et 67-1 du Code d'instruction criminelle devraient s'appliquer à ces cas de figure

[35] cf. le projet de loi 3 - 1824/1 (numéro de documents parlementaires du Sénat), commentaire des articles, Article 2, page 8 https://www.senate.be/www/webdriver?MItabObj=pdf&MIcolObj=pdf&MInamObj=pdfid&MItypeObj=application/pdf&MIvalObj=50335352

[36] Loi du 23 janvier 2007 modifiant l'article 46bis du Code d'instruction criminelle, cf. le projet de loi 3 - 1824/1 (numéro de documents parlementaires du Sénat), exposé des motifs, lettre A, page 2 https://www.senate.be/www/webdriver?MItabObj=pdf&MIcolObj=pdf&MInamObj=pdfid&MItypeObj=application/pdf&MIvalObj=50335352

[37] Voir l'arrêt rendu le 8 avril 2014 dans les affaires jointes C-293/12 et C-594/12, point 62 et l'arrêt rendu le 21 décembre 2016 dans les affaires jointes C-203/15 et C-698/15, point 120

Selon le commentaire des amendements, le texte inspiré de l'article 46bis du Code d'instruction criminelle belge vise des hypothèses telles que celle d'une victime d'une infraction grave sur le point de se commettre (telle une tentative de meurtre) lançant un appel d'urgence auprès de la Police ou celle d'une alerte à la bombe ou d'une prise d'otages.

L'amendement 4 remplace la formulation *« En cas d'extrême urgence »* par le passage suivant : *« Lorsqu'il existe une nécessité urgente de prévenir une atteinte grave à la vie, à la liberté ou à l'intégrité physique d'une personne ou lorsqu'il est impératif que les autorités qui procèdent à l'enquête agissent immédiatement pour éviter de compromettre sérieusement une procédure pénale … ».*

La CNPD comprend l'opportunité d'introduire une dérogation pour les cas de figure énumérés dans le commentaire des amendements (victime d'une infraction grave sur le point de se commettre telle une tentative de meurtre lançant un appel d'urgence auprès de la Police ou celles d'une alerte à la bombe ou d'une prise d'otages).

Ces hypothèses correspondent au premier cas d'ouverture de l'exception *« Lorsqu'il existe une nécessité urgente de prévenir une atteinte grave à la vie, à la liberté ou à l'intégrité physique d'une personne ».*

En revanche le deuxième cas d'ouverture *« lorsqu'il est impératif que les autorités qui procèdent à l'enquête agissent immédiatement pour éviter de compromettre sérieusement une procédure pénale »* semble très large et non justifiée au regard des finalités de cet alinéa telles qu'énoncées dans le commentaire des amendements. Cela est d'autant plus problématique que l'article 48-27 projeté s'applique à tous les crimes et délits indépendamment de leur gravité et non seulement aux crimes ayant trait au terrorisme.

Enfin, la CNPD partage la position du Conseil d'Etat qui estime que la mesure ne devrait pas pouvoir être effectuée par des officiers de police judiciaire autres que ceux énumérés à l'article 10 du Code d'instruction criminelle.

4.3.) Divers

La CNPD déplore que sa suggestion de soumettre le recours aux mesures de l'article 48-27 projeté à la condition qu'il soit *« nécessaire à la manifestation de la vérité »* n'a pas été retenu.

Par ailleurs, elle constate que le texte amendé ne comporte toujours pas de disposition particulière relative aux titulaires d'un secret professionnel.

5) articles 88-1 à 88-4 projetés du Code d'instruction criminelle (amendement 5)

5.1.) Protection du « Kernbereich privater Lebensgestaltung »

Dans son avis du 12 février 2016, la CNPD avait rendu attentif au concept d'un noyau dur de la vie privée, le *« Kernbereich privater Lebensgestaltung »* qui doit bénéficier d'une protection particulière aussi bien en matière de sonorisation qu'en matière de captation de données informatiques.

L'amendement 5 tente d'y répondre par l'alinéa qui suit : *« Les éléments de la communication qui ne sont pas pertinents pour l'instruction préparatoire ne peuvent être utilisés et leur enregistrement et leur transcription sont immédiatement détruits par le juge d'instruction. »*

Si l'insertion d'une disposition prévoyant l'effacement de données non nécessaires est louable, le texte amendé ne garantit pourtant pas une protection équivalente à celle du *« Kernbereich privater Lebensgestaltung »* existant en Allemagne.

Comme il a été relevé dans l'avis du 12 février 2016[38], suite à un arrêt de la Cour constitutionnelle allemande de 2004, la législation allemande s'appliquant en matière de sonorisation oblige d'une part l'autorité décidant de

[38] Point 7.1.

la mesure d'apprécier, dès le départ, l'atteinte à la vie privée et, d'autre part, impose le cas échéant une interruption de la mesure en fonction des circonstances.

En ce qui concerne la captation de données informatiques, un récent arrêt du Bundesverfassungsgericht[39] du 20 avril 2016 pose des conditions concernant la loi « BKA » dans le domaine de la lutte préventive contre le terrorisme, alors que la captation de données informatiques n'est pas prévue par le Code de procédure pénal allemand[40].

Ledit arrêt exige notamment que les informations obtenues par le biais de la captation soient visionnées par un organe indépendant avant de pouvoir être utilisées par les autorités répressives.

« Der Gesetzgeber hat insofern dem Schutzbedarf der Betroffenen durch Sicherungen auf der Aus- und Verwertungsebene Rechnung zu tragen und die Auswirkungen eines solchen Zugriffs zu minimieren. Entscheidende Bedeutung hierfür kommt dabei einer Sichtung durch eine unabhängige Stelle zu, die kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung durch das Bundeskriminalamt herausfiltert »[41].

Cette commission composée principalement de personnes indépendantes des autorités de sécurité visionnera et filtrera les données obtenues afin d'assurer la protection du «Kernbereich privater Lebensgestaltung» :

« Die verfassungsrechtlich gebotene Sichtung durch eine unabhängige Stelle dient neben der Rechtmäßigkeitskontrolle maßgeblich dem Ziel, kernbereichsrelevante Daten so frühzeitig herauszufiltern, dass sie den Sicherheitsbehörden nach Möglichkeit nicht offenbar werden. Dies setzt voraus, dass die Kontrolle im Wesentlichen von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen wird »[42].

5.2.) Sécurité en matière de captation de données informatiques

Dans son avis du 12 février 2016[43], la CNPD avait rendu attentif aux problèmes de sécurité considérables engendrés par la captation de données informatiques.

Les auteurs du projet tentent d'y remédier par le paragraphe suivant introduit par l'amendement 5 : *« Dans les cas visés à l'article 88-1, le jour, l'heure, la durée et, si nécessaire, le lieu de surveillance et du contrôle des télécommunications ou de la correspondance postale, de la sonorisation de certains lieux ou*

[39] BVerfG, Urteil des Ersten Senats vom 20. April 2016 - 1 BvR 966/09 - Rn. (1-29) http://www.bverfg.de/e/rs20160420_1bvr096609.html

[40] Et il semble que, selon la jurisprudence du Bundesgerichtshof, les dispositions existentes de la Strafprozessordnung ne permettent pas la captation des données informatiques Cf. BGH, 31.01.2007 - StB 18/06 http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=38779&pos=0&anz=1

[41] Point 220 de l'arrêt

[42] Point 224 de l'arrêt

[43] Point 7.3.

véhicules ou de la captation de données informatiques, ainsi que l'identité des personnes y ayant procédé sont indiqués et consignés dans un procès-verbal. »

Si l'alinéa cité ci-dessus constitue un avantage en termes de transparence, voire de procès équitable, il ne répond pourtant pas aux risques relatives à la sécurité des traitements effectués, ni ne permet de dissiper un certain flou entourant les scellés des enregistrements[44].

A titre de comparaison, on peut citer le futur article 269quater du Code de procédure pénale suisse[45] qui dispose ce qui suit :
« Art. 269quater Exigences posées aux programmes informatiques spéciaux de surveillance de la correspondance par télécommunication
1 Seuls peuvent être utilisés des programmes informatiques spéciaux qui génèrent un procès-verbal complet et inaltérable de la surveillance. Le procès-verbal est joint au dossier de la procédure.
2 Le transfert des données du système informatique surveillé à l'autorité de poursuite pénale compétente est sécurisé.
3 L'autorité de poursuite pénale s'assure que le code source peut être contrôlé, dans le but de vérifier que le programme ne contient que des fonctions admises par la loi. »

Si l'article susmentionné du Code de procédure pénale suisse est loin de résoudre tous les problèmes de sécurité liés à la captation de données informatiques, il a le mérite d'imposer au moins certaines exigences pour ce qui est des programmes informatiques utilisés par les autorités.

5.3.) Contenu des décisions ordonnant les mesures des articles 88-1 et suivants

Dans son avis du 12 février 2016[46], la CNPD avait suggéré que la loi exige que les décisions ordonnant la captation de données informatiques contiennent des informations relatives aux données à capter. En effet, le caractère attentatoire à la vie privée est très différent selon le type de données captées et les mesures précises de contrôle absolument nécessaires dans une affaire ne sont pas forcément les mêmes que celles nécessaires dans une autre affaire.

Selon les considérations générales des amendements gouvernements sous avis, une telle exigence se heurterait à des difficultés pratiques.

Si la CNPD comprend qu'il n'est pas opportun de déterminer, à l'avance, les données à capter de manière trop détaillée et précise, elle estime néanmoins qu'il serait indiqué d'exiger que la décision du juge d'instruction comprenne au moins une indication du type ou des catégories de données recherchées.

A titre d'exemple, on peut mentionner le futur article 269ter du Code de procédure pénale suisse[47] qui exige que l'ordre d'opérer la captation de données informatiques contienne le *« type de données qu'il*[48] *souhaite obtenir ».*

Le même article 269ter exige par ailleurs de manière expresse qu'en cas d'introduction dans un lieu non accessible au public, l'ordre d'opérer la mesure indique *« le local qui n'est pas public dans lequel il est, le cas échéant, nécessaire de pénétrer pour introduire des programmes informatiques spéciaux de surveillance de la correspondance par télécommunication dans le système informatique considéré »*, alors que l'article 88-3 projeté du Code d'instruction criminelle semble moins explicite à ce sujet. La CNPD suggère dès lors que l'ordonnance autorisant une introduction doive au moins indiquer l'adresse (en cas d'introduction dans une maison) ou le numéro d'immatriculation (en cas d'introduction dans une voiture).

5.4.) Information des personnes concernées

Dans son avis du 12 février 2016[49], la CNPD avait

---

[44] Cf l'avis de la CNPD du 12 février 2016, point 7.5.
[45] Article 269quater du Code de procédure pénale introduit par la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 18 mars 2016
https://www.admin.ch/opc/fr/federal-gazette/2016/1821.pdf
[46] point 7.2.
[47] Article 269ter du Code de procédure pénale introduit par la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 18 mars 2016
https://www.admin.ch/opc/fr/federal-gazette/2016/1821.pdf
[48] [le Procureur]
[49] point 7.6.1.

recommandé que la loi exige que doivent être informées non seulement la personne surveillée en vertu de l'ordonnance du juge d'instruction, mais aussi les autres personnes concernées comme par exemple des membres de famille cohabitant dans le même logement (faisant l'objet d'une sonorisation) ou utilisant le même ordinateur (faisant l'objet d'une captation de données informatiques) que la personne surveillée, dans l'hypothèse où ces autres personnes concernées sont connues.

Le texte amendé prévoit que soit informé également *« l'occupant des lieux soumis à une sonorisation »*. Selon le commentaire des amendements, il s'agit d'*« informer les habitants des lieux »*. La désignation de *« l'occupant »* (au singulier) dans le texte de l'amendement peut cependant prêter à confusion et pourrait ne viser qu'une personne déterminée (le locataire, l'occupant à titre précaire, le conjoint occupant le logement conjugal après une séparation …) et non tous les personnes habitant un logement et concernées par les mesures de sonorisation.

La CNPD regrette par ailleurs qu'en matière de captation de données informatiques, l'information reste limitée à la personne directement visée par l'ordonnance, alors que l'atteinte à la vie privée d'autres personnes concernées (par exemple cohabitant et utilisant le même ordinateur) inhérente à ce type de mesure peut être grave.

Il semble aussi y avoir une incohérence dans la mesure où des personnes habitant avec la personne surveillée seraient informées, si on a enregistré leurs conversations par le biais de microphones installés dans leur logement (sonorisation), mais qu'elles ne seraient pas informées si un résultat similaire est obtenu en activant les microphones des ordinateurs ou smartphones (captation de données informatiques) à l'intérieur de leur logement.

Enfin, la CNPD partage le souci du Conseil d'Etat concernant le risque que l'exercice d'un recours soit rendu impossible de fait, dans le cas où les données sont effacées avant que n'ait lieu l'information des intéressés eu égard aux délais de douze mois s'appliquant d'un côté à la destruction des enregistrements et de l'autre à l'information de la personne surveillée. Dès lors le texte devrait prévoir que l'information doit intervenir avant la destruction des enregistrements. Par ailleurs, un espace de temps permettant à la personne concernée d'exercer un recours devrait séparer le moment de l'information et celui de la destruction des enregistrements.

Pour le surplus la CNPD n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 30 mars 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis concernant le projet de règlement grand-ducal relatif à l'examen d'évaluation de la langue luxembourgeoise organisé dans le cadre des procédures d'acquisition de la nationalité luxembourgeoise

Délibération n°292/2017 du 7 avril 2017

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 8 mars 2017, le Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse (ci-après « le ministre ») a invité la Commission nationale à se prononcer au sujet du projet de règlement grand-ducal relatif à l'examen de la langue luxembourgeoise organisé dans le cadre des procédures d'acquisition de la nationalité luxembourgeoise (ci-après « le projet de règlement grand-ducal »).

Ce projet de règlement grand-ducal, pris en application de l'article 15 (3) de la loi du 8 mars 2017 sur la nationalité luxembourgeoise, encadre les modalités d'organisation de l'examen d'évaluation de la langue luxembourgeoise. Il confie à l'Institut national des langues (ci-après « l'Institut ») la mission d'organiser les sessions d'examen.

La CNPD regrette, à l'instar du Conseil d'Etat[50], que la saisine officielle concernant le projet de règlement grand-ducal soit intervenue tardivement, laissant ainsi des délais très serrés rendant difficile la prise en compte de ses observations.

La CNPD entend limiter ses observations aux dispositions du projet de règlement grand-ducal appelant des remarques particulières au regard de la loi modifiée du 2 août 2002, plus particulièrement aux articles 3, 7, 14 et 15 dudit projet de règlement grand-ducal.

Article 3 : Données collectées à des fins d'inscription à l'examen

L'article 3 du projet de règlement grand-ducal sous examen liste les informations et documents à fournir pour constituer un dossier d'inscription à l'examen. Le candidat doit fournir :

- le formulaire d'inscription établi par l'Institut, rempli et signé ;
- une photocopie de son passeport, ou à défaut, de sa

[50] Avis du Conseil d'Etat n°52.170 du 28 mars 2017

carte d'identité ou de son titre de voyage ;

- une photo récente en format passeport ;

- une copie du justificatif du paiement des frais d'inscription ;

- s'il y a lieu, sa demande motivée d'aménagement raisonnable de l'examen, pièces justificatives à l'appui.

S'agissant du formulaire d'inscription, la Commission nationale estime que ce document doit, a priori, limiter la collecte à des données objectives, strictement nécessaires à l'organisation de l'examen et aisément contrôlables par les intéressés grâce à l'exercice de leur droit d'accès. A cet égard, la CNPD relève que le formulaire d'inscription (version telle que disponible actuellement sur le site de l'Institut) permettra de collecter des données strictement nécessaires et proportionnées à la finalité poursuivie par le traitement en cause, à savoir : les données d'identification des personnes concernées (nom, prénoms), leurs coordonnées et moyens de contact (adresse, téléphone et/ ou adresse e-mail), leurs caractéristiques personnelles (nationalité, date et lieu de naissance, la langue maternelle), ainsi que des informations concernant les antécédents du candidat à l'Institut.

La CNPD tient à souligner qu'à titre facultatif uniquement, et sous réserve d'une information correspondante suffisante et préalable des personnes concernées, des données supplémentaires, non strictement nécessaires à l'organisation de l'examen, mais néanmoins utiles dans le cadre de l'analyse statistique des examens devant être réalisée annuellement par le ministre, en application de l'article 15 du projet de règlement grand-ducal[51], pourront être collectées.

A cet égard, la CNPD attire l'attention des auteurs du projet de règlement grand-ducal sur les dispositions de l'article 26 (1) (c) de la loi du 2 août 2002 prévoyant que les personnes concernées *« doivent être informées du fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse »*.
En l'espèce, cette distinction pourrait être réalisée par l'ajout d'un astérisque au niveau des informations obligatoires.

Enfin, la CNPD rappelle que ces données facultatives doivent rester proportionnées au regard de la finalité poursuivie[52] et qu'elles ne peuvent en aucun cas porter sur l'une des catégories particulières de données visées à l'article 6 (1) de la loi du 2 août 2002, c'est-à-dire qu'elles ne doivent pas être relatives aux infractions, condamnations ou mesures

[51] L'article 15 du projet de règlement grand-ducal dispose que *« Le ministre publie annuellement une analyse statistique des examens, indiquant le taux de réussite et d'échec »*.

[52] A titre d'exemple, des données concernant les autres langues parlées par le candidat ou sa profession pourraient être considérées comme pertinentes alors que des informations concernant la composition de son foyer ou son statut marital ne le seraient pas.

de sûreté ni faire apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, les convictions philosophiques ou religieuses, l'appartenance syndicale des personnes ni être relatives à la santé ou à la vie sexuelle de celles-ci.

S'agissant de la photocopie du passeport, ou à défaut, de la carte d'identité ou du titre de voyage du candidat, la CNPD note qu'en principe, une simple présentation du document d'identité et sa vérification de visu suffit pour s'assurer de l'identité d'une personne. La conservation d'une copie du document n'apparaît pas, d'une manière générale, justifiée. Toutefois, les relations à distance peuvent rendre nécessaire l'envoi d'une copie d'un document d'identité, dès lors que la vérification de l'identité ne peut se faire par un autre moyen. C'est par exemple le cas lorsque l'inscription à l'examen se fait par courrier ou en ligne. En l'absence de précisions de la part des auteurs du projet de règlement grand-ducal sur ce point, la Commission nationale estime qu'il sera ensuite de la responsabilité de l'Institut de supprimer la copie qui lui a été adressée au plus tard lors de la suppression des données du dossier de candidature (cf. les commentaires sous l'article 14).

S'agissant de la photo récente en format passeport, et après discussion avec le ministère, il ressort que la photo sera apposée sur la fiche de chaque candidat et ce afin que les examinateurs puissent vérifier qu'ils interrogent la bonne personne. A la lumière de ces explications, la CNPD estime que la collecte de la photo d'identité des candidats est proportionnée et légitime au regard des finalités poursuivies.

Néanmoins, la CNPD attire particulièrement l'attention des auteurs du texte sur le fait qu'une photographie numérique présente une particulière sensibilité, car elle permet à tout moment l'identification de la personne concernée sur la base de caractéristiques biologiques qui lui sont propres, permanentes et dont elle ne peut se défaire. Si une collecte de la photo d'identité au format papier des candidats pourrait apparaitre nécessaire et proportionnée, il est rappelé que la numérisation de ces photos et leur enregistrement systématique dans la base de données centralisée n'est a priori ni nécessaire, ni proportionné par rapport aux finalités poursuivies.

S'agissant des demandes motivées d'aménagement raisonnable de l'examen et des justificatifs y afférent, la CNPD attire l'attention des auteurs du règlement grand-ducal sur la particulière sensibilité des données contenues dans ces documents. Il conviendra dès lors de s'assurer que les données collectées ne concernent que les éléments objectifs et strictement nécessaires à l'évaluation des aménagements à mettre en œuvre.

La collecte d'une copie du justificatif du paiement des frais d'inscription n'appelle pas de remarque particulière.

Sous réserve des observations qui précèdent, la Commission nationale estime que les données collectées sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, conformément à l'article 4 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002.

Article 7 : Vérification d'identité dans la salle d'examen

Cet article prévoit que les candidats à l'examen doivent présenter leur convocation aux épreuves et leur passeport ou, à défaut, leur carte d'identité ou leur titre de voyage lors de leur admission en salle d'examen, et ce à des fins de vérification de leur identité. Cette vérification apparait nécessaire et proportionnée au but poursuivi.

Article 14 : Conservation des copies d'examen et des enregistrements des épreuves orales

Cet article prévoit que les copies d'examen ainsi que l'enregistrement des épreuves orales seront conservés pendant

une période de deux ans aux archives de l'Institut afin de servir de support en cas de contestation des résultats attribués par les examinateurs.

Le projet de règlement grand-ducal reste néanmoins silencieux quant à la durée de conservation de toutes les autres données personnelles collectées dans le cadre de l'organisation de l'examen de langue. Par ailleurs, il ne fournit pas non plus d'explication quant à la nécessité de conserver les copies d'examen et l'enregistrement des épreuves orales pendant une période de deux ans.

Si le règlement grand-ducal du 31 octobre 2008 concernant l'organisation des épreuves et l'attestation de la compétence de communication en langue luxembourgeoise parlée pour être admis à la naturalisation prévoit dans son article 9 que la *« durée de validité du certificat est limitée à deux ans à partir de la date figurant sur le certificat »*, ni le projet de règlement grand-ducal ici commenté, ni la loi du 8 mars 2017 sur la nationalité luxembourgeoise, ne prévoient une telle durée de validité.

En l'espèce, et compte tenu des éléments susmentionnés, la CNPD se demande, à l'instar du Conseil d'Etat[53], si la conservation des copies d'examen et des enregistrements des épreuves orales pour une durée de trois mois à compter de la communication des résultats aux candidats, ne serait pas suffisante à la finalité poursuivie.

Pour ce qui concerne les autres données comprises dans le dossier de candidature, et considérant que les candidats ont constitué le dossier dans l'unique but de passer l'examen, ces derniers peuvent légitimement s'attendre à ce que leurs données soient effacées ou anonymisées dans un délai raisonnable. C'est pourquoi, la CNPD est d'avis que ces données pourront être conservées jusqu'à trois mois après l'annonce des résultats de l'examen et le cas échéant, la transmission du certificat de réussite/échec.

Dans l'hypothèse où l'Institut envisagerait de conserver les données pour une durée plus longue, la CNPD recommande de recueillir leur consentement préalable[54], étant précisé que le candidat faisant valoir son droit de report d'inscription prévu à l'article 4 (2) du projet de règlement grand-ducal[55] consent à ce que son dossier d'inscription soit conservé jusqu'à la prochaine session d'examen.

Pour ce qui concerne les attestations de réussite, la CNPD est d'avis que l'Institut peut légitiment les conserver pendant toute la durée de validité de l'examen, notamment afin de permettre la délivrance de copies en cas de perte ou de vol. A cet égard, la CNPD considère

[53] Le Conseil d'Etat souligne dans son avis n°52.170 qu'il ne voit pas l'utilité de conserver ces documents pendant une durée de deux ans alors que le délai de recours administratif de droit commun de trois mois s'applique en la matière.
[54] Cela pourrait être utile pour les candidats ayant échoué et souhaitant se représenter à l'examen.
[55] *« Tout candidat peut, sur demande écrite, demander le report de son inscription à une session d'examen ultérieure ».*

qu'il pourrait être opportun de préciser la durée de validité de l'examen dans le projet de règlement grand-ducal à l'instar du règlement grand-ducal du 21 octobre 2008 précité.

Pour finir, la CNPD note que l'article 10 (2) du projet de règlement grand-ducal prévoit qu'un candidat exclu d'une session d'examen ne peut déposer un nouveau dossier d'inscription qu'à l'expiration d'un délai de douze mois à compter de la décision d'exclusion. Pour autant que cette disposition perdure dans la version finale du projet[56], la CNPD est d'avis que l'Institut est légitime à conserver la décision et les données personnelles y contenues pendant toute la durée de la sanction, à savoir 12 mois.

Article 15: Mission de statistiques

Cet article prévoit la réalisation et la publication de statistiques indiquant les taux de réussite et d'échec à l'examen. La CNPD rappelle que ces statistiques doivent être réalisées avec des données anonymisées, de sorte qu'il soit impossible d'établir un lien avec une personne physique en particulier. La CNPD réitère par ailleurs ses remarques et réserves formulées sous l'article 3 point (1) du projet de règlement grand-ducal, en ce qui concerne la collecte de données à des fins de statistique.

A titre subsidiaire, la Commission nationale observe que le projet de règlement grand-ducal est silencieux quant aux modalités d'information des personnes concernées. Elle rappelle, conformément aux articles 26 à 31 de la loi modifiée du 2 août 2002, que les personnes concernées doivent être informées des finalités du traitement, des destinataires des données, ainsi que des modalités d'exercice de leurs droits. Dans cet objectif, il est recommandé de préciser ces informations par écrit au plus tard lors de la collecte des données (par exemple dans le formulaire d'inscription).

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

Ainsi décidé à Esch-sur-Alzette en date du 7 avril 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Troisième avis complémentaire de la Commission nationale pour la protection des données relatif au projet de loi n°6921 adaptant la procédure pénale aux besoins liés à la menace terroriste portant :
1) modification de procédure pénale,
2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques,
3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques

Délibération n°395/2017 du 10 mai 2017

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

Par courrier du 7 avril 2017, Monsieur le Ministre de la Justice a fait parvenir à la CNPD des amendements concernant le projet de loi n°6921 adaptant

[56] A cet égard, le Conseil d'Etat attire l'attention des auteurs du texte sur le fait que ladite disposition risque d'encourir la sanction de l'article 95 de la constitution.

la procédure pénale aux besoins liés à la menace terroriste portant 1) modification du Code de procédure pénale, 2) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, 3) modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques.

Pour rappel, la Commission nationale a rendu un premier avis relatif au projet de loi n°6921 en date du 12 février 2016 (délibération n°147/2016), ainsi que deux avis relatifs à de précédents amendements gouvernementaux (délibération n°803/2016 du 14 septembre 2016 et délibération n°279/2017 du 30 mars 2017).

1) article 48-13 du Code de procédure pénale

La CNPD peut approuver la modification projetée de l'article 48-13 dans la mesure où elle clarifie la portée des mesures pouvant être effectuées sur la base de cet article.

2) article 48-26 projeté du Code de procédure pénale

L'article 48-26 paragraphe (1) projeté du Code de procédure pénale prévoit désormais que l'enquête sous pseudonyme est effectuée par des officiers de police judiciaire sur décision du procureur d'Etat ou du juge d'instruction.

En ce qui concerne le cas de figure d'une enquête sous pseudonyme effectuée en dehors d'une instruction judiciaire, la CNPD suggère de recourir à une procédure similaire à celle prévue par l'article 24-1 du Code de procédure pénale en matière de perquisition et de repérage de données de télécommunications afin de garantir un contrôle judiciaire préalable de l'enquête sous pseudonyme qui semble être très intrusive dans la vie privée.

Selon le paragraphe (3), la décision d'opérer l'enquête sous pseudonyme doit être écrite et contenir un certain nombre de mentions. Par dérogation, selon le paragraphe (4), la décision peut être orale en cas d'urgence. La CNPD aimerait rendre attentif au caractère vague de la notion de l'urgence (tout comme elle l'avait fait dans son premier avis du 12 février 2016 à propos de la condition de l'« *extrême urgence* » ayant figuré dans la version initiale de l'article 48-27 projeté du Code de procédure pénale).

Enfin, la CNPD note que, dans le point 2. de l'article 48-26 paragraphe (1) projeté du Code de procédure pénale, il est désormais expressément exclu qu'on ait recours, de manière délibérée, aux noms de personnes réellement existantes pour ce qui est des pseudonymes

à utiliser (sauf accord des personnes concernées). Elle s'interroge cependant sur la portée de cette interdiction puisque le point 1. du même article permet de « *participer sous un pseudonyme aux échanges électroniques* » sans poser les mêmes conditions que le point 2.

3) article 48-27 projeté du Code de procédure pénale

La CNPD note avec satisfaction que la mesure ne va pas pouvoir être effectuée par des officiers de police judiciaire autres que ceux énumérés à l'article 10 du Code d'instruction criminelle.

Pour le reste, elle se permet de renvoyer aux développements exposés dans ses précédents avis et plus particulièrement au point 4) de l'avis du 30 mars 2017 (délibération n°279/2017).

4) articles 88-1 à 88-4 projetés du Code de procédure pénale

4.1.) Les amendements sous avis introduisent la possibilité d'ordonner une fixation d'images à l'intérieur de maisons ou de véhicules notamment. La sonorisation tout comme la fixation d'images sont prévues par le même tiret de l'article 88-1 paragraphe (1) projeté. La CNPD se demande si cela signifie que les deux mesures sont toujours ordonnées simultanément ou s'il est à la discrétion des agents effectuant la mesure de choisir la forme de la surveillance opérée.

Comme elle l'a déjà souligné à propos de la captation de données informatiques[57], la CNPD plaide en faveur d'une obligation à charge du juge d'instruction décidant de la mesure de préciser, dans l'ordonnance, la nature des données à capter ou enregistrer. De telles précisions permettent de mieux adapter les mesures effectuées aux besoins de l'instruction et, par-là, de mieux respecter le principe de proportionnalité.

4.2.) A l'article 88-2 paragraphe (2) lettre a), la fixation d'images n'est pas mentionnée parmi les mesures possibles exclusivement dans le contexte d'infractions ayant trait au terrorisme tels qu'énumérées à l'article 88-2 paragraphe (2) lettre a) points 1. et 2. Si la sonorisation et la fixation d'images sont considérées comme deux mesures distinctes pouvant être ordonnées séparément, alors la fixation d'images pourrait être mise en place pour tous faits emportant une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à deux ans d'emprisonnement. Aux yeux de la CNPD, une utilisation aussi large de la fixation d'images parait disproportionnée. Elle suggère dès lors de rajouter la fixation d'images aux mesures ne pouvant être effectuées que dans le contexte d'infractions ayant trait au terrorisme (au même titre que la sonorisation et la captation de données informatiques).

4.3.) De même, en ce qui concerne l'information des personnes concernées habitant le même logement que la personne directement visée par la mesure, l'article 88-4 paragraphe (6) ne mentionne que l'hypothèse de la sonorisation et non celle la fixation d'images. La CNPD suggère d'y rajouter la fixation d'images (tout comme, en fonction des circonstances, la captation de données informatiques[58]).

4.4.) En ce qui concerne les mesures de sécurité, l'article 88-4 paragraphe (3) alinéa 3 prévoit désormais que « *les moyens appropriés sont utilisés pour garantir l'intégrité et la confidentialité des télécommunications, correspondances postales, images, conversations ou données enregistrées ou interceptées* ». La CNPD trouve cette formulation des « moyens appropriés » particulièrement vague compte tenu de l'ampleur des risques en matière de sécurité non seulement après l'obtention des données par les autorités judiciaires mais aussi et surtout en amont, au stade de collecte des données[59], et elle continue de plaider pour l'insertion de plus de précisions dans ce contexte[60].

---

[57] Cf le point 7.2. de l'avis n°147/2016 du 12 février 2016 et le point 5.3.) de l'avis n°279/2017 du 30 mars 2017.
[58] Cf le point 7.6.1. de l'avis n°147/2016 du 12 février 2016 et le point 5.4.) de l'avis n°279/2017 du 30 mars 2017.
[59] Cf le point 7.3. de l'avis n°147/2016 du 12 février 2016
[60] Cf le point 5.2.) de l'avis n°279/2017 du 30 mars 2017

4.5.) Un nouvel article 88-4 paragraphe (1) alinéas 2 et 3 prévoit ce qui suit : « *Le juge d'instruction peut ordonner, directement ou par l'intermédiaire du Service de police judiciaire, aux personnes dont il présume qu'elles ont une connaissance particulière du service de télécommunications qui fait l'objet d'une mesure de surveillance ou des services qui permettent de protéger ou de crypter les données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'accéder au contenu de la télécommunication qui est ou a été transmise, dans une forme compréhensible. Il peut ordonner aux personnes visées à l'alinéa qui précède de rendre accessible le contenu de la télécommunication, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.* » La CNPD s'interroge sur la portée de ce ces deux alinéas. Est-ce que, par exemple, un professeur en informatique, un fonctionnaire de la CNPD ou un membre d'une ONG militant pour la sécurité informatique et le cryptage de données pourraient, en quelque sorte, être réquisitionnés, sous peine d'amende[61], pour assister les autorités judiciaires dans l'application des futurs articles 88-1 à 88-4 du Code de procédure pénale ?

En revanche, si la mesure vise uniquement les entreprises du secteur des télécommunications comme le suggère le commentaire des amendements, pourquoi ne pas le préciser dans le texte de l'article ?
La CNPD note également que les mesures prévues aux article 88-4 paragraphe (1) alinéas 2 et 3 projetées ne sont pas réservées de manière exclusive à l'instruction de faits ayant trait au terrorisme tels qu'énumérées à l'article 88-2 paragraphe (2) lettre a) points 1. et 2.

4.6.) Enfin, la CNPD constate que désormais, davantage de conditions prévues aux articles 88-1 à 88-4 projetés du Code de procédure pénale sont prescrites à peine de nullité. Cependant, tel n'est toujours pas le cas pour toutes les conditions et, en particulier, pour les différentes conditions prévues aux articles 88-2 paragraphes (1) à (3) qui sont justement censées garantir que les mesures extrêmement intrusives des articles 88-1 à 88-4 projetés ne peuvent être opérées qu'en cas de nécessité absolue.

5) article 10 bis projeté de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

La CNPD approuve la suppression de la mention de l'accès au fichier de l'Institut

[61] Les amendes étant prévues article 88-4 paragraphe (1) alinéa dernier.

luxembourgeois de régulation accordé au central des secours d'urgence 112 ainsi qu'à la centrale du service d'incendie et de sauvetage de la Ville de Luxembourg. Cette suppression reprend une suggestion que la CNPD a formulée dans son avis initial et qui a été reprise par le Conseil d'Etat dans son avis du 7 février 2017.

Pour le surplus la CNPD n'a pas d'autres observations à formuler.

Ainsi décidé à Esch-sur-Alzette en date du 10 mai 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis de la Commission nationale pour la protection des données relatif au projet de loi sur la déclaration obligatoire de certaines maladies dans le cadre de la santé publique

Délibération n°401/2017 du 10 mai 2017

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

Par courrier en date du 20 décembre 2016, Madame la Ministre de la Santé a invité la Commission nationale à se prononcer sur un projet de loi concernant la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique (ci-après « le projet de loi »)[62].

Ce projet de loi est accompagné d'un règlement grand-ducal portant exécution de ladite loi et abrogeant le règlement grand-ducal du 10 septembre 2004 portant désignation des maladies infectieuses ou transmissibles sujettes à déclaration obligatoire.

Le projet de loi a pour objectif d'« *améliorer le système de surveillance des maladies infectieuses au Grand-Duché de Luxembourg et de regrouper les données portant sur les maladies infectieuses dans un système centralisé* »[63]. Il entend améliorer la qualité des données nécessaires à la surveillance épidémiologique au niveau national.

La Commission nationale entend limiter ses observations aux dispositions du projet de loi ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel.

VII. L'organisation de la surveillance des maladies infectieuses au Grand-Duché de Luxembourg

Le projet de loi modifie en profondeur le dispositif de collecte des données individuelles nécessaires à la surveillance des maladies infectieuses au Luxembourg. L'exposé des motifs précise que « *contrairement à d'autres Etats sur le continent européen, et plus particulièrement au sein de l'Union européenne, qui souvent disposent d'un institut de surveillance de santé publique*

[62] Ce projet de loi tend également à modifier :
- la loi modifiée du 29 avril 1983 concernant l'exercice des professions de médecin, de médecin-dentiste et de médecin-vétérinaire ;
- la loi modifiée du 16 juillet 1984 relative aux laboratoires d'analyses médicales ;
- la loi modifiée du 16 janvier 1990 relative aux dispositifs médicaux.

[63] *cf.* Exposé des motifs du projet de loi sous examen, p. 2.

unique spécialisé en la matière, la fonction de surveillance des maladies infectieuses a jusqu'à présent été remplie par trois institutions au Grand-Duché de Luxembourg :

- *le Laboratoire national de santé : le département de microbiologie pour les pathogènes entériques, le bioterrorisme, la tuberculose, la grippe ;*

- *la Direction de la Santé (Division de l'Inspection Sanitaire) pour les déclarations obligatoires selon le cadre légal de l'activité médicale ;*

- *l'ancien CRP-Santé : le laboratoire de rétrovirologie et d'immunologie du « Luxembourg Institute of Health » (LIH) pour la surveillance du HIV et de la rougeole/rubéole. »*

L'exposé des motifs précise en outre que « *cette division reposait plutôt sur un arrangement pratique, sans base légale, réglementaire ou ministérielle entre les responsables des services concernés* ».

Le dispositif actuellement en place et issu de la loi modifiée du 29 avril 1983 concernant l'exercice des professions de médecin, de médecin-dentiste et de médecin-vétérinaire ne permettant pas de collecter l'ensemble des données nécessaires à une surveillance épidémiologique exhaustive et centralisée, le projet de loi entend élargir le cercle des acteurs tenus de fournir les données nécessaires à une surveillance épidémiologique efficace, notamment par une implication des laboratoires de biologie clinique privés et hospitaliers, qui disposent de données microbiologiques indispensables.

La CNPD note à cet égard qu'en application de l'article 8 du projet de loi, le ministre ayant la Santé dans ses attributions aura la possibilité de désigner des laboratoires de référence pour certaines souches bactériennes, virales ou parasitaires, afin de permettre l'identification ou la confirmation rapide de la nature d'agents biologiques infectieux spécifiques.

Elle relève en outre que le dispositif proposé par les rédacteurs du projet de loi vise à centraliser dans une base de données nationale, gérée par la Direction de la Santé, l'ensemble des données concernant les maladies à déclaration obligatoire.

Elle note, à cet égard, que la loi du 24 novembre 2015[64] a expressément conféré à la Direction de la santé les missions suivantes :

- « *protéger et promouvoir la santé en tant que bien-être général sur les plans physique, psychique et social ;*

[64] *cf.* Loi du 24 novembre 2015 modifiant la loi modifiée du 21 novembre 1980 portant organisation de la Direction de la santé et la loi modifiée du 16 août 1968 portant création d'un Centre de logopédie et de services audiométrique et orthophonique.

- *étudier et surveiller et évaluer l'état de santé de la population et exécuter des mesures de santé publique, y compris les mesures d'urgence nécessaires à la protection de la santé.* »

Dès lors que la loi détermine les finalités et les moyens du traitement en cause, dont elle confie la responsabilité à la Direction de la santé, cette dernière doit être considérée comme le responsable de traitement au sens de l'article 2 lettre (n) de la loi modifiée du 2 août 2002.

VIII. Les finalités du système de surveillance des maladies infectieuses

Pour ce faire, l'article 1er du projet de loi instaure un principe de transmission obligatoire de données individuelles au Directeur de la Santé ou à son délégué par les médecins, les médecins-dentistes et les responsables des laboratoires d'analyses de biologie médicale pour les catégories suivantes de maladies à déclaration obligatoire[65] :

- les maladies qui nécessitent une intervention urgente locale, nationale ou internationale ;

- les maladies dont la surveillance est nécessaire à la conduite et à l'évaluation de la politique de santé publique ;

- les maladies qui doivent être rapportées aux organisations internationales dont l'Organisation Mondiale de la Santé (OMS), le Centre européen de prévention et de contrôle des maladies (« *European Centre for Disease Prevention and Control* » ou « ECDC »)[66].

La CNPD observe que l'Etat a « *une obligation d'organiser un système de prévention, de surveillance, et de contrôle pour protéger ses citoyens contre ces menaces microbiennes* »[67] et contre le risque infectieux. L'exposé des motifs du projet de loi précise en outre les objectifs de la surveillance centralisée des maladies à déclaration obligatoire instaurée par le projet de loi[68], à savoir la « *surveillance de maladies infectieuses d'un intérêt de santé publique particulier (notamment des maladies pour lesquelles il existe des activités de surveillance auprès de l'ECDC)* », l'« *identification d'épidémies ou de problèmes sanitaires touchant un nombre élevé de résidents* », l'« *identification d'événements rares ou risques infectieux émergents* », la « *surveillance de l'efficacité des programmes de vaccination* », la « *surveillance de résistance aux antibiotiques* » et l'« *échange de données pertinentes avec les instances internationales : OMS, ECDC* ».

La Commission nationale estime que les finalités poursuivies par le traitement de données sous-jacents à cette surveillance sont déterminées, explicites et légitimes, conformément à l'article 4 paragraphe (1) lettre (a) de la loi modifiée du 2 août 2002.

IX. Les données traitées

Les articles 2 et 3 du projet de loi définissent les informations minimales à déclarer ainsi que les modalités de cette déclaration par les médecins et médecins-dentistes, d'une part, et par les responsables de laboratoire d'analyse de biologie médicale, d'autre part.

La Commission nationale note, en application des articles 2 et 3 précités du projet de loi, que les informations minimales à transmettre ainsi que les modalités de cette transmission diffèrent selon la catégorie de professionnels de santé visés par le dispositif de déclaration obligatoire.

Les catégories de données devant être impérativement transmises par les professionnels de santé susmentionnés dans leurs déclarations sont les suivantes :

- les initiales du patient dans le cas des maladies marquées d'un astérisque dans le projet de règlement grand-ducal[69], ou dans les autres cas de maladie son nom, son prénom et son adresse ;

---

[65] L'article 1er du projet de loi renvoie à un règlement grand-ducal le soin d'établir la liste précise des maladies à déclaration obligatoire susmentionnées.

[66] Le Règlement (CE) n°851/2004 du Parlement européen et du Conseil du 21 avril 2004 instituant un Centre européen de prévention et de contrôle des maladies a institué une agence européenne indépendante de prévention et de contrôle des maladies, ayant pour mission de déceler, d'évaluer et de communiquer les menaces actuelles et émergentes que des maladies transmissibles représentent pour la santé.

[67] *cf.* Exposé des motifs p. 1.

[68] *cf.* Exposé des motifs p. 3.

[69] Parmi les maladies à déclaration obligatoire, les maladies sexuellement transmissibles sont marquées d'un astérisque dans le projet de règlement grand-ducal joint au projet de loi. Il s'agit des maladies suivantes : « Chlamydiose (Chlamydia trachomatis) », « Gonorrhée (Neisseria gonorrhoeae) », « Infection HIV », « SIDA », « Syphilis (Treponema pallidum) y compris Syphilis congénitale ».

- les caractéristiques personnelles : date de naissance et sexe

- les données relatives à la santé des personnes (« diagnostic » ; « date des premiers symptômes », « date du diagnostic », « pays d'origine de la maladie », « source d'infection si connue », « date de prélèvement », « origine du prélèvement »)

- des souches bactériennes, virales ou parasitaires isolées d'un patient ou du matériel biologique prélevé sur un patient[70], dans le cas des laboratoires d'analyses de biologie médicale.

La Commission nationale rappelle qu'en application de l'article 4 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002, seules doivent être collectées les informations pertinentes et nécessaires au regard des objectifs poursuivis par le traitement. Elle est par ailleurs d'avis que la protection de la confidentialité et la sécurité de leurs données à caractère personnel constituent des enjeux majeurs du dispositif de signalement des maladies à déclaration obligatoire.
Elle estime qu'il revient à la Direction de la Santé, chargée de la surveillance d'étudier, de surveiller et d'évaluer l'état de santé de la population, de garantir un niveau particulièrement élevé de protection de la confidentialité et de la sécurité des données des personnes concernées.

En l'absence de précisions sur les techniques utilisées, la Commission nationale n'est pas en mesure d'apprécier si le dispositif envisagé satisfait aux exigences de confidentialité et de sécurité des données traitées. Elle estime que des mesures spécifiques de protection de l'identité des patients devraient être mises en œuvre. Sur ce point, la CNPD observe que les auteurs du projet de loi se sont inspirés pour la rédaction de l'article 1er du projet de loi de l'article L. 3113-1 du code de la santé publique français, sans toutefois en reprendre le principe selon lequel l'anonymat des personnes doit être protégé.

L'exposé des motifs précise qu'*« afin d'éviter les doubles notifications, et de permettre l'investigation d'épidémies ou d'alertes, les déclarations doivent être nominatives, mais la confidentialité et la sécurité du traitement des données personnelles doivent être strictement garanties par l'ensemble des acteurs impliqués »*[71]. Compte tenu des risques sanitaires encourus, la CNPD peut tout à fait comprendre le souci d'éviter les doublons dans le cadre de la surveillance des maladies infectieuses, l'existence de tels doublons pouvant limiter l'efficacité du dispositif de surveillance. Elle se demande

[70] Les articles 6 et 7du projet de loi encadrent les hypothèses où une souche isolée ou du matériel biologique à partir duquel le diagnostic a été établi doit être transféré par le laboratoire d'analyses de biologie médicale au laboratoire nationale de référence, et ce dans un bref délai.
[71] *cf.* Exposé des motifs, p. 3.

toutefois si le recours aux données nominatives des patients pour écarter les doublons est véritablement proportionné et nécessaire compte tenu des autres données dont dispose déjà la Direction de la Santé. La CNPD note d'ailleurs que dans le cas des maladies sexuellement transmissibles, seules les initiales du patient seront collectées (« *pour les maladies marquées d'un astérisque dans le règlement grand-ducal visé à l'article 1er* » du projet de loi), alors même que l'impératif d'écarter les doublons demeure dans ces cas de figure. Dès lors, en l'absence de justification de la collecte systématique des nom, prénom et adresse des patients dans le cas des maladies non marquées d'un astérisque dans le projet de règlement grand-ducal et compte tenu du risque important que représente l'association de ces données d'identification à des données sensibles concernant la santé des personnes, la CNPD estime nécessaire que la collecte des données d'identification des patients se limite à leurs initiales, ce qui harmoniserait par ailleurs le régime de collecte de l'ensemble des cas de maladies à déclaration obligatoire. Elle considère par ailleurs, s'agissant des maladies non marquées d'un astérisque dans le projet de règlement grand-ducal, que la transmission systématique de l'adresse du patient n'est pas pertinente.

Au vu des observations qui précèdent et compte tenu de l'extrême sensibilité des données collectées, la Commission nationale est à se demander si la mise en place de mesures d'anonymisation irréversible des données, passé un certain délai, ne serait pas de nature à garantir une meilleure protection des personnes à l'égard de leurs données à caractère personnel, à l'instar de la procédure de gestion des données prévues par le code de la santé publique français. A cet égard, la CNPD pourrait comprendre la nécessité de pseudonymiser les données, dans un premier temps, afin de pouvoir ré-identifier un patient en cas de besoin particulier lié à la surveillance et au suivi des maladies à déclaration obligatoire. Toutefois, dans un second temps, l'utilisation de données épidémiologiques expurgées de toute donnée directement ou indirectement identifiantes pourrait être suffisante pour permettre à la Direction de la Santé de remplir sa mission de surveillance des maladies infectieuses.

Par ailleurs, la Commission nationale se demande, si la collecte de la date de naissance entière (jour/mois/année) est systématiquement nécessaire ou si cette collecte pourrait, au moins dans certaines hypothèses (patients adultes) se limiter à l'année de naissance ou à défaut au mois et à l'année de naissance.

En outre, la CNPD observe qu'il ne ressort pas clairement du projet de loi si des données concernant les professionnels de santé déclarants seront collectées dans le cadre du dispositif de déclaration obligatoire. Le cas échéant, la CNPD estime que le projet de loi devrait être complété sur ce point et qu'il devrait détailler les catégories de données traitées s'agissant de ces personnes.

Enfin, la CNPD note que l'article 5 du projet de loi précise qu'un règlement grand-ducal peut arrêter, sur avis du Conseil supérieur des maladies infectieuses, des formulaires spécifiques afin de structurer la transmission des données et présume qu'elle sera saisie pour avis en temps utile du projet de règlement grand-ducal susmentionné.

X. La durée de conservation des données

Le projet de loi est silencieux sur ce point.

La Commission nationale rappelle qu'en application de l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002, les données traitées doivent 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 ont été collectées* ». S'agissant

d'une matière réservée à la loi par la Constitution, l'essentiel du cadrage normatif doit résulter de la loi formelle. Une durée de conservation des données doit, par conséquent, être définie par la loi, au regard des finalités de la surveillance épidémiologique individuelle et collective.

En cas de recours à des techniques de pseudonymisation ou d'anonymisation des données, la Commission nationale invite également le responsable du traitement à préciser les conditions de conservation des données (le cas échéant, établissement d'une table de correspondance, auprès de qui cette table doit être conservée, pendant combien de temps et dans quelles conditions de sécurité).

Sous réserve des observations qui précèdent, la Commission nationale estime que les données collectées dans le cadre du dispositif de surveillance épidémiologique n'appellent pas d'observations particulières.

XI. L'information et les droits des personnes

Le droit à l'information

La CNPD rappelle qu'en application de l'article 26 paragraphe (1) de la loi modifiée du 2 août 2002, toute personne a le droit de savoir si des données la concernant font l'objet d'un traitement et en quoi consiste ce traitement. Elle note que le projet de loi est silencieux sur ce point.

Elle estime que le médecin ou le laboratoire qui signale une maladie à déclaration obligatoire devra en informer les personnes concernées, et ce au moment de l'annonce du diagnostic ou au moment qu'il jugera, en conscience, le plus opportun. Il devra notamment leur préciser quelles données seront transmises à l'autorité sanitaire et le caractère anonyme de la transmission. Un document d'information individuelle, dont le modèle pourrait être établi par l'autorité sanitaire, pourrait également être remis aux personnes concernées, expliquant notamment à quoi sert le dispositif de déclaration obligatoire et comportant les mentions requises par l'article 26 précité de la loi modifiée du 2 août 2002.

Le droit d'accès

La CNPD rappelle qu'en application de l'article 28 de la loi modifiée du 2 août 2002, toute personne dispose d'un droit d'accès aux données la concernant. Elle note toutefois que le projet de loi est silencieux sur ce point.

La CNPD estime que les personnes concernées devraient pouvoir exercer leur droit d'accès aux données les concernant auprès de la Direction de la Santé pour autant qu'elles ne

sont pas anonymisées, et ce par l'intermédiaire des médecins et laboratoires déclarants.

XII. S'agissant des destinataires

Ont accès aux données traités dans le cadre de la surveillance des maladies infectieuses :

- les professionnels de santé déclarants ;
- les laboratoires d'analyses de biologie médicale et les laboratoires de référence nationaux désignés par l'autorité sanitaire ;
- la Division de l'Inspection Sanitaire de la Direction de la Santé ;
- les instances en charge de la surveillance des maladies infectieuses au niveau européen (ECDC) et international (OMS).

L'implication du Laboratoire National de Santé (LNS) et du Luxembourg Institute of Health (LIH) dans le nouveau dispositif de surveillance des maladies ne ressort pas explicitement du projet de loi. Le cas échéant, la CNPD suggère de préciser ce point dans le projet de loi.

La Commission nationale note par ailleurs que le ministre ayant la Santé dans ses attributions rend public le nombre de cas de maladies infectieuses déclarés[72]. L'exposé des motifs précise que cette publication se fera par l'intermédiaire de sites web ou de publications statistiques[73]. La CNPD souligne que cette publication peut uniquement être effectuée sous une forme anonymisée ne permettant pas de révéler l'identité des personnes concernées.

XIII. Sur la sécurité des données

La Commission nationale rappelle qu'en application des articles 22 et 23 de la loi modifiée du 2 août 2002, le responsable de traitement doit adopter les mesures techniques et organisationnelles nécessaires afin d'assurer la sécurité des données, notamment un système de traçage des accès aux données dans la base centralisée de gestion des cas de maladies infectieuses déclarés. Elle estime qu'il conviendrait de rajouter une disposition, à l'instar d'autres lois ou règlements grand-ducaux, qui pourrait avoir la teneur suivante : *« Le système informatique par lequel l'accès au fichier est opéré doit être aménagé de sorte que l'accès aux fichiers soit sécurisé moyennant une authentification forte, que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle. ».*

De manière plus générale, la CNPD recommande que des mesures de sécurité à l'état de l'art soient mises en œuvre, afin de garantir la confidentialité des données particulièrement sensibles contenues dans le système centralisé.

En l'absence de précisions des auteurs du projet de loi, la CNPD n'est pas en mesure d'apprécier dans leur ensemble le niveau des mesures de sécurité envisagées. Elle note toutefois que l'article 4 du projet de loi pose des conditions applicables à la transmission des déclarations :

« Les déclarations prévues aux articles 2 et 3 peuvent être effectuées, par voie électronique sécurisée, par téléfax, ou par voie postale.
En cas de diagnostic, respectivement en cas de suspicion de diagnostic d'une maladie représentant une menace grave pour la santé publique la déclaration est faite sans délais, de jour et de nuit, par téléphone, sinon par tout autre moyen de communication approprié ».

La Commission nationale recommande, s'agissant des transmissions par voie électronique, que des mesures de chiffrement à l'état de l'art pour des données sensibles

[72] Article 10 du projet de loi.
[73] *cf.* Commentaire des articles, p. 2.

soient mises en œuvre. Elle recommande, s'agissant des transmissions par voie postale, que ces dernières soient effectuées sous pli confidentiel portant la mention « *secret médical* ».

Enfin, compte tenu de l'extrême sensibilité des données recueillies grâce aux déclarations obligatoires des professionnels de santé et des laboratoires d'analyse médicale, la CNPD insiste sur la nécessité de prévoir des mesures spécifiques de protection de l'identité des patients, tout en permettant une surveillance et un suivi efficace des cas de maladies infectieuses déclarés.

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

Ainsi décidé à Esch-sur-Alzette en date du 10 mai 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis relatif au projet de règlement grand-ducal fixant les conditions et modalités d'octroi de la subvention pour ménage à faible revenu et de la subvention du maintien scolaire

Délibération n°409/2017
du 10 mai 2017

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 : « 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 avril 2017, le Ministère de l'Education nationale, de l'Enfance et de la Jeunesse a invité la Commission nationale à se prononcer sur un projet de règlement grand-ducal fixant les conditions et modalités d'octroi de la subvention pour ménage à faible revenu et de la subvention du maintien scolaire (ci-après « le projet de règlement grand-ducal »).

Ce projet de règlement grand-ducal a pour objet de fixer les

NOTES PAGE 125

74 Avis du Conseil d'Etat n°6787/03 du 20 octobre 2015 relatif au projet de loi ayant pour objet a) l'organisation de la Maison de l'orientation, b) la cohérence de l'orientation scolaire et professionnelle et modifiant des dispositions diverses, pp. 7-8.

75 Amendements du 12 septembre 2016 relatifs au projet de loi ayant pour objet l'organisation de la Maison de l'orientation, document parlementaire n°6787/06, p. 13.

76 Avis complémentaire du Conseil d'Etat n°6787/07 du 29 novembre 2016 relatif au projet de loi ayant pour objet l'organisation de la Maison de l'orientation et modifiant des dispositions diverses, pp. 2-3.

77 Il s'agit en l'occurrence du projet de règlement grand-ducal sous examen.

78 Rapport n°6894/04 de la Commission des institutions et de la révision constitutionnelle du 29 juin 2016, point V. « Travaux en Commission », cité par le Conseil d'Etat dans son avis complémentaire n°6787/07 du 29 novembre 2016, p. 3.

modalités d'octroi et de calcul de la subvention pour ménages à faibles revenus d'une part, et de la subvention du maintien scolaire pour les élèves de l'enseignement secondaire d'autre part. Ces deux subventions devraient être introduites par le nouvel article 2 de la loi du 13 juillet 2006 portant réorganisation du Centre psycho-social et d'accompagnement scolaires, telle que modifiée par le projet de loi n°6787 ayant pour objet l'organisation de la Maison de l'orientation et modifiant des dispositions diverses (ci-après : « la loi modifiée du 13 juillet 2006 »).

La Commission nationale entend limiter ses observations aux questions liées à la protection des données à caractère personnel que pose le projet de règlement grand-ducal sous examen.

Articulation entre le projet de règlement grand-ducal et la loi modifiée du 13 juillet 2006

La Commission nationale regrette tout d'abord de n'avoir pas été saisie du projet de loi n°6787 ayant pour objet l'organisation de la Maison de l'orientation. Elle aurait pu à cette occasion formuler des observations qui auraient pu être prises en compte au stade de l'élaboration du projet de règlement grand-ducal sous examen. Elle observe, à la lecture des documents parlementaires relatifs au projet n°6787, que, suite à l'avis du Conseil d'Etat du 20 octobre 2015[74] et conformément à l'article 23, alinéa 3, de la Constitution, les auteurs de ce projet de loi ont souhaité inscrire dans un nouvel article 2 de la loi modifiée du 13 juillet 2006 les finalités, les conditions et les modalités, y compris les montants et les critères d'attribution, des subventions pour ménages à faible revenu et du maintien scolaire[75].

Dans son premier avis complémentaire sur le projet de loi n°6787[76], le Conseil d'Etat, en faisant application des critères de l'article 32 paragraphe (3) de la Constitution a considéré que ledit projet de loi, en particulier son nouvel article 2, « *constitue une disposition légale particulière qui renvoie à un règlement grand-ducal*[77] » et que « cette disposition légale détermine l'objectif qui est de fixer les modalités de l'octroi et de calcul des deux subventions ». Il a relevé en outre que « *les principes et points essentiels sur les modalités de l'octroi, les montants maximums et les conditions d'attribution de l'aide financière sont déterminés à suffisance* » par la loi, les mesures d'exécution, c'est-à-dire les éléments plus techniques et de détail pouvant être réglées par voie des dispositions d'ordre règlementaire[78].

La Commission nationale partage entièrement cette analyse du Conseil d'Etat. En revanche, elle se demande si une présentation plus précise des fichiers créés et des opérations de traitements effectués à l'occasion de la gestion et de l'octroi des subventions dans ce projet de loi ne présenterait pas un avantage de clarté et de prévisibilité juridique pour les personnes concernées.

Dans cette démarche, il pourrait être utile de consacrer plus explicitement, dans le projet de nouvel article 2 de la loi modifiée du 13 juillet 2006, la création de deux fichiers de données à caractère personnel : le fichier relatif aux subventions pour ménage à faible revenu, et le fichier relatif aux subventions du maintien scolaire. Il pourrait également être précisé que les opérations de traitements relatifs à ces deux fichiers répondent exclusivement aux finalités de gestion et de l'octroi des subventions[79]. Le projet de loi pourrait également indiquer que le Ministre ayant l'Education nationale dans ses attributions (ci-après : « le Ministre ») a la qualité de responsable du traitement[80], et le Centre psycho-social et d'accompagnement scolaires (ci-après : « le Centre ») celle de sous-traitrant[81]. Les catégories de personnes concernées pourraient également être précisées : il s'agit, pour la subvention pour ménage à faible revenu, des ménages à faible revenu selon détermination du revenu mensuel net disponible telle que prévue à l'article 2 paragraphe (1) point

---

[79] Il ressort déjà du projet de nouvel article 2 de la loi du 13 juillet 2006 que ces subventions sont destinées :
- pour la subvention pour ménages à faible revenu, « *à l'acquisition de matériel scolaire et à la participation aux frais d'activités périscolaires et parascolaires* » (article 2 paragraphe (1) point (1) alinéa 2) ;
- pour la subvention du maintien scolaire, à « *permettre à l'élève de poursuivre la scolarité jusqu'à l'obtention d'un diplôme de fin d'études secondaires, d'un diplôme de fin d'études secondaires techniques, d'un diplôme de technicien, d'un diplôme d'aptitude professionnelle ou d'un certificat de capacité professionnelle* » (article 2 paragraphe (2) point (1) alinéa 2).

[80] Au sens de l'article 2 lettre (n) de la loi modifiée du 2 août 2002. Ceci ressort déjà indirectement de l'article 2 paragraphes (1) et (2), point (1) alinéa 1 du projet de loi : « *une subvention est accordée par le ministre (…)* ».

[81] Au sens de l'article 2 lettre (o) de la loi modifiée du 2 août 2002. Ceci ressort de l'article 2 paragraphe (4) du projet de loi, selon lequel « *le Centre est chargé de la gestion des dossiers* ».

(3). Pour la subvention du maintien scolaire, les personnes concernées sont les élèves majeurs répondant aux conditions fixées par l'article 2 paragraphe (2) point (1) alinéa 1. Enfin, les catégories de données appelées à figurer dans ces fichiers sont celles que les personnes concernées doivent produire à l'appui de leur demande afin de prouver le respect des conditions d'octroi des subventions prévues par l'article 2 paragraphe (1) point (2), et par l'article 2 paragraphe (2) point (3). Les données collectées peuvent être plus amplement détaillées dans le projet de règlement grand-ducal sous examen[82], comme cela est prévu dans l'article 2 paragraphe (3) du projet de loi.

<u>Dispositions relatives à la protection des données</u>

La Commission nationale constate que le projet de règlement grand-ducal sous examen ne prévoit pas de disposition spécifique relative à la protection des données à caractère personnel. Dans la mesure où la loi du 13 juillet 2006 serait modifiée en ce sens qu'elle préciserait les traitements de données nécessaires à la gestion et l'octroi des subventions pour ménage à faible revenu et du maintien scolaire[83], elle peut admettre que le règlement grand-ducal ne prévoit que des éléments plus techniques et de détail.

Cependant, la Commission nationale se demande si, à l'occasion de la vérification des conditions requises pour l'octroi des subventions, le Ministre ou le Centre pourront être amenés à accéder à des données issues de fichiers d'autres administrations[84]. Si tel était le cas, il conviendrait de formaliser de tels accès dans une disposition légale (par exemple dans le projet de nouvel article 2 de la loi modifiée du 13 juillet 2006), conformément à l'article 11, paragraphe 3, de la Constitution. En effet, selon une position constante du Conseil d'Etat, l'accès à des fichiers externes et la communication de données à des tiers constituent *« une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi »*[85]. De plus, la Commission nationale estimerait dans cette hypothèse nécessaire, comme elle l'a déjà soulevé dans ses avis antérieurs relatifs à des textes de loi similaires, que soit prévue la mise en place d'une solution technique permettant de garantir, d'un point de vue informatique, que les agents du Centre ou du Service, puissent seulement accéder aux données concernant les personnes qui ont effectivement introduit une demande de subvention pour ménage à faible revenu ou du maintien scolaire, à l'exclusion du reste de la population résidente.

---

[82] Voir ci-dessous, la section consacrée aux catégories de données traitées.
[83] Voir ci-dessus, remarques préliminaires.
[84] Par exemple pour vérifier que le candidat n'est pas bénéficiaire d'une aide ou subvention visée à l'article 3 paragraphe (2) point 4 du projet de règlement grand-ducal sous examen, ou pour vérifier le revenu mensuel net disponible du ménage ou du demandeur conformément à l'article 5 paragraphe (5) ou 9 paragraphe (3) du projet de règlement grand-ducal sous examen.
[85] Voir par exemple l'avis du Conseil d'Etat n°6975/05 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.

Enfin, la Commission nationale rappelle que les données doivent être, aux termes de l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002, « *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* ». En l'absence de précisions de la part des auteurs du projet de loi, la Commission nationale estime qu'une disposition relative à la durée de conservation de ces données serait bienvenue dans le projet de loi, sinon le projet de règlement grand-ducal sous examen.

Catégories de données traitées

L'article 3 paragraphe (2) du projet de règlement grand-ducal indique les cinq conditions cumulatives que doit respecter un demandeur pour que sa demande en obtention d'une subvention pour ménage à faible revenu soit recevable. L'article 9 paragraphe (1) alinéa 2 prévoit quant à lui les pièces justificatives nécessaires à l'octroi de la subvention du maintien scolaire.

La Commission nationale estime que ces deux dispositions renseignent sur les catégories de données qui seront traitées par le Ministre dans le cadre de la gestion et de l'octroi de ces subventions.

En outre, elle note que l'article 4 paragraphe (3) alinéa 1 du projet de règlement grand-ducal prévoit, en ce qui concerne la subvention pour ménage à faible revenu, que « *le demandeur est tenu, dans un délai de dix jours ouvrables de fournir, sur demande du Service ou du Centre, tous les renseignements et documents jugés nécessaires pour constater si les conditions d'octroi de la subvention demandée sont remplies. Le défaut de présentation des pièces dans les délais prévus vaut refus de la demande* ». L'article 9 paragraphe (2) du projet de règlement grand-ducal prévoit une procédure similaire en ce qui concerne la subvention du maintien scolaire. Pour des raisons de prévisibilité juridique, la Commission nationale recommande d'énumérer limitativement les renseignements et documents qui pourraient être demandés.

Accès au registre national des personnes physiques

Selon l'article 4 paragraphe (3) alinéa 2 du projet de règlement grand-ducal, « *le Service et le Centre ont accès au registre national des personnes physiques, afin de vérifier la composition du ménage* » du demandeur de la subvention pour ménages à faibles revenus. L'article 9 paragraphe (2) alinéa 2 du projet de règlement grand-ducal prévoit la même disposition pour la subvention du maintien scolaire.

Les auteurs du projet de règlement grand-ducal expliquent dans le commentaire des articles qu'« *avec la loi modifiée du 13 juin 2013 relative à l'identification des personnes physiques, entrée en vigueur en date du 1er avril 2016, les communes n'émettent plus de certificats de résidence ou de composition du ménage à destination des administrations publiques. Celles-ci peuvent, via accès au registre national des personnes physiques, procéder elles-mêmes aux consultations nécessaires. Les Services et le Centre disposent, à cet effet, d'un accès au registre national des personnes physiques. Le recours à un certificat de résidence établi par la commune de résidence du demandeur reste possible, à titre exceptionnel, en cas de doute ou d'incohérence entre le registre national des personnes physiques et les réalités constatées* »[86].

Or, si les auteurs du projet de règlement grand-ducal entendent prévoir un tel accès au registre national des personnes physiques, il conviendrait selon le principe du parallélisme des formes de le consacrer dans une disposition légale, et non dans un règlement grand-ducal, par exemple dans le projet de loi n°6787 ayant pour objet l'organisation de la Maison de l'orientation.

Il convient cependant de noter que l'accès au registre national des personnes physiques par

[86] Projet de règlement grand-ducal fixant les conditions et modalités d'octroi de la subvention pour ménage à faible revenu et de la subvention du maintien scolaire, commentaires des articles, ad art. 4, p. 13.

Annexes

le Service et le Centre peut être accordé en dehors d'une disposition légale spécifique, sur demande au Ministre ayant le Centre des technologies de l'information de l'Etat dans ses attributions, après avis de la Commission du Registre National.

La loi modifiée du 13 juin 2013 prévoit en effet dans son article 7 paragraphe (2) que « *le ministre accorde l'accès au registre national en conformité avec les dispositions légales et réglementaires relatives au registre national et celles relatives à la législation sur la protection des données, après avoir demandé l'avis de la commission prévue à l'article 11* »[87].

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

Ainsi décidé à Esch-sur-Alzette en date du 10 mai 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis à l'égard de l'avant-projet de loi 1. fixant les prescriptions techniques des bateaux de navigation intérieure ; 2. modifiant la loi du 28 juillet 1973 portant création d'un service de la navigation.

Délibération n°447/2017
du 19 mai 2017

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

Faisant suite à la demande lui adressée par Monsieur le Ministre du Développement durable et des Infrastructures en date du 17 mars 2017, la CNPD entend présenter ci-après ses réflexions et commentaires au sujet de l'avant-projet de loi du XXX fixant les prescriptions techniques des bateaux de navigation intérieure et modifiant la loi du 28 juillet 1973 portant création d'un service de la navigation (ci-après : « l'avant-projet de loi »).

[87] Loi modifiée du 13 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques, article 7.

Suivant l'exposé des motifs, l'avant-projet de loi vise à transposer la directive 2016/1629 du Parlement européen et du Conseil du 14 septembre 2016 établissant les prescriptions techniques applicables aux bateaux de navigation intérieure, modifiant la directive 2009/100/CE et abrogeant la directive 2006/87/CE. La directive 2016/1629 susmentionnée est à transposer pour le 7 octobre 2018 au plus tard.

La CNPD rappelle que le règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD ») sera applicable à partir du 25 mai 2018. Il convient ainsi d'analyser l'avant-projet de loi à la lumière de la loi modifiée du 2 août 2002 qui est la législation actuellement en vigueur, d'une part, et du RGPD, d'autre part.

De manière générale, la CNPD félicite les auteurs de l'avant-projet de loi que la plupart des principes essentiels issus de la loi modifiée du 2 août 2002 aient été intégrés dans l'avant-projet de loi. Elle entend limiter ses observations aux questions traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel, soulevées plus particulièrement par les articles 17, 19 et 29 de l'avant-projet de loi.

I. S'agissant de l'article 17 : Registre électronique des certificats émis pour les bateaux de navigation intérieure

La Commission nationale note que l'article 17 de l'avant-projet de loi vise à instaurer un registre électronique des certificats émis pour les bateaux de navigation intérieure (ci-après : « le registre électronique »). Le ministère ayant le transport dans ses attributions (« le ministre ») a vocation à en être le responsable de traitement au sens de l'article 2 lettre (n) de la loi modifiée du 2 août 2002.

A titre préliminaire, la Commission nationale souhaiterait relever une erreur matérielle à l'article 17, paragraphe (4), dont les points 1 à 4 devraient se référer *« aux finalités visées à l'article 17, paragraphe 2, points […] »* au lieu de faire référence *« aux finalités visées à l'article 2, paragraphe 2, points […] »*.

1. *Prolifération des accès à divers fichiers étatiques et mise en place d'une solution technique visant à les restreindre*

Il ressort de l'article 17, paragraphe (3) que le ministre a la qualité de responsable du traitement au sens de l'article 2, lettre (n) de la loi modifiée du 2 août 2002. L'article 17, paragraphe (4) de l'avant-projet de loi établit une liste limitative des finalités pour lesquelles l'accès à certains fichiers tenus auprès d'autres entités étatiques doit être permis au responsable du traitement dans le cadre des missions qui lui sont dévolues en ce qui concerne le registre électronique. La Commission nationale salue le degré de détail avec lequel les auteurs de l'avant-projet de loi précisent les données auxquelles peut accéder le responsable de traitement.

Néanmoins, il ressort de ce qui précède que le ministre aura accès à plusieurs fichiers étatiques dans le cadre de la gestion des entreprises de transport fluvial. La Commission nationale estimerait dans cette hypothèse nécessaire, comme elle l'a déjà soulevé dans ses avis antérieurs relatifs à des textes de loi similaires, que soit prévue la mise en place d'une solution technique permettant de garantir, d'un point de vue informatique, que les agents du Département des Transports du Ministère du Développement durable et des Infrastructures, puissent seulement accéder aux données concernant les personnes qui soit ont introduit une demande d'obtention d'un certificat auprès du ministère précité, soit font l'objet d'un

contrôle de conformité dans le cadre de l'article 21 de l'avant-projet de loi.

2. *L'accès aux données et leur durée de conservation*

Le paragraphe (3) de l'article 17 prévoit que le ministre *« peut faire exécuter sous sa responsabilité tout ou partie des obligations qui lui incombent en vertu de la loi par un membre du cadre supérieur ou moyen de son ministère. »* La CNPD recommande à cet égard aux auteurs de l'avant-projet de loi de préciser davantage qui aura accès aux données présentes dans le registre électronique, ainsi que les modalités d'accès aux données y contenues. En effet, il est important que seules les personnes qui en ont besoin dans l'exercice de leur fonction et de leurs tâches professionnelles soient habilitées à y avoir accès.

Par ailleurs, la CNPD tient à souligner que l'article 4, paragraphe (1), lettre (d) de la loi modifiée du 2 août 2002, ainsi que l'article 5, paragraphe (1), lettre (e) du RGPD, imposent au responsable de traitement de veiller à ce que les données qu'il traite ne soient pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées.

À première vue, l'avant-projet de loi sous avis ne contient aucune disposition relative à la durée de conservation des données contenues dans le registre électronique. Néanmoins, la Commission nationale constate que le paragraphe (4) de l'article 19 concernant la base de données européenne sur les bateaux de navigation intérieure prévoit que le ministre doit s'assurer que les données relatives à un bâtiment sont supprimées de ladite base de données lorsque le bâtiment est démantelé. La CNPD se demande dans ce contexte si cette disposition s'appliquerait aussi aux données du registre électronique ou si la suppression de la base de données européenne aurait pour conséquence que les données disparaitraient de même de manière automatique du registre électronique national ? Ainsi, les auteurs de l'avant-projet de loi sont invités à clarifier les modalités de conservation et de suppression des données à l'article 17 de l'avant-projet de loi.

3. *Système de traçage des accès*

La CNPD estime nécessaire de prévoir un système de traçage des accès, qui constitue une garantie en matière de protection des données à caractère personnel des personnes concernées dans le cadre des articles 22 et 23 de la loi modifiée du 2 août 2002, et de l'article 32 du RGPD. Ainsi, à l'instar d'autres lois ou règlements

grand-ducaux, il conviendrait de rajouter une disposition qui pourrait avoir la teneur suivante :

« Le système informatique par lequel l'accès au registre électronique est opéré doit être aménagé de la manière suivante :

- *L'accès au registre est sécurisé moyennant une authentification forte;*

- *Les informations relatives aux personnes ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation peuvent être retracés;*

- *Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle ».*

II. S'agissant de l'article 19 : Base de données européenne sur les bateaux de navigation intérieure

Il ressort de l'article 19, paragraphe 1ier de la directive 2016/1629 du Parlement européen et du Conseil du 14 septembre 2016 établissant les prescriptions techniques applicables aux bateaux de navigation intérieure que la Commission européenne assure la fonction du responsable du traitement en ce qui concerne la base de données européenne sur les bateaux de navigation intérieure. Le ministre a quant à lui pour mission d'alimenter ladite base de données européenne à partir des données nationales.

La loi modifiée du 2 août 2002 et le RGPD n'ont vocation à s'appliquer qu'en présence de traitements automatisés de données à caractère personnel, c'est-à-dire de toute information concernant une personne physique identifiée ou identifiable.[88] Les textes légaux précités ne s'appliquent pas aux personnes morales.[89] La CNPD est toutefois d'avis que les données prévues à l'article 19, paragraphe 1ier de l'avant-projet de loi, ayant pour vocation d'identifier un bâtiment, pourraient permettre d'identifier indirectement certaines personnes physiques, comme par exemple le propriétaire ou le conducteur du bateau, et ce notamment à l'aide des données relatives aux certificats de navigation. Ainsi, la protection conférée par la loi modifiée du 2 août 2002 et par le RGPD a vocation à s'appliquer en l'espèce.

Par ailleurs, en parallèle de ce qui a été dit concernant le registre électronique, la CNPD conseille aux auteurs de l'avant-projet de loi :

- de préciser qui aura accès aux données présentes dans la base de données européenne, ainsi que les modalités d'accès auxdites données.

- de prévoir un système garantissant le traçage des accès, conformément aux articles 22 et 23 de la loi modifiée du 2 août 2002, et à l'article 32 du RGPD.

En outre, la CNPD regrette que le texte ne donne aucune précision sur l'origine des données. Est-ce que les données que le ministre introduit dans la base de données européenne sont reprises intégralement du registre électronique ou est-ce qu'elles sont collectées à partir d'autres fichiers étatiques ou encore par d'autres moyens de recherche ?

En dernier lieu et concernant le paragraphe (3) de l'article 19 portant sur les transferts de données personnelles vers un pays tiers, la CNPD tient à souligner que le RGPD n'est applicable qu'à partir du 25 mai 2018. Dans l'hypothèse où l'avant-projet de loi serait adopté avant ladite date, les dispositions des articles 18 à 20 de la loi modifiée du 2 août 2002 seront à respecter dans l'intervalle.

III. S'agissant de l'article 29 : Modification de la loi du 28 juillet 1973 portant création d'un service de la navigation

L'article 29 de l'avant-projet de loi vise à modifier la loi du 28 juillet 1973 portant création d'un

[88] Voir l'article 3, paragraphe (1) lettre (a) de la loi modifiée du 2 août 2002 et l'article 2 du RGDP.
[89] Voir dans ce contexte le considérant 14 du RGPD.

service de la navigation en y insérant une disposition autorisant ledit service à collecter et à traiter différentes données pour les besoins de l'exploitation des services d'information fluviale et notamment pour la diffusion d'informations sur le trafic et la gestion de trafic, ainsi que pour les besoins de la collecte des péages. Entre autres, les données d'identification (prénom, nom et adresse) du propriétaire, de l'exploitant, de l'affréteur, du locataire, du débiteur des péages ou du conducteur du bateau seront collectées, ainsi que les données bancaires du débiteur de péages.

La Commission nationale constate avec satisfaction que les dispositions de l'article 29 respectent les principes essentiels issus 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 19 mai 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis relatif au projet de loi n°7172 relative à i) la protection sanitaire des personnes contre les dangers résultant de l'exposition aux rayonnements ionisants et à la sécurité des sources de rayonnements ionisants contre les actes de malveillance, et ii) à la gestion des déchets radioactifs, du transport de matières radioactives et de l'importation, et iii) portant création d'un carnet radiologique électronique.

Délibération n°596/2017
du 14 juillet 2017

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 sur la protection des données »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») a notamment pour mission d'« *être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi* ».

Par courrier en date du 27 février 2017, Madame la Ministre de la Santé a invité la Commission

NOTES PAGE 133

[90] a) La loi modifiée du 25 mars 1963 concernant la protection de la population contre les dangers résultant des radiations ionisantes ; b) La loi du 10 août 1983 concernant l'utilisation médicale des rayonnements ionisants ; c) Le règlement grand-ducal modifié du 14 décembre 2000 concernant la protection de la population contre les dangers résultant des rayonnements ionisants.

[91] *cf.* Exposé des motifs, dernière phrase.

[92] *cf.* Communiqué du Ministère de la Santé publié le 15 décembre 2016.

nationale à se prononcer sur le projet de loi n°XXX relative à i) la protection sanitaire des personnes contre les dangers résultant de l'exposition aux rayonnements ionisants et à la sécurité des sources de rayonnements ionisants contre les actes de malveillance, et ii) à la gestion des déchets radioactifs, du transport de matières radioactives et de l'importation, et iii) portant création d'un carnet radiologique électronique (ci-après « le projet de loi »).

Le projet de loi intègre dans une seule loi les dispositions en vigueur des lois et règlements grand-ducaux principaux en matière de radioprotection[90] et transpose en droit luxembourgeois les deux directives européennes relatives à la protection contre les dangers du rayonnement ionisant et à la sûreté nucléaire : i) la directive 2013/59/EURATOM du Conseil du 5 décembre 2013, et ii) la directive 2014/87/EURATOM du Conseil du 8 juillet 2014.

Les objectifs principaux du projet de loi sont « *de garantir un haut niveau de protection de la population contre les conséquences d'une situation d'urgence nucléaire*»[91] et une « *amélioration de la protection sanitaire des personnes contre les dangers résultant de l'exposition aux rayonnements ionisants, y compris contre le radon au moyen d'un plan d'action radon et également un renforcement de la protection des patients soumis à une exposition médicale et la mise en place d'un carnet radiologique électronique* »[92].

Pour sa part, la Commission nationale entend limiter ses observations aux questions soulevées par les dispositions du projet de loi sous examen traitant des aspects liés au respect de la vie privée et à la protection des données à caractère personnel.

I) La surveillance radiologique individuelle des travailleurs exposés

a) Les personnes concernées :

L'article 66 du projet de loi distingue deux catégories de travailleurs exposés, la catégorie A et la catégorie B, en fonction du niveau d'exposition.[93]

Les deux catégories de travailleurs exposés font l'objet d'une surveillance systématique fondée sur des mesures individuelles réalisées par un service de dosimétrie[94]. Selon l'article 67 paragraphe (3) du projet de loi et avec l'accord de la Direction de santé, les travailleurs de la catégorie B peuvent être soumis à un autre système approprié de surveillance qui n'est pas nécessairement une surveillance individuelle.[95]

b) Le flux de l'information :

La surveillance radiologique individuelle des travailleurs exposés selon les articles 67 et 68 du projet de loi nécessite un flux d'informations qui peut s'analyser comme suit :

1. Le chef d'établissement ou l'employeur des travailleurs extérieurs détermine la classification de chaque travailleur et réexamine périodiquement cette classification « *sur la base de conditions de travail et en fonction des résultats de la surveillance médicale* »[96].

2. Les travailleurs exposés portent durant leur travail un dosimètre individuel adapté aux types de rayonnements. Ce dosimètre est mis à la disposition par un service de dosimétrie. Selon l'article 20 paragraphe (1) et (2) du projet de loi, le service de dosimétrie détermine les doses liées à l'exposition interne ou externe des travailleurs exposés et il est autorisé par le ministre. Le service de dosimétrie établit un relevé contenant les résultats de la surveillance radiologique individuelle (ci-après le « relevé de doses »).

3. Le relevé de doses est i) conservé par le chef d'établissement et ii) inscrit au registre de dosimétrie

---

[93] Selon l'article 66 (1) a) et b), un travailleur de la catégorie A est « susceptible de recevoir une dose efficace supérieure à six mSv par an ou une dose équivalente supérieure à quinze mSv par an pour le cristallin ou à cent cinquante mSv par an pour la peau et les extrémités » et un travailleur de la catégorie B est un travailleur exposé qui « ne relève pas de la catégorie A ».

[94] Définition du service de dosimétrie selon article 3 lettre (c) chiffre 77 du projet de loi : « un organisme compétent ou une personne compétente pour l'étalonnage, l'étalonnage, la lecture ou l'interprétation des appareils de surveillance individuels, ou pour la mesure de la radioactivité dans le corps humain ou dans des échantillons biologiques, ou pour l'évaluation des doses, et dont la qualification pour cette tâche est reconnue. »

[95] Les apprentis, les étudiants et le personnel d'un chef d'établissement exploitant des aéronefs sont aussi soumis à une surveillance individuelle ou à un autre système approprié de surveillance et cela en fonction de leur âge et/ou du niveau d'exposition.

[96] *cf.* article 66 (2) du projet de loi.

central[97] tenu par la Direction de la santé. C'est le chef d'établissement qui est responsable de s'assurer que le service de dosimétrie transmet les résultats dans un délai de quarante jours au registre de dosimétrie central.[98]

4. Le chef d'établissement est soutenu, dans l'accomplissement de ses tâches de radioprotection, par une personne chargée de la radioprotection ; une personne désignée par le chef d'établissement parmi son personnel. Néanmoins, les missions de la personne chargée de la radioprotection peuvent être assurées par un service de radioprotection mis en place au sein d'une entreprise ou par un expert en radioprotection[99]. Le chef d'établissement doit notifier la personne chargée de la radioprotection à la Direction de la santé.

5. a) S'agissant du cas où le service de dosimétrie ne constate aucun dépassement des limites de doses pour l'exposition professionnelle au cours d'une année calendaire :

   Le registre de dosimétrie central transmet les résultats de la surveillance individuelle des travailleurs exposés à la Direction de la santé de façon régulière, mais au moins une fois par année. Ensuite, la Direction de la santé soumet les résultats au médecin du travail chargé de la surveillance médicale des travailleurs exposés pour une interprétation de leurs incidences sur la santé humaine.

   b) S'agissant du cas où les 6/10 des limites de doses pour l'exposition professionnelle sont dépassées au cours d'une année calendaire :

   Le service de dosimétrie doit informer la Direction de la santé et le chef d'établissement. Le chef d'établissement doit informer le travailleur exposé et l'expert en radioprotection.[100]

   c) S'agissant du cas où le dépassement des limites des doses pour l'exposition professionnelle est constaté ou suspecté par le service de dosimétrie :

   Le service de dosimétrie doit en informer sans délai injustifié le médecin du travail chargé de la surveillance médicale des travailleurs exposés, la Direction de la santé, l'inspection du travail et des mines, ainsi que le chef d'établissement qui a l'obligation d'en informer le travailleur concerné et l'expert en radioprotection.[101]

6. Sur demande du médecin du travail chargé de la

[97] Selon l'article 68 (2) du projet de loi le registre de dosimétrie central comprend « *a) les informations relatives à l'identité du travailleur, les informations relatives à l'établissement et à l'employeur en cas de travailleurs extérieurs, les informations administratives non médicales relatives à la surveillance médicale du travailleur ; b) un relevé des expositions mesurées ou estimées, selon le cas, des doses individuelles résultant d'expositions planifiées, d'expositions accidentelles, des expositions des travailleurs extérieurs, des expositions sous autorisation spéciale et des expositions professionnelles d'urgence ; c) les rapports décrivant les circonstances de l'exposition et les mesures prises pour les expositions accidentelles, les expositions sous autorisation spéciale et les expositions professionnelles d'urgence ; d) le cas échéant, les résultats de la surveillance radiologique du lieu du travail qui ont servi à l'évaluation des doses individuelles.* »

[98] *cf.* article 69 (1) du projet de loi.

[99] *cf.* article 21 (3) du projet de loi.

[100] *cf.* article 69 (3) du projet de loi.

[101] *cf.* article 69 (4) du projet de loi.

surveillance médicale des travailleurs exposés, le chef d'établissement ou, dans le cas d'un travailleur extérieur, l'employeur, la division de la radioprotection, les services de médecine du travail, les experts de radioprotection, et, le cas échéant les services de dosimétrie agréés échangent toute information pertinente concernant les doses reçues antérieurement par un travailleur pour réaliser l'examen médical préalable à l'embauche ou à la classification en tant que travailleur de la catégorie A, et pour la surveillance de l'exposition ultérieure des travailleurs.

Ad 2.) : S'agissant du service de dosimétrie, la CNPD regrette de ne pas disposer de plus d'informations sur ce service. Il ne ressort pas clairement du projet de loi, et surtout de son article 20 ou de son commentaire afférent, si ce service de dosimétrie doit être créé en interne dans chaque établissement, si c'est un service externe ou s'il est rattaché à la Direction de la santé[102]. De ce fait, la Commission nationale regrette que le projet de loi sous examen n'ait pas immédiatement été accompagné du projet de règlement grand-ducal y afférent et mentionné dans l'article 20 paragraphe (3) du projet de loi et pour cette raison la CNPD ne peut pas se prononcer sur la légitimé des traitements des données effectuées.

Ad 5 b.) : S'agissant du cas où les 6/10 des limites de doses pour l'exposition professionnelle sont dépassées au cours d'une année calendaire, la CNPD constate que l'article 69 paragraphe (3) du projet de loi ne précise aucun délai pour la notification de la Direction de la santé, du chef d'établissement et des travailleurs exposés. La Commission nationale recommande d'ajouter un délai déterminé, comme cela a été fait dans le cas du paragraphe (4) du même article[103].

c) Les finalités :

La Commission nationale estime que la mise en place d'un système de surveillance individuelle radiologique se justifie par

- l'article 6 paragraphe (2) lettre (g) de la loi sur la protection des données qui pose comme condition que « *le traitement s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques (…)* » ; et par

- l'article 7 paragraphe (1) de la loi sur la protection des données qui dispose que « *le traitement de données relatives à la santé et à la vie sexuelle nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements peut être mis en œuvre par des instances médicales* » ; ainsi que par

- l'article 7 paragraphe (3) de la loi sur la protection des données qui dispose que « *le traitement de données relatives à la santé et à la vie sexuelle nécessaire aux fins de la gestion de services de santé peut être mis en œuvre par des instances médicales, ainsi que lorsque le responsable du traitement est soumis au secret professionnel, par les organismes de sécurité sociale et les administrations qui gèrent ces données en exécution de leurs missions légales et réglementaires (…)* ».

L'article 6 paragraphe (2) lettre (c) de la loi sur la protection des données qui dispose que « *le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement* » pourrait seulement s'appliquer dans des cas exceptionnels et limitatifs (p.ex. un accident nucléaire).

d) Les données concernées :

Le chef d'établissement assure que le relevé de doses, contenant les résultats de la surveillance radiologique individuelle des travailleurs exposés, est communiqué au registre de dosimétrie central. Selon l'article

[102] Selon l'article 6.5.4. paragraphe (1) du règlement grand-ducal du 14 décembre 2000 concernant la protection de la population contre les dangers résultant des rayonnements ionisants, le service de dosimétrie est un service qui doit être agrée par le Ministre de la Santé.
[103] L'article 69 paragraphe (4) du projet de loi dispose que, lorsque le dépassement des limites de doses pour l'exposition professionnelle est constaté ou suspecté, le service de dosimétrie doit informer « sans délai injustifié » les organismes mentionnés.

68 paragraphe (2) du projet de loi les informations suivantes relatives aux travailleurs exposés sont conservées au registre de dosimétrie central :

« a) les informations relatives à l'identité du travailleur, les informations relatives à l'établissement et à l'employeur en cas de travailleurs extérieurs, les informations administratives non médicales relatives à la surveillance médicale du travailleur ;

b) un relevé des expositions mesurées ou estimées, selon le cas, des doses individuelles résultant d'expositions planifiées, d'expositions accidentelles, des expositions des travailleurs extérieurs, des expositions sous autorisation spéciale et des expositions professionnelles d'urgence ;

c) les rapports décrivant les circonstances de l'exposition et les mesures prises pour les expositions accidentelles, les expositions sous autorisation spéciale et les expositions professionnelles d'urgence[104] *;*

d) le cas échéant, les résultats de la surveillance radiologique du lieu du travail qui ont servi à l'évaluation des doses individuelles. »

Selon l'article 68 paragraphe (5) du projet de loi, un règlement grand-ducal va détailler les données qui doivent figurer dans le registre de dosimétrie central. En l'absence de précision, la CNPD s'interroge sur les données d'identification du travailleur et plus précisément, sur les données exactes qui sont utilisées pour établir l'identité du travailleur (nom, prénom, date de naissance, matricule ?). La CNPD ne peut donc pas se prononcer sur la légitimité et la finalité de la collecte de ces données d'identification.
Selon l'article 66 paragraphe (2) du projet de loi, le chef d'établissement ou l'employeur des travailleurs extérieurs détermine la classification de chaque travailleur et réexamine périodiquement cette classification *« sur la base de conditions de travail et en fonction des résultats de la surveillance médicale »*.

S'agissant des données transmises au chef d'établissement ou l'employeur des travailleurs extérieurs, la CNPD se demande si le chef d'établissement ou l'employeur des travailleurs extérieurs sont autorisés à recevoir tous les résultats de la surveillance médicale, comme l'indique l'article 66 paragraphe (2) du projet de loi. Pour assurer la protection des données relatives à la santé des travailleurs exposés selon la loi sur la protection des données et partant du principe de minimisation des données, la Commission nationale recommande d'inclure un complément dans ce paragraphe (2) qui précise que

[104] Selon l'article 68 paragraphe (4) du projet de loi, les expositions visées au paragraphe (2) lettre (c) de l'article 68 sont conservées séparément dans le relevé de doses.

seuls les résultats nécessaires pour déterminer la classification de chaque travailleur exposé selon l'article 66 paragraphe (1) du projet de loi seront transférés au chef d'établissement ou à l'employeur des travailleurs extérieurs. Et ceci en considérant aussi le secret médical auquel sont soumis les médecins du travail qui sont responsables pour la surveillance médicale des travailleurs exposés.

e) Les destinataires :

Seront destinataires des données :

- Le chef d'établissement, en sa qualité de responsable de l'évaluation et de l'application des dispositions visant à assurer la radioprotection des travailleurs exposés, en application de l'article 61 paragraphe (1) et (2) du projet de loi ;

- La personne chargée de la radioprotection, qui est désignée parmi le personnel du chef d'établissement pour soutenir ce dernier dans l'accomplissement de ses tâches en matière de radioprotection, en application de l'article 21 du projet de loi ;

- L'expert en radioprotection chargé de prodiguer aux établissements des conseils éclairés sur les questions liées au respect des obligations applicables en vertu de la loi, en application des articles 17, 21 paragraphe (3) et 69 paragraphe (3) du projet de loi ;

- Le service de dosimétrie, qui est autorisé par le ministre pour déterminer les doses dues à l'exposition interne ou externe des travailleurs faisant l'objet d'une surveillance radiologique individuelle, en application de l'article 20 du projet de loi, et qui établit le relevé de doses ;

- Le registre de dosimétrie central dans lequel est inscrit le relevé de doses, en application de l'article 68 paragraphe (1) et (2) du projet de loi ;

- Le médecin du travail chargé avec la surveillance médicale des travailleurs exposés pour une interprétation de leurs incidences sur la santé humaine, en application des articles 19, 69 paragraphe (2), (3) et (4) et 70 du projet de loi ;

- L'inspection du travail et des mines qui est informée lorsque le dépassement des limites de doses pour l'exposition professionnelle est constaté ou suspecté par le service de dosimétrie, en application de l'article 69 paragraphe (4) du projet de loi.

f) L'information et les droits des personnes concernées :

i. L'information des travailleurs exposés :

Selon l'article 30 paragraphe (1) du projet de loi, le chef d'établissement doit assurer que l'information soit donnée à tout travailleur exposé et aux travailleurs intervenants en situation d'urgence sur les risques liés aux pratiques et leur impact sur la santé et la sécurité des personnes ainsi que sur l'environnement.

Outre les informations mentionnées dans l'article 30 paragraphe (2) du projet de loi, la CNPD rappelle que, selon article 26 paragraphe (1) de la loi sur la protection des données, le responsable du traitement a l'obligation de fournir à la personne concernée des informations relatives à l'identité du responsable du traitement, aux finalités déterminées du traitement, aux destinataires auxquels les données sont susceptibles d'être communiquées, ainsi qu'à l'existence d'un droit d'accès et de rectification de ces données.

ii. L'accès aux résultats de la surveillance radiologique individuelle :

Les travailleurs exposés ou, dans le cas des travailleurs extérieurs, les employeurs, ont accès aux résultats de la surveillance radiologique individuelle (y compris aux résultats des mesures qui ont pu être utilisées pour estimer ces résultats, ou aux résultats des évaluations de dose faites à partir de la surveillance

du lieu de travail) en application de l'article 69 paragraphe (1) du projet de loi.

La Commission nationale relève que, dans le cas des travailleurs extérieurs, il ne suffit pas que leurs employeurs aient accès aux résultats de la surveillance radiologique individuelle mais qu'il est nécessaire que le travailleur extérieur lui-même puisse accéder à ses résultats. Selon l'article 28 paragraphe (1) de la loi modifiée du 2 août 2002, la personne concernée dispose d'un droit d'accès aux données la concernant. De plus, la CNPD s'interroge sur le point de savoir si, dans ce cas-ci, les employeurs ont accès aux résultats de la surveillance radiologique individuelle dans des conditions respectueuses du secret médical ?

iii. Le droit d'opposition :

Le droit d'opposition selon l'article 30 paragraphe (1) de la loi sur la protection des données ne s'applique pas dans le cadre de la surveillance radiologique individuelle parce que le traitement de données se fonde sur des dispositions légales prévoyant expressément le traitement.

g) La durée de conservation des données :

L'article 68 paragraphe (3) du projet de loi dispose que le chef d'établissement conserve les informations contenues au relevé de doses pendant toute la durée de la vie professionnelle du travailleur exposé aux rayonnements ionisants, puis jusqu'au moment où celui-ci a ou aurait atteint l'âge de soixante-quinze ans, et en tout état de cause pendant une période d'au moins trente ans à compter de la fin de l'activité professionnelle comportant une exposition. La Commission nationale en prend acte.

Elle note que, pour les données conservées au registre de dosimétrie central et à la Direction de la santé, le projet de loi ne fait pas mention d'une durée de conservation limitée et elle rappelle que, selon l'article 4 paragraphe (1) lettre (d) de la loi sur la protection des données, les données traitées peuvent être conservées seulement pour une durée limitée. Par conséquent, la Commission nationale recommande d'inclure des précisions dans le projet de loi en relation avec la durée de conservation des données dans le registre de dosimétrie central et à la Direction de la santé. La durée de conservation de données ne peut pas excéder celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées et traitées.

II) La surveillance médicale des travailleurs exposés

Selon l'article 70 du projet de loi, la surveillance médicale des

travailleurs exposés de catégorie A incombe au médecin du travail chargé de la surveillance médicale des travailleurs exposés. À cette fin et *« pour ce qui est de leur capacité à remplir les tâches qui leur sont assignées »*, le médecin du travail accède à *« toute information pertinente qu'il estime nécessaire, y compris concernant les conditions ambiantes sur les lieux de travail »*[105].

Aux termes du paragraphe (3) de l'article 70 du projet de loi, la surveillance médicale comprend i) un examen médical préalable à l'embauche ou à la classification en tant que travailleur exposé, et ii) des examens de santé périodiques au moins une fois par an. La nature de ces examens, auxquels il peut être procédé aussi souvent que le médecin du travail l'estime nécessaire, dépend du type de travail et de l'état de santé du travailleur concerné. A chaque fois que l'une des limites de dose applicables aux travailleurs de la catégorie A, a été dépassée, une surveillance médicale exceptionnelle doit intervenir.

Cette surveillance médicale peut éventuellement se prolonger après la cessation du travail pendant le temps que le médecin du travail juge nécessaire pour préserver la santé de l'intéressé.

Le médecin du travail établit et tient à jour un dossier médical pour chaque travailleur de la catégorie A aussi longtemps que l'intéressé reste dans cette catégorie. Le dossier médical est ensuite conservé jusqu'au moment où l'intéressé a ou aurait atteint l'âge de soixante-quinze ans et, en tout état de cause, pendant une période d'au moins trente ans à compter de la fin de sa vie professionnelle, impliquant une exposition aux rayonnements ionisants[106].

Le dossier médical contient i) des renseignements concernant la nature des activités professionnels, ii) les résultats des examens médicaux préalables à l'embauche ou à la classification en tant que travailleur de la catégorie A, iii) les bilans de santé périodiques ainsi que iv) les résultats de la surveillance dosimétrique[107].

La CNPD observe que la surveillance médicale des travailleurs exposés par la médecine du travail peut être légitimé sur base de l'article 7 paragraphe (1) de la loi modifiée du 2 août 2002, alors qu'elle relève des traitements de la médecine préventive.

III) La recherche médicale ou biomédicale

La Commission nationale observe que l'article 78 du projet de loi dispose que les *« expositions à des fins médicales pour la recherche médicale ou biomédicale doivent être autorisées par le ministre, l'avis du Comité national d'éthique de recherche et d'un expert en physique médicale ayant été demandés au préalable »*.

Elle observe en outre que l'article 83 du projet de loi prévoit que pour chaque projet de recherche médicale ou biomédicale faisant intervenir une exposition à des fins médicales, a) les personnes sont informées préalablement par écrit sur les risques d'expositions ; b) les personnes concernées participent volontairement ; c) une contrainte de dose est fixée pour les personnes pour lesquelles aucun avantage médical direct n'est attendu de l'exposition ; et d) dans les cas de patients qui acceptent volontairement de se soumettre à une pratique expérimentale et qui devraient en retrier un avantage diagnostique ou thérapeutique, les niveaux de dose concernés sont établis au cas par cas par le médecin réalisateur et, le cas échéant le médecin demandeur, avant que l'exposition n'ait lieu.

La CNPD rappelle qu'en application de l'article 6 paragraphe (2) lettre (a) et (g) et de l'article 7 paragraphe (2) de la loi modifiée du 2 août 2002 l'interdiction des traitements de données relatives à la santé ne s'applique pas lorsque i) la personne concernée a donné son consentement exprès à un tel traitement[108], ii) le traitement s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou

[105] *cf.* article 70 paragraphe (2) du projet de loi.
[106] *cf.* article 72 du projet de loi.
[107] *cf.* article73 du projet de loi.
[108] *cf.* article 6 (2) (a) de la loi modifiée du 2 août 2002.

scientifiques[109] et iii) le traitement s'avère nécessaire aux fins de la recherche en matière de santé ou de la recherche scientifique (si le traitement est mis en place par les instances médicales, ainsi que par les organismes de recherche et par les personnes physiques ou morales dont le projet de recherche a été approuvé en vertu de la législation applicable en matière de recherche biomédicale et à condition de disposer du consentement écrit)[110]. La Commission nationale rappelle que les traitements nécessaires aux fins de recherche dans le domaine de la santé ou de la recherche scientifique sont strictement encadrés et doivent satisfaire aux conditions de légitimité et à la procédure particulière prévues par les articles 6, 7 et 14 de la loi sur la protection des données.

IV) La création du carnet radiologique électronique

1) Légitimité et Finalité

L'article 92 du projet de loi prévoit la création d'un carnet radiologique électronique (« CRE ») dont l'objectif est de tenir à disposition des différents acteurs un outil pour « guider le recours aux examens d'imagerie médicale et à en promouvoir le bon usage dans l'intérêt du patient ». Dans le commentaire des articles du projet de loi, il est précisé que le CRE « *recueille pour chaque patient concerné des données médicales et autres informations pour retracer de façon chronologique, exhaustive, non redondant et fidèle les actes de radiodiagnostic et de radiologie interventionnelle dont il bénéficie, y compris des types d'examens d'imagerie n'entrainant pas d'exposition aux rayonnements ionisants* »[111].

La CNPD estime que les finalités poursuivies par le CRE sont déterminées, explicites et légitimes, conformément à l'article 4 paragraphe (1) lettre (a) de la loi sur la protection des données.

En outre, elle estime que le traitement des données relatives à la santé dans le cadre du CRE peut être légitimé sur le fondement de l'article 7 paragraphe (1) de la loi relative au traitement de données relatives à la santé par des instances médicales aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements. Elle estime en outre que ce traitement de données peut être légitimé sur le fondement de l'article 6 paragraphe (2) lettre (g) de la loi sur la protection des données en relation avec un traitement de données qui s'avère nécessaire pour un motif d'intérêt public.

2) Responsable du traitement

Les auteurs du projet de loi soulignent dans le commentaire des articles en relation avec l'article 92 du projet de loi que l'Agence nationale des

[109] *cf.* article 6 (2) (g) de la loi modifiée du 2 août 2002.
[110] *cf.* article 7 (2) de la loi modifiée du 2 août 2002.
[111] Cf. Commentaire des articles, p. 91.

informations partagés dans le domaine de la santé (« l'Agence ») sera le responsable du traitement du CRE « *car elle le tient à la disposition en vertu d'une obligation légale et non sur instruction du Ministère ou de la Direction de la santé et puisque le carnet radiologique électronique sera un outil sur la plateforme nationale et l'Agence est le responsable de traitement de la plateforme* ». Dans ce commentaire il est aussi précisé que l'Agence :

- détermine (seule/avec ses sous-traitants) les moyens techniques, d'interopérabilité et de sécurité, et en cas d'accès illicite ou de faille de sécurité, elle en est responsable ;

- détermine certains moyens organisationnels et ceci dans la phase de conception ensemble avec la Direction de la santé ;

- met en œuvre les droits des personnes (p.ex. information, accès, rectification, effacement, opposition).

Selon l'article 94 du projet de loi, l'Agence est le gestionnaire du CRE et est chargée :

- de la mise à jour et du stockage des données recueillies ;

- du contrôle technique des données recueillies et dans ce cadre l'Agence peut établir des contacts avec les sources de données et peut leur demander les corrections ou les compléments d'information nécessaires à un enregistrement de l'acte ;

- de déterminer les modalités du transfert de données des sources vers le CRE, dont les critères de qualité, les exigences de sécurité et la fréquence du transfert de données ;

- d'informer le patient concerné sur l'ouverture du CRE et la transmission des données le concernant, lors du premier acte d'imagerie médicale du patient, sous réserve de son opposition.

La Commission nationale se demande pourquoi le projet de loi n'a pas envisagé que la responsabilité du traitement soit exercée de manière conjointe par les différents acteurs du CRE, chacun dans les limites de ses attributions. Comme dans son avis du 24 novembre 2010 relatif à la création d'un dossier médical électronique partagé[112] (le « DSP »), la CNPD relève que les différents acteurs en rapport avec la création et la mise en place du CRE ont des rôles et obligations différentes. Elle estime en outre que les raisons ayant conduit les auteurs du projet de loi à qualifier l'Agence de responsable de traitement unique du CRE ne ressortent pas clairement du projet de texte ni du commentaire de ses articles.

Une telle approche signifierait que toutes les obligations et responsabilités prévues par la loi sur la protection des données incomberaient à l'Agence. La Commission nationale constate que les différentes obligations qui incombent au responsable du traitement sont, dans le projet de loi, éclatées entre différents intervenants au CRE. Or, en cas de non-respect des différentes obligations légales, le texte sous examen ne règle pas la question de la responsabilité.

3) Les données traitées

Les catégories de données traitées au sein du CRE sont les suivantes :

- les données d'identification du patient ;

- les données médicales et autres informations relatives aux actes de radiodiagnostic, de radiologie interventionnelle et des types d'examens d'imagerie n'entraînant pas d'exposition aux rayonnements ionisants.

S'agissant des données d'identification, l'article 99 paragraphe (1) du projet de loi précise que les sources de données fournissent les données nécessaires à l'identification du patient. Il précise en outre qu'il peut être fait usage du numéro d'identification de la personne physique. La Commission nationale estime

[112] Avis de la Commission nationale relatif au projet de loi n°6196 portant réforme du système de soins de santé et modifiant : 1) le Code de la sécurité sociale ; 2) la loi modifiée du 28 août 1998 sur les établissements hospitaliers (Délibération n°345/2010 du 24 novembre 2010).

que la finalité d'utilisation du numéro d'identification de la personne devrait être explicitement mentionné au sein de cet article. En outre, la CNPD recommande d'ajouter dans le texte de l'article 99 du projet de loi que l'identification du patient soit faite sous les conditions de la loi du 19 juin 2013 relative à l'identification des personnes physiques, au registre national des personnes physiques, à la carte d'identité, aux registres communaux des personnes physiques. Concernant la formulation « *les sources de données* » dans l'article 99 paragraphe (1) du projet de loi, la CNPD recommande de préciser quelles sont ces sources.

S'agissant plus particulièrement des données d'identification géographique du patient, la Commission nationale accueille favorablement le fait que le code postal de l'adresse du patient sans ses deux derniers chiffres soit conservé au sein du CRE, en application de l'article 99 paragraphe (3) du projet de loi.

Le paragraphe (2) de l'article 99 du projet de loi prévoit que l'utilisation des données d'identification du patient est limitée aux opérations strictement nécessaires à l'interconnexion des données ou au contrôle technique des données. A cet égard, la CNPD s'interroge sur les données exactes qui seront utilisées par l'Agence à des fins d'interconnexion.

4) L'information préalable et les droits du patient

La Commission nationale constate que les articles 95 et 96 paragraphe (2) du projet de loi concernant l'information préalable du patient concerné ont été rédigés en conformité avec l'article 26 de la loi modifiée du 2 août 2002 en relation avec le droit à l'information de la personne concernée.

De manière plus générale, la CNPD note que, selon l'article 93 paragraphe (7) du projet de loi, les auteurs du projet de loi ont soumis le CRE à l'application de la loi modifiée du 2 août 2002, ce dont elle se félicite.

S'agissant du droit d'opposition du patient, la CNPD constate qu'à l'instar du dispositif prévu dans le cadre du DSP, le patient dispose de la possibilité de s'opposer avant le début du traitement de ses données mais aussi après, i.e. à tout moment, en utilisant un formulaire standard précisant les conséquences possibles d'une opposition. Elle note que ce droit d'opposition devra être exercé par le patient soit directement, soit par l'intermédiaire du médecin demandeur ou réalisateur de soins de santé responsable de sa prise en charge. La Commission nationale s'interroge toutefois sur la manière dont le formulaire standard est rendu accessible en pratique et si un tel formulaire va, entre autres, être distribué

lors de l'information préalable du patient.

La Commission nationale estime que l'information préalable du patient assortie d'un droit du patient de s'opposer à tout moment au traitement de ses données est respectueuse du droit du patient à son autodétermination informationnelle. En outre, la CNPD accueille favorablement la mention explicite du fait que l'opposition du patient ne portera pas atteinte au droit du patient à recevoir des soins de santé appropriés.

Lorsque le patient signale son opposition avant le début du traitement, il ressort de l'article 96 paragraphe (4) du projet de loi que ses données ne sont pas communiquées au carnet radiologique électronique.

Lorsque l'opposition est signalée après le début du traitement des données, il ressort de l'article 96 paragraphe (5) du projet de loi que cette opposition, ainsi que la demande de rectification ou d'effacement, n'a aucun effet rétroactif sur les données agrégées, le cas échéant déjà générées, par le CRE. Dans cette hypothèse, la CNPD s'interroge sur le sort des données enregistrées dans le CRE et leur destin après une opposition signalée du patient. Le paragraphe 5 de l'article mentionné ci-dessus n'est pas suffisamment précis en ce qui concerne les données existantes dans le CRE. La Commission nationale estime nécessaire de préciser ce que l'Agence fera des données individuelles déjà enregistrées dans le CRE (suppression ou destruction ? Immédiate ou dans un délai raisonnable ?). Elle recommande de compléter le paragraphe (5) de l'article 96 du projet de loi sur ce point.

Dans ce contexte, la CNPD regrette que le projet de loi n'ait pas été accompagné des projets des règlements grand-ducaux mentionnés dans l'article 94 paragraphe (4), l'article 95 paragraphe (2) et l'article 96 paragraphe (7) du projet de loi.

5) La conservation des données

En application de l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002, les données à caractère personnel traitées par l'Agence devraient en principe être conservées, sous une forme permettant l'identification des personnes concernées, pendant une période n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles les données ont été collectées.

La Commission nationale note une divergence entre la deuxième phrase de l'article 97 paragraphe (1) du projet de loi, et le paragraphe (2) du même article.

Les données à caractère personnel du patient peuvent, d'une part, être conservées pour une durée de vingt ans après la date du dernier acte d'imagerie intégré dans le CRE (article 97 paragraphe (1) du projet de loi) et, d'autre part, les données à caractère personnel se rapportant à la santé sont effacées au plus tard dix ans après le décès du patient ou, lorsque le devenir du patient concerné est inconnu, lorsque le patient atteint l'âge de cent quinze ans (article 97 paragraphe (2) du projet de loi).

Si les données mentionnées à l'article 97 paragraphe (1) du projet de loi ne se réfèrent pas à des données relatives à la santé, à quelles données cet article se réfère-t-il ? Dans le cadre du CRE il s'agit d'un traitement des données à caractère personnel relatives à la santé d'un patient. De ce chef, la différence entre le 1er paragraphe et le 2ème paragraphe n'est pas compréhensible dans la rédaction actuelle de l'article.

En outre, la CNPD s'interroge sur la justification des durées de conservation assez longues des données mentionnées au paragraphe 2 de l'article 97 du projet de loi, en l'absence de précisions des auteurs du projet de loi sur ce point.

6) L'interconnexion et le transfert de données

Annexes

L'article 98 paragraphe (1) du projet de loi prévoit que :
« (1) L'Agence est chargée de procéder à l'interconnexion des données visées à l'article 93, à la plateforme eSanté afin de faciliter et améliorer la coopération du médecin demandeur, du médecin réalisateur et des autres professionnels participant à la prise en charge du patient lors du recours aux examens d'imagerie médicale et à en promouvoir le bon usage dans l'intérêt du patient.»

La CNPD se demande si le traitement de données visé à l'article 98 du projet de loi constitue une interconnexion au sens de la loi sur la protection des données et s'interroge sur les opérations qui seront réalisées pour partager les données visées à l'article 93 à la plateforme eSanté.

7) La mise à disposition de données à des tiers

Selon l'article 100 paragraphe (1) du projet de loi, les données visées à l'article 93 du projet de loi peuvent être mises à disposition de tiers, soit à des fins statistiques ou scientifiques de santé publique, soit à des fins de recherche dans le cadre d'un projet de recherche dûment approuvé par le Comité National d'Ethique de Recherche. Cette mise à disposition est qualifiée comme un traitement ultérieur des données au sens de l'article 4 paragraphe (2). Conformément à la législation actuelle, à savoir l'article 14 paragraphe (1) lettre (c) de la loi modifiée du 2 août 2002 un tel traitement de données est soumis à l'autorisation préalable de la CNPD. La Commission nationale suggère dès lors de remplacer le mot « notifié » dans l'article 100 paragraphe (1) du projet de loi par « autorisé ».

L'article 100 paragraphe (2) du projet de loi prévoit un choix entre la pseudonymisation et l'anonymisation des données mises à disposition à des tiers. La CNPD rappelle que, chaque fois que les finalités statistiques ou de recherche scientifique peuvent être atteintes par un traitement ultérieur ne permettant pas ou plus l'identification des personnes concernées, il convient de procéder de cette manière. Dans l'hypothèse où il serait procédé à une anonymisation des données visées à l'article 93 du projet de loi, la Commission nationale souligne qu'une attention particulière doit être portée sur la robustesse du procédé utilisé, conformément à l'avis du groupe de travail de l'article 29 sur les techniques d'anonymisation[113].

En outre, la CNPD suggère de supprimer la deuxième phrase de l'article 100 paragraphe (2) du projet de loi parce qu'elle considère que la méthode de pseudonymisation à mettre en œuvre par le responsable de traitement dépend du contexte

[113] Avis 05/2014 du Groupe de travail « Article 29 » sur les techniques d'anonymisation (WP 216 du 10 avril 2014).

de mise en œuvre dudit traitement. Dès lors, la méthode de pseudonymisation décrite dans la deuxième phrase de l'article 100 paragraphe (2) pourrait ne pas correspondre aux pratiques et exigences d'une pseudonymisation ou anonymisation selon les règles de l'art. En effet, le simple remplacement du numéro d'identification d'une personne physique par un nouveau code ne saurait être considéré comme une pseudonymisation selon les règles de l'art.

8) Les mesures de sécurité

L'article 98 paragraphe (2) lettre a) du projet de loi indique que les modalités techniques d'intégration du CRE dans la plateforme eSanté et de son fonctionnement, y compris le transfert et le stockage des données recueillies au carnet, seront précisées par un règlement grand-ducal (pris après avoir demandé l'avis de la Commission nationale ; voir le commentaire de la CNPD sur ce point au chapitre IV chiffre 6) de cet avis).

Compte tenu de l'importance de garantir un niveau de sécurité particulièrement élevé du CRE, la Commission nationale salue le fait que les auteurs du projet de loi l'associent à cette démarche. Néanmoins, la CNPD regrette que le projet de loi sous examen n'ait pas immédiatement été accompagné des projets de règlements grand-ducaux y afférents, ce qui aurait mis la Commission nationale en mesure d'apprécier plus concrètement les mesures d'exécution des dispositions législatives en projet et d'éviter ainsi d'éventuelles lacunes législatives.

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

Ainsi décidé à Esch-sur-Alzette en date du 14 juillet 2017.

La Commission nationale pour la protection des données,

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

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

Délibération n°637/2017
du 21 juillet 2017

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'« *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*

Annexes

réglementaires ou administratives émises sur base de la présente loi ».

Par courrier du 24 avril 2017, Monsieur le Ministre de l'Economie a invité la Commission nationale à se prononcer sur les amendements parlementaires adoptés par la commission parlementaire de l'économie au sujet du projet de loi n°6708 relative au contrôle de l'exportation, du transfert, du transit et de l'importation des biens de nature strictement civile, des produits liés à la défense et des biens à double usage ; au courtage et à l'assistance technique ; au transfert intangible de technologie ; à la mise en œuvre de résolutions du Conseil de sécurité des Nations unies et d'actes adoptés par l'Union européenne comportant des mesures restrictives en matière commerciale à l'encontre de certains Etats, régimes politiques, personnes, entités et groupes (ci-après « les amendements parlementaires »).

Pour rappel, la CNPD a émis un premier avis relatif au projet de loi sous examen le 6 juillet 2016 (délibération n°611/2016)[114], dans lequel elle a formulé des observations relatives à l'article 37 dudit projet de loi, en l'absence de précisions dans le projet de règlement grand-ducal quant aux traitements de données effectués. Elle a également souligné que le projet de loi devrait préciser (i) qui est le responsable du traitement (ii) quelles sont les finalités des traitements et (iii) définir plus précisément les catégories de destinataires des données.

A la lecture des amendements parlementaires, la CNPD constate que ces précisions font toujours défaut dans le projet de loi sous examen. Sur ce point, la CNPD rappelle qu'un arrêt de la Cour constitutionnelle du 29 novembre 2013 précise que « *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* ».

Par ailleurs, le Conseil d'Etat a estimé, dans son avis du 15 juillet 2016 relatif au projet de loi sous examen, que le paragraphe 3 de l'article 37 dudit projet de loi, à savoir « *le traitement, par l'Office du contrôle des exportations, importations et du transit, des données à caractère personnel collectées dans le cadre de ses missions, est mis en œuvre par voie de règlement grand-ducal tel que prévu par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel* » pouvait être supprimé. Le Conseil d'Etat souligne, en effet, que « *la loi modifiée du 2 août 2002 (…) s'applique de toute façon et si des règlements grand-ducaux sont nécessaires, ils tireront leur*

[114] Document parlementaire n°6708/06.

base légale de cette loi et en particulier de son article 17 ».

La Commission nationale remarque que les auteurs des amendements parlementaires ont pris en compte les recommandations du Conseil d'Etat, en supprimant le paragraphe 3 de l'article 37 du projet de loi.

Quand bien même la Commission nationale comprend la suppression de cette disposition, elle regrette que le projet de règlement grand-ducal joint au projet de loi ne précise pas les conditions et modalités applicables aux traitements de données à caractère personnel effectués par l'Office du contrôle des exportations, importations et du transit, conformément à l'article 17 de la loi modifiée du 2 août 2002. En effet, en partant du principe que l'identification du responsable du traitement, les finalités et les destinataires du traitement des données devraient figurer dans la loi, le règlement grand-ducal devrait pour le moins préciser les données ou catégories de données traitées, l'origine de ces données, la durée de conservation des données ainsi que les mesures de sécurité et de confidentialités des données.

En l'absence de dispositions en ce sens dans le projet de loi et le projet de règlement grand-ducal joint, la Commission nationale est d'avis que les traitements de données effectués par l'Office du contrôle des exportations, importations et du transit ne repose pas sur une base légale suffisante lui permettant d'apporter une sécurité juridique aux traitements qu'il effectue. Elle estime dès lors nécessaire que le projet de loi et le projet de règlement grand-ducal joint soit complété sur ces points.

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

Ainsi décidé à Esch-sur-Alzette en date du 21 juillet 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis complémentaire relatif au projet de loi n°7024 portant mise en œuvre du règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, et portant modification : 1. de la loi modifiée du 5 avril 1993 relative au secteur financier ; 2. de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; 3. de la loi modifiée du 5 août 2005 sur les contrats de garantie financière ; 4. de la loi modifiée du 11 janvier 2008 relative aux obligations de transparence des émetteurs ; 5. de la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif ; 6. de la loi modifiée du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs ; et 7. de la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement

Délibération n°654/2017
du 27 juillet 2017

Conformément à l'article 32, paragraphe (3), lettre (e) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après « la loi du

2 août 2002 »), la Commission nationale pour la protection des données (ci-après « la CNPD » ou « 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 31 mars 2017, Monsieur le Ministre des Finances a fait parvenir à la CNPD des amendements gouvernementaux concernant le projet de loi n°7024 portant mise en œuvre du règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte, et portant modification : 1. de la loi modifiée du 5 avril 1993 relative au secteur financier ; 2. de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ; 3. de la loi modifiée du 5 août 2005 sur les contrats de garantie financière ; 4. de la loi modifiée du 11 janvier 2008 relative aux obligations de transparence des émetteurs ; 5. de la loi modifiée du 17 décembre 2010 concernant les organismes de placement collectif ; 6. de la loi modifiée du 12 juillet 2013 relative aux gestionnaires de fonds d'investissement alternatifs ; et 7. de la loi modifiée du 18 décembre 2015 relative à la défaillance des établissements de crédit et de certaines entreprises d'investissement (ci-après « les amendements » ou « les amendements gouvernementaux »).

Pour rappel, la CNPD a rendu un premier avis relatif au projet de loi n°7024 le 16 mars 2017 (délibération n°243/2017), dans lequel elle s'est limitée à formuler des observations concernant les modifications proposées à l'article 41 de la loi modifiée du 5 avril 1993 relative au secteur financier (ci-après « la loi modifiée du 5 avril 1993 »). Selon l'exposé des motifs des amendements gouvernementaux, les amendements ne se limitent pas à la modification du régime applicable à la sous-traitance dans le secteur financier, mais *« proposent de moderniser en outre le régime de l'outsourcing dans les secteurs de l'assurance et des services de paiement… »*[115], à savoir les régimes prévus par la loi modifiée du 10 novembre 2009 relative aux services de paiement (ci-après « la loi modifiée du 10 novembre 2009 ») et la loi modifiée du 7 décembre 2015 sur le secteur des assurances (ci-après « la loi modifiée du 7 décembre 2015 »). Compte tenu de l'élargissement du champ d'application du projet de loi, la Commission nationale entend formuler des observations sur les amendements traitant des aspects

[115] Doc. parl. 7024/5, Exposé des motifs, p. 1-2.

liés au respect de la vie privée et à la protection des données à caractère personnel.

A l'instar de son avis du 16 mars 2017, la CNPD analysera les amendements gouvernementaux à la lumière de la loi modifiée du 2 août 2002, d'une part, et du nouveau Règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (ci-après « le RGPD »), qui entrera en vigueur le 25 mai 2018, d'autre part.

I. S'agissant des amendements 5 et 6

Les amendements 5 et 6 prévoient d'ajouter un article 36-2 à la loi modifiée du 5 avril 1993, respectivement de modifier l'article 37-1 de cette même loi, afin d'assurer *« un encadrement adéquat de l'externalisation »*[116] par les établissements de crédit, les entreprises d'investissement et les professionnels du secteur financier (PSF) autres que les entreprises d'investissement.

La CNPD salue le choix des auteurs des amendements d'encadrer chaque situation de sous-traitance par un contrat de service. Elle note encore avec satisfaction que les amendements tendent à soumettre la sous-traitance en cascade à l'acceptation préalable par la personne, établie au Luxembourg et soumise à la surveillance prudentielle de la Commission de Surveillance du Secteur Financier (ci-après « la CSSF ») ou de la Banque centrale européenne (ci-après « la BCE »), à l'origine de la sous-traitance. La CNPD se demande toutefois qui est visé par le terme « personne ». Il y aurait lieu de préciser qu'il s'agit en fait de l'entité régulée. Ensuite, elle regrette que les amendements ne prévoient pas expressément que l'obligation de conclure un contrat de service s'étend à la sous-traitance en cascade et elle réitère à cet égard la recommandation émise au point III. de son avis du 16 mars 2017. La CNPD rappelle que l'article 28, paragraphe (4) du RGPD précise que *« [l]orsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément au paragraphe 3, sont imposées à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations. »*

Par ailleurs, la CNPD accueille favorablement l'ajout d'un nouvel alinéa 5 au nouvel article 37-1 de la loi modifiée du 5 avril 1993 (par le biais de l'amendement 6) qui encadre les mesures de sécurité à mettre en place par les établissements de crédit et les entreprises d'investissement. Bien que cette disposition constitue la transposition à l'identique de l'article 16, paragraphe (5), alinéa 3 de la Directive 2014/65/UE[117], il serait opportun d'ajouter à l'article 36-2 de la loi modifiée du 5 avril 1993 (dans sa version modifiée par les amendements gouvernementaux), une formulation similaire à celle prévue à l'alinéa 5 du nouvel article 37-1, tel que modifié par les amendements gouvernementaux, afin d'établir un niveau de sécurité cohérent entre les établissements de crédit, les entreprises d'investissement et les PSF

[116] Doc. parl. 7024/5, Texte et commentaire des amendements gouvernementaux, p. 8 et 9.
[117] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE.

autres que les entreprises d'investissement.

A cet égard, en ce qui concerne la protection des données à caractère personnel, la CNPD rappelle l'obligation, telle qu'exposée dans son avis du 16 mars 2017, pour ces entités de mettre en place des mesures appropriées afin d'assurer la protection des données et de garantir un niveau de sécurité adapté aux risques[118].

II. S'agissant de l'amendement 8

L'amendement 8 concerne la modification de l'article 41 de la loi modifiée du 5 avril 1993, qui traite du régime du secret professionnel dans le secteur financier.

La CNPD note que les auteurs des amendements ont supprimé la distinction faite entre la sous-traitance intra-groupe et la sous-traitance extra-groupe, de sorte que le projet de loi dans sa version amendée établit uniquement une distinction entre la sous-traitance des activités d'un prestataire établi au Luxembourg, soumis à la surveillance prudentielle de la CSSF, de la BCE ou du Commissariat aux Assurances et tenu à une obligation de secret pénalement sanctionnée, et « *tous les autres cas de sous-traitance* »[119].

Les amendements précisent que dans tous ces autres cas de sous-traitance, une entité régulée ne pourrait partager des données couvertes par le secret professionnel avec son sous-traitant sauf lorsque les clients ont préalablement consenti à la sous-traitance des services sous-traités, au type de renseignements transmis dans le cadre de la sous-traitance et au pays d'établissement des entités prestataires des services sous-traités « *conformément à la loi ou selon les modalités d'information convenues entre parties* ».

Cette dernière formulation suscite des interrogations au niveau de l a manière selon laquelle les clients doivent accepter la sous-traitance. La CNPD se demande en effet si un consentement « *conformément à la loi* » est celui qui doit être conforme à la règlementation relative à la protection des données à caractère personnel[120] ? Dans l'affirmative, ce consentement devrait respecter les exigences strictes relatives au consentement prévues par la loi modifiée du 2 août 2002, et à l'avenir par le RGPD[121]. La CNPD rappelle qu'afin d'être conforme aux exigences du RGPD à partir du 25 mai 2018, le consentement doit être libre, spécifique, éclairé et univoque et obtenu par une déclaration ou par un acte positif clair. Le RGPD s'oppose ainsi à ce que le consentement puisse être déduit « *en cas de silence, de cases cochées par défaut ou d'inactivité* »[122]. De plus, si le consentement de la personne concernée au traitement

[118] Délibération n°243/2017, point VI.
[119] Doc. parl. 7024/5, Commentaire des amendements gouvernementaux, p. 11.
[120] Voir l'avis complémentaire de la Chambre de Commerce du 30 mai 2017, doc. Parl. n°7024/06, p. 4-5 et l'avis complémentaire du Conseil d'Etat du 14 juillet 2017, doc. parl. n° 7024/08, p. 6-7.
[121] Voir les articles 2, lettre (c), et 5 de la loi modifiée du 2 août 2002 et les articles 4, paragraphe (11), 6 et 7 du RGPD.
[122] RGPD, considérant 32.

est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement doit être « *présentée sous une forme qui la distingue clairement de ces autres questions sous une forme compréhensible et aisément accessible* »[123]. Elle doit également être « *formulée en des termes clairs et simples* »[124].

Cependant, les auteurs des amendements laissent la possibilité aux entités régulées de recueillir le consentement « *selon les modalités d'information convenues entre parties* ». La CNPD se demande, tout comme le Conseil d'Etat, si ceci implique que le consentement du client pourrait être tacite[125]. Le texte présente dès lors une incertitude au niveau de la procédure du recueil du consentement qui devrait être mise en place par l'entité régulée dans la mesure où deux modes d'acceptation n'obéissant pas aux mêmes exigences seraient possibles.

A cet égard, la CNPD s'interroge aussi sur la précision dans le commentaire des amendements qu'« *outre les exigences qui [sont indiquées dans la disposition en question], l'entité luxembourgeoise qui sous-traite devra veiller au respect de la législation sur la protection des données* »[126]. En indiquant ceci, est-ce que les auteurs des amendements souhaitent souligner qu'il s'agit de deux régimes distincts et que l'acceptation « *conformément à la loi* » ne viserait pas la règlementation en matière de protection des données ?

Compte tenu de l'insécurité juridique que pourrait causer l'amendement 8, la CNPD estime nécessaire de préciser la disposition en question.

Pour le surplus, la CNPD réitère ses commentaires formulés aux points IV. et V. de son avis du 16 mars 2017 relatifs aux transferts de données vers des pays tiers et au sujet de l'information des personnes concernées, qui n'ont pas été pris en compte dans les amendements sous examen.

III. S'agissant des amendements 9 et 16

Les amendements 9 et 16 traitent de la modification de la loi modifiée du 10 novembre 2009 relative aux services de paiement et la loi modifiée du 7 décembre 2015 sur le secteur des assurances, afin d'aligner le libellé des dispositions relatives au secret professionnels desdites lois sur le nouveau libellé de l'article 41 de la loi modifiée du 5 avril 1993, tel qu'il résulte des amendements gouvernementaux[127].

Il ressort du commentaire des amendements gouvernementaux que ceux-ci visent à assurer une cohérence entre les régimes d'obligation au secret professionnel du secteur financier, du secteur des services de paiement et du secteur des assurances[128].

Cependant, contrairement aux exigences prévues pour les établissements de crédit, les entreprises d'investissement et les PSF autres que les entreprises d'investissement aux amendements 5 et 6, les amendements ne prévoient pas que la sous-traitance effectuée dans le secteur des services de paiement et dans le secteur des assurances devra être entouré d'un contrat de service, et ne prévoit pas non plus que l'entité à l'origine de la sous-traitance devra donner son accord à la sous-traitance en cascade.

Dans un souci de cohérence, la Commission nationale estime dès lors nécessaire d'imposer ces mêmes exigences pour la sous-traitance ayant lieu dans le secteur des services de paiement et dans le secteur des assurances.

Les commentaires de la CNPD précédemment formulés concernant l'acceptation de la sous-traitance, l'encadrement contractuel de la sous-traitance en cascade, le transfert de données vers des pays tiers, l'information des personnes concernées et aux mesures de sécurité restent bien évidemment valables pour les amendements 9 et 16.

---

[123] RGPD, art. 7, paragraphe (2).
[124] RGPD, art. 7, paragraphe (2).
[125] Voir l'avis complémentaire du Conseil d'Etat du 14 juillet 2017, doc. parl. n°7024/08, p. 7.
[126] Doc. parl. 7024/5, Commentaire des amendements gouvernementaux, p. 12.
[127] Doc. parl. 7024/5, Texte et commentaire des amendements gouvernementaux, p. 15 et 28.
[128] Doc. parl. 7024/5, Texte et commentaire des amendements gouvernementaux, p. 15 et 28.

Annexes

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

Ainsi décidé à Esch-sur-Alzette en date du 27 juillet 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis à l'égard du projet de loi portant modification de la loi modifiée du 25 février 1979 concernant l'aide au logement et modifiant certaines dispositions du Code civil

Délibération n°884/2017 du 27 octobre 2017

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 Monsieur le Ministre du Logement en date du 12 septembre 2017, la Commission nationale entend présenter ci-après ses observations au sujet du projet de loi portant modification de la loi modifiée du 25 février 1979 concernant l'aide au logement et modifiant certaines dispositions du Code civil.

Le projet de loi sous objet entend plus précisément modifier les articles 14*quinquies* et 14*sexies* de la loi précitée du 25 février

1979. Ces articles, relatifs à la subvention de loyer en faveur de ménages à faible revenu, ont été introduits par la loi du 9 décembre 2015 portant introduction d'une subvention de loyer. Lors du processus législatif ayant conduit à l'adoption de cette loi, la Commission nationale a déjà eu l'occasion d'émettre un avis en date du 21 juillet 2014[129], ainsi qu'un avis complémentaire en date du 2 juillet 2015[130]. Alors que la plupart des recommandations émises par la CNPD dans son premier avis avaient été prises en compte par les auteurs de ce projet de loi, les observations exprimées à l'occasion de son avis complémentaire n'ont par contre pas été intégrées dans la loi.

La Commission nationale constate que les modifications apportées aux articles 14*quinquies* et 14*sexies* par le projet de loi sous examen n'entraînent aucun changement en matière de protection des données à caractère personnel, et n'appellent par conséquent aucun commentaire supplémentaire.

La Commission nationale se demande s'il ne serait toutefois pas opportun de profiter du présent projet de loi pour intégrer les recommandations relatives à l'article 14*sexies* de la loi précitée du 25 février 1979, déjà exprimées dans son avis complémentaire du 2 juillet 2015[131], et qui n'ont pas été intégrées dans la loi du 9 décembre 2015 portant introduction d'une subvention de loyer.

Ainsi décidé à Esch-sur-Alzette en date du 27 octobre 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis complémentaire relatif au projet de loi n°7061 modifiant certaines dispositions du Code de la sécurité sociale

Délibération n°930/2017 du 17 novembre 2017

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 31 juillet 2017, Monsieur le Ministre de la Sécurité Sociale a fait parvenir à la Commission nationale une série d'amendements parlementaires au projet de loi n°7061 modifiant certaines dispositions du Code de la sécurité sociale (ci-après « les amendements » ou « les amendements parlementaires »).

Pour rappel, la CNPD a rendu, le 2 décembre 2016[132], un premier avis relatif au projet de loi

[129] Délibération no 339/2014 du 21 juillet 2014 de la Commission nationale pour la protection des données, document parlementaire 6542/06.
[130] Délibération no 258/2015 du 2 juillet 2015 de la Commission nationale pour la protection des données, document parlementaire 6542/11.
[131] *Idem*.
[132] Délibération n°1005/2016 du 2 décembre 2016 portant avis de la CNPD relatif au projet de loi n°7061 modifiant certaines dispositions du Code de la sécurité sociale.

Annexes

n°7061 (ci-après « le projet de loi ») dans lequel elle a formulé des observations concernant les adaptations apportées par le projet de loi à l'article 60*ter* du Code de la sécurité sociale concernant les missions et les moyens de l'Agence nationale des informations partagées dans le domaine de la santé (ci-après désignée « l'Agence eSanté »). Le Conseil d'Etat s'est quant à lui prononcé sur le projet de loi dans un avis rendu le 28 mars 2017[133]. Les auteurs des amendements parlementaires ont indiqué avoir pris en considération les observations formulées par le Conseil d'Etat dans son avis initial.

La CNPD regrette que les amendements parlementaires du 20 juin 2017 ne lui aient été communiqués que le 31 juillet 2017, soit plus d'un mois après leur adoption par la Commission du Travail, de l'Emploi et de la Sécurité sociale de la Chambre des députés. Elle espère toutefois que son avis complémentaire parviendra en temps utile aux auteurs du projet de loi.

La Commission nationale entend limiter ses observations à l'amendement parlementaire n°1, qui modifie l'article 60ter précité du Code de la sécurité sociale. Cet amendement prévoit de définir avec davantage de précisions les informations contenues dans les fichiers du Centre commun de la sécurité sociale (CCSS) et de la Caisse nationale de santé (CNS) auxquelles l'Agence eSanté sera habilitée à accéder, ainsi que la finalité de cet accès.

Dans son avis initial, la CNPD s'était souciée du manque de précisions de la rédaction initiale du projet de loi s'agissant des finalités poursuivies par cet accès octroyé à l'Agence eSanté. Elle avait par ailleurs souligné le risque que le projet de loi soit considéré comme incompatible avec les principes dégagés par la Cour constitutionnelle et la position constante du Conseil d'Etat sur le cadrage normatif devant résulter de la loi.

Par son avis du 28 mars 2017, le Conseil d'Etat s'était formellement opposé à la reformulation vague et permissive de l'article 60ter précité par les auteurs du projet de loi. Le Conseil d'Etat considère en effet dans son avis que la rédaction retenue par les auteurs du projet de loi permettrait à l'Agence eSanté un « *accès généralisé sans restriction aucune et sans indication des objectifs poursuivis* » aux données contenues dans les fichiers du CCSS et de la CNS, contraire aux exigences de protection de la vie privée telles qu'elles résultent de l'article 11, paragraphe 3 de la Constitution du Grand-Duché de Luxembourg.

La CNPD accueille donc favorablement l'effort des auteurs des amendements tendant à

[133] Conseil d'Etat, Avis du 28 mars 2017 relatif au projet de loi modifiant certaines dispositions du Code de la sécurité sociale, doc. parl. 7061/05, n °CE : 51.787.

délimiter plus clairement l'accès de l'Agence eSanté aux fichiers du CCSS et de la CNS et ainsi à préciser tant les informations visées que les finalités poursuivies par un tel accès.

Elle note qu'aux termes de l'amendement n°1, afin de pouvoir mettre en œuvre l'annuaire référentiel d'identification des patients, d'une part, et l'annuaire référentiel d'identification des prestataires de soins, d'autre part, l'Agence eSanté sera désormais habilitée à recourir aux données suivantes :

- les données énumérées à l'article 5, paragraphe 2, points a), b), c), d), e), h), j), k), et m) de la loi modifiée du 19 juin 2013 relative à l'identification des personnes physiques, à savoir, les nom et prénoms, la résidence habituelle, les date et lieu de naissance, la situation de famille, le sexe, les numéros d'identification des père et mère, les numéros d'identification des enfants, les date et lieu de décès ;

- les données d'affiliation des patients fournies par le CCSS ;

- les données des registres professionnels des personnes autorisées à exercer légalement une profession réglementée dans le domaine de la santé qui sont fournies par le ministre ayant la Santé dans ses attributions ;

- les données relatives à l'enregistrement d'un prestataire auprès de la CNS.

La Commission nationale estime ces données adéquates, pertinentes et non excessives au regard de la finalité de mise en œuvre des annuaires d'identification des patients et des prestataires de soins, conformément à l'article 4 paragraphe (1), lettre (a) de la loi modifiée du 2 août 2002. Elle observe que les auteurs des amendements ont pris le soin de préciser que l'accès aux données précitées devra s'effectuer dans le respect des dispositions légales en matière de protection des données et d'accès au registre national d'identification des personnes physiques. Bien que cette précision aille de soi, la CNPD l'accueille favorablement du fait du rôle pédagogique qu'elle pourra jouer à l'égard du responsable de traitement de ces annuaires et des personnes concernées.

La Commission nationale accueille également favorablement la proposition des auteurs du projet de loi de renvoyer à un règlement grand-ducal spécifique (et non au règlement grand-ducal visé à l'article 60*quater*, paragraphe 6 du code de la sécurité sociale qui concerne spécifiquement le Dossier de soins partagé) le soin de préciser les modalités de gestion de l'identification et les catégories de données contenues dans les annuaires référentiels d'identification, conformément aux recommandations formulées sur ce point par la CNPD[134] et par le Conseil d'Etat[135].

En dernier lieu, la Commission nationale regrette, en dépit des recommandations qu'elle a pu formuler à ce sujet, que les auteurs des amendements n'aient pas saisi l'opportunité des modifications sous examen pour clarifier les missions de l'Agence eSanté, s'agissant de l'offre d'un service de pseudonymisation en qualité de tiers de confiance. A ce titre, elle avait formulé dans son avis du 2 décembre 2016 les observations suivantes :

« Elle regrette toutefois que les auteurs du projet de loi n'aient pas saisi l'opportunité du projet de loi sous examen pour clarifier les missions de l'Agence eSanté, s'agissant plus particulièrement du cadre applicable à l'offre d'un service de pseudonymisation en qualité de tiers de confiance. La CNPD tient à souligner qu'un encadrement général de l'activité de tiers de confiance fournissant ce type de services serait préférable et permettrait d'accompagner le développement de services innovants en matière de pseudonymisation et d'anonymisation au Luxembourg. Elle considère en outre que de tels services devraient être

[134] Délibération n°1005/2016 du 2 décembre 2016 précitée.
[135] Conseil d'Etat, Avis n°51.787 du 28 mars 2017 précité.

réservés à des acteurs présentant des garanties d'indépendance, de compétence et ne se trouvant pas en situation de conflit d'intérêts au regard des données qu'ils traitent dans le cadre de leurs diverses activités. Pour autant, dans l'attente d'un encadrement général de l'activité de tiers de confiance et compte tenu des fortes attentes en la matière dans le secteur de la santé, la Commission nationale estime qu'une précision textuelle, prenant la forme d'un alinéa supplémentaire à l'article 60ter paragraphe (1), 1) du Code de la sécurité sociale aurait permis d'apporter une meilleure sécurité juridique au service de pseudonymisation développé par l'Agence eSanté, dont la mise en œuvre à vocation à accompagner des projets nationaux importants du point de vue de la santé publique. »

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

Ainsi décidé à Esch-sur-Alzette en date du 17 novembre 2017.

La Commission nationale pourla protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis à l'égard du projet de loi n°7151 relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave

Délibération n°958/2017
du 23 novembre 2017

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

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Sécurité intérieure en date du 15 juin 2017, la CNPD entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n°7151 relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave (ci-après : « le projet de loi »).

Ledit projet de loi a pour objet de transposer en droit national

la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (ci-après : « la directive PNR »).

Deux autres instruments européens qui constituent le « paquet sur la protection des données » s'ajoutent à la directive PNR, réformant en profondeur le droit de la protection des données au niveau de l'Union européenne. Ainsi, le Parlement européen et le Conseil ont adopté parallèlement en date du 27 avril 2016 :

- le règlement 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après : « le RGPD ») ;

- la directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après : « la directive 2016/680 »).

Suivant l'exposé des motifs, le projet de loi vise à « *régler le transfert des données PNR des transporteurs aériens vers une unité centrale nationale ayant pour mission la répression et la prévention des infractions terroristes et d'autres formes graves de criminalité ainsi que le traitement ultérieur de ces données.* »

La Commission nationale est bien consciente que le législateur a l'obligation de transposer la directive PNR en droit national au plus tard pour le 25 mai 2018, faute de risquer un recours en manquement de la part de la Commission européenne sur base des articles 258 et 260 du traité sur le fonctionnement de l'Union européenne.

De manière générale, l'intention de la CNPD n'est ainsi pas de remettre en cause en lui-même le système PNR, dont la mise en place a été décidée par le législateur européen « *pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.* »[136] Par ailleurs, à part une restructuration des articles, le projet de loi est quasiment une copie fidèle de la directive PNR. La Commission nationale limite ainsi ses observations aux dispositions où les auteurs du projet de loi ont usé la marge de manœuvre laissée aux Etats-membres lors de la transposition en droit national d'une directive européenne. En effet, une telle directive n'instaure qu'une obligation de résultat, tout en laissant les Etats-membres de l'Union européenne libres quant aux formes et moyens à prendre pour y parvenir.[137]

Néanmoins, la Commission nationale tient à relever à titre préliminaire que la Cour de Justice de l'Union européenne (ci-après : « la CJUE ») a critiqué dans son arrêt « Digital Rights Ireland » que la directive 2006/24 sur la conservation de données par les services de communications électroniques, directive annulée suite audit arrêt, n'avait établi aucune relation entre d'un côté les données collectées et conservées et de l'autre côté une menace à l'ordre public en n'étant pas « *limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves.* »[138]

---

[136] Considérant 6 de la directive PNR.

[137] L'article 288 du traité sur le fonctionnement de l'Union européenne dispose que la « *directive lie tout État membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens.* »

[138] CJUE, arrêt C-293/12 - Digital Rights Ireland et Seitlinger e.a. du 8 avril 2014, paragraphe 59; voir aussi arrêt C-203/15 - Tele2 Sverige du 21 décembre 2016, paragraphe 110.

S'agissant du contexte spécifique des données PNR, la CJUE a par ailleurs pris position dans son avis 1/15 du 26 juillet 2017 concernant l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers. Elle a souligné que pour les passagers aériens où aucun risque en matière de terrorisme ou de criminalité transnationale grave n'a pu être identifié à leur arrivée au Canada et jusqu'à leur départ de ce pays tiers, il n'y existe pas, une fois qu'ils sont repartis, de rapport (directe ou indirecte) entre leurs données PNR et l'objectif poursuivi par l'accord envisagé qui justifierait la conservation de ces données. La CJUE a rejeté les considérations avancées par le Conseil et la Commission se basant sur la durée de vie moyenne des réseaux internationaux de criminalité grave, ainsi que sur la durée et la complexité des enquêtes portant sur ces réseaux, afin de *« justifier un stockage continu des données PNR de l'ensemble des passagers aériens après leur départ du Canada aux fins d'un accès éventuel auxdites données, indépendamment d'un lien quelconque avec la lutte contre le terrorisme et la criminalité transnationale grave. »*[139]

La CJUE a néanmoins aussi relevé que, dans des cas particuliers, l'identification d'éléments objectifs permettant de considérer que certains passagers aériens pourraient, même après leur départ du Canada, présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave, la conservation de leurs données PNR paraissait admissible au-delà de leur séjour au Canada.[140]

Sur base des considérations ci-dessus, la CNPD doute que le système tel que prévu par la directive PNR, fixant une durée de conservation des toutes les données PNR pendant une durée de 5 ans (même si les données sont dépersonnalisées après six mois), indépendamment du fait si le passager est soupçonné d'avoir participé à un acte du terrorisme et de la criminalité grave ou non, garantit que la conservation et l'utilisation des données PNR soient limitées au strict nécessaire. Des inquiétudes quant à la proportionnalité entre le respect des droits des personnes concernées et les intérêts de poursuite des autorités compétentes subsistent. Il est fort probable que la CJUE sera saisi de recours en annulation de la directive PNR à l'instar de la directive 2006/24 sur la conservation de données par les services de communications électroniques.

- <u>Quant au champ d'application</u>

Tout d'abord, la CNPD tient à féliciter les auteurs du projet de loi d'avoir anticipé le dépôt à la Chambre des députés du projet de loi portant transposition de

[139] Avis 1/15 de la CJUE du 26 juillet 2017 concernant l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, paragraphe 205.
[140] Avis 1/15 de la CJUE, précité, paragraphe 207.

la directive 2016/680 et d'y faire référence aux endroits où la directive PNR renvoie encore à la décision-cadre 2008/977, décision qui sera abrogée à partir du 6 mai 2018 par ladite directive.

Dans son article 2, la directive PNR laisse le choix aux Etats-membres de collecter les données PNR, en sus des vols en provenance ou à destination d'un pays tiers, aussi pour l'ensemble ou seulement une partie des vols intra-UE. Dans l'exposé des motifs, les auteurs du projet de loi se réfèrent à une déclaration commune du 4 décembre 2015, par laquelle les ministres européens de la Justice et des Affaires intérieures se sont engagés à faire usage de cette faculté pour justifier la collecte des données PNR pour tous les vols à partir ou en provenance d'un Etat-membre vers le territoire luxembourgeois.

Ainsi, la Commission nationale prend note que les auteurs du projet de loi ont opté, à l'instar de leurs homologues belges, français ou allemands, d'inclure les vols intra-UE dans le champ d'application du projet de loi afin de maximiser l'efficacité du système PNR.

Par ailleurs, la CNPD approuve la décision des auteurs du projet de loi de ne pas avoir étendu le système PNR aux agences ou organisateurs de voyages, ainsi qu'aux d'opérateurs économiques autres que les transporteurs ou auprès de transporteurs autres que les transporteurs aériens.

Comme un tel élargissement du champ d'application du système PNR menacerait de manière encore plus importante les droits fondamentaux des personnes concernées, il paraît raisonnable d'attendre l'évaluation de la Commission européenne de tous les éléments de la directive PNR. Cette évaluation aura lieu au plus tard le 25 mai 2020, c'est-à-dire deux ans après le délai de transposition de la directive PNR, et elle portera notamment sur la nécessité, la proportionnalité, et l'efficacité d'inclure lesdits opérateurs économiques dans le champ d'application de la directive PNR.

Finalement, la CNPD se demande si l'obligation de transmettre à l'Unité d'informations passagers (ci-après : « l'UIP ») les données PNR de tous les passagers de vols à destination ou en provenance du Luxembourg s'impose aussi aux taxis aériens privés. A priori, il paraît qu'une compagnie aérienne privée offrant des vols du et vers le Grand-duché correspond à la définition d'un « transporteur aérien »[141], si elle possède une licence d'exploitation en cours de validité octroyée par la Direction de l'Aviation Civile et si elle assure un transport aérien de personnes.

- Quant aux bases de données et critères d'évaluation

Sur base de l'article 10 du projet de loi, transposant l'article 6, paragraphe (3) de la directive PNR, deux méthodes s'offrent à l'UIP pour évaluer des passagers avant leur arrivée ou leur départ prévu du Grand-duché afin d'identifier des personnes « suspectes » pour lesquelles un examen plus approfondi apparaît nécessaire:

- une comparaison des données PNR aux banques de données gérées par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions ;

- une comparaison des données PNR à des critères préétablis.

Le Contrôleur européen de la protection des données (ci-après : « le CEPD ») avait noté dans ce contexte qu'une évaluation sur base de critères inconnus en constante évolution suscite d'importantes inquiétudes en matière de transparence et de proportionnalité.[142] De même, il a soulevé le caractère controverse, excessif et disproportionné d'un système permettant une confrontation systématique des données PNR à un nombre illimité de bases de données non définies.[143]

Dans le même contexte, l'avocat général Mengozzi avait relevé dans ses conclusions présentées

[141] Article 2, lettre a) du projet de loi : « *transporteur aérien* » : *toute entreprise de transport aérien possédant une licence d'exploitation en cours de validité ou l'équivalent lui permettant d'assurer le transport aérien de personnes* ».

[142] Avis 2011/C 181/02 du 22 juin 2011 du Contrôleur européen de la protection des données sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, paragraphe 16.

[143] Deuxième avis n°5/2015 du CEPD sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, paragraphe 37.

le 8 septembre 2016 sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers le manque de précisions dans l'accord en cause concernant les bases de données et les critères d'évaluation dont la détermination restait de ce fait à l'entière discrétion des autorités canadiennes. Il avait souligné qu'un encadrement précis des critères d'évaluation devrait *« permettre, dans une large mesure, d'aboutir à des résultats ciblant des individus à l'égard desquels pourraient peser un « soupçon raisonnable » de participation à des infractions terroristes ou de criminalité transnationale grave. »*[144] La CJUE a repris la position de l'avocat général dans son avis 1/15 tout en précisant que les bases de données avec lesquelles les données PNR seraient recoupées devraient être fiables, actuelles et limitées à des bases de données exploitées par le Canada en rapport avec la lutte contre le terrorisme et la criminalité transnationale grave.[145]

En prenant en compte les commentaires ci-dessus, la Commission nationale est d'avis que le projet de loi en son état actuel ne définit pas avec exactitude les banques de données en cause. Le commentaire des articles quant à lui mentionne uniquement à titre d'exemple le *« Schengen Information System ou Interpol »*. Or, la Commission nationale se demande si toutes les bases de données prévues à l'article 54 du projet de loi n°7045 portant réforme de la Police grand-ducale et abrogeant la loi du 31 mai 1999 sur la Police et l'Inspection générale de la Police sont visées ? Qu'en est-il de l'accès aux bases de données par le personnel détaché de l'Administration des Douanes et Accises et du Service de Renseignement de l'Etat qui peuvent être membre de l'UIP ?

Par ailleurs, la CNPD constate que l'article 10 du projet de loi ne contient pas de liste exhaustive énumérant les critères d'évaluation, mais prévoit uniquement que les critères doivent *« être ciblés, proportionnés et spécifiques et ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle. »* Le commentaire des articles quant à lui énumère seulement des exemples de critères tel le mode de paiement, le poids du bagage ou l'itinéraire choisi.

La Commission nationale tient à souligner dans ce contexte l'importance fondamentale du principe de licéité d'un traitement de données à caractère personnel qui doit être lu à la lumière de l'article 8, paragraphe 2 de la Convention européenne

[144] Conclusions de l'avocat général M. Paolo Mengozzi présentées le 8 septembre 2016 concernant l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, paragraphes 253 et 256.
[145] Avis 1/15 de la CJUE, précité, paragraphe 172.

des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52, paragraphes (1) et (2) de la Charte des droits fondamentaux de l'Union européenne. En substance, ces deux articles, ensemble avec la jurisprudence constante de la Cour européenne des droits de l'homme, retiennent qu'un traitement de données effectué par une autorité publique peut constituer une ingérence dans le droit au respect de la vie privée ou limiter l'exercice du droit à la protection des données. Cette ingérence ou limitation peut être justifiée à condition qu'elle :

- soit prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante ;

- soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité ;

- respecte le contenu essentiel du droit à la protection des données ;

- réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui.

L'article 6, paragraphe (3) du RGPD, qui sera applicable à partir du 25 mai 2018 dans tous les Etats membres de l'Union européenne, prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans ces deux cas de figure, le fondement et les finalités des traitements de données doivent spécifiquement être prévus soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis.

Suivant ledit article, ces bases légales devraient contenir des dispositions spécifiques concernant, entre autres, les types de données traitées, les personnes concernées, les entités auxquelles les données peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

Au niveau national, la Commission nationale tient à rappeler à cet égard l'exigence de la Cour constitutionnelle selon laquelle « *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.* »[146]

Le Conseil d'Etat rappelle lui aussi régulièrement dans ses avis que « *(…) l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.*

La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication (…). »[147]

Dans l'optique de la CNPD, le projet de loi devrait identifier et énumérer expressément dans le corps du texte les différentes banques de données gérées par les services compétents ou qui leur sont accessibles dans l'exercice de leurs missions. Un règlement grand-ducal pourra alors prévoir une liste exhaustive des critères d'évaluation prédéterminés qui pourrait au besoin être complétée ou modifiée si nécessaire. Le groupe de travail européen « article 29 » a rappelé dans ce contexte l'importance fondamentale de l'existence de critères spécifiques, nécessaires, justifiés et qui sont révisés régulièrement.[148]

La CNPD estime ainsi qu'en l'état actuel, le texte du projet de loi

[146] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015.
[147] Voir par exemple : Conseil d'Etat, Avis n°6975/5 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.
[148] Opinion 10/2011 du groupe de travail "article 29" sur la Proposition de la directive PNR, p. 5.

ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal et ne peut pas être considéré comme étant conforme à l'article 4 de la loi modifiée du 2 août 2002, ni à l'article 8 de la Convention européenne des droits de l'homme, à l'article 52 de la Charte des droits fondamentaux de l'Union européenne, ainsi qu'à l'article 6, paragraphe (3) du RGPD.

- Quant aux différentes catégories de données PNR

L'annexe 1 du projet de loi reprend mot par mot la liste des données PNR prévue à l'annexe 1 de la directive PNR. De même, la liste des données PNR que les transporteurs aériens seraient appelés à transférer en application de l'accord prévu entre le Canada et l'Union Européenne contient pour l'essentiel les mêmes dix-neuf catégories de données. A ce titre, dans les conclusions précitées, l'avocat général Mengozzi avait éprouvé des doutes sérieux quant au libellé suffisamment clair et précis de certaines catégories de données PNR contenues dans ledit accord. Il avait notamment critiqué que parmi les différentes catégories, il y en avait qui étaient « *formulées de manière très, voire excessivement, ouverte, sans qu'une personne raisonnablement informée puisse déterminer soit la nature, soit la portée des données à caractère personnel que ces catégories sont susceptibles de contenir.* »[149] L'avocat général s'était surtout référé à la rubrique relative aux informations disponibles sur les « grands voyageurs ». La même critique avait été soulevée par le CEPD dans son avis de 2011 concernant le champ « remarques générales ».[150]

Dans l'avis 1/15 précité concernant le projet d'accord PNR entre le Canada et l'Union européenne, la Grande Chambre de la CJUE a repris les observations de l'avocat général quant au manque de clarté et de précision de certaines données PNR à transférer. Entre-autres, la CJUE avait estimé que les rubriques « grands-voyageurs » et « remarques générales » « *n'encadrent pas de manière suffisamment claire et précise la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte.* »[151]

Dans le souci de respecter le principe de légalité, la Commission nationale se rallie aux avis de la CJUE et du CEPD et recommande aux auteurs du projet de loi de décrire de manière plus précise et concise les deux catégories de données PNR susmentionnées.

- Quant à la conservation des données

D'après le considérant 26 de la directive PNR, le droit national

[149] Conclusions de l'avocat général M. Paolo Mengozzi, précitées, paragraphe 217.
[150] Avis 2011/C 181/02 du 22 juin 2011 du Contrôleur européen de la protection des données, précité, paragraphe 39.
[151] Avis 1/15 de la CJUE précité, paragraphe 163.

des Etats-membres de l'Union européenne devrait prévoir des durées de conservation spécifiques, si des données PNR ont été transmises à une autorité compétente dans le cadre d'enquêtes ou de poursuites pénales spécifiques. Or, l'article 25, alinéa 2 du projet de loi, prévoyant une obligation d'effacement des données PNR à l'issue de cinq ans, ne s'impose pas si des « *données PNR spécifiques ont été transférées à un service compétent et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière* ». Ainsi, ledit article ne contient pas en lui-même de durée de conservation spécifique à respecter par les services compétents en cas de transfert de données par l'UIP. Dès lors, la Commission nationale recommande aux auteurs du projet de loi d'inclure dans le corps du texte une telle durée de conservation.

- Quant au droit à l'information des personnes concernées

S'agissant du droit des passagers aériens d'être informés du traitement des données à caractère personnel les concernant, la directive PNR ne prévoit qu'en son considérant (29) que les États membres devraient veiller à ce que les passagers reçoivent des informations précises, aisément accessibles et facilement compréhensibles sur la collecte des données PNR, le transfert de celles-ci à l'UIP, ainsi que sur leurs droits en tant que personnes concernées.

En vertu de l'article 30 du projet de loi, l'UIP a l'obligation de mettre à la disposition du public, par les moyens de communication appropriés, un certain nombre d'informations, comme par exemple ses coordonnées, celles du délégué à la protection des données, ou encore les finalités du traitement envisagé. Le corollaire de cette disposition figure à l'article 13 du projet de loi transposant la directive 2016/680. Or, ledit article contient en son paragraphe (2), en sus des informations prévues à l'article 30 du projet de loi, d'autres indications à communiquer à la personne concernée. Il s'agit notamment de la durée de conservation des données à caractère personnel et le cas échéant, des catégories de destinataires des données à caractère personnel, y compris dans les pays tiers ou au sein d'organisations internationales.

Dès lors, dans un souci de concordance entre les deux textes, la Commission nationale suggère aux auteurs du projet de loi d'inclure les deux indications susmentionnées dans les informations que l'UIP doit transmettre au public.

Par ailleurs, la CJUE a mentionné dans son avis 1/15 précité que l'accord PNR prévu entre le Canada et l'Union européenne devrait préciser que l'autorité canadienne compétente a l'obligation d'informer individuellement les passagers aériens, dont les données PNR ont été utilisées et conservées, ainsi que ceux dont les données ont été communiquées à d'autres autorités publiques, d'une telle utilisation et d'une telle communication, et ceci à partir du moment où cette information n'est plus susceptible de compromettre les enquêtes conduites par les autorités publiques visées par l'accord envisagé.[152]

La Commission nationale partage la position de la CJUE et recommande dès lors aux auteurs du projet de loi de prévoir dans le texte sous examen une disposition selon laquelle l'UIP est obligée d'informer les personnes concernées dont les données PNR ont été utilisées ou transférées, tout en y incluant la possibilité d'un retard ou d'une limitation du droit à l'information des personnes concernées conformément à l'article 13, paragraphe (3) du projet de loi transposant la directive 2016/680.

[152] Avis 1/15 de la CJUE précité, paragraphes 223 à 225.

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 23 novembre 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis à l'égard du : 1. projet de règlement grand-ducal modifiant le règlement grand-ducal modifié du 18 décembre 1998 fixant les modalités de la détermination de la dépendance ; 2. projet de règlement grand-ducal déterminant le contenu de la documentation de la prise en charge et les indicateurs de qualité et de la prise en charge ; 3. projet de règlement grand-ducal modifiant le règlement grand-ducal du 21 décembre 2006 fixant les modalités spécifiques de la détermination de la dépendance de l'enfant

Délibération n°959/2017
du 23 novembre 2017

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

Faisant suite à la demande lui adressée par Monsieur le Ministre de la Sécurité sociale en date du 1ier septembre 2017, la CNPD entend présenter ci-après ses

réflexions et commentaires au sujet de trois différents projets de règlements grand-ducaux. Il s'agit du projet de règlement grand-ducal modifiant le règlement grand-ducal modifié du 18 décembre 1998 fixant les modalités de la détermination de la dépendance, du projet de règlement grand-ducal déterminant le contenu de la documentation de la prise en charge et les indicateurs de qualité et de la prise en charge, et finalement du projet de règlement grand-ducal modifiant le règlement grand-ducal du 21 décembre 2006 fixant les modalités spécifiques de la détermination de la dépendance de l'enfant.

1. Quant au projet de règlement grand-ducal modifiant le règlement grand-ducal modifié du 18 décembre 1998 fixant les modalités de la détermination de la dépendance

La loi modifiée du 2 août 2002 définit en son article 2, lettre n) le responsable du traitement 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 personne. »* Pour des raisons de clarté et de précision, la CNPD propose aux auteurs de préciser dans le corps du texte de l'article 1ier, point 1ier du projet de règlement grand-ducal sous examen le responsable du traitement concernant l'outil d'évaluation et de détermination des prestations de l'assurance dépendance (ci-après : « l'outil »). Il devrait s'agir a priori du ministre ayant dans ses attributions la sécurité sociale.

Quant à la partie « données générales » de l'outil, la CNPD recommande aux auteurs de circonscrire plus clairement les catégories de données personnelles qui seront collectées et traitées. Dans ce contexte, la Commission nationale regrette que le texte ne donne aucune précision sur l'origine des données, c'est-à-dire de qui / d'où proviennent les données et comment elles ont été obtenues. Le commentaire des articles précise à cet égard que des éléments ressortant de la conversation avec le demandeur, l'aidant et/ou le personnel soignant s'il intervient dans la prise en charge sont introduits dans l'outil. La CNPD se demande ainsi si toutes les données personnelles sont fournies par le demandeur lui-même, par l'aidant et/ou le personnel soignant ou si certaines données sont collectées à partir d'autres fichiers étatiques ou encore par d'autres moyens.

Par ailleurs, la CNPD veut tirer l'attention des auteurs du projet de règlement grand-ducal sur l'article 4, paragraphe (1), lettre (d) de la loi modifiée du 2 août 2002, qui impose au responsable de traitement l'obligation de veiller à ce que les données qu'il traite ne sont pas conservées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées sans préjudice du paragraphe (2) de l'article en cause.

Or, la CNPD constate que le projet de règlement grand-ducal sous avis ne contient aucune disposition relative à la durée de conservation des données.

De même, la CNPD recommande aux auteurs du projet de règlement grand-ducal de préciser qui aura accès au sein de l'Administration d'évaluation et de contrôle de l'assurance dépendance aux données contenues dans l'outil. En particulier, il est important que seules les personnes qui en ont besoin dans l'exercice de leur fonction et de leurs tâches professionnelles soient habilitées à y avoir accès.

La Commission nationale tient à souligner dans ce contexte l'importance fondamentale du principe de licéité d'un traitement de données à caractère personnel qui doit être lu à la lumière de l'article 8, paragraphe 2 de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52, paragraphes (1) et (2) de la

7 Annexes

Charte des droits fondamentaux de l'Union européenne. En substance, ces deux articles, ensemble avec la jurisprudence constante de la Cour européenne des droits de l'homme, retiennent qu'un traitement de données effectué par une autorité publique peut constituer une ingérence dans le droit au respect de la vie privée ou limiter l'exercice du droit à la protection des données, à condition que cette ingérence ou limitation :

- soit prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante ;

- soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité ;

- respecte le contenu essentiel du droit à la protection des données ;

- réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui.

L'article 6, paragraphe (3) du règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après : « le RGPD »), qui sera applicable à partir du 25 mai 2018 dans tous les Etats membres de l'Union européenne, prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans ces deux cas de figure, le fondement et les finalités des traitements de données doivent spécifiquement être prévus soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis.

Suivant ledit article, ces bases légales devraient contenir des dispositions spécifiques concernant, entre autres, les types de données traitées, les personnes concernées, les entités auxquelles les données peuvent être communiquées et pour quelles finalités, les durées de conservation des données ou encore les opérations et procédures de traitement.

Au niveau national, la Commission nationale tient à rappeler à cet égard l'exigence de la Cour constitutionnelle selon laquelle « *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. »[153]

Le Conseil d'Etat rappelle lui aussi régulièrement dans ses avis que *« (…) l'accès à des fichiers externes et la communication de données informatiques à des tiers constituent une ingérence dans la vie privée et partant, en vertu de l'article 11, paragraphe 3, de la Constitution, une matière réservée à la loi formelle. Dans ce cas, l'essentiel du cadrage normatif doit figurer dans la loi.*

La loi doit indiquer les bases de données auxquelles une autorité publique peut avoir accès ou dont une autorité publique peut se faire communiquer des données, tout comme les finalités de cet accès ou de cette communication (…). »[154]

La CNPD estime ainsi qu'en l'état actuel, le texte du projet de règlement grand-ducal ne respecte pas les exigences de précision et de prévisibilité auxquelles doit répondre un texte légal et ne peut pas être considéré comme étant conforme à l'article 4 de la loi modifiée du 2 août 2002, ni à l'article 8 de la Convention européenne des droits de l'homme, à l'article 52 de la Charte des droits fondamentaux de l'Union européenne, ainsi qu'à l'article 6, paragraphe (3) du RGPD.

Finalement, la CNPD estime nécessaire de prévoir un système de traçage des accès, ce qui constitue une garantie en matière de protection des données à caractère personnel des personnes concernées dans le cadre des articles 22 et 23 de la loi modifiée du 2 août 2002. Ainsi, à l'instar d'autres lois ou règlements grand-ducaux, il conviendrait de rajouter une disposition qui pourrait avoir la teneur suivante :
« Le système informatique par lequel l'accès à l'outil est opéré doit être aménagé de sorte que les informations relatives à la personne ayant procédé à la consultation, les informations consultées, la date, l'heure et la référence du dossier dans le cadre duquel la consultation a été effectuée, ainsi que le motif précis de la consultation puissent être retracés. Les données de journalisation doivent être conservées pendant un délai de cinq ans à partir de leur enregistrement, délai après lequel elles sont effacées, sauf lorsqu'elles font l'objet d'une procédure de contrôle ».

En tout état de cause, la CNPD suggère que l'accès à l'outil soit sécurisé moyennant une authentification forte (par exemple via le système d'authentification « LuxTrust »).

2. Quant au projet de règlement grand-ducal déterminant le contenu de la documentation de la prise en charge et les indicateurs de qualité et de la prise en charge

Sur base de l'article 4, paragraphe (1), lettre a) de la loi modifiée du 2 août 2002, le responsable du traitement doit s'assurer que les données qu'il traite sont collectées pour des finalités déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités.

Il ressort de l'exposé des motifs du projet de règlement grand-ducal sous avis que la documentation de la prise en charge servira d'un côté à soutenir les prestataires d'aides et de soins à assurer un suivi de qualité et une réalisation de l'accompagnement et des aides et soins en toute sécurité, et de l'autre côté, elle sera utilisée dans le cadre du contrôle de la qualité des prestations fournies à la personne dépendante par l'Administration d'évaluation et de contrôle de l'assurance dépendance selon l'article 384bis du Code de la sécurité sociale. Or, dans l'optique de la CNPD, le projet en cause devrait identifier et énumérer expressément dans le corps du texte les différentes finalités de la documentation de la prise en charge.

En ce qui concerne les données administratives à figurer dans la documentation de la prise en charge, elles n'apparaissent pas comme disproportionnées par rapport aux finalités susmentionnées. Le catalogue des données est clairement

[153] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015.
[154] Voir par exemple : Conseil d'Etat, Avis n°6975/5 du 7 juin 2016 relatif au projet de loi portant modification de la loi du 24 juillet 2014 concernant l'aide financière de l'Etat pour études supérieures.

circonscrit. Néanmoins, la Commission nationale se demande qu'elle est l'origine de ces données, c'est-à-dire de qui / d'où elles proviennent et comment elles ont été obtenues.

De même, la CNPD comprend que les données administratives énumérées à l'article 2 du projet de règlement grand-ducal sous avis sont accessibles aux prestataires d'aides et de soins qui fournissent des soins à la personne dépendante en cause, tandis que les données administratives contenues dans la partie des « données générales » de l'outil prévu à l'article 1ier, alinéa 1ier du projet de règlement grand-ducal modifiant le règlement grand-ducal modifié du 18 décembre 1998 fixant les modalités de la détermination de la dépendance sont accessibles à l'Administration d'évaluation et de contrôle de l'assurance dépendance.

Or, comme le commentaire des articles précise que *« la documentation de la prise en charge soit accessible par des moyens informatiques »*, la Commission nationale se demande comment cette accessibilité informatique à la documentation de la prise en charge de la personne dépendante par les prestataires d'aides et de soins se réalisera concrètement. Qui aura accès à cette documentation? Est-ce que l'Administration d'évaluation et de contrôle de l'assurance dépendance aura un accès direct à cette documentation dans le cadre du contrôle de la qualité de la prise en charge de la personne dépendante tel que prévu par l'article 384bis du Code de la sécurité sociale ?

Finalement, la Commission nationale rappelle que les articles 22 et 23 de la loi modifiée du 2 août 2002 obligent le responsable du traitement de mettre en place des mesures techniques et organisationnelles nécessaires afin d'assurer la protection des données à caractère personnel. Cette obligation est reprise à l'article 32 du RGPD, en application duquel le responsable du traitement doit mettre en œuvre les mesures appropriées afin de garantir un niveau de sécurité adapté au risque.

Elle est par ailleurs d'avis que la protection de la confidentialité et de la sécurité des données à caractère personnel constitue un enjeu majeur en cas de traitement de données sensibles (données de santé) dans la mesure où la divulgation de ces données pourrait causer un préjudice grave aux patients. Ces risques augmentent avec le recours accru aux nouvelles technologies par les prestataires de soins qui utilisent souvent des dispositifs mobiles (tablettes) pour documenter les prestations de soins.

Eu égard au caractère sensible des données traitées et en

tenant compte des risques susmentionnés, la CNPD suggère de préciser dans le texte du projet de règlement grand-ducal que des mesures particulièrement élevées doivent être imposées aux prestataires de soins concernant le contrôle de l'utilisation, de l'accès et de la transmission des données administratives à figurer dans la documentation de la prise en charge. Quant à la mise en place d'un système de traçage des accès, la Commission nationale renvoie à ses commentaires ci-dessus relatifs au projet de règlement grand-ducal modifiant le règlement grand-ducal modifié du 18 décembre 1998 fixant les modalités de la détermination de la dépendance.

3. Quant au projet de règlement grand-ducal modifiant le règlement grand-ducal du 21 décembre 2006 fixant les modalités spécifiques de la détermination de la dépendance de l'enfant

La CNPD renvoie à ses commentaires ci-dessus relatifs au projet de règlement grand-ducal modifiant le règlement grand-ducal modifié du 18 décembre 1998 fixant les modalités de la détermination de la dépendance en ce qui concerne les modalités et conditions d'utilisation de l'outil.

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

Ainsi décidé à Esch-sur-Alzette en date du 23 novembre 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis complémentaire relatif au projet de loi n°7045 sur la Police grand-ducale et portant modification :1. du Code de procédure pénale ; 2. de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat ; 3. de la loi du 10 décembre 2009 relative à l'hospitalisation sans leur consentement de personnes atteintes de troubles mentaux ; 4. de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat ; 5. de la loi du 18 décembre 2015 relative à l'accueil des demandeurs de protection internationale et de protection temporaire, et modifiant la loi modifiée du 10 août 1991 sur la profession d'avocat ; et portant abrogation 1. de la loi du 29 mai 1992 relative au Service de Police Judiciaire et modifiant 1. la loi modifiée du 23 juillet 1952 concernant l'organisation militaire, 2. le Code d'instruction criminelle, 3. la loi du 16 avril 1979 ayant pour objet la discipline dans la force publique ; 2. de la loi modifiée du 31 mai 1999 sur la Police et l'Inspection générale de la Police

Délibération n°971/2017
du 1er décembre 2017

7 Annexes

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

Par courrier du 26 août 2016, Monsieur le Ministre de la Sécurité intérieure a invité la Commission nationale à se prononcer au sujet du projet de loi n°7045 portant réforme de la Police grand-ducale et abrogeant la loi du 31 mai 1999 sur la Police et l'Inspection générale de la Police.

La Commission nationale a rendu un premier avis relatif au projet de loi n°7045[155] en date du 24 mars 2017(délibération n°264/2017).

En date du 20 septembre 2017, le projet de loi a fait l'objet d'amendements gouvernementaux.

La CNPD regrette que son avis du 24 mars 2017 n'ait pas eu de répercussions sur le texte du projet de loi tel qu'amendé.

En particulier, il convient de relever que si le projet de loi n°7045 règle l'accès de la Police grand-ducale aux bases de données des administrations, il ne contient toujours pas de dispositions sur les bases de données opérées par la Police elle-même.

En ce qui concerne les fichiers de journalisation régis par l'article 54 alinéa 4 lettre (b) devenu l'article 44 alinéa 4 numéro 2° du projet de loi n°7045, la CNPD rappelle aussi qu'elle estime que le motif de la consultation devrait selon elle également être indiqué par l'agent au moment de la consultation et conservé et que la durée de conservation des fichiers de journalisation devrait être porté de trois ans à cinq ans.

Pour le surplus la CNPD réitère ses observations et propositions formulées dans son avis du 24 mars 2017 (délibération n°264/2017).

Ainsi décidé à Esch-sur-Alzette en date du 1er décembre 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

[155] ainsi que relatif au projet de loi n°7044 portant réforme de l'Inspection générale de la Police et au projet de règlement de règlement grand-ducal relatif au fonctionnement de l'Inspection générale de la Police.

Avis de la Commission nationale pour la protection des données relatif au :
- *Projet de loi n°7136 relatif aux voyages à forfait et aux prestations de voyage liées et portant modification 1) du Code de la Consommation et 2) de la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales*
- *Projet de règlement grand-ducal précisant les informations standards à communiquer par le professionnel conformément aux articles L.225-3 et L.225-17 paragraphe 2 du Code de la consommation*

Délibération n° 972/2017
du 1er décembre 2017

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'« *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 2 mai 2017, Monsieur le Ministre de l'Économie a invité la Commission nationale à se prononcer sur les deux projets de texte suivants :

- le projet de loi n°7136 relatif aux voyages à forfait et aux prestations de voyage liées et portant modification 1) du Code de la Consommation et 2) de la loi modifiée du 2 septembre 2011 réglementant l'accès aux professions d'artisan, de commerçant, d'industriel ainsi qu'à certaines professions libérales (ci-après « le projet de loi »), d'une part ;

- un projet de règlement grand-ducal précisant les informations standards à communiquer par le professionnel conformément aux articles L.225-3 et L.225-17 paragraphe 2 du Code de la consommation (ci-après « le projet de règlement grand-ducal »), d'autre part.

Aux termes de son exposé des motifs, le projet de loi a pour objectif principal de transposer en droit national la directive 2015/2302 relative aux voyages à forfait et aux prestations de voyage liées, modifiant le règlement (CE) No 2006/2004 et la directive 2011/83/UE du Parlement européen et du Conseil et abrogeant la directive 90/314/CEE du Conseil.

La Commission nationale entend limiter ses observations aux dispositions du projet de loi ayant une répercussion sur le respect de la vie privée et la protection des données à caractère personnel des personnes physiques.

I) S'agissant des données à caractère personnel traitées

De façon générale, la Commission nationale observe que les auteurs du projet de loi ont choisi de copier fidèlement les articles de la directive dans le Code de la consommation luxembourgeois en suivant le principe « toute la directive et rien que la directive ».

Conformément à l'article 26, paragraphe 2, et à l'article 49 du traité sur le fonctionnement de l'Union européenne, le marché intérieur doit comporter un espace sans frontières intérieures dans lequel la libre circulation des marchandises et des services ainsi que la liberté d'établissement sont assurées. A ce titre, l'enjeu de la directive 2015/2302 consiste à contribuer au bon fonctionnement de ce marché intérieur à l'égard des consommateurs et à atteindre un niveau élevé de protection des consommateurs dans le secteur des voyages à forfait[156]. Plus particulièrement, la directive renforce la protection du voyageur en établissant de nouvelles obligations précontractuelles d'information pour les professionnels (organisateurs ou détaillants)[157].

[156] La directive 2015/2302 introduit une nouvelle définition du consommateur « voyageur », élargit les définitions du « *voyage à forfait* » (voyages réservés en ligne comprenant diverses parties telles que le transport de personnes, l'hébergement en hôtel ou encore une location de voiture) et du « *contrat de voyage à forfait* » et introduit la notion de « *prestation de voyage liée* » (qui concerne la combinaison de plusieurs services de voyages vendus séparément).

[157] Aux termes du projet de loi, l'organisateur est celui qui produit le voyage (tour opérateur) et le détaillant est le professionnel qui vend ledit voyage (l'agence de voyage par exemple).

Parmi ces obligations, il y a lieu de citer l'obligation pour les professionnels de communiquer au voyageur des informations liées au voyage par l'intermédiaire d'un formulaire standard dont le contenu est défini par le règlement grand-ducal sous-examen[158]. Afin que le voyageur puisse être en mesure de choisir en connaissance de cause parmi les différentes modalités de voyage proposées, la directive et le projet de loi obligent les professionnels à mentionner d'une manière claire, compréhensible et apparente si ce qu'ils proposent est considéré comme un forfait ou comme une prestation de voyage liée.

Dans ce contexte, les données des organisateurs (nom, adresse, coordonnées téléphoniques ou électroniques) ainsi que celles des entités chargées de la protection contre l'insolvabilité (garants financiers) doivent être mises à disposition des voyageurs. L'organisateur doit également fournir les données relatives au garant financier au Ministère de l'Economie. Ainsi, la CNPD observe que les nouvelles obligations créées par la directive 2015/2302 pourraient conduire à des traitements et à des transmissions de données à caractère personnel concernant les catégories de personnes susmentionnées dès lors qu'il s'agit de personnes physiques identifiées ou identifiables, étant entendu que les données relatives aux personnes morales ne sont pas protégées par la loi modifiée du 2 août 2002.

En ce qui concerne la transmission des données d'un professionnel à un autre dans le cadre des prestations de voyage liées[159], le texte du projet de loi fait référence, comme la directive, au « *nom du voyageur* », à ses « *modalités de paiement* » et à son « *adresse électronique* ».

La Commission nationale n'a pas d'observations à formuler s'agissant de ces traitements. Sous réserve qu'il s'agisse de données à caractère personnel concernant des personnes physiques, la collecte et/ou la transmission aux voyageurs et/ou aux professionnels de ces données sont nécessaires et proportionnées par rapport aux finalités déterminées par la directive 2015/2302.

Ceci étant, la Commission nationale recommande aux auteurs du projet de loi d'inclure à la fin du texte une disposition spécifique qui oblige tant les professionnels concernés que les services compétents du Ministère de l'Economie (en tant que « point de contact ») à respecter les principes[160] qui découlent de la loi modifiée du 2 août 2002 et, à partir du 25 mai 2018, du règlement (UE) 2016/679[161]. A noter que la directive 2015/2302, dans son considérant (49), précise que ladite directive ne doit pas porter atteinte aux règles sur la protection

[158] Le projet de règlement grand-ducal sous examen reprend les formulaires d'information figurant en annexe de la directive 2015/2302.
[159] V. p.ex. Art. L.225-2, paragraphe (2), lettre (b), (v) du projet de loi.
[160] Principes relatifs à la légitimation des traitements de données et à la qualité des données, aux droits des personnes concernées, à la confidentialité et la sécurité des traitements, aux transferts de données à caractère personnel vers des pays tiers, etc.
[161] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

des données à caractère personnel énoncées dans la directive 95/46/CE précitée.

Par ailleurs, la Commission nationale tient à souligner qu'en cas de collecte et de traitement de données sensibles (par exemple des données de santé lorsqu'un organisateur sera amené à traiter les données de voyageurs à mobilité réduite ou nécessitant une assistance médicale spécifique, tel qu'il est prévu par l'article L.225-11 paragraphe (8) projeté du Code de la consommation), il est essentiel que les responsables du traitement visés par le projet de loi se conforment aux dispositions de l'article 6 de la loi modifiée du 2 août 2002 et, à partir du 25 mai 2018, aux dispositions de l'article 9 du règlement (UE) 2016/679.

La CNPD souligne également, qu'en cas de transfert de données à caractère personnel vers des pays tiers, il importe que les responsables du traitement visés par le projet de loi se conforment aux dispositions des articles 18 et 19 de la loi modifiée du 2 août 2002 et, à partir du 25 mai 2018, aux dispositions des articles 44 à 49 du règlement (UE) 2016/679.

II) S'agissant des données échangées dans le cadre de la coopération

La Commission nationale note que le voyageur bénéficiera d'une garantie étendue contre l'insolvabilité de professionnels du voyage y compris si ceux-ci ne sont pas établis dans un Etat membre de l'Union européenne. Dans ce contexte, la directive prévoit un système de reconnaissance mutuelle des garanties financières et de coopération entre les Etats membres. Les États membres sont ainsi tenus de désigner des points de contact pour faciliter la coopération administrative et la surveillance des organisateurs qui y exercent leur activité. Ces points de contact mettent à la disposition les uns aux autres toutes les informations nécessaires sur les exigences contre l'insolvabilité au niveau national et sur l'identité de l'entité ou des entités chargées des organisateurs établis sur leur territoire. En outre, ces points de contact s'accordent mutuellement l'accès à tout registre disponible des organisateurs qui se conforment à leurs obligations de protection contre l'insolvabilité.

Dans le cadre de cette coopération, les seules données qui seront susceptibles d'être traitées seront l'identité des personnes physiques (et morales) établies au Luxembourg offrant des voyages à forfait et des prestations de voyage liées et qui ont contracté une garantie financière ainsi que les coordonnées (numéro de téléphone, adresse, adresse électronique, etc.) des entités chargées de la protection contre l'insolvabilité (garants financiers).

La CNPD observe que cette coopération entre autorités compétentes, qui tend à garantir le respect des lois protégeant les intérêts des consommateurs, est expressément prévue par le règlement européen (CE) n°2006/2004 relatif à la coopération en matière de protection des consommateurs. Elle rappelle que les échanges d'informations intervenant dans le cadre de cette coopération doivent respecter les garanties[162] de sécurité et de confidentialité qui s'imposent à tout traitement de données à caractère personnel, comme le souligne d'ailleurs le considérant (9) du règlement n°2006/2004[163].

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

Ainsi décidé à Esch-sur-Alzette en date du 1er décembre 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

---

[162] Notamment les articles 23 et 23 de la loi modifiée du 2 août 2002 et, à partir du 25 mai 2018, l'article 32 du règlement 2016/679.

[163] *cf.* Considérant (9) du règlement (CE) 2006/2004 selon lequel : « *Pour faire en sorte que les enquêtes ne soient pas compromises ou que la réputation des vendeurs ou des fournisseurs ne soit pas injustement entachée, les informations échangées entre les autorités compétentes devraient bénéficier des garanties de confidentialité et de secret professionnel les plus rigoureuses. La directive 95/46/CE (…) et le règlement (CE) no 45/2001 (…) devraient s'appliquer dans le contexte du présent règlement* ».

7 Annexes

Avis relatif au projet de loi n°7182 portant modification 1) de la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat ; 2) de la loi modifiée du 3 août 1998 instituant des régimes de pension spéciaux pour les fonctionnaires de l'Etat et des communes ainsi que pour les agents de la Société nationale des Chemins de Fer luxembourgeois ; 3) de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat ; 4) de la loi modifiée du 12 mai 2009 portant création d'une Ecole de la 2e Chance ; 5) de la loi modifiée du 22 mai 2009 portant création a) d'un Institut national des langues; b) de la fonction de professeur de langue luxembourgeoise ; 6) de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat ; 7) de la loi modifiée du 25 mars 2015 instituant un régime de pension spécial transitoire pour les fonctionnaires de l'Etat et des communes ainsi que pour les agents de la Société nationale des Chemins de Fer luxembourgeois ; 8) de la loi modifiée du 25 mars 2015 fixant les conditions et modalités de l'accès du fonctionnaire à un groupe de traitement supérieur au sien et de l'employé de l'Etat à un groupe d'indemnité supérieur au sien ; 9) de la loi modifiée du 25 mars 2015 déterminant le régime et les indemnités des employés de l'Etat et portant abrogation de la loi modifiée du 22 juin 1963 portant fixation de la valeur numérique des traitements des fonctionnaires de l'Etat ainsi que des modalités de mise en vigueur de la loi du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat

Délibération n°973/2017
du 7 décembre 2017

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 de 2002 »), la Commission nationale pour la protection des données (ci-après désignée « la Commission nationale » ou « la CNPD ») a notamment pour mission d'*« être demandée en son avis sur tous les projets ou propositions de loi portant création d'un traitement de même que sur toutes les mesures réglementaires ou administratives émises sur base de la présente loi »*.

Le 8 septembre 2017, Monsieur le Ministre de la Fonction publique et de la Réforme administrative a déposé à la Chambre des députés le

projet de loi n°7182 portant modification de la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat et de dispositions diverses (ci-après désigné « le projet de loi »).

Ce projet de loi vise entre autres à insérer un nouveau chapitre 10bis dans la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat, qui porterait sur la « *Protection des données nominatives* »[164]. Les auteurs du projet de loi justifient cette insertion par la nécessité de « *mettre le statut général des fonctionnaires de l'Etat en conformité avec les nouvelles règles relatives à la protection des données prévues par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*[165] *qui entreront en vigueur le 25 mai 2018* »[166].

Au vu de la nature des dispositions prévues par ce nouveau chapitre 10bis, la Commission nationale regrette de ne pas avoir été saisie formellement du projet de loi par Monsieur le Ministre de la Fonction publique et de la Réforme administrative. Dès lors et en application de l'article 32, paragraphe (3), lettre (f) de la loi modifiée du 2 août 2002, la Commission nationale a pris la décision de se saisir elle-même pour aviser le présent projet de loi.

Le nouveau chapitre 10bis que les auteurs du projet de loi proposent d'ajouter à la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat comporterait sept articles traitant de la protection des données à caractère personnel, numérotés 35-1 à 35-7. Dans la première section du présent avis, la Commission nationale entend tout d'abord faire part de ses remarques générales par rapport à cette proposition de nouveau chapitre. Elle va ensuite préciser ses commentaires par rapport à chacun de ces articles dans les sections 2 à 8 ci-dessous.

1. Remarques générales

Tout d'abord, la Commission tient à saluer la proposition des auteurs du projet de loi qui entendent, comme indiqué dans le commentaire des articles précité, « *mettre le statut général des fonctionnaires de l'Etat en conformité avec les nouvelles règles relatives à la protection des données* ».

Dans son récent avis du 21 novembre 2017[167], le Conseil d'Etat estime qu' « *il appartient au législateur de régler dans le cadre* [du projet de loi n°7184 portant création de la Commission nationale pour la protection des données et la mise en œuvre du règlement général sur la protection des données (UE) 2016/679] *la question de la portée du règlement européen précité de manière générale, et plus particulièrement à l'égard de la fonction publique* ». Il recommande dès lors aux auteurs du projet de loi de supprimer l'article 1 point 11° de ce projet, qui vise précisément à insérer ce nouveau chapitre 10bis dans la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat. Le Conseil d'Etat propose en outre de supprimer l'article 1 point 12° du projet de loi sous objet, et donc de maintenir dans ladite loi l'article 35bis actuel qui « *sera, le cas échéant, modifié pour tenir compte des dispositions de la loi à intervenir (doc. parl. n°7184)* ».

La Commission nationale ne partage toutefois pas cette recommandation du Conseil d'Etat.

L'article 6, paragraphe (3) du règlement général sur la protection des données (UE) 2016/679, lu ensemble avec son paragraphe (1) lettres (c) et (e), prévoit une contrainte particulière liée à la licéité d'un traitement de données nécessaire au respect d'une obligation légale ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. Dans ces deux cas de figure, le fondement et

[164] Article 1er, point (11) du projet de loi, pp. 6-8.
[165] Ci-après : « le règlement général sur la protection des données (UE) 2016/679 » ou « le RGPD ».
[166] Commentaire des articles, ad. article 1er, point (1), p. 22.
[167] Document parlementaire 7182/02, pp. 4-5.

les finalités des traitements de données doivent spécifiquement être prévus soit par le droit de l'Union européenne, soit par le droit de l'État membre auquel le responsable du traitement est soumis.

Le considérant 45 du RGPD explique à cet égard que « *lorsque le traitement est effectué conformément à une obligation légale à laquelle le responsable du traitement est soumis ou lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, le traitement devrait avoir un fondement dans le droit de l'Union ou dans le droit d'un État membre* ».

L'article 6, paragraphe (3) du règlement général sur la protection des données (UE) 2016/679 précise encore que la « *base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du règlement, entre autres : les conditions générales régissant la licéité du traitement par le responsable du traitement ; les types de données qui font l'objet du traitement ; les personnes concernées ; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être; la limitation des finalités ; les durées de conservation ; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX* ».

La Commission nationale tient à souligner dans ce contexte l'importance fondamentale du principe de licéité d'un traitement de données à caractère personnel qui doit être lu à la lumière de l'article 8, paragraphe 2 de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52, paragraphes (1) et (2) de la Charte des droits fondamentaux de l'Union européenne.
En substance, ces deux articles, ensemble avec la jurisprudence constante de la Cour européenne des droits de l'homme, retiennent qu'un traitement de données effectué par une autorité publique peut constituer une ingérence dans le droit au respect de la vie privée ou limiter l'exercice du droit à la protection des données. Cette ingérence ou limitation peut être justifiée à condition qu'elle :

- soit prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante ;

- soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité ;

- respecte le contenu essentiel du droit à la protection des données ;

- réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui.

En ce qui concerne la première condition, selon la jurisprudence de la Cour européenne des droits de l'Homme, une ingérence au droit au respect de la vie privée n'est *« prévue par la loi »*, au sens de l'article 8 paragraphe (2) de la Convention, que si elle repose sur un article du droit national qui présente certaines caractéristiques. La loi doit être *« accessible aux personnes concernées et prévisible quant à ses répercussions »*[168]. Une règle est prévisible *« si elle est formulée avec une précision suffisante pour per¬mettre à toute personne – bénéficiant éventuellement d'une assistance appropriée – d'adapter son comportement »*[169]. *« Le degré de précision requis de la "loi" à cet égard dépendra du sujet en question. »*[170]

Or, la création de traitements de données à caractère personnel par les ministres des ressorts respectifs portant sur la gestion de leur personnel constitue indéniablement un traitement visé à l'article 6 paragraphes (1) lettres (c) ou (e) du RGPD.

Il s'ensuit qu'un tel traitement doit être prévu au Grand-Duché de Luxembourg dans une base légale contenant des dispositions spécifiques. Le nouveau chapitre 10bis vise à créer les conditions nécessaires pour la création et la mise en œuvre de tels traitements. C'est donc à raison que les auteurs du projet de loi ont inséré un tel chapitre dans la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat.

Certes, l'article 35bis actuel de ladite loi prévoit déjà que *« les ministres des ressorts respectifs traitent au sein des administrations et services qui relèvent de leur compétence, pour ce qui est des candidats aux postes qui en dépendent, du personnel y nommé ou affecté et des bénéficiaires d'une pension de la part de l'Etat, les données à caractère personnel nécessaires à l'exécution des processus centraux et locaux de gestion du personnel (…) »*.

Cependant, la Commission nationale est d'avis que la disposition actuelle ne correspond pas au degré de précision requis par l'article 8, paragraphe (2) de la Convention européenne des droits de l'Homme tel qu'interprété par la Cour européenne des droits de l'Homme dans sa jurisprudence, ainsi que par l'article 6 paragraphe (3) du règlement général sur la protection des données (UE) 2016/679.

Au contraire, le projet de chapitre 10*bis* apparaît davantage conforme à ces exigences, dans la mesure où il énumère les finalités des traitements envisagés, les personnes concernées ainsi que les opérations et procédures de traitement envisagées (article 35-1), les conditions générales régissant la licéité du traitement par le responsable du traitement (article 35-2), les durées de conservation des données (article 35-3), et les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être (article 35-4). Il précise en outre les mesures de sécurité envisagées (article 35-5), l'information et les droits des personnes concernées (article 35-6), ainsi que les transferts de données (article 35-7).

Cependant, il ne liste pas les catégories de données qui seront traitées[171].

En conséquence, la Commission nationale recommande vivement de maintenir le nouveau chapitre 10bis dans la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat.

Le libellé de ce chapitre devrait toutefois être modifié et prendre la forme de : *« Protection des données à caractère personnel »*, afin de s'aligner sur la terminologie de l'article 4 numéro (1) du règlement général sur la protection des données (UE) 2016/679, par ailleurs utilisée dans les différents articles du chapitre 10*bis*.

---

[168] CouEDH, Amann c. Suisse [GC], n°27798/95, 16 février 2000, para. 50 ; voir également CouEDH, Kopp c. Suisse, n°23224/94, 25 mars 1998, para. 55 et CouEDH, Iordachi et autres c. Moldavie, n°25198/02, 10 février 2009, para. 50.

[169] CouEDH, Amann c. Suisse [GC], n°27798/95, 16 février 2000, para. 56 ; voir également CouEDH, Malone c. Royaume-Uni, n°8691/79, 26 avril 1985, para. 66 ; CouEDH, Silver et autres c. Royaume-Uni, n°5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.

[170] CouEDH, The Sunday Times c. Royaume-Uni, n°6538/74, 26 avril 1979, para. 49 ; voir également CouEHD, Silver et autres c. Royaume-Uni, n°5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.

[171] Voir remarques ci-dessous, section 3. « la pertinence des données (article 35-2) ».

2. La finalité des traitements
(article 35-1)

La Commission nationale tient à saluer la décision des auteurs du projet de loi de prévoir un article relatif aux finalités des traitements. A la lecture de ce dernier, la CNPD constate qu'il définit également les responsables de traitement (« *les ministres des ressorts respectifs ainsi que les administrations* »), les catégories de personnes concernées (« *[les] candidats aux postes qui en dépendent, [le] personnel y nommé ou affecté et [les] bénéficiaires d'une pension de la part de l'Etat* »), ainsi que les opérations de traitement envisagés (« *ces processus concernent : (…)* »).

La Commission nationale suggère, pour des raisons de clarté et afin de s'aligner sur la terminologie utilisée aux articles 4 numéro (1) et 5, paragraphe (1), lettre (b) du règlement général sur la protection des données (UE) 2016/679, de remplacer les termes « *Ces processus concernent :* » par « *Ces traitements de données à caractère personnel répondent aux finalités suivantes :* ».

Cependant, le dernier alinéa de cet article 35-1 (« *Les ministres des ressorts respectifs ainsi que les administrations qui relèvent de leur compétence déterminent seuls ou conjointement avec d'autres, les finalités et les moyens du traitement* ») n'apparaît pas correct aux yeux de la CNPD. En effet, dans le cas de traitements effectués par l'administration, c'est au législateur de définir les finalités qui peuvent être poursuivies par le responsable du traitement, ainsi que les moyens pour y parvenir. Il n'appartient pas aux ministres des ressorts respectifs de déterminer d'autres finalités que celles fixées par le législateur. Bien évidemment, dans l'hypothèse où les ministres des ressorts respectifs estiment qu'il est nécessaire d'élargir des finalités d'un traitement de données, la législation devra être adaptée. La CNPD propose dès lors de supprimer le dernier alinéa de l'article 35-1.

3. La pertinence des données
(article 35-2)

Les trois premiers paragraphes de l'article 35-2 énumèrent des principes qui ressortent du règlement général sur la protection des données (UE) 2016/679 respectivement de la loi modifiée du 2 août 2002 : les principes de licéité et de loyauté, le principe de minimisation des données, ainsi que le principe d'exactitude des données. Ces principes étant en tout état de cause applicables sur base du RGPD respectivement de la loi de 2002, il apparaît superflu de les répéter dans l'article 35-2. La Commission nationale propose donc de supprimer les trois premiers paragraphes de cet article.

En ce qui concerne le quatrième paragraphe de l'article 35-2, la CNPD souhaite relever qu'il ne répond pas à ses yeux aux exigences de précision et de prévisibilité auxquelles doit répondre un texte légal. En effet, comme l'explique le considérant 41 du règlement général sur la protection des données (UE) 2016/679, une base juridique ou une mesure législative qui sert de base à un traitement licite de données *« devrait être claire et précise et son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne (ci-après dénommée « Cour de justice ») et de la Cour européenne des droits de l'homme »*[172].

De plus, comme déjà indiqué plus haut[173], les catégories de données qui font l'objet du traitement ne sont pas précisés dans le chapitre 10*bis* ni dans une autre disposition légale ou réglementaire. Or, il relève du rôle du législateur d'appliquer le principe de nécessité et de proportionnalité (également appelé principe de minimisation des données) aux différents traitements qui sont créés par la loi, en fixant et en précisant quelles catégories de données peuvent être traitées par l'administration. Dès lors, la Commission nationale estime nécessaire d'indiquer dans ce chapitre 35-2 les catégories de données qui pourront être traitées par les ministres des ressorts respectifs ainsi que les administrations qui relèvent de leur compétence[174]. Cet article pourra le cas échéant être complété d'un règlement grand-ducal qui prévoirait avec plus de précisions les données à caractère personnel concernées.

4. La conservation limitée des données (article 35-3)

La Commission nationale tient à saluer l'initiative des auteurs du projet de loi de lister la durée de conservation pour chaque catégorie de données.

A défaut d'explication des durées de conservation envisagées sous les points (1) à (7) dans le commentaire des articles, la Commission nationale n'est par contre pas en mesure d'apprécier la pertinence de ces différents délais. Toutefois, elle se demande si les durées indiquées aux points (3), (4) et (7), qui ne constituent pas des délais fixes, ne devraient pas être précisées, ou à défaut davantage explicitées dans le commentaire des articles.

5. Accès restreint aux données (article 35-4)

L'article 35-4 vise à restreindre les accès aux données à caractère personnel aux seules *« personnes habilitées à y accéder en raison de leurs fonctions »*. La Commission nationale estime en effet qu'une telle mesure technique et organisationnelle de restriction des accès (qui pourra le cas échéant être définie dans un règlement grand-ducal pris en exécution du paragraphe (2) de cet article) s'avère nécessaire pour garantir la confidentialité des données.

La CNPD estime nécessaire de prévoir un système de journalisation des accès aux données. Ainsi, à l'instar d'autres textes légaux, la CNPD propose le rajout d'un nouveau paragraphe 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 fichiers de données à caractère personnel qui sont gérés par les ministres des ressorts respectifs ainsi que leurs administrations, 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*

[172] Voir notes de bas de page 6, 7 et 8.
[173] Cf. section 1. « remarques générales ».
[174] Ces catégories de données pourraient par exemple reprendre les libellés de l'article 35-3, points (1) à (7) de loi du 16 avril 1979 fixant le statut général des fonctionnaires de l'Etat, telle que modifiée.

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

En ce qui concerne en particulier le consentement écrit préalable de la personne concernée, la CNPD tient à souligner qu'un tel consentement devra répondre aux exigences de l'article 4 point (11) du règlement général sur la protection des données (UE) 2016/679. En d'autres termes, le consentement doit être « *libre, spécifique, éclairé et univoque* », c'est-à-dire que la personne concernée doit avoir un véritable choix. Le consentement ne doit dès lors pas être conditionné et la personne concernée ne doit pas subir de conséquences négatives lorsqu'elle ne donne pas son consentement.

6. La sécurité (article 35-5)

La Commission nationale se demande si les trois mesures visées au paragraphe (2) de cet article sont exhaustives, ou si elles sont citées à titre illustratif. Par ailleurs, les ministres des ressorts respectifs ainsi que les administrations doivent en tout état de cause mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, conformément aux articles 22 et 23 de la loi modifiée du 2 août 2002, respectivement à l'article 32 du GDPR.

Alors que les mesures listées constituent des exemples de mesures de sécurité qui peuvent être considérées comme appropriées afin de garantir un niveau de sécurité adapté au risque, au titre de l'article 32 du règlement général sur la protection des données (UE) 2016/679, la Commission nationale se pose la question de la pertinence de lister de telles mesures précises dans un texte de loi, de sorte que cet article ne paraît pas nécessaire.

7. L'information et les droits des personnes (article 35-6)

7.1. L'information des personnes concernées (article 35-6 paragraphe (1))

L'article 35-6 paragraphe (1) indique les informations qui seront communiquées aux personnes concernées. La Commission nationale relève qu'en application des articles 13 et 14 du RGPD, les personnes concernées devront en tout état de cause être informées des finalités des traitements, des destinataires des données et des droits des personnes concernées, mais aussi

de l'identité et des coordonnées du responsable du traitement (c'est-à-dire du Ministère ou de l'administration concernée), des coordonnées du délégué à la protection des données[175], de la base juridique du traitement (en l'espèce, des dispositions du chapitre 10*bis* que le projet de loi sous examen vise à insérer), et dans l'hypothèse où les données à caractère personnel n'auraient pas été collectées auprès de la personne concernée, des catégories de données à caractère personnel concernées.

En ce qui concerne les destinataires des données, la Commission nationale tient en outre à se référer à la jurisprudence de la Cour de justice de l'Union européenne, selon laquelle « *l'exigence de traitement loyal des données personnelles prévue à l'article 6 de la directive 95/46 oblige une administration publique à informer les personnes concernées de la transmission de ces données à une autre administration publique en vue de leur traitement par cette dernière en sa qualité de destinataire desdites données* »[176].

Ce paragraphe, qui énumère certaines informations qui devraient en tout état de cause être fournies aux agents des ministères et administrations concernées, s'avère dès lors superflu. Si les auteurs du projet de loi décident tout de même de maintenir ce paragraphe, la CNPD suggère cependant de remplacer les termes « *des destinataires de ces traitements* » par « *des destinataires de ces données* », afin de se référer à la terminologie adéquate.

7.2. Les droits des personnes concernées (article 35-6 paragraphe (2))

L'article 35-6 paragraphe (2) énumère les droits des personnes concernées. Ainsi, les auteurs du projet de loi se réfèrent au droit d'accès de la personne concernée, du droit de rectification et du droit à l'effacement, tels que prévus par l'article 28 de la loi modifiée du 2 août 2002.

La CNPD relève qu'outre ces droits, le règlement général sur la protection des données 2016/679 (UE) prévoit encore le droit à la limitation du traitement (article 18 du RGPD) et le droit d'opposition (article 21 du RGPD) ainsi que le cas échéant, le droit à la portabilité des données (article 20 du RGPD)[177] et le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé[178] (article 22 du RGPD).

Ce paragraphe, qui répertorie certains des droits des personnes concernées déjà visés par la loi de 2002 respectivement par le RGPD, apparaît donc également superflu aux yeux de la CNPD.

8. Les transferts de données (article 35-7)

Les auteurs du projet de loi ont souhaité indiquer que « les ministres des ressorts respectifs ainsi que les administrations qui relèvent de leur compétence ne procèdent pas à des transferts de données hors de l'Union européenne ».

La Commission nationale n'est pas en mesure d'apprécier si des transferts ponctuels de données à caractère personnel (par exemple dans le cadre d'accords ou de conventions internationales) pourraient toute de même avoir lieu vers des pays tiers ne disposant pas d'un niveau de protection adéquat en matière de protection des données.

Afin d'éviter la situation dans laquelle une administration se verrait dans l'impossibilité de transférer ponctuellement et légitimement des données à caractère personnel vers des pays tiers, la CNPD suggère de supprimer cet article. Bien entendu, les éventuels transferts de données devront alors respecter les dispositions des articles 18 et 19 de la loi de 2002 respectivement des articles 44 à 49 du règlement général sur la protection des données 2016/679 (UE).

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

[175] Qui doit être désigné en tout état de cause lorsque le traitement est effectué par une autorité publique ou un organisme public (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle), conformément à l'article 37 paragraphe (1) lettre (a) du règlement général sur la protection des données (UE) 2016/679.
[176] Cour de Justice de l'Union européenne, affaire Smaranda Bara e.a. c. ANAF, n°C 201/14, 1er octobre 2015, para. 34.
[177] Par exemple dans l'hypothèse où un agent public change d'administration et souhaite recevoir communication des données traitées par l'administration qui l'employait, pour les transmettre à l'administration pour laquelle il est amené à travailler.
[178] Si un tel traitement automatisé était prévu par un Ministère ou une administration à l'égard de ses agents.

7 Annexes

Ainsi décidé à Esch-sur-Alzette
en date du 7 décembre 2017.

La Commission nationale pour
la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis relatif au projet de loi n°7168 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification de certaines lois

Délibération n°1049/2017
du 28 décembre 2017

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

Par lettre du 9 août 2017, Monsieur le Ministre de la Justice a invité la Commission nationale à se prononcer au sujet du projet de loi n°7168 - projet de loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification de certaines lois.

Le projet de loi sous avis est censé transposer la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

La Commission nationale pour la protection des données (CNPD ou Commission nationale) formule les observations ci-après.

Ad article 5

L'article 5 du projet de loi est censé transposer l'article 5 de la directive 2016/680 relatif à la durée de conservation.

L'article 5 de la directive 2016/680 dispose que *« les États membres prévoient que des délais appropriés sont fixés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel »*.

L'article 5 paragraphe (1) du projet de loi prévoit que c'est le responsable du traitement qui *« fixe des délais appropriés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel »*.

La CNPD est cependant d'avis qu'il n'appartient pas au responsable du traitement (c'est-à-dire la Police Grand-ducale, le Service de renseignement de l'Etat, l'Administration des douanes et accises etc.) de fixer les délais de conservation des données, mais qu'il revient au législateur de les fixer.

Des lois spéciales devront fixer, de manière précise, la durée de conservation pour chaque traitement de données tout comme elles devront prévoir l'existence même des différents traitements de données.

Dans ce contexte, la Commission nationale tient à souligner l'importance fondamentale du principe de licéité des traitements de données à caractère personnel qui doit être lu à la lumière de l'article 8, paragraphe 2 de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que de l'article 52, paragraphes (1) et (2) de la Charte des droits fondamentaux de l'Union européenne. En substance, ces deux articles, ensemble avec la jurisprudence constante de la Cour européenne des droits de l'homme, retiennent qu'un traitement de données effectué par une autorité publique peut constituer une ingérence dans le droit au respect de la vie privée ou limiter l'exercice du droit à la protection des données. Cette ingérence ou limitation peut être justifiée à condition qu'elle :

- soit prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante ;

- soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité ;

- respecte le contenu essentiel du droit à la protection des données ;

- réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui.

En ce qui concerne la première condition, selon la jurisprudence de la Cour européenne des droits de l'Homme, une ingérence au droit au respect de la vie privée n'est *« prévue par la loi »*, au sens de l'article 8 paragraphe (2) de la Convention, que si elle repose sur une disposition du droit national qui présente certaines caractéristiques.
La loi doit être *« accessible aux personnes concernées et prévisible quant à ses*

répercussions »[179]. Une règle est prévisible « *si elle est formulée avec une précision suffisante pour permettre à toute personne – bénéficiant éventuellement d'une assistance appropriée – d'adapter son comportement* »[180]. « *Le degré de précision requis de la "loi" à cet égard dépendra du sujet en question.* »[181]

Au niveau national, la Commission nationale tient à rappeler à cet égard l'exigence de la Cour constitutionnelle selon laquelle « *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.* »[182]

En effet, il ne fait aucun doute que les traitements de données effectués par les autorités compétentes en matière pénale ainsi qu'en matière de sécurité nationale constituent une ingérence dans le droit au respect de la vie privée et le droit à la protection des données, de sorte que les conditions et les modalités de ces traitements doivent obligatoirement être prévues dans la loi.

Ces exigences relatives au principe de légalité découlent par ailleurs des dispositions de l'article 4 paragraphe 2 de la directive 2016/680.

Concrètement, des textes légaux spécifiques doivent autoriser les autorités compétentes à procéder à des traitements de données personnelles, alors que le traitement en lui-même devra respecter les dispositions du projet de loi sous avis.

A titre d'exemple, la loi résultant du projet de loi n°7151 relative au traitement des données des dossiers passagers dans le cadre de la prévention et de la répression du terrorisme et de la criminalité grave pourrait constituer une telle base légale pour un traitement de données, alors que le traitement opéré par l'Unité d'informations passagers créé au sein de la Police Grand-Ducale devra en lui-même respecter les dispositions du projet de loi de transposition sous avis.

En revanche, dans d'autres domaines, des textes législatifs assez détaillés font défaut.

On peut mentionner ainsi les traitements de données effectuées par la Police Grand-Ducale en matière policière à des fins de prévention et de détection des infractions pénales. Ceux-ci sont régis par le règlement grand-ducal modifié du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police générale (« règlement Ingepol ») ne répond pas à toutes les exigences juridiques de protection des données

[179] CouEDH, Amann c. Suisse [GC], n°27798/95, 16 février 2000, para. 50 ; voir également CouEDH, Kopp c. Suisse, n°23224/94, 25 mars 1998, para. 55 et CouEDH, Iordachi et autres c. Moldavie, n°25198/02, 10 février 2009, para. 50.
[180] CouEDH, Amann c. Suisse [GC], n°27798/95, 16 février 2000, para. 56 ; voir également CouEDH, Malone c. Royaume-Uni, n°8691/79, 26 avril 1985, para. 66 ; CouEDH, Silver et autres c. Royaume-Uni, n°5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.
[181] CouEDH, The Sunday Times c. Royaume-Uni, n°6538/74, 26 avril 1979, para. 49 ; voir également CouEHD, Silver et autres c. Royaume-Uni, n°5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 mars 1983, para. 88.
[182] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015.

découlant de la directive 2016/680 et du projet de loi sous avis. Ce règlement grand-ducal datant d'il y a plus de 25 ans a d'ailleurs été pris en exécution de la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, loi qui fût abrogée en 2002.

De même, les traitements de données effectués par l'Administration des douanes et accises en matière douanière ne sont pas basés sur des textes légaux répondant aux principes de la protection des données et aux exigences de la jurisprudence de la Cour de Strasbourg.

Eu égard aux développements qui précèdent, la Commission nationale estime que l'article 5 de la directive 2016/680 n'est pas correctement transposé en droit national par le projet de loi sous examen.

Ad article 9

Le paragraphe (2) de l'article 9 prévoit que *« lorsque des autorités compétentes sont chargées d'exécuter des missions autres que celles énoncées à l'article 1er, le règlement (UE) n°2016/679 s'applique au traitement des données effectué à de telles fins, y compris à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. »*

Eu égard aux termes[183] de l'article 9 paragraphe (2) de la directive 2016/680 et au principe de légalité énoncé ci-dessus à article 5, la CNPD suggère d'insérer les mots *« par une loi luxembourgeoise »* derrière le mot *« chargés »*.

Le paragraphe (3) précise ce qui suit : *« Lorsqu'une autorité compétente qui transmet des données soumet leur traitement à des conditions spécifiques, elle en informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter. »* Or, ce paragraphe déforme le sens du paragraphe (3) de l'article 9 de la directive 2016/680 qu'il est censé transposer, puisque celui-ci régit l'hypothèse dans laquelle *« le droit de l'Union ou le droit d'un État membre […] soumet le traitement à des conditions spécifiques »*.[184] Il y a par conséquent également lieu de préciser que le traitement ne peut être soumis qu'à des conditions spécifiques prévues par la loi luxembourgeoise.

Ad article 13

L'article 13 régit le droit à l'information de la personne concernée. Le paragraphe (1) énumère les informations qui doivent être systématiquement fournies à la personne concernée.

L'article 13 paragraphe (2) de la directive 2016/680, transposé par l'article 13 paragraphe (2) du projet de loi, prévoit les informations additionnelles que le responsable du traitement doit fournir *« dans certains cas particuliers »*. Cependant, le projet de loi reprend simplement la formulation de *« certains cas particuliers »* de la directive sans déterminer ces cas particuliers. A propos du texte de transposition français, similaire sur cette question au projet de loi sous avis, la Commission nationale de l'informatique et des libertés (CNIL) française estime que *« cette absence de lisibilité peut être un frein à l'exercice des droits tout en étant source d'insécurité juridique pour les responsables des traitements concernés »*[185].

On pourrait par exemple prévoir que lesdites informations additionnelles doivent être fournies à la personne concernée chaque fois que le responsable collecte les données directement auprès de la personne concernée[186]. Dans ce cas, les informations pourraient être fournies, le cas échéant, au moment de la collecte des données.

La CNPD ne partage par ailleurs pas l'interprétation du paragraphe (2) de l'article 13 que fournit le commentaire des articles selon laquelle le paragraphe s'applique notamment au cas où la personne concernée demande ces informations. En effet, ce dernier cas de figure est régi - en

[183] *« Lorsque les autorités compétentes sont chargées par le droit d'un État membre d'exécuter des missions autres […] »*
[184] *« Les États membres prévoient que, lorsque le droit de l'Union ou le droit d'un État membre applicable à l'autorité compétente qui transmet les données soumet le traitement à des conditions spécifiques, l'autorité compétente qui transmet les données informe le destinataire de ces données à caractère personnel de ces conditions et de l'obligation de les respecter. »*
[185] Délibération n°2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978 https://www.cnil.fr/sites/default/files/atoms/files/projet_davis_cnil.pdf
[186] Cf. en ce sens l'avis du 29 novembre 2017 du groupe de travail institué en vertu de l'article 29 de la directive 95/46/CE

majeure partie - par l'article 14 relatif au droit d'accès.

Le paragraphe (3) de l'article 13 paragraphe permet de limiter le droit à l'information.

Or, le texte ne précise rien quant aux cas dans lesquels ces limitations peuvent jouer et se borne à copier les termes de l'article 13 paragraphe (3) de la directive 2016/680 qui permet ces limitations alors que le paragraphe (4) du même article 13 de la directive prévoit justement la possibilité pour le législateur national d' « *adopter des mesures législatives afin de déterminer des catégories de traitements susceptibles de relever, dans leur intégralité ou en partie, d'un quelconque des points énumérés au paragraphe 3* ».

Selon le groupe de travail institué en vertu de l'article 29 de la directive 95/46/CE[187], le législateur devra préciser dans quels cas et sous quelles conditions le responsable du traitement peut retenir les informations en question. Selon le groupe de travail, la directive n'autorise pas de restriction générale.

Ad article 15

L'article 15 du projet de loi prévoit la possibilité de limitations du droit d'accès, droit qui est régi par l'article 14.

Tout comme elle l'a soulevé à propos du droit à l'information prévu par l'article 13, la CNPD considère que le texte ne précise pas suffisamment ces limitations alors que l'article 15 paragraphe (2) de la directive prévoit justement la possibilité pour le législateur national d' « *adopter des mesures législatives afin de déterminer des catégories de traitements de données susceptibles de relever, dans leur intégralité ou en partie, des points a) à e) du paragraphe 1* » de l'article 15 de la directive.

Ad article 16

L'article 16 du projet de loi prévoit le droit de rectification ou d'effacement des données. Le paragraphe (3) permet des limitations à ce droit.

Ici encore, la CNPD constate que la loi ne comporte pas de précisions relatives au cas de figure dans lesquelles il peut être fait usage de ces limitations.

Ad article 17

L'article 17 prévoit qu'en cas d'exercice des droits par l'intermédiaire de l'autorité de contrôle - suite à une limitation des droits à l'information, d'accès et de rectification ou d'effacement des données telle que prévue par les articles 13 paragraphe (3), 15 paragraphe (1) et 16 paragraphe (4) -, l'autorité de contrôle informe la personne concernée le cas échéant uniquement « *du fait*

[187] Avis adopté le 29 novembre 2017.

qu'elle a procédé à toutes les vérifications nécessaires ou à un examen ». Selon le commentaire des articles, « *ce paragraphe permet donc d'arriver au même résultat que la disposition analogue actuellement en vigueur, à savoir l'article 17, paragraphe 2, alinéa 5, de la loi modifiée du 2 août 2002 relative à la protection des données à l'égard du traitement des données à caractère personnel* ».

Concrètement, cela signifie que, le cas échéant, la personne concernée ne peut pas se voir confirmer - par l'autorité de contrôle - qu'une violation de ses droits a effectivement eu lieu si tel est le cas.

La CNPD tient cependant à remarquer que le mécanisme d'accès indirect représentera désormais l'exception - confiné aux hypothèses prévues par les articles 13 paragraphe (3), 15 paragraphe (1) et 16 paragraphe (4), alors sous le régime de l'article 17 de la loi modifiée du 2 août 2002, il constitue la règle en matière de traitements de données dans le domaine de la police et de la sécurité nationale. En effet, l'article 14 de la directive 2016/680 et du projet de loi posent le principe du droit d'accès direct.

Ad article 18

L'article 18 prévoit que lorsque « *les données à caractère personnel sont relatives à des faits qui font l'objet d'une enquête préliminaire, d'une instruction préparatoire ou qui ont été renvoyées devant une juridiction de jugement, les droits visés aux articles 13, 14 et 16 sont exercés conformément aux dispositions du Code de procédure pénale ou à d'autres dispositions légales applicables* ».

La CNPD doute que dans tous les cas de figure (où les données sont relatives à des faits qui font l'objet d'une enquête préliminaire, d'une instruction préparatoire ou qui ont été renvoyées devant une juridiction de jugement), les droits à l'information, d'accès et de rectification ou d'effacement des données sont garantis de manière spécifique par le Code de procédure pénale ou d'autres dispositions légales applicables. Il se pose la question de savoir si, pour ces cas, on retombe dans le « droit commun » des articles 13, 14 et 16 de la loi projetée alors que le projet de loi ne précise rien à ce sujet.

Ad article 25

L'article 25 prévoit la mise en place de fichiers de journalisation qui permettent de vérifier - a posteriori - le respect de certaines règles relatives à la protection des données.

La CNPD note que l'article ne prévoit aucune durée de conservation pour les fichiers de journalisation. Dès lors, il sera indispensable que pour chaque traitement de données concerné, la loi respective créant le traitement ou servant de base légale au traitement fixera la durée de conservation applicable.

Ad article 38

L'article 38 paragraphe (1) lettres d) et e) permet des transferts de données vers un pays tiers ou à une organisation internationale dans des cas particuliers. La CNPD constate le manque de précision dans le projet de loi au regard de ces cas particuliers. Afin d'éviter l'arbitraire, il appartient au législateur de définir les cas particuliers en question.

Ad article 39

L'article 39 paragraphe (1) permet également des transferts de données « dans certains cas particuliers » sans cependant définir ou énumérer ces cas particuliers, ce qui laisse une marge de manœuvre très large aux responsables du traitement au détriment des personnes concernées. Ici, il appartient au législateur de définir les cas particuliers en question pour éviter l'arbitraire.

Egalement au paragraphe (1), les termes « de la présente directive » devraient être remplacés par les mots « de la présente loi ».

7 Annexes

Ad article 41

L'article 41 instaure l'autorité de contrôle judiciaire exclusivement compétente pour surveiller les opérations de traitement effectués par les juridictions de l'ordre judiciaire, y compris le ministère public et de l'ordre administratif, dans l'exercice de leurs fonctions juridictionnelles.

La Commission nationale salue que parmi les membres de cette autorité de contrôle judiciaire figure également un représentant de la CNPD. En effet, ceci contribuera à une application et interprétation cohérente et harmonisée de la matière et permettra ainsi d'éviter des positions différentes entre les deux autorités de contrôle.

Ad article 43

Au paragraphe (1), lettre i), les termes « de la présente directive » devraient être remplacés par les mots « de la présente loi ».

Ad article 48

L'article 48 prévoit le droit pour une personne concernée de mandater un organisme qui œuvre à la protection des droits et intérêts des personnes concernées dans le domaine de la protection des données à caractère personnel pour que celui-ci introduise une réclamation en son nom auprès d'une autorité de contrôle et pour qu'il exerce le droit à un recours juridictionnel.

Le paragraphe (2) lettre d) de l'article 48 prévoit que l'organisme en question doit disposer de la personnalité active au moment de l'introduction de la réclamation ou de l'action en justice au nom de la personne concernée.

La CNPD suggère de remplacer l'expression de la « personnalité active » par celle de la « personnalité juridique active ».

Ad article 49

1) En matière de sanctions, l'article 49 paragraphe (1) du projet de loi sous avis renvoie à l'article 49 du projet de loi n°7184 (projet de loi portant création de la Commission nationale pour la protection des données et la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel).

Cet article régit les amendes administratives.

L'article 49 du projet de loi 7184 met en œuvre l'article 83 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. L'article 83 précité prévoit à son tour entre autres le niveau des amendes administratives. Il prévoit des sanctions d'un niveau maximal différent en fonction de la disposition respective du règlement (UE) 2016/679 qui a fait l'objet d'une violation. Les montants respectifs des amendes sont fixés par les paragraphes (4), (5) et (6) de l'article 83 du règlement 2016/679.

Imaginons par exemple qu'une disposition de la loi projetée sous avis est violée par un responsable du traitement. Comment peut-on savoir lequel parmi les paragraphes (4), (5) et (6) de l'article 83 du règlement 2016/679 il faut appliquer pour prononcer la sanction ?

Etant donné que l'article 49 du projet de loi n°7184 se rapporte, en matière d'amendes administratives, de manière spécifique à des violations de dispositions du règlement (UE) 2016/679 et non à des violations de la loi projetée sous avis le présent projet de loi ne peut y référer, du moins pour ce qui est du montant maximal des amendes, sans avoir déterminé de manière spécifique le plafond des amendes administratives dans le cadre du présent projet de loi pour la violation de dispositions de ce même projet de loi. Une omission risque de créer une insécurité ou un vide juridique alors que les intéressés ne sauraient pas à l'avance quelles sanctions seraient applicables à quelle violation, voire que les sanctions ne pourraient pas être déterminées.

2) L'article 49 paragraphe (1) prévoit en sa deuxième phrase que les *« amendes administratives et astreintes prononcées sont à charge de l'Etat, sauf lorsqu'il résulte de la décision y afférente prise par la Commission nationale pour la protection des données que le fait justifiant la sanction ou l'astreinte a été commis intentionnellement »*.

Le commentaire des articles fournit l'explication suivante : *« Cette différenciation se justifie par le fait que tous les traitements de données à caractère personnel effectués en application de la loi en projet sont faits par des fonctionnaires ou employés de l'Etat dans l'exercice de leurs missions et qu'il serait excessif de mettre toutes les amendes et astreintes prononcées à charge du patrimoine personnel du fonctionnaire ou de l'agent concerné. Toutefois, il convient d'exclure de cette disposition les violations commises intentionnellement, pour lesquelles les amendes et astreintes restent alors à charge du patrimoine personnel du fonctionnaire ou de l'agent sanctionné. »*

Ce passage de l'article 49 soulève plusieurs questions.

Est-ce que la CNPD devra rechercher un élément intentionnel à l'image de ce qui se fait en matière pénale ? Et devra-t-elle en faire état dans ses décisions prononçant une amende ou une astreinte ?

Par ailleurs, les conséquences d'une violation de la loi commise intentionnellement ne sont pas claires. Est-ce que l'amende ou l'astreinte est prononcée par la CNPD contre l'institution responsable du traitement (voire contre l'Etat tout court, le texte ne le précisant pas), l'Etat pouvant ensuite se retourner contre l'agent, eu égard au contenu de la décision. Ou bien la CNPD devra-t-elle

prononcer la sanction contre le fonctionnaire en question ?

Des clarifications à ces sujets sont nécessaires.

3) L'article 49 paragraphe (2) prévoit que la violation des articles 10, 11 ou 30 du projet de loi sous avis peut être sanctionnée pénalement – outre les sanctions pénales de l'article 53 du projet de loi n°7184.

La CNPD propose de créer une nouvelle infraction destinée à sanctionner certains abus, qui, dans le passé ont été sanctionnées pénalement notamment sur base des dispositions pénales des articles 4 et 5 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

A ce sujet, elle renvoie à ses développements exposés au point 11 b (sanctions pénales) de son avis relatif au projet de loi n°7184 (délibération n°1050/2017 du 28 décembre 2017).

Par ailleurs, ladite infraction devrait être rajoutée aux infractions pouvant donner lieu à une coopération entre le Parquet d'un côté et la CNPD ou l'autorité de contrôle judiciaire de l'autre (article 49 paragraphe (4) alinéa premier).

4) Les paragraphes (3) à (5) de l'article 49 du projet de loi sous avis prévoient une coopération entre la CNPD et le procureur d'Etat.

Les paragraphes (4) et (5) de l'article 49 prévoient notamment des informations et des transmissions de dossiers entre la CNPD et le procureur d'Etat en cas de violation des dispositions du paragraphe (7) du même article 49 (qui prévoit le délit d'entrave en ce qui concerne l'autorité de contrôle judiciaire), des articles 10, 11 ou 30 du projet de loi sous avis ainsi que de l'article 49 du projet de loi n°7184.

En revanche n'est pas mentionné le délit d'entrave prévu à l'article 53 du projet de loi n°7184. La CNPD suggère dès lors de rajouter ledit article 53 à la liste des articles pouvant donner lieu à une coopération.

5) L'article 49 paragraphe (4) alinéa 3 du projet de loi prévoit que lorsqu' « ***au cours de la procédure*** *la Commission nationale pour la protection des données constate l'existence d'indices que les personnes suspectées sont susceptibles d'avoir contrevenu aux dispositions du paragraphe 7, d'un ou de plusieurs articles visés au paragraphe 2 ou de l'article 49 de la loi du jj/mm/*

aaaa portant création de la Commission nationale pour la protection des données et du régime général sur la protection des données, elle se dessaisit du dossier et le transmet au procureur d'Etat qui procède conformément au Code de procédure pénale. »

On peut se demander quelle « procédure » est précisément visée.

S'agit-il de la procédure administrative mentionné à l'alinéa 2 in fine de l'article 49 paragraphe (4) ? Or, dans ce cas de figure, par hypothèse, le procureur d'Etat a déjà informé la CNPD du fait qu'il n'allait pas poursuivre et on ne voit pas de raison pour laquelle la CNPD se dessaisirait du dossier.

Ou bien s'agit-il d'une procédure qui n'a pas encore fait l'objet d'une information au procureur d'Etat de la part de la CNPD ? Or, ce cas de figure est a priori régi par l'alinéa premier de l'article 49 paragraphe (4).

Ou bien s'agit-il de la procédure pénale dans le cas où l'affaire a déjà fait l'objet d'une information de la CNPD au procureur d'Etat qui a décidé de poursuivre mais où la CNPD reçoit encore des informations supplémentaires après la décision du procureur de poursuivre ?

La Commission nationale souhaiterait obtenir des clarifications à cet égard.

6) Le paragraphe (6) de l'article 49 prévoit une coopération entre l'autorité de contrôle judiciaire et le procureur d'Etat selon les mêmes modalités que celles de la coopération entre la CNPD et le procureur d'Etat « *lorsqu'elle [l'autorité de contrôle judiciaire] exerce les missions et dispose des pouvoirs prévus par le règlement (UE) n°2016/679* ».

La CNPD constate que le projet de loi n°7184 (censée mettre en œuvre le règlement (UE) n°2016/679) ne crée pas d'infractions pénales mise à part le délit d'entrave prévu à l'article 53. Celui-ci se rapporte cependant de manière spécifique à l'égard la CNPD, le délit d'entrave à l'accomplissement des missions de l'autorité de contrôle judiciaire étant prévu à l'article 49 paragraphe (7) du projet de loi sous avis.

Faut-il déduire de la mention du règlement (UE) n°2016/679 que la coopération entre l'autorité de contrôle judiciaire et le procureur d'Etat ne concerne pas la violation des articles 10,11 et 30 de la loi projetée sous avis, sanctionnée par l'article 49 paragraphe (2) du projet de loi ? En effet, ces articles ne relèvent pas du règlement (UE) n°2016/679, mais de la directive (UE) 2016/680.

Et en ce qui concerne le délit d'entrave prévu au paragraphe (7), il semble s'appliquer à l'action de l'autorité de contrôle judiciaire aussi bien dans le champ d'application du règlement (UE) n°2016/679 que dans celui de la directive (UE) 2016/680 et de la loi projetée sous avis. Mais vu la mention du règlement (UE) n°2016/679 par l'article 49 paragraphe (6), il se pose la question de savoir si la coopération joue seulement si l'autorité de contrôle judiciaire a agi dans le champ d'application du règlement (UE) n°2016/679, et non si elle a agi dans le champ d'application de la directive (UE) 2016/680 et de la loi projetée sous avis?

Ad article 57

L'article 57 modifie la deuxième phrase du point 2 de l'article 8 de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire qui, dans la version projetée, prévoit que le Service de renseignement de l'Etat (SRE) transmet sur une base trimestrielle la liste de ses demandes de délivrance

du bulletin N°2 du casier judiciaire et les motifs des demandes à l'autorité de contrôle judiciaire.

S'agissant sûrement d'une confusion entre les deux autorités de contrôle, la CNPD estime que ladite transmission devrait se faire à la CNPD et non à l'autorité de contrôle judiciaire puisque les traitements de données effectués par le service de renseignement relèvent de la CNPD.

D'ailleurs, à l'heure actuelle, le service de renseignement doit transmettre ladite liste de ses demandes de délivrance et les motifs de celles-ci à l'autorité de contrôle spécifique prévue à l'article 17 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, autorité de contrôle dont les compétences seront reprises par la CNPD dorénavant.

Enfin, l'article 60 du projet de loi modifiant l'article 10, paragraphe 2, l'alinéa 3 de loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat prévoit par ailleurs également l'obligation à charge du SRE de transmettre les listes des demandes de délivrance, sauf qu'en vertu dudit article 10, la transmission doit se faire à la CNPD et non à l'autorité de contrôle judiciaire.

Ad article 60

Il est renvoyé aux commentaires relatifs à l'article 57.

Ad article 63

L'article 63 paragraphes (2) de la directive 2016/680 permet aux Etats-membres de retarder la mise en place des fichiers de journalisation prévus par l'article 25 de la directive *« à titre exceptionnel et lorsque cela exige des efforts disproportionnés »*.

La CNPD estime que cet article manque de précision car il ne détermine pas ce qu'il faut entendre par « efforts disproportionnés ».

La CNPD tient encore à souligner que si des dérogations temporaires sont possibles concernant les fichiers de journalisation prescrits par l'article 25 du projet de loi sous avis, aucune telle possibilité n'existe pour les obligations comparables édictées par l'article 29 paragraphe (2) lettres f) et g) du projet de loi. Les mesures résultant de l'article 29 paragraphe (2) lettres f) et g) doivent donc être mises en application pour le 6 mai 2018 au plus tard.

Ainsi décidé à Esch-sur-Alzette
en date du 28 décembre 2017.

La Commission nationale pour
la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Avis relatif au projet de loi n°7184 portant création de la Commission nationale pour la protection des données et la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

Délibération n°1050/2017
du 28 décembre 2017

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

Faisant suite à la demande lui adressée par Monsieur le Ministre des Communications et des Médias en date du 22 août 2017, la CNPD entend présenter ci-après ses réflexions et commentaires au sujet du projet de loi n°7184 relative à la création de la Commission nationale pour la protection des données et la mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, portant modification de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et abrogeant la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après : « le projet de loi »).

La protection des données à caractère personnel constitue une des dimensions du droit au respect de la vie privée ; elle est désormais consacrée comme un droit fondamental à part entière dans la Charte des droits fondamentaux de l'Union européenne (article 8). Depuis l'avènement de l'ère du numérique, elle revêt une dimension particulière.

7 Annexes

La Commission nationale rejoint les auteurs du présent projet de loi, en ce que le cadre législatif actuel relatif à la protection des données qui date de 1995 est dépassé par l'évolution rapide des technologies et la mondialisation qui ont créé de nouveaux enjeux pour la protection des données à caractère personnel, vu l'ampleur de la collecte et du partage de données à caractère personnel qui a augmenté de manière importante.

Il est vrai que ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union européenne, assorti d'une application rigoureuse des règles via des sanctions dissuasives en cas de violation constatée. S'il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur européen, il est également indispensable de renforcer la protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement de leurs données personnelles. En 2012, la Commission européenne a initié une réforme du cadre existant, visant à adapter les règles aux nouveaux défis réglementaires, et ceci en assurant une neutralité technologique dans un souci de pérennité et en tenant compte de l'évolution technologique et sociétale des deux dernières décennies.

Une réforme de la protection des données sous Présidence luxembourgeoise du Conseil de l'Union européenne, a conduit à l'adoption du règlement (UE) 2016/679 (ci-après : « le RGPD »), tenant à harmoniser les règles nationales existantes et à moderniser la directive 1995/46/CE, a pour but de renforcer la protection des données à caractère personnel dans une société de plus en plus digitale en redonnant aux citoyens le contrôle des données qui les concernent, que celles-ci soient collectées et utilisées par les acteurs économiques privés ou par les acteurs du service public.

En outre, le RGPD uniformise et simplifie les règles auxquelles les organismes traitant des données personnelles sont soumis en renforçant les garanties d'ores et déjà offertes par la directive 95/46 (CE). Il prévoit en particulier la réduction des formalités préalables pour la mise en œuvre des traitements comportant moins de risques, avec le passage d'un système de contrôle a priori par la CNPD, par le biais de notifications et d'autorisations, à un contrôle a posteriori plus adapté aux réalités du terrain.

En contrepartie, la CNPD voit ses pouvoirs de contrôle et de sanctions renforcés avec la possibilité d'infliger des amendes pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre

d'affaires mondial de l'organisme concerné.

Un tel changement de paradigme nécessite une évolution des missions et pouvoirs de l'ensemble des autorités de protection des données de l'Union européenne dont la CNPD.

Dans ce nouvel environnement juridique, la CNPD devra notamment guider encore plus les acteurs, notamment les petites et moyennes entreprises qui doivent s'adapter aux nouvelles obligations en matière de protection des données.

Les autorités de contrôle européennes devront également coopérer rapidement dans le cadre du « guichet unique » instauré par le RGPD, un mécanisme de coopération renforcé entre les autorités de protection des données qui devront dorénavant adopter des décisions communes lorsque les traitements de données seront transnationaux, ainsi que pour parvenir à une position commune unique pour toute l'Union européenne au sein du nouveau Comité européen pour la protection des données. Les décisions prises par cet organe constitueront le gage d'une plus grande sécurité juridique pour les responsables de traitement et d'une application uniforme de la législation européenne en matière de protection des données.

Deux autres instruments européens s'ajoutent au RGPD pour constituer le « paquet sur la protection des données », réformant en profondeur le droit de la protection des données au niveau de l'Union européenne. Ainsi, le Parlement européen et le Conseil ont adopté parallèlement en date du 27 avril 2016:

- la directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après : « la directive 2016/680 ») faisant l'objet de l'avis 1049 de la CNPD du 28 décembre 2017 et

- la directive 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (ci-après : « la directive PNR ») faisant l'objet de l'avis 958 de la CNPD du 23 novembre 2017.

Comme il s'agit en la matière d'un règlement européen qui est d'application directe, c'est le règlement (UE) 2016/679 qui déterminera la majorité des dispositions de fond désormais applicables en matière de protection des données.

Selon les auteurs du projet de loi sous examen, ce dernier, qui doit se lire conjointement avec le règlement (UE) 2016/679, se limite à compléter ce cadre européen par les dispositions nationales qui s'imposent, à savoir :

- la mise en place / l'adaptation de la loi organique de la Commission nationale pour la protection des données (actuellement contenue dans la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel qui devra être abrogée), afin d'octroyer à la CNPD les nouveaux pouvoirs qui lui seront nécessaires pour que celle-ci puisse exercer les missions qui lui sont dévolues par le nouveau règlement (UE) 2016/679 (chapitre 1) ;

- les dispositions spécifiques dans des domaines où le règlement (UE) 2016/679 prévoit qu'une législation nationale complémentaire peut être adoptée (chapitre 2).

Les auteurs du projet de loi ont fait le choix d'abroger

la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. La Commission nationale acquiesce ce choix qui permet une meilleure articulation entre les dispositions prises en exécution du RGPD et celles visant à transposer la directive 2016/680. D'autant plus que les auteurs du projet de loi visant à transposer la directive 2016/680 vont au-delà du champ d'application de la directive pour y intégrer les traitements de données personnelles effectuées en matière de sécurité nationale et de désigner la future CNPD comme successeur de l'autorité de contrôle de l'article 17 de la loi de 2002, actuellement compétente en la matière.

Elle constate que de manière générale, le projet de loi sous avis remplit globalement l'objectif principal qui lui est assigné, à savoir adapter le droit luxembourgeois au nouveau cadre européen pour en assurer la pleine effectivité pour les citoyens et les responsables de traitement et sous-traitants.

Il donne ainsi corps au RGDP, qui constitue une avancée considérable pour la protection des données à caractère personnel dans l'Union européenne.

Sous réserve des clarifications demandées, omissions relevées ou compléments proposés ci-après dans le cadre de l'examen section par section, le projet de loi dote en effet le régulateur des pouvoirs nécessaires à l'exercice de ses missions.

A_ Quant à la mise en place d'une nouvelle loi organique pour la CNPD

Le règlement (UE) 2016/679, tenant à harmoniser les règles nationales existantes et à moderniser la directive 1995/46/CE, déterminera la majorité des dispositions de fond désormais applicables en matière de protection des données.

Il se caractérise par la mise en place d'une approche dite de « l'accountability » c'est-à-dire une responsabilisation des acteurs qui traitent des données personnelles, via un autocontrôle des entreprises.

Il s'ensuit que la nouvelle CNPD passera d'un système de contrôle a priori (donc le système des notifications et autorisations tel que prévu actuellement par la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel) vers un contrôle a posteriori.

Ce changement de paradigme permettra à la nouvelle CNPD de se concentrer davantage sur sa mission de sensibilisation et de guidance des responsables de traitement de données. Pour

que le système soit dissuasif, la nouvelle Commission nationale devra disposer d'une compétence plus large et de moyens de contrôle et de sanction nettement plus conséquents et dissuasifs en cas de violation constatée que ce dont l'actuelle CNPD dispose.

Le présent avis est donné à l'égard du projet de loi 7184, mais pour ce qui concerne la mise en place d'une nouvelle Commission nationale pour la protection des données, ce dernier est indissociable du projet de loi 7168. Il s'ensuit que non seulement le présent avis devra être lu ensemble avec l'avis de la Commission nationale sur le projet de loi 7168 (délibération n°1049/2017 du 28 décembre 2017), mais le présent avis y référera aussi.

1. Statut juridique et indépendance

Malgré son nom, le projet de loi n'entend pas créer une nouvelle autorité de surveillance générale mais plutôt revoir les fondements de l'autorité existante et élargir ses compétences, tout comme ses missions et pouvoirs.

La nécessité de prévoir une telle autorité de contrôle réside dans l'article 16, paragraphe 2 du Traité sur le fonctionnement de l'Union européenne, qui est précisément la base légale du RGPD et de la Directive 2016/680, ainsi que dans l'article 8, paragraphe 3, de la Charte des droits fondamentaux de l'Union européenne, qui prévoient tous les deux que le respect des règles y prévues est soumis au contrôle d'autorités indépendantes.

Tout comme la CNPD actuelle, la nouvelle commission prendra la forme d'un établissement public, seule forme juridique qui permette d'atteindre le but de garantir un niveau d'indépendance certain à la CNPD.

La CNPD dispose ainsi de la personnalité juridique et jouit de l'autonomie financière et administrative nécessaire à garantir son indépendance face à l'exécutif, auquel elle n'est attachée que pour des questions liées aux spécificités de fonctionnement de l'Etat luxembourgeois et aucunement sous une tutelle au sens littéral du terme qui ne lui permettrait pas de prendre librement ses décisions. Autrement comprise, la disposition se heurterait à l'article 52 du RGPD qui dispose que dans l'exercice de leurs missions et de leurs pouvoirs, le ou les membres de chaque autorité de contrôle demeurent libre de toute influence extérieure, qu'elle soit directe ou indirecte et ne sollicitent et n'acceptent d'instructions de quiconque. L'article 4 du projet de loi reprend d'ailleurs à juste titre cette disposition.

Il importe également que la CNPD dispose d'un budget annuel qui lui permette de remplir ses missions tout comme le prévoit le RGPD dans le paragraphe 4 de l'article 52 : « Chaque Etat membre veille à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsque celle-ci doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au Comité. » Il est de la volonté du législateur européen que le budget des autorités de contrôle soit pris en charge par l'Etat directement et non que l'autorité de contrôle couvre l'entièreté de ses frais de fonctionnement par des redevances qu'elle serait autorisée à percevoir.

La Commission nationale salue l'introduction d'un nouveau pouvoir par rapport à la loi de 2002, à savoir la possibilité d'adopter des règlements CNPD dans la limite de sa spécialité. Cette disposition permettra à la nouvelle Commission nationale de réagir rapidement aux développements sur le terrain pour mieux guider les acteurs et si nécessaire de spécifier certaines règles dans un objectif d'augmenter la sécurité juridique.

2. Compétences de la CNPD

A l'heure actuelle, la loi du 2 août 2002 sur la protection des

personnes à l'égard du traitement des données à caractère personnel institue en son article 32 (1) une autorité de contrôle dénommée « Commission nationale pour la protection des données » chargée de contrôler et de vérifier si les données soumises à un traitement sont traitées en conformité avec les dispositions de cette loi et ses règlements d'exécution. Cette autorité de contrôle a une compétence générale de supervision en matière de protection des données. On peut considérer qu'elle est l'autorité de contrôle de droit commun pour ce qu'on peut appeler le « régime général » de la protection des données à caractère personnel, en ce sens qu'elle est compétente pour toute la matière, sauf disposition légale contraire.

La loi de 2002 prévoit une autorité de contrôle spécifique composée du Procureur Général d'Etat, ou de son délégué et de deux membres de la Commission nationale, communément appelée « Autorité de contrôle Article 17 » d'après l'article qui l'institut. Cette autorité de contrôle spécifique est exclusivement compétente pour surveiller les traitements de données visés à l'article 17 de ladite loi (p.ex. traitements effectués par la Police grand-ducale, le Service de renseignement de l'Etat, l'Administration des Douanes et Accises etc.).

Une nouveauté majeure apportée par le projet de loi est l'élargissement des compétences de la CNPD à des traitements des données à caractère personnel en matière pénale et de sécurité nationale. La nouvelle Commission nationale aura donc également compétence pour des matières revenant actuellement de l'autorité de contrôle de l'article 17, qui disparaîtra toutefois avec l'abrogation de la loi de 2002 prévue par le projet de loi sous avis. La nouvelle Commission nationale sera dès lors la seule autorité de contrôle pour les traitements de données personnelles généraux tant sous le RGPD que le projet de loi de la Directive 2016/680 et le garant pour une application correcte de ces deux instruments ainsi que de tous les textes normatifs se rapportant à la protection des données, ce qui permettra d'assurer une mise en œuvre et une interprétation cohérente des règles en matière de protection des données.

Tant le RGPD que la Directive prévoient que les données à caractère personnel traitées par les juridictions dans l'exercice de leur fonctions juridictionnelles sont exclues de la surveillance des autorités de contrôle.

L'article 55 paragraphe 3 du RGPD laisse présumer que lesdits traitements pourraient être exempts de contrôle. Ce n'est toutefois pas la voie choisie par le législateur luxembourgeois qui préconise

la création d'une nouvelle autorité de contrôle séparée, aux termes de l'article 41 du projet de loi N°7168. Cette autorité de contrôle judiciaire sera compétente pour la supervision des traitements effectuées par les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif dans l'exercice de leurs fonctions juridictionnelles, que ce soit pour les finalités prévues par l'article 1 dudit projet de loi 7168 ou pour celles visées par le RGPD. Ces traitements sont donc exclus de la compétence de la nouvelle Commission nationale.

L'article 8 du projet de la loi prévoit que c'est la Commission nationale qui représente le Luxembourg au « Comité européen de la protection des données » institué par l'article 68 de RGPD et contribue à ses activités. C'est une disposition très claire, permettant d'éviter la confusion quant à la question de savoir quelle autorité de contrôle siègera au Comité européen, alors que ce dernier est non seulement compétent pour l'application du RGPD, mais dispose également de certains pouvoirs dans le cadre de la Directive 2016/680.

3. Missions de la CNPD

La nouvelle Commission nationale voit ses missions élargies par rapport à celles actuellement prévues. Elle se verra attribuer de nouvelles missions en vertu de la loi de transposition de la directive 2016/680.

a) Dans le cadre du règlement 2016/679

C'est l'article 57 du RGPD qui énumère les missions de droit commun de la Commission nationale. Elles ne sont pas reprises expressément dans le projet de loi sous avis, l'article 9 se limitant à se référer au prédit article 57 du RGPD.

b) Dans le cadre du projet de loi de transposition de la Directive 2016/680

La liste de missions de la nouvelle Commission nationale reprise dans l'article 10 du projet de loi concerne exclusivement les traitements visés par la Directive 2016/680 qui nécessite une transposition dans le droit national.

Il s'agit d'une copie conforme aux missions prévues aux articles 46 et 48 de la directive 2016/680, ce qui n'appelle pas de remarques particulières en soi. L'article 43 du projet de loi 7168 prévoit exactement la même liste de missions pour l'autorité de contrôle judiciaire.

Les deux autorités de contrôle devront non seulement veiller à ne pas empiéter sur le champ de compétence de l'une et de l'autre, mais également se concerter dans un souci d'harmonisation dans l'application et l'interprétation des textes législatifs nationaux, européens et internationaux en matière de protection des données. Les auteurs du projet de loi 7168 ont toutefois déjà devancé le risque de disparité de jurisprudence en prévoyant qu'un membre de la CNPD fasse partie de l'autorité de contrôle judiciaire.

4. Les pouvoirs de la CNPD

« Afin de veiller à faire appliquer le RGPD et à contrôler son application de manière cohérente dans l'ensemble de l'Union, les autorités de contrôle devraient avoir dans chaque Etat membre les mêmes pouvoirs effectifs… » prévoit le considérant (129) du RGPD. L'article 58 paragraphes 1, 2 et 3 du RGPD qui énumère ces pouvoirs obligatoires pour chaque État membre. Ces derniers ne peuvent que rajouter des pouvoirs additionnels, ce que les auteurs du projet de loi sous avis ne font pas, mais pas en retirer.

Par contre, chaque État membre doit en vertu de l'article 58 paragraphe 5 du RGPD prévoir, par la loi, que son *« autorité de contrôle a le pouvoir de porter toute violation du RGPD à l'attention des autorités judiciaires et, le cas échéant, d'ester en justice d'une manière ou d'une autre, en vue de faire appliquer les dispositions du présent règlement. »* C'est un article qui impose une action

aux États membres en laissant à leur appréciation les moyens déployés pour atteindre le résultat escompté.

Alors que l'article 15 du projet de loi sous avis se borne à indiquer le principe que la CNPD a le droit d'ester en justice, les auteurs du projet de loi restent muets sur la procédure judiciaire à suivre.

Le projet de loi ne précise rien non plus sur l'obligation de prévoir dans le droit national le pouvoir de la nouvelle CNPD de porter toute violation du RGPD à l'attention des autorités judiciaires.

Comme le spectre des infractions pénales a presque été réduit à néant dans les deux projets de lois, la CNPD ne pourra porter une violation du RGPD à l'attention des autorités judiciaires, par le biais d'une dénonciation au parquet, que dans cinq cas, dans la mesure où le projet de loi sous avis prévoit une seule infraction pénale et le projet de loi N°7186 en prévoit quatre : La possibilité de saisir les autorités judiciaires de violations du RGPD par ce biais est donc presque inexistante. La question de savoir s'il ne serait pas judicieux de prévoir des sanctions pénales pour des violations intentionnelles du RGPD sera traitée dans la section relative aux sanctions.

Il n'en reste pas moins qu'en vertu de l'article 58 paragraphe 5 du RGPD, la CNPD doit avoir la possibilité de porter toute violation du RGPD à l'attention des autorités judiciaires et notamment aussi des violations commises par les institutions européennes.

Etant donné que la Commission nationale dispose de la personnalité juridique, il va de soi qu'elle peut ester en justice pour défendre ces décisions dans le cadre de l'article 54 du projet de loi sous avis. Or, quelle procédure judiciaire peut-elle emprunter pour faire appliquer les dispositions du présent règlement, notamment pour faire analyser la validité de certaines décisions prises par les institutions européennes sur base du RGPD par la Cour de justice de l'Union européenne ?

Dans ce contexte, il convient par ailleurs de rappeler et de souligner l'importance de l'obligation faite aux Etats membres dans l'arrêt « Schrems » du 6 octobre 2015 rendu par la CJUE (affaire C-362/14).

Les juges retiennent au point 65 de l'arrêt que « Dans l'hypothèse contraire, où ladite autorité estime fondés les griefs avancés par la personne l'ayant saisie d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de ses données à caractère personnel, cette même autorité doit, conformément à l'article 28, paragraphe 3, premier alinéa, troisième tiret,

de la directive 95/46, lu à la lumière notamment de l'article 8, paragraphe 3, de la Charte, pouvoir ester en justice. À cet égard, ***il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision*** *».*

La décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis reprend à son compte la décision de la CJUE dans son point 144 :

« La Cour de justice a par ailleurs considéré que, conformément à l'article 25, paragraphe 6, second alinéa, de la directive 95/46/CE, les États membres et leurs organes doivent prendre les mesures nécessaires pour se conformer aux actes des institutions de l'Union, car ces derniers jouissent, en principe, d'une présomption de légalité et produisent, dès lors, des effets juridiques aussi longtemps qu'ils n'ont pas été retirés, annulés dans le cadre d'un recours en annulation ou déclarés invalides à la suite d'un renvoi préjudiciel ou d'une exception d'illégalité. En conséquence, une décision d'adéquation de la Commission adoptée conformément à l'article 25, paragraphe 6, de la directive 95/46/CE a un caractère contraignant pour tous les organes des États membres destinataires, y compris leurs autorités de surveillance indépendantes. Lorsqu'une telle autorité a été saisie d'une plainte concernant la compatibilité d'une décision d'adéquation de la Commission avec la protection des droits fondamentaux que constituent le respect de la vie privée et la protection des données et qu'elle estime que les griefs avancés sont fondés, le droit national doit prévoir des voies de recours lui permettant de faire valoir ces griefs devant les juridictions nationales, qui, en cas de doute, doivent surseoir à statuer et procéder à un renvoi préjudiciel devant la Cour de justice. »

Le droit national actuel n'est donc pas conforme à la jurisprudence de la CJUE, alors qu'il ne prévoit actuellement pas de voie de recours ou de procédure judiciaire permettant à la CNPD de saisir directement une juridiction nationale dans le cas de figure visé ci-avant. Ce n'est qu'à l'occasion d'un recours devant les juridictions administratives, intenté par une personne concernée ou un responsable de traitement, contre une décision administrative prise par la CNPD, qu'un renvoi préjudiciel devant la CJUE peut être demandé. Or, ceci n'est pas suffisant au regard de l'arrêt précité, alors que les juges européens exigent clairement la possibilité d'une saisine directe des juridictions nationales par l'autorité de contrôle, c'est-à-dire la CNPD.

Le projet de loi sous avis ne comble pas cette lacune et ne lève pas cette non-conformité, de sorte que la CNPD doit insister à ce que le projet de loi soit complété et précisé sur ce point.

Ainsi, il y a lieu de prévoir une disposition dans le projet de loi qui permette à la nouvelle Commission nationale de demander au Tribunal administratif d'ordonner la suspension ou la cessation du transfert de données, dans le cas où, saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, elle estime fondés les griefs avancés, dans l'attente de l'appréciation par la Cour de Justice de la validité d'une décision d'adéquation de la commission européenne prise sur le fondement du RGPD ou des articles de la Directive ou de tout acte pris par la Commission européenne autorisant ou approuvant les garanties appropriés prises sur le fondement du RGPD ou des articles de la Directive.

Annexes

Cette saisine devra également être possible tant dans le cadre d'une réclamation dirigée contre un responsable de traitement ou d'un sous-traitant, qu'en dehors d'une telle réclamation, afin que la nouvelle CNPD puisse également agir lorsqu'elle estime que la décision européenne permettant le transfert n'est pas valide.

La teneur d'une disposition pour la nouvelle loi luxembourgeoise sur la protection des données personnelles pourrait être la suivante :

Demande de contrôle juridictionnel par l'autorité de contrôle en cas de présomption d'illégalité d'une décision de la Commission Européenne

(1) Dans le cas où, saisie d'une réclamation dirigée contre un responsable de traitement ou un sous-traitant, la Commission nationale pour la protection des données estime fondés les griefs avancés relatifs à la protection des droits d'une personne à l'égard du traitement de ses données à caractère personnel, ou de manière générale afin d'assurer la protection de ces droits dans le cadre de sa mission, peut demander au Tribunal administratif d'ordonner la suspension ou la cessation d'un transfert de données en cause, le cas échéant, sous astreinte, et assortit alors ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de la décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE) 2016/679 ainsi que de tous les actes pris par la Commission européenne autorisant ou approuvant les garanties appropriées dans le cadre des transferts de données pris sur le fondement de l'article 46 de même règlement.

(2) Lorsque le transfert de données en cause ne constitue pas une opération de traitement effectuée par une juridiction dans l'exercice de sa fonction juridictionnelle ou le Ministère public, la Commission nationale pour la protection des données peut saisir dans les mêmes conditions le Tribunal administratif pour obtenir la suspension du transfert de données fondé sur une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de la directive (UE) 2016/680 dans l'attente de l'appréciation par la Cour de justice de l'Union européenne de la validité de cette décision d'adéquation.

(3) Si la Commission nationale pour la protection des données estime qu'une décision d'adéquation de la Commission européenne,

prise sur le fondement de l'article 45 du règlement (UE) 2016/679 ainsi que de tous les actes pris par la Commission européenne autorisant ou approuvant les garanties appropriées dans le cadre des transferts de données pris sur le fondement de l'article 46 de même règlement ou règles de conduite approuvées sur fondement de l'article 40 de ce même règlement ou une décision d'adéquation de la Commission européenne prise sur le fondement de l'article 36 de la directive (UE) 2016/680, dont la validité est nécessaire pour une décision de l'autorité de contrôle, est invalide, elle suspend la procédure et demande un contrôle juridictionnel devant le Tribunal administratif.

(4) La loi du 21 juin 1999 portant règlement de procédure devant les juridictions administratives s'applique conformément au paragraphe (5).

(5) Dans la procédure visée aux paragraphes (1) à (4), la Commission nationale pour la protection des données agit en qualité de demandeur. Le tribunal administratif peut mettre la Cour de justice en mesure de présenter ses observations endéans un délai qu'il impartit.

(6) Si un recours sur le contrôle de validité d'une décision de la Commission européenne visée aux paragraphes (1) à (4) est pendante devant la Cour de Justice de l'Union européenne, le tribunal administratif peut ordonner la suspension de l'affaire jusqu'à ce que la Cour de Justice de l'Union européenne ait rendue sa décision.

(7) Si, à l'issue d'un recours visé aux paragraphes (1) à (4), le tribunal administratif parvient à la conviction que la décision de la Commission européenne est valide, il le constate dans sa décision. Autrement, il soumet la question sur la validité de la décision conformément à l'article 267 du Traité sur le Fonctionnement de l'Union Européenne à la Cour de Justice de l'Union européenne pour décision.

L'article 16 du projet de loi énumère un nombre de pouvoirs de la CNPD dans le cadre des missions de l'article 10 du projet sous examen. Transposition littérale de l'article y afférent, à savoir de l'article 47 de la directive 2016/680, les pouvoirs de la nouvelle CNPD dans ce contexte diffèrent de ceux prévus à l'article 58 du RGPD, qui prend le soin de prévoir plus en détail les pouvoirs d'enquête de l'autorité de contrôle. Afin d'aligner les pouvoirs d'enquête de la CNPD dans le contexte du contrôle des traitements de données en matière pénale ainsi qu'en matière de sécurité nationale sur ceux exercés dans le cadre du RGPD, la Commission nationale estime notamment que « *le pouvoir d'obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement…* » tel que prévu à l'article 58 paragraphe 1 lettre f) du RGPD devrait aussi être prévu explicitement pour éviter qu'un responsable de traitement ou sous-traitant refuse l'accès à la nouvelle CNPD au motif qu'elle ne disposerait pas de ce pouvoir. Il est peu concevable que la nouvelle Commission nationale puisse exercer son pouvoir d'accès à toutes les données à caractère personnel qui sont traitées et à toutes les informations nécessaires à l'exercice de ses missions si elle n'a pas explicitement le pouvoir d'accès aux locaux. Etant donné que ce pouvoir est prévu textuellement dans le RGPD, il peut difficilement être contenu implicitement parmi les pouvoirs de la Commission nationale dans le cadre du projet de loi de transposition de la Directive.

5. Certification

En matière de certification, le RDPD laisse le soin aux Etats membres de décider quelle entité devra « agréer les certificateurs ». Sous le RGPD cela peut être

soit l'autorité de contrôle, soit un organisme national d'accréditation, voire les deux. Entre l'ILNAS, l'organisme national de standardisation et la CNPD, le législateur propose de donner cette compétence à la Commission nationale.

La Commission nationale accueille favorablement le choix de la désigner comme organisme national compétent pour délivrer les agréments aux organismes de certification visés à l'article 43, paragraphe 1, du règlement (UE) 2016/679.

Non seulement, la CNPD dispose des connaissances nécessaires spécifiques pour pouvoir assurer cette mission, mais la désignation de l'organisme national d'accréditation désigné conformément au règlement (CE) no 765/2008 (ce qui aurait constitué le choix alternatif) comme organisme national compétent pour sa part, aurait limité la marge de manœuvre pour la mise en place de schémas de certifications adaptés aux besoins de la place. En effet, en application de l'article 43, paragraphe 3, du règlement (UE) 2016/679, le fait de désigner compétent l'organisme national d'accréditation limiterait un agrément aux organismes de certification qui sont conformes à la norme EN-ISO/IEC 17065/2012 (i.e. norme pour laquelle l'organisme national d'accréditation est compétent). Or, d'autres référentiels, qui sortent du domaine de compétence de l'organisme national d'accréditation, bien établis sur la place et offrant un niveau de qualité similaire existent (p.ex. la norme internationale ISAE 3000 « Missions d'assurance autres que les missions d'audit ou d'examen d'informations financières historiques »).

La CNPD estime par ailleurs que le choix qui a été fait ne l'empêche pas de faire appel aux compétences de l'organisme national d'accréditation luxembourgeois ou d'un autre État membre. En effet, l'article 43 paragraphe 3, du règlement (UE) 2016/679 laisse à l'autorité de contrôle l'appréciation des critères sur base desquels l'agrément est pris. Ainsi, il est tout à fait possible de retenir pour un schéma de certification donné, comme un critère d'agrément, l'accréditation par un organisme national d'accréditation.

6. Composition et nomination de la CNPD

Afin de pouvoir gérer les compétences élargies de la nouvelle Commission nationale, celle-ci est dirigée par un organe collégial composé de quatre membres, soit un de plus qu'actuellement.

Les membres du collège sont autorisés à porter le titre de « Commissaire ». Cette nouveauté ne change rien à la situation

des membres du collège au Luxembourg, mais elle apporte une clarification dans le cadre de la coopération européenne. Le terme de « commissaire » est définitivement plus compréhensible à l'étranger que celui de « membre effectif », seul titre que les membres effectifs de la Commission nationale ont jusqu'à présent pu porter sans risque de se rendre coupable d'un abus de titre. Par ailleurs, le terme de « Commissaire » est celui communément utilisé dans les pays francophones pour désigner un membre d'une Commission.

Les Commissaires et membres suppléants sont nommés pour un terme de six ans, renouvelable une fois, ce qui constitue un changement par rapport à la loi de 2002 qui en son article 34 ne prévoyait pas de limitation des mandats. Le RGPD en son article 54 paragraphe 1 e) dispose que « *le caractère renouvelable ou non du mandat du ou des membres de chaque autorité de contrôle et, si c'est le cas, le nombre des mandats* » doit être prévu dans une loi nationale. Le principe de la limitation de mandats est très peu répandu parmi les institutions luxembourgeoises et certains États membres qui ont déjà adopté une nouvelle loi organique pour leurs autorités de surveillance, comme l'Autriche[188] se sont bornés à prévoir le caractère renouvelable du mandat de leur(s) commissaires, sans spécifier le nombre de mandats. La question se pose si le RGPD n'admet pas une interprétation plus large que celle que les auteurs du projet de loi luxembourgeois en font et prévoir un mandat renouvelable sans précision du nombre de mandats.

Tandis qu'aujourd'hui la Commission nationale devra comporter au moins un juriste et un informaticien, le profil combiné des membres du Collège devra à l'avenir être tel que soit assurée au sein du collège une expérience professionnelle solide à la fois en matière juridique, en technologies de l'information et des communications, en matière de protection des données et dans le domaine de la prévention, la recherche, la constatation et la poursuite des infractions pénales.

C'est une approche innovante, qui compte tenu de difficultés de cerner des profils spécifiques, indispensables dans une matière aussi complexe que la protection des données, pour des tâches encore peu connues, ne peut-être qu'accueillie favorablement.

7. Les agents de la CNPD

L'article 52 paragraphe 4 du RGPD prévoit que chaque État membre veille à ce que chaque autorité de contrôle dispose des ressources humaines nécessaires à l'exercice effectif de ses missions et de ses pouvoirs, y compris lorsque celle-ci doit agir dans le cadre de l'assistance mutuelle, de la coopération et de la participation au comité.

Afin de garantir l'indépendance des autorités de contrôle, le RGPD prévoit que ces dernières doivent elle-même choisir et disposer de leurs propres agents, qui sont placés sous les ordres exclusifs du ou des membres de l'autorité de contrôle concernée.

L'article 31 apporte une ouverture par rapport aux possibilités de recrutement très rigides prévues par la loi de 2002. À l'avenir la CNPD pourra puiser dans toutes les carrières de l'Etat pour satisfaire ses besoins qui vont au-delà de juristes, d'informaticiens et de rédacteurs.

La question de savoir si la CNPD devrait se doter d'officiers de police judiciaire pour exécuter ses missions d'investigation et d'enquête a été longuement débattue et finalement écartée lorsqu'il se cristallisait que d'un côté, tant le présent projet de loi, que le projet de loi de transposition de la Directive ne comporteraient que très peu de sanctions pénales et que d'autre côté, conférer le statut d'officier de police judiciaire aux agents de la nouvelle CNPD pose un problème par rapport aux exigences d'indépendance des autorités de contrôle nationales alors que les officiers de police judiciaire seraient sous la direction du Parquet et que tous les officiers de police judiciaire

[188] § 20 du Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG).

sont soumis à la surveillance du procureur général.

8. Fonctionnement de la CNPD

La nouvelle CNPD établira son règlement d'ordre intérieur dans le mois de son installation. Le règlement d'ordre interne doit être pris à l'unanimité des membres du collège réuni au complet c'est-à-dire au nombre de quatre.

Elle devra se doter de règles procédurales claires, définir son fonctionnement et prévoir l'organisation de ses services. Ce qui est nouveau par rapport à la loi de 2002, c'est que la nouvelle CNPD doit également déterminer les modalités de convocation de membres et de la tenue des réunions collégiales, dispositions qui étaient auparavant prévues par la loi, ce qui pourtant limitait le Collège dans son organisation. Partant, la Commission nationale accueille favorablement la nouvelle flexibilité à ce sujet.

L'adoption du règlement d'ordre intérieur sera certainement une des décisions qui sera prise par les quatre membres du Collège au complet alors que l'article 36 du projet de loi dispose que le Collège ne peut valablement siéger, ni délibérer qu'à condition de réunir trois membres du collège au moins. Pour les cas où le Collège prendrait des décisions au grand complet, il serait toutefois judicieux de prévoir que la voix du président est prépondérante, ce qui permettrait d'éviter une situation de blocage en cas d'égalité des voix.

Etant donné que beaucoup de décisions qui devront être prises par la nouvelle CNPD seront des décisions d'ouverture et de clôture d'enquête et des décisions relatives à des sanctions dans ce cadre, décisions pour lesquelles le Collège ne peut que siéger en formation restreinte pour préserver le principe de la séparation des pouvoirs, il est judicieux de prévoir que trois membres puissent délibérer valablement alors que le chef d'enquête ne peut pas siéger.

Pour les dossiers ayant trait aux enquêtes, il n'y aura que trois commissaires qui pourront valablement siéger, ce qui permettra également de dégager une majorité des voix en cas de décision. Lorsqu'un ou plusieurs membres effectifs non chef d'enquête sera ou seront empêché(s) pour des raisons personnelles ou de conflit d'intérêt, il(s) pourra ou pourront être remplacés par les membres suppléants.

9. Enquête et décision sur l'issue de l'enquête

Afin de veiller à l'application du RGPD et à contrôler son application de manière cohérente dans l'ensemble de l'Union européenne, les autorités de contrôle devraient avoir, dans

chaque État membre, les mêmes missions et les mêmes pouvoirs effectifs, y compris de pouvoirs d'enquête. C'est l'article 58 du RGPD qui confère ces pouvoirs aux autorités de contrôle, en s'appuyant en partie sur l'article 28, paragraphe 3, de la directive 95/46/CE.

Les auteurs du projet de loi restent sommaires dans l'énoncé des dispositions concernant un domaine qui à l'avenir, avec la disparition des formalités préalables constituera un pilier substantiel du travail de la future Commission nationale. Afin de garantir la prévisibilité du droit applicable, il est indispensable que le Collège de la future Commission nationale adopte un règlement relatif à la procédure applicable aux enquêtes conformément à l'article 5 du projet de loi.

Le projet de loi tend toutefois à régler une question essentielle de procédure liée aux enquêtes, à savoir celle de la séparation des fonctions d'enquête de celles de sanction au sein d'une même entité afin de satisfaire aux critères de l'article 6 § 1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ainsi qu'aux principes d'indépendance et d'impartialité et la nécessité de démontrer une apparence objective de la structure interne de l'autorité de régulation nationale.

Ainsi, le commissaire ayant ordonné l'enquête, ne pourra pas siéger, ni délibérer lorsque le collège décide sur l'issue de l'enquête. Le président pour sa part ne pourra jamais être nommé chef d'enquête.

10. Dispositions financières

La Commission nationale pour la protection des données est une autorité de contrôle indépendante, qui en vertu du paragraphe 4 de l'article 52 du RGPD cité ci-avant, se voit doter par l'Etat des ressources financières nécessaires à l'exercice effectif de ses missions et de ses pouvoirs.

L'article 52 paragraphe 4 précité prévoit que les autorités de contrôle doivent également disposer des ressources humaines et techniques, ainsi que des locaux et de l'infrastructure nécessaires. Etant donné que le projet de loi est muet à ce sujet, il y a lieu de constater que la dotation financière de l'Etat doit être suffisante pour couvrir tous les besoins de la nouvelle Commission nationale.

Il est de la volonté du législateur européen que ce soit l'Etat qui couvre les besoins de l'autorité de contrôle bien qu'il ouvre la possibilité à ces dernières de percevoir des redevances dans le cadre de ses pouvoirs d'autorisation et de consultation en vertu de l'article 58, paragraphe 3, du RGPD. Bien évidemment, ces redevances ne peuvent pas être perçues auprès de la personne concernée et, le cas échéant, du délégué à la protection des données dans le cadre de ses missions, alors que pour eux, l'accomplissement des missions des autorités de contrôles est gratuit. Le projet de loi sous avis dans son article 13 rappelle ce principe de gratuité introduit par l'article 57 paragraphe 3 du RGPD. Par contre, rien empêche de percevoir des redevances de la part des responsables de traitements et sous-traitants, pourvu que le montant des redevances soit prévisible. Un règlement de la CNPD devra par conséquent les prévoir.

La vocation de la CNPD n'étant toutefois pas commerciale et son activité n'étant pas commerciale et ne pouvant pas être comparée à une activité commerciale, les redevances ne sont pas destinées à financer la CNPD. Bien que le coût de revient peut être un élément dans la détermination du montant, il ne doit pas nécessairement l'être.

Il en est différent des paiements que la CNPD peut réclamer en vertu de l'article 13 du projet de loi lorsqu'une demande est manifestement infondée ou excessive. La CNPD peut alors exiger le paiement de frais raisonnables basés sur ses coûts administratifs ou refuser de donner suite à la demande.

Il peut y avoir d'autres cas, comme par exemple dans le cadre de la coopération avec des partenaires pour l'exécution de projets communs, que la CNPD pourra être amenée à percevoir des fonds pour lesquels elle devra tenir une comptabilité. Cette situation est couverte par l'article 48 paragraphe 2 du projet de loi.

11. Sanctions

a) Amendes administratives

Une des nouveautés du RGPD consiste dans la flexibilité laissée aux responsables de traitement et sous-traitants à organiser eux-mêmes leur conformité au nouveau règlement. En contrepartie de cette flexibilité, toute violation aux dispositions de ce règlement peut entraîner des sanctions administratives financières qui sont « effectives, proportionnées et dissuasives ». Le RGPD confère en effet à la CNPD une nouveau pouvoir de sanction, à savoir d'imposer des amendes administratives.

Vu la spécificité des décisions prises par la CNPD, la Commission nationale conseille de régler toute la procédure liée à l'exécution de ces décisions, dont notamment pour ce qui est des astreintes, dans le présent projet de loi à l'instar de la loi du 23 octobre 2011 relative à la concurrence au lieu de se référer aux articles 2059 à 2066 du Code civil.

Pour ce qui est du recouvrement des amendes administratives et astreintes, l'article 51 du projet de loi donne compétence à l'Administration de l'Enregistrement et des Domaines pour ce qui est des sanctions prononcées à l'égard des personnes physiques et morales de droit privé. La Commission nationale se pose la question de savoir quelle procédure s'applique au recouvrement des amendes administratives et astreintes prononcées à l'égard des personnes morales de droit public, pourtant bel et bien visées par l'article 49 du projet de loi.

b) Sanctions pénales

Sous le régime actuel de la loi modifiée du 2 août 2002, les violations des règles en matière de protection des données peuvent surtout être sanctionnées pénalement, la CNPD ne disposant que du pouvoir d'imposer des sanctions administratives, mais non financières.

La loi de 2002 contient en effet pas moins de dix-huit infractions pénales, qui constituent toutes des infractions sui generis et ne figurent pas dans le Code pénal. Le projet loi sous examen se propose d'abroger toutes ces infractions pénales et se limite à n'en conserver qu'une seule, à savoir le délit d'entrave à l'accomplissement des missions de la CNPD, prévu à l'article 53 du projet de loi.

Compte tenu de l'importance des amendes administratives que la CNPD pourra, à l'avenir, imposer en cas de violation du RGPD, nous pouvons entièrement souscrire au choix des auteurs du projet de loi de réduire au maximum les infractions pénales.

Toutefois, il importe de relever que les amendes administratives prévues à l'article 83 du RGPD, peuvent seulement être infligées à l'égard d'un responsable du traitement ou d'un sous-traitant, c'est-à-dire à l'égard de personnes morales privées ou publiques, sauf dans les très rares cas où le responsable du traitement ou le sous-traitant serait une personne physique qui exerce son commerce en nom personnel.

Force est donc de constater que le système des sanctions repose uniquement sur une logique de faire supporter toute la charge des sanctions par les responsables du traitement ou sous-traitants personnes morales, tandis que les personnes physiques qui violent délibérément le RGPD profitent d'une impunité.

Il est vrai que pratiquement toutes les obligations en matière de protection des personnes reposent sur les responsables de traitements ou sous-traitants et qu'il leur incombe de mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires pour garantir la sécurité et la confidentialité des données. Toujours est-il que même si toutes les mesures imaginables et conformes à l'état de l'art, sont prises, un responsable du traitement ou sous-traitant ne pourra jamais éviter ou exclure que des individus malintentionnés font un usage abusif des données auxquelles ils ont accès dans le cadre de leurs activités.

L'expérience acquise par la CNPD, après quinze ans d'existence, montre que ces cas d'abus de données par des personnes physiques ne sont pas rares, eu égard au nombre important de plaintes de ce genre dont la CNPD a été saisie.

Ainsi p.ex. lorsqu'un salarié ou un agent public utilise abusivement des données auxquelles il a accès dans le cadre de son travail à des fins privées et dans l'intention de nuire à un tiers, la CNPD pourra constater qu'il y a eu violation du RGPD et imposer une amende administrative à l'employeur, responsable du traitement des données ; or, le salarié ne pourra pas faire l'objet de sanction, à l'exception de sanctions disciplinaires infligées par l'employeur.

Ceci n'est bien entendu pas satisfaisant pour une victime d'un usage abusif de ses données qui aura subi un dommage matériel ou moral et qui aura le sentiment que l'Etat accepte que les agissements de l'auteur des faits restent impunis, alors que l'auteur ne pourra pas être poursuivi pénalement. La victime ne pourra pas faire valoir ses droits elle-même, à moins qu'elle n'engage une action judiciaire en matière civile coûteuse.

L'article 84 paragraphe 1 du RGPD prévoit que « Les États membres déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre. Ces sanctions sont effectives, proportionnées et dissuasives. » Le considérant (149) y afférent énonce à ce titre que « *Les États membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violation du présent règlement, y compris de violation des dispositions nationales adoptées en application et dans les limites du présent règlement. Ces sanctions pénales peuvent aussi permettre la saisie des profits réalisés en violation du présent règlement. Toutefois, l'application de sanctions pénales en cas de violation de ces dispositions nationales et l'application de sanctions administratives ne devrait pas entraîner la violation du principe ne bis in idem tel qu'il a été interprété par la Cour de justice* ».

La dualité du régime de sanction des violations du RGPD peut

donc être prévu par les États membres et tant l'Autriche, que l'Allemagne font usage de cette possibilité dans leurs lois d'adaptation respectives, tout comme la France dans son projet de loi d'adaptation, par lequel elle n'abroge pas les sanctions pénales existantes, et comme la Belgique a l'intention de le faire dans son projet de loi portant exécution du RGPD.

Partant, afin de ne pas laisser impunis des agissements illicites perpétrés par des personnes physiques, que ce soit dans le cadre de traitements de données visées par le présent projet de loi ou du projet de loi 7168, la Commission nationale estime indispensable que le projet de loi érige en infraction pénale :

- le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite ou par des manœuvres trompeuses,

- le fait de vendre les données à caractère personnel obtenues par les moyens précités et

- le fait, par une personne qui a recueillie, à l'occasion de l'enregistrement, du classement, de la transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir (c'est-à-dire un détournement de finalité).

Dans le cas où il serait tenu compte des suggestions de la CNPD, l'infraction nouvellement créée devrait être ajoutée à l'article 49 du projet de loi 7168.

c) L'action en cessation

L'article 52 du projet de loi prévoit l'action en cessation qui est actuellement déjà prévue à l'article 39 de la loi modifiée du 2 août 2002. La CNPD salue les modifications et ajustements apportés par les auteurs du projet de loi à cette procédure, alors qu'elle aura désormais la possibilité de porter une requête devant le président du tribunal d'arrondissement de Luxembourg-Ville sans devoir attendre l'expiration du délai d'un recours ou la confirmation de sa décision par une juridiction. En effet, en raison de l'attente d'expiration des prédits délais, la procédure actuelle de l'action en cessation peut, le cas échéant, seulement être entamée par la CNPD après un délai d'attente de deux à trois ans. Ceci est peu effectif pour une action qui est censée être jugée comme en matière de référé.

Les auteurs du projet de loi énoncent dans le commentaire de l'article 52 que l'action y prévue

permettra à la CNPD de faire assurer l'exécution de ses décisions, non respectées par un responsable du traitement, par une juridiction. Or, si l'article 39 de la loi de 2002 permet au président du tribunal d'arrondissement d'ordonner la cessation d'un traitement de données contraires à la loi, l'article 52 du projet de loi lui permet seulement d'ordonner la suspension provisoire d'un traitement de données contraire au RGPD.

L'article 52 du projet de loi soulève donc toujours des questions quant à l'effectivité et l'utilité de cette action, dans la mesure où une cessation du traitement telle qu'actuellement prévu à l'article 39 paragraphe (1) ne peut pas être ordonnée et que la suspension provisoire du traitement de données, ordonnée par le président du tribunal d'arrondissement, prend fin au plus tard à l'expiration d'un délai de deux ans à partir de la décision initiale de suspension provisoire en vertu du paragraphe (4) de l'article 52.

Cela signifie-t-il qu'un responsable du traitement, ayant violé le RGPD et qui fait l'objet d'une décision de suspension provisoire d'un traitement de données, pourrait recommencer avec le même traitement de données, pourtant illégal, après un délai d'attente de deux ans ?

Ou, l'action étant jugée comme en matière de référé, faut-il comprendre que la CNPD devrait en plus intenter une action judiciaire au fond et dans l'affirmative, devant quel juge ?

L'article 52 mériterait donc d'être précisé eu égard aux questions ci-avant posées.

Il serait également utile de prévoir les modalités sous lesquelles la future CNPD sera autorisée à publier des décisions rendues dans un but dissuasif tel qu'il est déjà prévu en tant que sanction disciplinaire par la loi de 2002 en son article 33 paragraphe 1 (d) qui dispose que la CNPD peut « ordonner l'insertion intégrale ou par extraits de la décision d'interdiction par la voie des journaux ou de toute autre manière, aux frais de la personne sanctionnée. » L'article 58 paragraphe 6 du RGPD autorise en effet les États membres à prévoir des pouvoirs additionnels pour son autorité de contrôle.

12. Autres dispositions

a) Disposition modificative

Une conséquence de l'approche des auteurs du présent projet de loi et de la loi de transposition de la Directive d'avoir opté pour une loi générale et une loi spéciale séparée, est la complexité du changement des références à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel dans toute la législation comportant une telle référence.

Si le présent projet de loi devra toujours être mentionné, la mention de la future loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale, ainsi qu'en matière de sécurité nationale et celle du règlement (UE) 2016/679 doit être appréciée au cas par cas et la solution retenue ne facilitera pas la lecture de la législation applicable en matière de protection des données personnelles.

b) Disposition abrogatoire

Afin d'assurer le respect des dispositions du règlement (UE) 2016/679, une abrogation de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel est inévitable.

Il s'avère qu'un grand nombre de décisions avaient été prises au cours des 15 dernières années sur base de cette loi. Etant donné que le projet de loi ne prévoit rien quant à leur valeur juridique, il y a lieu de présumer que ces actes perdent leur valeur à la date d'abrogation de la loi de 2002, c'est-à-dire à partir du 25 mai 2018.

Annexes

Dans un souci de sécurité juridique, la CNPD estime nécessaire de prévoir clairement le sort des décisions prises sur base de la loi modifiée du 2 août 2002. Le projet belge prévoit que les autorisations accordées antérieurement gardent leur valeur juridique, sans préjudice des contrôles de la nouvelle autorité.

Pour autant qu'ils ne soient pas contraires aux dispositions de la future loi et du RGPD, la Commission nationale suggère de prévoir p.ex. que les autorisations délivrées sur base des articles 14 et 19 de la loi de 2002 resteraient en vigueur pour une durée de 3 ans, à titre de période transitoire, sans préjudice des pouvoirs de contrôle de la nouvelle CNPD. Pour le surplus, il y a encore lieu de prévoir que les procédures de traitement de demandes d'autorisation en cours introduites avant le 25 mai 2018 sont arrêtées de plein droit.

Pour ce qui est des agréments délivrés aux actuels chargés de la protection des données, sur base de l'article 40 de la loi de 2002, la Commission nationale considère comme nécessaire de prévoir expressément que ces agréments sont abrogés ou annulés à compter de la date d'entrée en vigueur de la loi en projet et au plus tard à partir du 25 mai 2018, pour éviter que des intéressés profitent d'un statut qui n'existera plus.

Conformément aux articles 37 à 39 du RGPD, relatifs au régime du délégué à la protection des données, l'identité du délégué à la protection des données sera dorénavant simplement communiquée à la CNPD, sans obligation de publicité et sans procédure d'agrément ou de certification quelconque. En effet, la loi de 2002 prévoit un régime applicable au chargé de la protection des données qui est purement national, mais qui ne sera plus compatible avec les dispositions du RGPD.

c) Dispositions transitoires

L'article 64 prévoit que la durée du mandat des membres du collège nommés avant l'entrée en vigueur du projet de loi sous avis est calculée à partir de la date de nomination de leur mandat en cours lors de l'entrée en vigueur de cette loi. Cette disposition garantit le maintien des droits acquis pour les membres effectifs en fonction à la CNPD actuelle.

Il ne ressort pas explicitement des articles 64 à 67 s'ils s'appliquent aux seuls membres effectifs ou également aux membres suppléants, ce qui ne semble toutefois pas être le cas pour les articles 65 à 67. Pour des raisons de prévisibilité de la loi, il serait prudent de préciser explicitement les catégories de personnes concernées par les articles concernés.

Pour le cas où ces mêmes membres effectifs devraient voir leur mandat renouvelé sous la nouvelle loi, ils risquent de perdre le bénéfice des dispositions des articles 65 et 66 qui pourtant visent à préserver leurs droits acquis. En effet, alors que les articles 64 à 66 visent les membres nommés « avant l'entrée en vigueur de la présente loi », un renouvellement du mandat, c'est-à-dire une nouvelle nomination, pourrait être interprétée comme intervenant sous la nouvelle loi et tombant sous la procédure de l'art 20 de la nouvelle loi.

Afin de renforcer la prévisibilité de la loi pour les intéressés et garantir leurs droits acquis sous la loi actuellement en vigueur, il y a lieu d'ajouter « *nommés pour la première fois avant l'entrée en vigueur de la présente loi* » aux articles 65 et 66. Cet ajout permettrait d'assurer que les membres effectifs actuellement en fonction ne subissent pas une dégradation de leur situation personnelle sans en avoir été informé avant d'accéder à leur fonction sous la loi 2002.

B Quant à la législation nationale complémentaire

1. Remarque générale

La Commission nationale salue l'effort des auteurs de la loi de concilier les intérêts tant des responsables de traitement et sous-traitants que des personnes intéressées dans ce projet de loi élancé, qui dans l'esprit d'harmonisation des législations européennes propagé par le RGPD, limite les dispositions spécifiques nationales à un minium.

2. Champ d'application des dispositions spécifiques

Le champ d'application des dispositions spécifiques du Chapitre 2 est défini dans l'article 55 du projet de loi de la manière suivante : *« Les dispositions du présent chapitre s'appliquent aux responsables du traitement et aux sous-traitants établis sur le territoire luxembourgeois ».* Dans le cas où un sous-traitant établi sur le territoire luxembourgeois agit pour le compte et sur instruction d'un responsable du traitement situé en dehors du Luxembourg, il n'est pas clair si ces mesures devront s'appliquer. En effet, l'application de ces mesures aux sous-traitants n'est pas mentionnée dans l'article.

La CNPD estime par ailleurs que dans le cas contraire, un responsable du traitement établi au Luxembourg qui fait appel à un sous-traitant établi hors Luxembourg devra aussi « assurer » que les mesures additionnelles mentionnées à l'article 58 du projet de loi soient appliquées (cf. commentaire ci-dessous).

3. Traitement à des fins de recherche scientifique ou historique ou à des fins statistiques

Les articles 57 et 58 du projet de loi limitent les droits des personnes concernées prévus aux articles 15, 16, 18 et 21 du règlement (UE) 2016/679, en conformité avec l'article 89, paragraphe 2, du règlement (UE) 2016/679 moyennant des garanties appropriées. Il y a lieu de constater que les articles 57 et 58 ne couvrent pas les traitements de données à des fins archivistiques dans l'intérêt public tel que le permet pourtant l'article 89 du RGPD. Se pose la question si ces traitements de données ont été exclus intentionnellement par les auteurs du projet de loi ? Le commentaire des articles reste muet sur cette question. La CNPD est donc à se demander si des dérogations ou limitations aux droits des personnes concernées seront, le cas échéant, spécifiquement prévues dans le cadre du projet de loi N°6913 relatif à l'archivage. Si tel n'était pas le cas, la CNPD donne à considérer que le RGPD s'appliquera aux traitements de données à des fins archivistiques dans l'intérêt public avec toutes les conséquences que cela implique.

La formulation actuelle de l'article 58 stipule que « le responsable d'un traitement » … « doit mettre en œuvre des mesures

appropriées additionnelles ». Or, dans de très nombreux cas, les projets de recherche impliquent un ou plusieurs sous-traitants. La CNPD estime qu'il incombe au responsable du traitement de données de garantir que ces mesures soient mises en place dans les relations contractuelles obligatoires avec le sous-traitant suivant l'article 28 paragraphe (3) du RGPD – ce qui ne signifie pas nécessairement que c'est au responsable de traitement de les mettre en place lui-même. Aussi la CNPD estime que la documentation à laquelle est fait référence au dernier alinéa devra comprendre une analyse au cas par cas pour déterminer quelles mesures s'appliquent au responsable du traitement et quelles mesures s'appliquent au sous-traitant.

4. Traitement de catégories particulières de données à caractère personnel par les services de la santé

La section IV comportant un seul article porte le titre « *Traitement de catégories particulières de données à caractère personnel par les services de la santé* ». Comme l'indique le commentaire des articles, l'article 59 est une copie avec quelques ajustements de l'actuel article 7 de la loi modifiée du 2 août 2002.

Si l'article 7 de la loi de 2002 se limitait à réglementer les traitements de données relatives à la santé et à la vie sexuelle par les services de santé, la CNPD s'étonne que l'article 59 du projet de loi couvre dorénavant l'ensemble des catégories particulières de données, données dites « sensibles » visés à l'article 9 paragraphe 1 du RGPD, à savoir :

- les données qui révèlent l'origine raciale ou ethnique,
- les opinions politiques,
- les convictions religieuses ou philosophiques,
- l'appartenance syndicale,
- les données biométriques aux fins d'identifier une personne physique de manière unique,
- les données concernant la santé,
- les données concernant la vie sexuelle ou l'orientation sexuelle,
- les données génétiques.

Se pose d'abord la question pourquoi un service de santé - notion qui n'est d'ailleurs pas définie - serait amené à traiter p.ex. des données relatives aux opinions politiques ou à l'appartenance syndicale.
Ensuite, la CNPD s'interroge surtout sur la raison d'être de l'article 59. En effet, si l'article 7 de la loi modifiée du 2 août 2002 doit être lu dans une

logique de transposition d'une directive en droit national, en l'occurrence la directive 95/46/CE, il en est autrement s'agissant d'un règlement européen qui s'applique directement dans les Etats membres, sans mesures de transposition. Ainsi, l'article 9 paragraphe 2 lettre h) du RGPD constitue la base juridique (directement applicable en droit national) pour légitimer les traitements de données visés aux paragraphes (1), (3) et (4) dernière phrase de l'article 59 du projet de loi, de sorte que ces dispositions apparaissent superflues et qu'elles peuvent être supprimées du projet de loi.

Pour ce qui est du paragraphe (3) de l'article 59 plus particulièrement, la CNPD se demande en outre pourquoi les entreprises d'assurances, les sociétés gérant les fonds de pension et la Caisse médico-chirurgicale mutualiste (CMCM) y sont énumérées. Ces trois catégories d'organisme peuvent-elles raisonnablement être assimilées à des services de santé ? Enfin, l'on peut aussi se poser la question pourquoi un texte de loi privilégie une société de secours mutuels particulière par rapport à d'autres sociétés de secours mutuels luxembourgeoises. Ces interrogations valent tout aussi bien pour ce qui est de l'actuel article 7 de la loi de 2002.

Le paragraphe (2) de l'article 59 du projet de loi vise les traitements de catégories particulières de données à des fins de recherche. De l'avis de la CNPD ce paragraphe aurait plutôt sa place dans la section III (articles 57 et 58 du projet de loi), alors que celle-ci réglemente plus précisément les traitements de données à des fins de recherches.

Le paragraphe (4) de l'article 59 du projet de loi sous avis est aussi reprise de l'actuel article 7 de la loi de 2002. Cette disposition en projet tout comme l'article 7(4) de la loi de 2002 font référence à un règlement grand-ducal obligatoire qui devrait préciser les modalités et les conditions suivant lesquelles des données « sensibles » peuvent être communiquées à des tiers ou utilisées à des fins de recherche, ce qui correspond en quelque sorte aux « *mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* » visées à l'article 9 paragraphe 2 lettre j) du RGPD respectivement introduites à l'article 58 du projet de loi. Or, soulignons que jusqu'à ce jour, soit 15 ans après l'entrée en vigueur de la loi modifiée du 2 août 2002, un tel règlement grand-ducal n'a pas été adopté. Un projet de règlement n'a par ailleurs pas été soumis pour avis ensemble avec le projet de loi sous examen. Ceci dit, la CNPD estime que les modalités et les conditions à déterminer par règlement grand-ducal, devraient être précisés dans la loi et non pas dans un règlement grand-ducal, alors que le droit à la protection des données et à la vie privée, s'agissant d'un droit fondamental, est une matière réservée à la loi par la Constitution. A ce titre, il convient de rappeler l'exigence de la Cour constitutionnelle selon laquelle « *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.* »[189]

En ce qui concerne la mention de l'utilisation des données « sensibles » à des fins de recherche dans le paragraphe (4) de l'article 59, se pose à nouveau la question de l'agencement et de la cohérence de cette disposition avec celle des articles 57 et 58 du projet de loi.

Enfin, la CNPD regrette et se soucie que le projet de loi ne prévoit pas de règles spécifiques relatives aux traitements des données génétiques. La loi modifiée du 2 août 2002 prévoit actuellement en son article 6 paragraphe (3) un encadrement très strict pour la collecte et l'utilisation des données génétiques. La CNPD souligne que ces données sont les plus sensibles qui soient et méritent

[189] Arrêt 117 de la Cour constitutionnelle du 20 mars 2015.

une protection et encadrement législatif encore plus stricte que les autres données « sensibles ». Tel a aussi été l'avis du législateur en 2002.

L'article 9 paragraphe 4 du RGPD prévoit d'ailleurs expressément que *« Les Etats membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé ».*

En conclusion, la CNPD recommande fortement qu'un encadrement spécifique des données génétiques soit prévu dans la loi, afin de ne pas en abaisser le niveau de protection actuel. Elle suggère par ailleurs de supprimer les paragraphes (1), (3) et (4) dernière phrase de l'article 59 et d'intégrer les dispositions du paragraphe (2) et paragraphe (4) première phrase de l'article 59 dans la section III du projet de loi sous avis.

C Remarque générale

La Commission nationale regrette que les règlements d'exécution prévues dans le projet de loi n'aient pas été déposées avec loi, voire qu'ils ne lui ont pas été communiqués. Elle n'a par conséquent pas été en mesure de se prononcer à cet égard.

Ainsi décidé à Esch-sur-Alzette en date du 28 décembre 2017.

La Commission nationale pour la protection des données

Tine A. Larsen
Présidente

Thierry Lallemang
Membre effectif

Christophe Buschmann
Membre effectif

Participations aux travaux européens

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

Document	Date d'adoption	Référence
Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679	03.10.2018	WP 253
Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)	04.10.2017	WP 252
Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679	03.10.2017	WP 251
Guidelines on Personal data breach notification under Regulation 2016/679	03.10.2017	WP 250
Opinion 2/2017 on data processing at work	08.06.2017	WP 249
Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679	04.10.2017	WP 248
Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)	04.04.2017	WP 247
EU-US PRIVACY SHIELD F.A.Q. FOR EUROPEAN INDIVIDUALS	13.12.2016	WP 246
EU-US PRIVACY SHIELD F.A.Q. FOR EUROPEAN BUSINESSES	13.12.2016	WP 245
Guidelines for identifying a controller or processor's lead supervisory authority	05.04.2017	WP 244
Guidelines on Data Protection Officers ('DPOs')	05.04.2017	WP 243
Guidelines on the right to data portability	05.04.2017	WP 242

Tous les documents de travail du groupe de travail « Article 29 » peuvent être téléchargés sur Internet[190].

[190] http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

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